УДК 512.7+519.6
ББК 22.14+22.19
К55

Кокс Д., Литтл Дж., О'Ши Д.

К55 Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры: Пер. с англ. — М.: Мир, 2000. — 687 с., ил.

ISBN 5-03-003320-3

Монография известных американских математиков посвящена изложению результатов бурно развивающейся области, связанной с алгоритмами, превращающими базисные понятия коммутативной алгебры и алгебраической геометрии из абстрактно-теоретических в конкретно вычислимые. Обсуждение алгоритмов основывается на обобщении алгоритма деления для полиномов от одной переменной, найденном лишь в шестидесятых годах. Эти алгоритмы в соединении с мощью быстрых компьютеров привели к некоторым интересным приложениям — например, в роботике и в доказательстве геометрических теорем.

Для математиков-теоретиков, специалистов по компьютерной технике и инженеров, а также для студентов соответствующих специальностей.

ББК 22.14+22.19

РФФИ

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту № 98-01-14096

Редакция литературы по математическим наукам

Original published in English under the title: Ideals, Varieties, and Algorithms by David Cox, John Little, and Donal O'Shea
Copyright © 1997, 1992 Springer-Verlag New York, Inc. All Rights Reserved.
© перевод на русский язык, «Мир», 2000

ISBN 5-03-003320-3 (русск.)
ISBN 0-387-94680-2 (англ.)

Предисловие к русскому изданию

Перед читателем книга, посвященная началам алгебраической геометрии и коммутативной алгебры. Она предполагает лишь скромное знание алгебры в объеме базисного университетского курса первых двух лет обучения (и даже меньше: например, в гл. 7 не предполагается даже знания основ теории групп). И, тем не менее, книга наверняка окажется полезной и интересной не только для начинающих, но и для искушенных читателей. Дело в том, что в ней рассматриваются естественные вопросы, которые, с одной стороны, сразу возникают при изучении предмета, а с другой, ранее не освещались в литературе на русском языке. Речь идет о способах явного нахождения объектов, существование которых устанавливается в ключевых утверждениях теории. Как найти конечный базис идеала в кольце полиномов? Как найти конечный базис его радикала? Как найти уравнения, задающие образ проективного алгебраического многообразия при регулярном отображении? Эти и подобные вопросы являются центральными в книге, определяя и выбор доказательств фундаментальных фактов теории. Ответы на них удается получить за счет объединения классических методов, в последние десятилетия ушедших в тень (теории исключения), и современных идей, основанных на теории базисов Грёбнера. Наличие в настоящее время мощных пакетов компьютерной алгебры делает такое изложение и саму книгу полезной и чисто практически: с их помощью читатель может получить явные ответы в конкретных интересующих его случаях. Для начинающих изучать алгебраическую геометрию и коммутативную алгебру последнее является важным методическим достоинством, опуская абстрактную теорию down to earth и позволяя все «потрогать» своими руками. Этому же способствуют и многочисленные упражнения. Среди англоязычных читателей эта книга, первое издание которой появилось в 1992 г., устойчиво пользуется хорошей репутацией и стала для многих настольной. Теперь она станет доступной и для русскоязычных читателей, встав в ряд с другими замечательными книгами по алгебраической геометрии и коммутативной алгебре, переведенными на русский язык.

В. Л. Попов

- Бернду Штурмфелсу, чья книга STURMFELS (1993) послужила для нас источником вдохновения при написании гл. 7.

Также надо упомянуть читателей, обнаруживших многочисленные опечатки и приславших свое мнение о книге. Мы благодарны всем вам!

Мы (как и в первом издании) будем признательны за замечания и предложения. Мы готовы платить $ 1 за каждую найденную опечатку.

Октябрь 1996 г.

Дэвид Кокс,
Джон Литтл,
Донал О'Ши.

1

Геометрия, алгебра и алгоритмы

В этой главе вводятся некоторые из основных тем книги. Под геометрией мы здесь понимаем геометрию ***аффинных многообразий***, которые являются кривыми и поверхностями (а также объектами более высокой размерности), задаваемыми полиномами. Понимание теории аффинных многообразий требует знания некоторых разделов алгебры, в частности теории *идеалов* в кольцах полиномов $k[x_1, \ldots, k_n]$. Наконец, мы рассмотрим полиномы от одной переменной, чтобы проиллюстрировать роль *алгоритмов*.

§ 1. Полиномы и аффинное пространство

Чтобы установить связь между алгеброй и геометрией, мы будем изучать полиномы с коэффициентами из некоторого поля. Мы все знаем, что такое полином, но термин *поле* может быть незнаком некоторым читателям. Интуитивно поле — это множество, на котором заданы операции сложения, вычитания, умножения и деления с обычными свойствами. Множества вещественных чисел $\mathbb{R}$ и комплексных чисел $\mathbb{C}$ — обычные примеры полей, в то время как множество целых чисел $\mathbb{Z}$ полем не является — в нем не определено деление (3 и 2 — целые числа, а их частное $3/2$ — нет). Формальное определение поля дано в приложении A.

Одной из причин важности понятия поля является то, что определения и утверждения линейной алгебры справедливы над *любым* полем: если скаляры в вашем курсе линейной алгебры были из $\mathbb{R}$ или из $\mathbb{C}$, то большинство теорем и методов, которые вы изучали, применимо для произвольного поля k. В этой книге разные поля будут использоваться в разных целях. Наиболее часто нам будут встречаться следующие поля:

- поле рациональных чисел $\mathbb{Q}$: большая часть наших примеров компьютерных вычислений использует это поле;
- поле вещественных чисел $\mathbb{R}$: это поле используется, чтобы рисовать кривые и поверхности;

- поле комплексных чисел $\mathbb{C}$: многие теоремы в книге справедливы именно в этом поле.

Иногда мы будем встречать и другие поля, как, например, поле рациональных функций (оно будет определено позже). Существует также очень интересная теория конечных полей — один из простейших примеров этих полей появится в упражнениях.

Теперь мы можем дать определение полинома. Читатель, конечно, знаком с полиномами от одной или двух переменных, но мы будем рассматривать полиномы от n переменных $x_1, \ldots, x_n$ с коэффициентами из произвольного поля k. Сначала мы дадим определение монома.

Определение 1. *Мономом* от переменных $x_1, \ldots, x_n$ называется произведение вида

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n},$$

где показатели степеней $\alpha_1, \ldots, \alpha_n$ — неотрицательные целые числа. *Полной степенью* монома называется сумма $\alpha_1 + \ldots + \alpha_n$.

Мы будем использовать следующие упрощенные обозначения для мономов. Пусть $\alpha = (\alpha_1, \ldots, \alpha_n)$ — набор n неотрицательных целых чисел. Положим

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n}.$$

Отметим, что если $\alpha = (0, \ldots, 0)$, то $x^\alpha = 1$. Через $|\alpha| = \alpha_1 + \cdots + \alpha_n$ мы будем обозначать полную степень монома x^α.

Определение 2. *Полиномом* f от переменных $x_1, \ldots, x_n$ с коэффициентами из k называется конечная линейная комбинация мономов (с коэффициентами из k). Полином f будет записываться в виде

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in k,$$

где суммирование проводится по конечному множеству наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$. Множество всех полиномов от переменных $x_1, \ldots, x_n$ с коэффициентами из k обозначается $k[x_1, \ldots, x_n]$.

Когда мы будем работать с полиномами от малого количества переменных, то обычно будем обходиться без индексов. Так, полиномы от одной, двух или трех переменных принадлежат множествам $k[x]$, $k[x, y]$ и $k[x, y, z]$ соответственно. Например,

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$$

является полиномом из $\mathbb{Q}[x, y, z]$. Как правило, мы будем использовать для обозначения полиномов буквы f, g, h, p, q, r.

При работе с полиномами будут использоваться следующие термины.

Определение 3. Пусть $f = \sum_\alpha a_\alpha x^\alpha$ — полином из $k[x_1, \ldots, x_n]$.

(i) a_α называется *коэффициентом* монома x^α.

(ii) Если $a_\alpha \neq 0$, то $a_\alpha x^\alpha$ называется *членом* полинома f.

(iii) *Полной степенью* полинома f, обозначаемой $\deg(f)$, называется максимум степеней $|\alpha|$ по всем мономам с ненулевыми коэффициентами a_α.

Например, полином $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$, выписанный выше, содержит четыре члена и имеет полную степень шесть. Отметим, что f содержит два члена максимальной степени, что невозможно в случае полинома от одной переменной. В гл. 2 мы узнаем, как ввести *порядок* на множестве членов полинома.

Сумма и произведение двух полиномов являются полиномами. Мы говорим, что полином f *делит* полином g, если $g = fh$ для некоторого полинома $h \in k[x_1, \ldots, x_n]$.

Легко доказать, что операции сложения и умножения на множестве $k[x_1, \ldots, x_n]$ удовлетворяют всем аксиомам поля, за исключением аксиомы существования обратного элемента по умножению ($1/x_1$, например, не является полиномом). Такая структура называется коммутативным кольцом (в приложении A дано строгое определение), и по этой причине мы будем называть $k[x_1, \ldots, x_n]$ *кольцом полиномов* или *полиномиальным кольцом*.

Определение 4. Пусть дано поле k и натуральное число n; тогда n-мерным *аффинным пространством* над k называется множество

$$k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}.$$

Пусть, например, $k = \mathbb{R}$. Пространство $\mathbb{R}^n$ — объект, знакомый из курсов математического анализа и линейной алгебры. Отметим также, что $k^1 = k$ называется *аффинной прямой*, а k^2 — *аффинной плоскостью*.

Рассмотрим теперь связь между полиномами и аффинными пространствами. Основным здесь является тот факт, что полином $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ задает функцию

$$f : k^n \to k,$$

определенную следующим образом. Пусть $(a_1, \ldots, a_n) \in k^n$. В формуле, определяющей f, заменим каждое x_i на a_i. Так как коэффициенты принадлежат k, то эта операция дает элемент $f(a_1, \ldots, a_n) \in k$. Возможность рассматривать полином как функцию и определяет связь между алгеброй и геометрией.

Двойная природа полинома приводит к некоторым неожиданным следствиям. Например, вопрос «верно ли, что $f = 0$?» допускает два истолкования: «является ли f нулевым полиномом?», т. е. верно ли, что все коэффициенты a_α равны нулю, или «является ли f нулевой функцией?», т. е. верно ли, что $f(a_1, \ldots, a_n) = 0$ для всех $(a_1, \ldots, a_n) \in k^n$. Удивительно, но эти два утверждения в общем случае не эквивалентны! Рассмотрим, например, множество из двух элементов 0 и 1. В упражнениях мы увидим, что это множество можно сделать полем, в котором $1+1=0$. Это поле обычно обозначается $\mathbb{F}_2$. Теперь рассмотрим полином $x^2 - x = x(x-1) \in \mathbb{F}_2[x]$. Так как этот полином обращается в нуль в точках 0 и 1, то он дает пример ненулевого полинома, являющегося нулевой функцией на аффинном пространстве $\mathbb{F}_2^1$. Другие примеры будут рассмотрены в упражнениях[1)].

Однако если k бесконечно, то никаких проблем не возникает.

Предложение 5. *Пусть k — бесконечное поле и $f \in k[x_1, \ldots, x_n]$. Тогда $f = 0$ в $k[x_1, \ldots, x_n]$ в том и только том случае, когда $f : k^n \to k$ является нулевой функцией.*

Доказательство. В одну сторону утверждение очевидно, так как нулевой полином определяет нулевую функцию. Рассмотрим обратное утверждение. Нам нужно доказать, что если $f(a_1, \ldots, a_n) = 0$ для всех $(a_1, \ldots, a_n) \in k^n$, то f — нулевой полином. Доказательство использует индукцию по числу переменных n.

Пусть $n = 1$. Хорошо известно, что ненулевой полином из $k[x]$ степени m имеет не более m различных корней (этот факт будет доказан в следствии 3 в § 5). Пусть $f \in k[x]$ и $f(a) = 0$ для всех $a \in k$. Так как k бесконечно, то f имеет бесконечно много корней; следовательно, f — нулевой полином.

Пусть теперь обратное утверждение справедливо для $n-1$, и пусть $f \in k[x_1, \ldots, x_n]$ — полином, обращающийся в нуль во всех точках из k^n. Объединяя члены по степеням переменной x_n, запишем f в следующем виде:

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

где $g_i \in k[x_1, \ldots, x_{n-1}]$. Мы покажем, что каждый полином g_i — нулевой полином от $n-1$ переменных, откуда будет следовать, что f — нулевой полином из $k[x_1, \ldots, x_n]$.

[1)] Если поле k конечно, то и множество k^n конечно. Поэтому в этом случае множество всех функций $f : k^n \to k$ тоже конечно. С другой стороны, множество $k[x_1, \ldots, x_n]$ бесконечно. Отсюда следует, что эти утверждения неэквивалентны ни для какого конечного поля k.— *Прим. ред.*

Если мы зафиксируем $(a_1, \ldots, a_{n-1}) \in k^{n-1}$, то получим полином $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ от одной переменной. По предположению f обращается в нуль в каждой точке $a_n \in k$. Следовательно, $f(a_1, \ldots, a_{n-1}, x_n)$ является нулевым полиномом из $k[x_n]$. Значит, его коэффициенты равны нулю, т. е. $g_i(a_1, \ldots, a_{n-1}) = 0$ для всех i. Так как точка $(a_1, \ldots, a_{n-1})$ выбрана в k^{n-1} произвольно, то каждый $g_i \in k[x_1, \ldots, x_{n-1}]$ является нулевой функцией на k^{n-1}. Тогда по предположению индукции каждый g_i является нулевым полиномом в $k[x_1, \ldots, x_{n-1}]$. Отсюда следует, что f является нулевым полиномом в $k[x_1, \ldots, x_n]$. Предложение доказано. □

Отметим, что в формулировке предложения 5 утверждение «$f = 0$ в $k[x_1, \ldots, x_n]$» означает, что f является нулевым полиномом, т. е. все его коэффициенты равны нулю. Таким образом, символ 0 обозначает и нулевой элемент в k, и нулевой полином в $k[x_1, \ldots, x_n]$. Из контекста всегда будет ясно, что именно имеется в виду.

В качестве следствия мы получаем, что два полинома равны в том и только том случае, когда они определяют одну и ту же функцию на аффинном пространстве.

Следствие 6. *Пусть k — бесконечное поле и $f, g \in k[x_1, \ldots, x_n]$. Тогда $f = g$ в $k[x_1, \ldots, x_n]$ в том и только том случае, когда функции $f : k^n \to k$ и $g : k^n \to k$ равны.*

Доказательство. В одну сторону утверждение тривиально. Пусть теперь $f, g \in k[x_1, \ldots, x_n]$ задают одну и ту же функцию на k^n. Тогда полином $f - g$ обращается в нуль во всех точках из k^n, т. е. по предложению 5 полином $f - g$ является нулевым. Значит, $f = g$ в $k[x_1, \ldots, x_n]$. □

Наконец, необходимо упомянуть одно специальное свойство полиномов над полем комплексных чисел $\mathbb{C}$.

Теорема 7. *Каждый непостоянный полином $f \in \mathbb{C}[x]$ имеет корень в $\mathbb{C}$.*

Доказательство. Это утверждение называется основной теоремой алгебры, и его доказательство можно найти в любом учебнике по комплексному анализу (хотя известно и много других доказательств). □

Поле k называется *алгебраически замкнутым*, если любой непостоянный полином из $k[x]$ имеет корень в k. Например, поле $\mathbb{R}$ не является алгебраически замкнутым (какие корни имеет полином x^2+1?), в то время как $\mathbb{C}$ алгебраически замкнуто (по предыдущей теореме). В гл. 4 мы докажем теорему Гильберта о нулях, которая является сильным обобщением теоремы 7.

Упражнения к § 1

1. Пусть $\mathbb{F}_2 = \{0, 1\}$. Определим операции сложения и умножения на этом множестве следующими равенствами: $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ и $1 \cdot 1 = 1$. Докажите, что $\mathbb{F}_2$ — поле. (Проверять ассоциативность и дистрибутивность не обязательно, но надо проверить существование аддитивной и мультипликативной единиц и обратных элементов.)

2. Пусть $\mathbb{F}_2$ — поле из упр. 1.
   (a) Рассмотрим полином $g(x, y) = x^2y + y^2x \in \mathbb{F}_2[x, y]$. Докажите, что[1] $g(x, y) = 0$ для всех $(x, y) \in \mathbb{F}_2^2$. Объясните, почему этот факт не противоречит предложению 5.
   (b) Найдите ненулевой полином в $\mathbb{F}_2[x, y, z]$, который обращается в нуль в каждой точке из $\mathbb{F}_2^3$ и который является полиномом именно от трех переменных[2].
   (c) Найдите ненулевой полином в $\mathbb{F}_2[x_1, \ldots, x_n]$, который обращается в нуль в каждой точке из $\mathbb{F}_2^n$. Можете ли вы отыскать такой полином, который при этом был бы полиномом именно от n переменных[2]?

3. (Это упражнение требует знания абстрактной алгебры.) Пусть p — простое число. Кольцо вычетов по модулю p является полем из p элементов, которое обозначается через $\mathbb{F}_p$.
   (a) Выясните, почему $\mathbb{F}_p - \{0\}$ является группой по умножению.
   (b) Используя теорему Лагранжа, докажите, что $a^{p-1} = 1$ для всех $a \in \mathbb{F}_p - \{0\}$.
   (c) Докажите, что $a^p = a$ для всех $a \in \mathbb{F}_p$. Указание: случаи $a = 0$ и $a \neq 0$ рассматриваются отдельно.
   (d) Найдите ненулевой полином из $\mathbb{F}_p[x]$, который обращается в нуль в каждой точке поля $\mathbb{F}_p$. Указание: используйте результат п. (c) этого упражнения.

4. (Это упражнение требует знания абстрактной алгебры). Пусть F — конечное поле из q элементов. Используя рассуждения упр. 3, докажите, что ненулевой полином $x^q - x \in F[x]$ обращается в нуль в каждой точке поля F. Этот результат показывает, что ни для какого конечного поля утверждение предложения 5 не имеет места[3].

5. При доказательстве предложения 5 мы представили полином $f \in k[x_1, \ldots, x_n]$ как полином от одной переменной x_n с коэффициентами из $k[x_1, \ldots, x_{n-1}]$. Чтобы посмотреть, как эта процедура выглядит в конкретном случае, рассмотрите полином

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

   (a) Запишите f как полином от x с коэффициентами из $k[y, z]$.
   (b) Запишите f как полином от y с коэффициентами из $k[x, z]$.
   (c) Запишите f как полином от z с коэффициентами из $k[x, y]$.

6. Рассмотрим в $\mathbb{C}^n$ подмножество $\mathbb{Z}^n$, которое состоит из всех точек с целыми координатами.
   (a) Докажите, что если $f \in \mathbb{C}[x_1, \ldots, x_n]$ обращается в нуль в каждой точке множества $\mathbb{Z}^n$, то f — нулевой полином. Указание: используйте доказательство предложения 5.
   (b) Пусть $f \in \mathbb{C}[x_1, \ldots, x_n]$, а M — наибольшая из степеней входящих в f переменных. Определим $\mathbb{Z}_{M+1}^n$ как подмножество в $\mathbb{Z}^n$, состоящее из точек, все координаты которых — целые положительные числа, не превосходящие $M + 1$. Пусть f обращается в нуль в каждой точке из $\mathbb{Z}_{M+1}^n$. Докажите, что f — нулевой полином.

[1] Точнее, $g(a, b) = 0$ для всех $(a, b) \in \mathbb{F}_2^2$.— *Прим. ред.*

[2] Используйте примечание редактора на с. 14 для построения примеров такого рода.— *Прим. ред.*

[3] См. примечание редактора на стр. 14.— *Прим. ред.*

§ 2. Аффинные многообразия

Теперь мы можем определить основной геометрический объект исследований в данной книге.

Определение 1. Пусть k — некоторое поле, а $f_1, \ldots, f_s$ — полиномы в $k[x_1, \ldots, x_n]$. Положим

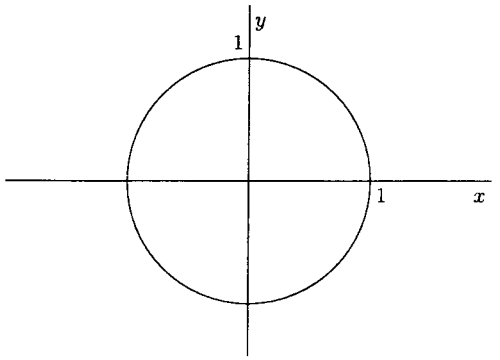
$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \quad \text{для всех } 1 \leq i \leq s\}.$$

$\mathbf{V}(f_1, \ldots, f_s)$ называется ***аффинным многообразием***, определенным полиномами $f_1, \ldots, f_s$[1].

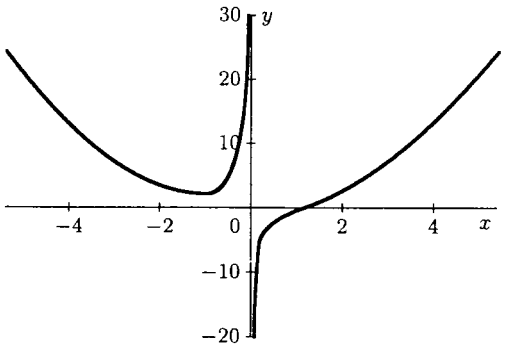
Другими словами, аффинное многообразие $\mathbf{V}(f_1, \ldots, f_s) \subset k^n$ — это множество решений системы уравнений $f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0$. Мы будем использовать буквы V, W и др. для обозначения аффинных многообразий. Главная цель этого параграфа — познакомить читателя с большим количеством примеров, среди которых будут знакомые и незнакомые объекты. Мы рассматриваем случай $k = \mathbb{R}$, что позволяет нам рисовать картинки.

[1] Хотя это и не вполне аккуратно, часто используется название «многообразие $f_1 = \ldots = f_s = 0$». (Эта терминология используется и в настоящей книге.) — *Прим. ред.*

Начнем с многообразия $\mathbf{V}(x^2+y^2-1)$ на плоскости $\mathbb{R}^2$, которое, конечно же, является окружностью радиуса 1 с центром в начале координат:



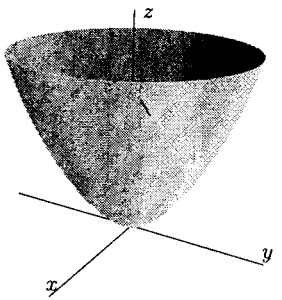
Конические сечения, которые изучаются в курсе аналитической геометрии (окружности, эллипсы, параболы и гиперболы), являются аффинными многообразиями. Аналогично, графики полиномов также являются аффинными многообразиями (график функции $y = f(x)$ есть аффинное многообразие $\mathbf{V}(y - f(x))$). Хотя это и не так очевидно, графики рациональных функций — тоже аффинные многообразия. Рассмотрим, например, график функции $y = \frac{x^3-1}{x}$:



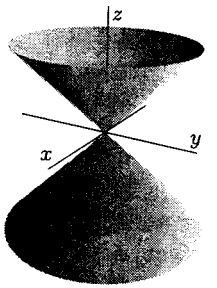
Легко видеть, что это аффинное многообразие $\mathbf{V}(xy - x^3 + 1)$.

Перейдем теперь к трехмерному пространству $\mathbb{R}^3$. Параболоид вращения $\mathbf{V}(z - x^2 - y^2)$ представляет собой красивое аффинное многообразие, которое получается при вращении параболы $z = x^2$

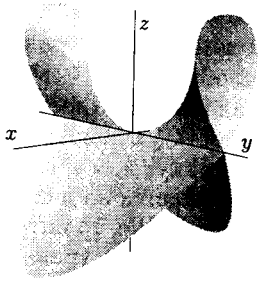
вокруг оси z (этот факт легко доказывается с помощью перехода к полярным координатам). Вот как выглядит это многообразие:



Наверное, вам знаком конус $\mathbf{V}(z^2 - x^2 - y^2)$:



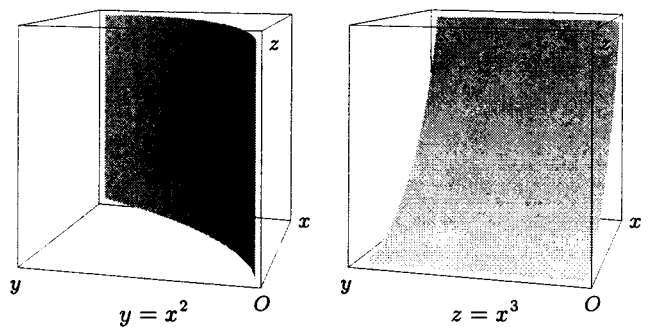
Многообразие $\mathbf{V}(x^2 - y^2z^2 + z^3)$ является более сложной поверхностью:



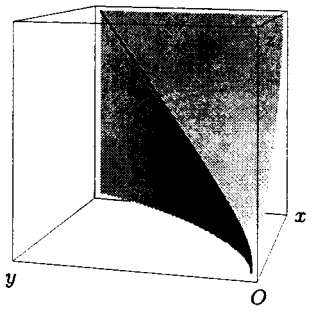
Поверхности из последних двух примеров не везде гладкие: конус имеет острие в начале координат, а в последнем примере ось y является линией самопересечения поверхности. Это примеры *особых точек*, которые будут изучаться далее.

Интересным примером кривой в $\mathbb{R}^3$ является *скрученная кубика* — многообразие $\mathbf{V}(y - x^2, z - x^3)$. Для простоты мы рисуем ту

часть кривой, которая лежит в первом октанте. Сначала изобразим поверхности $y = x^2$ и $z = x^3$ [1] отдельно:



Их пересечение и есть скрученная кубика:

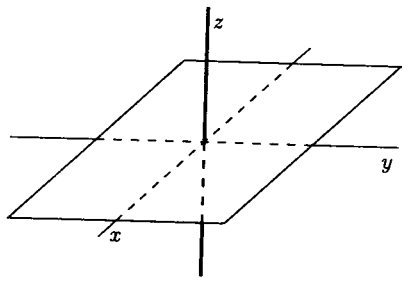


Скрученная кубика

Отметим, что когда мы имеем одно уравнение в $\mathbb{R}^2$, то получаем кривую — одномерный объект. В $\mathbb{R}^3$ ситуация аналогична: одно уравнение в $\mathbb{R}^3$ обычно задает поверхность, которая имеет размерность два. Опять размерность уменьшается на единицу. Рассмотрим теперь скрученную кубику: два уравнения в $\mathbb{R}^3$ задают кривую, т. е. размерность уменьшается на два. Так как каждое уравнение задает дополнительное условие, то интуиция подсказывает, что введение каждого дополнительного уравнения должно понижать размерность на единицу. Значит, в $\mathbb{R}^4$ два уравнения должны определять поверхность. К сожалению, понятие размерности является более сложным, чем может показаться из рассмотренных примеров. Рассмотрим, например, многообразие $\mathbf{V}(xz, yz)$. Легко проверить,

[1] См. примечание редактора на с. 17. — *Прим. ред.*

что уравнения $xz = yz = 0$ задают объединение плоскости (x, y) и оси z:



Таким образом, многообразие состоит из двух частей разной размерности, и одна из частей (плоскость) имеет «неправильную» размерность (согласно описанным выше интуитивным соображениям).

Приведем несколько многомерных примеров. Хорошо известный объект возникает в линейной алгебре. Рассмотрим систему из m линейных уравнений с n неизвестными $x_1, \ldots, x_n$ и с коэффициентами из данного поля k:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n &= b_m. \end{aligned} \tag{1}$$

Решения этой системы образуют аффинное многообразие в k^n, которое называется ***линейным многообразием***. Так, прямые и плоскости являются линейными многообразиями. Существуют линейные многообразия произвольно больших размерностей. Метод исключения Гаусса, изучаемый в курсе линейной алгебры, представляет собой алгоритм нахождения всех решений такой системы. В гл. 2 мы изучим обобщение этого метода, которое применимо для решения систем полиномиальных уравнений.

Линейные многообразия дают хороший материал для обсуждения проблемы размерности. А именно, если $V \subset k^n$ является линейным многообразием, определяемым системой (1), то его размерность не обязательно равна $n - m$, хотя V и определено m уравнениями. Действительно, если V непусто, то его размерность равна $n - r$, где r — ранг матрицы (a_{ij}). Таким образом, в случае линейных многообразий размерность определяется числом ***независимых*** уравнений. Именно это интуитивное соображение и применимо в общем случае, хотя понятие «независимости» требует существенного уточнения.

Некоторые сложные многомерные примеры дает математический анализ. Пусть, например, мы хотим отыскать минимум и мак-

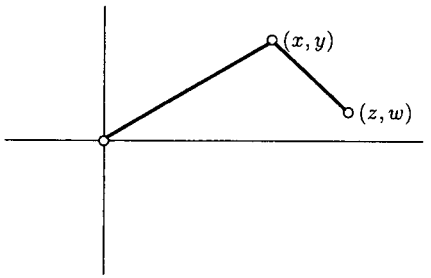
симум функции $f(x,y,z)=x^3+2xyz-z^2$ при условии, что $g(x,y,z)=x^2+y^2+z^2=1$. Согласно методу множителей Лагранжа, $\nabla f=\lambda\nabla g$ в точках локального экстремума (напомним, что градиент функции f — это вектор частных производных $\nabla f=(f'_x,f'_y,f'_z)$). Это дает нам следующую систему из четырех уравнений с четырьмя неизвестными x,y,z,λ:

$$\begin{aligned} 3x^2+2yz &= 2x\lambda,\\ 2xz &= 2y\lambda,\\ 2xy-2z &= 2z\lambda,\\ x^2+y^2+z^2 &= 1. \end{aligned} \tag{2}$$

Эти уравнения определяют аффинное многообразие в $\mathbb{R}^4$, и наша интуиция подсказывает нам, что оно состоит из конечного множества точек (т. е. имеет размерность 0), потому что оно задано четырьмя уравнениями. Студенты обычно считают метод множителей Лагранжа сложным, так как получаемые системы уравнений обычно трудно решать. Алгоритмы, которые будут рассмотрены в гл. 2, являются мощным инструментом решения подобных задач. В частности, будет получено и решение системы (2).

Необходимо также отметить, что аффинное многообразие может быть пустым множеством. Пусть, например, $k=\mathbb{R}$; тогда $\mathbf{V}(x^2+y^2+1)=\varnothing$, так как уравнение $x^2+y^2=-1$ не имеет вещественных решений (хотя оно и имеет решения, когда $k=\mathbb{C}$). Другой пример — это многообразие $\mathbf{V}(xy,xy-1)$, которое пусто при любом поле, так как фиксированные x и y не могут одновременно удовлетворять двум равенствам: $xy=0$ и $xy=1$. В гл. 4 будет рассмотрен метод, позволяющий определить, когда аффинное многообразие непусто над $\mathbb{C}$.

Скажем несколько слов о применениях аффинных многообразий. Вот пример из роботики. Пусть рука робота, состоящая из двух соединенных стержней длины 1 и 2 совершает движения в плоскости. Длинный стержень закреплен в начале координат:



«Состояние» руки полностью определено координатами (x,y) и (z,w), указанными на рисунке. Таким образом, состояние может рассматриваться как точка $(x,y,z,w)\in\mathbb{R}^4$. Однако не все точки из $\mathbb{R}^4$ могут представлять состояния руки. Легко видеть, что множество состояний есть аффинное многообразие в $\mathbb{R}^4$, определенное уравнениями

$$\begin{aligned} x^2+y^2 &= 4,\\ (x-z)^2+(y-w)^2 &= 1. \end{aligned}$$

Отметим, как естественно возникают многомерные задачи: если мы будем рассматривать ту же самую руку в трехмерном пространстве, то многообразие состояний определяется двумя уравнениями в $\mathbb{R}^6$. Техника, развитая в этой книге, имеет важные приложения в роботике.

До сих пор все наши картинки рисовались над $\mathbb{R}$. Далее в этой книге мы будем рассматривать многообразия над $\mathbb{C}$. В этом случае труднее (но не невозможно) представить себе геометрию многообразия.

Перечислим, наконец, основные свойства аффинных многообразий.

Лемма 2. *Если $V,W\subset k^n$ — аффинные многообразия, то $V\cup W$ и $V\cap W$ также являются аффинными многообразиями.*

Доказательство. Пусть $V=\mathbf{V}(f_1,\dots,f_s)$ и $W=\mathbf{V}(g_1,\dots,g_t)$. Мы утверждаем, что

$$\begin{aligned} V\cap W &= \mathbf{V}(f_1,\dots,f_s,g_1,\dots,g_t),\\ V\cup W &= \mathbf{V}(f_ig_j : 1\le i\le s, 1\le j\le t). \end{aligned}$$

Первое утверждение тривиально: если точка принадлежит $V\cap W$, то как функции $f_1,\dots,f_s$, так и функции $g_1,\dots,g_t$ обращаются в этой точке в нуль. Это то же самое, что обращение в нуль набора функций $f_1,\dots,f_s,g_1,\dots,g_t$.

Доказательство второго утверждения требует больших усилий. Если $(a_1,\dots,a_n)\in V$, то все f_i обращаются в нуль в этой точке; значит, и все функции f_ig_j обращаются в нуль в $(a_1,\dots,a_n)$. Таким образом, $V\subset\mathbf{V}(f_ig_j)$ и, аналогично, $W\subset\mathbf{V}(f_ig_j)$. Следовательно, $V\cup W\subset\mathbf{V}(f_ig_j)$. С другой стороны, пусть $(a_1,\dots,a_n)\in\mathbf{V}(f_ig_j)$. Если эта точка принадлежит V, то все доказано, если же нет, то $f_{i_0}(a_1,\dots,a_n)\ne 0$ для некоторого i_0. Так как функции $f_{i_0}g_j$ обращаются в нуль в $(a_1,\dots,a_n)$ при всех j, то все g_j равны нулю в этой точке. Значит, $(a_1,\dots,a_n)\in W$ и $\mathbf{V}(f_ig_j)\subset V\cup W$. □

Из этой леммы вытекает, что конечные объединения и пересечения аффинных многообразий являются аффинными многообра-

зиями. На самом деле мы уже встречались с объединениями и пересечениями. Рассмотрим, например, объединение плоскости (x, y) и оси z в $\mathbb{R}^3$. По формуле из доказательства леммы 2

$$\mathbf{V}(z) \cup \mathbf{V}(x, y) = \mathbf{V}(xz, yz).$$

Это, разумеется, один из рассмотренных нами ранее примеров. Что касается пересечений, отметим, что скрученная кубика была задана как пересечение двух поверхностей.

Анализ двух примеров из этого параграфа ведет к постановке интересных задач об аффинных многообразиях. Пусть $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Тогда можно сформулировать следующие проблемы:

- (Совместность) Можем ли мы выяснить, будет ли $\mathbf{V}(f_1, \dots, f_s)$, непустым, т. е. имеют ли уравнения $f_1 = \cdots = f_s = 0$ общее решение?
- (Конечность) Можем ли мы выяснить, конечно ли множество $\mathbf{V}(f_1, \dots, f_s)$, и если да, то как найти все решения в явном виде?
- (Размерность) Можем ли мы найти «размерность» многообразия $\mathbf{V}(f_1, \dots, f_s)$?

Ответ на все эти вопросы утвердительный, хотя мы с осторожностью должны относиться к выбору поля k, над которым определяются многообразия. Самая трудная задача — о размерности, так как для ее решения нам понадобится весьма непростая теория. Тем не менее мы дадим полные ответы на все три вопроса.

Упражнения к § 2

1. Нарисуйте следующие аффинные многообразия в $\mathbb{R}^2$:
   (a) $\mathbf{V}(x^2 + 4y^2 + 2x - 16y + 1)$;
   (b) $\mathbf{V}(x^2 - y^2)$;
   (c) $\mathbf{V}(2x + y - 1, 3x - y + 2)$.
   Имеет ли многообразие в каждом из этих примеров интуитивно ожидаемую размерность?

2. Нарисуйте многообразие $\mathbf{V}(y^2 - x(x-1)(x-2))$ в $\mathbb{R}^2$. Указание: для каких x равенство $y^2 = x(x-1)(x-2)$ можно разрешить относительно y? Сколько значений y отвечают одному значению x? Какие симметрии имеет кривая?

3. В плоскости $\mathbb{R}^2$ нарисуйте картинку, иллюстрирующую пересечение
$$\mathbf{V}(x^2 + y^2 - 4) \cap \mathbf{V}(xy - 1) = \mathbf{V}(x^2 + y^2 - 4, xy - 1),$$
   и найдите точки пересечения. Отметим, что этот пример является частным случаем леммы 2.

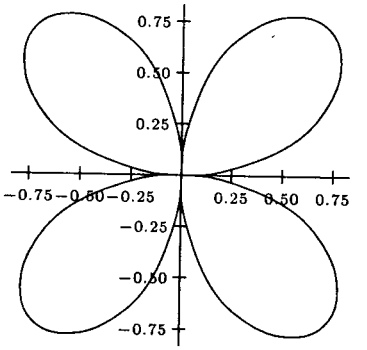
4. Нарисуйте следующие аффинные многообразия в $\mathbb{R}^3$:
   (a) $\mathbf{V}(x^2 + y^2 + z^2 - 1)$;

   (b) $\mathbf{V}(x^2 + y^2 - 1)$;
   (c) $\mathbf{V}(x + 2, y - 1\frac{1}{2}, z)$;
   (d) $\mathbf{V}(xz^2 - xy)$. Указание: разложите $xz^2 - xy$ на множители;
   (e) $\mathbf{V}(x^4 - xz, x^3 - xy)$;
   (f) $\mathbf{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 1)$.
   Имеет ли многообразие в каждом из этих случаев интуитивно ожидаемую размерность?

5. Используйте доказательство леммы 2 для того, чтобы нарисовать многообразие $\mathbf{V}((x-2)(x^2-y), y(x^2-y), (z+1)(x^2-y))$ в $\mathbb{R}^3$. Указание: объединением каких двух многообразий является это многообразие?

6. Докажем, что любое конечное подмножество в k^n является аффинным многообразием.
   (a) Докажите, что точка $(a_1, \dots, a_n) \in k^n$ является аффинным многообразием.
   (b) Докажите, что каждое конечное подмножество в k^n является аффинным многообразием. Указание: используйте лемму 2.

7. Один из красивейших примеров построения графика кривой в полярных координатах дает четырехлепестковая роза



   Эта кривая задана полярным уравнением $r = \sin(2\theta)$. Докажем, что она является аффинным многообразием.
   (a) Используя связь между декартовыми и полярными координатами $r^2 = x^2 + y^2$, $x = r\cos\theta$, $y = r\sin\theta$, докажите, что четырехлепестковая роза содержится в аффинном многообразии $\mathbf{V}((x^2 + y^2)^3 - 4x^2y^2)$. Указание: разложите $\sin(2\theta)$ в произведение.
   (b) Докажите, что многообразие $\mathbf{V}((x^2 + y^2)^3 - 4x^2y^2)$ содержится в четырехлепестковой розе. Эта задача сложнее, чем кажется на первый взгляд, так как r в равенстве $r = \sin(2\theta)$ может оказаться отрицательным.

Объединяя задачи (a) и (b), мы и получим доказательство того, что четырехлепестковая роза является аффинным многообразием $\mathbf{V}((x^2+y^2)^3-4x^2y^2)$.

8. Доказательство того, что некоторое множество *не является* аффинным многообразием, может потребовать некоторых усилий. Рассмотрим, например, множество

$$X = \{(x,x) : x \in \mathbb{R}, x \neq 1\} \subset \mathbb{R}^2,$$

которое представляет собой прямую $y = x$ с удаленной точкой $(1,1)$. Докажем, что X не есть аффинное многообразие. Предположим противное: $X = \mathbf{V}(f_1,\dots,f_s)$. Каждая функция f_i обращается в нуль на X, и если мы покажем, что f_i равна нулю и в точке $(1,1)$ тоже, то тем самым мы придем к нужному нам противоречию. То есть нужно доказать следующее утверждение: пусть $f \in \mathbb{R}[x,y]$ равна нулю на X; тогда $f(1,1) = 0$. Указание: положим $g(t) = f(t,t)$; тогда $g \in \mathbb{R}[t]$. Теперь можно применить предложение 5 из § 1.

9. Пусть $R = \{(x,y) \in \mathbb{R}^2 : y > 0\}$ — верхняя полуплоскость. Докажите, что R не является аффинным многообразием.

10. Пусть множество $\mathbb{Z}^n \subset \mathbb{C}^n$ состоит из точек с целыми координатами. Докажите, что $\mathbb{Z}^n$ не является аффинным многообразием. Указание: примените результат упр. 6 из § 1.

11. До сих пор мы рассматривали многообразия над $\mathbb{R}$ и $\mathbb{C}$. Можно, однако, изучать многообразия над полем $\mathbb{Q}$. Задачи о многообразиях в этом случае становятся *значительно* труднее. Пусть, например, n — натуральное число. Рассмотрим многообразие $F_n \subset \mathbb{Q}^2$, заданное уравнением

$$x^n + y^n = 1.$$

Это уравнение имеет очевидные решения, когда x или y равно нулю. Мы назовем их *тривиальными решениями*. Возникает интересный вопрос о существовании нетривиальных решений.

(a) Докажите, что F_n имеет два тривиальных решения, если n нечетно, и четыре, если n четно.

(b) Докажите, что F_n имеет нетривиальное решение при $n \geq 3$ в том и только в том случае, когда великая теорема Ферма неверна. *Великая теорема Ферма* утверждает, что при $n \geq 3$ уравнение

$$x^n + y^n = z^n$$

не имеет целых ненулевых решений. В общем случае эта теорема была доказана Эндрю Вайлсом в 1994 г. с использованием весьма сложных теоретико-числовых методов. Доказательство является *исключительно* трудным.

12. Возьмите какую-нибудь задачу на метод множителей Лагранжа из учебника по анализу и составьте систему уравнений. Убедитесь сначала, что это задача о минимуме или максимуме именно полинома с полиномиальными же условиями. Тогда построенная система уравнений (иногда довольно сложная) определяет аффинное многообразие. Позже мы будем использовать базисы Грёбнера для решения подобных систем.

13. Рассмотрим руку робота в $\mathbb{R}^2$, которая состоит из трех стержней длины 3, 2 и 1 соответственно. Стержень длины 3 закреплен в начале координат, стержень длины 2 соединен со свободным концом первого стержня, а стержень длины 1 соединен со свободным концом второго стержня. «Кисть» робота прикреплена к концу стержня длины 1.

(a) Нарисуйте картинку руки робота.

(b) Сколько переменных определяют «состояние» руки?

(c) Составьте уравнения многообразия возможных состояний.

(d) Используя интуитивные соображения о размерности, которые обсуждались в этом параграфе, подумайте, какой может быть размерность многообразия состояний.

14. В этом упражнении изучаются возможные состояния «кисти» робота из упр. 13.

(a) Пусть (u,v) — координаты кисти. Объясните, почему $u^2+v^2 \leq 36$.

(b) Предположим, что второй стержень закреплен так, что он образует прямолинейное продолжение первого, причем в остальных соединениях свобода движения не ограничена. Изобразите эту ситуацию и покажите, что в этом случае (u,v) может быть *любой* точкой кольца $16 \leq u^2+v^2 \leq 36$.

(c) С помощью рисунка покажите, что (u,v) может быть любой точкой в круге $u^2+v^2 \leq 36$. Указание: фиксируйте специальным образом второе соединение.

15. В лемме 2 мы доказали, что объединение и пересечение двух аффинных многообразий V и W являются аффинными многообразиями. В этом упражнении мы рассмотрим другие теоретико-множественные операции над аффинными многообразиями.

(a) Докажите, что конечные объединения и пересечения аффинных многообразий являются аффинными многообразиями. Указание: индукция.

(b) Приведите пример бесконечного объединения аффинных многообразий, которое не является аффинным многообразием. Указание: в упр. 8–10 указаны подмножества в k^n, не являющиеся аффинными многообразиями. Удивительно, но бесконечное пересечение аффинных многообразий является-таки аффинным многообразием. Этот результат — следствие теоремы Гильберта о базисе, которая будет рассматриваться в гл. 2 и 4.

(c) Покажите, что теоретико-множественная разность $V - W$ двух аффинных многообразий не обязательно является аффинным многообразием.

(d) Пусть $V \subset k^n$ и $W \subset k^m$ — два аффинных многообразия, и пусть

$$\begin{aligned} V \times W = \{&(x_1,\dots,x_n,y_1,\dots,y_m) \in k^{n+m} : \\ &(x_1,\dots,x_n) \in V, (y_1,\dots,y_m) \in W\} \end{aligned}$$

— их декартово произведение. Докажите, что $V \times W$ является аффинным многообразием в k^{n+m}. Указание: если V задано полиномами $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, то мы можем рассматривать f_i как полиномы из $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$; аналогично мы можем рассуждать и в случае W. Покажите, что это рассуждение позволяет построить определяющие уравнения для произведения $V \times W$.

§ 3. Параметризации аффинных многообразий

В этом параграфе мы рассмотрим задачу описания точек аффинного многообразия $\mathbf{V}(f_1, \ldots, f_s)$. Эту задачу можно переформулировать как задачу описания всех решений системы полиномиальных уравнений $f_1 = \ldots = f_s = 0$. Если решений конечное число, то наша цель — просто перечислить их. Но что делать, если их бесконечно много? Здесь мы должны ввести понятие параметризации аффинного многообразия.

Рассмотрим сначала пример из линейной алгебры — следующую систему уравнений над $\mathbb{R}$:

$$\begin{aligned} x + y + z &= 1, \\ x + 2y - z &= 3. \end{aligned} \tag{1}$$

С геометрической точки зрения эта система определяет прямую в $\mathbb{R}^3$, которая является пересечением плоскости $x + y + z = 1$ и плоскости $x + 2y - z = 3$. Таким образом, система имеет бесконечно много решений. Для описания решений, используя приемы из метода Гаусса, преобразуем систему (1) к виду

$$\begin{aligned} x + 3z &= -1, \\ y - 2z &= 2. \end{aligned}$$

Пусть $z = t$, где t — произвольное вещественное число; тогда все решения системы (1) можно записать в виде

$$\begin{aligned} x &= -1 - 3t, \\ y &= 2 + 2t, \\ z &= t. \end{aligned} \tag{2}$$

Мы назовем t *параметром*, а (2), таким образом, является *параметризацией* множества решений системы (1).

Рассмотрим, как метод параметризации решений применяется к изучению аффинных многообразий. Возьмем в качестве примера единичную окружность

$$x^2 + y^2 = 1. \tag{3}$$

Обычный метод параметризации в этом случае — использование тригонометрических функций

$$\begin{aligned} x &= \cos t, \\ y &= \sin t. \end{aligned}$$

Существует, однако, и алгебраическая параметризация окружности:

$$\begin{aligned} x &= \frac{1 - t^2}{1 + t^2}, \\ y &= \frac{2t}{1 + t^2}. \end{aligned} \tag{4}$$

Читателю надо проверить, что так определенные точки лежат на окружности (3). Следует отметить, что эта параметризация не описывает точки окружности полностью: так как $x = \frac{1-t^2}{1+t^2}$ не может быть равно -1, то точка $(-1, 0)$ не параметризована. В конце параграфа мы объясним, как была построена эта параметризация.

Отметим, что в уравнениях (4) использованы отношения полиномов — *рациональные функции*. И прежде чем мы всерьез займемся задачей параметризации, дадим общее определение рациональной функции.

Определение 1. Пусть k — некоторое поле. *Рациональной функцией* от переменных $t_1, \ldots, t_m$ с коэффициентами из k называется отношение f/g двух полиномов $f, g \in k[t_1, \ldots, t_m]$, где g не является нулевым полиномом. Далее, две рациональные функции f/g и h/k равны, если $kf = gh$ в $k[t_1, \ldots, t_m]$. Множество всех рациональных функций от переменных $t_1, \ldots, t_m$ с коэффициентами из k обозначается $k(t_1, \ldots, t_m)$.

Легко показать, что сумма и произведение рациональных функций являются рациональными функциями и что $k(t_1, \ldots, t_m)$ — поле. Мы не будем давать доказательства этих утверждений.

Рассмотрим многообразие $V = \mathbf{V}(f_1, \ldots, f_s) \subset k^n$. Его *рациональной параметризацией* (или *рациональным параметрическим представлением*) называется набор из n рациональных функций $r_1, \ldots, r_n \in k(t_1, \ldots, t_m)$, такой, что точки с координатами

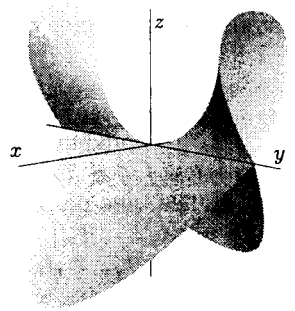
$$\begin{aligned} x_1 &= r_1(t_1, \ldots, t_m), \\ x_2 &= r_2(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= r_n(t_1, \ldots, t_m) \end{aligned}$$

принадлежат[1)] V. Мы также требуем, чтобы V было «наименьшим» многообразием, содержащим эти точки. Как показывает пример окружности, может случиться, что не все точки многообразия V будут параметризованы. В гл. 3 мы дадим точное определение того, что мы имеем в виду под словом «наименьшее».

Часто встречается такая параметризация многообразия V, когда $r_1, \ldots, r_n$ — полиномы. В этом случае параметризация называется *полиномиальной*.

Отметим, что первоначальный набор уравнений $f_1 = \ldots = f_s = 0$, определяющих многообразие V, иногда называется его *неявным представлением*. В предыдущих примерах (1) и (3) — неявные представления, а (2) и (4) — параметрические представления.

Одним из главных достоинств параметрического представления кривой или поверхности является то, что оно позволяет легко нарисовать ее на экране компьютерного монитора. Зная формулы параметризации, компьютер вычисляет координаты точек многообразия при различных значениях параметров и рисует их на экране. В § 2, например, был приведен рисунок поверхности $\mathbf{V}(x^2 - y^2z^2 + z^3)$:



При построении этого рисунка не использовалось, разумеется, неявное представление $x^2 - y^2z^2 + z^3 = 0$. Мы использовали параметрическое представление, заданное формулами

$$\begin{aligned} x &= t(u^2 - t^2), \\ y &= u, \\ z &= u^2 - t^2. \end{aligned} \tag{5}$$

Так как мы описываем поверхность, то параметров два — это t и u. Рисунок изображает часть поверхности, когда $-1 \le t, u \le 1$. В

[1)] Точнее, для любых элементов $a_1, \ldots, a_m$ поля k точка с координатами $r_1(a_1, \ldots, a_m), \ldots, r_n(a_1, \ldots, a_m)$ принадлежит многообразию V. Подчеркнем, что *не* предполагается, что разным наборам значений параметров $t_1, \ldots, t_m$ отвечают разные точки многообразия V.— *Прим. ред.*

упражнениях будет предложено получить эту параметризацию и доказать, что она описывает всю поверхность $\mathbf{V}(x^2 - y^2z^2 + z^3)$.

В то же время для решения некоторых задач более удобным бывает неявное представление. Пусть, например, мы должны выяснить, принадлежит или нет точка $(1, 2, -1)$ нашей поверхности. Если мы работаем с параметризацией (5), то решение этой задачи сводится к решению системы

$$\begin{aligned} 1 &= t(u^2 - t^2), \\ 2 &= u, \\ -1 &= u^2 - t^2 \end{aligned} \tag{6}$$

с неизвестными t и u. С другой стороны, если мы работаем с неявным представлением $x^2 - y^2z^2 + z^3 = 0$, то нам достаточно подставить координаты точки в уравнение. Так как

$$1^2 - 2^2(-1)^2 + (-1)^3 = 1 - 4 - 1 = -4 \neq 0,$$

то точка $(1, 2, -1)$ не лежит на поверхности (значит, система (6) не имеет решений).

Удобство работы сразу с двумя представлениями приводит к постановке двух проблем:

- (Параметризация) Всякое ли аффинное многообразие имеет рациональную параметризацию?
- (Неявное представление) Пусть аффинное многообразие задано параметрическим представлением. Можно ли найти уравнения, которые его определяют (т. е. найти неявное представление)?

Ответ на первый вопрос отрицательный. В действительности большинство аффинных многообразий не имеют рациональной параметризации. Те многообразия, которые могут быть рационально параметризованы, называются *унирациональными*. Как правило, ответить на вопрос об унирациональности данного многообразия довольно трудно. Положение со вторым вопросом значительно лучше. В гл. 3 мы увидим, что ответ на второй вопрос утвердительный: если дано параметрическое представление, то мы всегда можем найти определяющие уравнения.

Посмотрим на примере, как построить неявное представление. Рассмотрим параметрически заданную кривую на плоскости

$$\begin{aligned} x &= 1 + t, \\ y &= 1 + t^2. \end{aligned} \tag{7}$$

Пока мы не знаем, лежит ли эта кривая на каком-либо аффинном многообразии. Для того чтобы построить искомое уравнение, выразим t из первого уравнения системы:

$$t = x - 1.$$

Подставляя t во второе уравнение, получим

$$y = 1 + (x-1)^2 = x^2 - 2x + 2.$$

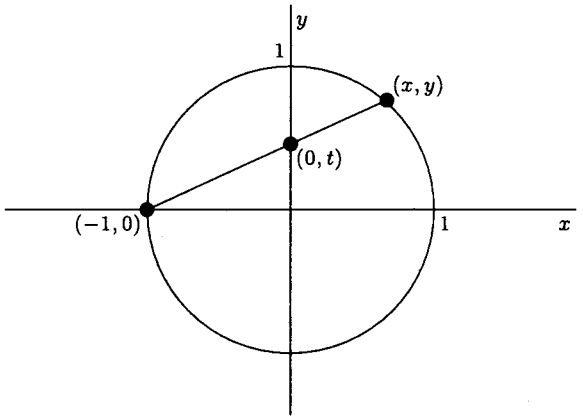
Отсюда следует, что параметрическое уравнение (7) описывает аффинное многообразие $\mathbf{V}(y - x^2 + 2x - 2)$.

Таким образом, в предыдущем примере основа стратегии состояла в исключении переменной t так, чтобы осталось одно уравнение, содержащее только x и y. Этот пример демонстрирует роль *теории исключения*, которая будет подробно рассмотрена в гл. 3.

В следующих двух примерах мы рассмотрим, как геометрические соображения позволяют найти параметризацию многообразий. Рассмотрим сначала единичную окружность. Ее параметризация (4) уже нам известна:

$$x = \frac{1-t^2}{1+t^2},$$
$$y = \frac{2t}{1+t^2}$$

Откуда же возникла такая параметризация? Отметим, что каждая невертикальная прямая, проходящая через точку $(-1,0)$, пересекает окружность еще в одной точке (x,y):



Кроме того, каждая невертикальная прямая пересекает ось y в какой-то точке $(0,t)$ (см. рисунок).

Все это и дает нам геометрическую параметризацию окружности: по заданному t строим прямую линию, соединяющую точки $(-1,0)$ и $(0,t)$; тогда эта прямая пересекает окружность еще в какой-то точке (x,y). Отметим, что это построение действительно задает параметризацию: когда t пробегает ось y от $-\infty$ до $+\infty$, то

соответствующая точка (x,y) пробегает всю окружность за исключением точки $(-1,0)$.

Осталось явно выразить x и y через t. Для этого рассмотрим *наклон* прямой. Мы можем вычислить величину[1)] наклона двумя способами: или с использованием точек $(-1,0)$ и $(0,t)$, или с использованием точек $(-1,0)$ и (x,y). Получаем уравнение

$$\frac{t-0}{0-(-1)} = \frac{y-0}{x-(-1)},$$

откуда

$$t = \frac{y}{x+1}.$$

Если мы подставим $y = t(x+1)$ в уравнение окружности $x^2+y^2=1$, то получим

$$x^2 + t^2(x+1)^2 = 1,$$

что дает нам квадратное уравнение для определения x:

$$(1+t^2)x^2 + 2t^2x + t^2 - 1 = 0. \tag{8}$$

Так как прямая пересекает окружность в двух точках, то это уравнение имеет два решения, одно из которых равно -1. Поэтому (8) может быть записано как произведение

$$(x+1)((1+t^2)x - (1-t^2)) = 0.$$

Так как искомая x-координата определяется вторым сомножителем, то

$$x = \frac{1-t^2}{1+t^2}.$$

А так как $y = t(x+1)$, то

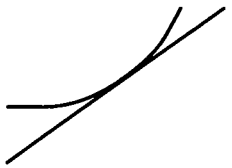
$$y = \frac{2t}{1+t^2},$$

и мы получили параметризацию, описанную ранее. Отметим, что геометрические соображения точно показывают, какая именно часть окружности параметризована.

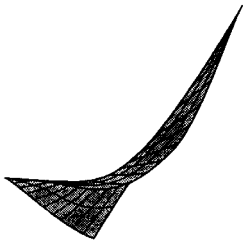
В качестве второго примера рассмотрим скрученную кубику из § 2. Касательные к этой кривой в трехмерном пространстве образу-

[1)] Точнее, тангенс угла.— *Прим. ред.*

ют интересную поверхность. Идея ее построения такова. Для каждой точки кривой существует касательная (в этой точке):



Теперь представим себе, что проведены касательные ко *всем* точкам скрученной кубики. Это дает нам следующую поверхность:



На рисунке показано несколько касательных. А вся поверхность называется *касательной поверхностью* скрученной кубики.

Переведем теперь это геометрическое рассуждение на алгебраический язык. Сначала отметим, что, положив $x = t$ в уравнениях $y - x^2 = z - x^3 = 0$, мы получаем параметризацию

$$\begin{aligned} x &= t, \\ y &= t^2, \\ z &= t^3 \end{aligned}$$

скрученной кубики. Мы запишем ее в виде $\mathbf{r}(t) = (t, t^2, t^3)$. Зафиксируем некоторое t и рассмотрим соответствующую точку на кривой. Мы знаем из курса анализа, что касательный вектор к кривой в точке $\mathbf{r}(t)$ равен $\mathbf{r}'(t) = (1, 2t, 3t^2)$, а параметрическое уравнение касательной прямой записывается в виде

$$\mathbf{r}(t) + u\mathbf{r}'(t) = (t, t^2, t^3) + u(1, 2t, 3t^2) = (t + u, t^2 + 2tu, t^3 + 3t^2u),$$

где u — параметр на касательной. Пусть теперь t меняется; тогда мы получаем параметризацию всей касательной поверхности:

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned}$$

Параметры t и u имеют следующую интерпретацию: t говорит нам о положении на кубике, а u — о положении на касательной прямой. Именно эта параметризация была использована для построения рисунка касательной поверхности выше.

Последний вопрос относится к неявному заданию касательной поверхности: как найти ее уравнение? Это частный случай упомянутой выше задачи построения неявного представления. В нашем случае задача решается исключением t и u из параметрических уравнений. В гл. 2 и 3 мы увидим, что существует алгоритм исключения, и докажем, что касательная поверхность скрученной кубики задается уравнением

$$-4x^3z + 3x^2y^2 - 4y^3 + 6xyz - z^2 = 0.$$

Мы закончим эту главу примером компьютерного геометрического проектирования (КГП). Если необходимо спроектировать сложную поверхность, вроде кузова автомобиля или крыла самолета, инженерам нужен банк кривых и поверхностей разной формы, просто описываемых и легко строящихся. Рациональные и полиномиальные параметрические уравнения удовлетворяют этим требованиям (существует большая литература на эту тему).

Предположим для простоты, что проектировщик хочет описать кривую на плоскости. Сложные кривые, как правило, составляются из нескольких простых кусков, а чтобы части соединялись гладко, направления касательных двух кусков должны совпадать в точке соединения. То есть для каждого куска нужно контролировать следующие геометрические параметры:

(i) начальную и конечную точку куска;
(ii) касательные направления в начальной и конечной точке.

Кубика Безье, открытая конструктором фирмы «Рено» П. Безье, хорошо подходит для этой цели. Она определена параметрически следующими уравнениями:

$$\begin{aligned} x &= (1-t)^3x_0 + 3t(1-t)^2x_1 + 3t^2(1-t)x_2 + t^3x_3, \\ y &= (1-t)^3y_0 + 3t(1-t)^2y_1 + 3t^2(1-t)y_2 + t^3y_3 \end{aligned} \tag{9}$$

для $0 \le t \le 1$, где $x_0, y_0, x_1, y_1, x_2, y_2, x_3, y_3$ — константы, которые задает проектировщик. Мы должны выяснить, как связаны между собой константы и геометрические данные.

Подставляя $t = 0$ и $t = 1$ в (9), получаем

$$\begin{aligned} (x(0), y(0)) &= (x_0, y_0), \\ (x(1), y(1)) &= (x_3, y_3). \end{aligned}$$

Когда t меняется от 0 до 1, то (9) описывает кривую, начинающуюся в (x_0, y_0) и заканчивающуюся в (x_3, y_3). Это дает нам половину

необходимых данных. Найдем теперь касательные направления к кривой при $t = 0$ и $t = 1$. Касательный вектор к кривой (9) при $t = 0$ равен $(x'(0), y'(0))$. Дифференцируя первое из уравнений (9), получаем

$$x' = -3(1-t)^2 x_0 + 3((1-t)^2 - 2t(1-t))x_1 + \\ + 3(2t(1-t) - t^2)x_2 + 3t^2 x_3.$$

Пусть $t = 0$. Тогда

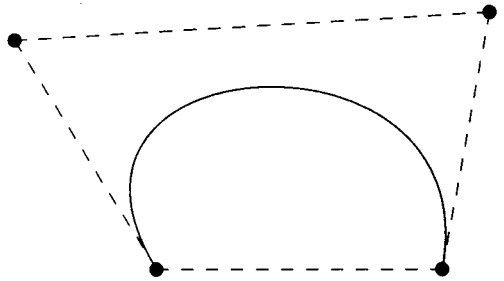
$$x'(0) = -3x_0 + 3x_1 = 3(x_1 - x_0).$$

Аналогично получаем

$$\begin{aligned} (x'(0), y'(0)) &= 3(x_1 - x_0, y_1 - y_0), \\ (x'(1), y'(1)) &= 3(x_3 - x_2, y_3 - y_2). \end{aligned} \tag{10}$$

Так как $(x_1 - x_0, y_1 - y_0) = (x_1, y_1) - (x_0, y_0)$, то вектор $(x'(0), y'(0))$ — это просто утроенный вектор, идущий от (x_0, y_0) к (x_1, y_1). То есть, задав (x_1, y_1), конструктор задает направление касательной в начале кривой. Аналогично, задав (x_2, y_2), конструктор задает касательное направление в конце кривой.

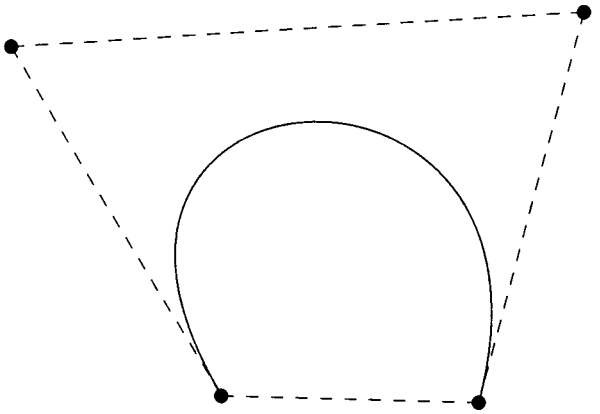
Точки $(x_0, y_0), (x_1, y_1), (x_2, y_2)$ и (x_3, y_3) называются *управляющими точками* кубики Безье. Обычно они обозначаются P_0, P_1, P_2 и P_3, а определяемый ими выпуклый четырехугольник называется *управляющим многоугольником*. Ниже приведен рисунок кривой Безье и ее управляющего многоугольника:



В упражнениях будет доказано, что кубика Безье всегда лежит внутри своего управляющего многоугольника.

Параметры, определяющие кубику Безье, имеют отчетливый геометрический смысл и их легко задать. Единственное, что осталось неясным, — это геометрический смысл *длины* касательных векторов $(x'(0), y'(0))$ и $(x'(1), y'(1))$. Согласно равенствам (10), можно изменить точки (x_1, y_1) и (x_2, y_2), не меняя касательных направлений. Так, например, направления могут остаться такими же, как

на предыдущем рисунке, но длины векторов увеличатся. Тогда мы получим следующую кривую:



То есть увеличение скорости в концевых точках заставляет кривую дольше оставаться вблизи касательных. Опыт помогает конструктору строить разнообразные кривые из кубик Безье. Интересно отметить, что конструктор может даже не догадываться о существовании уравнений (9), задающих кривую.

Кроме КГП, кубика Безье применяется в языке PostScript. В команде `curveto` в PostScript координаты управляющих точек задаются как входные параметры, и тогда на выходе строится кубика Безье. Именно так и были построены рисунки кубик — каждая кривая задавалась одной командной строкой `curveto` в PostScript.

Упражнения к § 3

1. Параметризуйте все решения линейной системы
$$x + 2y - 2z + w = -1,$$
$$x + y + z - w = 2.$$

2. Используйте тригонометрические тождества для доказательства того, что уравнения
$$x = \cos t,$$
$$y = \cos 2t$$
параметризуют часть параболы. Какая именно часть параметризована?

3. Пусть $f \in k[x]$. Найдите параметризацию многообразия $\mathbf{V}(y - f(x))$.

4. Рассмотрим параметрическое представление

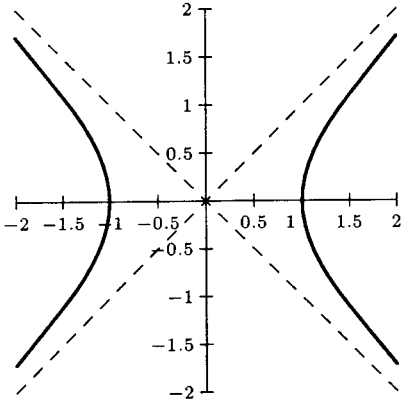
$$x = \frac{t}{1+t},$$

$$y = 1 - \frac{1}{t^2}.$$

(a) Найдите уравнения аффинного многообразия, которое определено этим параметрическим представлением.

(b) Докажите, что эти уравнения параметризуют все многообразие из п. (a), кроме точки $(1, 1)$.

5. В этом упражнении мы будем рассматривать гиперболу $x^2 - y^2 = 1$.



(a) Аналогично тому, как тригонометрические функции используются для параметризации окружности, гиперболические функции используются для параметризации гиперболы. Докажите, что точка с координатами

$$x = \operatorname{ch} t,$$

$$y = \operatorname{sh} t$$

лежит на гиперболе. Какая часть гиперболы параметризована?

(b) Покажите, что прямая может иметь с гиперболой 0, 1 или 2 общие точки, и приведите примеры. Указание: рассмотрите случаи $x = a$ и $y = mx + b$ отдельно.

(c) Используйте рассуждения из конца параграфа для вывода параметрического представления гиперболы. Указание: рассмотрите невертикальные прямые, проходящие через точку $(-1, 0)$ на гиперболе.

(d) Параметризация, построенная в п. (c), не определена для двух значений t. Объясните связь этого факта с существованием у гиперболы асимптот.

6. Цель этого упражнения — доказать, что сфера $x^2 + y^2 + z^2 = 1$ в трехмерном пространстве может быть параметризована так:

$$x = \frac{2u}{u^2+v^2+1},$$

$$y = \frac{2v}{u^2+v^2+1},$$

$$z = \frac{u^2+v^2-1}{u^2+v^2+1}.$$

Для этого нужно рассуждения из конца параграфа применить к случаю трехмерного пространства.

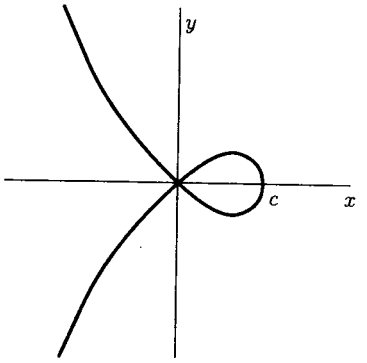
(a) Пусть точка с координатами $(u, v, 0)$ принадлежит плоскости xy. Соединим прямой эту точку с «северным полюсом» сферы, т. е. точкой $(0, 0, 1)$. Пусть (x, y, z) — другая точка пересечения сферы с этой прямой. Сделайте рисунок и докажите геометрически, что отображение точки (u, v) в (x, y, z) задает параметризацию всей сферы за исключением северного полюса.

(b) Докажите, что прямая, соединяющая точки $(u, v, 0)$ и $(0, 0, 1)$, имеет параметризацию $(tu, tv, 1-t)$, где t — параметр на прямой.

(c) Подставьте $x = tu$, $y = tv$ и $z = 1 - t$ в уравнение сферы $x^2 + y^2 + z^2 = 1$ и выведите формулы, приведенные в начале этого упражнения.

7. Используйте рассуждения предыдущего упражнения для параметризации «сферы» $x_1^2 + \cdots + x_n^2 = 1$ в n-мерном аффинном пространстве. Указание: количество параметров равно $n - 1$.

8. Рассмотрим кривую, заданную уравнением $y^2 = cx^2 - x^3$, где c — некоторая константа. График этой кривой при $c > 0$ имеет следующий вид:



Как найти ее параметризацию?

(a) Покажите, что прямая может иметь с этой кривой $0, 1, 2$ или 3 общие точки. Проиллюстрируйте это рисунком. Указание: уравнение прямой может иметь либо вид $x = a$, либо вид $y = mx + b$.

(b) Докажите, что невертикальная прямая, проходящая через начало координат, пересекает эту кривую еще ровно в одной точке в случае, когда $m^2 \neq c$. Проиллюстрируйте этот факт рисунком и постарайтесь найти наглядное объяснение, почему так происходит.

(c) Рассмотрите вертикальную прямую $x = 1$. Проведите прямую через точку $(1, t)$ (лежащую на этой вертикальной прямой) и начало координат. Эта прямая пересекает кривую в точке (x, y). Проиллюстрируйте это рисунком и объясните геометрически, что таким образом мы получаем параметризацию всей кривой.

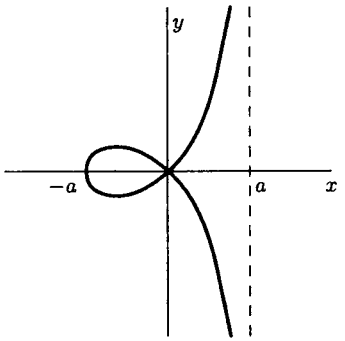
(d) Докажите, что описанное выше геометрическое построение приводит к параметризации

$$x = c - t^2,$$
$$y = t(c - t^2).$$

9. Кривая, называемая *строфоидой*, изучалась многими математиками, включая Исаака Барроу (1630–1677), Иоганна Бернулли (1667–1748), Марию Аньези (1718–1799). Тригонометрическая параметризация этой кривой дается формулами

$$x = a \sin t,$$
$$y = a \operatorname{tg} t(1 + \sin t),$$

где a — константа. Пусть t пробегает интервал $-4.5 \leq t \leq 1.5$; тогда мы получим следующий рисунок кривой:

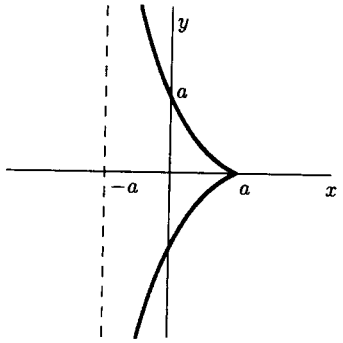


(a) Найдите неявное уравнение строфоиды в координатах x и y. Указание: если вы не проявите аккуратности, то получите уравнение $(a^2 - x^2)y^2 = x^2(a + x)^2$. Для того чтобы понять, почему это уравнение не вполне корректно, посмотрите, что происходит при $x = -a$.

(b) Найдите алгебраическую параметризацию строфоиды.

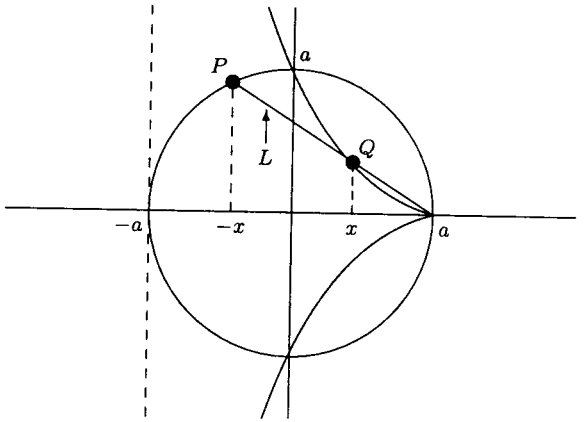
10. Около 180 г. н. э., Диокл написал книгу «Об увеличительных стеклах», в которой рассматривалась кривая, называемая *циссоидой*.

Диокл использовал эту кривую для решения проблемы удвоения куба (см. п. (c)). Циссоида задана уравнением $y^2(a + x) = (a - x)^3$, где a — константа. Вот график этой кривой:



(a) Найдите алгебраическую параметризацию циссоиды.

(b) Диокл описал циссоиду при помощи следующего геометрического построения. Рассмотрим окружность радиуса a с центром в начале координат, и пусть $-a \leq x \leq a$. Проведем прямую L, соединяющую точку $(a, 0)$ с точкой $P = (-x, \sqrt{a^2 - x^2})$ на окружности. Теперь мы можем определить точку $Q = (x, y)$ на L:



Докажите, что циссоида является геометрическим местом всех таких точек Q.

(c) Удвоение куба — это классическая греческая задача о геометрическом построении числа $\sqrt[3]{2}$ с помощью циркуля и линейки. Известно, что, используя только циркуль и линейку, этого сделать нельзя. Диокл доказал, что если использовать еще и циссоиду,

то построить $\sqrt[3]{2}$ можно. Вот как это делается. Проведите прямую, соединяющую точки $(-a, 0)$ и $(0, a/2)$. Эта прямая пересекает циссоиду в точке (x, y). Теперь докажите, что

$$2 = \left(\frac{a-x}{y}\right)^3.$$

Эта формула и показывает, как построить $\sqrt[3]{2}$, используя циркуль, линейку и циссоиду[1)].

11. В этой задаче мы построим параметризацию

$$x = t(u^2 - t^2),$$
$$y = u,$$
$$z = u^2 - t^2$$

поверхности $x^2 - y^2z^2 + z^3 = 0$, рассмотренной выше.

(a) Примените формулы п. (d) упр. 8 и докажите, что кривая $x^2 = cz^2 - z^3$ имеет параметризацию

$$z = c - t^2,$$
$$x = t(c - t^2).$$

(b) Замените теперь параметр c на y^2 и объясните, почему таким образом мы получаем приведенную выше параметризацию поверхности $x^2 - y^2z^2 + z^3 = 0$.

(c) Объясните, почему таким образом параметризуется вся поверхность $\mathbf{V}(x^2 - y^2z^2 + z^3)$. Указание: обратите внимание на п. (c) упр. 8.

12. Пусть дано многообразие $V = \mathbf{V}(y - x^2, z - x^4) \subset \mathbb{R}^3$.

(a) Изобразите его.

(b) Найдите параметризацию многообразия V тем же методом, каким была построена параметризация скрученной кубики.

(c) Параметризуйте касательную поверхность многообразия V.

13. В общем виде задача нахождения уравнения параметризованной поверхности будет рассмотрена в гл. 2 и 3. Однако если идет речь о плоскости, то можно применить методы линейной алгебры. Рассмотрим, например, плоскость в $\mathbb{R}^3$, заданную параметрическим представлением

$$x = 1 + u - v,$$
$$y = u + 2v,$$
$$z = -1 - u + v.$$

[1)] Читатель может найти массу интересных сведений (в том числе и исторических) о различных кривых в книге BRIESKORN, KNÖRRER (1986) (см. список литературы).— *Прим. ред.*

Найдите уравнение этой плоскости. Указание: пусть эта плоскость задана уравнением $ax + by + cz = d$. Подставьте вместо x, y и z их параметрические выражения; тогда вы получите систему уравнений, из которой можно найти a, b, c, d. Второй способ — это записать параметризацию в векторном виде: $(1, 0, -1) + u(1, 1, -1) + v(-1, 2, 1)$. Теперь можно быстро получить решения с помощью векторного произведения.

14. В этой задаче рассматриваются выпуклые множества, а результат будет использован в следующем упражнении для доказательства утверждения о том, что кубика Безье лежит внутри своего управляющего многоугольника. Подмножество $C \subset \mathbb{R}^2$ называется *выпуклым*, если для любой пары точек $P, Q \in C$ отрезок, соединяющий P и Q, также принадлежит C.

(a) Пусть точки $P = (x, y)$ и $Q = (z, w)$ лежат в C. Докажите, что

$$t(x, y) + (1 - t)(z, w) \in C$$

при $0 \le t \le 1$.

(b) Пусть точки $P_i = (z, w)$, $1 \le i \le n$, принадлежат выпуклому множеству C. Докажите, что

$$\sum_{i=1}^{n} t_i(x_i, y_i) \in C,$$

если t_i — неотрицательные числа, такие, что $\sum_{i=1}^{n} t_i = 1$. Указание: воспользуйтесь индукцией по n.

15. Пусть кубика Безье задана уравнениями

$$x = (1-t)^3x_0 + 3t(1-t)^2x_1 + 3t^2(1-t)x_2 + t^3x_3,$$
$$y = (1-t)^3y_0 + 3t(1-t)^2y_1 + 3t^2(1-t)y_2 + t^3y_3.$$

(a) Покажите, что эти уравнения могут быть записаны в векторном виде:

$$(x, y) = (1-t)^3(x_0, y_0) + 3t(1-t)^2(x_1, y_1) + 3t^2(1-t)(x_2, y_2) + t^3(x_3, y_3).$$

(b) Используйте результат предыдущего упражнения для доказательства того, что кубика Безье лежит внутри управляющего многоугольника. Указание: что можно сказать о сумме коэффициентов уравнения из п. (a)?

16. Кубики Безье не могут, к сожалению, точно аппроксимировать такие кривые, как окружности и гиперболы. В этом упражнении мы рассмотрим метод параметризации конических сечений, аналогичный методу, рассмотренному в примере 4. Наше изложение основано на работе BALL (1987).

Коническим сечением называется плоская кривая, заданная уравнением второй степени вида $ax^2 + bxy + cy^2 + dx + ey + f = 0$.

Окружности, эллипсы, параболы и гиперболы являются коническими сечениями. Рассмотрим теперь кривую, параметризованную следующим образом:

$$x = \frac{(1-t)^2x_1 + 2t(1-t)wx_2 + t^2x_3}{(1-t)^2 + 2t(1-t)w + t^2},$$

$$y = \frac{(1-t)^2y_1 + 2t(1-t)wy_2 + t^2y_3}{(1-t)^2 + 2t(1-t)w + t^2},$$

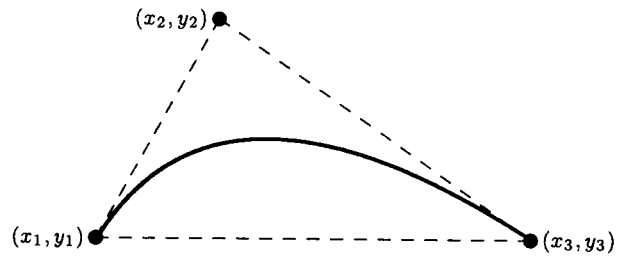
$0 \le t \le 1$. Константы $w, x_1, y_1, x_2, y_2, x_3, y_3$ определяются проектировщиком, и мы будем считать, что $w \ge 0$. В гл. 3 мы докажем, что эти уравнения параметризуют коническое сечение. Цель этого упражнения — дать геометрическую интерпретацию значений параметров $w, x_1, y_1, x_2, y_2, x_3, y_3$.

(a) Докажите, что если $w \ge 0$, то знаменатель в приведенных выше формулах не обращается в нуль.

(b) Вычислите значения x и y при $t = 0$ и $t = 1$. Результат этих вычислений объяснит вам геометрический смысл параметров x_1, y_1, x_3, y_3.

(c) Теперь найдите $(x'(0), y'(0))$ и $(x'(1), y'(1))$. Докажите, что точка (x_2, y_2) является пересечением касательных к кривой в ее начальной и конечной точках. Объясните, почему (x_1, y_1), (x_2, y_2) и (x_3, y_3) называются управляющими точками кривой.

(d) Определите управляющий многоугольник (в нашем случае он будет треугольником) и докажите, что кривая всегда лежит внутри своего управляющего многоугольника. Указание: используйте метод предыдущего упражнения. Таким образом, мы получаем следующий рисунок:

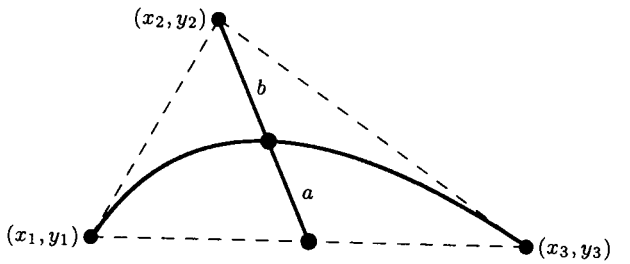


Нам осталось дать геометрическую интерпретацию константы w, которая называется *фактором формы*. Некоторый намек здесь дает п. (c), где w входит в формулы, задающие касательные векторы при $t = 0$ и $t = 1$. Можно сказать, что w управляет «скоростью» и чем больше w, тем меньше расстояние от кривой до точки (x_2, y_2). В двух последних пунктах этого упражнения мы определим точно роль w.

(e) Докажите, что

$$(x(1/2), y(1/2)) = \frac{1}{1+w}\left(\frac{1}{2}(x_1, y_1) + \frac{1}{2}(x_3, y_3)\right) + \frac{w}{1+w}(x_2, y_2).$$

Применяя эту формулу, докажите, что точка $(x(1/2), y(1/2))$ принадлежит отрезку, соединяющему точку (x_2, y_2) с серединой отрезка $[(x_1, y_1), (x_3, y_3)]$.



(f) Пусть точка $(x(1/2), y(1/2))$ разбивает отрезок на две части, имеющие длины a и b (см. предыдущий рисунок). Докажите, что $w = a/b$, т. е. w указывает, где кривая пересекает отрезок. Указание: примените формулу для нахождения расстояния между двумя точками на плоскости.

17. Примените результаты предыдущего упражнения для параметризации дуги окружности $x^2 + y^2 = 1$ с концевыми точками $(1, 0)$ и $(0, 1)$. Указание: примените п. (f) упр. 16 и докажите, что $w = 1/\sqrt{2}$.

§ 4. Идеалы

Определим теперь основной алгебраический объект этой книги.

Определение 1. Подмножество $I \subset k[x_1, \ldots, x_n]$ называется *идеалом*, если выполнены следующие условия:

(i) $0 \in I$;
(ii) если $f, g \in I$, то $f + g \in I$;
(iii) если $f \in I$ и $h \in k[x_1, \ldots, k_n]$, то $hf \in I$.

Цель этого параграфа — показать читателю, насколько естественно понятие идеала, как идеалы связаны с аффинными многообразиями и как на языке идеалов формулировать и решать вычислительные задачи аффинной геометрии.

Самый простой пример идеала — это идеал, порожденный конечным множеством полиномов.

Определение 2. Пусть $f_1, \dots, f_s$ — полиномы в $k[x_1, \dots, x_n]$. Положим

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\}.$$

Оказывается, что множество $\langle f_1, \dots, f_s \rangle$ — идеал.

Лемма 3. *Пусть $f_1, \dots, f_s$ принадлежат кольцу $k[x_1, \dots, x_n]$; тогда множество $\langle f_1, \dots, f_s \rangle$ является идеалом в $k[x_1, \dots, x_n]$. Оно называется* идеалом, порожденным полиномами $f_1, \dots, f_s$, *а полиномы $f_1, \dots, f_s$* — образующими *этого идеала или его* порождающими элементами.

Доказательство. Прежде всего, $0 \in \langle f_1, \dots, f_s \rangle$, поскольку $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Пусть теперь $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} q_i f_i$ и $h \in k[x_1, \dots, x_n]$. Тогда из равенств

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i,$$

$$hf = \sum_{i=1}^{s} (h p_i) f_i$$

вытекает, что $\langle f_1, \dots, f_s \rangle$ — идеал. □

Идеал $\langle f_1, \dots, f_s \rangle$ имеет изящную интерпретацию на языке полиномиальных уравнений. Пусть $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Рассмотрим систему уравнений

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_s &= 0. \end{aligned}$$

Из этих уравнений мы можем вывести другие, используя обычные алгебраические преобразования. Так, например, если мы умножим первое уравнение на $h_1 \in k[x_1, \dots, x_n]$, второе — на $h_2 \in k[x_1, \dots, x_n]$ и т. д., а затем сложим произведения, то получим уравнение

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0,$$

которое является следствием уравнений первоначальной системы. Отметим, что левая часть этого уравнения принадлежит идеалу $\langle f_1, \dots, f_s \rangle$, т. е. идеал $\langle f_1, \dots, f_s \rangle$ можно рассматривать как множество всех «полиномиальных следствий» системы $f_1 = f_2 = \dots = f_s = 0$.

Чтобы понять, что это означает практически, рассмотрим пример из § 3 — систему

$$\begin{aligned} x &= 1 + t, \\ y &= 1 + t^2. \end{aligned}$$

В § 3 мы исключили t и получили уравнение

$$y = x^2 - 2x + 2$$

(см. обсуждение уравнения (7) в § 3). Теперь решим эту задачу еще раз, используя новую идеологию. Перепишем уравнения в виде

$$\begin{aligned} x - 1 - t &= 0, \\ y - 1 - t^2 &= 0. \end{aligned} \tag{1}$$

Чтобы исключить t, умножим первое уравнение на $x - 1 + t$, а второе — на -1:

$$\begin{aligned} (x-1)^2 - t^2 &= 0, \\ -y + 1 + t^2 &= 0, \end{aligned}$$

а потом сложим их:

$$(x-1)^2 - y + 1 = x^2 - 2x + 2 - y = 0.$$

Если теперь рассмотреть идеал, порожденный левыми частями уравнений системы (1), то полученный результат можно сформулировать так:

$$\begin{aligned} &x^2 - 2x + 2 - y \\ &\quad = (x - 1 + t)(x - 1 - t) + (-1)(y - 1 - t^2) \in \langle x - 1 - t, y - 1 - t^2 \rangle. \end{aligned}$$

Аналогичным образом и другие «полиномиальные следствия» системы (1) являются элементами этого идеала.

Идеал I называется *конечно порожденным*, если существуют полиномы $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, такие, что $I = \langle f_1, \dots, f_s \rangle$; при этом множество полиномов $f_1, \dots, f_s$ называется *базисом* идеала I. В гл. 2 мы докажем удивительный факт, что *каждый* идеал в $k[x_1, \dots, x_n]$ конечно порожден, т. е. имеет конечную систему образующих (это утверждение называется теоремой Гильберта о базисе). Отметим, что идеал может иметь много различных базисов. В гл. 2 мы покажем, что можно определить особенно удобный базис, называемый базисом Грёбнера.

Следует обратить внимание на аналогию с линейной алгеброй. Определение идеала похоже на определение подпространства: и то, и другое множества замкнуты относительно операций сложения и умножения, только в случае подпространства идет речь об умножении на скаляры, а в случае идеала мы умножаем на полиномы.

Далее, идеал, порожденный полиномами $f_1, \ldots, f_s$, аналогичен линейной оболочке векторов $v_1, \ldots, v_s$. В обоих случаях мы строим линейные комбинации — с числовыми коэффициентами для линейной оболочки и с полиномиальными коэффициентами для идеала. Связи теории идеалов с линейной алгеброй будут также рассматриваться в упр. 5.

О роли идеалов говорит и следующее предложение, в котором доказывается, что многообразие зависит лишь от *идеала*, порожденного определяющими уравнениями.

Предложение 4. *Пусть $f_1, \ldots, f_s$ и $g_1, \ldots, g_t$ — базисы одного и того же идеала в $k[x_1, \ldots, x_n]$, так что $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. Тогда $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.*

Доказательство этого утверждения достаточно просто и его можно оставить читателю в качестве упражнения. □

Рассмотрим в качестве примера многообразие $\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$. Легко показать, что $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ (см. упр. 3), так что в силу предложения 4

$$\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}.$$

Таким образом, изменяя базис идеала, мы упрощаем процедуру описания многообразия.

Возможность изменять базис, не меняя многообразия, очень важна и полезна. Немного позже мы увидим, что многообразия определяются *идеалами*, а не уравнениями. (Соответствие между идеалами и многообразиями — главный предмет рассмотрения гл. 4). С точки зрения практики вычислений мы увидим, что предложение 4 и упомянутые выше базисы Грёбнера представляют собой мощный метод изучения аффинных многообразий.

Теперь мы обсудим, как аффинные многообразия связаны с интересным классом идеалов. Пусть $V = \mathbf{V}(f_1, \ldots, f_s) \subset k^n$ — аффинное многообразие, определенное полиномами $f_1, \ldots, f_s \in k[x_1, \ldots, k_n]$. Мы знаем, что $f_1, \ldots, f_s$ обращаются в нуль на V, но только ли они? Есть ли другие полиномы, равные нулю на V? Рассмотрим, например, скрученную кубику из § 2. Эта кубика определена как множество, где полиномы $y - x^2$ и $z - x^3$ равны нулю. Однако параметризация (t, t^2, t^3) из § 3 показывает нам, что и полиномы $z - xy$ и $y^2 - xz$, обращаются в нуль на кубике. Есть ли еще полиномы с тем же свойством? Как найти все такие полиномы?

Чтобы ответить на эти вопросы, надо рассматривать множество *всех* полиномов, которые обращаются в нуль на заданном многообразии.

Определение 5. Пусть $V \subset k^n$ — аффинное многообразие. Положим

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ для всех } (a_1, \ldots, a_n) \in V\}.$$

Оказывается, что $\mathbf{I}(V)$ — идеал.

Лемма 6. *Пусть $V \subset k^n$ — аффинное многообразие. Тогда $\mathbf{I}(V)$ — идеал, который мы будем называть* идеалом многообразия V.

Доказательство. Ясно, что $0 \in \mathbf{I}(V)$, так как нулевой полином обращается в нуль на k^n и на V в частности. Пусть $f, g \in \mathbf{I}(V)$ и $h \in k[x_1, \ldots, x_n]$. Пусть $(a_1, \ldots, a_n)$ — произвольная точка из V. Тогда

$$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0,$$
$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0.$$

Отсюда следует, что $\mathbf{I}(V)$ — идеал. □

В качестве примера рассмотрим многообразие $\{(0,0)\}$, состоящее только из одной точки — начала координат в k^2. Элементами его идеала $\mathbf{I}(\{(0,0)\})$ являются полиномы, равные нулю в точке $(0,0)$. Мы утверждаем, что

$$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle.$$

В одну сторону доказательство тривиально — любой полином вида $A(x,y)x + B(x,y)y$ обращается в нуль в начале координат. Пусть теперь полином $f = \sum_{i,j} a_{ij} x^i y^j$ равен нулю в точке $(0,0)$. Тогда $a_{00} = f(0,0) = 0$ и, следовательно,

$$f = a_{00} + \sum_{i,j \neq 0} a_{ij} x^i y^j$$
$$= 0 + \left(\sum_{\substack{i,j \\ i>0}} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle.$$

Доказательство окончено.

Пусть теперь V совпадает со всем пространством k^n. Тогда $\mathbf{I}(k^n)$ состоит из полиномов, везде равных нулю. Следовательно, по предложению 5 § 1

$$\mathbf{I}(k^n) = \{0\}, \quad \text{если} \quad k \quad \text{бесконечно.}$$

(Здесь 0 обозначает нулевой полином из $k[x_1, \ldots, x_n]$.) Следует отметить, что предложение 5 § 1 эквивалентно приведенному выше

утверждению. В упражнениях мы обсудим случай конечного поля k.

Скрученная кубика $V = \mathbf{V}(y - x^2, z - x^3) \subset \mathbb{R}^3$ представляет собой более интересный пример. Докажем, что

$$\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle.$$

Для этого сначала докажем, что любой полином $f \in \mathbb{R}[x, y, z]$ можно представить в виде

$$f = h_1(y - x^2) + h_2(z - x^3) + r, \tag{2}$$

где $h_1, h_2 \in \mathbb{R}[x, y, z]$, а r зависит только от x. Пусть сначала f является мономом $x^\alpha y^\beta z^\gamma$. Тогда по формуле бинома

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (x^2 + (y - x^2))^\beta (x^3 + (z - x^3))^\gamma \\ &= x^\alpha (x^{2\beta} + \text{члены, содержащие } y - x^2) \\ &\quad \times (x^{3\gamma} + \text{члены, содержащие } z - x^3), \end{aligned}$$

и, приводя подобные члены, получаем

$$x^\alpha y^\beta z^\gamma = h_1(y - x^2) + h_2(z - x^3) + x^{\alpha+2\beta+3\gamma}$$

для некоторых полиномов $h_1, h_2 \in \mathbb{R}[x, y, z]$. Другими словами, утверждение (2) в этом случае справедливо. Но так как любой полином $f \in \mathbb{R}[x, y, z]$ является $\mathbb{R}$-линейной комбинацией мономов, то, значит, (2) верно всегда.

Теперь мы можем доказать, что $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$. Сначала заметим, что $y - x^2, z - x^3 \in \mathbf{I}(V)$ согласно определению скрученной кубики V, а так как $\mathbf{I}(V)$ идеал, то $h_1(y - x^2) + h_2(z - x^3) \in \mathbf{I}(V)$. Поэтому $\langle y - x^2, z - x^3 \rangle \subset \mathbf{I}(V)$. Докажем теперь обратное включение. Пусть $f \in \mathbf{I}(V)$ и

$$f = h_1(y - x^2) + h_2(z - x^3) + r$$

— разложение, указанное формулой (2). Для доказательства равенства $r = 0$ мы используем параметризацию кубики (t, t^2, t^3). Так как f равен нулю на V, то

$$0 = f(t, t^2, t^3) = 0 + 0 + r(t)$$

(напомним, что r зависит только от x). Так как t может быть любым вещественным числом, то $r \in \mathbb{R}[x]$ — нулевой полином по предложению 5 § 1. Но если $r = 0$, то f имеет требуемое представление и $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$.

То, что мы делали в (2), напоминает деление полиномов, но только мы делим сразу на два полинома, а не на один. На самом деле (2) есть частный случай обобщенного алгоритма деления, который будет рассмотрен в гл. 2.

Мы можем сформулировать красивое следствие наших рассуждений: если $f \in \mathbb{R}[x, y, z]$, то $f \in \langle y - x^2, z - x^3 \rangle$ в том и только том случае, когда полином $f(t, t^2, t^3)$ тождественно равен нулю. Это дает нам эффективный алгоритм для решения вопроса о принадлежности полинома идеалу. Но этот метод связан с параметризацией. Можно ли ответить на этот вопрос, не опираясь на параметризацию (t, t^2, t^3)? В гл. 2 мы узнаем, как это сделать, используя базисы Грёбнера и обобщенный алгоритм деления.

Пример скрученной кубики подсказывает нам, как сформулировать задачу в общем виде. Сначала мы взяли полиномы $y - x^2$ и $z - x^3$, с их помощью определили аффинное многообразие, затем рассмотрели идеал функций, обращающихся в нуль на этом многообразии, и в результате получили идеал, порожденный теми же двумя полиномами. Естественно спросить, всегда ли это верно. Пусть $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Имеем

$$\begin{matrix} \text{полиномы} \\ f_1, \ldots, f_s \end{matrix} \longrightarrow \begin{matrix} \text{многообразие} \\ \mathbf{V}(f_1, \ldots, f_s) \end{matrix} \longrightarrow \begin{matrix} \text{идеал} \\ \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)). \end{matrix}$$

Возникает естественный вопрос: верно ли, что $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$? К сожалению, ответ здесь не всегда оказывается положительным. Наилучший ответ, который мы можем дать, — это следующее утверждение.

Лемма 7. *Пусть* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. *Тогда* $\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, *но эти два идеала не всегда совпадают.*

Доказательство. Пусть $f \in \langle f_1, \ldots, f_s \rangle$. Тогда $f = \sum_{i=1}^s h_i f_i$, $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$. Так как $f_1, \ldots, f_s$ обращаются в нуль на $\mathbf{V}(f_1, \ldots, f_s)$, то и $\sum_{i=1}^s h_i f_i$ также обращается в нуль на $\mathbf{V}(f_1, \ldots, f_s)$; значит, $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.

Теперь нам нужно привести пример, когда идеал $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ строго больше идеала $\langle f_1, \ldots, f_s \rangle$. Мы докажем, что включение

$$\langle x^2, y^2 \rangle \subset \mathbf{I}(\mathbf{V}(x^2, y^2))$$

не является равенством. Сначала опишем идеал $\mathbf{I}(\mathbf{V}(x^2, y^2))$. Система уравнений $x^2 = y^2 = 0$ определяет многообразие, состоящее из одной точки $\mathbf{V}(x^2, y^2) = \{(0, 0)\}$. Но мы видели раньше, что идеал многообразия $\{(0, 0)\}$ есть $\langle x, y \rangle$, т. е. $\mathbf{I}(\mathbf{V}(x^2, y^2)) = \langle x, y \rangle$. Для того чтобы убедиться, что этот идеал строго больше идеала $\langle x^2, y^2 \rangle$, достаточно заметить, что $x \notin \langle x^2, y^2 \rangle$, так как все члены полинома $h_1(x, y)x^2 + h_2(x, y)y^2$ имеют степень не меньше двух. □

В случае произвольных полей связь между идеалами $\langle f_1, \ldots, f_s \rangle$ и $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ может быть довольно сложной (в упражнениях

рассмотрено несколько примеров на эту тему). Однако если поле алгебраически замкнуто, как $\mathbb{C}$, то связь между этими идеалами достаточно проста. Все это будет объяснено в ходе доказательства теоремы Гильберта о нулях в гл. 4.

Хотя в общем случае $\mathbf{I}(\mathbf{V}(f_1,\dots,f_s))$ не равен $\langle f_1,\dots,f_s\rangle$, идеал многообразия всегда определяет многообразие однозначно.

Предложение 8. *Пусть V и W — аффинные многообразия в k^n. Тогда*

(i) *$V \subset W$ в том и только том случае, когда $\mathbf{I}(V) \supset \mathbf{I}(W)$.*
(ii) *$V = W$ в том и только том случае, когда $\mathbf{I}(V) = \mathbf{I}(W)$.*

Доказательство. Мы оставляем читателю в качестве упражнения доказательство того, что п. (ii) является непосредственным следствием п. (i). Докажем (i). Пусть сначала $V \subset W$; тогда любой полином, равный нулю на W, равен нулю и на V, а значит, $\mathbf{I}(W) \subset \mathbf{I}(V)$. Пусть теперь $\mathbf{I}(W) \subset \mathbf{I}(V)$. Пусть многообразие W определено полиномами $g_1,\dots,g_t \in k[x_1,\dots,x_n]$. Тогда $g_1,\dots,g_t \in \mathbf{I}(W) \subset \mathbf{I}(V)$; значит, g_i обращаются в нуль на V. Но W есть множество общих нулей полиномов g_i, а следовательно, $V \subset W$. □

Связь между аффинными многообразиями и идеалами сложна и разнообразна. Здесь мы затронули только верхушку айсберга. Далее эта связь будет рассмотрена в гл. 4. В частности, мы увидим, что теоремы об идеалах имеют разнообразные геометрические следствия. А теперь сформулируем три проблемы, касающиеся идеалов в $k[x_1,\dots,x_n]$:

- (Описание идеала) Каждый ли идеал $I \subset k[x_1,\dots,x_n]$ является конечно порожденным, т. е. всегда ли $I = \langle f_1,\dots,f_s\rangle$ для некоторых $f_1,\dots,f_s \in k[x_1,\dots,x_n]$?
- (Принадлежность идеалу) Пусть $f_1,\dots,f_s \in k[x_1,\dots,x_n]$. Существует ли алгоритм, позволяющий решить вопрос о принадлежности полинома $f \in k[x_1,\dots,x_n]$ идеалу $\langle f_1,\dots,f_s\rangle$?
- (Теорема о нулях) Пусть $f_1,\dots,f_s \in k[x_1,\dots,x_n]$. Какова точная связь между $\langle f_1,\dots,f_s\rangle$ и $\mathbf{I}(\mathbf{V}(f_1,\dots,f_s))$?

В следующих главах эти проблемы будут полностью решены (мы также объясним происхождение названия теоремы о нулях), хотя следует быть осторожным в вопросе о выборе основного поля.

Упражнения к § 4

1. Рассмотрим уравнения
$$x^2 + y^2 - 1 = 0,$$
$$xy - 1 = 0,$$
которые описывают пересечение окружности и гиперболы.
   (a) Алгебраическим преобразованием исключите y из этих уравнений.
   (b) Покажите, что полином, найденный в п. (a), принадлежит $\langle x^2 + y^2 - 1, xy - 1\rangle$. Указание: надо умножить второе уравнение на $xy + 1$.

2. Пусть $I \subset k[x_1,\dots,x_n]$ — идеал, а $f_1,\dots,f_s \in k[x_1,\dots,x_n]$. Докажите эквивалентность следующих условий:
   (i) $f_1,\dots,f_s \in I$;
   (ii) $\langle f_1,\dots,f_s\rangle \subset I$.
   Этот критерий полезен при доказательстве того, что один идеал принадлежит другому (как множество).

3. Примените критерий из предыдущего упражнения для доказательства следующих утверждений об идеалах в $k[x,y]$:
   (a) $\langle x+y, x-y\rangle = \langle x, y\rangle$.
   (b) $\langle x+xy, y+xy, x^2, y^2\rangle = \langle x, y\rangle$.
   (c) $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle = \langle x^2-4, y^2-1\rangle$.
   Это упражнение показывает, что идеал может иметь несколько базисов, и различные базисы могут иметь даже различное число элементов[1)].

4. Докажите предложение 4.

5. Докажите, что $\mathbf{V}(x+xy, y+xy, x^2, y^2) = \mathbf{V}(x,y)$. Указание: воспользуйтесь результатом упр. 3.

6. Термин «базис» используется в математике во многих смыслах. В этом упражнении мы увидим, что «базис идеала», определенный в этом параграфе, — это совсем не то же самое, что «базис подпространства», определяемый в линейной алгебре.
   (a) Рассмотрим идеал $I = \langle x\rangle \subset k[x]$. Как идеал I обладает базисом, состоящим из одного элемента x. Но I также является подпространством в векторном пространстве $k[x]$. Докажите, что любой базис идеала I как векторного пространства содержит бесконечное количество элементов. Указание: достаточно найти один бесконечный базис. Таким образом, то, что мы можем умножать x на элементы из $k[x]$, а не только из k, позволяет идеалу $\langle x\rangle$ иметь конечный базис.

[1)] Это, впрочем, видно и из равенства $\langle f_1,\dots,f_m\rangle = \langle f_1,\dots,f_m,h\rangle$, $h \in \langle f_1,\dots,f_m\rangle$, которое читатель легко докажет сам.— *Прим. ред.*

(b) В линейной алгебре элементы базиса данного подпространства должны быть линейно независимыми над k, и, кроме того, их линейная оболочка и есть это подпространство. В случае идеала оболочка его базиса совпадает с идеалом, но о независимости в определении нет речи. Причина здесь в том, что, как только коэффициенты становятся полиномиальными, независимость невозможна. В качестве примера рассмотрим идеал $\langle x, y\rangle \subset k[x, y]$. Покажите, что 0 является линейной комбинацией полиномов x и y с ненулевыми полиномиальными коэффициентами.

(c) Обобщим предыдущую задачу. Пусть $f_1, \ldots, f_s$ — базис идеала $I \subset k[x_1, \ldots, x_n]$. Пусть $s \geq 2$ и $f_i \neq 0$ для всех i. Докажите, что 0 является линейной комбинацией с ненулевыми полиномиальными коэффициентами полиномов f_i и f_j для любой пары i, j.

(d) Отсутствие независимости означает, что коэффициенты h_i разложения $f = \sum_{i=1}^{s} h_i f_i$ элемента $f \in \langle f_1, \ldots, f_s\rangle$ не определены однозначно. Рассмотрим, например, $f = x^2 + xy + y^2 \in \langle x, y\rangle$. Представьте f как линейную комбинацию x и y двумя разными способами. (Хотя h_i и не определены однозначно, мы можем измерить степень их неоднозначности. Это приводит к интересной теме сизигий.)

(e) Базис $f_1, \ldots, f_s$ идеала I называется *минимальным*, если никакое собственное подмножество множества $f_1, \ldots, f_s$ не является базисом этого идеала I. Например, x, x^2 — базис некоторого идеала, но не минимальный, так как x порождает тот же самый идеал. К сожалению, идеал может иметь минимальные базисы, состоящие из различного числа элементов. Докажите, что x и $x + x^2, x^2$ — минимальные базисы одного и того же идеала в $k[x]$. Объясните, чем отличается этот результат от ситуации в линейной алгебре.

7. Докажите, что $\mathbf{I}(\mathbf{V}(x^n, y^m)) = \langle x, y\rangle$ для любых положительных n и m.

8. Идеал многообразия $\mathbf{I}(V)$ обладает особым свойством, которым не обладает произвольный идеал. А именно, идеал I называется *радикальным*, если из условия $f^m \in I$ следует, что $f \in I$ (показатель степени m может быть любым). Точнее, идеал I называется радикальным, если $f \in I$ тогда и только тогда, когда $f^m \in I$ для некоторого натурального m.
   (a) Докажите, что $\mathbf{I}(V)$ всегда является радикальным идеалом.
   (b) Докажите, что идеал $\langle x^2, y^2\rangle$ не является радикальным. Отсюда следует, что $\langle x^2, y^2\rangle \neq \mathbf{I}(V)$ ни для какого многообразия $V \subset k^2$.

Радикальные идеалы будут играть важную роль в гл. 4. В частности, теорема о нулях устанавливает взаимно однозначное соответствие между многообразиями в $\mathbb{C}^n$ и радикальными идеалами в $\mathbb{C}[x_1, \ldots, x_n]$.

9. Обозначим через V скрученную кубику $V = \mathbf{V}(y - x^2, z - x^3)$. Ранее мы доказали, что $\mathbf{I}(V) = \langle y - x^2, z - x^3\rangle$.
   (a) Примените параметризацию скрученной кубики, чтобы доказать, что $y^2 - xz \in \mathbf{I}(V)$.
   (b) Используя метод, описанный в тексте параграфа, представьте $y^2 - xz$ в виде комбинации $y - x^2$ и $z - x^3$.

10. Метод, использованный в тексте параграфа при рассмотрении скрученной кубики, примените для доказательства того, что $\mathbf{I}(\mathbf{V}(x - y)) = \langle x - y\rangle$. Аргументы должны быть применимы в случае любого основного бесконечного поля k.

11. Пусть $V \subset \mathbb{R}^3$ — кривая с параметризацией (t, t^3, t^4).
   (a) Докажите, что V — аффинное многообразие.
   (b) Опишите идеал $\mathbf{I}(V)$ с помощью метода, использованного в случае скрученной кубики.

12. Пусть $V \subset \mathbb{R}^3$ — кривая с параметризацией (t^2, t^3, t^4).
   (a) Докажите, что V — аффинное многообразие.
   (b) Опишите идеал $\mathbf{I}(V)$.

Эта задача немного труднее предыдущей: найти аналог уравнения (2) не очень легко. Алгоритм деления из гл. 2 делает подобные задачи значительно менее сложными.

13. В упр. 2 § 1 мы доказали, что функция $x^2y + y^2x$ равна нулю во всех точках пространства $\mathbb{F}_2^2$. Пусть теперь $I \subset \mathbb{F}_2[x, y]$ — идеал полиномов, равных нулю во всех точках из $\mathbb{F}_2^2$. Цель этого упражнения — доказать, что $I = \langle x^2 - x, y^2 - y\rangle$.
   (a) Докажите, что $\langle x^2 - x, y^2 - y\rangle \subset I$.
   (b) Докажите, что любой полином $f \in \mathbb{F}_2[x, y]$ может быть записан в виде $f = A(x^2 - x) + B(y^2 - y) + axy + bx + cy + d$, где $A, B \in \mathbb{F}_2[x, y]$ и $a, b, c, d \in \mathbb{F}_2$. Указание: запишите f в виде $\sum_i p_i(x)y^i$ и примените алгоритм деления (предложение 2 § 5), чтобы разделить каждый p_i на $x^2 - x$. Мы получим, что $f = A(x^2 - x) + q_1(y)x + q_2(y)$. Теперь следует разделить q_1 и q_2 на $y^2 - y$. Опять-таки все рассуждения становятся много проще при использовании алгоритма деления из гл. 2.
   (c) Докажите, что $axy + bx + cy + d \in I$ в том и только том случае, когда $a = b = c = d = 0$.
   (d) Завершите доказательство того, что $I = \langle x^2 - x, y^2 - y\rangle$.
   (e) Представьте $x^2y + y^2x$ как комбинацию полиномов $x^2 - x$ и $y^2 - y$. Указание: используйте тот факт, что $2 = 1 + 1 = 0$ в $\mathbb{F}_2$.

14. В этом упражнении рассматривается предложение 8.
   (a) Докажите, что п. (ii) этого предложения является следствием п. (i).

(b) Докажите такое следствие предложения 8: пусть V и W — аффинные многообразия в k^n; тогда V строго содержится в W в том и только том случае, когда $\mathbf{I}(W)$ строго содержится в $\mathbf{I}(V)$.

15. Мы дали определение идеала $\mathbf{I}(V)$ многообразия $V \subset k^n$. Можно обобщить это определение следующим образом: пусть $S \subset k^n$ — *произвольное* подмножество; положим

$$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \quad \text{для всех} \quad (a_1, \ldots, a_n) \in S\}.$$

(a) Докажите, что $\mathbf{I}(S)$ — идеал.

(b) Пусть $X = \{(a, a) \in \mathbb{R}^2 : a \neq 1\}$. Из упр. 8 § 2 мы знаем, что X не является аффинным многообразием. Найдите $\mathbf{I}(X)$. Указание: обратите внимание на то, что именно было доказано в упр. 8 § 2. Используйте также упр. 10 из этого параграфа.

(c) Пусть $\mathbb{Z}^n$ — подмножество точек в $\mathbb{C}^n$ с целыми координатами. Найдите $\mathbf{I}(\mathbb{Z}^n)$. Указание: воспользуйтесь результатами упр. 6 § 1.

§ 5. Полиномы от одной переменной

В этом параграфе мы будем рассматривать *алгоритм деления* полиномов от одной переменной, который изучается в старших классах школы. Применение этого простого алгоритма дает неожиданно сильные результаты. Например, с его помощью мы определим структуру идеалов в $k[x]$ и исследуем понятие *наибольшего общего делителя*. Рассматриваемые здесь методы позволяют (в случае $k[x]$) решить большинство проблем, сформулированных в предыдущих параграфах. Мы приблизимся тут также к пониманию важной роли алгоритмов.

Студент, который читает эту книгу, уже изучал различные алгоритмы, хотя сам термин «алгоритм» мог и не произноситься. Неформально говоря, алгоритм — это набор инструкций для работы с символьными или численными данными. Примерами здесь являются формулы дифференцирования или метод приведения матриц к ступенчатому виду. Для каждого алгоритма определено множество *входных данных* — т. е. множество объектов, которые обрабатываются алгоритмом, и множество *выходных данных* — результат работы алгоритма. На каждом шаге работы алгоритм «знает», что он должен делать на следующем шаге.

Как правило, работая с алгоритмами, мы будем использовать «псевдокод», что облегчит нам понимание формальных структур. Описание псевдокода дано в приложении B. Псевдокод похож на язык программирования Паскаль, и алгоритмы, написанные на нем, легко компьютеризуются. Следует отметить, что большинство рассматриваемых здесь алгоритмов реализованы в системах компьютерной алгебры AXIOM, Macsyma, Maple, Mathematica, REDUCE и других. В приложении C дано краткое описание этих систем.

Мы начнем с рассмотрения алгоритма деления в $k[x]$. Важнейшей частью алгоритма является понятие «старшего члена» полинома от одной переменной. Вот точное определение.

Определение 1. Пусть $f \in k[x]$ — ненулевой полином,

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$

где $a_i \in k$ и $a_0 \neq 0$ (т. е. $\deg(f) = m$). Тогда $a_0 x^m$ называется *старшим членом* полинома f и обозначается $\mathrm{LT}(f) = a_0 x^m$ («LT» — первые буквы английского термина «leading term»).

Например, если $f = 2x^3 - 4x + 3$, то $\mathrm{LT}(f) = 2x^3$. Следует отметить, что если f и g — ненулевые полиномы, то

$$\deg(f) \leq \deg(g) \iff \mathrm{LT}(f) \text{ делит } \mathrm{LT}(g). \tag{1}$$

Теперь мы можем дать описание алгоритма деления.

Предложение 2 (алгоритм деления). *Пусть $g \in k[x]$ — ненулевой полином. Тогда любой полином $f \in k[x]$ может быть записан в виде*

$$f = qg + r,$$

где $q, r \in k[x]$ и либо $r = 0$, либо $\deg(r) < \deg(g)$. Более того, q и r определены однозначно и имеется алгоритм для их вычисления.

Доказательство. Вот алгоритм вычисления q и r, записанный в псевдокоде:

Вход: g, f
Выход: q, r
$q := 0$; $r := f$
WHILE $r \neq 0$ AND $\mathrm{LT}(g)$ делит $\mathrm{LT}(r)$ DO
    $q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$
    $r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$

Операции, подчиненные оператору цикла WHILE ... DO, выполняются, пока выполняется условие, записанное между WHILE и DO; $q := \ldots$ и $r := \ldots$ — это операторы определения или переопределения значений q и r. И q и r являются *переменными* в этом алгоритме — на каждом шаге их значения меняются. Мы должны доказать, что в некоторый момент алгоритм прекращает работу и что окончательные значения q и r удовлетворяют условиям предложения 2.

Приступим к доказательству корректности алгоритма. Заметим сначала, что равенство $f = qg + r$ выполняется при начальных значениях q и r. Далее, на каждом шаге после переопределения q и r это равенство продолжает выполняться, потому что

$$f = qg + r = (q + \mathrm{LT}(r)/\mathrm{LT}(g))g + (r - (\mathrm{LT}(r)/\mathrm{LT}(g))g).$$

Отметим, что выполнение циклического оператора WHILE ... DO прекращается, когда утверждение «$r \neq 0$ и $\mathrm{LT}(g)$ делит $\mathrm{LT}(r)$» становится ложным, т. е. когда или $r = 0$, или $\mathrm{LT}(g)$ не делит $\mathrm{LT}(r)$. По (1) последнее условие эквивалентно условию $\deg(r) < \deg(g)$. Другими словами, если алгоритм прекращает работу, то он выдает требуемые q и r.

Осталось доказать, что алгоритм обязательно остановится, т. е. что утверждение между WHILE и DO в какой-то момент станет ложным (иначе цикл будет выполняться бесконечно много раз). Здесь самым важным является тот факт, что полином $r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$ или равен нулю, или имеет степень, меньшую, чем степень полинома r. Докажем это. Пусть

$$\begin{aligned} r &= a_0x^m + \cdots + a_m, & \mathrm{LT}(r) &= a_0x^m, \\ g &= b_0x^k \ + \cdots + b_k, & \mathrm{LT}(g) &= \ b_0x^k, \end{aligned}$$

и пусть $m \geq k$. Тогда

$$r - (\mathrm{LT}(r)/\mathrm{LT}(g))g = (a_0x^m + \ldots) - (a_0/b_0)x^{m-k}(b_0x^k + \ldots),$$

и степень полинома r обязана уменьшиться (или r обращается в нуль). Так как эта степень конечна, то алгоритм останавливается после конечного числа шагов.

Сравним работу этого алгоритма с процедурой деления полиномов в том виде, как она изучается в школе[1]. Вот пример незаконченного деления:

$$\begin{array}{rl} & \frac{1}{2}x^2 \\ 2x+1 & \overline{\left)x^3+2x^2+x+1\right.} \\ & \underline{x^3+\frac{1}{2}x^2} \\ & \quad \frac{3}{2}x^2+x+1 \end{array}$$

[1] Мы сохранили принятую в англоязычной литературе (и непривычную для российского школьника) форму записи деления полиномов, так как она согласуется с формой записи деления полиномов от нескольких переменных, которая будет использоваться в дальнейшем.— *Прим. ред.*

Здесь $f = x^3+2x^2+x+1$, $g = 2x+1$, а текущие (но *не* окончательные) значения q и r — это $q = \frac{1}{2}x^2$ и $r = \frac{3}{2}x^2 + x + 1$. Теперь заметим, что операторы

$$\begin{aligned} q &:= q + \mathrm{LT}(r)/\mathrm{LT}(g), \\ r &:= r - (\mathrm{LT}(r)/\mathrm{LT}(g))g \end{aligned}$$

в цикле WHILE ... DO в точности описывают следующий шаг деления.

Теперь нам осталось доказать, что q и r определены однозначно. Предположим, что $f = qg + r = q'g + r'$ и степени полиномов r и r' меньше, чем степень полинома g (либо оба или один из них равен нулю). Если $r \neq r'$, то $\deg(r - r') < \deg(g)$. С другой стороны, так как

$$(q - q')g = r' - r, \tag{2}$$

то $q' - q \neq 0$ и, следовательно,

$$\deg(r' - r) = \deg((q' - q)g) = \deg(q' - q) + \deg(g) \geq \deg(g).$$

Значит $r = r'$, и тогда из (2) следует, что $q = q'$. Доказательство закончено. □

В большинстве систем компьютерной алгебры реализован этот алгоритм, может быть, с некоторыми изменениями (см. DAVENPORT, SIRET, TOURNIER (1993)).

Следствием существования алгоритма деления является такое утверждение о количестве корней полинома от одной переменной:

Следствие 3. *Пусть $f \in k[x]$ — ненулевой полином. Тогда он имеет в k не более чем $\deg(f)$ корней.*

Доказательство. Применим индукцию по $m = \deg(f)$. Если $m = 0$, то f — ненулевая константа, и утверждение справедливо. Пусть утверждение выполняется для всех полиномов степени $m - 1$, и пусть f имеет степень m. Если f не имеет корней в k, то утверждение доказано. Пусть теперь $a \in k$ — корень полинома f. Поделим f на $x - a$. Тогда по предложению 2 имеем $f = q(x - a) + r$, где $r \in k$, так как $x - a$ имеет степень один. Положив в этом равенстве $x = a$, получим $0 = f(a) = q(a)(a - a) + r = r$, т. е. $f = q(x - a)$, и, значит, степень полинома q равна $m - 1$.

Мы утверждаем, что любой корень полинома f, отличный от a, является корнем полинома q. Если $b \neq a$ — корень полинома f, то $0 = f(b) = q(b)(b - a)$, откуда $q(b) = 0$ (так как k — поле). По предположению индукции q имеет не более $m - 1$ корней; значит, f имеет не более m корней в k. □

Именно следствие 3 и было использовано для доказательства предложения 5 § 1, где утверждалось, что если k бесконечно, то

$\mathbf{I}(k^n) = \{0\}$. Это пример того, как геометрический результат устанавливается с помощью алгоритма.

Предложение 2 позволяет также описать все идеалы в $k[x]$.

Следствие 4. *Пусть k — поле. Тогда каждый идеал в $k[x]$ может быть представлен в виде $\langle f \rangle$ для некоторого полинома $f \in k[x]$. Более того, f определен однозначно с точностью до умножения на ненулевую константу из k.*

Доказательство. Пусть $I \subset k[x]$ — некоторый идеал. Если $I = \{0\}$, то $I = \langle 0 \rangle$ и утверждение доказано. Пусть теперь $I \neq \{0\}$, и пусть $f \in I$ — ненулевой полином минимальной степени (в множестве полиномов, содержащихся в I). Мы утверждаем, что $I = \langle f \rangle$. Включение $\langle f \rangle \subset I$ очевидно, так как I — идеал. Рассмотрим теперь полином $g \in I$. В соответствии с алгоритмом деления (предложение 2) $g = qf + r$, где или $r = 0$, или $\deg(r) < \deg(f)$. Так как I — идеал, то $qf \in I$ и, значит $r = g - qf \in I$. Если $r \neq 0$, то $\deg(r) < \deg(f)$, что противоречит выбору полинома f. Значит, $r = 0$, т. е. $g = qf \in \langle f \rangle$, что доказывает равенство $I = \langle f \rangle$.

Докажем теперь единственность. Пусть $\langle f \rangle = \langle g \rangle$. Так как $f \in \langle g \rangle$, то $f = hg$ для некоторого полинома h. Имеем

$$\deg(f) = \deg(h) + \deg(g), \tag{3}$$

т. е. $\deg(f) \geq \deg(g)$. Аналогично получаем, поменяв местами f и g, что $\deg(g) \geq \deg(f)$, т. е. $\deg(f) = \deg(g)$. Теперь из (3) следует, что $\deg(h) = 0$. Значит, h — ненулевая константа. □

Идеал, порожденный одним элементом, называется *главным идеалом*. Таким образом, ввиду следствия 4 мы говорим, что $k[x]$ является *областью главных идеалов* или сокращенно ОГИ.

В доказательстве следствия 4 в качестве порождающего элемента мы взяли полином минимальной степени из числа содержащихся в идеале. Этот метод на практике неприменим, так как он требует проверки степеней всех полиномов (а их бесконечно много) из идеала. Есть ли более простой способ найти порождающий элемент? Например, как найти порождающий элемент идеала

$$\langle x^4 - 1, x^6 - 1 \rangle \subset k[x]?$$

Инструментом решения таких задач является наибольший общий делитель.

Определение 5. *Наибольшим общим делителем* полиномов $f, g \in k[x]$ называется полином h, такой, что

(i) h делит и f, и g;
(ii) если p — некоторый полином, который делит и f, и g, то p делит h.

Наибольший общий делитель будет обозначаться через $\mathrm{GCD}(f, g)$ (GCD — начальные буквы английского термина greatest common divisor).

Основные свойства наибольших общих делителей сформулированы в следующем предложении.

Предложение 6. *Пусть $f, g \in k[x]$. Тогда*

(i) $\mathrm{GCD}(f, g)$ *существует и единствен с точностью до умножения на ненулевую константу из k;*
(ii) $\mathrm{GCD}(f, g)$ *является образующим идеала $\langle f, g \rangle$;*
(iii) *существует алгоритм для вычисления* $\mathrm{GCD}(f, g)$.

Доказательство. Рассмотрим идеал $\langle f, g \rangle$. Так как каждый идеал в $k[x]$ главный (следствие 4), то найдется полином $h \in k[x]$, такой, что $\langle f, g \rangle = \langle h \rangle$. Мы утверждаем, что $h = \mathrm{GCD}(f, g)$. Сначала отметим, что h делит f и g, так как $f, g \in \langle h \rangle$. Таким образом, первый пункт определения 5 выполняется. Пусть теперь $p \in k[x]$ делит f и g. Это означает, что $f = Cp$ и $g = Dp$ для некоторых $C, D \in k[x]$. Так как $h \in \langle f, g \rangle$, то существуют полиномы A и B, такие, что $Af + Bg = h$, откуда

$$h = Af + Bg = ACp + BDp = (AC + BD)p,$$

т. е. p делит h. Значит, $h = \mathrm{GCD}(f, g)$.

Доказательство существования GCD закончено. Перейдем к доказательству единственности. Пусть h' — другой наибольший общий делитель полиномов f и g. Тогда в силу второго пункта определения 5 полиномы h и h' делят друг друга. Откуда следует, что h равен h' с точностью до умножения на ненулевую константу. Пункты (i) и (ii) предложения 6 доказаны.

Только что полученное нами доказательство существования GCD бесполезно с практической точки зрения. Рецепт вычисления GCD сводится к определению порождающего элемента идеала $\langle f, g \rangle$. Как отмечалось выше, это требует нахождения степеней бесконечного количества полиномов. К счастью, есть классический алгоритм, называемый *алгоритмом Евклида*, который позволяет вычислить наибольший общий делитель двух полиномов в $k[x]$. Описание этого алгоритма и завершит доказательство предложения 6.

Дадим сначала необходимые определения. Пусть $f, g \in k[x]$, $g \neq 0$. Запишем f в виде $f = qg + r$, где q и r определены, как в предложении 2. Тогда r называется остатком от деления f на g (мы будем писать $r = \text{остаток}(f, g)$). Теперь мы можем дать описание алгоритма Евклида:

Вход: f, g
Выход: h
$h := f$
$s := g$
WHILE $s \neq 0$ DO
$\quad rem := \text{остаток}(h, s)$
$\quad h := s$
$\quad s := rem$

Далее, необходимо объяснить, почему этот алгоритм действительно вычисляет GCD. Пусть $f = qg + r$ (как в предложении 2). Мы утверждаем, что

$$\text{GCD}(f, g) = \text{GCD}(f - qg, g) = \text{GCD}(r, g). \tag{4}$$

В силу п. (ii) этого предложения достаточно доказать, что идеалы $\langle f, g\rangle$ и $\langle f - qg, g\rangle$ совпадают. Это доказательство мы оставляем читателю в качестве упражнения.

Перепишем (4) в виде

$$\text{GCD}(f, g) = \text{GCD}(g, r).$$

Отметим, что или $\deg(g) > \deg(r)$, или $r = 0$. Если $r \neq 0$, то мы можем уменьшить степени, повторяя эту процедуру, т. е. мы записываем g в виде $g = q'r + r'$ и получаем

$$\text{GCD}(g, r) = \text{GCD}(r, r'),$$

где $\deg(r) > \deg(r')$ или $r' = 0$. Таким образом, мы имеем цепочку равенств

$$\text{GCD}(f, g) = \text{GCD}(g, r) = \text{GCD}(r, r') = \text{GCD}(r', r'') = \ldots, \tag{5}$$

причем либо степени уменьшаются:

$$\deg(g) > \deg(r) > \deg(r') > \deg(r'') > \ldots,$$

либо процесс останавливается, когда один из $r, r', r'', \ldots$ становится равным нулю.

Теперь мы можем объяснить, как работает алгоритм Евклида. Переменными алгоритма являются h и s, и эти переменные входят в состав соотношения (5): значением h является первый полином в каждом GCD, а значением s — второй. Легко убедиться, что переход в (5) от очередного GCD к следующему происходит так же, как и соответствующий переход в цикле WHILE ... DO алгоритма. Таким образом, на каждом шаге алгоритма $\text{GCD}(h, s) = \text{GCD}(f, g)$.

Работа алгоритма должна прекратиться, так как степени полинома s уменьшаются и в некоторый момент s станет равным нулю. В этот момент мы имеем $\text{GCD}(h, 0) = \text{GCD}(f, g)$, а так как $\langle h, 0\rangle = \langle h\rangle$, то $\text{GCD}(h, 0) = h$. Таким образом, $h = \text{GCD}(f, g)$, когда s обращается в нуль, т. е. в момент остановки алгоритма h равен наибольшему общему делителю полиномов f и h. Доказательство предложения 6 завершено. □

Следует также отметить, что существует вариант алгоритма Евклида, вычисляющий наибольший общий делитель двух целых чисел. В большинстве систем компьютерной алгебры реализован модифицированный алгоритм Евклида для вычисления наибольшего общего делителя двух полиномов или целых чисел (см. DAVENPORT, SIRET, TOURNIER (1993)).

Как пример работы алгоритма Евклида рассмотрим процесс вычисления $\text{GCD}(x^4 - 1, x^6 - 1)$. Сначала мы применяем алгоритм деления:

$$\begin{aligned} x^4 - 1 &= 0(x^6 - 1) + x^4 - 1, \\ x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1, \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0. \end{aligned}$$

Теперь по (5) мы имеем

$$\begin{aligned} \text{GCD}(x^4 - 1, x^6 - 1) &= \text{GCD}(x^6 - 1, x^4 - 1) = \\ &= \text{GCD}(x^4 - 1, x^2 - 1) = \text{GCD}(x^2 - 1, 0) = x^2 - 1. \end{aligned}$$

Следует отметить, что вычисление GCD дает ответ и на вопрос об определении порождающего элемента идеала $\langle x^4 - 1, x^6 - 1\rangle$, а именно из предложения 6 и того факта, что $\text{GCD}(x^4 - 1, x^6 - 1) = x^2 - 1$, следует, что $\langle x^4 - 1, x^6 - 1\rangle = \langle x^2 - 1\rangle$.

Однако здесь можно задать естественный вопрос: а как быть, когда идеал порожден тремя или большим количеством полиномов? Для этого необходимо определить наибольший общий делитель нескольких полиномов.

Определение 7. *Наибольшим общим делителем* полиномов $f_1, \ldots, f_s \in k[x]$ называется полином h, такой, что

(i) h делит $f_1, \ldots, f_s$;
(ii) если p — некоторый полином, который делит $f_1, \ldots, f_s$, то p делит h.

Такой полином h обозначается через $\text{GCD}(f_1, \ldots, f_s)$[1)].

[1)] GCD — аббревиатура английского термина greatest common divisor.— *Прим. перев.*

Основные свойства наибольшего общего делителя сформулированы в следующем предложении.

Предложение 8. *Пусть* $f_1, \dots, f_s \in k[x]$, $s \geq 2$. *Тогда*

(i) $\mathrm{GCD}(f_1, \dots, f_s)$ *существует и определен однозначно с точностью до умножения на ненулевую константу из* k;
(ii) $\mathrm{GCD}(f_1, \dots, f_s)$ *порождает идеал* $\langle f_1, \dots, f_s \rangle$;
(iii) *если* $s \geq 3$, *то* $\mathrm{GCD}(f_1, \dots, f_s) = \mathrm{GCD}(f_1, \mathrm{GCD}(f_2, \dots, f_s))$;
(iv) *существует алгоритм для вычисления* $\mathrm{GCD}(f_1, \dots, f_s)$.

Доказательство. Доказательство пп. (i) и (ii) аналогично доказательству тех же пунктов предложения 6. Докажем (iii). Пусть $h = \mathrm{GCD}(f_2, \dots, f_s)$. Тогда

$$\langle f_1, h \rangle = \langle f_1, \dots, f_s \rangle.$$

Доказательство этого факта мы оставляем читателю в качестве упражнения. Из (ii) следует, что

$$\langle \mathrm{GCD}(f_1, h) \rangle = \langle \mathrm{GCD}(f_1, \dots, f_s) \rangle.$$

Теперь равенство $\mathrm{GCD}(f_1, h) = \mathrm{GCD}(f_1, \dots, f_s)$ вытекает из второго утверждения (о единственности) следствия 4.

Наконец, нам нужно доказать существование алгоритма, вычисляющего $\mathrm{GCD}(f_1, \dots, f_s)$. Для этого нужно объединить п. (iii) и алгоритм Евклида. Пусть, например, мы хотим найти наибольший общий делитель четырех полиномов f_1, f_2, f_3, f_4. Имеем

$$\begin{aligned} \mathrm{GCD}(f_1, f_2, f_3, f_4) &= \mathrm{GCD}(f_1, \mathrm{GCD}(f_2, f_3, f_4)) \\ &= \mathrm{GCD}(f_1, \mathrm{GCD}(f_2, \mathrm{GCD}(f_3, f_4))). \end{aligned} \tag{6}$$

Таким образом, для вычисления наибольшего общего делителя полиномов f_1, f_2, f_3, f_4 нам нужно применить алгоритм Евклида три раза. Одно из упражнений к этому параграфу — написать псевдокод, реализующий алгоритм вычисления GCD для произвольного количества полиномов. Предложение 8 доказано. □

Процедура вычисления GCD в большинстве систем компьютерной алгебры может находить наибольший делитель только двух полиномов. Поэтому в случае трех и более полиномов необходимо использовать метод предложения 8. Рассмотрим, например, идеал

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle \subset k[x].$$

Мы знаем, что $\mathrm{GCD}(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$ порождает этот идеал. Далее, легко проверить, что

$$\begin{aligned} \mathrm{GCD}(x^3-3x+2, x^4-1, x^6-1) &= \mathrm{GCD}(x^3-3x+2, \mathrm{GCD}(x^4-1, x^6-1)) \\ &= \mathrm{GCD}(x^3-3x+2, x^2-1) = x-1, \end{aligned}$$

т. е.

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle = \langle x - 1 \rangle.$$

Теперь понятно, как должен быть построен алгоритм вычисления порождающего элемента идеала $\langle f_1, \dots, f_s \rangle$, $f_1, \dots, f_s \in k[x]$.

В качестве следующего приложения алгоритмов деления и вычисления GCD рассмотрим *задачу о принадлежности идеалу*, упомянутую в § 4: существует ли алгоритм, позволяющий определить для произвольного полинома $f \in k[x]$ и заданных полиномов $f_1, \dots, f_s \in k[x]$, лежит f в идеале $\langle f_1, \dots, f_s \rangle$ или нет. Ответ утвердительный, и такой алгоритм несложно описать. Первый шаг — это вычисление $\mathrm{GCD}(f_1, \dots, f_s)$, т. е. определение порождающего элемента h идеала $\langle f_1, \dots, f_s \rangle$. Так как включение $f \in \langle f_1, \dots, f_s \rangle$ эквивалентно включению $f \in \langle h \rangle$, то нам осталось только поделить f на h с остатком: $f = qh + r$, $\deg(r) < \deg(h)$. Таким образом, f принадлежит идеалу в том и только том случае, когда $r = 0$. Пусть, например, мы хотим узнать, верно ли, что

$$x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle.$$

Мы знаем, что $x - 1$ — порождающий элемент этого идеала, так что нам нужно ответить на вопрос, верно ли, что

$$x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle?$$

Но

$$x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1.$$

Значит, $x^3 + 4x^2 + 3x - 7$ *не* принадлежит идеалу $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$. В гл. 2 мы научимся решать задачу о принадлежности идеалу для полиномов из $k[x_1, \dots, x_n]$, используя аналогичную стратегию: сначала мы находим хороший базис идеала (базис Грёбнера), а затем применяем обобщенный алгоритм деления для решения задачи.

В упражнениях мы увидим, что в случае одной переменной ряд задач, сформулированных ранее, допускает алгоритмическое решение с помощью методов этого параграфа.

Упражнения к § 5

1. Над полем $\mathbb{C}$ следствие 3 может быть сформулировано в более сильной форме. А именно, докажите, что если $f \in \mathbb{C}[x]$ — полином степени $n > 0$, то f может быть представлен в виде произведения $f = c(x - a_1) \dots (x - a_n)$, где $c, a_1, \dots, a_n \in \mathbb{C}$ и $c \neq 0$. Указание: примените теорему 7 из § 1. Отметим, что этот результат справедлив для *любого* алгебраически замкнутого поля.
2. Хотя следствие 3 кажется простым, из него вытекает несколько интересных результатов. Например, рассмотрим определитель Вандер-

монда порядка n, где $a_1, \dots, a_n \in k$:

$$\det \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix}.$$

Докажите, что этот определитель не равен нулю, если a_i попарно различны. Указание: если определитель равен нулю, то столбцы линейно зависимы. Тогда коэффициенты линейного соотношения между столбцами определяют полином степени $\leq n-1$, который имеет n корней. Теперь примените следствие 3.

3. Утверждение, что каждый идеал в $k[x]$ является главным (т. е. порожден одним элементом), справедливо только для полиномов от одной переменной. В этом упражнении мы увидим почему. А именно, рассмотрим идеал $I = \langle x, y\rangle \subset k[x, y]$. Докажите, что I не является главным идеалом. Указание: пусть $x = fg$, где $f, g \in k[x, y]$. Докажите, что f или g — константа. Отсюда следует, что методы вычисления и работы с GCD, рассмотренные в этом параграфе, применимы только в случае одной переменной. Наибольший общий делитель может быть найден и для полиномов от $n \geq 2$ переменных, но теория и методы здесь значительно сложнее (см. DAVENPORT, SIRET, TOURNIER (1993), § 4.12).

4. Пусть $h = \mathrm{GCD}(f, g)$, $f, g \in k[x]$. Докажите, что существуют полиномы $A, B \in k[x]$, такие, что $Af + Bg = h$.

5. Пусть $f, g \in k[x]$; тогда $\langle f - qg, g\rangle = \langle f, g\rangle$ для любого $q \in k[x]$. Это докажет равенство (4).

6. Пусть $f_1, \dots, f_s \in k[x]$, и пусть $h = \mathrm{GCD}(f_2, \dots, f_s)$ (т. е. $\langle h\rangle = \langle f_2, \dots, f_s\rangle$); тогда $\langle f_1, h\rangle = \langle f_1, f_2, \dots, f_s\rangle$. Это докажет п. (iii) предложения 8.

7. Предположим, что наша процедура вычисления наибольшего общего делителя позволяет за один раз находить GCD только двух полиномов (это справедливо для большинства систем компьютерной алгебры). Напишите псевдокод алгоритма, который находит GCD полиномов $f_1, \dots, f_s \in k[x]$, $s \geq 2$. Докажите корректность алгоритма. Указание: примените равенства (6). Это завершит доказательство п. (iv) предложения 8.

8. Используйте какую-нибудь систему компьютерной алгебры для вычисления следующих GCD:
   (a) $\mathrm{GCD}(x^4 + x^2 + 1, x^4 - x^2 - 2x - 1, x^3 - 1)$.
   (b) $\mathrm{GCD}(x^3 + 2x^2 - x - 2, x^3 - 2x^2 - x + 2, x^3 - x^2 - 4x + 4)$.

9. Используйте метод, рассмотренный в тексте параграфа, для решения следующей задачи о принадлежности полинома идеалу: верно ли, что $x^2 - 4 \in \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2\rangle$?

10. Напишите псевдокод следующего алгоритма: по заданным двум полиномам $f, g \in k[x]$ он вычисляет $h, A, B \in k[x]$, где $h = \mathrm{GCD}(f, g)$, а $Af + Bg = h$. Указание: нужно добавить переменные A, B, C, D в алгоритм вычисления GCD так, чтобы соотношения $Af + Bg = h$ и $Cf + Dg = s$ выполнялись на каждом шаге алгоритма. Начальными значениями для A, B, C, D являются $1, 0, 0, 1$ соответственно. Возможно, вам покажется удобным через частное(f, g) обозначить частное от деления f на g, т. е. если в алгоритме деления $f = qg + r$, то $q =$ частное(f, g).

11. В этом упражнении мы рассмотрим *задачу совместности* из § 2 в случае одной переменной. Пусть $f_1, \dots, f_s \in k[x]$. Существует ли алгоритм, позволяющий определить пустоту или непустоту многообразия $\mathbf{V}(f_1, \dots, f_s)$? Мы увидим, что ответ утвердительный, если $k = \mathbb{C}$.
   (a) Пусть $f \in \mathbb{C}[x]$ — ненулевой полином. Примените теорему 6 из § 1 и докажите, что $\mathbf{V}(f) = \varnothing$ тогда и только тогда, когда f — константа.
   (b) Пусть $f_1, \dots, f_s \in \mathbb{C}[x]$; тогда $\mathbf{V}(f_1, \dots, f_s) = \varnothing$ в том и только том случае, когда $\mathrm{GCD}(f_1, \dots, f_s) = 1$.
   (c) Дайте (неформальное) описание алгоритма, решающего задачу о пустоте или непустоте многообразия $\mathbf{V}(f_1, \dots, f_s)$.

   Если $k = \mathbb{R}$, то задача совместности становится существенно более трудной. Здесь необходимо знать метод, позволяющий определить наличие или отсутствие вещественных корней у произвольного полинома $f \in \mathbb{R}[x]$[1)].

12. В этом упражнении мы рассмотрим *теорему о нулях* из § 4 в случае одной переменной. В этой теореме изучается связь между $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ и $\langle f_1, \dots, f_s\rangle$, когда $f_1, \dots, f_s \in \mathbb{C}[x]$. Использование GCD позволяет редуцировать задачу к случаю одного порождающего элемента. Так что задача теперь формулируется следующим образом: явно описать идеал $\mathbf{I}(\mathbf{V}(f))$, где $f \in \mathbb{C}[x]$ не является константой. Так как основное поле — это поле $\mathbb{C}$, то, согласно упр. 1, f

---

[1)] Такой метод дается одной классической теоремой Сильвестра (см. по этому поводу Procesi C. Positive Symmetric Functions, Adv. Math., **29**, 1978, 219–222). Ответ состоит в следующем (мы воспользуемся для его формулировки материалом § 1 гл. 7). Пусть $f = x^n - b_1 x^{n-1} + \dots + (-1)^n b_n, b_i \in \mathbb{R}$. Тогда $f = (x - a_1)\dots(x - a_n)$ для некоторых $a_i \in \mathbb{C}$ и $b_j = \sigma_j(a_1, \dots, a_n)$ (см. § 1 гл. 7). Положим $\psi_s = \sum_j a_j^s$ и рассмотрим симметрическую матрицу Bez, у которой на пересечении i-й строки и j-го столбца стоит элемент ψ_{i+j-2}.

Поскольку ψ_s — симметрическая функция от $a_1, \dots, a_n$, то она является полиномом от $b_1, \dots, b_n$. Для любого s этот полином, а значит, для любого n и матрица Bez могут быть явно выписаны с помощью тождеств Ньютона (см. § 1 гл. 7).

Теорема. *Сигнатура матрицы* Bez *равна числу различных вещественных корней полинома* f.

— *Прим. ред.*

полностью разлагается на множители, т. е.

$$f = c(x - a_1)^{r_1} \dots (x - a_l)^{r_l},$$

где $a_1, \dots, a_l \in \mathbb{C}$ попарно различны и $c \in \mathbb{C} - \{0\}$. Определим теперь полином

$$f_{\text{red}} = c(x - a_1) \dots (x - a_l).$$

Корни полиномов f и f_{red} совпадают, но их *кратности* могут быть различными. В частности, все корни полинома f_{red} простые (имеют кратность один). Полином f_{red} называется *редуцированной* или *свободной от квадратов* частью полинома f. Последний термин означает, что f_{red} является свободным от квадратов делителем полинома f максимальной степени.

(a) Докажите, что $\mathbf{V}(f) = \{a_1, \dots, a_l\}$.

(b) Докажите, что $\mathbf{I}(\mathbf{V}(f)) = \langle f_{\text{red}} \rangle$.

Упражнение (b), конечно, описывает $\mathbf{I}(\mathbf{V}(f))$, но ответ не является вполне удовлетворительным, так как, чтобы найти f_{red}, нам нужно полностью разложить f на множители. В упр. 13, 14 и 15 мы покажем, как найти f_{red}, *не разлагая* f на множители.

13. В этом упражнении мы рассмотрим понятие формальной производной полинома $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{C}[x]$. *Формальная производная* определяется обычной формулой из математического анализа: $f' = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1} + 0$. Докажите справедливость следующих правил дифференцирования:

$$\begin{aligned} (af)' &= af', \quad \text{когда} \quad a \in \mathbb{C}, \\ (f+g)' &= f' + g', \\ (fg)' &= f'g + fg'. \end{aligned}$$

14. В этом упражнении свойства дифференцирования, сформулированные в предыдущем упражнении, будут применены для вычисления $\text{GCD}(f, f')$, $f \in \mathbb{C}[x]$.

(a) Пусть $f = (x-a)^r h \in \mathbb{C}[x]$, где $h(a) \neq 0$; тогда $f' = (x-a)^{r-1}h_1$, где $h_1 \in \mathbb{C}[x]$ и $h_1(a) \neq 0$. Указание: примените правило дифференцирования произведения.

(b) Пусть $f = c(x-a_1)^{r_1} \dots (x-a_l)^{r_l}$, где $a_1, \dots, a_l$ попарно различны. Докажите, что $f' = (x-a_1)^{r_1-1} \dots (x-a_l)^{r_l-1}H$, где $H \in \mathbb{C}[x]$ и H отличен от нуля в точках $a_1, \dots, a_l$.

(c) Докажите, что $\text{GCD}(f, f') = (x-a_1)^{r_1-1} \dots (x-a_l)^{r_l-1}$.

15. В этом упражнении изучается свободная от квадратов часть f_{red} полинома $f \in \mathbb{C}[x]$, которая была определена в упр. 12.

(a) Примените упр. 14 и докажите, что

$$f_{\text{red}} = \frac{f}{\text{GCD}(f, f')}.$$

Ценность этой формулы состоит в том, что она позволяет находить свободную от квадратов часть, не разлагая f на множители. Это дает возможность значительно упростить вычисления.

(b) Используйте какую-нибудь систему компьютерной алгебры и найдите свободную от квадратов часть следующего полинома:

$$x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1.$$

16. Используйте упр. 12 и 15 и дайте неформальное описание алгоритма, который вычисляет базис идеала $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ для данных $f_1, \dots, f_s \in \mathbb{C}[x]$. Построить подобный алгоритм для случая полиномов от нескольких переменных *значительно* труднее.

17. Найдите базис идеала $\mathbf{I}(\mathbf{V}(x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1))$.

2
Базисы Грёбнера

§ 1. Введение

В гл. 1 мы увидели, что существует связь между алгебраическими свойствами полиномиальных колец $k[x_1, \ldots, x_n]$ и геометрическими свойствами аффинных многообразий. В этой главе будут изучаться базисы Грёбнера, которые позволяют решать алгоритмически задачи о полиномиальных идеалах. Метод базисов Грёбнера реализован во всех достаточно мощных системах компьютерной алгебры и применяется для изучения полиномиальных идеалов, возникающих в прикладных задачах. В гл. 1 мы сформулировали ряд проблем, касающихся алгебраических свойств полиномиальных идеалов и геометрии аффинных многообразий. В этой главе и в гл. 3 нас особенно будут интересовать следующие четыре задачи.

Задачи

(a) Задача описания идеала. Является ли произвольный идеал $I \subset k[x_1, \ldots, x_n]$ конечно порожденным? Другими словами, верно ли, что $I = \langle f_1, \ldots, f_s \rangle$ для некоторых $f_i \in k[x_1, \ldots, x_n]$?

(b) Задача о принадлежности идеалу. Пусть $f \in k[x_1, \ldots, x_n]$, и пусть задан идеал $I = \langle f_1, \ldots, f_s \rangle$. Принадлежит полином f идеалу I или нет? На геометрическом языке эта задача может быть сформулирована так: содержится ли многообразие $\mathbf{V}(f_1, \ldots, f_s)$ в многообразии $\mathbf{V}(f)$?

(c) Задача решения полиномиальных уравнений. Описать множество решений в k^n системы полиномиальных уравнений

$$f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0.$$

Конечно, это то же самое, что описать аффинное многообразие $\mathbf{V}(f_1, \ldots, f_s)$.

(d) Задача неявного представления. Пусть V — подмножество в k^n, заданное параметрически:

$$\begin{aligned} x_1 &= g_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= g_n(t_1, \ldots, t_m). \end{aligned}$$

Если g_i — полиномы (или рациональные функции) от переменных t_j, то V будет аффинным многообразием или его частью. Задача состоит в том, чтобы задать V полиномиальными уравнениями от переменных x_i.

Здесь необходимы некоторые пояснения. В задаче (a) спрашивается, верно ли, что любой идеал можно задать конечным числом образующих. Идеалы, с которыми мы встречались ранее, именно таковы — на самом деле мы и определяли их с помощью конечного числа образующих. Оказывается, есть и другие способы задать идеал, и не очевидно, что так заданный идеал конечно порожден. Главный пример — это идеал многообразия $\mathbf{I}(V)$. Полезно будет узнать, что такие идеалы также конечно порождены. С другой стороны, мы увидим в упражнениях, что в случае полиномов от *бесконечного* числа переменных ответ на вопрос (a) будет отрицательным.

Отметим, что задачи (c) и (d) в некотором смысле взаимно обратны. В (c) мы хотим описать множество решений полиномиальной системы. А в (d), наоборот, множество решений дано, а задача состоит в построении полиномиальной системы с такими решениями.

Прежде чем мы начнем изучать базисы Грёбнера, рассмотрим частные случаи, когда известная нам техника позволяет эти задачи решить.

Пример 1. Если $n = 1$, то задача описания идеала была решена в § 5 гл. 1. А именно, если дан идеал $I \subset k[x]$, то $I = \langle g \rangle$ для некоторого $g \in k[x]$ (следствие 4 из § 5 гл. 1). То есть в этом случае идеалы имеют совсем простое описание.

В § 5 гл. 1 было также показано, что алгоритм деления решает задачу о принадлежности идеалу: если $f \in k[x]$, то, для того чтобы узнать, принадлежит f идеалу $I = \langle g \rangle$ или нет, мы делим f на g:

$$f = qg + r,$$

где $q, r \in k[x]$ и $r = 0$ или $\deg(r) < \deg(g)$. Мы доказали, что $f \in I$ в том и только том случае, когда $r = 0$. Таким образом, в случае $n = 1$ у нас есть алгоритмический метод проверки принадлежности полинома идеалу.

Пример 2. Рассмотрим случай n переменных. Пусть дана система полиномиальных уравнений первой степени (т. е. линейная система)

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n + b_1 &= 0, \\ &\vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n + b_m &= 0. \end{aligned} \tag{1}$$

Например, рассмотрим систему

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0, \\ x_1 + x_2 - 1 &= 0, \\ x_1 + x_3 - 3 &= 0. \end{aligned} \tag{2}$$

После приведения матрицы системы к ступенчатому виду мы получаем

$$\begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Мы видим, что x_3 — свободная переменная, и, полагая $x_3 = t$ (произвольный элемент из k), можем записать решение в виде

$$\begin{aligned} x_1 &= -t + 3, \\ x_2 &= t - 2, \\ x_3 &= t. \end{aligned}$$

Эти параметрические уравнения задают прямую L в k^3, а исходная система определяет L как аффинное многообразие.

В общем случае мы, используя элементарные преобразования строк, приводим матрицу системы (1)

$$\begin{pmatrix} a_{11} & \dots & a_{1n} & -b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & -b_m \end{pmatrix}$$

к *главному ступенчатому виду* (где главный, т. е. первый ненулевой, элемент в каждой строке равен 1, а все другие элементы столбца, содержащего эту 1, равны нулю). Теперь мы находим все решения системы (1), задавая значения *свободных переменных* в ступенчатой матрице. Система может иметь единственное решение, а может и не иметь решений вообще. Последнее возможно в том случае, когда ступенчатая матрица системы содержит строку $(0 \dots 0\, 1)$, которой отвечает уравнение $0 = 1$, не имеющее решений.

Пример 3. Пусть снова n произвольно, и рассмотрим подмножество $V \subset k^n$ со следующей параметризацией:

$$\begin{aligned} x_1 &= a_{11}t_1 + \dots + a_{1m}t_m + b_1, \\ &\vdots \\ x_n &= a_{n1}t_1 + \dots + a_{nm}t_m + b_n. \end{aligned} \tag{3}$$

Мы видим, что V является аффинным линейным подпространством в k^n, потому что оно есть образ отображения $F : k^m \to k^n$,

задаваемого формулой

$$F(t_1, \dots, t_m) = (a_{11}t_1 + \dots + a_{1m}t_m + b_1, \dots, a_{n1}t_1 + \dots + a_{nm}t_m + b_n).$$

F есть композиция линейного отображения и сдвига. Рассмотрим задачу неявного представления в этом случае. Другими словами, мы должны найти линейную систему типа (1), решениями которой будут точки из V.

Рассмотрим, например, аффинное линейное подпространство $V \subset k^4$, заданное следующей параметрической системой:

$$\begin{aligned} x_1 &= t_1 + t_2 + 1, \\ x_2 &= t_1 - t_2 + 3, \\ x_3 &= 2t_1 - 2, \\ x_4 &= t_1 + 2t_2 - 3. \end{aligned}$$

Перепишем уравнения, перенося x_i в правую часть. Теперь матрица системы имеет следующий вид:

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{pmatrix}$$

(порядок переменных в новой системе таков: $t_1, t_2, x_1, x_2, x_3, x_4$). Приводя матрицу к главному ступенчатому виду, получим

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{pmatrix}$$

Последние две строчки ступенчатой матрицы соответствуют уравнениям, не содержащим t_j:

$$\begin{aligned} x_1 - (1/4)x_3 - (1/2)x_4 - 3 &= 0, \\ x_2 - (3/4)x_3 + (1/2)x_4 - 3 &= 0. \end{aligned}$$

(Отметим, что матрица этой системы также главная ступенчатая.) Два этих уравнения и определяют V в k^4.

Этот метод применим для нахождения неявного представления любого аффинного линейного подпространства V, заданного параметрически системой типа (3): приводим матрицу системы к главному ступенчатому виду. Тогда строки, содержащие только $x_1, \dots, x_n$, и дают уравнения, определяющие V. Таким образом, в этом случае у нас есть алгоритмический метод решения задачи нахождения неявного представления.

Цель этой главы — обобщить методы, рассмотренные в примерах, и перенести их на произвольные полиномиальные системы любой степени и с любым количеством переменных. Мы увидим, что некоторая «комбинация» приведения к ступенчатому виду и деления полиномов — упомянутый в начале главы метод базисов Грёбнера — и позволяет решить эти задачи.

Упражнения к § 1

1. Используя метод примера 1, определите, принадлежит ли данный полином данному идеалу $I \subset \mathbb{R}[x]$.
   (a) $f(x) = x^2 - 3x + 2$, $I = \langle x - 2 \rangle$.
   (b) $f(x) = x^5 - 4x + 1$, $I = \langle x^3 - x^2 + x \rangle$.
   (c) $f(x) = x^2 - 4x + 4$, $I = \langle x^4 - 6x^2 + 12x - 8, 2x^3 - 10x^2 + 16x - 8 \rangle$.
   (d) $f(x) = x^3 - 1$, $I = \langle x^9 - 1, x^5 + x^3 - x^2 - 1 \rangle$.
2. Параметризуйте аффинное многообразие, заданное следующей системой:
   (a) В $\mathbb{R}^3$ или в $\mathbb{C}^3$:
   $$\begin{aligned} 2x + 3y - z &= 9, \\ x - y &= 1, \\ 3x + 7y - 2z &= 17. \end{aligned}$$
   (b) В $\mathbb{R}^4$ или в $\mathbb{C}^4$:
   $$\begin{aligned} x_1 + x_2 - x_3 - x_4 &= 0, \\ x_1 - x_2 + x_3 &= 0. \end{aligned}$$
   (c) В $\mathbb{R}^3$ или в $\mathbb{C}^3$:
   $$\begin{aligned} y - x^3 &= 0, \\ z - x^5 &= 0. \end{aligned}$$
3. Найдите неявное представление аффинного многообразия, заданного параметрически.
   (a) В $\mathbb{R}^3$ или в $\mathbb{C}^3$:
   $$\begin{aligned} x_1 &= t - 5, \\ x_2 &= 2t + 1, \\ x_3 &= -t + 6. \end{aligned}$$
   (b) В $\mathbb{R}^4$ или в $\mathbb{C}^4$:
   $$\begin{aligned} x_1 &= 2t - 5u, \\ x_2 &= t + 2u, \\ x_3 &= -t + u, \\ x_4 &= t + 3u. \end{aligned}$$
   (c) В $\mathbb{R}^3$ или в $\mathbb{C}^3$:
   $$\begin{aligned} x &= t, \\ y &= t^4, \\ z &= t^7. \end{aligned}$$

4. Пусть $x_1, x_2, x_3, \ldots$ — бесконечная последовательность независимых переменных. *Полиномом* от переменных x_i с коэффициентами в поле k называется конечная линейная комбинация (конечных) мономов $x_{i_1}^{e_1} \ldots x_{i_n}^{e_n}$. Обозначим через R множество всех полиномов от x_i. Мы можем складывать и умножать элементы из R обычным способом, т. е. R является кольцом полиномов $k[x_1, x_2, \ldots]$ от бесконечного числа переменных.
   (a) Пусть $I = \langle x_1, x_2, x_3, \ldots \rangle$ обозначает множество полиномов вида $x_{t_1} f_1 + \ldots + x_{t_m} f_m$, где $f_i \in R$. Докажите, что I является идеалом в R.
   (b) Рассуждая от противного, докажите, что I не является конечно порожденным идеалом. Указание: нельзя ограничиться только рассмотрением подмножеств множества $\{x_i : i \geq 1\}$.
5. В этом упражнении мы докажем, что каждая полиномиальная параметрическая кривая в k^2 содержится в некотором аффинном многообразии.
   (a) Докажите, что количество различных мономов $x^e y^f$ степени $\leq m$ (т. е. $e + f \leq m$) в $k[x, y]$ равно $(m + 1)(m + 2)/2$. Указание: это биномиальный коэффициент $\binom{m+2}{2}$.
   (b) Пусть $f(t)$ и $g(t)$ — полиномы степени $\leq n$ от переменной t; тогда если m достаточно велико, то «мономы»
   $$[f(t)]^e [g(t)]^f,$$
   где $e + f \leq m$, образуют линейно *зависимое* множество в $k[t]$.
   (c) Выведите из п. (b), что если $C : x = f(t), y = g(t)$ — произвольная полиномиальная параметрическая кривая в k^2, то C содержится в некотором аффинном многообразии $\mathbf{V}(F)$, где $F \in k[x, y]$.
   (d) Обобщите пп. (a), (b) и (c) и докажите, что произвольная полиномиальная параметрическая поверхность
   $$x = f(t, u), \quad y = g(t, u), \quad z = h(t, u)$$
   содержится в некоторой алгебраической поверхности $\mathbf{V}(F)$, $F \in k[x, y, z]$.

§ 2. Упорядочение мономов в $k[x_1, \ldots, x_n]$

Тщательное рассмотрение алгоритма деления в $k[x]$ и алгоритма приведения системы (или матрицы) к ступенчатому виду методом исключения Гаусса показывает, что понятие *упорядочения членов* полинома является ключевым в обоих алгоритмах (хотя это, как

правило, не подчеркивается). При делении, например, полинома $f(x) = x^5 - 3x^2 + 1$ на полином $g(x) = x^2 - 4x + 7$ мы должны

- записать члены полиномов в порядке убывания степеней;
- на первом шаге поделим старший член x^5 (т. е. член наибольшей степени) полинома f на x^2 — старший член полинома g: $x^5 = x^3 \cdot x^2$. Затем мы вычитаем $x^3 \cdot g(x)$ из $f(x)$, уничтожая тем самым старший член полинома f, и получаем $4x^4 - 7x^3 - 3x^2 + 1$.
- Повторяем эту процедуру с $f(x) - x^3 \cdot g(x)$ вместо $f(x)$ и т. д. до тех пор, пока не получим полином степени, меньшей двух.

Алгоритм деления полиномов от одной переменной имеет дело, таким образом, со следующим упорядочением мономов:

$$\ldots > x^{m+1} > x^m > \ldots > x^2 > x > 1. \tag{1}$$

Результативность алгоритма связана именно с тем, что мы работаем последовательно со старшими членами полиномов f и g, а не «случайным образом» убираем члены из f, используя произвольные члены из g.

Аналогично, при приведении матрицы к ступенчатому виду мы систематически обращаем в нуль главные элементы, т. е. первые слева ненулевые элементы в строках. На языке линейных систем это означает следующий порядок переменных:

$$x_1 > x_2 > \ldots > x_n. \tag{2}$$

Каждое уравнение системы записывается в порядке убывания членов. Более того, в ступенчатом виде уравнения системы записаны в порядке убывания старших (главных) членов. (Следует отметить, что определение ступенчатого вида системы может быть сформулировано в терминах этого упорядочения — см. упр. 8.)

Рассмотрение этих примеров заставляет предположить, что обобщение алгоритмов деления и приведения к ступенчатому виду на случай произвольных полиномов от нескольких переменных должно базироваться на упорядочении членов полиномов из $k[x_1, \ldots, x_n]$. В этом параграфе мы обсудим, какими свойствами должно обладать такое упорядочение, и определим несколько упорядочений, обладающих этими свойствами. Каждое из этих упорядочений имеет свою область применения.

Отметим сначала, что существует взаимно однозначное соответствие между мономами $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ и n-наборами (n-векторами) показателей степеней $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Упорядочение, которое мы определим на $\mathbb{Z}^n_{\geq 0}$, определит и упорядочение на множестве мономов: если $\alpha > \beta$ в $\mathbb{Z}^n_{\geq 0}$, то мы будем говорить, что $x^\alpha > x^\beta$.

Упорядочение на $\mathbb{Z}^n_{\geq 0}$ можно задать многими способами. Однако большинство из них нам не подходит, так как желательно, чтобы наше упорядочение было «совместимо» с алгебраической структурой полиномиального кольца.

Так как полином есть сумма мономов, то мы должны уметь расположить его члены в порядке убывания (или возрастания). Для этого мы должны уметь сравнивать любую пару мономов и определять, какой из них больше, т. е. наше упорядочение должно быть *линейным*. Это означает, что для любой пары мономов x^α и x^β должно выполняться ровно одно из следующих соотношений:

$$x^\alpha > x^\beta, \quad x^\alpha = x^\beta, \quad x^\alpha < x^\beta.$$

Далее мы должны учесть связь упорядочения с операциями сложения и умножения полиномов. Когда мы складываем полиномы, то после приведения подобных мы просто можем переписать члены суммы в требуемом порядке. Ситуация с произведением более сложная. Дистрибутивность умножения по отношения к сложению позволяет свести задачу к случаю умножения монома на полином. Если такое умножение нарушает порядок членов, то трудности могут возникнуть в любом процессе, аналогичном алгоритму деления в $k[x]$, где мы должны находить «старший» член полинома. Причина в том, что произведение старшего члена полинома на моном может не быть старшим членом произведения.

Поэтому мы потребуем, чтобы упорядочение мономов обладало следующим дополнительным свойством. Если $x^\alpha > x^\beta$, а x^γ — произвольный моном, то $x^\alpha x^\gamma > x^\beta x^\gamma$. В терминах векторов — показателей степеней это означает, что если $\alpha > \beta$ в $\mathbb{Z}^n_{\geq 0}$, то для любого $\gamma \in \mathbb{Z}^n_{\geq 0}$, $\alpha + \gamma > \beta + \gamma$.

Теперь мы можем дать следующее определение.

Определение 1. *Мономиальным упорядочением* на $k[x_1, \ldots, x_n]$ называется любое бинарное отношение $>$ на $\mathbb{Z}^n_{\geq 0}$, обладающее следующими свойствами:

(i) $>$ является линейным упорядочением на $\mathbb{Z}^n_{\geq 0}$.

(ii) если $\alpha > \beta$ и $\gamma \in \mathbb{Z}^n_{\geq 0}$, то $\alpha + \gamma > \beta + \gamma$;

(iii) $>$ вполне упорядочивает $\mathbb{Z}^n_{\geq 0}$, т. е. любое непустое подмножество в $\mathbb{Z}^n_{\geq 0}$ имеет минимальный (наименьший) элемент (по отношению к упорядочению $>$).

Следующая лемма помогает понять, что означает условие вполне упорядоченности (iii).

Лемма 2. *Упорядочение $>$ на $\mathbb{Z}^n_{\geq 0}$ вполне упорядочивает это множество тогда и только тогда, когда каждая строго убывающая*

последовательность элементов из $\mathbb{Z}_{\geq 0}^n$

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

обрывается.

Доказательство. Мы докажем эквивалентное утверждение: $>$ не является вполне упорядочением тогда и только тогда, когда существует бесконечная строго убывающая последовательность элементов из $\mathbb{Z}_{\geq 0}^n$.

Если $>$ не есть вполне упорядочение, то существует непустое подмножество $S \subset \mathbb{Z}_{\geq 0}^n$, которое не имеет минимального элемента. Возьмем в качестве $\alpha(1)$ произвольный элемент из S. Так как он не минимален, то в S найдется элемент $\alpha(2) < \alpha(1)$. Так как $\alpha(2)$ не минимален, то в S найдется элемент $\alpha(3) < \alpha(2)$. Продолжая этот процесс, мы получим бесконечную строго убывающую последовательность

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots.$$

Обратно, если существует такая бесконечная строго убывающая последовательность, то множество $\{\alpha(1), \alpha(2), \alpha(3), \dots\}$ является непустым подмножеством в $\mathbb{Z}_{\geq 0}^n$, которое не имеет минимального элемента, т. е. $>$ не является вполне упорядочением. □

Полезность и важность этой леммы станут очевидными в следующих параграфах. Доказательства корректности алгоритмов (т. е. остановки работы и получения требуемого результата) будут базироваться на том, что старший член выражения (с которым работает алгоритм) строго убывает относительно некоторого фиксированного упорядочения на каждом шаге работы.

В § 4 будет доказано, что условие вполне упорядоченности (п. (iii) определения 1) вытекает из условий (i) и (ii) и требования $\alpha \geq 0$ для всех $\alpha \in \mathbb{Z}_{\geq 0}^n$.

В качестве примера мономиального упорядочения рассмотрим обычное упорядочение натуральных чисел $\mathbb{Z}_{\geq 0}$:

$$\dots > m+1 > m > \dots > 3 > 2 > 1 > 0.$$

Все три условия определения 1 здесь выполнены. Следовательно, упорядочение мономов из $k[x]$ по степени (1) является мономиальным упорядочением.

Нашим первым примером упорядочения n-векторов будет лексикографическое упорядочение (или сокращенно lex-*упорядочение*).

Определение 3 (лексикографическое упорядочение). Пусть $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. Мы говорим, что $\alpha >_{\text{lex}} \beta$, если

самая левая ненулевая координата вектора $\alpha - \beta \in \mathbb{Z}^n$ положительна. Мы будем писать $x^\alpha >_{\text{lex}} x^\beta$, если $\alpha >_{\text{lex}} \beta$.

Вот несколько примеров:

(a) $(1,2,0) >_{\text{lex}} (0,3,4)$, так как $\alpha - \beta = (1,-1,-4)$.
(b) $(3,2,4) >_{\text{lex}} (3,2,1)$, так как $\alpha - \beta = (0,0,3)$.
(c) Обычный порядок (2) переменных $x_1, \dots, x_n$ является lex-упорядочением. Так как

$$(1,0,\dots,0) >_{\text{lex}} (0,1,0,\dots,0) >_{\text{lex}} \dots >_{\text{lex}} (0,\dots,0,1),$$

то $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \dots >_{\text{lex}} x_n$.

Работая с полиномами от двух или трех переменных, мы обозначаем переменные через x, y, z, а не x_1, x_2, x_3. В дальнейшем мы будем также, как правило, предполагать, что алфавитный порядок $x > y > z$ переменных и определяет лексикографическое упорядочение мономов.

Лексикографическое упорядочение аналогично упорядочению слов в словарях (откуда и происходит термин). Мы можем рассматривать координаты n-вектора $\alpha \in \mathbb{Z}_{\geq 0}^n$ как аналоги букв в слове. Буквы упорядочены по алфавиту

$$\text{а} > \text{б} > \dots > \text{ю} > \text{я},$$

откуда

$$\text{стрела} >_{\text{lex}} \text{строка},$$

так как четвертая буква слова «строка» в алфавите идет после четвертой буквы слова «стрела», в то время как первые три буквы в обоих словах одинаковы. Так как векторы $\alpha \in \mathbb{Z}_{\geq 0}^n$ имеют фиксированную длину n, то аналогия распространяется только на слова с одинаковым числом букв.

Нам осталось проверить, что лексикографическое упорядочение удовлетворяет трем условиям определения 1.

Предложение 4. *Лексикографическое упорядочение на* $\mathbb{Z}_{\geq 0}^n$ *является мономиальным упорядочением.*

Доказательство. (i) Тот факт, что $>_{\text{lex}}$ — линейное упорядочение, прямо следует из определения и из того, что обычное упорядочение на $\mathbb{Z}_{\geq 0}$ линейно.

(ii) Пусть $\alpha >_{\text{lex}} \beta$. Тогда самая левая ненулевая координата вектора $\alpha - \beta$ положительна. Пусть это, например, $\alpha_k - \beta_k$. Но $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ и $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Тогда $(\alpha+\gamma) - (\beta+\gamma) = \alpha - \beta$, и самой левой ненулевой координатой опять является $\alpha_k - \beta_k > 0$.

(iii) Предположим, что $>_{\text{lex}}$ не является вполне упорядочением. Тогда по лемме 2 должна существовать строго убывающая бесконечная последовательность

$$\alpha(1) >_{\text{lex}} \alpha(2) >_{\text{lex}} \alpha(3) >_{\text{lex}} \dots$$

элементов из $\mathbb{Z}^n_{\geq 0}$. Докажем, что это невозможно.

Рассмотрим первые координаты векторов $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. По определению лексикографического упорядочения они образуют невозрастающую последовательность неотрицательных целых чисел. Так как $\mathbb{Z}_{\geq 0}$ вполне упорядочено, то эта последовательность «стабилизируется», т. е. существует такое k, что первые координаты векторов $\alpha(i)$ одинаковы при $i \geq k$.

Начиная с $\alpha(k)$, будем рассматривать вторые (а затем третьи и т. д.) координаты. Последовательность вторых координат векторов $\alpha(k), \alpha(k+1), \dots$ не возрастает; значит, она «стабилизируется». Продолжая это рассуждение, мы можем найти такое l, что у векторов $\alpha(l), \alpha(l+1), \dots$ равны все координаты. Значит, это одинаковые векторы, что противоречит строгому убыванию последовательности. □

Необходимо отметить, что существует много лексикографических упорядочений: каждому упорядочению переменных отвечает свое. До сих пор мы рассматривали лексикографическое упорядочение, порожденное упорядочением $x_1 > x_2 > \dots > x_n$. Но, задав *произвольный* порядок переменных $x_1, \dots, x_n$, мы получим соответствующее ему лексикографическое упорядочение. Пусть, например, переменных две, скажем, x и y. Тогда мы можем определить два лексикографических упорядочения: одно порождается порядком $x > y$, а другое — порядком $y > x$. В общем случае n переменных имеется $n!$ лексикографических упорядочений. В дальнейшем термин «лексикографическое упорядочение» будет означать, что имеется в виду порядок $x_1 > x_2 > \dots > x_n$.

В случае лексикографического упорядочения переменная больше *любого* монома, который содержит только меньшие переменные, вне зависимости от его степени. Так, при упорядочении $x > y > z$ мы имеем $x >_{\text{lex}} y^5 z^3$. В ряде случаев нам будет необходимо учитывать также степени мономов и сравнивать сначала именно степени. Это можно сделать с помощью градуированного лексикографического упорядочения (сокращенно grlex-*упорядочения*).

Определение 5 (градуированное лексикографическое упорядочение). Пусть $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Мы говорим, что $\alpha >_{\text{grlex}} \beta$, если

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i \quad \text{или} \quad |\alpha| = |\beta| \quad \text{и} \quad \alpha >_{\text{lex}} \beta.$$

Таким образом, grlex сначала упорядочивает по степени, а если степени равны, то используется лексикографическое упорядочение. Вот несколько примеров:

(a) $(1,2,3) >_{\text{grlex}} (3,2,0)$, так как $|(1,2,3)| = 6 > |(3,2,0)| = 5$.
(b) $(1,2,4) >_{\text{grlex}} (1,1,5)$, так как $|(1,2,4)| = |(1,1,5)|$, но $(1,2,4) >_{\text{lex}} (1,1,5)$.
(c) Переменные упорядочиваются в соответствии с лексикографическим порядком, т. е. $x_1 >_{\text{grlex}} \dots >_{\text{grlex}} x_n$.

Доказательство того, что grlex-упорядочение удовлетворяет трем условиям определения 1, мы оставляем читателю в качестве упражнения. Как и в лексикографическом случае, имеется $n!$ grlex-упорядочений для n переменных.

Следующее (интуитивно несколько менее естественное) упорядочение, как было недавно доказано, является для некоторых операций наиболее эффективным при вычислениях.

Определение 6 (градуированное обратное лексикографическое упорядочение grevlex). Пусть $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Тогда мы говорим, что $\alpha >_{\text{grevlex}} \beta$, если

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$$

или $|\alpha| = |\beta|$ и самая правая ненулевая координата вектора $\alpha - \beta \in \mathbb{Z}^n$ отрицательна.

Как и grlex, grevlex сначала сравнивает степени мономов, но упорядочивает мономы по-другому в случае равенства их степеней. Например:

(a) $(4,7,1) >_{\text{grevlex}} (4,2,3)$, так как $|(4,7,1)| = 12 > |(4,2,3)| = 9$.
(b) $(1,5,2) >_{\text{grevlex}} (4,1,3)$, так как $|(1,5,2)| = |(4,1,3)|$ и $\alpha - \beta = (-3,4,-1)$.

В упражнениях будет доказано, что grevlex-упорядочение является мономиальным.

Отметим, что grlex и grevlex одинаково упорядочивают переменные:

$$(1,0,\dots,0) >_{\text{grevlex}} (0,1,0,\dots,0) >_{\text{grevlex}} \dots >_{\text{grevlex}} (0,\dots,0,1),$$

или

$$x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \dots >_{\text{grevlex}} x_n.$$

Значит, grevlex-упорядочение не есть grlex-упорядочение с обращением порядка переменных (как может показаться на первый взгляд).

Для того чтобы объяснить связь между grlex и grevlex, отметим сначала, что оба эти упорядочения одинаково оценивают степень монома. В случае равенства степеней grlex использует lex-упорядочение, т. е. обращает внимание на самую левую (большую) переменную и «предпочитает» *большую* степень. Напротив, grevlex в случае равенства степеней обращает внимание на самую правую (меньшую) переменную и «предпочитает» *меньшую* степень. В упражнениях мы увидим, что это эквивалентно «двойному обращению» lex-упорядочения. Например,

$$x^5yz >_{\text{grlex}} x^4yz^2,$$

так как оба монома имеют степень 7 и $x^5yz >_{\text{lex}} x^4yz^2$. В этом же случае

$$x^5yz >_{\text{grevlex}} x^4yz^2,$$

но по другой причине: x^5yz больше, так как меньшая переменная z имеет меньшую степень.

Как и в lex- и grlex-случаях, существует $n!$ различных grevlex-упорядочений, зависящих от порядка переменных.

Существуют и другие мономиальные упорядочения. Некоторые из них будут рассмотрены в упражнениях к § 4. Большинство систем компьютерной алгебры работают с lex-упорядочением, но также могут поддерживать и другие упорядочения, grlex и grevlex, например. Как только тип упорядочения задан, система позволяет пользователю выбрать любое из $n!$ упорядочений переменных. Как мы увидим в § 8 этой главы (а также в дальнейших главах), подобные возможности системы весьма полезны при решении разнообразных задач.

Мы закончим этот параграф обсуждением того, как мономиальные упорядочения могут помочь при работе с полиномами. Пусть $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \dots, x_n]$, и пусть выбрано мономиальное упорядочение $>$. Тогда мы можем однозначно упорядочить члены полинома f в соответствии с $>$. Пусть, например, $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$. Тогда:

(a) при lex-упорядочении мы записываем полином f в порядке убывания членов так:

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2;$$

(b) при grlex-упорядочении запись f такова:

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2;$$

(c) при grevlex-упорядочении запись f такова:

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

Далее мы будем пользоваться следующими понятиями.

Определение 7. Пусть $f = \sum_\alpha a_\alpha x^\alpha$ — ненулевой полином в $k[x_1, \dots, x_n]$, и пусть $>$ — мономиальное упорядочение.

(i) *Мультистепень* полинома f определяется так:

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$$

(максимум берется по отношению к $>$).

(ii) *Старший коэффициент* полинома f — это

$$\text{LC}(f) = a_{\text{multideg}(f)} \in k.$$

(iii) *Старший моном* полинома f — это

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

(с коэффициентом 1).

(iv) *Старший член* полинома f — это

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

Пусть, например, $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$, как и выше, и пусть $>$ обозначает lex-упорядочение. Тогда

$$\begin{aligned} \text{multideg}(f) &= (3, 0, 0), \\ \text{LC}(f) &= -5, \\ \text{LM}(f) &= x^3, \\ \text{LT}(f) &= -5x^3. \end{aligned}$$

В упражнениях будет доказано, что мультистепень имеет следующие полезные свойства.

Лемма 8. *Пусть* $f, g \in k[x_1, \dots, x_n]$ *— ненулевые полиномы. Тогда*

(i) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.

(ii) *Если* $f + g \neq 0$, *то* $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. *Если, кроме того,* $\text{multideg}(f) \neq \text{multideg}(g)$, *то указанное неравенство становится равенством.*

Начиная с этого места, мы будем считать, что выбрано некоторое мономиальное упорядочение и старшие члены, мультистепени и пр. определяются относительно этого упорядочения.

Упражнения к § 2

1. Запишите следующие полиномы с использованием lex-, grlex- и grevlex-упорядочений. Найдите $\text{LM}(f), \text{LT}(f)$ и $\text{multideg}(f)$ в каждом случае.
   (a) $f(x, y, z) = 2x + 3y + z + x^2 - z^2 + x^3$.
   (b) $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$.

2. Каждый из следующих полиномов записан в соответствии с одним из упорядочений: lex, grlex или grevlex. Определите, какое упорядочение использовалось в каждом случае.
   (a) $f(x,y,z) = 7x^2y^4z - 2xy^6 + x^2y^2$.
   (b) $f(x,y,z) = xy^3z + xy^2z^2 + x^2z^3$.
   (c) $f(x,y,z) = x^4y^5z + 2x^3y^2z - 4xy^2z^4$.
3. Выполните упр. 1 с использованием порядка переменных $z > y > x$.
4. Докажите, что grlex является мономиальным упорядочением, т. е. удовлетворяет условиям определения 1.
5. Докажите, что grevlex является мономиальным упорядочением, т. е. удовлетворяет условиям определения 1.
6. Определим *противоположное* (inverse) *лексикографическое* упорядочение (сокращенно invlex-*упорядочение*) следующим образом: если $\alpha, \beta \in Z^n_{\geq 0}$, то $\alpha >_{\text{invlex}} \beta$ в том и только том случае, когда самая правая ненулевая координата вектора $\alpha - \beta$ положительна. Докажите, что invlex — это lex-упорядочение с другим порядком переменных. (Каким?)
7. Пусть $>$ — некоторое мономиальное упорядочение.
   (a) Докажите, что $\alpha \geq 0$ для всех $\alpha \in \mathbb{Z}^n_{\geq 0}$.
   (b) Докажите, что если x^α делит x^β, то $\alpha \leq \beta$. Верно ли обратное?
   (c) Пусть $\alpha \in \mathbb{Z}^n_{\geq 0}$. Тогда α является минимальным элементом множества $\alpha + \mathbb{Z}^n_{\geq 0}$.
8. Используя упорядочение (2), дайте точное определение линейной системы ступенчатого вида.
9. В этом упражнении мы подробнее изучим grevlex-упорядочение. Пусть $>_{\text{invlex}}$ — упорядочение, определенное в упр. 6, и пусть $>_{\text{rinvlex}}$ — упорядочение, обратное к нему, т. е. для $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$

$$\alpha >_{\text{rinvlex}} \beta \Longleftrightarrow \beta >_{\text{invlex}} \alpha.$$

   Отметим, что rinvlex является «двойным обращением» упорядочения lex в следующем смысле: мы сначала обращаем порядок переменных, а потом само упорядочение.
   (a) Докажите, что $\alpha >_{\text{grevlex}} \beta$ в том и только том случае, когда $|\alpha| > |\beta|$ или $|\alpha| = |\beta|$ и $\alpha >_{\text{rinvlex}} \beta$.
   (b) Является ли rinvlex мономиальным упорядочением? Если да, то докажите, если нет, то укажите, какое свойство определения 1 нарушается.
10. При обычном упорядочении $\mathbb{Z}_{\geq 0}$ между двумя целыми числами находится только конечное число других целых чисел. Верно ли это для $\mathbb{Z}^n_{\geq 0}$ в случае произвольного мономиального упорядочения? Верно ли это в случае grlex-упорядочения?
11. Пусть $>$ — некоторое мономиальное упорядочение в $k[x_1, \ldots, x_n]$.
   (a) Пусть $f \in k[x_1, \ldots, x_n]$ и m — моном. Докажите, что $\text{LT}(m \cdot f) = m \cdot \text{LT}(f)$.
   (b) Пусть $f, g \in k[x_1, \ldots, x_n]$. Верно ли, что $\text{LT}(f \cdot g) = \text{LT}(f) \cdot \text{LT}(g)$?
   (c) Пусть f_i, g_i — полиномы из $k[x_1, \ldots, x_n]$, $1 \leq i \leq s$. Верно ли, что $\text{LM}(\sum_{i=1}^s f_i g_i) = \text{LM}(f_i) \cdot \text{LM}(g_i)$ для некоторого i?
12. В лемме 8 сформулированы два свойства мультистепени.
   (a) Докажите лемму 8. Указание: примените рассуждения, использованные при решении упр. 11.
   (b) Пусть $\text{multideg}(f) = \text{multideg}(g)$ и $f + g \neq 0$. Покажите на примерах, что $\text{multideg}(f+g)$ может быть как равна, так и отлична от $\max(\text{multideg}(f), \text{multideg}(g))$.

§ 3. Алгоритм деления в $k[x_1, \ldots, x_n]$

В § 1 было объяснено, как алгоритм деления для полиномов от одной переменной может быть применен для решения задачи о принадлежности идеалу. Для решения этой же задачи в случае нескольких переменных необходимо обобщить алгоритм деления в $k[x]$ на общий случай полиномиального кольца $k[x_1, \ldots, x_n]$. Наша цель — научиться делить полином $f \in k[x_1, \ldots, x_n]$ на полиномы $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Как мы увидим, это означает научиться представлять f в виде

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

где «частные» $a_1, \ldots, a_s$ и остаток r принадлежат $k[x_1, \ldots, x_n]$. Самое трудное в этом вопросе — это корректно определить остаток. Именно здесь будут использованы мономиальные упорядочения из § 2. После этого мы применим этот алгоритм для решения задачи о принадлежности идеалу.

Основная идея алгоритма та же, что и в случае одной переменной: мы должны уничтожать старший член полинома f (определенный заданным мономиальным упорядочением), умножая некоторый f_i на подходящий моном и вычитая. Этот моном будет членом соответствующего a_i. Прежде чем давать общее описание алгоритма, проанализируем его работу на нескольких примерах.

Пример 1. Поделим $f = xy^2 + 1$ на $f_1 = xy + 1$ и $f_2 = y + 1$ при lex-упорядочении с $x > y$. Будет использоваться та же схема, что и в случае одной переменной, но теперь у нас несколько делителей и частных. Будем записывать делители f_1, f_2 и частные a_1, a_2 *в столбец* слева, т. е. мы имеем следующую схему:

$$\begin{array}{rl} a_1: & \\ a_2: & \\ xy+1 & \sqrt{xy^2+1} \\ y+1 & \end{array}$$

Старшие члены $\mathrm{LT}(f_1) = xy$ и $\mathrm{LT}(f_2) = y$ оба делят старший член $\mathrm{LT}(f) = xy^2$. Так как f_1 является первым в списке делителей, то на первом шаге мы будем работать с ним, т. е. мы делим xy^2 на xy, записывая y как член полинома a_1 и вычитая $y \cdot f_1$ из f:

$$\begin{array}{rll} a_1: & y & \\ a_2: & & \\ xy+1 & \sqrt{xy^2+1} & \\ y+1 & \underline{xy^2+y} & \\ & \quad -y+1 & \end{array}$$

Теперь на следующем шаге мы работаем с f_2, так как $\mathrm{LT}(f_1) = xy$ не делит $\mathrm{LT}(-y+1) = -y$. Имеем

$$\begin{array}{rll} a_1: & y & \\ a_2: & -1 & \\ xy+1 & \sqrt{xy^2+1} & \\ y+1 & \underline{xy^2+y} & \\ & \quad -y+1 & \\ & \quad \underline{-y-1} & \\ & \qquad 2 & \end{array}$$

Так как $\mathrm{LT}(f_1)$ и $\mathrm{LT}(f_2)$ не делят 2, то $r = 2$ и процесс деления окончен, т. е. мы можем записать $f = xy^2 + 1$ в виде

$$x^2y + 1 = y \cdot (xy+1) + (-1) \cdot (y+1) + 2.$$

Пример 2. В этом примере мы столкнемся с неожиданной трудностью, которая не возникает в случае одной переменной. Мы будем делить $f = x^2y + xy^2 + y^2$ на $f_1 = xy - 1$ и $f_2 = y^2 - 1$. Как и в предыдущем примере, мы используем lex-упорядочение с $x > y$. Первые два шага алгоритма деления выполняются, как выше. Вот их результат (напомним, что если оба старших члена являются делителями, то мы работаем с первым):

$$\begin{array}{rll} a_1: & x+y & \\ a_2: & & \\ xy-1 & \sqrt{x^2y+xy^2+y^2} & \\ y^2-1 & \underline{x^2y-x} & \\ & \quad xy^2+x+y^2 & \\ & \quad \underline{xy^2-y} & \\ & \qquad x+y^2+y & \end{array}$$

Теперь обратим внимание на то, что ни $\mathrm{LT}(f_1) = xy$, ни $\mathrm{LT}(f_2) = y^2$ не делят $\mathrm{LT}(x + y^2 + y) = x$. Но $x + y^2 + y$ — *не* остаток, так как $\mathrm{LT}(f_2)$ делит y^2, т. е. если мы отправим x в остаток, то деление можно продолжить. (Эта трудность не может встретиться в случае одной переменной: если старший член делителя не делит старшего члена делимого, то остатком является последняя разность и процесс деления прекращается.)

Чтобы реализовать эту идею, мы создадим новый столбец в записи процесса деления, справа от радикала, куда будем записывать члены, принадлежащие остатку. Полином, расположенный ниже радикала, который мы делим, будем называть *промежуточным делимым*. Процесс деления продолжается до тех пор, пока промежуточное делимое не обратится в нуль. На следующем шаге нашего примера мы перемещаем x в колонку остатка (это показано стрелкой):

$$\begin{array}{rll} a_1: & x+y & \\ a_2: & & r \\ xy-1 & \sqrt{x^2y+xy^2+y^2} & \\ y^2-1 & \underline{x^2y-x} & \\ & \quad xy^2+x+y^2 & \\ & \quad \underline{xy^2-y} & \\ & \qquad x+y^2+y & \\ & \qquad \underline{y^2+y} \quad \longrightarrow & x \end{array}$$

Теперь мы продолжаем деление. Если мы можем поделить старший член промежуточного делимого на $\mathrm{LT}(f_1)$ или на $\mathrm{LT}(f_2)$, то делаем обычный шаг деления, если нет, то мы перемещаем старший член в колонку остатка и т. д. Вот полная запись решения этого примера:

$$\begin{array}{rll} a_1: & x+y & \\ a_2: & 1 & r \\ xy-1 & \sqrt{x^2y+xy^2+y^2} & \\ y^2-1 & \underline{x^2y-x} & \\ & \quad xy^2+x+y^2 & \\ & \quad \underline{xy^2-y} & \\ & \qquad x+y^2+y & \\ & \qquad \underline{y^2+y} \quad \longrightarrow & x \\ & \qquad y^2-1 & \\ & \qquad \underline{y+1} & \\ & \qquad\quad 1 \quad \longrightarrow & x+y \\ & \qquad\quad 0 \quad \longrightarrow & x+y+1 \end{array}$$

Таким образом, остаток равен $x + y + 1$, и мы имеем

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1. \quad (1)$$

Следует отметить, что остаток есть сумма мономов, ни один из которых не делится ни на $\mathrm{LT}(f_1)$, ни на $\mathrm{LT}(f_2)$.

Этот пример дает довольно полное представление о работе алгоритма деления. Он также показывает, каким свойством должен обладать остаток: ни один член остатка нельзя поделить на старший член хотя бы одного делителя. Теперь мы можем дать полное описание алгоритма деления.

Теорема 3 (алгоритм деления в $k[x_1, \ldots, x_n]$). *Зафиксируем некоторое мономиальное упорядочение $>$ на $\mathbb{Z}^n_{\geq 0}$, и пусть $F = (f_1, \ldots, f_s)$ — упорядоченный s-набор полиномов из $k[x_1, \ldots, x_n]$. Тогда любой полином $f \in k[x_1, \ldots, x_n]$ может быть записан в виде*

$$f = a_1f_1 + \ldots + a_sf_s + r,$$

где $a_i, r \in k[x_1, \ldots, x_s]$ и или $r = 0$, или r есть линейная комбинация мономов (с коэффициентами из k), ни один из которых не делится ни на один из старших членов $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Мы называем r остатком *от деления полинома f на F. Более того, если $a_if_i \neq 0$, то*

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_if_i).$$

Доказательство. Доказательство существования полиномов $a_1, \ldots, a_s$ и r будет состоять в предъявлении алгоритма, вычисляющего $a_1, \ldots, a_s, r$, и в доказательстве корректности его работы. Мы рекомендуем читателю еще раз изучить работу алгоритма деления в $k[x]$ (предложение 2 § 5 гл. 1), прежде чем рассматривать его обобщение. Вот формальное описание алгоритма:

Вход: $f_1, \ldots, f_s, f$
Выход: $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
  $i := 1$
  естьделение := false
  WHILE $i \leq s$ AND естьделение = false DO
    IF $\mathrm{LT}(f_i)$ делит $\mathrm{LT}(p)$ THEN
      $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
      естьделение := true
    ELSE
      $i := i + 1$
  IF естьделение = false THEN
    $r := r + \mathrm{LT}(p)$
    $p := p - \mathrm{LT}(p)$

В этом алгоритме переменная p на каждом шаге выполняет роль промежуточного делимого, переменная r выполняет ту же роль, что и колонка справа в предыдущем примере, а переменные $a_1, \ldots, a_s$ выполняют роль частных из того же примера. Наконец, логическая переменная «естьделение» говорит нам, делится ли старший член промежуточного переменного на какой-либо из $\mathrm{LT}(f_i)$. Вы должны проверить, что каждый раз, когда мы находимся в главном цикле WHILE ... DO, может произойти ровно одно из двух событий:

- (Шаг деления) Если некоторый член $\mathrm{LT}(f_i)$ делит $\mathrm{LT}(p)$, то алгоритм продолжает работу, как в случае одной переменной.
- (Шаг вычисления остатка) Если никакой из $\mathrm{LT}(f_i)$ не делит $\mathrm{LT}(p)$, то алгоритм прибавляет $\mathrm{LT}(p)$ к остатку.

Эти шаги в точности соответствуют нашим действиям в примере 2.

Чтобы проверить корректность алгоритма, мы сначала докажем, что равенство

$$f = a_1f_1 + \ldots + a_sf_s + p + r \quad (2)$$

выполняется на каждом шаге. Очевидно, что (2) выполнено для начальных значений $a_1, \ldots, a_s, p$ и r. Пусть на некотором шаге имеет место (2). Если следующим является шаг деления, то некоторый $\mathrm{LT}(f_i)$ делит $\mathrm{LT}(p)$ и равенство

$$a_if_i + p = (a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i))f_i + (p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i)$$

показывает, что сумма $a_if_i + p$ не изменилась. Так как все остальные переменные остались теми же, то (2) выполняется и на этом шаге тоже. Если же следующим является шаг вычисления остатка, то меняются и p, и r, но их сумма остается неизменной, так как

$$p + r = (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p)).$$

И опять (2) выполняется на следующем шаге.

Далее, обратим внимание, что алгоритм прекращает работу, когда $p = 0$. В этом случае (2) выглядит так:

$$f = a_1f_1 + \ldots + a_sf_s + r.$$

Так как к r добавлялись только такие члены, которые не делятся ни на один из $\mathrm{LT}(f_i)$, то это означает, что $a_1, \ldots, a_s$ и r удовлетворяют условиям теоремы 3 в случае остановки работы алгоритма.

Наконец, нам осталось доказать, что алгоритм в какой-то момент останавливается. Для этого нужно заметить, что каждый раз, когда мы заново вычисляем переменную p, или ее мультистепень уменьшается (относительно заданного упорядочения), или p обращается в нуль. Чтобы доказать это, предположим сначала, что p изменилась в ходе шага деления:

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i.$$

По лемме 8 из § 2 мы имеем

$$\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \mathrm{LT}(f_i) = \mathrm{LT}(p),$$

так что p и $(\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$ имеют одинаковые старшие члены. Следовательно, их разность p' имеет строго меньшую мультистепень (если $p' \neq 0$). Пусть теперь p меняется в ходе шага вычисления остатка:

$$p' = p - \mathrm{LT}(p).$$

Очевидно, что здесь $\mathrm{multideg}(p') < \mathrm{multideg}(p)$, если $p' \neq 0$, т. е. в обоих случаях мультистепень уменьшается. Если алгоритм не останавливается, то мы получаем бесконечную строго убывающую последовательность мультистепеней. Но так как $>$ является вполне упорядочением, то это противоречит лемме 2 § 2. Таким образом, в какой-то момент p обратится в нуль, и алгоритм остановится после конечного числа шагов.

Осталось установить связь между $\mathrm{multideg}(f)$ и $\mathrm{multideg}(a_i f_i)$. Каждый член полинома a_i равен $\mathrm{LT}(p)/\mathrm{LT}(f_i)$ для некоторого значения переменной p. Начальное значение p есть f, и мы только что доказали, что мультистепень p строго убывает; значит, $\mathrm{LT}(p) \leq \mathrm{LT}(f)$. Таким образом (см. условие (ii) в определении 1 § 2), $\mathrm{multideg}(a_i f_i) \leq \mathrm{multideg}(f)$, если $a_i f_i \neq 0$ (см. упр. 4). Доказательство теоремы закончено. □

Алгебраическая техника, использованная в алгоритме, очень проста и не выходит за рамки первого года обучения. Тем более удивительно, что этот алгоритм был разработан и применен только 30 лет назад.

В заключение параграфа мы обсудим, имеет ли в общем случае алгоритм деления те хорошие свойства, которыми он обладает в случае одной переменной. К сожалению, ответ отрицательный — примеры ниже показывают, что алгоритм весьма несовершенен. На самом деле он работает в полную силу только при использовании базисов Грёбнера (они будут рассмотрены в §§ 5 и 6).

Первым важным свойством алгоритма деления в $k[x]$ является то, что остаток определен однозначно. Покажем на примере, что в случае нескольких переменных это свойство не выполняется.

Пример 4. Поделим $f = x^2y + xy^2 + y^2$ на $f_1 = y^2 - 1$ и на $f_2 = xy - 1$. Мы используем lex-упорядочение с $x > y$. Этот пример отличается от примера 2 только переменой порядка делителей. Если читатель проведет деление сам, то он получит следующую схему:

$$\begin{array}{rl} a_1: & x+1 \\ a_2: & x \\ y^2-1 & \left|\begin{array}{l} x^2+xy^2+y^2 \\ x^2y-x \end{array}\right. \\ xy-1 & \left|\begin{array}{l} xy^2+x+y^2 \\ xy^2-x \end{array}\right. \\ & \left|\begin{array}{l} 2x+y^2 \\ y^2 \end{array}\right. \\ & \left|\begin{array}{l} y^2-1 \\ 1 \end{array}\right. \\ & \left|\begin{array}{l} 0 \end{array}\right. \end{array} \qquad \begin{array}{l} r \\ \hline \\ \\ \\ \longrightarrow \quad 2x \\ \\ \longrightarrow \quad 2x+1 \end{array}$$

Это дает нам

$$x^2y + xy^2 + y^2 = (x+1)\cdot(y^2-1) + x\cdot(xy-1) + 2x + 1. \quad (3)$$

Если мы сравним (3) с (1), то увидим, что полученный нами остаток не равен остатку в примере 2.

Этот пример показывает, что остаток r не определен однозначно требованием, чтобы ни один его член не делился ни на один из $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Положение, однако, не является совсем неконтролируемым: аккуратное выполнение алгоритма (самое главное, проверка делимости $\mathrm{LT}(p)$ на $\mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots$, соблюдая порядок полиномов f_i) гарантирует однозначность вычисления $a_1, \ldots, a_s$ и r. (См. упр. 11, где обсуждается, как охарактеризовать результат работы алгоритма.) Примеры 2 и 4 показывают, однако, что *упорядочение* полиномов в s-наборе $(f_1, \ldots, f_s)$ влияет и на количество шагов алгоритма, и на результат. Полиномы a_i и r могут измениться при изменении порядка делителей f_i. (Они могут измениться при переходе к другому мономиальному упорядочению, но это уже совсем другая история.)

Важным достоинством алгоритма деления в $k[x]$ является возможность с его помощью решать задачу о принадлежности идеалу (см. упр. 1 из § 1). Обладает ли подобным свойством обобщенный

алгоритм деления? Вот простое следствие теоремы 3: если остаток от деления f на $F = (f_1, \ldots, f_s)$ равен нулю, $r = 0$, т. е.

$$f = a_1 f_1 + \ldots + a_s f_s,$$

то $f \in \langle f_1, \ldots, f_s \rangle$. Другими словами, $r = 0$ — это *достаточное* условие принадлежности идеалу. Следующий пример показывает, однако, что $r = 0$ не является *необходимым* условием.

Пример 5. Пусть $f_1 = xy + 1$, $f_2 = y^2 - 1 \in k[x, y]$ с lex-упорядочением. Если мы разделим $f = xy^2 - x$ на $F = (f_1, f_2)$, то в результате получим

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

С другой стороны, деля f на $F = (f_2, f_1)$, получаем

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Из второго равенства следует, что $f \in \langle f_1, f_2 \rangle$. Но тогда первое равенство демонстрирует, что, хотя f и принадлежит идеалу $\langle f_1, f_2 \rangle$, остаток от деления f на F не равен нулю.

Таким образом, алгоритм деления, определенный теоремой 3, является несовершенным обобщением алгоритма деления в $k[x]$. Чтобы исправить ситуацию, следует вспомнить об одном правиле, сформулированном в гл. 1: если мы работаем с набором полиномов $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, то следует рассматривать идеал I, ими порожденный. Другими словами, следует рассматривать и другие наборы полиномов, порождающие тот же идеал. Можно сформулировать естественную задачу: существует ли для произвольного идеала I «хорошее» порождающее множество, т. е. такое, что остаток r от деления на множество «хороших» образующих элементов был бы однозначно определен и условие $r = 0$ было бы *необходимым и достаточным* условием принадлежности идеалу. В § 6 мы увидим, что базисы Грёбнера обладают этими «хорошими» свойствами.

Решая упражнения к этому параграфу, вы с помощью системы компьютерной алгебры должны самостоятельно определить свойства «хороших» порождающих множеств. Точное определение «хорошего» множества будет дано в § 5 этой главы.

Упражнения к § 3

1. Найдите (вручную) остаток от деления данного полинома f на упорядоченный набор F, используя grlex- и lex-упорядочения.
   (a) $f = x^7y^2 + x^3y^2 - y + 1$, $F = (xy^2 - x, x - y^3)$.
   (b) Проделайте задачу (a) еще раз, изменив порядок делителей в F.

2. Вычислите остаток от деления:
   (a) $f = xy^2z^2 + xy - yz$, $F = (x - y^2, y - z^3, z^2 - 1)$.
   (b) Проделайте задачу (a) еще раз, циклически изменив порядок делителей в F.
3. Используя систему компьютерной алгебры, проверьте ваши решения упр. 1 и 2. (Возможно, вам придется разобраться в командах вашей системы и понять, может ли она выполнять деление автоматически или для этого понадобится создать группу команд.)
4. Пусть $f = a_1 f_1 + \ldots + a_s f_s + r$ — результат деления. Завершите доказательство (начатое в тексте параграфа) того, что $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$, если $a_i f_i \neq 0$.

В следующих задачах рассматривается зависимость остатка от порядка делителей в s-наборе $F = (f_1, \ldots, f_s)$ и от мономиального упорядочения. Для вычислений вы можете использовать какую-либо систему компьютерной алгебры.

5. В этой задаче мы подробно рассмотрим деление полинома $f = x^3 - x^2y - x^2z + x$ на $f_1 = x^2y - z$ и $f_2 = xy - 1$.
   (a) Используя grlex-упорядочение, найдите:

   $$r_1 = \text{остаток от деления } f \text{ на } (f_1, f_2).$$
   $$r_2 = \text{остаток от деления } f \text{ на } (f_2, f_1).$$

   Вы получите два *разных* ответа. На каком именно шаге алгоритма деления возникает это различие? (Здесь вам придется несколько шагов вычислить вручную.)
   (b) Верно ли, что $r = r_1 - r_2 \in \langle f_1, f_2 \rangle$? Если да, то найдите явное представление $r = Af_1 + Bf_2$, если нет, то объясните почему.
   (c) Найдите остаток от деления r на (f_1, f_2). Можете ли вы дать ответ, не решая задачу?
   (d) Найдите другой полином $g \in \langle f_1, f_2 \rangle$, такой, что остаток от деления g на (f_1, f_2) не равен нулю. Указание: $(xy + 1) \cdot f_2 = x^2y^2 - 1$, в то время как $y \cdot f_1 = x^2y^2 - yz$.
   (e) Решает ли алгоритм деления задачу о принадлежности идеалу $\langle f_1, f_2 \rangle$? Объясните ваш ответ.
6. Используя grlex-упорядочение, найдите элемент $g \in \langle f_1, f_2 \rangle = \langle 2xy^2 - x, 3x^2y - y - 1 \rangle \subset \mathbb{R}[x, y]$, остаток от деления которого на (f_1, f_2) не равен нулю. Указание: вы можете найти такой элемент g, что остаток равен самому g.
7. Решите упр. 6 для $\langle f_1, f_2, f_3 \rangle = \langle x^4y^2 - z, x^3y^3 - 1, x^2y^4 - 2z \rangle \subset \mathbb{R}[x, y, z]$. Найдите два различных полинома g (отличающиеся не только на ненулевой постоянный множитель) с этим свойством.
8. Попытайтесь найти общую схему построения примеров в упр. 5 (c), (d), 6 и 7. Какое свойство старшего члена полинома $g = A_1 f_1 + \ldots + A_s f_s$ гарантирует, что остаток от деления g на $(f_1, \ldots, f_s)$ отличен от

нуля? Может ли это свойство помочь при решении задачи о принадлежности идеалу?

9. Обсуждение уравнения (2) § 4 гл. 1 показало, что любой полином $f \in \mathbb{R}[x, y, z]$ может быть записан в виде

$$f = h_1(y - x^2) + h_2(z - x^3) + r,$$

где r зависит только от x ($\mathbf{V}(y-x^2, z-x^3)$ — скрученная кубика в $\mathbb{R}^3$).
   (a) Докажите это, используя алгоритм деления. Указание: для этого необходимо правильно выбрать мономиальное упорядочение.
   (b) Используя параметризацию скрученной кубики, докажите, что функция $z^2 - x^4y$ обращается в нуль во всех точках кубики.
   (c) Используя алгоритм деления, найдите явное представление

$$z^2 - x^4y = h_1(y - x^2) + h_2(z - x^3).$$

10. Пусть $V \subset \mathbb{R}^3$ — кривая с параметризацией $(t, t^m, t^n), n, m \geq 2$.
   (a) Докажите, что V — аффинное многообразие.
   (b) Примените метод упр. 9 для определения $\mathbf{I}(V)$.

11. В этом упражнении мы полностью охарактеризуем выражение

$$f = a_1f_1 + \ldots + a_sf_s + r,$$

которое является результатом работы алгоритма деления (среди других подобных представлений полинома f в таком виде). Пусть $LM(f_i) = x^{\alpha(i)}$. Положим

$$\begin{aligned}
\Delta_1 &= \alpha(1) + \mathbb{Z}^n_{\geq 0},\\
\Delta_2 &= (\alpha(2) + \mathbb{Z}^n_{\geq 0}) - \Delta_1,\\
&\vdots\\
\Delta_s &= (\alpha(s) + \mathbb{Z}^n_{\geq 0}) - \left(\bigcup_{i=1}^{s-1} \Delta_i\right),\\
\bar{\Delta} &= \mathbb{Z}^n_{\geq 0} - \left(\bigcup_{i=1}^{s} \Delta_i\right).
\end{aligned}$$

(Обратите внимание, что $\mathbb{Z}^n_{\geq 0}$ является несвязным объединением Δ_i и $\bar{\Delta}$.)
   (a) Докажите, что $\beta \in \Delta_i$ в том и только том случае, когда $x^{\alpha(i)}$ делит x^β, но $x^{\alpha(j)}$ не делит x^β при $j < i$.
   (b) Докажите, что $\gamma \in \bar{\Delta}$ в том и только том случае, когда никакой моном $x^{\alpha(i)}$ не делит x^γ.
   (c) Пусть $f = a_1f_1 + \ldots + a_sf_s + r$ — результат применения алгоритма деления. Докажите, что для любого i справедлив следующий факт: если моном x^β участвует в записи a_i, то $\beta + \alpha(i) \in \Delta_i$. Кроме того, если моном x^γ участвует в записи r, то $\gamma \in \bar{\Delta}$.

   (d) Докажите, что только одно выражение $f = a_1f_1 + \ldots + a_sf_s + r$ удовлетворяет условиям п. (c).

12. Докажите, что оператор вычисления остатка от деления на $F = (f_1, \ldots, f_s)$ линеен над k. Таким образом, если остаток от деления g_i на F равен r_i, $i = 1, 2$, то остаток от деления $c_1g_1 + c_2g_2$ на F равен $c_1r_1 + c_2r_2$, $c_1, c_2 \in k$. Указание: используйте результат упр. 11.

§ 4. Мономиальные идеалы и лемма Диксона

В этом параграфе мы рассмотрим задачу описания идеала из § 1 для частного случая мономиальных идеалов. Для этого нам будет нужно подробно изучить свойства таких идеалов. Полученные результаты найдут неожиданное применение в теории мономиальных упорядочений.

Сначала мы дадим определение мономиального идеала в $k[x_1, \ldots, x_n]$.

Определение 1. Идеал $I \subset k[x_1, \ldots, x_n]$ называется *мономиальным*, если существует подмножество $A \subset \mathbb{Z}^n_{\geq 0}$ (которое может быть бесконечным), такое, что I состоит из всех конечных сумм вида $\sum_{\alpha \in A} h_\alpha x^\alpha$, где $h_\alpha \in k[x_1, \ldots, x_n]$. Такой идеал I будет обозначаться через $\langle x^\alpha : \alpha \in A \rangle$.

Вот пример мономиального идеала: $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subset k[x, y]$. Более интересные примеры мономиальных идеалов будут рассматриваться в § 5.

Сначала мы охарактеризуем *все* мономы, принадлежащие заданному мономиальному идеалу.

Лемма 2. *Пусть $I = \langle x^\alpha : \alpha \in A \rangle$ — мономиальный идеал. Тогда моном x^β принадлежит I в том и только том случае, когда x^β делится на некоторый моном $x^\alpha, \alpha \in A$.*

Доказательство. Если x^β делится на некоторый x^α, $\alpha \in A$, то по определению мономиального идеала $x^\beta \in I$. Докажем обратное. Пусть $x^\beta \in I$; тогда $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, где $h_i \in k[x_1, \ldots, x_n]$, а $\alpha(i) \in A$. Если мы рассмотрим каждый h_i как линейную комбинацию мономов, то получим, что каждый член в равенстве справа делится на некоторый $x^{\alpha(i)}$. Значит, и левая часть равенства, т. е. x^β, обладает тем же свойством, потому что моном x^β содержится как член хотя бы в одном слагаемом $h_ix^{\alpha(i)}$. □

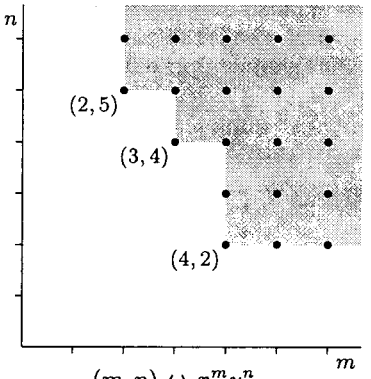
Напомним, что x^β делится на x^α, если $x^\beta = x^\alpha \cdot x^\gamma$ для некоторого $\gamma \in \mathbb{Z}^n_{\geq 0}$. Значит, $\beta = \alpha + \gamma$, т. е. множество

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\}$$

состоит из показателей степеней всех мономов, которые делятся на x^α. Это наблюдение и лемма 2 позволяют графически представить множество всех мономов, принадлежащих данному мономиальному идеалу. Например, если $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle$, то показатели степени мономов, принадлежащих I, образуют множество

$$((4,2) + \mathbb{Z}^2_{\geq 0}) \cup ((3,4) + \mathbb{Z}^2_{\geq 0}) \cup ((2,5) + \mathbb{Z}^2_{\geq 0}).$$

Мы можем изобразить это множество как объединение целочисленных точек в трех сдвинутых экземплярах первого квадранта на плоскости:



$(m,n) \leftrightarrow x^m y^n$

Теперь мы докажем, что принадлежность полинома f мономиальному идеалу определяется мономами, линейной комбинацией которых является f.

Лемма 3. *Пусть I — некоторый мономиальный идеал, а $f \in k[x_1,\dots,x_n]$. Тогда следующие условия эквивалентны:*

(i) $f \in I$;
(ii) *каждый член полинома f принадлежит I;*
(iii) *f является k-линейной комбинацией мономов из I.*

Доказательство. Цепочка импликаций (iii)⇒(ii)⇒(i) очевидна. Доказательство импликации (i)⇒(iii) аналогично доказательству леммы 2, и мы оставляем его читателю в качестве упражнения. □

Следствием п. (iii) леммы 3 является тот факт, что мономиальный идеал однозначно определен своими мономами. То есть мы имеем следующее утверждение.

Следствие 4. *Два мономиальных идеала совпадают в том и только том случае, когда совпадают множества мономов, содержащихся в них.*

Главный результат этого параграфа состоит в том, что все мономиальные идеалы в $k[x_1,\dots,x_n]$ конечно порождены.

Теорема 5 (лемма Диксона). *Любой мономиальный идеал $I = \langle x^\alpha : \alpha \in A\rangle \subset k[x_1,\dots,x_n]$ может быть представлен в виде $I = \langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$, где $\alpha(1),\dots,\alpha(s) \in A$. В частности, I имеет конечный базис.*

Доказательство. Доказательство проводится индукцией по n — числу переменных. Если $n = 1$, то I порожден мономами x_1^α, где $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Пусть β — наименьший элемент в A. Тогда для всех $\alpha \in A$ имеем $\beta \leq \alpha$. Таким образом, x_1^β делит все образующие x_1^α, т. е. $I = \langle x_1^\beta\rangle$.

Пусть $n > 1$ и теорема справедлива для $n-1$. Обозначим переменные через $x_1,\dots,x_{n-1},y$, так что мономы в $k[x_1,\dots,x_{n-1},y]$ будут записываться в виде $x^\alpha y^m$, где $\alpha \in \mathbb{Z}^{n-1}_{\geq 0}$, а $m \in \mathbb{Z}_{\geq 0}$.

Пусть $I \subset k[x_1,\dots,x_{n-1},y]$ — мономиальный идеал. Рассмотрим идеал $J \subset k[x_1,\dots,x_{n-1}]$, порожденный такими мономами x^α, что $x^\alpha y^m \in I$ для некоторого $m \geq 0$. Так как J — мономиальный идеал в $k[x_1,\dots,x_{n-1}]$, то по предположению индукции он конечно порожден, $J = \langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$. Идеал J может рассматриваться, как «проекция» идеала I в $k[x_1,\dots,x_{n-1}]$.

По определению J для каждого i, $1 \leq i \leq s$, существует $m_i \geq 0$, такое, что $x^{\alpha(i)}y^{m_i} \in I$. Пусть m — наибольшее из m_i. Для каждого l, $0 \leq l \leq m-1$, рассмотрим идеал $J_l \subset k[x_1,\dots,x_{n-1}]$, порожденный такими мономами x^β, что $x^\beta y^l \in I$. Неформально можно сказать, что J_l — это «срез» идеала I, порожденный мономами, которые содержат y точно в степени l. По предположению индукции J_l конечно порожден, $J_l = \langle x^{\alpha_l(1)},\dots,x^{\alpha_l(s_l)}\rangle$.

Мы утверждаем, что I порожден мономами, перечисленными в следующем списке:

$$\begin{array}{lll}
\text{из} & J: & x^{\alpha(1)}y^m,\dots,x^{\alpha(s)}y^m,\\
\text{из} & J_0: & x^{\alpha_0(1)},\dots,x^{\alpha_0(s_0)},\\
\text{из} & J_1: & x^{\alpha_1(1)}y,\dots,x^{\alpha_1(s_1)}y,\\
 & \vdots & \\
\text{из} & J_{m-1}: & x^{\alpha_{m-1}(1)}y^{m-1},\dots,x^{\alpha_{m-1}(s_{m-1})}y^{m-1}.
\end{array}$$

Сначала докажем, что каждый моном в I делится хотя бы на один моном из списка. Пусть $x^\alpha y^p \in I$. Если $p \geq m$, то по определению J моном $x^\alpha y^p$ делится на некоторый моном $x^{\alpha(i)}y^m$. С другой стороны, если $p \leq m-1$, то по определению идеала J_p моном $x^\alpha y^p$ делится на некоторый моном $x^{\alpha_p(j)}y^p$. Из леммы 2 следует, что мономы

из списка порождают идеал, содержащий те же мономы, которые содержит I. Тогда по следствию 4 эти идеалы совпадают, и наше утверждение доказано.

Чтобы закончить доказательство теоремы, нам нужно доказать, что конечное множество образующих можно выбрать из заданного множества образующих идеала I. Будем обозначать переменные, как и раньше, $x_1, \dots, x_n$. Тогда $I = \langle x^\alpha : \alpha \in A\rangle \subset k[x_1, \dots, x_n]$. Нам нужно доказать, что I порожден конечным набором x^α, $\alpha \in A$. Выше мы уже доказали, что $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)}\rangle$, где $x^{\beta(i)} \in I$. Так как $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A\rangle$, то по лемме 2 каждый моном $x^{\beta(i)}$ делится на некоторый моном $x^{\alpha(i)}$, где $\alpha(i) \in A$. Теперь очевидно, что $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle$ (пропущенные детали доказательства разобраны в упр. 6). Доказательство теоремы закончено. □

Чтобы лучше понять структуру доказательства теоремы 5, разберем пример идеала $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle$, с которым мы уже имели дело в этом параграфе. Из рисунка видно, что «проекция» есть $J = \langle x^2\rangle \subset k[x]$. Так как $x^2y^5 \in I$, то $m = 5$. Выпишем теперь «срезы» J_l, $0 \le l \le 4 = m - 1$, порожденные мономами, содержащими y^l:

$$\begin{aligned} J_0 = J_1 &= \{0\}, \\ J_2 = J_3 &= \langle x^4\rangle, \\ J_4 &= \langle x^3\rangle. \end{aligned}$$

Эти «срезы» легко увидеть на рисунке. Теперь из доказательства теоремы 5 следует, что $I = \langle x^2y^5, x^4y^2, x^4y^3, x^3y^4\rangle$.

Теорема 5 решает задачу описания идеала в мономиальном случае, так как доказывает существование у него конечного базиса. Этот факт, в свою очередь, позволяет решить задачу о принадлежности мономиальному идеалу. А именно, пусть $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle$. Тогда легко доказать, что данный полином f принадлежит I в том и только том случае, когда остаток от деления f на $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ равен нулю. В упр. 9 уточняются детали этого рассуждения.

Лемма Диксона применяется для доказательства следующего важного утверждения о мономиальных упорядочениях на $k[x_1, \dots, x_n]$.

Следствие 6. *Пусть $>$ — некоторое отношение на $\mathbb{Z}^n_{\ge 0}$, удовлетворяющее следующим условиям:*

(i) *$>$ — линейное упорядочение на $\mathbb{Z}^n_{\ge 0}$;*
(ii) *если $\alpha > \beta$ и $\gamma \in \mathbb{Z}^n_{\ge 0}$, то $\alpha + \gamma > \beta + \gamma$.*

Тогда $>$ является вполне упорядочением в том и только том случае, когда $\alpha \ge 0$ для всех $\alpha \in \mathbb{Z}^n_{\ge 0}$.

Доказательство. $\Rightarrow$. Пусть $>$ является вполне упорядочением, и пусть α_0 — наименьший элемент в $\mathbb{Z}^n_{\ge 0}$. Достаточно доказать, что $\alpha_0 \ge 0$. Это просто: если $0 > \alpha_0$, то по (ii) мы можем прибавить α_0 к обеим частям неравенства и получить $\alpha_0 > 2\alpha_0$, а это противоречит тому, что α_0 — наименьший элемент в $\mathbb{Z}^n_{\ge 0}$.

$\Leftarrow$. Пусть $\alpha \ge 0$ для всех $\alpha \in \mathbb{Z}^n_{\ge 0}$, и пусть $A \subset \mathbb{Z}^n_{\ge 0}$ — некоторое непустое множество. Нам нужно доказать, что в A существует наименьший элемент. Рассмотрим мономиальный идеал $I = \langle x^\alpha : \alpha \in A\rangle$. По лемме Диксона существуют мономы $\alpha(1), \dots, \alpha(s) \in A$, такие, что $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle$. Пусть $\alpha(1) < \alpha(2) < \dots < \alpha(s)$ (в противном случае перенумеруем мономы). Мы утверждаем, что $\alpha(1)$ — наименьший элемент множества A. Докажем это. Рассмотрим произвольный элемент $\alpha \in A$. Тогда $x^\alpha \in \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle$. По лемме 2 моном x^α делится на некоторый моном $x^{\alpha(i)}$, т. е. $\alpha = \alpha(i) + \gamma$, $\gamma \in \mathbb{Z}^n_{\ge 0}$. Тогда $\gamma \ge 0$ и по (ii) мы имеем

$$\alpha = \alpha(i) + \gamma \ge \alpha(i) + 0 = \alpha(i) \ge \alpha(1).$$

Значит, $\alpha(1)$ — наименьший элемент в A. □

Теперь мы можем упростить определение мономиального упорядочения (определение 1 § 2). Условия (i) и (ii) определения сохраняются, а условие (iii) заменяется на более простое: $\alpha \ge 0$ для всех $\alpha \in \mathbb{Z}^n_{\ge 0}$. Новое условие *значительно* упрощает проверку того, что данное упорядочение является мономиальным. В упр. 10–12 рассмотрены соответствующие примеры.

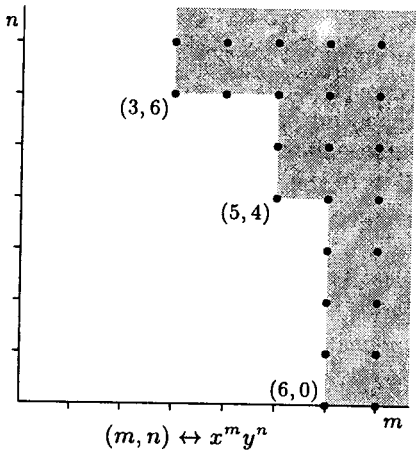
Упражнения к § 4

1. Рассмотрим идеал $I \subset k[x_1, \dots, x_n]$, который обладает следующим свойством: если $f = \sum_\alpha c_\alpha x^\alpha \in I$, то любой моном x^α из f принадлежит I. Докажите, что I — мономиальный идеал.

2. Завершите доказательство леммы 3.

3. Пусть $I = \langle x^6, x^2y^3, xy^7\rangle \subset k[x, y]$.
   (a) На плоскости (m, n) изобразите точки (m, n), такие, что мономы $x^m y^n$ встречаются в элементах из I.
   (b) Если мы поделим с помощью алгоритма деления полином $f \in k[x, y]$ на набор образующих идеала I, то какие мономы могут появиться в остатке?

4. Пусть $I \subset k[x,y]$ — мономиальный идеал, базис которого над k образуют мономы x^β, такие, что β принадлежит выделенной области на рисунке:



   (a) Используя метод, примененный в доказательстве теоремы 5, найдите базис идеала I.
   (b) Является ли найденный базис наименьшим или при удалении какого-нибудь β оставшееся множество по-прежнему порождает I?

5. Пусть $I = \langle x^\alpha : \alpha \in A\rangle$ — мономиальный идеал, а множество $S \subset \mathbb{Z}^n_{\geq 0}$ определено так: $\beta \in S$ в том и только том случае, когда моном x^β встречается в I. Пусть $>$ — некоторое мономиальное упорядочение. Докажите, что наименьший элемент в S (по отношению к $>$) принадлежит A.

6. Пусть $I = \langle x^\alpha : \alpha \in A\rangle$ — некоторый мономиальный идеал, и пусть I имеет конечный базис, $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)}\rangle$. Из доказательства леммы Диксона следует, что каждый моном $x^{\beta(i)}$ делится на некоторый моном $x^{\alpha(i)}$, где $\alpha(i) \in A$. Докажите, что $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle$.

7. Докажите, что лемма Диксона эквивалентна следующему утверждению: пусть $A \subset \mathbb{Z}^n_{\geq 0}$ — некоторое подмножество; тогда существует конечный набор элементов $\alpha(1), \dots, \alpha(s) \in A$, таких, что для любого $\alpha \in A$ существуют число i и вектор $\gamma \in \mathbb{Z}^n_{\geq 0}$, такие, что $\alpha = \alpha(i) + \gamma$.

8. Базис $\{x^{\alpha(1)}, \dots, x^{\alpha(s)}\}$ мономиального идеала I называется *минимальным*, если $x^{\alpha(i)}$ не делит $x^{\alpha(j)}$ ни для каких $i \neq j$.
   (a) Докажите, что любой мономиальный идеал имеет минимальный базис.
   (b) Докажите, что любой мономиальный идеал имеет *единственный* минимальный базис.

9. Пусть $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle$ — мономиальный идеал. Докажите, что $f \in I$ в том и только том случае, когда остаток от деления f на $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ равен нулю. Указание: воспользуйтесь леммами 2 и 3.

10. Рассмотрим кольцо полиномов $k[x_1, \dots, x_n, y_1, \dots, y_m]$. Зададим мономиальное упорядочение $>_{\text{mixed}}$ в этом кольце, которое сочетает lex-упорядочение для $x_1, \dots, x_n$ и grlex-упорядочение для $y_1, \dots, y_m$. Моном от $n+m$ переменных мы будем записывать как $x^\alpha y^\beta$, где $\alpha \in \mathbb{Z}^n_{\geq 0}$, $\beta \in \mathbb{Z}^m_{\geq 0}$. Тогда

$$x^\alpha y^\beta >_{\text{mixed}} x^\gamma y^\delta \iff x^\alpha >_{\text{lex}} x^\gamma \quad \text{или} \quad x^\alpha = x^\gamma \quad \text{и} \quad y^\beta >_{\text{grlex}} y^\delta.$$

Докажите, используя следствие 6, что $>_{\text{mixed}}$ является мономиальным упорядочением. Это пример того, что называется *произведением упорядочений*. Очевидно, что таким способом можно получить много новых мономиальных упорядочений.

11. В этом упражнении мы рассмотрим частный случай *взвешенного упорядочения*. Пусть $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{R}^n$, причем $u_1, \dots, u_n$ положительны и линейно независимы над $\mathbb{Q}$. Мы назовем $\mathbf{u}$ *независимым весовым вектором*. Определим упорядочение $>_{\mathbf{u}}$ следующим образом: пусть $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$; тогда

$$\alpha >_{\mathbf{u}} \beta \iff \mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta,$$

где $\cdot$ обозначает скалярное произведение. Оно называется *взвешенным упорядочением*, определенным вектором $\mathbf{u}$.
   (a) Используя следствие 6, докажите, что $>_{\mathbf{u}}$ является мономиальным упорядочением. Указание: почему существенно требование, чтобы $u_1, \dots, u_n$ были линейно независимы?
   (b) Докажите, что $\mathbf{u} = (1, \sqrt{2})$ — независимый весовой вектор, так что $>_{\mathbf{u}}$ — взвешенное упорядочение на $\mathbb{Z}^2_{\geq 0}$.
   (c) Докажите, что $\mathbf{u} = (1, \sqrt{2}, \sqrt{3})$ — независимый весовой вектор, так что $>_{\mathbf{u}}$ — взвешенное упорядочение на $\mathbb{Z}^3_{\geq 0}$.

12. Другое важное взвешенное упорядочение может быть построено следующим образом. Пусть $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{Z}^n_{\geq 0}$. Зафиксируем некоторое мономиальное упорядочение $>_\sigma$ (такое, как $>_{\text{lex}}$ или $>_{\text{grevlex}}$, например) на $\mathbb{Z}^n_{\geq 0}$. Теперь для $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ положим $\alpha >_{\mathbf{u},\sigma} \beta$ в том и только том случае, когда

$$\mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta \quad \text{или} \quad \mathbf{u} \cdot \alpha = \mathbf{u}, \cdot \beta \quad \text{и} \quad \alpha >_\sigma \beta.$$

Мы назовем $>_{\mathbf{u},\sigma}$ *взвешенным упорядочением, определенным вектором* $\mathbf{u}$ *и упорядочением* σ.
   (a) Используя следствие 6, докажите, что $>_{\mathbf{u},\sigma}$ — мономиальное упорядочение.
   (b) Найдите $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$, такой, что взвешенное упорядочение $>_{\mathbf{u},lex}$ является grlex-упорядочением.

(c) В определение взвешенного упорядочения $>_{\mathbf{u},\sigma}$ упорядочение $>_\sigma$ начинает работать только в случае равенства скалярных произведений. Такие равенства, однако, *всегда* встречаются. А именно, докажите, что для данного $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$ всегда найдутся $\alpha \neq \beta$ в $\mathbb{Z}^n_{\geq 0}$, такие, что $\mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta$. Указание: рассмотрите линейное уравнение $u_1 a_1 + \ldots + u_n a_n = 0$ над $\mathbb{Q}$. Докажите, что существует ненулевое целочисленное решение $(a_1, \ldots, a_n)$ этого уравнения и затем докажите, что существуют $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, такие, что $\alpha - \beta = (a_1, \ldots, a_n)$.

(d) Полезным примером взвешенного упорядочения является *исключающее упорядочение*, определенное в работе BAYER, STILLMAN (1987b). Пусть i — целое число, $1 \leq i \leq n$. Пусть $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$ (i единиц и $n - i$ нулей). Тогда i-е *исключающее упорядочение* $>_i$ — это взвешенное упорядочение $>_{\mathbf{u},\text{grevlex}}$. Докажите, что $>_i$ обладает следующим свойством: пусть x^α — моном, который содержит хотя бы одну из переменных $x_1, \ldots, x_i$; тогда $x^\alpha >_i x^\beta$ для *любого* монома x^β, который не содержит ни одной из переменных $x_1, \ldots, x_i$. Исключающие упорядочения играют важную роль в теории исключения, которой мы будем заниматься в следующей главе.

Упорядочения, рассмотренные в упр. 11 и 12, являются лишь частными случаями взвешенных упорядочений. Конструкция общего случая такова: рассмотрим вектор $\mathbf{u}_1 \in \mathbb{R}^n$, координаты которого не обязательно линейно независимы над $\mathbb{Q}$. Положим $\alpha > \beta$, если $\mathbf{u}_1 \cdot \alpha > \mathbf{u}_1 \cdot \beta$. Однако может случиться так, что скалярные произведения равны. В случае равенства мы используем другой вектор $\mathbf{u}_2 \in \mathbb{R}^n$. Будем считать, что $\alpha > \beta$, если $\mathbf{u}_1 \cdot \alpha = \mathbf{u}_1 \cdot \beta$ и $\mathbf{u}_2 \cdot \alpha > \mathbf{u}_2 \cdot \beta$. Если $\mathbf{u}_1 \cdot \alpha = \mathbf{u}_1 \cdot \beta$ и $\mathbf{u}_2 \cdot \alpha = \mathbf{u}_2 \cdot \beta$, то используется третий вектор $\mathbf{u}_3$ и т. д. Можно доказать, что *любое* мономиальное упорядочение на $\mathbb{Z}^n_{\geq 0}$ может быть построено таким образом. Подробное изложение теории взвешенных упорядочений и ее связи с теорией мономиальных упорядочений можно найти в работе ROBBIANO (1986).

§ 5. Теорема Гильберта о базисе и базисы Грёбнера

В этом параграфе мы дадим полное решение *задачи описания идеала* из § 1. Для этого нам будет необходимо определить базисы с «хорошими» (по отношению к алгоритму деления из § 3) свойствами. Ключевая идея состоит в том, что как только задано мономиальное упорядочение, то однозначно определен старший член каждого полинома $f \in k[x_1, \ldots, x_n]$. Тогда для каждого идеала I мы можем определить его *идеал старших членов* следующим образом.

Определение 1. Пусть $I \subset k[x_1, \ldots, x_n]$ — ненулевой идеал.

(i) Обозначим через $\text{LT}(I)$ множество старших членов элементов из I, т. е.

$$\text{LT}(I) = \{cx^\alpha : \text{существует } f \in I \text{ и } \text{LT}(f) = cx^\alpha\}.$$

(ii) Обозначим через $\langle \text{LT}(I) \rangle$ идеал, порожденный элементами из $\text{LT}(I)$.

Мы уже видели важную роль старших членов в алгоритме деления. Следует отметить один тонкий, но важный момент в определении $\langle \text{LT}(I) \rangle$. А именно, пусть I конечно порожден, $I = \langle f_1, \ldots, f_s \rangle$. Тогда $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$ и $\langle \text{LT}(I) \rangle$ могут быть *разными* идеалами. Конечно, $\text{LT}(f_i) \in \text{LT}(I) \subset \langle \text{LT}(I) \rangle$; поэтому $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle \subset \langle \text{LT}(I) \rangle$. Однако $\langle \text{LT}(I) \rangle$ может быть строго больше. Рассмотрим следующий пример.

Пример 2. Пусть $I = \langle f_1, f_2 \rangle$, где $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$, и на мономах из $k[x, y]$ задано grlex-упорядочение. Тогда

$$x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2,$$

так что $x^2 \in I$, т. е. $x^2 = \text{LT}(x^2) \in \langle \text{LT}(I) \rangle$. С другой стороны, x^2 не делится на $\text{LT}(f_1) = x^3$ и на $\text{LT}(f_2) = x^2y$. Поэтому $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$ по лемме 2 из § 4.

В упражнениях к § 3 рассматривались другие примеры идеалов $I = \langle f_1, \ldots, f_s \rangle$, где $\langle \text{LT}(I) \rangle$ строго больше, чем $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$. В упражнениях к этому параграфу мы обсудим, как этот факт влияет на решение задачи о принадлежности идеалу.

Мы докажем, что $\langle \text{LT}(I) \rangle$ — мономиальный идеал. Это позволит нам применять результаты § 4. В частности, это означает, что $\langle \text{LT}(I) \rangle$ порожден конечным множеством старших членов.

Предложение 3. *Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Тогда*

(i) $\langle \text{LT}(I) \rangle$ — *мономиальный идеал;*
(ii) *существуют полиномы $g_1, \ldots, g_s \in I$, такие, что $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$.*

Доказательство. (i) Старшие мономы $\text{LM}(g)$ элементов $g \in I - \{0\}$ порождают мономиальный идеал $\langle \text{LM}(g) : g \in I - \{0\} \rangle$. Так как $\text{LM}(g)$ отличается от $\text{LT}(g)$ на ненулевой множитель из поля k, то этот идеал совпадает с идеалом $\langle \text{LT}(g) : g \in I - \{0\} \rangle = \langle \text{LT}(I) \rangle$ (см. упр. 4). Таким образом, $\langle \text{LT}(I) \rangle$ — мономиальный идеал.

(ii) Так как $\langle \mathrm{LT}(I)\rangle$ порожден мономами $\mathrm{LM}(g)$, $g \in I - \{0\}$, то по лемме Диксона из § 4 $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)\rangle$ для конечного набора $g_1, \ldots, g_t \in I$. Так как $\mathrm{LM}(g_i)$ отличается от $\mathrm{LT}(g_i)$ на ненулевой множитель из поля k, то $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. Доказательство окончено. □

Теперь, используя предложение 3 и алгоритм деления, мы можем доказать конечную порожденность *любого* полиномиального идеала. Это дает утвердительный ответ на вопрос об описании идеала из § 1. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал, и пусть $\langle \mathrm{LT}(I)\rangle$ — его идеал старших членов. Как всегда, мы считаем, что задано некоторое мономиальное упорядочение, используемое в алгоритме деления.

Теорема 4 (теорема Гильберта о базисе). *Каждый идеал $I \subset k[x_1, \ldots, x_n]$ является конечно порожденным, т. е. $I = \langle g_1, \ldots, g_s\rangle$, где $g_1, \ldots, g_s \in I$.*

Доказательство. Если $I = \{0\}$, то наше порождающее множество состоит из одного элемента — нулевого полинома. Если I — ненулевой идеал, то порождающее множество $g_1, \ldots, g_s$ мы будем строить следующим образом. Из предложения 3 вытекает, что существуют полиномы $g_1, \ldots, g_s \in I$, такие, что $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. Мы утверждаем, что $I = \langle g_1, \ldots, g_s\rangle$.

Так как каждый g_i принадлежит I, то $\langle g_1, \ldots, g_s\rangle \subset I$. Пусть теперь $f \in I$ — некоторый элемент. Применим алгоритм деления из § 3 и поделим f на $g_1, \ldots, g_s$. В результате f будет представлен в виде

$$f = a_1 g_1 + \ldots + a_s g_s + r,$$

где ни один член полинома r нельзя поделить ни на один из $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Мы утверждаем, что $r = 0$. Имеем

$$r = f - a_1 g_1 - \ldots - a_s g_s \in I.$$

Если $r \neq 0$, то $\mathrm{LT}(r) \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. Тогда по лемме 2 из § 4 $\mathrm{LT}(r)$ должен делиться хотя бы на один $\mathrm{LT}(g_i)$. Но это противоречит определению остатка. Значит, $r = 0$, т. е.

$$f = a_1 g_1 + \ldots + a_s g_s + 0 \in \langle g_1, \ldots, g_s\rangle,$$

откуда $I \subset \langle g_1, \ldots, g_s\rangle$. Теорема доказана[1]). □

Базис $\{g_1, \ldots, g_s\}$ из теоремы 4 не только дает описание идеала, он обладает еще и специальным свойством $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. Как мы видели в примере 2, не все базисы идеала обладают этим свойством. Таким базисам мы дадим специальное название.

[1]) Доказательство Гильберта было иным. Оно не давало алгоритма нахождения базиса идеала I. (См. Гильберт Д. Избранные труды. Том 1. — М.: Факториал, 1998, с. 26.) — *Прим. ред.*

Определение 5. Пусть задано мономиальное упорядочение. Конечное подмножество $G = \{g_1, \ldots, g_s\}$ элементов идеала I называется его *базисом Грёбнера* (или *стандартным базисом*), если

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(I)\rangle.$$

Чуть менее формально это определение можно переформулировать так: множество $\{g_1, \ldots, g_s\} \subset I$ называется базисом Грёбнера идеала I в том и только том случае, когда старший член любого элемента из I делится на хотя бы один старший член $\mathrm{LT}(g_i)$ (эквивалентность этих определений следует из леммы 2 § 4 — см. упр. 5). Из доказательства теоремы 4 также вытекает следующий результат.

Следствие 6. *Пусть задано некоторое мономиальное упорядочение. Тогда любой ненулевой идеал $I \subset k[x_1, \ldots, x_n]$ обладает базисом Грёбнера. Более того, базис Грёбнера идеала I является его базисом.*

Доказательство. Пусть I — ненулевой идеал и $G = \{g_1, \ldots, g_s\}$ — множество, построенное в теореме 4. Это множество является базисом Грёбнера по определению. Что касается второго утверждения, то, как доказано в теореме 4, если $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$, то $I = \langle g_1, \ldots, g_s\rangle$, т. е. G является базисом в I. (Другое доказательство приведено в упр. 6.) □

В § 6 мы подробно рассмотрим свойства базисов Грёбнера, в частности, мы увидим, что с их помощью можно решить задачу о принадлежности идеалу. Базисы Грёбнера и являются теми «хорошими» порождающими множествами, о которых мы говорили в конце § 3.

В качестве примера рассмотрим идеал I из примера 2. Он имеет базис $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$. Этот базис *не* является базисом Грёбнера по отношению к grlex-упорядочению, так как $x^2 \in \langle \mathrm{LT}(I)\rangle$, но $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2)\rangle$. В § 7 мы научимся строить базисы Грёбнера.

Рассмотрим идеал $J = \langle g_1, g_2\rangle = \langle x + z, y - z\rangle$. Мы утверждаем, что g_1, g_2 образуют базис Грёбнера идеала J по отношению к lex-упорядочению в $\mathbb{R}[x, y, z]$. Для этого мы должны доказать, что старший член каждого ненулевого элемента из J принадлежит идеалу $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2)\rangle = \langle x, y\rangle$. По лемме 2 § 4 это означает, что старший член *любого* ненулевого элемента из J делится на x или на y.

Докажем это. Пусть $f = Ag_1 + Bg_2 \in I$. Пусть $f \neq 0$ и $\mathrm{LT}(f)$ не делится ни на x, ни на y. Тогда по определению lex-упорядочения f

является полиномом от z. С другой стороны, f обращается в нуль на линейном подпространстве $L = \mathbf{V}(x+z, y-z) \subset \mathbb{R}^3$ (так как $f \in J$). Легко проверить, что $(-t, t, t) \in L$ для любого вещественного t. Но единственным полиномом от z, обращающимся в нуль на L, является нулевой полином. Противоречие. Значит, $\langle g_1, g_2 \rangle$ — базис Грёбнера идеала J. В § 6 мы рассмотрим метод, который позволяет определять, когда базис идеала является базисом Грёбнера.

Обратите внимание, что образующие идеала J связаны со ступенчатой формой матрицы коэффициентов

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

Это не случайно: если идеал порожден линейными полиномами, то базис Грёбнера для lex-упорядочения определяется ступенчатой формой матрицы коэффициентов порождающих элементов (см. упр. 9).

Базисы Грёбнера идеалов в полиномиальных кольцах были открыты Б. Бухбергером в 1965 г. и названы им в честь В. Грёбнера (1899–1980) — научного руководителя Бухбергера. Родственное понятие «стандартного базиса» идеала в кольце степенных рядов было независимо введено Х. Хиронакой в 1964 г. Как мы увидим далее в этой главе, Бухбергер также разработал основные алгоритмы для работы с базисами Грёбнера. Термин «базис Грёбнера» используется в английском написании «Groebner base» в качестве команды в некоторых системах компьютерной алгебры.

В конце этого параграфа мы рассмотрим два приложения теоремы Гильберта о базисе. Первое из них — это чисто алгебраическое утверждение об идеалах в $k[x_1, \ldots, x_n]$. *Возрастающей цепью* идеалов называется последовательность:

$$I_1 \subset I_2 \subset I_3 \subset \ldots \quad .$$

Например, последовательность

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \ldots \subset \langle x_1, \ldots, x_n \rangle \tag{1}$$

образует конечную возрастающую цепь идеалов. Если мы попытаемся *продолжить* эту цепь идеалом с бо́льшим числом образующих, то мы столкнемся с одной из двух возможностей. Рассмотрим идеал $\langle x_1, \ldots, x_n, f \rangle$, $f \in k[x_1, \ldots, x_n]$. Если $f \in \langle x_1, \ldots, x_n \rangle$, то наш идеал совпадает с идеалом $\langle x_1, \ldots, x_n \rangle$. Если же $f \notin \langle x_1, \ldots, x_n \rangle$, то $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$. Мы оставляем доказательство этого утверждения читателю (упр. 11). Другими словами, возрастающая цепь (1) может быть продолжена двумя способами: или путем повторения последнего идеала *ad infinitum*, или добавлением $k[x_1, \ldots, x_n]$, а потом повторением его *ad infinitum*. В любом случае возрастающая цепь «стабилизируется» после конечного числа шагов в том смысле, что, начиная с некоторого момента, все идеалы в цепи одинаковы. Нашим следующим результатом будет теорема о том, что «стабилизация» происходит в *каждой* возрастающей цепи идеалов в $k[x_1, \ldots, x_n]$.

Теорема 7 (условие обрыва возрастающих цепей). *Пусть*

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

— возрастающая цепь идеалов в $k[x_1, \ldots, x_n]$. Тогда существует $N \geq 1$, такое, что

$$I_n = I_{N+1} = I_{N+2} = \ldots \quad .$$

Доказательство. Пусть $I_1 \subset I_2 \subset I_3 \subset \ldots$ — возрастающая цепь. Рассмотрим множество $I = \bigcup_{i=1}^{\infty} I_i$. Докажем, что I является идеалом в $k[x_1, \ldots, x_n]$. Имеем $0 \in I$, так как $0 \in I_i$ для любого i. Далее, если $f, g \in I$, то по определению $f \in I_i$, а $g \in I_j$ для некоторых i и j. Пусть, например, $i \leq j$. Так как идеалы образуют возрастающую цепь, то $f, g \in I_j$ (потому что $I_i \subset I_j$). Так как I_j — идеал, то $f+g \in I_j$; значит, $f+g \in I$. Аналогично, пусть $f \in I$ и $r \in k[x_1, \ldots, x_n]$. Тогда $f \in I_i$ для некоторого i и $r \cdot f \in I_i \subset I$. Следовательно, I — идеал.

По теореме Гильберта о базисе I имеет конечный базис $I = \langle f_1, \ldots, f_s \rangle$. Но каждый из образующих элементов f_i содержится в некотором идеале из цепи, т. е. $f_i \in I_{j_i}$, $i = 1, \ldots, s$. Пусть N — максимум j_i; тогда $f_i \in I_N$ для всех i. Следовательно,

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \ldots \subset I.$$

Таким образом, возрастающая цепь стабилизируется, начиная с I_N. Все следующие идеалы в цепи равны друг другу. □

Утверждение о том, что возрастающая цепь идеалов в $k[x_1, \ldots, x_n]$ стабилизируется, часто называется *условием обрыва возрастающих цепей* или, сокращенно, УОВЦ. В упр. 4 надо будет доказать, что из справедливости УОВЦ следует конечная порожденность идеалов, так что УОВЦ эквивалентно заключению теоремы Гильберта о базисе. УОВЦ будет играть ключевую роль в § 7, где мы будем рассматривать алгоритм Бухбергера для построения базисов Грёбнера. Также УОВЦ будет использоваться в гл. 4 при изучении структуры аффинных многообразий.

Второе приложение теоремы Гильберта о базисе — геометрическое. До сих пор мы рассматривали аффинные многообразия как множества решений конечных полиномиальных систем:

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_s) = 0 \quad \text{для всех} \quad i\}.$$

Теорема Гильберта о базисе показывает, что имеет смысл говорить об аффинном многообразии, определенном *идеалом* $I \subset k[x_1, \ldots, x_n]$.

Определение 8. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Положим

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \quad \text{для всех} \quad f \in I\}.$$

Хотя ненулевой идеал содержит бесконечно много различных полиномов, множество $\mathbf{V}(I)$ определено конечным числом полиномиальных уравнений.

Предложение 9. $\mathbf{V}(I)$ *является аффинным многообразием. В частности, если* $I = \langle f_1, \ldots, f_s \rangle$, *то* $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

Доказательство. По теореме Гильберта о базисе идеал I конечно порожден, $I = \langle f_1, \ldots, f_s \rangle$. Мы утверждаем, что $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$. Если $f(a_1, \ldots, a_n) = 0$ для всех полиномов $f \in I$, то $f_i(a_1, \ldots, a_n) = 0$ (так как $f_i \in I$). Следовательно, $\mathbf{V}(I) \subset \mathbf{V}(f_1, \ldots, f_s)$. С другой стороны, пусть $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$, и пусть $f \in I$. Так как $I = \langle f_1, \ldots, f_s \rangle$, то

$$f = \sum_{i=1}^{s} h_i f_i$$

для некоторых $h_i \in k[x_1, \ldots, x_n]$. Но тогда

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_s) \cdot 0 = 0. \end{aligned}$$

Следовательно, $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(I)$, а значит, эти два идеала равны. □

Наиболее важным следствием этого предложения является то, что *многообразия определены идеалами*. Например, в гл. 1 мы доказали, что $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$, если $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$ (предложение 4 § 4 гл. 1). Это предложение является непосредственным следствием предложения 9. Связь между идеалами и многообразиями будет подробно рассмотрена в гл. 4.

В упражнениях, используя предложение 9, мы покажем, как, выбирая подходящее порождающее множество идеала I, можно лучше понять структуру многообразия $\mathbf{V}(I)$.

Упражнения к § 5

1. Пусть $I = \langle g_1, g_2, g_3 \rangle \subset \mathbb{R}[x, y, z]$, где $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$ и $g_3 = x - yz^4$. Используя lex-упорядочение, приведите пример полинома $g \in I$, такого, что $\mathrm{LT}(g) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle$.
2. Для идеалов и их образующих из упр. 5, 6 и 7 к § 3 докажите, что идеал $\langle \mathrm{LT}(I) \rangle$ строго больше, чем идеал $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. Указание: внимательно посмотрите, что именно вы сделали в каждом упражнении.
3. Здесь ситуация упр. 1 и 2 будет обобщена. Пусть $I = \langle f_1, \ldots, f_s \rangle$ — идеал, такой, что $\langle \mathrm{LT}(I) \rangle$ строго больше, чем $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$.
   (a) Докажите, что существует элемент $f \in I$, такой, что остаток от деления f на $f_1, \ldots, f_s$ не равен нулю. Указание: сначала найдите $f \in I$, такой, что $\mathrm{LT}(f) \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$, потом примените лемму 2 из § 4.
   (b) Что упр. (a) говорит о задаче принадлежности идеалу?
   (c) Существует ли связь между упр. (a) и гипотезой, которую вы должны были сформулировать в упр. 8 § 3?
4. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Докажите, что $\langle \mathrm{LT}(g) : g \in I - \{0\} \rangle = \langle \mathrm{LM}(g) : g \in I - \{0\} \rangle$.
5. Пусть I — произвольный идеал в $k[x_1, \ldots, x_n]$. Докажите, что множество $G = \{g_1, \ldots, g_s\} \subset I$ является базисом Грёбнера идеала I в том и только том случае, когда старший член любого элемента из I делится хотя бы на один старший член $\mathrm{LT}(g_i)$.
6. Следствие 6 утверждает, что базис Грёбнера $G = \{g_1, \ldots, g_s\}$ является базисом, т. е. если $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, то $I = \langle g_1, \ldots, g_s \rangle$. Доказательство этого утверждения приведено в теореме 4. Приведем набросок другого доказательства. Пусть $f \in I$. Поделим f на $(g_1, \ldots, g_s)$. На каждом шаге алгоритма деления старший член делимого принадлежит $\langle \mathrm{LT}(I) \rangle$ и, следовательно, делится на один из $\mathrm{LT}(g_i)$. Значит, ни один член не прибавляется к остатку, так что $f = \sum_{i=1}^{s} a_i g_i$ в момент остановки алгоритма. Превратите этот набросок в подробное доказательство.
7. Здесь мы используем grlex-упорядочение с $x > y > z$. Верно ли, что множество $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ является базисом Грёбнера идеала, порожденного этими тремя полиномами? Объясните ваш ответ.
8. Здесь мы используем lex-упорядочение с $x > y > z$. Верно ли, что множество $\{x - z^2, y - z^3\}$ является базисом Грёбнера идеала, порожденного этими двумя полиномами? Объясните ваш ответ. Указание: трудная часть упражнения — определить, какие именно полиномы принадлежат $\langle \mathrm{LT}(I) \rangle$.
9. Пусть $A = (a_{ij})$ — вещественная ступенчатая $m \times n$-матрица, и пусть $J \subset \mathbb{R}[x_1, \ldots, x_n]$ — идеал, порожденный линейными полиномами

$\sum_{j=1}^{n} a_{ij}x_j$, $1 \le i \le m$. Докажите, что множество этих образующих составляет базис Грёбнера идеала J по отношению к подходящему lex-упорядочению. Указание: главные переменные должны быть старше свободных.

10. Пусть $I \subset k[x_1, \ldots, x_n]$ — *главный идеал*, т. е. I порожден одним полиномом $f \in I$ (см. § 5 гл. 1). Докажите, что любое конечное подмножество элементов из I, содержащее f, является базисом Грёбнера для I.

11. Пусть $f \in k[x_1, \ldots, x_n]$ и $f \notin \langle x_1, \ldots, x_n \rangle$. Докажите, что $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$.

12. Докажите, что из справедливости условия обрыва возрастающих цепей идеалов в $k[x_1, \ldots, x_n]$ следует теорема Гильберта о базисе. Указание: рассуждайте от противного, предположив, что существует идеал $I \subset k[x_1, \ldots, x_n]$, не являющийся конечно порожденным. Ваши рассуждения не должны использовать каких-то специальных свойств полиномов. В самом деле, в любом коммутативном кольце R два следующих условия:
    (i) каждый идеал $I \subset R$ конечно порожден,
    (ii) любая возрастающая цепь идеалов в R стабилизируется,
    эквивалентны.

13. Пусть
$$V_1 \supset V_2 \supset V_3 \supset \ldots$$
— *убывающая цепь* аффинных многообразий. Докажите, что существует такое $N \ge 1$, что $V_N = V_{N+1} = V_{N+2} = \ldots$. Указание: используйте упр. 14 § 4 гл. 1.

14. Пусть $f_1, f_2, \ldots \in k[x_1, \ldots, x_n]$ — бесконечная последовательность полиномов, и пусть $I = \langle f_1, f_2, \ldots \rangle$ — идеал, ими порожденный. Докажите, что существует N, такое, что $I = \langle f_1, \ldots, f_N \rangle$. Указание: используйте полиномы $f_1, f_2, \ldots$ для того, чтобы построить возрастающую цепь идеалов.

15. Пусть $f_1, f_2, \ldots \in k[x_1, \ldots, x_n]$, и пусть $\mathbf{V}(f_1, f_2, \ldots) \subset k^n$ — множество решений бесконечной системы уравнений $f_1 = f_2 = \ldots = 0$. Докажите, что существует N, такое, что $\mathbf{V}(f_1, f_2, \ldots) = \mathbf{V}(f_1, \ldots, f_N)$.

16. В § 4 гл. 1 мы определили идеал $\mathbf{I}(V)$ многообразия $V \subset k^n$. А в этом параграфе было определено многообразие, определенное произвольным идеалом (определение 8[1]). В частности, это означает, что $\mathbf{V}(\mathbf{I}(V))$ является многообразием. Докажите, что $\mathbf{V}(\mathbf{I}(V)) = V$. Указание: воспользуйтесь доказательством леммы 7 из § 4 гл. 1.

17. Рассмотрим многообразие $V = \mathbf{V}(x^2 - y, y + x^2 - 4) \subset \mathbb{C}^2$. Отметим, что $V = \mathbf{V}(I)$, где $I = \langle x^2 - y, y + x^2 - 4 \rangle$.
    (a) Докажите, что $I = \langle x^2 - y, x^2 - 2 \rangle$.

[1] И предложение 9. — *Прим. ред.*

    (b) Используя базис идеала I, найденный в п. (a), докажите, что $\mathbf{V}(I) = \{(\pm\sqrt{2}, 2)\}$.

Одна из причин, почему второй базис удобнее для описания многообразия V, состоит в том, что $x^2 - 2$ *разлагается на множители*. Это означает, что V «распадается» на две части. В упр. 18 мы сформулируем утверждение, которое обобщает это наблюдение.

18. Если какие-то элементы базиса идеала разлагаются на множители, то мы можем использовать этот факт для описания многообразия.
    (a) Пусть полином $g \in k[x_1, \ldots, x_n]$ приводим: $g = g_1 g_2$. Докажите, что $\mathbf{V}(f, g) = \mathbf{V}(f, g_1) \cup \mathbf{V}(f, g_2)$ для любого f.
    (b) Докажите, что $\mathbf{V}(y - x^2, xz - y^2) = \mathbf{V}(y - x^2, xz - x^4)$ в $\mathbb{R}^3$.
    (c) Используйте п. (a) для того, чтобы описать (или нарисовать) многообразие из п. (b).

§ 6. Свойства базисов Грёбнера

В § 5 мы показали, что каждый ненулевой идеал $I \subset k[x_1, \ldots, x_n]$ имеет базис Грёбнера. В этом параграфе мы рассмотрим свойства базисов Грёбнера и узнаем, как выяснить, является ли данный базис базисом Грёбнера или нет. Мы начнем с доказательства того факта, что нежелательные свойства алгоритма деления в $k[x_1, \ldots, x_n]$, указанные в § 3, не проявляются, если делители образуют базис Грёбнера.

Предложение 1. *Пусть $G = \{g_1, \ldots, g_s\}$ — базис Грёбнера идеала $I \subset k[x_1, \ldots, x_n]$, и пусть $f \in k[x_1, \ldots, x_n]$. Тогда существует единственный полином $r \in k[x_1, \ldots, x_n]$, который обладает следующими двумя свойствами:*

(i) *ни один член полинома r не делится ни на один из старших членов $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$;*
(ii) *существует $g \in I$, такой, что $f = g + r$.*

То есть r является остатком от деления f на G, не зависящим от порядка делителей в G.

Доказательство. Алгоритм деления позволяет записать f в виде $f = a_1 g_1 + \ldots + a_s g_s + r$, где r удовлетворяет условию (i). Условие (ii) также выполняется, так как $g = a_1 g_1 + \ldots + a_s g_s \in I$. Существование полинома r доказано.

Докажем единственность. Пусть $f = g + r = g' + r'$, где g, r, g', r' удовлетворяют условиям (i) и (ii). Тогда $r - r' = g - g' \in I$. Поэтому если $r \ne r'$, то $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Тогда по лемме 2 из § 4 $\mathrm{LT}(r - r')$ делится на какой-то старший член $\mathrm{LT}(g_i)$. Но это невозможно в силу условия (i). Значит, $r = r'$, и единственность доказана. □

Остаток r называется *нормальной формой* полинома f, и его единственность будет рассмотрена в упр. 1 и 4. Фактически базисы Грёбнера могут быть охарактеризованы требованием единственности остатка — см. теорему 5.35 в книге BECKER, WEISPFENNING (1993), где доказано это утверждение и найдены другие условия, эквивалентные тому, что множество G является базисом Грёбнера идеала I.

Хотя единственность остатка и имеет место, но «частные» a_i, вычисляемые алгоритмом деления $f = a_1g_1 + \ldots + a_sg_s + r$, зависят от порядка делителей даже в том случае, когда G — базис Грёбнера. См. пример в упр. 2.

Как следствие мы получаем такое условие принадлежности идеалу.

Следствие 2. *Пусть $G = \{g_1, \ldots, g_s\}$ — базис Грёбнера идеала $I \subset k[x_1, \ldots, x_n]$, и пусть $f \in k[x_1, \ldots, x_n]$. Тогда $f \in I$ в том и только том случае, когда остаток от деления полинома f на G равен нулю.*

Доказательство. Если остаток равен нулю, то, как уже отмечалось, $f \in I$. Обратно, пусть $f \in I$. Тогда равенство $f = f + 0$ удовлетворяет обоим условиям предложения 1. Из единственности представления полинома f в таком виде следует, что 0 является остатком от деления f на G. □

Свойство, сформулированное в следствии 2, иногда используется как определение базиса Грёбнера: можно доказать, что G обладает этим свойством в том и только том случае, когда является базисом Грёбнера (см. упр. 3). См. также предложение 5.38 в книге BECKER, WEISPFENNING (1993).

Следствие 2 позволяет построить алгоритм, решающий задачу о принадлежности идеалу из § 1 (однако *только* в том случае, когда мы знаем базис Грёбнера G идеала): нам нужно только найти остаток от деления на G. В § 7 мы узнаем, как строить базисы Грёбнера, и дадим полное решение задачи о принадлежности идеалу в § 8.

Введем следующее обозначение.

Определение 3. Остаток от деления полинома f на упорядоченный s-набор $F = (f_1, \ldots, f_s)$ будет обозначаться $\bar{f}^F$. Если F является базисом Грёбнера идеала $\langle f_1, \ldots, f_s \rangle$, то по предложению 1 его можно рассматривать как (неупорядоченное) множество.

Пусть, например, $F = (x^2y - y^2, x^4y^2 - y^2) \subset k[x, y]$ и используется lex-упорядочение. Тогда

$$\overline{x^5y}^F = xy^3,$$

потому что применение алгоритма деления дает

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Теперь мы обсудим, как определить, является данный базис идеала его базисом Грёбнера или нет. Как мы уже отмечали, «препятствием» к тому, чтобы набор $\{f_1, \ldots, f_s\}$ был базисом Грёбнера, является существование такой полиномиальной комбинации полиномов f_i, что ее старший член не принадлежит идеалу $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. Это может произойти, например, в том случае, когда в некоторой комбинации $ax^\alpha f_i - bx^\beta f_j$ старшие члены полиномов $ax^\alpha f_i$ и $bx^\beta f_j$ *сокращаются*. Но $ax^\alpha f_i - bx^\beta f_j \in I$, так что старший член этой комбинации принадлежит $\langle \mathrm{LT}(I) \rangle$. Проверьте, что именно это и происходит в примере 2 § 5. Для изучения сокращений мы определим специальные комбинации.

Определение 4. Пусть $f, g \in k[x_1, \ldots, x_n]$ — ненулевые полиномы.

(i) Пусть $\mathrm{multideg}(f) = \alpha$ и $\mathrm{multideg}(g) = \beta$. Положим $\gamma = (\gamma_1, \ldots, \gamma_n)$, $\gamma_i = \max(\alpha_i, \beta_i)$ для любого i. Тогда x^γ называется *наименьшим общим кратным* мономов $\mathrm{LM}(f)$ и $\mathrm{LM}(g)$. Используется обозначение $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$[1].

(ii) S-*полиномом* от f и g называется комбинация

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

(Заметим, что в знаменателе стоят не мономы, а старшие члены.)

Пусть, например, $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$, $f, g \in \mathbb{R}[x, y]$, и используется grlex-упорядочение. Тогда $\gamma = (4, 2)$ и

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

S-полином $S(f, g)$ специально «сконструирован» для сокращения старших членов. Фактически следующая лемма утверждает, что любое сокращение старших членов в комбинациях полиномов одинаковой мультистепени связано с сокращениями в S-полиномах.

Лемма 5. *Рассмотрим сумму $\sum_{i=1}^s c_if_i$, где $\mathrm{multideg}(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$, а $c_i \in k$ для всех i. Если $\mathrm{multideg}(\sum_{i=1}^s c_if_i) < \delta$, то*

[1] LCM — аббревиатура английского термина least common multiple.— *Прим. перев.*

$\sum_{i=1}^{s} c_i f_i$ *является линейной комбинацией с коэффициентами в* k S-*полиномов* $S(f_j, f_l)$, $1 \le j, l \le s$. *Более того, мультистепень каждого* $S(f_j, f_l)$ *меньше* δ.

Доказательство. Пусть $d_i = \mathrm{LC}(f_i)$, так что $c_i d_i$ является старшим коэффициентом полинома $c_i f_i$. Так как $c_i f_i$ имеет мультистепень δ и мультистепень суммы полиномов $c_i f_i$ меньше δ, то $\sum_{i=1}^{s} c_i d_i = 0$.

Пусть $p_i = f_i / d_i$; тогда старший коэффициент полинома p_i равен 1. Преобразуем рассматриваемую сумму:

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \ldots$$

$$+ (c_1 d_1 + \ldots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \ldots + c_s d_s) p_s.$$

Так как $\mathrm{LT}(f_i) = d_i x^\delta$, то $\mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_l)) = x^\delta$. Значит,

$$S(f_j, f_l) = \frac{x^\delta}{\mathrm{LT}(f_j)} f_j - \frac{x^\delta}{(\mathrm{LT}(f_l)} f_l = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_l x^\delta} f_l = p_j - p_l. \quad (1)$$

Используя это равенство и равенство $\sum_{i=1}^{s} c_i d_i = 0$, мы можем переписать сумму в виде

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \ldots$$

$$+ (c_1 d_1 + \ldots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s),$$

а это тот вид, который нам и нужен. Так как p_i и p_l имеют одинаковую мультистепень δ и одинаковые старшие коэффициенты — единицы, то разность $p_j - p_l$ имеет мультистепень $< \delta$. В силу (1) то же самое верно и относительно $S(f_j, f_l)$. Лемма доказана. □

Если $f_1, \ldots, f_s$ удовлетворяют условиям леммы 5, то

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,l} c_{jl} S(f_j, f_l).$$

Посмотрим, где именно происходит сокращение. В сумме слева каждое слагаемое $c_i f_i$ имеет мультистепень δ, т. е. сокращение получается в результате суммирования. С другой стороны, в сумме справа каждое слагаемое $c_{jl} S(f_j, f_l)$ имеет мультистепень $< \delta$, т. е. сокращение уже произошло. Интуитивно это означает, что S-полиномы как бы «ответственны» за все сокращения.

Используя S-полиномы и лемму 5 мы можем теперь доказать следующий критерий (принадлежащий Бухбергеру) того, что базис идеала является базисом Грёбнера.

Теорема 6. *Пусть* I *— некоторый полиномиальный идеал. Тогда базис* $G = \{g_1, \ldots, g_s\}$ *идеала* I *является базисом Грёбнера в том и только том случае, когда для всех пар* $i \ne j$ *остаток от деления* $S(g_i, g_j)$ *на* G *(в любом порядке) равен нулю.*

Доказательство. $\Rightarrow$. Пусть G является базисом Грёбнера. Тогда так как $S(g_i, g_j) \in I$, то остаток от деления $S(g_i, g_j)$ на G равен нулю в силу следствия 2.

$\Leftarrow$. Пусть $f \in I$ — ненулевой полином. Мы должны доказать, что если остатки от деления всех S-полиномов на G равны нулю, то $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Сначала наметим общую стратегию доказательства.

Так как $f \in I = \langle g_1, \ldots, g_s \rangle$, то существуют полиномы $h_i \in k[x_1, \ldots, x_n]$, такие, что

$$f = \sum_{i=1}^{s} h_i g_i. \quad (2)$$

Из леммы 8 § 2 следует, что

$$\mathrm{multideg}(f) \le \max(\mathrm{multideg}(h_i g_i)). \quad (3)$$

Если здесь нет равенства, то, следовательно, произошло сокращение старших членов в (2). Лемма 5 позволяет выразить это в терминах S-полиномов. Тогда наше условие, что S-полиномы имеют нулевые остатки от деления, позволяет заменить S-полиномы на выражения с меньшим числом сокращений, т. е. мы получим выражение для f с меньшим числом сокращаемых старших членов. Продолжая этот процесс, мы в конце концов получим выражение типа (2) для f, причем в (3) будет иметь место равенство. Тогда $\mathrm{multideg}(f) = \mathrm{multideg}(h_i g_i)$ для некоторого i, т. е. $\mathrm{LT}(f)$ делится на некоторый $\mathrm{LT}(g_i)$. Значит, $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, что и требуется доказать.

Приступим к подробному изложению доказательства. Рассмотрим (2). Пусть $m(i) = \mathrm{multideg}(h_i g_i)$, и положим $\delta = \max(m(1), \ldots, m(s))$. Теперь неравенство (3) имеет вид $\mathrm{multideg}(f) \le \delta$. Рассмотрим *все* способы, какими f может быть записано в виде (2). Для каждого такого способа мы будем иметь свое δ. Так как мономиальное упорядочение является вполне упорядочением, то мы можем выбрать такое выражение (2), для которого δ *минимально*.

Мы покажем, что если δ минимально, то $\mathrm{multideg}(f) = \delta$. Тогда в (3) равенство имеет место и, как мы видели выше, отсюда следует, что $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Это и докажет теорему.

Осталось доказать, что $\mathrm{multideg}(f) = \delta$. Мы докажем это от противного. Если равенство места не имеет, то $\mathrm{multideg}(f) < \delta$. Пере-

пишем (2) в следующем виде:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{4}$$

Мономы во второй и третьей суммах в самой правой части равенства имеют мультистепени $< \delta$. Поэтому предположение $\mathrm{multideg}(f) < \delta$ означает, что первая сумма также имеет мультистепень $< \delta$.

Если $\mathrm{LT}(h_i) = c_i x^{\alpha(i)}$, то сумма

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$$

имеет в точности тот вид, который описан в условии леммы 5 с $f_i = x^{\alpha(i)} g_i$. Теперь из леммы 5 следует, что эта сумма есть линейная комбинация S-полиномов $S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l)$. Но

$$\begin{aligned} S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l) &= \frac{x^\delta}{x^{\alpha(j)}\,\mathrm{LT}(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(l)}\,\mathrm{LT}(g_l)} x^{\alpha(l)} g_l \\ &= x^{\delta - \gamma_{jl}} S(g_j, g_l), \end{aligned}$$

где $x^{\gamma_{jl}} = \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_l))$. Значит, существуют константы $c_{jl} \in k$, такие, что

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,l} c_{jl} x^{\delta - \gamma_{jl}} S(g_j, g_l). \tag{5}$$

Теперь вспомним, что, согласно нашему предположению, остаток от деления $S(g_j, g_l)$ на $g_1, \ldots, g_s$ равен нулю, т. е. каждый S-полином может быть записан в виде

$$S(g_j, g_l) = \sum_{i=1}^{s} a_{ijl} g_i, \tag{6}$$

где $a_{ijl} \in k[x_1, \ldots, x_n]$. Из алгоритма деления также следует, что

$$\mathrm{multideg}(a_{ijl} g_i) \le \mathrm{multideg}(S(g_j, g_l)) \tag{7}$$

для всех i, j, l (см. теорему 3 из § 3). Значит, можно сказать, что если остаток равен нулю, то существует такое представление $S(g_j, g_l)$ в виде комбинации g_i, что старшие члены слагаемых этой комбинации не сокращаются.

Умножим теперь (6) на $x^{\delta - \gamma_{jl}}$ и получим

$$x^{\delta - \gamma_{jl}} S(g_j, g_l) = \sum_{i=1}^{s} b_{ijl} g_i,$$

где $b_{ijl} = x^{\delta - \gamma_{jl}} a_{ijl}$. Теперь из (7) и леммы 5 следует, что

$$\mathrm{multideg}(b_{ijl} g_i) \le \mathrm{multideg}(x^{\delta - \gamma_{jl}} S(g_j, g_l)) \le \delta. \tag{8}$$

Если мы подставим полученное нами выражение для $x^{\delta - \gamma_{jl}} S(g_j, g_l)$ в (5), то получим равенство

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,l} c_{jl} x^{\delta - \gamma_{jl}} S(g_j, j_l) = \sum_{j,l} c_{jl} \left(\sum_i b_{ijl} g_i \right) = \sum_i \tilde{h}_i g_i.$$

Но по (8) для всех i

$$\mathrm{multideg}(\tilde{h}_i g_i) < \delta.$$

Теперь, чтобы завершить доказательство, осталось подставить равенство $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_i \tilde{h}_i g_i$ в (4) и получить выражение для f в виде полиномиальной комбинации полиномов g_i, где *все* члены имеют мультистепень $< \delta$. Этот факт противоречит минимальности δ. Доказательство теоремы закончено. □

Теорема 6 называется также критерием Бухбергера S-пар и является одним из основных результатов в теории базисов Грёбнера. Мы знаем, что базисы Грёбнера обладают многими хорошими свойствами, однако до сих пор нам было трудно определить, является ли базис идеала его базисом Грёбнера (примеры, рассмотренные в § 5, достаточно тривиальны). Применение же критерия S-пар позволяет легко доказать, что данный базис является или не является базисом Грёбнера. Как мы увидим в § 7, этот критерий позволяет сконструировать естественный алгоритм построения базисов Грёбнера.

Рассмотрим в качестве примера идеал $I = \langle y - x^2, z - x^3 \rangle$ скрученной кубики в $\mathbb{R}^3$. Мы утверждаем, что $G = \{y - x^2, z - x^3\}$ является базисом Грёбнера для lex-упорядочения $y > z > x$. Чтобы доказать это, рассмотрим S-полином

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Алгоритм деления дает

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0,$$

т. е. $\overline{S(y - x^2, z - x^3)}^{G} = 0$. Отсюда, согласно теореме 6, следует, что G является базисом Грёбнера для I. Можно проверить, что G *не* является базисом Грёбнера для lex-упорядочения $x > y > z$ (см. упр. 8).

Упражнения к § 6

1. Докажите, что предложение 1 может быть несколько усилено следующим образом. Зафиксируем мономиальное упорядочение. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал и $f \in k[x_1, \ldots, x_n]$.
   (a) Докажите, что f может быть записан в виде $f = g + r$, где $g \in I$ и ни один член полинома r не делится ни на один элемент из $\mathrm{LT}(I)$.
   (b) Пусть $f = g + r = g' + r'$ — два представления f, удовлетворяющие условиям п. (a). Докажите, что $r = r'$, т. е. r определено однозначно.

   Этот результат показывает, что, как только мономиальное упорядочение зафиксировано, мы можем однозначно определить «остаток от деления f на I». Это наблюдение будет использовано нами в гл. 5.
2. В § 5 мы доказали, что $G = \{x + z, y - z\}$ является базисом Грёбнера для lex-упорядочения. Рассмотрим на примере этого базиса задачу об однозначности алгоритма деления.
   (a) Разделите xy на $x + z, y - z$.
   (b) Измените порядок и разделите xy на $y - z, x + z$.

   В обоих случаях вы получите один и тот же остаток (как и утверждает предложение 1), но «частные» будут разными. Это доказывает, что однозначная определенность остатка — это самое большее, на что можно рассчитывать.
3. В следствии 2 мы доказали, что если $I = \langle g_1, \ldots, g_s \rangle$ и $G = \{g_1, \ldots, g_s\}$ — базис Грёбнера, то $\bar{f}^G = 0$ для всех $f \in I$. Докажите обратное утверждение. А именно, докажите, что если G является базисом идеала I и $\bar{f}^G = 0$ для всех $f \in I$, то G — базис Грёбнера.
4. Пусть G и G' — базисы Грёбнера идеала I по отношению к одному и тому же мономиальному упорядочению в $k[x_1, \ldots, x_n]$. Докажите, что $\bar{f}^G = \bar{f}^{G'}$ для всех $f \in k[x_1, \ldots, x_n]$. Это означает, что остаток от деления не зависит от того, какой именно базис Грёбнера мы использовали в качестве делителя (при условии, что мономиальное упорядочение не меняется). Указание: воспользуйтесь упр. 1.
5. Вычислите $S(f, g)$, используя lex-упорядочение.
   (a) $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$.
   (b) $f = x^4y - z^2$, $g = 3xz^2 - y$.
   (c) $f = x^7y^2z + 2ixyz$, $g = 2x^7y^2z + 4$.
   (d) $f = xy + z^3$, $g = z^2 - 3z$.
6. Зависит ли $S(f, g)$ от используемого мономиального упорядочения? Приведите примеры.
7. Докажите, что $\mathrm{multideg}(S(f, g)) < \gamma$, где $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. Объясните, почему это неравенство является точной формулировкой утверждения, что S-полиномы сконструированы для того, чтобы осуществлять сокращение.
8. Докажите, что $\{y - x^2, z - x^3\}$ не является базисом Грёбнера для lex-упорядочения с $x > y > z$.

9. Применяя результат теоремы 6, определите, являются ли следующие множества G базисами Грёбнера для идеалов, которые они порождают. Вы можете использовать компьютерную систему для вычисления S-полиномов и остатков.
   (a) $G = \{x^2 - y, x^3 - z\}$, grlex-упорядочение.
   (b) $G = \{x^2 - y, x^3 - z\}$, invlex-упорядочение (см. упр. 6 § 2).
   (c) $G = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$, lex-упорядочение.
10. Пусть $f, g \in k[x_1, \ldots, x_n]$ — полиномы, такие, что $\mathrm{LM}(f)$ и $\mathrm{LM}(g)$ *взаимно просты* и $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$.
    (a) Докажите, что $S(f, g) = -(g - \mathrm{LT}(g))f + (f - \mathrm{LT}(f))g$.
    (b) Докажите, что в этом случае старший моном полинома $S(f, g)$ делится или на $\mathrm{LM}(f)$, или на $\mathrm{LM}(g)$.
11. Пусть $f, g \in k[x_1, \ldots, x_n]$, а x^α, x^β — мономы. Проверьте, что
$$S(x^\alpha f, x^\beta g) = x^\gamma S(f, g),$$
где
$$x^\gamma = \frac{\mathrm{LCM}(x^\alpha \mathrm{LM}(f), x^\beta \mathrm{LM}(g))}{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}.$$
Не забудьте доказать, что x^γ — моном.
12. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал, а G — его базис Грёбнера.
    (a) Докажите, что $\bar{f}^G = \bar{g}^G$ в том и только том случае, когда $f - g \in I$. Указание: воспользуйтесь упр. 1.
    (b) Докажите, что
$$\overline{f + g}^G = \bar{f}^G + \bar{g}^G.$$
Указание: примените п. (a).
    (c) Докажите, что
$$\overline{fg}^G = \overline{\bar{f}^G \cdot \bar{g}^G}^G.$$

Интересные следствия этих утверждений будут обсуждаться нами в гл. 5.

§ 7. Алгоритм Бухбергера

В следствии 6 § 5 доказано, что каждый ненулевой идеал в $k[x_1, \ldots, x_n]$ имеет базис Грёбнера. К сожалению, доказательство неконструктивно в том смысле, что оно не дает никаких указаний, как можно построить базис Грёбнера. В этом параграфе будет решаться следующая задача: как построить базис Грёбнера заданного идеала $I \subset k[x_1, \ldots, x_n]$? Сначала проиллюстрируем на примере основные идеи рассматриваемого здесь метода. Возьмем идеал из примера 2 § 5.

Пример 1. Рассмотрим кольцо $k[x, y]$ с grlex-упорядочением и идеал $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Напомним, что множество

$\{f_1, f_2\}$ не образует базиса Грёбнера для I, так как $\mathrm{LT}(S(f_1, f_2)) = -x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2)\rangle$.

Как же построить базис Грёбнера? Первая мысль, которая приходит в голову, — это расширить имеющийся базис идеала до базиса Грёбнера, добавляя полиномы из I. Может показаться, что эта процедура не вносит ничего нового и только создает избыточность. Однако информация, которую мы получим, зная базис Грёбнера, вполне компенсирует избыточность.

Какие же новые порождающие элементы надо добавить? Если мы вспомним, что говорилось об S-полиномах в предыдущем параграфе, то станет понятно, что надо добавлять S-полиномы от элементов базиса. Имеем $S(f_1, f_2) = -x^2 \in I$, и остаток от деления $-x^2$ на $F = \{f_1, f_2\}$ равен $-x^2 \neq 0$. Добавим остаток $f_3 = -x^2$ в порождающее множество. Теперь $F = \{f_1, f_2, f_3\}$, и мы можем применить теорему 6 и проверить, является ли F базисом Грёбнера для I. Имеем $S(f_1, f_2) = f_3$; значит,

$$\begin{aligned} \overline{S(f_1, f_2)}^F &= 0, \\ S(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy, \quad \text{но} \\ \overline{S(f_1, f_3)}^F &= -2xy \neq 0. \end{aligned}$$

Следовательно, мы должны добавить $f_4 = -2xy$ к порождающему множеству, т. е. $F = (f_1, f_2, f_3, f_4)$. Имеем

$$\begin{aligned} &\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0, \\ &S(f_1, f_4) = y(x^3 - 2xy) - (-1/2)x^2(-2xy) = -2xy^2 = yf_4, \end{aligned}$$

так что

$$\begin{aligned} \overline{S(f_1, f_4)}^F &= 0, \\ S(f_2, f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \\ \overline{S(f_2, f_3)}^F &= -2y^2 + x \neq 0, \end{aligned}$$

так что мы должны добавить $f_5 = -2y^2 + x$ к порождающему множеству, т. е. $F = (f_1, f_2, f_3, f_4, f_5)$. Легко убедиться, что

$$\overline{S(f_i, f_j)}^F = 0 \quad \text{для всех} \quad 1 \leq i < j \leq 5.$$

Теперь из теоремы 6 § 6 следует, что базис Грёбнера идеала I для grlex-упорядочения выглядит следующим образом:

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

Пример 1 подсказывает, что и в общем случае можно построить базис Грёбнера, расширяя какой-нибудь базис F путем последовательного добавления ненулевых остатков $\overline{S(f_i, f_j)}^F$ к F. Эта идея

естественно вытекает из критерия S-пар из § 6, и алгоритм Бухбергера, который мы сейчас начнем изучать, является реализацией этой идеи.

Теорема 2. *Пусть дан некоторый ненулевой полиномиальный идеал $I = \langle f_1, \ldots, f_s\rangle$. Тогда базис Грёбнера для I может быть построен за конечное число шагов с помощью следующего алгоритма:*

Вход: $F = (f_1, \ldots, f_s)$
Выход: базис Грёбнера $G = (g_1, \ldots, g_t)$ идеала I, где $F \subset G$
$G := F$
REPEAT
  $G' = G$
  FOR каждой пары $\{p, q\}, p \neq q$ в G' DO
    $S := \overline{S(p, q)}^{G'}$
    IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$

Доказательство. Сначала введем удобные обозначения. Если $G = \{g_1, \ldots, g_s\}$, то через $\langle G\rangle$ и $\langle \mathrm{LT}(G)\rangle$ будем обозначать следующие идеалы:

$$\begin{aligned} \langle G\rangle &= \langle g_1, \ldots, g_s\rangle, \\ \langle \mathrm{LT}(G)\rangle &= \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle. \end{aligned}$$

Теперь займемся доказательством. Докажем сначала, что условие $G \subset I$ выполняется на каждом шаге алгоритма. Это верно в начале работы алгоритма. Далее, при каждом расширении множества G мы добавляем остаток $S = \overline{S(p, q)}^{G'}$, где $p, q \in G$. Если $G \subset I$, то p, q и $S(p, q)$ принадлежат I. А так как мы делим на $G' \subset I$, то и остаток S принадлежит I; значит, $G \cup \{S\} \subset I$. Кроме того, G содержит исходный базис F, а следовательно, является базисом идеала I.

Алгоритм заканчивает работу, когда $G = G'$, т. е. когда $\overline{S(p, q)}^{G'} = 0$ для всех $p, q \in G$. Следовательно, G является базисом Грёбнера для $I = \langle G\rangle$ по теореме 6, § 6.

Осталось доказать, что алгоритм в какой-то момент останавливается. Посмотрим, что происходит во время каждого выполнения основного цикла. Множество G состоит из G' (старое G) и ненулевых остатков от деления S-полиномов от элементов из G' на G', т. е.

$$\langle \mathrm{LT}(G')\rangle \subset \langle \mathrm{LT}(G)\rangle, \tag{1}$$

так как $G' \subset G$. Мы утверждаем, что если $G' \neq G$, то $\langle \mathrm{LT}(G')\rangle$ строго меньше, чем $\langle \mathrm{LT}(G)\rangle$. Докажем это. Пусть ненулевой остаток r

от деления S-полинома на G' был добавлен к G. Тогда, так как r — остаток, $\mathrm{LT}(r)$ не делится ни на один старший член элемента из G', т. е. $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$. Однако $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$. Утверждение доказано.

По (1) идеалы $\langle \mathrm{LT}(G') \rangle$, получающиеся в результате последовательных выполнений основного цикла, образуют возрастающую цепь в $k[x_1, \ldots, x_n]$. Тогда условие обрыва возрастающих цепей (теорема 7 из § 5) утверждает, что эта цепь стабилизируется, т. е. условие $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ станет выполняться после конечного числа итераций основного цикла. Это означает в силу доказанного в предыдущем параграфе, что условие $G' = G$ станет выполняться и алгоритм остановится через конечное число шагов. □

Критерий S-пар (теорема 6 из § 6) и алгоритм Бухбергера (теорема 2) составляют основу алгоритмической теории базисов Грёбнера и являются ключевыми в этой области алгебры. В § 8 мы познакомимся с приложениями этих методов, а большая часть книги посвящена их развитию и применению.

Необходимо отметить, что алгоритм, описанный в теореме 2, является лишь упрощенной версией оригинального алгоритма Бухбергера. Мы рассмотрели именно эту версию, чтобы сделать основные идеи ясными для читателя, хотя она и мало пригодна в практических вычислениях. Обратите внимание (вот первое усовершенствование), что если остаток $\overline{S(p,q)}^{G'}$ равен нулю, то он будет нулем и при расширении множества G'. Поэтому нет смысла снова и снова вычислять этот остаток при итерациях цикла. На самом деле, так как мы добавляем новые порождающие элементы f_j по одному, то нам нужно только вычислять остатки $\overline{S(f_i, f_j)}^{G'}$ при $i < j$. Хорошим упражнением было бы усовершенствовать алгоритм так, чтобы учесть это замечание. Другие усовершенствования, более глубокие и важные, будут обсуждаться в § 9.

Базисы Грёбнера, построенные с помощью алгоритма теоремы 2, часто оказывается избыточными — бóльшими, чем необходимо. Мы можем исключить лишние образующие, используя следующий факт.

Лемма 3. *Пусть G — базис Грёбнера полиномиального идеала I, и пусть $p \in G, \mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. Тогда $G - \{p\}$ также является базисом Грёбнера для I.*

Доказательство. Мы знаем, что $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. Если $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$, то $\langle \mathrm{LT}(G - \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. Следовательно, $G - \{p\}$ является базисом Грёбнера по определению. □

Подберем константы и сделаем все старшие коэффициенты единицами, а также исключим из G все p, такие, что $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. В результате мы получим *минимальный* базис Грёбнера.

Определение 4. *Минимальным базисом Грёбнера* полиномиального идеала I называется его базис Грёбнера G, такой, что

(i) $\mathrm{LC}(p) = 1$ для всех $p \in G$;
(ii) $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\}) \rangle$ для всех $p \in G$.

Минимальный базис Грёбнера для данного ненулевого идеала можно построить с помощью алгоритма из теоремы 2 с последующим применением леммы 3 для исключения лишних образующих. В качестве примера рассмотрим идеал I из примера 1. Ранее мы нашли базис Грёбнера этого идеала для grlex-упорядочения:

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2y - 2y^2 + x \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

Так как некоторые старшие коэффициенты не равны 1, то на первом шаге мы делаем их единицами, умножая на подходящие константы. Теперь заметим, что $\mathrm{LT}(f_1) = x^3 = -x \cdot \mathrm{LT}(f_3)$. По лемме 3 полином f_1 нужно исключить. Аналогично, так как $\mathrm{LT}(f_2) = x^2y = -(1/2)x \cdot \mathrm{LT}(f_4)$, то f_2 также исключается. Старшие члены f_3, f_4, f_5 не образуют делящихся пар. Следовательно, полиномы

$$\tilde{f}_3 = x^2, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x$$

образуют минимальный базис Грёбнера для I.

К сожалению, идеал может иметь несколько минимальных базисов Грёбнера. Легко проверить, что для только что рассмотренного идеала I полиномы

$$\hat{f}_3 = x^2 + axy, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x \tag{2}$$

образуют минимальный базис Грёбнера при любом $a \in k$. Значит, мы нашли бесконечно много (если k бесконечно) минимальных базисов Грёбнера для I. К счастью, мы можем определить единственным образом наилучший минимальный базис Грёбнера.

Определение 5. *Редуцированным базисом Грёбнера* полиномиального идеала I называется его базис Грёбнера G, такой, что

(i) $\mathrm{LC}(p) = 1$ для всех $p \in G$;
(ii) никакой моном никакого $p \in G$ не принадлежит $\langle \mathrm{LT}(G - \{p\}) \rangle$.

Отметим, что среди базисов Грёбнера, заданных формулой (2), только один (при $a = 0$) является редуцированным. Редуцированные базисы обладают следующим полезным свойством.

Предложение 6. *Пусть $I \neq \{0\}$ — полиномиальный идеал, и пусть задано некоторое мономиальное упорядочение. Тогда существует единственный редуцированный базис Грёбнера идеала I.*

Доказательство. Пусть G — некоторый минимальный базис Грёбнера для I. Элемент $g \in G$ называется *редуцированным для G*, если никакой моном из g не принадлежит $\langle \mathrm{LT}(G - \{g\})\rangle$. Мы будем преобразовывать G до тех пор, пока все его элементы не станут редуцированными.

Отметим сначала, что если g редуцирован для G, то g редуцирован для любого другого минимального базиса Грёбнера (идеала I), содержащего g и имеющего то же множество старших членов. Это утверждение справедливо, так как определение редуцированности оперирует только старшими членами.

Пусть $g \in G$. Положим $g' = \bar{g}^{G-\{g\}}$ и $G' = (G - \{g\}) \cup \{g'\}$. Мы утверждаем, что G' также является минимальным базисом Грёбнера для I. Чтобы доказать это, отметим сначала, что $\mathrm{LT}(g') = \mathrm{LT}(g)$ (если мы поделим g на $G - \{g\}$, то $\mathrm{LT}(g)$ попадет в остаток, так как этот моном не делится ни на один элемент из $\mathrm{LT}(G - \{g\})$). Поэтому $\langle \mathrm{LT}(G')\rangle = \langle \mathrm{LT}(G)\rangle$. Так как $G' \subset I$, то G' — базис Грёбнера для I (минимальность очевидна). Наконец, g' редуцирован для G' по построению.

Преобразуем таким способом каждый элемент из G. Отметим теперь, что базис Грёбнера может измениться при каждом преобразовании, но как только элемент стал редуцированным, то он и останется таковым при дальнейших преобразованиях элементов из G (так как старший член не меняется). В конце концов мы получим редуцированный базис Грёбнера.

Теперь докажем единственность. Пусть G и $\widetilde{G}$ — редуцированные (а значит, и минимальные) базисы Грёбнера для I. В упражнении 7 будет доказано, что минимальные базисы идеала I имеют одно и то же множество старших членов:

$$\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G}).$$

Таким образом, для данного $g \in G$ найдется $\tilde{g} \in \widetilde{G}$, такой, что $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. Если мы докажем, что из этого следует равенство $g = \tilde{g}$, то тем самым и равенство $G = \widetilde{G}$, и единственность редуцированного базиса будут доказаны.

Рассмотрим разность $g - \tilde{g}$. Эта разность принадлежит I, а так как G — базис Грёбнера, то $\overline{g - \tilde{g}}^{G} = 0$. Но мы знаем также, что

$\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$; значит, старшие члены в $g - \tilde{g}$ сократились, а оставшиеся члены не делятся ни на один элемент из $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$, так как G и $\widetilde{G}$ редуцированные. Поэтому $\overline{g - \tilde{g}}^{G} = g - \tilde{g} = 0$. Доказательство завершено. □

Во многих системах компьютерной алгебры реализован алгоритм Бухбергера для вычисления базисов Грёбнера. Эти системы, как правило, находят базис, элементы которого отличаются от элементов редуцированного базиса постоянным множителем. Это означает, что базисы, вычисляемые разными системами, по существу совпадают. Таким образом, полученные результаты легко проверить, переходя от одной системы к другой.

Другим следствием единственности, доказанной в предложении 6, является то, что теперь у нас есть *алгоритм проверки равенства идеалов*. Пусть нам даны два множества $\{f_1, \ldots, f_s\}$ и $\{g_1, \ldots, g_t\}$. Как выяснить, порождают они разные идеалы или один и тот же? Ответ: задайте мономиальное упорядочение и вычислите редуцированные базисы Грёбнера для $\langle f_1, \ldots, f_s\rangle$ и $\langle g_1, \ldots, g_t\rangle$. Идеалы совпадают в том и только в том случае, когда совпадают редуцированные базисы.

В заключение кратко рассмотрим связь между алгоритмом Бухбергера и алгоритмом приведения матрицы к главному ступенчатому виду (по Гауссу). Интересно, что алгоритм приведения на самом деле является лишь частным случаем алгоритма, рассмотренного в этом параграфе. В качестве примера рассмотрим линейную систему

$$\begin{aligned} 3x - 6y - 2z &= 0,\\ 2x - 4y + 4w &= 0,\\ x - 2y - z - w &= 0. \end{aligned}$$

Элементарными преобразованиями строк мы приводим матрицу системы к ступенчатому виду

$$\begin{pmatrix} 1 & -2 & -1 & -1\\ 0 & 0 & 1 & 3\\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{3}$$

а затем к главному ступенчатому виду

$$\begin{pmatrix} 1 & -2 & 0 & 2\\ 0 & 0 & 1 & 3\\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{4}$$

Теперь опишем эти преобразования на алгебраическом языке. Рассмотрим идеал

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w\rangle \subset k[x, y, z, w],$$

который соответствует исходной системе. Будем использовать lex-упорядочение с $x > y > z > w$. В упражнениях будет доказано, что линейные формы, определенные матрицей (3), задают минимальный базис Грёбнера:

$$I = \langle x - 2y - z - w, z + 3w \rangle,$$

а матрица (4) определяет редуцированный базис:

$$I = \langle x - 2y + 2w, z + 3w \rangle.$$

В курсе линейной алгебры доказывается, что главный ступенчатый вид матрицы определен однозначно. Этот факт можно рассматривать как частный случай утверждения о единственности редуцированного базиса Грёбнера.

В упражнениях мы также проанализируем связь между алгоритмом Бухбергера и алгоритмом Евклида вычисления образующего элемента идеала $\langle f, g \rangle \subset k[x]$.

Упражнения к § 7

1. В примере 1 проверьте, что $\overline{S(f_i, f_j)}^F = 0$ для всех пар $1 \le i < j \le 5$.
2. Примените алгоритм теоремы 2 для вычисления базисов Грёбнера следующих идеалов. Если хотите, воспользуйтесь компьютерной системой для вычисления S-полиномов и остатков. Сначала используйте lex-, а затем grlex-упорядочение и сравните результаты.
   (a) $I = \langle x^2 y - 1, xy^2 - x \rangle$.
   (b) $I = \langle x^2 + y, x^4 + 2x^2 y + y^2 + 3 \rangle$. (Что можно сказать о многообразии $\mathbf{V}(I)$?)
   (c) $I = \langle x - z^4, y - z^5 \rangle$.
3. Найдите редуцированные базисы Грёбнера идеалов из упр. 2 по отношению к lex- и grlex-упорядочениям.
4. Примените результат упр. 7 из § 4 и дайте другое доказательство того, что алгоритм Бухбергера останавливается после конечного числа шагов.
5. Пусть G — базис Грёбнера идеала I и $\mathrm{LC}(g) = 1$ для всех $g \in G$. Докажите, что G является минимальным базисом в том и только том случае, когда никакое собственное подмножество множества G не является базисом Грёбнера.
6. В упр. 8 § 4 было введено понятие *минимального* базиса мономиального идеала. Докажите, что базис Грёбнера G идеала I минимален в том и только том случае, когда $\mathrm{LC}(g) = 1$ для всех $g \in G$ и $\mathrm{LT}(G)$ является минимальным базисом мономиального идеала $\langle \mathrm{LT}(I) \rangle$.
7. Пусть задано некоторое мономиальное упорядочение, и пусть G и $\widetilde{G}$ — минимальные базисы Грёбнера идеала I.

   (a) Докажите, что $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$.
   (b) Выведите отсюда, что G и $\widetilde{G}$ имеют одинаковое количество элементов.
8. Придумайте алгоритм, который вычисляет редуцированный базис Грёбнера (определение 5) идеала I по заданному базису Грёбнера. Докажите корректность алгоритма.
9. В тексте параграфа рассматривался идеал

   $$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle \subset k[x, y, z, w].$$

   Пусть задано lex-упорядочение $x > y > z > w$.
   (a) Докажите, что линейные полиномы, определенные ступенчатой матрицей (3), образуют минимальный базис Грёбнера: $I = \langle x - 2y - z - w, z + 3w \rangle$. Указание: примените результат теоремы 6 § 6.
   (b) Докажите, что линейные полиномы, определенные главной ступенчатой матрицей (4), образуют редуцированный базис Грёбнера, $I = \langle x - 2y + 2w, z + 3w \rangle$.
10. Рассмотрим $n \times m$-матрицу $A = (a_{ij})$ с элементами из k, и пусть $f_i = a_{i1}x_1 + \ldots + a_{im}x_m$ — линейные полиномы из $k[x_1, \ldots, x_m]$, определенные строками матрицы A. Рассмотрим идеал $I = \langle f_1, \ldots, f_n \rangle$. Мы будем использовать lex-упорядочение с $x_1 > \ldots > x_m$. Пусть $B = (b_{ij})$ — главная ступенчатая матрица для A, а $g_1, \ldots, g_s$ — линейные полиномы, определенные ненулевыми строками матрицы B ($s \le n$). Наша цель — доказать, что полиномы $g_1, \ldots, g_s$ образуют редуцированный базис Грёбнера для I.
    (a) Докажите, что $I = \langle g_1, \ldots, g_s \rangle$. Указание: докажите, что любое элементарное преобразование строк матрицы A даст нам матрицу, строки которой порождают тот же идеал.
    (b) Используя теорему 6 § 6, докажите, что $g_1, \ldots, g_s$ образуют базис Грёбнера I. Указание: если главная единица в i-й строке матрицы B находится на t-м месте, то $g_i = x_t + C$, где линейный полином C не содержит переменных, соответствующих главным столбцам. Аналогично, пусть $g_j = x_l + D$. Нам нужно поделить $S(g_i, g_j) = x_l C - x_t D$ на $g_1, \ldots, g_s$. Теперь заметьте, что процесс деления использует только g_i и g_j.
    (c) Объясните, почему $g_1, \ldots, g_s$ образуют редуцированный базис Грёбнера.
11. Докажите, что применение алгоритма Евклида к полиномам $f, g \in k[x]$ дает в результате редуцированный базис Грёбнера идеала $\langle f, g \rangle$ (после деления на константу, чтобы сделать старший коэффициент равным 1). Покажите, что шаги алгоритма Евклида могут рассматриваться как частные случаи процедур, используемых в алгоритме Бухбергера.

§ 8. Первые применения базисов Грёбнера

В § 1 мы сформулировали четыре задачи об идеалах и многообразиях. Первая из этих задач — задача описания идеала, была решена в § 5 с помощью теоремы Гильберта о базисе. Здесь мы рассмотрим, как базисы Грёбнера могут помочь нам при решении трех оставшихся задач.

Задача о принадлежности идеалу

Одновременное использование базисов Грёбнера и алгоритма деления дает следующий *алгоритм решения задачи о принадлежности идеалу*: пусть даны идеал $I = \langle f_1, \dots, f_s \rangle$ и полином f; надо выяснить, принадлежит f идеалу I или нет. Сначала, применяя алгоритм теоремы 2 § 7 (или аналогичный), находим базис Грёбнера $G = \{g_1, \dots, g_t\}$ для I. Тогда по следствию 2 § 6

$$f \in I \quad \text{в том и только том случае, когда} \quad \bar{f}^G = 0.$$

Пример 1. Пусть $I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^2 \rangle \subset \mathbb{C}[x, y, z]$, и пусть используется grlex-упорядочение. Рассмотрим полином $f = -4x^2y^2z^2 + y^6 + 3z^5$. Верно ли, что $f \in I$?

Множество образующих не является базисом Грёбнера, потому что $\mathrm{LT}(I)$ содержит, например, полином $\mathrm{LT}(S(f_1, f_2)) = \mathrm{LT}(-x^2y^2 + z^3) = x^2y^2$, который не принадлежит идеалу $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = \langle xz, x^3 \rangle$. Следовательно, на первом шаге необходимо найти базис Грёбнера G для I. Используя компьютерную систему, получаем

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = 0 \cdot f_1 + 0 \cdot f_2 - 4z^2 f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Так как остаток от деления равен нулю, то $f \in I$.

В качестве другого примера возьмем $f = xy - 5z^2 + x$. Здесь можно даже не проводить процесс деления — очевидно, что $f \notin I$. Причина состоит в том, что $\mathrm{LT}(f) = xy$ не принадлежит идеалу $\langle \mathrm{LT}(G) \rangle = \langle xz, x^3, x^2y^2, xy^4, y^6 \rangle$, т. е. $\bar{f}^G \neq 0$, так что $f \notin I$.

Последнее наблюдение иллюстрирует, как форма элементов базиса Грёбнера отражает свойства идеала.

Решение полиномиальных уравнений

Техника базисов Грёбнера может быть применена для решения систем полиномиальных уравнений. Сначала рассмотрим несколько примеров.

Пример 2. Рассмотрим систему уравнений

$$\begin{aligned} x^2 + y^2 + z^2 &= 1, \\ x^2 + z^2 &= y, \\ x &= z \end{aligned} \tag{1}$$

в $\mathbb{C}^3$. Эти уравнения задают идеал $I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subset \mathbb{C}[x, y, z]$. Наша задача — найти все точки многообразия $\mathbf{V}(I)$. Из предложения 9 § 5 следует, что мы можем сделать это, используя *любой* базис идеала I. Посмотрим, что получится, если мы будем работать с базисом Грёбнера.

Хотя это и не обязательно, мы будем использовать lex-упорядочение. Базис Грёбнера по отношению к этому упорядочению состоит из следующих элементов:

$$\begin{aligned} g_1 &= x - z, \\ g_2 &= -y + 2z^2, \\ g_3 &= z^4 + (1/2)z^2 - 1/4. \end{aligned}$$

Если мы внимательно посмотрим на эти полиномы, то увидим нечто замечательное. Во-первых, g_3 зависит только от z и его корни легко вычисляются (они являются корнями биквадратного уравнения):

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1},$$

что дает нам четыре возможных значения z. Далее, подставляя каждое из этих значений в уравнения $g_1 = 0$ и в $g_2 = 0$, мы однозначно определяем x и y. Таким образом, система $g_1 = g_2 = g_3 = 0$ имеет четыре решения, два вещественных и два комплексных. Так как $\mathbf{V}(I) = \mathbf{V}(g_1, g_2, g_3)$ (предложение 9 § 5), то тем самым мы нашли *все* решения системы (1).

Пример 3. Рассмотрим теперь полиномиальную систему (2) из § 2 гл. 1

$$\begin{aligned} 3x^2 + 2yz - 2\lambda x &= 0, \\ 2xz - 2\lambda y &= 0, \\ 2xy - 2z - 2\lambda z &= 0, \\ x^2 + y^2 + z^2 - 1 &= 0. \end{aligned}$$

Эта система была получена при применении метода множителей Лагранжа для нахождения экстремума функции $x^3 + 2xyz - z^2$ при условии $x^2 + y^2 + z^2 = 1$. Мы используем уже испытанную выше технику и сначала находим базис Грёбнера идеала, порожденного левыми частями четырех уравнений системы. Этот идеал принадлежит $\mathbb{R}[x, y, z, \lambda]$. Используется lex-упорядочение с $\lambda > x > y > z$.

Базис Грёбнера состоит из следующих элементов:

$$
\begin{aligned}
&\lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 - \frac{36717}{590}z^4 - \frac{134419}{7670}z^2,\\
&x^2 + y^2 + z^2 - 1,\\
&xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z,\\
&xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z,\\
&y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z,\\
&y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z,\\
&yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2,\\
&z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z.
\end{aligned}
\tag{2}
$$

На первый взгляд этот набор полиномов выглядит чудовищно. (Коэффициенты элементов базиса Грёбнера могут быть гораздо сложнее, чем коэффициенты элементов исходного базиса.) Однако мы видим, что последний полином зависит только от z. Мы «исключили» другие переменные в процессе вычисления базиса Грёбнера. Волшебным образом этот последний полином имеет совсем простые корни

$$z = 0, \quad \pm 1, \quad \pm 2/3, \quad \pm\sqrt{11}/8\sqrt{2}.$$

Последовательно подставляя эти значения в оставшиеся уравнения, мы можем решить их относительно x и z (и относительно λ также, хотя значения λ нам не нужны). Итак, мы получаем следующий список решений:

$$
\begin{aligned}
&z = 0; \quad y = 0; \quad x = \pm 1.\\
&z = 0; \quad y = \pm 1; \quad x = 0.\\
&z = \pm 1; \quad y = 0; \quad x = 0.\\
&z = 2/3; \quad y = 1/3; \quad x = -2/3.\\
&z = -2/3; \quad y = -1/3; \quad x = -2/3.\\
&z = \sqrt{11}/8\sqrt{2}; \quad y = -3\sqrt{11}/8\sqrt{2}; \quad x = -3/8.\\
&z = -\sqrt{11}/8\sqrt{2}; \quad y = 3\sqrt{11}/8\sqrt{2}; \quad x = -3/8.
\end{aligned}
$$

Теперь легко найти минимальное и максимальное значение функции.

Примеры 2 и 3 показывают, что вычисление базиса Грёбнера по отношению к lex-упорядочению существенно упрощает форму уравнений. В частности, мы получаем уравнения с последовательно исключенными переменными. Следует отметить, что *порядок* исключения соответствует порядку переменных. В примере 3, например, переменные упорядочены так: $\lambda > x > y > z$, и, если взглянуть на базис Грёбнера (2), то можно увидеть, что переменная λ исключается первой, x — второй и т. д.

Системы такого вида легко решаются, особенно если последнее уравнение зависит только от одной переменной. Мы можем использовать технику вычисления корней полиномов от одной переменной, а затем подставлять найденные корни в другие уравнения системы и решать их относительно других переменных (как в примерах 2 и 3). Читателю следует обратить внимание на сходство между этой процедурой решения полиномиальных систем и методом «обратной подстановки» для решения линейных систем с треугольной матрицей.

Исключение переменных при решении полиномиальных систем будет подробно изучаться в гл. 3. В частности, мы увидим, почему lex-упорядочение приводит к базису Грёбнера с последовательно исключенными переменными.

Задача нахождения неявного представления

Пусть параметрические уравнения

$$
\begin{aligned}
x_1 &= f_1(t_1, \ldots, t_m),\\
&\vdots\\
x_n &= f_n(t_1, \ldots, t_m)
\end{aligned}
\tag{3}
$$

определяют подмножество аффинного многообразия $V \subset k^n$. [1] Как будет показано в гл. 3, это именно так и происходит, если f_i являются рациональными функциями от $t_1, \ldots, t_m$. Как найти полиномиальные уравнения от x_i, которые задают V? Эта задача также может быть решена с использованием базисов Грёбнера, хотя полное доказательство будет дано только в гл. 3.

Для простоты мы ограничимся случаем, когда f_i являются *полиномами*. Рассмотрим аффинное многообразие в k^{m+n}, опреде-

[1] Поскольку само пространство k^n тоже является аффинным многообразием, смысл этого предложения нуждается в уточнении (ср. определение 1 в § 3 гл. 1). Читатель найдет его в гл. 3.— *Прим. ред.*

ленное уравнениями (3), или

$$\begin{aligned} x_1 - f_1(t_1, \ldots, t_m) &= 0, \\ &\vdots \\ x_n - f_n(t_1, \ldots, t_m) &= 0. \end{aligned}$$

Теперь мы должны исключить $t_1, \ldots, t_m$ из этих уравнений, что и даст нам уравнения для V.

Примеры 2 и 3 подсказывают нам, что разумно использовать базис Грёбнера для исключения переменных. Мы будем использовать lex-упорядочение в $k[t_1, \ldots, t_m, x_1, \ldots, x_n]$, заданное следующим порядком переменных:

$$t_1 > \ldots > t_m > x_1 > \ldots > x_n.$$

Теперь предположим, что мы знаем базис Грёбнера идеала $\widetilde{I} = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$. Так как мы используем lex-упорядочение, то можно ожидать, что базис Грёбнера содержит полиномы с исключенными переменными, причем $t_1, \ldots, t_m$ исключаются первыми, так как они являются наибольшими переменными в нашем мономиальном упорядочении. Таким образом, базис Грёбнера для $\widetilde{I}$ должен содержать полиномы, зависящие только от $x_1, \ldots, x_n$. Эти полиномы и будут определять V.

Описанная выше схема будет детально проанализирована в гл. 3, посвященной теории исключения. А теперь рассмотрим на примерах, как работает этот метод.

Пример 4. Рассмотрим параметрическую кривую V, заданную уравнениями

$$\begin{aligned} x &= t^4, \\ y &= t^3, \\ z &= t^2 \end{aligned}$$

в $\mathbb{C}^3$. Вычислим базис Грёбнера G идеала $I = \langle t^4 - x, t^3 - y, t^2 - z \rangle$ по отношению к lex-упорядочению в $\mathbb{C}[t, x, y, z]$. Имеем

$$G = \{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}.$$

Последние два полинома зависят только от x, y, z; следовательно, они определяют аффинное многообразие в $\mathbb{C}^3$, содержащее нашу кривую V. Размерностная интуиция, о которой говорилось в гл. 1, позволяет предположить, что эти два уравнения определяют кривую в $\mathbb{C}^3$ (одномерное многообразие). Теперь осталось ответить на вопрос, совпадает ли V с пересечением двух поверхностей

$$x - z^2 = 0, \quad y^2 - z^3 = 0.$$

Не может ли это пересечение содержать и другие кривые (или даже поверхности)? Общие результаты гл. 3 позволяют утверждать, что ответ отрицательный.

Пример 5. Рассмотрим теперь касательную поверхность скрученной кубики в $\mathbb{R}^3$, определенную в гл. 1. Эта поверхность задана следующими параметрическими уравнениями:

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned}$$

Базис Грёбнера соответствующего идеала по отношению к lex-упорядочению $t > u > x > y > z$ содержит 6 полиномов. Только один из них не зависит от t и u:

$$-(4/3)x^3z + x^2y^2 + 2xyz - (4/3)y^3 - (1/3)z^2 = 0. \tag{4}$$

Аффинное многообразие, определенное этим уравнением, содержит касательную поверхность скрученной кубики. Возможно, однако, что поверхность, заданная уравнением (4), строго больше, чем эта касательная поверхность, т. е. могут существовать решения уравнения (4), не принадлежащие этой касательной поверхности. Мы вернемся к этому примеру в гл. 3.

Подведем итоги. Мы выяснили, что применение базисов Грёбнера и алгоритма деления полностью решает задачу принадлежности идеалу. Более того, мы увидели, как можно решать системы полиномиальных уравнений и как находить уравнения параметрически заданных подмножеств аффинного пространства. Наш успех в рассмотренных примерах зависел от того, что базисы Грёбнера в случае lex-упорядочения, похоже, очень удачно исключают переменные. В гл. 3 мы докажем, что это действительно всегда так, а также рассмотрим другие аспекты того, что называется теорией исключения.

Упражнения к § 8

Во всех следующих упражнениях необходимо использовать систему компьютерной алгебры для вычислений (вручную большинство вычислений проделать весьма трудно).

1. Определите, принадлежит ли полином $f = xy^3 - z^2 + y^5 - z^3$ идеалу $I = \langle -x^3 + y, x^2y - z \rangle$.
2. Сделайте то же самое для $f = x^3z - 2y^2$ и $I = \langle xz - y, xy + 2z^2, y - z \rangle$.

3. Используя методы примеров 2 и 3, найдите точки в $\mathbb{C}^3$, принадлежащие многообразию

$$\mathbf{V}(x^2+y^2+z^2-1, x^2+y^2+z^2-2x, 2x-3y-z).$$

4. Сделайте то же самое для многообразия $\mathbf{V}(x^2y-z^3, 2xy-4z-1, z-y^2, x^3-4zy)$.

5. Напомним, что в математическом анализе *особой точкой* дифференцируемой функции $f(x,y)$ называется точка, в которой обе частные производные $\frac{\partial f}{\partial x}$ и $\frac{\partial f}{\partial y}$ обращаются в нуль одновременно. Если $f \in \mathbb{R}[x,y]$, то особые точки можно найти, используя нашу технику для решения полиномиальной системы

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

В качестве примера рассмотрим функцию

$$f(x,y) = (x^2+y^2-4)(x^2+y^2-1) + (x-3/2)^2 + (y-3/2)^2.$$

(a) Найдите все особые точки функции $f(x,y)$.
(b) Определите, какие из них являются локальными максимумами, какие — минимумами, а какие — седлами. Указание: используйте вторую производную.

6. Восстановите детали рассуждения, пропущенные в примере 5. В частности, найдите базис Грёбнера и проверьте, что он дает (с точностью до постоянного множителя) полином из левой части равенства (4).

7. Рассмотрим поверхность S в $\mathbb{R}^3$, которая является *объединением* прямых линий, соединяющих пары точек на прямых

$$\left\{\begin{matrix} x=t \\ y=0 \\ z=1 \end{matrix}\right\}, \quad \left\{\begin{matrix} x=0 \\ y=1 \\ z=t \end{matrix}\right\}$$

с *одним и тем же значением параметра* (т. е. t). (S относится к классу поверхностей, называемых *линейчатыми*.)

(a) Докажите, что S имеет следующее параметрическое представление:

$$\begin{aligned} x &= ut, \\ y &= 1-u, \\ z &= u+t-ut. \end{aligned}$$

(b) Применяя методы примеров 4 и 5, найдите (неявное) уравнение поверхности V, содержащей S.
(c) Докажите, что $V = S$ (т. е. докажите, что любая точка из V описывается формулами п. (a) при подходящих значения t и u). Указание: попытайтесь *разрешить* уравнение, задающее V, относительно одной из переменных.

8. Иногда параметрические кривые и поверхности являются алгебраическими многообразиями, хотя их параметрическое задание использует трансцендентные функции, такие, как sin или cos. В этой задаче надо доказать, что параметрическая поверхность T, заданная уравнениями

$$\begin{aligned} x &= (2+\cos t)\cos u, \\ y &= (2+\cos t)\sin u, \\ z &= \sin t \end{aligned}$$

принадлежит некоторому аффинному многообразию в $\mathbb{R}^3$.

(a) Нарисуйте T. Указание: используйте цилиндрические координаты.
(b) Положите $a=\cos t, b=\sin t, c=\cos u, d=\sin u$ и перепишите уравнения поверхности в переменных a,b,c,d,x,y,z.
(c) Пары переменных a,b и c,d не являются *независимыми*, так как выполняются полиномиальные тождества (основные тригонометрические тождества)

$$a^2+b^2-1=0, \quad c^2+d^2-1=0.$$

Составьте систему из пяти уравнений, присоединяя уравнения-тождества к трем уравнениям, полученным в п. (b). Найдите базис Грёбнера соответствующего идеала, используя lex-упорядочение с

$$a > b > c > d > x > y > z.$$

В найденном базисе должен быть один полином, который зависит только от x,y,z. Он и задает многообразие, содержащее T.

9. Рассмотрим параметрическую кривую $K \subset \mathbb{R}^3$, заданную следующими уравнениями:

$$\begin{aligned} x &= (2+\cos 2s)\cos 3s, \\ y &= (2+\cos 2s)\sin 3s, \\ z &= \sin 2s. \end{aligned}$$

(a) Перепишите уравнения кривой K как полиномиальные уравнения в переменных $x,y,z,a=\cos s, b=\sin s$. Указание: используйте тригонометрические тождества.
(b) Найдите базис Грёбнера идеала, порожденного уравнениями п. (a) и полиномом a^2+b^2-1 (как в упр. 8), и докажите, что K является подмножеством аффинной алгебраической кривой. Найдите неявные уравнения кривой, содержащей K.
(c) Докажите, что уравнение поверхности из упр. 8 *принадлежит* идеалу, определенному в п. (b). Какова геометрическая интерпретация этого факта? (На самом деле можно понять это сразу, сравнив параметрические уравнения для T и K.)

10. Примените метод множителей Лагранжа и найдите точку s на поверхности $x^4+y^2+z^2-1=0$, ближайшую к точке $(1,1,1)$ в $\mathbb{R}^3$.

Указание: надо действовать, как в примере 3. (Возможно, вам придется *численно* решать полученные уравнения.)

11. Пусть числа a, b, c удовлетворяют следующим уравнениям:

$$a+b+c=3$$
$$a^2+b^2+c^2=5$$
$$a^3+b^3+c^3=7.$$

(a) Докажите, что $a^4+b^4+c^4=9$. Указание: рассматривая a, b, c как переменные, докажите, что $a^4+b^4+c^4-9 \in \langle a+b+c-3, a^2+b^2+c^2-5, a^3+b^3+c^3-7\rangle$.

(b) Докажите, что $a^5+b^5+c^5 \neq 11$.

(c) Чему равны суммы $a^5+b^5+c^5$ и $a^6+b^6+c^6$? Указание: вычислите остатки[1)].

§ 9. Дополнение. Усовершенствования алгоритма Бухбергера

При разработке математического обеспечения следует обращать внимание не только на *корректность* используемых алгоритмов, но и на их *эффективность*. В этом параграфе мы обсудим усовершенствования алгоритма Бухбергера. Эти усовершенствования позволяют значительно ускорить процесс вычисления базисов Грёбнера. Некоторые из них реализованы в системах компьютерной алгебры. В конце параграфа мы вкратце рассмотрим задачу о сложности алгоритма Бухбергера. Хотя эта задача активно исследуется, окончательных результатов пока не получено.

Первая группа изменений алгоритма имеет отношение к теореме 6 § 6 о том, что базис идеала G является базисом Грёбнера, если $\overline{S(f,g)}^G = 0$ для всех $f, g \in G$. В § 7 показано, что именно этот результат является «ядром» алгоритма Бухбергера. Следовательно, один из способов улучшить алгоритм — это уменьшить количество рассматриваемых S-полиномов $S(f,g)$. Выполненные вручную примеры показали нам, что деление — необходимая процедура при анализе S-полинома — это наиболее трудоемкая в вычислительном отношении часть алгоритма. Поэтому желательно уменьшить количество делений.

Чтобы понять, какие S-полиномы могут не рассматриваться, нам сначала нужно понять, что это значит — иметь нулевой остаток от деления.

[1)] Читателю стоит вернуться к этому упражнению после прочтения гл. 7, заметив, что $a^n+b^n+c^n$ является симметрическим полиномом от a, b, c для любого n. — *Прим. ред.*

Определение 1. Пусть задано мономиальное упорядочение и множество $G = \{g_1, \ldots, g_s\} \subset k[x_1, \ldots, x_n]$. Функция $f \in k[x_1, \ldots, x_n]$ называется *редуцируемой к нулю по модулю* G (запись $f \to_G 0$), если f может быть представлена в виде

$$f = a_1 g_1 + \cdots + a_s g_s,$$

причем $\operatorname{multideg}(f) \geq \operatorname{multideg}(a_i g_i)$, если $a_i g_i \neq 0$.

Следующая лемма проясняет связь между определением 1 и алгоритмом деления.

Лемма 2. *Пусть $G = (g_1, \ldots, g_s)$ — упорядоченное множество элементов из $k[x_1, \ldots, x_n]$, и пусть дана функция $f \in k[x_1, \ldots, x_n]$. Тогда если $\bar{f}^G = 0$, то $f \to_G 0$, хотя обратное, как правило, неверно:*

Доказательство. Если $\bar{f}^G = 0$, то из алгоритма деления следует, что

$$f = a_1 g_1 + \ldots + a_s g_s + 0,$$

и по теореме 3 § 3

$$\operatorname{multideg}(f) \geq \operatorname{multideg}(a_i g_i),$$

если $a_i g_i \neq 0$, т. е. $f \to_G 0$. Чтобы показать, что обратное утверждение не всегда выполняется, снова рассмотрим пример 5 из § 3. Если мы поделим $f = xy^2 - x$ на $G = (xy+1, y^2-1)$, то получим

$$xy^2 - x = y \cdot (xy+1) + 0 \cdot (y^2-1) + (-x-y),$$

так что $\bar{f}^G = -x - y \neq 0$. С другой стороны,

$$xy^2 - x = 0 \cdot (xy+1) + x \cdot (y^2-1),$$

а так как

$$\operatorname{multideg}(xy^2 - x) \geq \operatorname{multideg}(x \cdot (y^2-1))$$

(на самом деле эти мультистепени равны), то $f \to_G 0$. □

Теперь, используя определение 1, дадим более общую формулировку критерия из теоремы 6 § 6.

Теорема 3. *Базис $G = \{g_1, \ldots, g_s\}$ идеала I является базисом Грёбнера в том и только том случае, когда $S(g_i, g_j) \to_G 0$ для всех $i \neq j$.*

Доказательство. Напомним, что в теореме 6 § 6 условие формулировалось так: $\overline{S(g_i, g_j)}^G = 0$ для всех $i \neq j$. Но если мы внимательно проанализируем ее доказательство, то увидим, что мы использовали только следующее свойство S-полиномов:

$$S(g_j, g_l) = \sum_{i=1}^{s} a_{ijl} g_i,$$

где

$$\operatorname{multideg}(a_{ijl}g_i) \le \operatorname{multideg}(S(g_j, g_l))$$

(см. формулы (6) и (7) из § 6). Но это в точности означает, что $S(g_j, g_l) \to_G 0$. Теорема доказана. □

Из леммы 2 следует, что теорема 6 из § 6 является частным случаем теоремы 3. Чтобы использовать теорему 3 для усовершенствования алгоритма, нам надо убедиться, что некоторые S-полиномы «автоматически» редуцируемы к нулю.

Предложение 4. *Пусть дано конечное множество* $G \subset k[x_1, \dots, x_n]$, *и пусть* $f, g \in G$ *таковы, что*

$$\operatorname{LCM}(\operatorname{LM}(f), \operatorname{LM}(g)) = \operatorname{LM}(f) \cdot \operatorname{LM}(g),$$

т. е. старшие мономы полиномов f *и* g *взаимно просты. Тогда* $S(f, g) \to_G 0$.

Доказательство. Предположим для простоты, что $\operatorname{LC}(f) = \operatorname{LC}(g) = 1$. Тогда $f = \operatorname{LM}(f) + p$, $g = \operatorname{LM}(g) + q$. Из условия предложения следует, что

$$\begin{aligned} S(f, g) &= \operatorname{LM}(g) \cdot f - \operatorname{LM}(f) \cdot g \\ &= (g - q) \cdot f - (f - p) \cdot g \\ &= g \cdot f - q \cdot f - f \cdot g + p \cdot g \\ &= p \cdot g - q \cdot f. \end{aligned} \tag{1}$$

Мы утверждаем, что

$$\operatorname{multideg}(S(f, g)) = \max(\operatorname{multideg}(p \cdot g), \operatorname{multideg}(q \cdot f)). \tag{2}$$

Из (1) и (2) следует, что $S(f, g) \to_G 0$. Докажем (2). Для этого заметим, что в полиноме $p \cdot g - q \cdot f$ из (1) старшие мономы полиномов $p \cdot g$ и $q \cdot f$ различны и, следовательно, не могут сократиться. Действительно, если бы они были одинаковыми, то выполнялось бы равенство

$$\operatorname{LM}(p) \cdot \operatorname{LM}(g) = \operatorname{LM}(q) \cdot \operatorname{LM}(f).$$

Но $\operatorname{LM}(f)$ и $\operatorname{LM}(g)$ взаимно просты, а следовательно, $\operatorname{LM}(g)$ делит $\operatorname{LM}(q)$. Но это невозможно, так как $\operatorname{LM}(g) > \operatorname{LM}(q)$. □

Рассмотрим пример. Пусть $G = (yz + z, x^3 + y, z^4)$ и используется grlex-упорядочение в $k[x, y, z]$. Тогда

$$S(x^3 + y, z^4) \to_G 0$$

по предложению 4. Однако применение алгоритма деления дает

$$S(x^3 + y, z^4) = yz^4 = (z^3 - z^2 + z - 1)(yz + y) + y,$$

т. е.

$$\overline{S(x^3 + y, z^4)}^G = y \neq 0.$$

Этот пример объясняет, почему полезно определение 1: предложение 4 становится ошибочным, если мы потребуем равенства нулю остатка от деления.

Отметим также, что предложение 4 позволяет усовершенствовать теорему 3: нам достаточно проверять условие $S(g_i, g_j) \to_G 0$, $i < j$, только в тех случаях, когда $\operatorname{LM}(g_i)$ и $\operatorname{LM}(g_j)$ не взаимно просты. Прежде чем применять предложение 4 для повышения эффективности алгоритма Бухбергера, обсудим еще один способ улучшить теорему 3.

Постараемся лучше понять, какую роль играют S-полиномы в доказательстве теоремы 6 § 6. Назначение S-полиномов — реализация сокращения старших членов. Это означает, что нам нужно изучить процесс сокращения в большей общности. Для этого мы вводим понятие *сизигии* старших членов множества $F = \{f_1, \dots, f_s\}$. Это понятие использовалось в астрономии, чтобы обозначить *расположение на одной прямой* трех планет или других небесных тел. Корнем термина является греческое слово, означающее «упряжь». Астрономическая сизигия означает, что планеты «запряжены вместе», математическая сизигия — что вместе «запряжены» полиномы.

Определение 5. Пусть $F = (f_1, \dots, f_s)$. *Сизигией* старших членов $\operatorname{LT}(f_1), \dots, \operatorname{LT}(f_s)$ называется s-набор полиномов $S = (h_1, \dots, h_s) \in (k[x_1, \dots, x_n])^s$, такой, что

$$\sum_{i=1}^{s} h_i \cdot \operatorname{LT}(f_i) = 0.$$

Мы будем обозначать через $S(F)$ подмножество в $(k[x_1, \dots, x_n])^s$, состоящее изо всех сизигий старших членов набора F.

В качестве примера рассмотрим $F = (x, x^2 + z, y + z)$ с lex-упорядочением. Тогда $S = (-x + y, 1, -x) \in (k[x, y, z])^3$ является сизигией из $S(F)$, так как

$$(-x + y) \cdot \operatorname{LT}(x) + 1 \cdot \operatorname{LT}(x^2 + z) + (-x) \cdot \operatorname{LT}(y + z) = 0.$$

Обозначим через $\mathbf{e}_i$ набор $(0, \dots, 0, 1, 0, \dots, 0) \in (k[x_1, \dots, x_n])^s$, где единица стоит на i-м месте. Тогда сизигия $S \in S(F)$ может быть записана в виде $S = \sum_{i=1}^{s} h_i \mathbf{e}_i$. Как пример использования этих обозначений рассмотрим сизигии, порожденные S-полиномами. А именно, рассмотрим пару $\{f_i, f_j\} \subset F$, где $i < j$, и пусть x^γ — наи-

меньшее общее кратное старших мономов f_i и f_j. Тогда

$$S_{ij} = \frac{x^\gamma}{\mathrm{LT}(f_i)}\mathbf{e}_i - \frac{x^\gamma}{\mathrm{LT}(f_j)}\mathbf{e}_j \qquad (3)$$

является сизигией старших членов набора F. На самом деле термин S-полином — это аббревиатура термина «полином сизигии» (syzygy polynomial).

Легко проверить, что множество сизигий замкнуто относительно покоординатного сложения и покоординатного умножения на полиномы (упр. 1). Особенно хорошим свойством множества $S(F)$ является то, что оно имеет конечный *базис*, т. е. существует конечный набор сизигий, такой, что любая сизигия является линейной комбинацией базисных сизигий с полиномиальными коэффициентами.

Прежде чем доказывать это утверждение, нам нужно больше узнать о структуре множества $S(F)$. Сначала дадим определение *однородной* сизигии.

Определение 6. Элемент $S \in S(F)$ называется *однородным мультистепени* α, где $\alpha \in \mathbb{Z}^n_{\geq 0}$, если

$$S = (c_1 x^{\alpha(1)}, \ldots, c_s x^{\alpha(s)}),$$

где $c_i \in k$ и $\alpha(i) + \mathrm{multideg}(f_i) = \alpha$ при $c_i \neq 0$.

Легко видеть, что сизигия S_{ij} из формулы (3) однородна мультистепени γ (упр. 4). Мы можем представить любую сизигию как сумму однородных.

Лемма 7. *Каждый элемент из $S(F)$ единственным образом может быть разложен в сумму однородных сизигий из $S(F)$.*

Доказательство. Пусть $S = (h_1, \ldots, h_s) \in S(F)$. Зафиксируем вектор $\alpha \in \mathbb{Z}^n_{\geq 0}$, и пусть $h_{i\alpha}$ — член полинома h_i (если он существует), такой, что $h_{i\alpha} f_i$ имеет мультистепень α. Тогда $\sum_{i=1}^s h_{i\alpha}\,\mathrm{LT}(f_i) = 0$, так как $h_{i\alpha}\,\mathrm{LT}(f_i), 1 \leq i \leq s$, — это все члены мультистепени α в $\sum_{i=1}^s h_i\,\mathrm{LT}(f_i) = 0$. Тогда $S_\alpha = (h_{1\alpha}, \ldots, h_{s\alpha})$ является однородным элементом в $S(F)$ мультистепени α и $S = \sum_\alpha S_\alpha$.

Доказательство единственности мы оставляем читателю (упр. 5). □

Теперь мы можем доказать, что S_{ij} образуют базис всех сизигий старших членов.

Предложение 8. *Если $F = (f_1, \ldots, f_s)$, то каждая сизигия $S \in S(F)$ может быть представлена как сумма,*

$$S = \sum_{i<j} u_{ij} S_{ij},$$

где $u_{ij} \in k[x_1, \ldots, x_n]$, а сизигии S_{ij} определены в (3).

Доказательство. По лемме 7 мы можем считать S однородной сизигией мультистепени α. Тогда S имеет по меньшей мере две ненулевых компоненты, например $c_i x^{\alpha(i)}$ и $c_j x^{\alpha(j)}$, $i < j$, и $\alpha(i) + \mathrm{multideg}(f_i) = \alpha(j) + \mathrm{multideg}(f_j) = \alpha$. Из этого следует, что $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))$ делит x^α. Так как

$$S_{ij} = \frac{x^\gamma}{\mathrm{LT}(f_i)}\mathbf{e}_i - \frac{x^\gamma}{\mathrm{LT}(f_j)}\mathbf{e}_j,$$

то i-я компонента сизигии

$$S - c_i\,\mathrm{LC}(f_i) x^{\alpha-\gamma} S_{ij}$$

равна нулю и все другие компоненты, кроме j-й, не изменились. Таким образом мы построили новую однородную сизигию, у которой количество ненулевых компонент меньше, чем у S. Продолжая этот процесс, мы разложим S в линейную комбинацию сизигий S_{ij}. □

Это предложение объясняет наше замечание в § 6 о том, что S-полиномы описывают все возможные сокращения старших членов.

Интересно отметить, что иногда базис пространства сизигий образуют и не *все* S_{ij}. Пусть, например, $F = (x^2y^2 + z, xy^2 - y, x^2y + yz)$, и мы используем lex-упорядочение в $k[x, y, z]$. Тогда

$$\begin{aligned} S_{12} &= (1, -x, 0), \\ S_{13} &= (1, 0, -y), \\ S_{23} &= (0, x, -y). \end{aligned}$$

Однако $S_{23} = S_{13} - S_{12}$, т. е. S_{23} — *лишний* элемент в том смысле, что он является линейной комбинацией S_{12} и S_{13}. (Здесь коэффициенты линейной комбинации — константы; в более общем случае эти коэффициенты могут быть полиномами.) Пара $\{S_{12}, S_{13}\}$ образует базис пространства сизигий. Далее в этом параграфе мы дадим общий метод построения малых базисов множества $S(F)$.

Теперь мы готовы дать уточненную формулировку алгоритмического критерия для базисов Грёбнера.

Теорема 9. *Базис $G = \{g_1, \ldots, g_s\}$ идеала I является его базисом Грёбнера в том и только том случае, когда для каждого элемента*

$S = (h_1, \dots, h_s)$ из однородного базиса пространства сизигий $S(G)$ выполнено следующее условие

$$S \cdot G = \sum_{i=1}^{s} h_i g_i \longrightarrow_G 0.$$

Доказательство. Мы будем использовать схему доказательства (и обозначения) теоремы 6 из § 6. Начинаем с представления $f = \sum_{i=1}^{s} h_i g_i$, где $f \in I$. Пусть $m(i) = \operatorname{multideg}(h_i g_i)$ и $\delta = \max(m(i))$. Мы выбираем такое представление f в виде линейной комбинации g_i, чтобы мультистепень δ была минимальной. Как и прежде, мы должны привести к противоречию предположение $\operatorname{multideg}(f) < \delta$.

В силу равенства (4) из § 6 из неравенства $\operatorname{multideg}(f) < \delta$ следует, что полином $\sum_{m(i)=\delta} \operatorname{LT}(h_i) g_i$ имеет строго меньшую мультистепень. Это означает, что $\sum_{m(i)=\delta} \operatorname{LT}(h_i) \operatorname{LT}(g_i) = 0$; поэтому

$$S = \sum_{m(i)=\delta} \operatorname{LT}(h_i) \mathbf{e}_i$$

является сизигией из $S(G)$. Отметим, что S — однородная сизигия мультистепени δ. Пусть $S_1, \dots, S_m$ — однородный базис сизигий. Из условия теоремы следует, что $S_j \cdot G \to_G 0$ для всех j. Запишем S в виде

$$S = u_1 S_1 + \dots + u_m S_m. \tag{4}$$

Тогда разложение каждого u_j в сумму членов позволит нам представить S как сумму однородных сизигий. Но S — однородная сизигия мультистепени δ; значит, из единственности представления (лемма 7) следует, что мы можем игнорировать все сизигии другой мультистепени, т. е. в (4) мы можем считать, что для каждого j

$$\text{или } u_j = 0, \text{ или } u_j S_j \text{ однородна мультистепени } \delta.$$

Пусть S_j имеет мультистепень γ_j. Если $u_j \neq 0$, то u_j может быть записан в виде $u_j = c_j x^{\delta - \gamma_j}$ для некоторого $c_j \in k$. Перепишем (4):

$$S = \sum_j c_j x^{\delta - \gamma_j} S_j,$$

где сумма берется по тем j, для которых $u_j \neq 0$. Скалярно умножим это равенство на G и получим

$$\sum_{m(i)=\delta} \operatorname{LT}(h_i) g_i = S \cdot G = \sum_j c_j x^{\delta - \gamma_j} S_j \cdot G. \tag{5}$$

По условию $S_j \cdot G \to_G 0$, т. е.

$$S_j \cdot G = \sum_{i=1}^{s} a_{ij} g_i, \tag{6}$$

где

$$\operatorname{multideg}(a_{ij} g_i) \leq \operatorname{multideg}(S_j \cdot G) \tag{7}$$

для всех i, j. Теперь надо заметить, что соотношения (5), (6) и (7) аналогичны соотношениям (5), (6) и (7) теоремы 6 из § 6. Далее доказательство повторяет доказательство теоремы 6. Единственное, что надо проверить, это что $x^{\delta - \gamma_j} S_j \cdot G$ имеет мультистепень $< \delta$ (см. упр. 6). Теорема доказана. □

Следует отметить, что теорема 6 § 6 является частным случаем теоремы 9. А именно, если мы возьмем $\{S_{ij}\}$ в качестве базиса пространства сизигий $S(G)$, то анализ полиномов $S_{ij} \cdot G$ будет происходить точно так же, как происходил анализ S-полиномов $S(g_i, g_j)$.

Чтобы использовать все возможности теоремы 9, нам надо научиться строить маленькие базисы пространства $S(G)$. Мы покажем, как, начиная с базиса $\{S_{ij} : i < j\}$, можно систематически исключать «лишние» элементы.

Предложение 10. *Пусть $G = (g_1, \dots, g_s)$, и пусть подмножество $\mathcal{S} \subset \{S_{ij} : 1 \leq i < j \leq s\}$ является базисом в $S(G)$. Кроме того, предположим, что существуют три разных полинома $g_i, g_j, g_l \in G$, такие, что*

$$\operatorname{LT}(g_l) \text{ делит } \operatorname{LCM}(\operatorname{LT}(g_i), \operatorname{LT}(g_j)).$$

Если $S_{il}, S_{jl} \in \mathcal{S}$, то $\mathcal{S} - \{S_{ij}\}$ также является базисом в $S(G)$. (Если $i > j$, то мы полагаем $S_{ij} = S_{ji}$.)

Доказательство. Пусть для простоты $i < j < l$. Положим $x^{\gamma_{ij}} = \operatorname{LCM}(\operatorname{LM}(g_i), \operatorname{LM}(g_j))$ ($x^{\gamma_{il}}$ и $x^{\gamma_{jl}}$ определены аналогично). Тогда по условию $x^{\gamma_{il}}$ и $x^{\gamma_{jl}}$ оба делят $x^{\gamma_{ij}}$. Мы оставляем читателю проверить, что

$$S_{ij} = \frac{x^{\gamma_{ij}}}{x^{\gamma_{il}}} S_{il} - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jl}}} S_{jl}.$$

Предложение доказано. □

Использование этого предложения в алгоритме построения базисов Грёбнера предполагает работу с упорядоченными парами (i, j), $i < j$, и отбор нужных сизигий. Так как при работе с парами $\{i, j\}$ нам не будет заранее известно, какой из индексов больше, то мы введем следующее обозначение:

$$[i, j] = \begin{cases} (i, j), & \text{если } i < j, \\ (j, i), & \text{если } i > j. \end{cases}$$

Теперь мы можем дать усовершенствованную версию алгоритма Бухбергера.

Теорема 11. *Пусть $I = \langle f_1, \dots, f_s \rangle$ — полиномиальный идеал. Его базис Грёбнера может быть построен за конечное число шагов с использованием следующего алгоритма:*

Вход: $F = (f_1, \dots, f_s)$
Выход: G, *базис Грёбнера идеала* $I = \langle f_1, \dots, f_s \rangle$
{инициализация}
$B := \{(i,j) | 1 \le i < j \le s\}$
$G := F$
$t := s$
{итерация}
WHILE $B \neq \emptyset$ *DO*
Выбрать $(i,j) \in B$
IF $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) \neq \mathrm{LT}(f_i)\,\mathrm{LT}(f_j)$ *AND*
критерий(f_i, f_j, B) *не выполняется THEN*
$S := \overline{S(f_i, f_j)}^{G}$
IF $S \neq 0$ *THEN*
$t := t + 1; f_t := S$
$G := G \cup \{f_t\}$
$B := B \cup \{(i,t) | 1 \le i \le t-1\}$
$B := B - \{(i,j)\}$.

Здесь «критерий(f_i, f_j, B) выполняется», *если существует некоторое* $l \notin \{i,j\}$, *для которого пары* $[i,l]$ *и* $[j,l]$ не принадлежат B *и* $\mathrm{LT}(f_l)$ *делит* $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$. (*Основа этого критерия — предложение* 10.)

Доказательство. Основная идея алгоритма состоит в том, что B есть список пар, которые нужно проверить. Кроме того, мы вычисляем остаток от деления только для тех S-полиномов $S(f_i, f_j)$, которые не удовлетворяют условиям предложения 4 или предложения 10.

Докажем корректность алгоритма. Отметим сначала, что на каждом шаге B удовлетворяет следующему условию: если $1 \le i < j \le t$ и $(i,j) \notin B$, то

$$S(f_i, f_j) \to_G 0 \text{ или критерий } (f_i, f_j, B) \text{ выполняется.} \qquad (8)$$

На первом шаге условие выполнено, так как B есть множество всех пар. Нам нужно доказать, что если (8) выполняется для некоторого B, то оно продолжает выполняться, когда B изменяется и превращается в B'.

Пусть $(i,j) \notin B'$. Если $(i,j) \in B$, то из описания алгоритма следует, что $B' = B - \{(i,j)\}$. Теперь поймем, что происходит на шаге, предшествующем исключению пары (i,j) из B. Если $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) = \mathrm{LT}(f_i)\,\mathrm{LT}(f_j)$, то $S(f_i, f_j) \to_G 0$ по предложению 4, и (8) выполнено. Точно также, если критерий(f_i, f_j, B) выполнен, то (8) имеет место. Предположим теперь, что оба эти условия не выполняются. Тогда алгоритм вычисляет остаток $S = \overline{S(f_i, f_j)}^{G}$. Если $S = 0$, то $S(f_i, f_j) \to_G 0$ по лемме 2. Если же $S \neq 0$, то мы увеличиваем G: $G' = G \cup \{S\}$ и $S(f_i, f_j) \to_{G'} 0$ (докажите это).

Осталось рассмотреть случай, когда $(i,j) \notin B$. Так как (8) выполняется для B, то (8) выполняется и для B' (докажите самостоятельно).

Теперь мы должны доказать, что G является базисом Грёбнера, когда B становится пустым множеством. Пусть t — количество элементов в G. Обозначим через $\mathcal{L}$ множество, состоящее из всех пар $(i,j), 1 \le i < j \le t$, таких, что критерий(f_i, f_j, B) *не выполняется*, если пара (i,j) выбрана алгоритмом. Мы утверждаем, что множество $\mathcal{S} = \{S_{ij} : (i,j) \in \mathcal{L}\}$ является базисом пространства $S(G)$ со следующим свойством: $S_{ij} \cdot G = S(f_i, f_j) \to_G 0$ для всех $S_{ij} \in \mathcal{S}$. Это утверждение и теорема 9 докажут, что G есть базис Грёбнера.

Чтобы доказать наше утверждение, заметим, что из $B = \varnothing$ следует, что (8) выполняется для *всех* пар $(i,j), 1 \le i < j \le t$. Значит, $S(f_i, f_j) \to_G 0$ для всех $(i,j) \in \mathcal{L}$. Осталось доказать, что $\mathcal{S}$ является базисом пространства $S(G)$. Заметим сначала, что мы можем *упорядочить* все пары в том порядке, в каком они исключаются из B при работе алгоритма (в упр. 10 это упорядочение подробно рассматривается). Начнем рассматривать пары в обратном порядке, начиная с последней исключенной, и теперь будем исключать те пары (i,j), для которых критерий(f_i, f_j, B) выполнялся именно на этом шаге алгоритма. Когда эта работа будет закончена, то оставшиеся пары — это в точности элементы из $\mathcal{L}$. Покажем, что на каждом шаге этого процесса сизигии, соответствующие пока не исключенным парам (i,j), образуют базис пространства $S(G)$. На первом шаге это верно, так как вначале у нас были все S_{ij}, которые, конечно, образуют базис. Если на каком-то шаге мы исключаем (i,j), то в силу определения условия «критерий(f_i, f_j, B)» существует l, такое, что $\mathrm{LT}(f_l)$ удовлетворяет условию LCM и $[i,l], [j,l] \notin B$. Таким образом, $[i,l]$ и $[j,l]$ были исключены из B ранее, и, значит, S_{il} и S_{jl} принадлежат множеству, которое мы строим, так как мы двигаемся в обратном направлении. Теперь из предложения 10 следует, что мы по-прежнему имеем базис и после удаления S_{ij}.

Наконец, необходимо доказать, что алгоритм в некоторый мо-

мент останавливается. Как и в доказательстве теоремы 2 из § 7, G всегда является базисом идеала, и каждый раз, когда мы увеличиваем G, мономиальный идеал $\langle \mathrm{LT}(G)\rangle$ строго увеличивается. По условию обрыва возрастающих цепей в некоторый момент G стабилизируется, т. е. мы прекращаем добавлять новые элементы в множество B. Начиная с этого момента, каждый цикл WHILE ... DO исключает один элемент из B, и в конце концов мы получим $B = \varnothing$. □

Построенный нами алгоритм по-прежнему не оптимален, и существует несколько способов увеличить его эффективность. Например, при рассмотрении алгоритма деления в $k[x_1, \ldots, x_n]$ (теорема 3 из § 3) мы допускали любой порядок делителей $f_1, \ldots, f_s$. Однако расположение f_i в порядке возрастания старших членов дает некоторую экономию вычислительных ресурсов. Так как небольшие $\mathrm{LT}(f_i)$ чаще используются в алгоритме деления, то расположение их в начале списка делителей означает, что количество сравнений уменьшится. Второе замечание относится к тому шагу алгоритма (теорема 11), на котором мы выбираем пару $(i, j) \in B$. Бухбергер в работе BUCHBERGER (1985) предположил, что выгоднее выбирать такую пару (i, j), для которой моном $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$ *минимален*. Соответствующий S-полином будет чаще выдавать ненулевые остатки (т. е. новые элементы базиса Грёбнера) в начале работы алгоритма; следовательно, повышается вероятность того, что затем остатки $\overline{S(f_i, f_j)}^{G}$ будут нулевыми. Эта так называемая *стратегия нормального выбора* подробно рассмотрена в работах BECKER, WEISPFENNING (1993), BUCHBERGER (1985) и GEBAUER, MÖLLER (1988). Наконец, еще есть *сахарная* стратегия, которая является усовершенствованием стратегии нормального выбора. Сахарная и ее вариант *двойная сахарная* стратегии рассмотрены в работе GIOVINI, MORA, NIESI, ROBBIANO, TRAVERSO (1991).

Другая идея состоит в том, чтобы сразу получать редуцированный базис Грёбнера, определенный в § 7. Для этого мы редуцируем G каждый раз, когда G увеличивается. Этот метод позволяет уменьшить число S-полиномов, с которыми мы работаем. Он обсуждается в работе BUCHBERGER (1985).

Мы закончим параграф кратким обсуждением вопроса о сложности алгоритма Бухбергера. Нетрудно придумать примеры идеалов, когда даже наилучшие современные версии алгоритма затрачивают колоссальное время и ресурсы памяти для вычисления базисов Грёбнера. Этому есть причины:

- Степени промежуточных полиномов, генерируемых в процессе вычисления, могут быть очень велики.

- Коэффициенты элементов базиса Грёбнера могут быть очень сложными рациональными числами, даже если исходные коэффициенты — небольшие целые числа.

По этим причинам большое количество усилий было затрачено, чтобы теоретически оценить верхнюю границу степеней промежуточных полиномов в зависимости от степеней начальных элементов базиса. С результатами этих исследований можно ознакомиться в работах DUBÉ (1990) и MÖLLER, MORA (1984). Идея состоит в том, чтобы понять, до каких пор сложность вычисления базиса Грёбнера остается разумной при возрастании сложности исходного базиса.

Оценки степеней элементов базиса Грёбнера весьма велики, и было показано, что это — неизбежное явление. Например, в работе MAYR, MEYER (1982) приведены примеры идеалов, порожденных полиномами степени $\leq d$, когда вычисление базиса Грёбнера приводит к полиномам степени порядка 2^{2^d}. При $d \to \infty$ число 2^{2^d} растет *очень* быстро. Даже если применяется grevlex-упорядочение (которое, как мы увидим, дает наименьший базис Грёбнера), степени остаются очень большими. Рассмотрим, например, полиномы

$$x^{n+1} - yz^{n-1}w, \quad xy^{n-1} - z^n, \quad x^n z - y^n w.$$

Если используется grevlex-упорядочение с $x > y > z > w$, то Мора (см. LAZARD (1983)) доказал, что редуцированный базис Грёбнера идеала, порожденного этими полиномами, содержит полином

$$z^{n^2+1}x - y^{n^2}w.$$

Эти результаты вызвали чувство пессимизма относительно практичности метода базисов Грёбнера в целом. Дальнейшие работы показали, однако, что в случае двух или трех переменных справедливы гораздо более разумные верхние оценки степеней (см., например, работы LAZARD (1983) и WINKLER (1984)). Более того, время работы и требуемая память гораздо меньше «в среднем» (это в том числе относится к задачам геометрического содержания), чем в наихудших случаях. Растет также понимание того, что вычисление чисто «алгебраических» данных (например, примарного разложения идеала, см. гл. 4) гораздо сложнее, чем вычисление «геометрических» (например, размерности многообразия, см. гл. 9). Эти вопросы обсуждаются в работе GUISTI, HEINTZ (1993), а обсуждение многообразных вопросов, связанных со сложностью вычисления базисов Грёбнера, содержится в работе BAYER, MUMFORD (1993).

Наконец, следует отметить, что замена переменных или изменение их порядка могут радикально упростить вычисления. В статье BAYER, STILLMAN (1987a) доказано, что в большинстве случаев grevlex-упорядочение дает базис Грёбнера с наименьшей полной

степенью. С другой стороны, некоторые версии алгоритма меняют упорядочение в ходе работы с целью получить более компактный базис Грёбнера. Эти вопросы обсуждаются в работе GRITZMANN STURMFELS (1993).

Упражнения к § 9

1. Пусть $S = (c_1, \dots, c_s)$ и $T = (d_1, \dots, d_s) \in (k[x_1, \dots, x_n])^s$ — сизигии старших членов набора $F = (f_1, \dots, f_s)$.
   (a) Докажите, что $S + T = (c_1 + d_1, \dots, c_s + d_s)$ — также сизигия.
   (b) Пусть $g \in k[x_1, \dots, x_n]$. Докажите, что $g \cdot S = (gc_1, \dots, gc_s)$ — также сизигия.

2. Пусть $G = (g_1, \dots, g_s) \in (k[x_1, \dots, x_n])^s$. Тогда мы можем определить сизигию для G как s-набор $S = (h_1, \dots, h_s) \in (k[x_1, \dots, x_n])^s$, такой что $\sum_i h_i g_i = 0$. (Заметим, что сизигии определялись нами ранее для набора старших членов $\mathrm{LT}(G) = (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s))$.)
   (a) Пусть $G = (x^2 - y, xy - z, y^2 - xz)$; тогда $(z, -y, x)$ есть сизигия для G.
   (b) Найдите какую-нибудь другую сизигию для G.
   (c) Докажите, что если S и T — сизигии для G, то $S + T$ и gS также являются сизигиями для G.

3. Пусть M есть $n \times (n+1)$-матрица полиномов из $k[x_1, \dots, x_n]$, и пусть I — идеал, порожденный определителями всех ее $n \times n$-подматриц (такие идеалы являются примерами так называемых *детерминантных* идеалов).
   (a) Найдите 2×3-матрицу M, такую, что ее детерминантный идеал 2×2-подматриц совпадает с идеалом, заданным образующими G из упр. 2.
   (b) Объясните происхождение сизигии в п. (a) упр. 2 в терминах построенной выше матрицы.
   (c) Найдите общий способ построения сизигий образующих детерминантного идеала. Указание: найдите способ построения вырожденных $(n+1) \times (n+1)$-матриц, содержащих M в качестве подматрицы.

4. Докажите, что сизигии S_{ij}, определенные в (3), являются однородными сизигиями мультистепени γ.

5. Завершите доказательство леммы 7, т. е. докажите, что разложение на однородные компоненты единственно. Указание: докажите сначала, что если $S = \sum_\alpha S'_\alpha$, где S'_α имеет мультистепень α, то i-е компоненты слагаемых S'_α для фиксированного i или равны нулю, или имеют мультистепень $\alpha - \mathrm{multideg}(f_i)$, и, следовательно, они различны для различных α.

6. Пусть S_j — однородная сизигия мультистепени γ_j в $S(G)$. Докажите, что $S_j \cdot G$ имеет мультистепень $< \gamma_j$. Из этого следует, что $x^{\delta - \gamma_j} S_j \cdot G$ имеет мультистепень $< \delta$ — результат, необходимый нам для доказательства теоремы 9.

7. Завершите доказательство предложения 10, доказав формулу, выражающую S_{ij} через S_{il} и S_{jl}.

8. Пусть G — конечное подмножество в $k[x_1, \dots, x_n]$ и $f \in \langle G \rangle$. Пусть $\bar{f}^G = r \neq 0$. Докажите, что $f \to_{G'} 0$, где $G' = G \cup \{r\}$. Этот факт использовался в доказательстве теоремы 11.

9. В доказательстве теоремы 11 мы использовали следующий факт: для любого значения B, если $1 \leq i < j \leq t$ и $(i,j) \notin B$, то условие (8) выполняется. Чтобы доказать это, мы рассуждали следующим образом: мы предполагали справедливость утверждения для некоторого B и доказывали, что справедливость сохраняется, когда B превращается в B'. Случай, когда $(i,j) \notin B'$, но $(i,j) \in B$, был подробно разобран в тексте. Осталось рассмотреть случай, когда $(i,j) \notin B \cup B'$. Докажите, что и в этом случае (8) выполняется для B'. Указание: (8) выполняется для B. Нужно рассмотреть два случая: когда B' больше B и когда B' меньше B. В последнем случае $B' = B - \{(k,l)\}$, причем $(k,l) \neq (i,j)$.

10. В этом упражнении мы рассмотрим упорядочение на множестве $\{(i,j) : 1 \leq i < j \leq t\}$, описанное в доказательстве теоремы 11. Пусть $B = \varnothing$; напомним, что t — это размер базиса G в момент остановки алгоритма.
    (a) Докажите, что любая пара $(i,j), 1 \leq i < j \leq t$, принадлежала B на каком-то шаге.
    (b) Используйте п. (a) и условие $B = \varnothing$ для объяснения, как упорядочиваются *все* пары в соответствии с порядком их удаления из B.

11. Пусть $f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x$ и используется grlex-упорядочение. Эти полиномы рассматривались в упр. 1 из § 7, где алгоритм Бухбергера использовался для построения базиса Грёбнера. Решите эту задачу с использованием алгоритма теоремы 11, в частности, укажите, сколько раз вам пришлось применять алгоритм деления.

12. Рассматриваются полиномы

$$x^{n+1} - yz^{n-1}w, \quad xy^{n-1} - z^n, \quad x^n z - y^n w,$$

и используется grevlex-упорядочение с $x > y > z > w$. Мора (см. LAZARD (1983)) доказал, что редуцированный базис Грёбнера содержит полином

$$z^{n^2+1} - y^{n^2} w.$$

Докажите, что это так, когда $n = 3, 4, 5$. Сколько элементов содержат базисы Грёбнера в этих случаях?

13. В этом упражнении на примерах мы рассмотрим, как порядок членов влияет на размер базиса Грёбнера и сложность его вычисления.
   (a) Найдите базис Грёбнера идеала $I = \langle x^5+y^4+z^3-1, x^3+y^2+z^2-1\rangle$, используя lex- и grevlex-упорядочения с $x > y > z$. Возможно, вам трудно будет заметить различие во времени вычисления, но вы заметите, что базис Грёбнера заметно проще в grevlex-случае.
   (b) Найдите базис Грёбнера идеала $I = \langle x^5+y^4+z^3-1, x^3+y^3+z^2-1\rangle$, используя lex- и grevlex-упорядочения с $x > y > z$. Этот пример отличается от предыдущего в одном члене, но базис Грёбнера в lex-случае оказывается много хуже (один из полиномов имеет 282 члена, полная степень равна 25, а наибольший коэффициент равен 170255391). Это, конечно, зависит от компьютера и версии алгоритма, но вычисление в lex-случае может быть очень долгим.
   (c) Пусть $I = \langle x^4 - yz^2w, xy^2 - z^3, x^3z - y^3w\rangle$ — идеал из упр. 12, где $n = 3$. Используя lex- и grevlex-упорядочения с $x > y > z > w$, покажите, что базисы Грёбнера в обоих случаях совпадают. Так что grevlex-упорядочение не всегда лучше, чем lex-упорядочение, но на практике рекомендуется использовать именно grevlex-упорядочение, когда это возможно.

3
Теория исключения

В этой главе мы рассмотрим методы, позволяющие исключать переменные в системах полиномиальных уравнений. Основы стратегии исключения будут сформулированы в двух теоремах: теореме об исключении и теореме о продолжении. Мы докажем их, используя базисы Грёбнера и классическую теорию результантов. Геометрический смысл исключения будет описан в теореме о замыкании. Из многих приложений теории исключения два мы рассмотрим подробно: задачу неявного представления и задачу об огибающей семейства кривых.

§ 1. Теоремы об исключении и продолжении

Чтобы понять, как работает процедура исключения, рассмотрим пример, аналогичный тому, который рассматривался в конце гл. 2. Мы будем решать систему уравнений

$$\begin{aligned} x^2 + y + z &= 1, \\ x + y^2 + z &= 1, \\ x + y + z^2 &= 1. \end{aligned} \tag{1}$$

Пусть

$$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1\rangle. \tag{2}$$

Тогда базис Грёбнера этого идеала по отношению к lex-упорядочению состоит из четырех полиномов

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned} \tag{3}$$

Системы (1) и (3) имеют одинаковое множество решений. Но так как

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1)$$

зависит только от z, то возможными значениями z могут быть только корни полинома g_4, т. е. $0, 1$ и $-1 \pm \sqrt{2}$. Подставляя их в $g_2 = y^2 - y - z^2 + z = 0$ и в $g_3 = 2yz^2 + z^4 - z^2 = 0$, мы можем определить возможные значения y. А затем $g_1 = x + y + z^2 - 1 = 0$ позволит определить x. Таким образом, мы получаем, что система (1) имеет в точности 5 решений:

$$(1,0,0), (0,1,0), (0,0,1),$$
$$(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}),$$
$$(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

Как же нам удалось решить систему? Наш успех стал возможным по двум причинам:

- (Шаг исключения) Мы смогли найти следствие $g_4 = z^6 - 4z^4 + 4z^3 - z^2 = 0$ исходных уравнений системы, которое зависит только от z, т. е. мы исключили x и y из системы уравнений.
- (Шаг продолжения) Как только мы нашли решения простого уравнения $g_4 = 0$, т. е. нашли значения z, то смогли продолжить эти решения до решений исходных уравнений.

Основная идея *теории исключения* состоит в том, что и шаг исключения, и шаг продолжения должны рассматриваться в большей общности.

Посмотрим, как работает шаг исключения. Тот факт, что g_4 зависит только от z, означает, что

$$g_4 \in I \cap \mathbb{C}[z],$$

где идеал I задан равенством (2). На самом деле множество $I \cap \mathbb{C}[z]$ состоит из *всех* тех следствий исходных уравнений, которые не зависят от x и y. Обобщая это наблюдение, приходим к следующему определению.

Определение 1. Пусть дан идеал $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$. Тогда l-м *исключающим идеалом* I_l называется идеал в $k[x_{l+1}, \ldots, x_n]$, равный

$$I \cap k[x_{l+1}, \ldots, x_n].$$

Другими словами, I_l состоит из всех следствий системы $f_1 = \ldots = f_s = 0$, которые не зависят от переменных $x_1, \ldots, x_l$. В упражнениях мы проверим, что I_l в самом деле является идеалом в $k[x_{l+1}, \ldots, x_n]$. Отметим, что $I = I_0$ является нулевым (по номеру) исключающим идеалом. Также отметим, что изменение порядка переменных приводит к другим исключающим идеалам.

На этом языке исключение переменных $x_1, \ldots, x_l$ означает нахождение ненулевых полиномов в l-м исключающем идеале I_l. Таким образом, *решение шага исключения означает предъявление процедуры построения элементов из* I_l. При правильном упорядочении базисы Грёбнера сразу решают эту задачу.

Теорема 2 (теорема об исключении). *Пусть* $I \subset k[x_1, \ldots, x_s]$ — *идеал и* G — *его базис Грёбнера по отношению к* lex-*упорядочению с* $x_1 > x_2 > \ldots > x_n$. *Тогда для любого* $0 \le l \le n$ *множество*

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

является базисом Грёбнера l*-го исключающего идеала* I_l.

Доказательство. Зафиксируем l в интервале между 0 и n. Так как $G_l \subset I_l$ по построению, то достаточно доказать, что

$$\langle \mathrm{LT}(I_l) \rangle = \langle \mathrm{LT}(G_l) \rangle$$

(по определению базиса Грёбнера). Включение в одну сторону очевидно. Для доказательства другого включения $\langle \mathrm{LT}(I_l) \rangle \subset \langle \mathrm{LT}(G_l) \rangle$ нам достаточно доказать, что старший член $\mathrm{LT}(f)$, где f — произвольный полином из I_l, делится на некоторый старший член $\mathrm{LT}(g)$, $g \in G_l$.

Докажем это. Отметим сначала, что f принадлежит также и I, т. е. $\mathrm{LT}(f)$ делится на $\mathrm{LT}(g)$ для некоторого $g \in G$ (так как G является базисом Грёбнера идеала I). Так как $f \in I_l$, то $\mathrm{LT}(g)$ содержит только переменные $x_{l+1}, \ldots, x_n$. Теперь решающее замечание: так как используется lex-упорядочение с $x_1 > \ldots > x_n$, то любой моном, содержащий хотя бы одну из переменных $x_1, \ldots, x_l$, больше всех мономов из $k[x_{l+1}, \ldots, x_n]$. Поэтому из включения $\mathrm{LT}(g) \in k[x_{l+1}, \ldots, x_n]$ следует, что $g \in k[x_{l+1}, \ldots, x_n]$. Значит, $g \in G_l$. Теорема доказана. □

В качестве примера использования этой теоремы вернемся к системе (1) из начала параграфа. Здесь $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$, а базис Грёбнера для lex-упорядочения указан в (3). Из теоремы об исключении следует, что

$$I_1 = I \cap \mathbb{C}[y,z] = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2 \rangle,$$
$$I_2 = I \cap \mathbb{C}[z] = \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle.$$

То есть использование полинома $g_4 = z^6 - 4z^4 + 4z^3 - z^2$ — это наилучший (а не какой-то случайный) способ исключить x и y из системы (все другие полиномы, исключающие x и y, кратны g_4).

Теорема об исключении показывает, что базис Грёбнера в случае lex-упорядочения исключает не только первую переменную, но первые две переменные, первые три переменные и т. д.

В некоторых случаях (как в случае задачи неявного представления, которая будет рассмотрена в § 3) нам нужно исключить не все, а только некоторые переменные. Здесь применение базиса Грёбнера для lex-упорядочения переусложняет решение. В частности, это связано с тем, что вычисление базиса в lex-случае может привести к очень неприятным полиномам (см., например, упр. 13 § 9 гл. 2). В упражнениях мы рассмотрим другие формулировки теоремы об исключении, которые используют более эффективные упорядочения, чем lex.

Теперь рассмотрим шаг продолжения. Пусть дан идеал $I \subset k[x_1, \ldots, x_n]$. Аналогично тому, как это делалось в гл. 2, мы будем рассматривать аффинное многообразие

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \quad \text{для всех} \quad f \in I\}.$$

Как найти все его точки? Основная идея — строить решения, определяя одну координату за другой. Пусть $1 \leq l \leq n$. Рассмотрим исключающий идеал I_l. Точка $(a_{l+1}, \ldots, a_l) \in \mathbf{V}(I_l)$ называется *частичным решением* исходной системы. Чтобы продолжить $(a_{l+1}, \ldots, a_n)$ до полного решения системы, нам сначала нужно добавить одну координату. Это означает, что надо найти a_l такое, что $(a_l, \ldots, a_n) \in \mathbf{V}(I_{l-1})$. Точнее, пусть $I_{l-1} = \langle g_1, \ldots, g_r \rangle \subset k[x_l, \ldots, x_n]$. Нам нужно найти решения $x_l = a_l$ системы уравнений

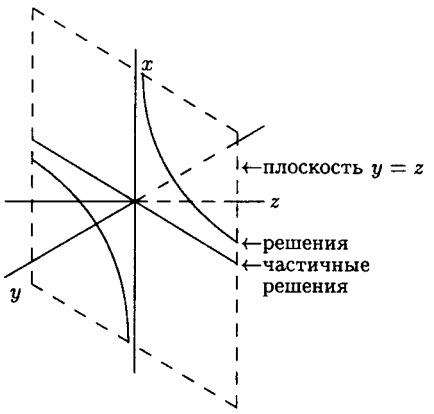
$$g_1(x_l, a_{l+1}, \ldots, a_n) = \ldots = g_r(x_l, a_{l+1}, \ldots, a_n) = 0.$$

Так как здесь мы работаем с полиномами от одной переменной x_l, то a_l является корнем наибольшего общего делителя этих r полиномов.

Это рассуждение позволяет сформулировать основную проблему: приведенные выше полиномы могут не иметь общего корня, т. е. может существовать частичное решение, не имеющее продолжения до полного. В качестве примера рассмотрим систему

$$\begin{aligned} xy &= 1, \\ xz &= 1. \end{aligned} \tag{4}$$

Здесь $I = \langle xy - 1, xz - 1 \rangle$, и из теоремы об исключении следует, что $y - z$ порождает первый исключающий идеал I_1. Частичные решения описываются формулой (a, a) и все они продолжаются до полного решения $(1/a, a, a)$, *кроме* частичного решения $(0, 0)$. Рассмотрим геометрию этого явления. Уравнение $y = z$ задает плоскость в трехмерном пространстве. Многообразие (4) — гипербола, лежащая в этой плоскости:



Очевидно, что многообразие, определенное уравнениями (4), не имеет точек, лежащих над частичным решением $(0, 0)$. Подобные рисунки будут подробно рассматриваться в § 2, где будет излагаться геометрическая интерпретация исключения. Теперь наша цель — понять, как определить *заранее*, какие частичные решения могут быть продолжены до полного.

Ограничимся случаем исключения первой переменной x_1, т. е. мы хотим узнать, может ли частичное решение $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ быть продолжено до решения $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$? Следующая теорема отвечает на этот вопрос.

Теорема 3 (теорема о продолжении). *Пусть* $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$, *и пусть* I_1 *— первый исключающий идеал для* I. *Для каждого* $1 \leq i \leq s$ *запишем* f_i *в виде*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \textit{члены, содержащие}\, x_1 \textit{ в степени} < N_i,$$

где $N_i \geq 0$, *а* $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ *— ненулевые полиномы. Рассмотрим частичное решение* $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. *Тогда если* $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$, *то существует* $a_1 \in \mathbb{C}$, *такое, что* $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Доказательство этой теоремы использует теорию результантов и будет дано в § 6. В оставшейся части параграфа мы объясним смысл теоремы о продолжении и обсудим некоторые следствия из нее. Геометрическая интерпретация теоремы будет рассмотрена в § 2.

Отметим сначала, что теорема формулируется для поля $k = \mathbb{C}$. Чтобы понять почему, положим $k = \mathbb{R}$ и рассмотрим систему

$$\begin{aligned} x^2 &= y, \\ x^2 &= z. \end{aligned} \tag{5}$$

Исключая x, получаем $y = z$, т. е. (a, a) является частичным решением для всех $a \in \mathbb{R}$. Так как старшие коэффициенты по x в $x^2 - y$ и $x^2 - z$ не обращаются в нуль, то теорема о продолжении гарантирует продолжаемость решений (a, a) *при условии*, что мы работаем над $\mathbb{C}$. Над $\mathbb{R}$ ситуация иная. Уравнение $x^2 = a$ не имеет вещественных решений, если a отрицательно, т. е. только частичные решения с $a \geq 0$ продолжаются до вещественных решений системы (5). Этот пример показывает, что теорема о продолжении не имеет места над $\mathbb{R}$.

Теперь рассмотрим условие $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$. Напомним, что g_i — это старшие коэффициенты полиномов f_i по отношению к переменной x_1, т. е. условие $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$ означает, что старшие коэффициенты не обращаются одновременно в нуль на частичном решении. Чтобы понять необходимость этого условия, вернемся к системе (4). Эта система

$$\begin{aligned} xy &= 1, \\ xz &= 1 \end{aligned}$$

имеет частичные решения $(y, z) = (a, a)$. Единственное непродолжаемое решение $(0, 0)$ — как раз то, которое обращает в нуль старшие коэффициенты при x (т. е. y и z). Теорема о продолжении утверждает, что *шаг продолжения может не выполниться, если старшие коэффициенты одновременно равны нулю.*

Наконец, следует отметить, что многообразие $\mathbf{V}(g_1, \ldots, g_s)$, где старшие коэффициенты $g_1, \ldots, g_s$ обращаются в нуль, зависит от базиса $\{f_1, \ldots, f_s\}$ идеала I: изменяя базис идеала, мы можем изменить $\mathbf{V}(g_1, \ldots, g_s)$. В гл. 8 мы узнаем, как выбрать базис $\{f_1, \ldots, f_s\}$ так, чтобы многообразие $\mathbf{V}(g_1, \ldots, g_s)$ стало как можно меньше. Отметим также, что переход к проективному пространству (определенному в гл. 8) упрощает формулировку теоремы о продолжении: в проективном пространстве *все* частичные решения продолжаемы.

Хотя теорема о продолжении сформулирована для случая исключения первой переменной x_1, она может применяться для исключения любого набора переменных. Рассмотрим, например, уравнения

$$\begin{aligned} x^2 + y^2 + z^2 &= 1, \\ xyz &= 1. \end{aligned} \tag{6}$$

Базис Грёбнера идеала $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$ по отношению к lex-упорядочению состоит из двух элементов

$$\begin{aligned} g_1 &= y^4z^2 + y^2z^4 - y^2z^2 + 1, \\ g_2 &= x + y^3z + yz^3 - yz. \end{aligned}$$

По теореме об исключении

$$\begin{aligned} I_1 &= I \cap \mathbb{C}[y, z] = \langle g_1 \rangle, \\ I_2 &= I \cap \mathbb{C}[z] = \{0\}. \end{aligned}$$

Так как $I_2 = \{0\}$, то $\mathbf{V}(I_2) = \mathbb{C}$ и, значит, *любое* $c \in \mathbb{C}$ является частичным решением. Теперь требуется решить следующий вопрос:

Какие частичные решения $c \in \mathbb{C} = \mathbf{V}(I_2)$
продолжаются до $(a, b, c) \in \mathbf{V}(I)$?

Идея состоит в пошаговом продолжении c: сначала до (b, c), потом до (a, b, c). На каждом шаге теорема указывает, какие решения продолжаются. Ключевым здесь является факт, что I_2 есть первый исключающий идеал для I_1. Это очевидно для нашего примера, а общий случай разобран в упражнениях. Применим теорему о продолжении, чтобы перейти от $c \in \mathbf{V}(I_2)$ к $(b, c) \in \mathbf{V}(I_1)$, а затем к $(a, b, c) \in \mathbf{V}(I)$. Тогда мы и узнаем, какие c продолжаются.

Сначала применим теорему о продолжении для перехода от I_2 к $I_1 = \langle g_1 \rangle$. Старший коэффициент в g_1 (при y^4) равен z^2; поэтому $c \in \mathbb{C} = \mathbf{V}(I)$ продолжается до (b, c), если $c \neq 0$. Следует отметить, что уравнение $g_1 = 0$ вообще не имеет решений при $c = 0$. Следующий шаг — это переход от I_1 к I, т. е. поиск такого a, что $(a, b, c) \in \mathbf{V}(I)$. Если мы подставим $(y, z) = (b, c)$ в (6), то получим два уравнения относительно x, причем совсем не очевидно, что они имеют общее решение $x = a$. Здесь теорема о продолжении показывает свою силу. Старшие коэффициенты при x в $x^2 + y^2 + z^2 - 1$ и $xyz - 1$ — это 1 и yz соответственно. Так как 1 не обращается в нуль, то теорема о продолжении *гарантирует* существование общего решения a. Мы доказали, что *все* частичные решения $c \neq 0$ продолжаются до элемента из $\mathbf{V}(I)$.

Особенно удобно применять теорему о продолжении, когда один из старших коэффициентов — константа. Зафиксируем этот полезный случай как отдельное утверждение.

Следствие 4. *Пусть* $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$, *и пусть* f_i *для некоторого* i *имеет следующий вид:*

$$f_i = cx_1^N + \textit{члены, которые содержат } x_1 \textit{ в степени } < N,$$

где $c \in \mathbb{C}$ — *ненулевая константа и* $N > 0$. *Пусть* I_1 — *первый исключающий идеал и* $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. *Тогда существует* $a_1 \in \mathbb{C}$, *такое, что* $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Доказательство. Это утверждение прямо следует из теоремы о продолжении: так как $g_i = c \neq 0$, то многообразие $\mathbf{V}(g_1, \ldots, g_s)$ пусто и $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$ для всех частичных решений. □

В заключение мы рассмотрим систему уравнений, не имеющую хороших решений. Пусть даны уравнения

$$\begin{aligned} xy &= 4, \\ y^2 &= x^3 - 1. \end{aligned}$$

Базис Грёбнера для lex-упорядочения имеет вид

$$\begin{aligned} g_1 &= 16x - y^2 - y^4, \\ g_2 &= y^5 + y^3 - 64. \end{aligned}$$

Полином $y^5 + y^3 - 64$, однако, *не имеет* рациональных корней (на самом деле он *неприводим* над $\mathbb{Q}$ — понятие, которое будет рассматриваться в § 4). Нам остается найти приближенные значения корней. Это можно сделать многими способами (с использованием метода Ньютона–Рафсона, например). Получаем

$$y = 2.21363, \quad -1.78719 \pm 1.3984i \quad \text{или} \quad 0.680372 \pm 2.26969i.$$

Эти значения можно подставить в $g_1 = 16x - y^2 - y^4 = 0$ и найти x. Здесь, в отличие от предыдущих примеров, мы можем найти только приближенные решения.

Существует много интересных задач, связанных с численным решением полиномиальных уравнений. Мы можем рекомендовать работы LAZARD (1993) и MANOCHA (1994). Читатель также может ознакомиться с работами COX, LITTLE, O'SHEA (1998), MIGNOTTE (1992) и MISHRA (1993).

Упражнения к § 1

1. Рассмотрим идеал $I \subset k[x_1, \ldots, x_n]$.
   (a) Докажите, что $I_l = I \cap k[x_{l+1}, \ldots, x_n]$ — идеал в $k[x_{l+1}, \ldots, x_n]$.
   (b) Докажите, что идеал $I_{l+1} \subset k[x_{l+2}, \ldots, x_n]$ является первым исключающим идеалом идеала $I_l \subset k[x_{l+1}, \ldots, x_n]$. Это утверждение позволяет применять теорему о продолжении пошагово, когда исключается несколько переменных.
2. Рассмотрим систему уравнений
$$\begin{aligned} x^2 + 2y^2 &= 3, \\ x^2 + xy + y^2 &= 3. \end{aligned}$$
   (a) Пусть I — соответствующий идеал. Найдите базисы идеалов $I \cap k[x]$ и $I \cap k[y]$.
   (b) Найдите все решения системы.
   (c) Какие из этих решений рациональны, т. е. принадлежат $\mathbb{Q}^2$?

   (d) Найдите наименьшее поле k, такое, что все решения принадлежат k^2.
3. Найдите все решения $(x, y) \in \mathbb{Q}^2$ системы уравнений
$$\begin{aligned} x^2 + 2y^2 &= 2, \\ x^2 + xy + y^2 &= 2. \end{aligned}$$
   Найдите все решения $(x, y) \in \mathbb{C}^2$.
4. Найдите базисы исключающих идеалов I_1 и I_2 идеала I, определенного уравнениями
$$\begin{aligned} x^2 + y^2 + z^2 &= 4, \\ x^2 + 2y^2 &= 5, \\ xz &= 1. \end{aligned}$$
   Сколько рациональных (т. е. принадлежащих $\mathbb{Q}^3$) решений имеет эта система?
5. В этом упражнении мы докажем теорему об исключении в более общей формулировке. Зафиксируем l, $1 \leq l \leq n$. Мономиальное упорядочение $>$ на $k[x_1, \ldots, x_n]$ называется упорядочением *l-исключающего типа*, если любой моном, содержащий хотя бы одну из переменных $x_1, \ldots, x_l$, больше любого монома из $k[x_{l+1}, \ldots, x_n]$. Докажите следующую обобщенную теорему об исключении. Пусть I — идеал в $k[x_1, \ldots, x_n]$ и G — его базис Грёбнера по отношению к мономиальному упорядочению l-исключающего типа. Тогда $G \cap k[x_{l+1}, \ldots, x_n]$ является базисом Грёбнера l-го исключающего идеала $I \cap k[x_{l+1}, \ldots, x_n]$.
6. Чтобы применять обобщенную теорему об исключении из упр. 5, нам нужно знать, какие существуют упорядочения l-исключающего типа (кроме lex). Рассмотрим два примера.
   (a) Зафиксируем число $1 \leq l \leq n$ и определим упорядочение $>_l$ следующим образом: если $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, то $\alpha >_l \beta$, когда
$$\begin{aligned} &\alpha_1 + \ldots + \alpha_l > \beta_1 + \ldots + \beta_l \quad \text{или} \\ &\alpha_1 + \ldots + \alpha_l = \beta_1 + \ldots + \beta_l \quad \text{и} \quad \alpha >_{\text{grevlex}} \beta. \end{aligned}$$
   Это упорядочение называется l-м *исключающим упорядочением* Байера и Стиллмана (BAYER, STILLMAN (1987b)). Докажите, что $>_l$ является мономиальным упорядочением и упорядочением l-го исключающего типа. Указание: если вы сделали упр. 12 § 4 из гл. 2, то эта задача вами уже решена.
   (b) В упр. 10 § 4 из гл. 2 рассматривалось произведение упорядочений, «смешивающее» lex- и grlex-упорядочения на различных множествах переменных. Объясните, как определить произведение, индуцирующее grevlex-упорядочение на $k[x_1, \ldots, x_l]$ и на $k[x_{l+1}, \ldots, x_n]$. Докажите, что это упорядочение есть упорядочение l-исключающего типа.

(c) Пусть G — базис Грёбнера идеала $I \subset k[x_1, \ldots, x_n]$ как для упорядочения из п. (a), так и для упорядочения из п. (b). Докажите, что $G \cap k[x_{l+1}, \ldots, x_n]$ является базисом Грёбнера идеала I_l по отношению к grevlex-упорядочению.

7. Рассмотрим систему

$$\begin{aligned} t^2 + x^2 + y^2 + z^2 &= 0, \\ t^2 + 2x^2 - xy - z^2 &= 0, \\ t + y^3 - z^3 &= 0. \end{aligned}$$

Мы хотим исключить t. Пусть $I = \langle t^2 + x^2 + y^2 + z^2, t^2 + 2x^2 - xy - z^2, t + y^3 - z^3 \rangle$ — соответствующий идеал.

(a) Используя lex-упорядочение с $t > x > y > z$, найдите базис Грёбнера для I, а затем базис для $I \cap k[x, y, z]$. Вы должны получить четыре полинома, один из которых имеет степень 12.

(b) Используя grevlex-упорядочение, найдите базис Грёбнера идеала $I \cap k[x, y, z]$. Вы должны получить более простое множество из двух элементов.

(c) Объедините базис, полученный в п. (b), с полиномом $t + y^3 - z^3$ и докажите, что это объединение является базисом Грёбнера для I по отношению к упорядочению $>_1$ из упр. 6. Этот базис много проще базиса, найденного в п. (a). Проверьте вычисления, если ваша система компьютерной алгебры умеет работать с исключающими упорядочениями.

8. При решении системы (6) мы показали, что $z \neq 0$ может быть задано произвольно. Следовательно, z является «параметром». Определите x и y как функции от z. Указание: решите g_1 относительно y. Затем используйте уравнение $xyz = 1$, чтобы найти x. Полученные вами формулы, «параметризующие» $\mathbf{V}(I)$, не похожи на параметризации из § 3 гл. 1. А именно, в гл. 1 мы рассматривали *рациональные* параметризации (т. е. параметризации рациональными функциями), в то время как здесь мы получили *алгебраическую* параметризацию (т. е. параметризацию алгебраическими функциями). Заметим, что x и y *неоднозначно* выражаются через z.

9. Рассмотрим систему уравнений

$$\begin{aligned} x^5 + \frac{1}{x^5} &= y, \\ x + \frac{1}{x} &= z. \end{aligned}$$

Пусть $I \subset \mathbb{C}[x, y, z]$ — идеал, определенный этими уравнениями.

(a) Найдите базис идеала $I_1 \subset \mathbb{C}[y, z]$ и докажите, что $I_2 = \{0\}$.

(b) Используя теорему о продолжении, докажите, что любое частичное решение $c \in \mathbf{V}(I_2) = \mathbb{C}$ продолжается до решения из многообразия $\mathbf{V}(I) \subset \mathbb{C}^3$.

(c) Какие частичные решения $(y, z) \in \mathbf{V}(I_1) \subset \mathbb{R}^2$ продолжаются до решений из $\mathbf{V}(I) \subset \mathbb{R}^3$? Объясните, почему ваш ответ не противоречит теореме о продолжении.

(d) Рассмотрим z как параметр (см. предыдущее упражнение). Найдите алгебраические формулы, выражающие x и y через z, т. е. найдите «параметризацию» многообразия $\mathbf{V}(I)$.

§ 2. Геометрия исключения

В этом параграфе мы рассмотрим геометрическую интерпретацию теорем, доказанных в § 1. Основная идея состоит в том, что процессу исключения соответствует проектирование многообразия на подпространство меньшей размерности. Будет рассмотрена также теорема о замыкании, которая описывает связь между частичными решениями и исключающими идеалами. Чтобы избежать излишних трудностей, в качестве основного поля мы выберем $k = \mathbb{C}$.

Начнем с определения проекции. Пусть дано аффинное многообразие $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$. Для исключения первых l переменных $x_1, \ldots, x_l$ мы рассмотрим *отображение проекции*

$$\pi_l : \mathbb{C}^n \to \mathbb{C}^{n-l},$$

которое вектор $(a_1, \ldots, a_n)$ переводит в вектор $(a_{l+1}, \ldots, a_n)$. Применяя отображение π_l к многообразию $V \subset \mathbb{C}^n$, мы получим множество $\pi_l(V) \subset \mathbb{C}^{n-l}$. Свяжем $\pi_l(V)$ с l-м исключающим идеалом следующим образом.

Лемма 1. *Пусть $I_l = \langle f_1, \ldots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \ldots, x_n]$ есть l-й исключающий идеал. Тогда*

$$\pi_l(V) \subset \mathbf{V}(I_l) \subset \mathbb{C}^{n-l}.$$

Доказательство. Рассмотрим полином $f \in I_l$. Если $(a_1, \ldots, a_n)$ принадлежит V, то его значение в точке $(a_1, \ldots, a_n)$ равно нулю, так как $f \in \langle f_1, \ldots, f_s \rangle$. Но f зависит только от $x_{l+1}, \ldots, x_n$; значит,

$$f(a_{l+1}, \ldots, a_n) = f(\pi_l(a_1, \ldots, a_n)) = 0.$$

Следовательно, f равен нулю во всех точках из $\pi_l(V)$. □

Как и в § 1, точки многообразия $\mathbf{V}(I_l)$ будут называться *частичными решениями*. Теперь мы можем описать $\pi_l(V)$ следующим образом:

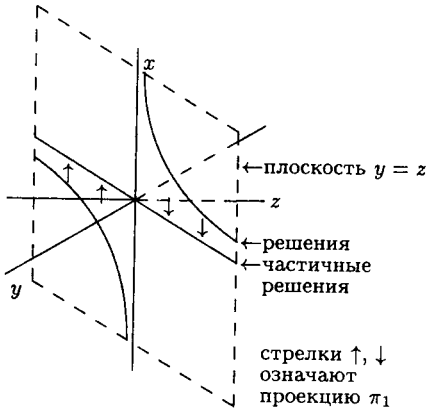
$$\pi_l(V) = \{(a_{l+1}, \ldots, a_n) \in \mathbf{V}(I_l) : \exists \text{ элементы } a_1, \ldots, a_l \in \mathbb{C}, \\ \text{такие, что } (a_1, \ldots, a_l, a_{l+1}, \ldots, a_n) \in V\}.$$

Другими словами, $\pi_l(V)$ состоит *в точности* из тех частичных решений, которые могут быть продолжены до полных. Рассмотрим,

например, многообразие V, заданное системой (4) из § 1:

$$\begin{aligned} xy &= 1, \\ xz &= 1. \end{aligned} \tag{1}$$

На следующем рисунке показаны и полные, и частичные решения:



Отметим, что $\mathbf{V}(I_1)$ — это прямая $y = z$ в yz-плоскости и что

$$\pi_1(V) = \{(a, a) \in \mathbb{C}^2 : a \neq 0\}.$$

В частности, $\pi_1(V)$ *не является* аффинным многообразием — недостает точки $(0, 0)$.

Теорема о продолжении из § 1 является основным инструментом анализа «недостающих» точек. Теорема сформулирована только для отображения проекции π_1 (т. е. для исключения x_1) и дает хорошее описание того, что происходит в этом случае. Переведем формулировку теоремы о продолжении на геометрический язык.

Теорема 2. *Пусть дано многообразие* $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$, *и пусть* g_i *определены так же, как в формулировке теоремы о продолжении из* § 1. *Если* I_1 *— первый исключающий идеал для идеала* $\langle f_1, \ldots, f_s \rangle$, *то в* $\mathbb{C}^{n-1}$ *имеет место следующее равенство:*

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)),$$

где $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$ *— отображение проекции на последние* $n - 1$ *компонент.*

Доказательство. Это утверждение является следствием теоремы о продолжении и леммы 1. Детали доказательства мы оставляем читателю. □

Эта теорема утверждает, что $\pi_1(V)$ покрывает все аффинное многообразие $\mathbf{V}(I_1)$, кроме, разве что, части, лежащей в $\mathbf{V}(g_1, \ldots, g_s)$. К сожалению, остается неясным, насколько велика может быть эта часть. Иногда $\mathbf{V}(g_1, \ldots, g_s)$ может быть весьма велико. Легко доказать, например, что система

$$\begin{aligned} (y - z)x^2 + xy &= 1, \\ (y - z)x^2 + xz &= 1 \end{aligned} \tag{2}$$

порождает тот же идеал, что и система (1). Так как полиномы $g_1 = g_2 = y - z$ порождают исключающий идеал I_1, то геометрическая теорема о продолжении *ничего* не может сказать нам о размере $\pi_1(V)$ в этом случае.

Тем не менее мы можем сформулировать довольно сильные утверждения о связи между $\pi_l(V)$ и $\mathbf{V}(I_l)$.

Теорема 3 (теорема о замыкании). *Пусть* $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$, *и пусть* I_l *есть* l*-й исключающий идеал идеала* $\langle f_1, \ldots, f_s \rangle$. *Тогда*

(i) $\mathbf{V}(I_l)$ *является наименьшим аффинным многообразием, содержащим* $\pi_l(V) \subset \mathbb{C}^{n-l}$;

(ii) *Если* $V \neq \varnothing$, *то существует аффинное многообразие* $W \subsetneq \mathbf{V}(I_l)$, *такое, что* $\mathbf{V}(I_l) - W \subset \pi_l(V)$.

Доказательство. Термин «наименьшее многообразие» в п. (i) означает «наименьшее по отношению к теоретико-множественному включению», т. е. утверждение о том, что $\mathbf{V}(I_l)$ — наименьшее многообразие, означает две вещи:

- $\pi_l(V) \subset \mathbf{V}(I_l)$;
- если Z — *любое другое* аффинное многообразие в $\mathbb{C}^{n-l}$, содержащее $\pi_l(V)$, то $\mathbf{V}(I_l) \subset Z$.

В гл. 4 мы сможем сформулировать эти два свойства так: $\mathbf{V}(I_l)$ является *замыканием Зарисского* множества $\pi_l(V)$. Именно это и дало теореме ее название. Здесь мы не сможем доказать п. (i), так как доказательство использует теорему Гильберта о нулях. Оно будет дано в гл. 4.

Вторая часть теоремы утверждает, что, хотя $\pi_l(V)$ может отличаться от $\mathbf{V}(I_l)$, проекция заполняет «большую часть» многообразия $\mathbf{V}(I_l)$ в том смысле, что разность принадлежит строго меньшему аффинному многообразию. Мы докажем это утверждение в случае $l = 1$. Доказательство в случае $l > 1$ будет дано в § 6 гл. 5.

Нашим главным инструментом будет разложение

$$\mathbf{V}(I_1) = \pi_1 \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$$

из геометрической теоремы о продолжении. Пусть $W = \mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)$. Отметим, что W является аффинным многообразием по лемме 2 из § 2 гл. 1. Из указанного разложения следует, что $\mathbf{V}(I_1) - W \subset \pi_1(V)$, так что если $W \neq \mathbf{V}(I_1)$, то утверждение доказано. Но система (2) показывает, что равенство $W = \mathbf{V}(I_1)$ возможно.

В этом случае нам надо так изменить уравнения, определяющие V, чтобы W уменьшилось. Ключевым моментом здесь является следующий факт:

$$\text{если} \quad W = \mathbf{V}(I_1), \quad \text{то} \quad V = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_s). \tag{3}$$

Это утверждение доказывается следующим образом. Прежде всего, так как мы добавили уравнения, то $\mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_s) \subset \mathbf{V}(f_1, \ldots, f_s) = V$. Докажем обратное включение. Пусть точка $(a_1, \ldots, a_n)$ лежит в V. Каждый полином f_i обращается в нуль в этой точке, а так как $(a_2, \ldots, a_n) \in \pi_1(V) \subset \mathbf{V}(I_1) = W$, то и полиномы g_i в этой точке также равны нулю. Следовательно, $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_s)$. Доказательство утверждения (3) закончено.

Пусть $I = \langle f_1, \ldots, f_s \rangle$ — исходный идеал и $\widetilde{I} = \langle f_1, \ldots, f_s, g_1, \ldots, g_s \rangle$. Отметим, что идеалы I и $\widetilde{I}$ могут не совпадать, хотя многообразия, ими определяемые, совпадают (утверждение (3)). Поэтому и исключающие идеалы I_1 и $\widetilde{I}_1$ также могут различаться. Но так как $\mathbf{V}(I_1)$ и $\mathbf{V}(\widetilde{I}_1)$ оба являются наименьшими многообразиями, содержащими $\pi_1(V)$ (п. (i) теоремы), то $\mathbf{V}(I_1) = \mathbf{V}(\widetilde{I}_1)$.

На следующем шаге мы улучшим базис идеала $\widetilde{I}$. Напомним, что g_i определены следующим образом:

$$f_i = g_i(x_2, \ldots, x_n) x_1^{N_i} + \text{члены, содержащие } x_1 \text{ в степени } < N_i,$$

где $N_i > 0$ и $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ — ненулевые полиномы. Положим

$$\tilde{f}_i = f_i - g_i x_1^{N_i}.$$

Для каждого i или $\tilde{f}_i = 0$, или $\tilde{f}_i$ имеет строго меньшую степень по x_1, чем f_i. Имеем

$$\widetilde{I} = \langle \tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s \rangle.$$

Доказательство этого утверждения мы оставляем читателю.

Теперь применим геометрическую теорему о продолжении к многообразию $V = \mathbf{V}(\tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s)$. Старшие коэффициенты образующих теперь другие, и поэтому мы получаем другое разложение

$$\mathbf{V}(I_1) = \mathbf{V}(\widetilde{I}_1) = \pi_1(V) \cup \widetilde{W},$$

где точки из $\widetilde{W}$ — это те частичные решения, которые обращают в нуль старшие члены полиномов $\tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s$.

Прежде чем продолжать доказательство, рассмотрим пример, показывающий, что $\widetilde{W}$ может быть меньше, чем W. Как и в (2), пусть $I = \langle (y-z)x^2 + xy - 1, (y-z)x^2 + xz - 1 \rangle$. Мы знаем, что $I_1 = \langle y - z \rangle$ и $g_1 = g_2 = y - z$. Поэтому $W = \mathbf{V}(I_1)$. Теперь легко проверить, что

$$\begin{aligned} \widetilde{I} &= \langle (y-z)x^2 + xy - 1, (y-z)x^2 + xz - 1, y - z \rangle = \\ &= \langle xy - 1, xz - 1, y - z \rangle. \end{aligned}$$

Применяя теперь геометрическую теорему о продолжении к $\widetilde{I}$, мы видим, что $\widetilde{W}$ состоит из тех частичных решений, на которых y и z обращаются в нуль, т. е. $\widetilde{W} = \{(0,0)\}$; значит, $\widetilde{W}$ строго меньше, чем $W = \mathbf{V}(I_1)$.

К сожалению, в общем случае мы не можем гарантировать, что $\widetilde{W}$ окажется меньше, чем $W = \mathbf{V}(I_1)$. Равенство $\widetilde{W} = \mathbf{V}(I_1)$ не исключено. В этом случае мы повторяем описанную выше процедуру. Если на каком-то шаге мы получим нечто, строго меньшее, чем $\mathbf{V}(I_1)$, то утверждение доказано.

Осталось рассмотреть, что происходит, когда мы *всегда* получаем $\mathbf{V}(I_1)$. На каждом шаге описанной выше процедуры степень образующих по x_1 уменьшается (или остается равной нулю), так что в конце концов все образующие будут иметь степень 0 по x_1. Это означает, что V определяется полиномами из $\mathbb{C}[x_2, \ldots, x_n]$. Таким образом, если $(a_2, \ldots, a_n)$ — частичное решение, то $(a_1, a_2, \ldots, a_n) \in V$ *для любого* $a_1 \in \mathbb{C}$. Поэтому *любое* частичное решение продолжается, а следовательно, $\pi_1(V) = \mathbf{V}(I_1)$. Но тогда п. (ii) теоремы выполняется для $W = \varnothing$ (именно здесь используется предположение, что $V \neq \varnothing$). Теорема доказана. □

Теорема о замыкании дает частичное описание множества $\pi_l(V)$: эта проекция заполняет многообразие $\mathbf{V}(I_l)$, кроме некоторых точек, лежащих в строго меньшем, чем $\mathbf{V}(I_l)$, многообразии. К сожалению, эти точки не обязательно заполняют все меньшее многообразие. Точную структуру множества $\pi_l(V)$ можно описать следующим образом: существуют аффинные многообразия $Z_i \subset W_i \subset \mathbb{C}^{n-l}, 1 \leq i \leq m$, такие, что

$$\pi_l(V) = \bigcup_{i=1}^{m} (W_i - Z_i).$$

Множества подобного вида называются ***конструктивными***. Это утверждение будет доказано в гл. 5.

В § 1 мы рассмотрели простейший случай теоремы о продолжении, когда один из старших коэффициентов g_i является ненулевой константой. В этом случае g_i *не* могут одновременно обращаться в нуль в точке $(a_2, \ldots, a_n)$, и, следовательно, частичные решения *всегда* продолжаются до полных. Сформулируем геометрическую версию следствия 4 из § 1.

Следствие 4. *Пусть* $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$, *и пусть* f_i *для некоторого* i *имеет вид*

$$f_i = cx_1^N + \textit{члены, содержащие } x_1 \textit{ в степени } < N,$$

где $c \in \mathbb{C}$ *— ненулевая константа и* $N > 0$. *Если* I_1 *— первый исключающий идеал, то в* $\mathbb{C}^{n-1}$ *имеет место равенство*

$$\pi_1(V) = \mathbf{V}(I_1),$$

где π_1 *— отображение проекции на последние* $n-1$ *компонент.*

Наконец, сделаем несколько замечаний об основном поле. Теорема о продолжении и теорема о замыкании (и их следствия) сформулированы для поля комплексных чисел $\mathbb{C}$. В § 6 мы увидим, что теорема продолжения справедлива для любого *алгебраически замкнутого* поля k, а в гл. 4 мы докажем то же утверждение для теоремы о замыкании.

Упражнения к § 2

1. Используя теорему о продолжении и лемму 1, докажите геометрическую теорему о продолжении.
2. Для системы (2) проверьте, что $\langle (y-z)x^2+xy-1, (y-z)x^2+xz-1\rangle = \langle xy-1, xz-1\rangle$. Докажите, что $y-z$ обращается в нуль на всех частичных решениях из $\mathbf{V}(I_1)$.
3. В этой задаче мы проанализируем ход рассуждений в доказательстве теоремы 3 на примере идеала $I = \langle f_1, f_2, f_3\rangle$, где
$$\begin{aligned} f_1 &= yx^3 + x^2, \\ f_2 &= y^3x^2 + y^2, \\ f_3 &= yx^4 + x^2 + y^2. \end{aligned}$$
   (a) Найдите базис Грёбнера для I и докажите, что $I_1 = \langle y^2\rangle$.
   (b) Докажите, что $\mathbf{V}(I_1) = \mathbf{V}(I_1) \cap \mathbf{V}(g_1, g_2, g_3)$, где g_i — коэффициенты при старших степенях переменной x в f_i. В обозначениях теоремы 3 этот результат означает, что $W = \mathbf{V}(I_1)$.
   (c) Пусть $\widetilde{I} = \langle f_1, f_2, f_3, g_1, g_2, g_3\rangle$. Докажите, что $I \neq \widetilde{I}$, хотя $\mathbf{V}(I) = \mathbf{V}(\widetilde{I})$. Также докажите, что $\mathbf{V}(I_1) = \mathbf{V}(\widetilde{I}_1)$.

   (d) Используя метод теоремы 3, постройте новый базис идеала $\widetilde{I}$. С помощью этого базиса докажите, что $\widetilde{W} \neq \mathbf{V}(I_1)$.
4. Пусть $f_i, g_i, h_i \in k[x_1, \ldots, x_n]$, где $1 \leq i \leq s$. Положим $\tilde{f}_i = f_i + g_ih_i$. Докажите, что
$$\langle f_1, \ldots, f_s, g_1, \ldots, g_s\rangle = \langle \tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s\rangle.$$
Объясните, как в доказательстве теоремы 3 используется частный случай этого результата.
5. Покажите на примере, что теорема о замыкании не справедлива для поля $\mathbb{R}$. Рассмотрите идеал
$$I = \langle x^2 + y^2 + z^2 + 2, 3x^2 + 4y^2 + 4z^2 + 5\rangle.$$
Пусть $V = \mathbf{V}(I)$ и π_1 — отображение проекции, отображающее (x, y, z) в (y, z).
   (a) В случае поля $\mathbb{C}$ докажите, что $\mathbf{V}(I_1) = \pi_1(V)$.
   (b) В случае поля $\mathbb{R}$ докажите, что $V = \varnothing$, но $\mathbf{V}(I_1)$ — бесконечное множество. Таким образом, если основное поле не является алгебраически замкнутым, то $\mathbf{V}(I_1)$ может быть значительно больше, чем наименьшее многообразие, содержащее $\pi_1(V)$.

§ 3. Неявное представление

В гл. 1 мы показали, что многообразие V иногда может быть описано параметрическими уравнениями. Смысл *задачи неявного представления* состоит в преобразовании параметрических уравнений в неявные уравнения, определяющие V. Термин «неявное представление» появился в гл. 1, где уравнения, определяющие V, были названы «неявным представлением» многообразия V. Однако к точному определению того, что такое неявное представление, надо подходить с известной осторожностью. Проблема состоит в том, что параметризованной может быть только часть многообразия V — см., например, уравнение (4) из § 3 гл. 1. Поэтому в задаче неявного представления требуется найти уравнения, определяющие *наименьшее* многообразие V, содержащее параметризованное множество. В этом параграфе, используя теорию исключения, развитую в §§ 1 и 2, мы дадим полное решение этой задачи.

Предположим теперь, что наименьшее многообразие V найдено. Здесь сразу возникают два существенных вопроса. Первый: совпадает ли параметризованное множество с V? Второй: если в V есть незапараметризованные точки, то как найти их? Мы увидим, что базисы Грёбнера и теорема о продолжении представляют собой мощные инструменты для решения подобных задач.

В качестве примера рассмотрим касательную поверхность скрученной кубики в $\mathbb{R}^3$, определенную в § 3 гл. 1. Напомним параме-

трическое представление этой поверхности:

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned} \tag{1}$$

В § 8 гл. 2 мы доказали, что множество, параметризованное этими уравнениями, принадлежит многообразию $V \subset \mathbb{R}^3$, заданному уравнением

$$x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2 = 0.$$

Но мы не знаем, является ли V наименьшим многообразием, содержащим касательную поверхность, т. е. в данном случае мы не можем считать решенной задачу неявного представления. Более того, даже если V — наименьшее многообразие, мы не знаем, совпадает V с касательной поверхностью или нет. Таким образом, даже здесь остается еще много работы.

Рассмотрение задачи неявного представления мы начнем со случая *полиномиальной параметризации*

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned} \tag{2}$$

где $f_1, \ldots, f_n$ являются полиномами из $k[t_1, \ldots, t_m]$. Эта система описывает функцию

$$F : k^m \to k^n,$$

определенную формулой

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Тогда $F(k^m) \subset k^n$ — подмножество в k^n, параметризованное уравнениями (2). Множество $F(k^m)$ может не быть аффинным многообразием (примеры будут рассмотрены в упражнениях); поэтому решить задачу неявного представления — это найти наименьшее аффинное многообразие, содержащее $F(k^m)$.

Существует следующая связь между задачей неявного представления и теорией исключения. Уравнения (2) определяют аффинное многообразие $V = \mathbf{V}(x_1 - f_1, \ldots, x_n - f_n) \subset k^{n+m}$. Его точки имеют координаты

$$(t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)),$$

т. е. V может рассматриваться как график функции F. Рассмотрим две функции

$$\begin{aligned} i &: k^m \to k^{n+m}, \\ \pi_m &: k^{n+m} \to k^n, \end{aligned}$$

определенные следующим образом:

$$\begin{aligned} i(t_1, \ldots, t_m) &= (t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)), \\ \pi_m(t_1, \ldots, t_m, x_1, \ldots, x_n) &= (x_1, \ldots, x_n). \end{aligned}$$

Это дает следующую диаграмму множеств и отображений:

$$\begin{array}{ccccc} & & k^{n+m} & & \\ & \overset{i}{\nearrow} & & \overset{\pi_m}{\searrow} & \\ k^m & & \xrightarrow{F} & & k^n \end{array} \tag{3}$$

Отметим, что F является композицией, $F = \pi_m \circ i$. Легко видеть, что $i(k^m) = V$. Таким образом,

$$F(k^m) = \pi_m(i(k^m)) = \pi_m(V). \tag{4}$$

Можно сказать, что параметризованное множество — это проекция графика параметризации. Теперь мы можем использовать теорию исключения для поиска наименьшего многообразия, содержащего $F(k^m)$.

Теорема 1 (полиномиальное неявное представление). *Пусть k — бесконечное поле и $F : k^m \to k^n$ — функция, определенная полиномиальной параметризацией* (2). *Рассмотрим идеал $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subset k[t_1, \ldots, t_m, x_1, \ldots, x_n]$, и пусть $I_m = I \cap k[x_1, \ldots, x_n]$ есть m-й исключающий идеал. Тогда $\mathbf{V}(I_m)$ является наименьшим многообразием в k^n, содержащим $F(k^m)$.*

Доказательство. Рассмотрим многообразие $V = \mathbf{V}(I) \subset k^{n+m}$. Мы уже знаем, что V является графиком функции $F : k^m \to k^n$. Пусть $k = \mathbb{C}$. Так как $F(\mathbb{C}^m) = \pi_m(V)$ в силу (4), то по теореме о замыкании из § 2 многообразие $\mathbf{V}(I_m)$ — это наименьшее многообразие, содержащее $\pi_m(V)$. В случае $k = \mathbb{C}$ теорема доказана.

Пусть теперь k является подполем в $\mathbb{C}$, т. е. $k \subset \mathbb{C}$ и операции в k такие же, как в $\mathbb{C}$. Такие поля всегда содержат кольцо целых чисел $\mathbb{Z}$ (а также поле $\mathbb{Q}$ — почему?) и, значит, являются бесконечными. Так как k строго меньше, чем $\mathbb{C}$, то мы не можем прямо применять теорему о замыкании. Идея состоит в замене k на $\mathbb{C}$, а потом в возвращении к k. Индекс k или $\mathbb{C}$ будет указывать, с каким полем мы работаем. Таким образом, $\mathbf{V}_k(I_m)$ — это многообразие в k^n, а $\mathbf{V}_{\mathbb{C}}(I_m)$ — это большее множество решений в $\mathbb{C}^n$. (Следует отметить, что переход к большему полю не меняет исключающего идеала I_m, потому что на алгоритм, вычисляющий I_m, не влияет переход от k к $\mathbb{C}$.) Нам нужно доказать, что $\mathbf{V}_k(I_m)$ — это наименьшее многообразие в k^n, содержащее $F(k^m)$.

Из равенства (4) и леммы 1 из § 2 следует, что $F(k^m) = \pi_m(V_k) \subset \mathbf{V}_k(I_m)$. Рассмотрим произвольное многообразие $Z_k = \mathbf{V}_k(g_1, \ldots, g_s) \subset k^n$, содержащее $F(k^m)$. Требуется доказать, что

$\mathbf{V}_k(I_m) \subset Z_k$. По определению Z_k полиномы g_i обращаются в нуль на Z_k; значит, они равны нулю и на меньшем множестве $F(k^m)$. Это показывает, что $g_i \circ F$ обращаются в нуль на всем k^m. Но g_i — полиномы из $k[x_1, \dots, x_n]$, а $F = (f_1, \dots, f_n)$ — вектор полиномов из $k[t_1, \dots, t_m]$. Следовательно, $g_i \circ F \in k[t_1, \dots, t_m]$.

Таким образом, $g_i \circ F$ — это полиномы, тождественно равные нулю на k^m. Но так как поле k бесконечно, то по предложению 5 из § 1 гл. 1 полиномы $g_i \circ F$ нулевые. В частности, это означает, что $g_i \circ F$ обращаются в нуль на $\mathbb{C}^m$, а значит, g_i равны нулю на $F(\mathbb{C}^m)$. Следовательно, $Z_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(g_1, \dots, g_s) \subset \mathbb{C}^n$ — многообразие, содержащее $F(\mathbb{C}^m)$. Так как теорема справедлива над $\mathbb{C}$, то $\mathbf{V}_{\mathbb{C}}(I_m) \subset Z_{\mathbb{C}}$. Отсюда следует, что $\mathbf{V}_{\mathbb{C}}(I_m) \cap k^n \subset Z_{\mathbb{C}} \cap k^n$. Но это включение в точности означает, что $\mathbf{V}_k(I_m) \subset Z_k$. Это доказывает, что $V_k(I_m)$ — наименьшее среди всех многообразий в k^n, содержащих $F(k^m)$.

Пусть теперь k не содержится в $\mathbb{C}$; тогда существует алгебраически замкнутое поле K, содержащее k, $k \subset K$ (см., например, учебник LANG (1965)). Как мы отмечали в конце § 2, теорема о замыкании справедлива над любым алгебраически замкнутым полем. Теперь осталось заменить в наших рассуждениях $\mathbb{C}$ на K. □

Теорема 1 позволяет сконструировать следующий *алгоритм построения неявного представления для полиномиальной параметризации*: пусть даны параметрические уравнения $x_i = f_i(t_1, \dots, t_m)$, где $f_1, \dots, f_n \in k[t_1, \dots, t_m]$. Рассмотрим идеал $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle$ и найдем его базис Грёбнера по отношению к lex-упорядочению, где каждое t_i больше любого x_j. По теореме об исключении элементы базиса, не зависящие от $t_1, \dots, t_m$, образуют базис Грёбнера идеала I_m, и по теореме 1 они определяют наименьшее многообразие в k^n, содержащее параметризованное множество.

В качестве примера рассмотрим касательную поверхность скрученной кубики в $\mathbb{R}^3$, которая параметрически задана уравнениями (1). Рассмотрим идеал

$$I = \langle x - t - u, y - t^2 - 2tu, z - t^3 - 3t^2u \rangle \subset \mathbb{R}[t, u, x, y, z].$$

Его базис Грёбнера для lex-упорядочения с $t > u > x > y > z$ имеет вид

$$\begin{aligned}
g_1 &= t + u - x, \\
g_2 &= u^2 - x^2 + y, \\
g_3 &= ux^2 - uy - x^3 + (3/2)xy - (1/2)z, \\
g_4 &= uxy - uz - x^2y - xz - 2y^2, \\
g_5 &= uxz - uy^2 + x^2z - (1/2)xy^2 - (1/2)yz, \\
g_6 &= uy^3 - uz^2 - 2x^2yz + (1/2)xy^3 - xz^2 + (5/2)y^2z, \\
g_7 &= x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2.
\end{aligned}$$

Теорема об исключении утверждает, что $I_2 = I \cap \mathbb{R}[x, y, z] = \langle g_7 \rangle$, т. е. по теореме 1 многообразие $\mathbf{V}(g_7)$ решает задачу неявного представления для касательной поверхности скрученной кубики. Уравнение $g_7 = 0$ уже рассматривалось в начале этого параграфа, но теперь мы знаем, что оно определяет наименьшее многообразие в $\mathbb{R}^3$, содержащее эту касательную поверхность.

Но мы по-прежнему не знаем, *совпадает ли* касательная поверхность с $\mathbf{V}(g_7)$. Чтобы понять это, мы должны проверить, какие частичные решения $(x, y, z) \in \mathbf{V}(g_7) = \mathbf{V}(I_2)$ продолжаются до решений $(t, u, x, y, z) \in \mathbf{V}(I)$. Сначала мы будем работать над $\mathbb{C}$, чтобы можно было использовать теорему о продолжении. Мы сделаем два шага продолжения — на каждом шаге решение, как обычно, продолжается на одну координату.

Пусть $(x, y, z) \in \mathbf{V}(I_2) = \mathbf{V}(g_7)$. В § 1 отмечалось, что I_2 можно рассматривать как первый исключающий идеал для $I_1 = \langle g_2, \dots, g_7 \rangle$. Теперь теорема о продолжении (в форме следствия 4 § 2) утверждает, что (x, y, z) всегда может быть продолжено до $(u, x, y, z) \in \mathbf{V}(I_1)$, так как I_1 имеет образующий элемент с постоянным старшим коэффициентом при u (найдите его). На следующем шаге мы переходим от $(u, x, y, z) \in \mathbf{V}(I_1)$ к $(t, u, x, y, z) \in \mathbf{V}(I)$; здесь опять-таки следствие 4 § 2 обеспечивает продолжаемость частичного решения ($g_1 = t + u - x$ имеет постоянный старший коэффициент по t). Таким образом, мы доказали, что касательная поверхность скрученной кубики совпадает с многообразием $\mathbf{V}(g_7)$ в $\mathbb{C}^3$.

Осталось понять, что происходит над $\mathbb{R}$. Если мы возьмем вещественное частичное решение $(x, y, z) \in \mathbb{R}^3$ уравнения $g_7 = 0$, то, как мы знаем, оно продолжается до полного решения $(t, u, x, y, z) \in \mathbf{V}(I) \subset \mathbb{C}^5$. Но являются ли параметры t и u вещественными? Это не очевидно. Однако рассмотрение базиса Грёбнера показывает, что t и u вещественны, если $(x, y, z) \in \mathbb{R}^3$ (упр. 4), т. е. касательная поверхность скрученной кубики в $\mathbb{R}^3$ совпадает с многообразием, определенным уравнением

$$x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2 = 0.$$

В общем случае на вопрос о том, совпадает ли параметризованное множество с минимальным многообразием, ответить трудно. Каждый случай приходится рассматривать отдельно. Но разобранный выше пример показывает, что совместное применение базиса Грёбнера и теоремы о продолжении позволяет значительно прояснить суть вопроса в каждом отдельном случае.

До сих пор мы рассматривали только полиномиальную параметризацию. Теперь будем рассматривать параметризацию, заданную рациональными функциями. Следующий пример демонстри-

рует возникающие здесь трудности:

$$x = \frac{u^2}{v},$$
$$y = \frac{v^2}{u}, \tag{5}$$
$$z = u.$$

Легко проверить, что точка (x, y, z) всегда лежит на поверхности $x^2y = z^3$. Посмотрим, что происходит, если мы избавимся от знаменателей в системе (5) и попытаемся применить теорему о полиномиальном неявном представлении. Мы должны рассмотреть идеал

$$I = \langle vx - u^2, uy - v^2, z - u\rangle \subset k[u, v, x, y, z].$$

Легко показать (сделайте это как упражнение), что $I_2 = I \cap k[x, y, z] = \langle z(x^2y - z^3)\rangle$. Отсюда следует, что

$$\mathbf{V}(I_2) = \mathbf{V}(x^2y - z^3) \cup \mathbf{V}(z),$$

т. е. $\mathbf{V}(I_2)$ *не* является наименьшим многообразием, содержащим параметризованное множество. Значит, идеал I — это не то, что нам нужно: «избавиться от знаменателей» — это слишком наивно. Чтобы построить идеал, с которым можно работать, надо действовать тоньше.

В общем случае рациональная параметризация задается системой

$$x_1 = \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)},$$
$$\vdots \tag{6}$$
$$x_n = \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)},$$

где $f_1, g_1, \ldots, f_n, g_n \in k[t_1, \ldots, t_m]$. Отображение $F : k^m \to k^n$, заданное системой (6), не обязательно определено на всем k^m, потому что знаменатели могут обращаться в нуль. Пусть $W = \mathbf{V}(g_1 g_2 \ldots g_n) \subset k^m$; тогда

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}\right)$$

задает отображение

$$F : k^m - W \to k^n.$$

Решить задачу неявного представления — это значит найти наименьшее многообразие в k^n, содержащее $F(k^m - W)$.

Диаграмма (3) в нашем случае имеет вид

$$\begin{array}{ccc} & & k^{n+m} \\ & {\scriptstyle i}\nearrow & \\ k^m - W & \xrightarrow{F} & k^n \end{array} \qquad \searrow^{\pi_m} \tag{7}$$

Легко проверить включение $i(k^m - W) \subset \mathbf{V}(I)$, где $I = \langle g_1x_1 - f_1, \ldots, g_nx_n - f_n\rangle$ — идеал, построенный «избавлением от знаменателей». Проблема состоит в том, что $\mathbf{V}(I)$ *не* обязательно является наименьшим многообразием, содержащим $i(k^m - W)$ (как, например, в случае параметризации (5), подробно рассмотренной в упражнениях).

Чтобы избежать этой неприятности, мы изменим I с помощью добавления лишней размерности для контроля знаменателей. Рассмотрим полиномиальное кольцо $k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$, соответствующее аффинному пространству k^{n+m+1}. Пусть $g = g_1 \cdot g_2 \ldots g_n$; тогда $W = \mathbf{V}(g)$. Теперь рассмотрим идеал

$$J = \langle g_1x_1 - f_1, \ldots, g_nx_n - f_n, 1 - gy\rangle \subset k[y, t_1, \ldots, t_m, x_1, \ldots, x_n].$$

Уравнение $1 - gy = 0$ означает, что знаменатели $g_1, \ldots, g_n$ не равны нулю на $\mathbf{V}(J)$. Диаграмма (7) в этой новой ситуации должна быть преобразована. Для этого рассмотрим отображения

$$j : k^m - W \to k^{n+m+1},$$
$$\pi_{m+1} : k^{n+m+1} \to k^n,$$

заданные формулами

$$j(t_1, \ldots, t_m) = \left(\frac{1}{g(t_1, \ldots, t_m)}, t_1, \ldots, t_m, \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}\right),$$
$$\pi_{m+1}(y, t_1, \ldots, t_m, x_1, \ldots, x_n) = (x_1, \ldots, x_n).$$

Тогда диаграмма имеет вид

$$\begin{array}{ccc} & & k^{n+m+1} \\ & {\scriptstyle j}\nearrow & \\ k^m - W & \xrightarrow{F} & k^n \end{array} \qquad \searrow^{\pi_{m+1}}$$

Как и выше, $F = \pi_{m+1} \circ j$. Но удивительно, что $j(k^m - W) = \mathbf{V}(J)$ в k^{n+m+1}. Легко видеть, что $j(k^m - W) \subset \mathbf{V}(J)$ — это сразу следует из определений j и J. С другой стороны, если $(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in \mathbf{V}(J)$, то из уравнения $g(t_1, \ldots, t_m)y = 1$ следует, что *ни один* полином g_i не обращается в нуль в точке $(t_1, \ldots, t_m)$; значит, равенства $g_i(t_1, \ldots, t_m)x_i = f_i(t_1, \ldots, t_m)$ могут быть разрешены относительно x_i: $x_i = f_i(t_1, \ldots, t_m)/g_i(t_1, \ldots, t_m)$.

Так как $y = 1/g(t_1, \ldots, t_m)$, то эта точка принадлежит множеству $j(k^m - W)$, т. е. $\mathbf{V}(J) \subset j(k^m - W)$.

Теперь из равенств $F = \pi_{m+1} \circ j$ и $j(k^m - W) = \mathbf{V}(J)$ получаем

$$F(k^m - W) = \pi_{m+1}(j(k^m - W)) = \pi_{m+1}(\mathbf{V}(J)). \tag{8}$$

То есть параметризованное множество равно проекции многообразия $\mathbf{V}(J)$. Как и в полиномиальном случае, теперь мы можем применить теорию исключения для решения задачи неявного представления.

Теорема 2 (рациональное неявное представление). *Пусть k — бесконечное поле, а $F : k^m - W \to k^n$ — функция, заданная рациональной параметризацией* (6). *Рассмотрим идеал $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \subset k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$, где $g = g_1 \cdot \ldots \cdot g_n$, и пусть $J_{m+1} = J \cap k[x_1, \ldots, x_n]$ есть $(m+1)$-й исключающий идеал. Тогда $\mathbf{V}(J_{m+1})$ — это наименьшее многообразие в k^n, содержащее $F(k^m - W)$.*

Доказательство. Доказательство этой теоремы повторяет доказательство теоремы 1, только нужно использовать уравнение (8) вместо уравнения (4). Единственный нетривиальный момент — это утверждение, что полином, равный нулю на $k^m - W$, является нулевым полиномом. Доказательство этого утверждения подробно разобрано в упражнениях. □

Суть теоремы 2 состоит в следующем: рассмотрим рациональную параметризацию (6), избавимся от знаменателей и добавим уравнение (и новую переменную y), чтобы не дать знаменателям обратиться в нуль:

$$\begin{aligned} g_1 x_1 &= f_1, \\ &\vdots \\ g_n x_n &= f_n, \\ g_1 g_2 \ldots g_n y &= 1. \end{aligned}$$

Тогда исключение переменных $y, t_1, \ldots, t_m$ решает задачу неявного представления.

Более точно можно сказать так: теорема 2 определяет *алгоритм построения неявного представления в случае рациональной параметризации*. А именно, пусть $x_i = f_i/g_i$, где $f_1, g_1, \ldots, f_n, g_n \in k[t_1, \ldots, t_m]$. Введем новую переменную y и рассмотрим идеал $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle$, где $g = g_1 \ldots g_n$. Найдем базис Грёбнера идеала J по отношению к lex-упорядочению, где y и каждое t_i больше любого x_j. Элементы базиса Грёбнера, не зависящие от $y, t_1, \ldots, t_m$, определяют в k^n наименьшее многообразие, содержащее параметризованное множество.

Посмотрим, как работает этот алгоритм, на примере параметризации (5). Обозначим через w новую переменную. Тогда

$$J = \langle vx - u^2, uy - v^2, z - u, 1 - uvw \rangle \subset k[w, u, v, x, y, z].$$

Легко проверить, что $J_3 = J \cap k[x, y, z] = \langle x^2 y - z^3 \rangle$, т. е. $\mathbf{V}(x^2 y - z^3)$ и есть многообразие, определенное параметризацией (5). В упражнениях мы увидим какую часть этого многообразия составляет параметризованное множество.

Следует упомянуть, что на практике задачи неявного представления часто решаются с помощью результантов. Задача неявного представления для кривых и поверхностей рассматривается в работах ANDERSON, GOLDMAN, SEDERBERG (1984a, 1984b). В недавней работе CANNY, MANOCHA (1993) показано, как задачи неявного представления параметрических поверхностей могут быть решены с использованием мультиполиномиальных результантов.

Упражнения к § 3

1. Докажите аккуратно, что в диаграмме (3) $F = \pi_m \circ i$ и $i(k^m) = V$.
2. Если $k = \mathbb{C}$, то теорема 1 может быть усилена. А именно, используя теорему о замыкании, докажите, что существует многообразие $W \subset \mathbf{V}(I_m), W \neq \mathbf{V}(I_m)$, такое, что $\mathbf{V}(I_m) - W \subset F(\mathbb{C}^m)$.
3. Приведите пример, показывающий, что результат упр. 2 не верен над $\mathbb{R}$. Указание: t^2 в вещественном случае всегда положительно.
4. В этом параграфе было доказано, что над $\mathbb{C}$ касательная поверхность скрученной кубики задается уравнением

$$g_7 = x^3 z - (3/4)x^2 y^2 - (3/2)xyz + y^3 + (1/4)z^2 = 0.$$

Мы хотим доказать, что то же самое верно над $\mathbb{R}$. Пусть (x, y, z) — вещественное решение этого уравнения. Тогда мы доказали (используя теорему о продолжении), что существуют $t, u \in \mathbb{C}$, такие, что

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2 u. \end{aligned}$$

С использованием базиса Грёбнера (приведенного в тексте), докажите, что t и u вещественны. Это докажет, что точка (x, y, z) лежит на рассматриваемой касательной поверхности в $\mathbb{R}^3$. Указание: докажите сначала вещественность u.

5. В задаче о касательной поверхности скрученной кубики докажите, что параметры t и u однозначно определены параметрами x, y, z. Указание: используйте метод упр. 4.

6. Пусть S — параметрическая поверхность, заданная системой

$$\begin{aligned} x &= uv, \\ y &= u^2, \\ z &= v^2. \end{aligned}$$

   (a) Найдите уравнение наименьшего многообразия V, содержащего S.
   (b) В случае поля $\mathbb{C}$, используя теорему о продолжении, докажите, что $S = V$. Указание: это делается так же, как и в случае касательной поверхности скрученной кубики.
   (c) В случае поля $\mathbb{R}$ покажите, что S есть только «половина» многообразия V. Какая параметризация описывает другую «половину»?

7. Пусть S — параметрическая поверхность, заданная системой

$$\begin{aligned} x &= uv, \\ y &= uv^2, \\ z &= u^2. \end{aligned}$$

   (a) Найдите уравнение наименьшего многообразия V, содержащего S.
   (b) В случае поля $\mathbb{C}$ покажите, что V содержит точки, не принадлежащие S. Определите, какие именно точки из V не принадлежат S. Указание: используйте lex-упорядочение с $u > v > x > y > z$.

8. *Поверхность Эннепера* задается следующей параметрической системой:

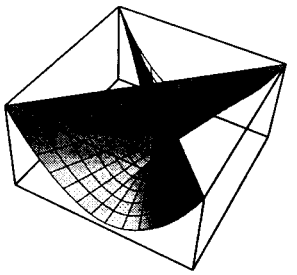
$$\begin{aligned} x &= 3u + 3uv^2 - u^3, \\ y &= 3v + 3u^2v - v^3, \\ z &= 3u^2 - 3v^2. \end{aligned}$$

   (a) Найдите уравнение наименьшего многообразия V, содержащего поверхность Эннепера. Это будет очень сложное уравнение!
   (b) Используя теорему о продолжении (над $\mathbb{C}$), докажите, что указанные параметрические уравнения параметризуют всю поверхность V. Указание: в базисе Грёбнера много элементов, среди них найдутся нужные.

9. *Зонтик Уитни* задан следующей параметрической системой:

$$\begin{aligned} x &= uv, \\ y &= v, \\ z &= u^2. \end{aligned}$$

Вот рисунок этой поверхности:



   (a) Найдите уравнение наименьшего многообразия, содержащего зонтик Уитни.
   (b) Докажите, что параметризованное множество совпадает с этим многообразием над $\mathbb{C}$ и не совпадает над $\mathbb{R}$. Какие именно точки многообразия не параметризованы над $\mathbb{R}$?
   (c) Докажите, что параметры u и v не всегда определены однозначно значениями x, y и z. Найдите точки, в которых нет однозначности; укажите положение этих точек на рисунке.

10. Рассмотрим кривую в $\mathbb{C}^n$, параметризованную уравнениями $x_i = f_i(t)$, где $f_1, \dots, f_n \in \mathbb{C}[t]$, и идеал

$$I = \langle x_1 - f_1(t), \dots, x_n - f_n(t) \rangle \subset \mathbb{C}[t, x_1, \dots, x_n].$$

   (a) Докажите, что параметризованное множество совпадает с многообразием $\mathbf{V}(I_1) \subset \mathbb{C}^n$.
   (b) Покажите, что утверждение п. (a) может быть неверным, если f_i — рациональные функции. Указание: см. § 3 гл. 1.
   (c) Покажите, что утверждение п. (a) может быть неверным, если мы работаем над $\mathbb{R}$ (даже если f_i — полиномы).

11. В этом упражнении рассматривается доказательство теоремы 2.
   (a) Пусть k — бесконечное поле и $f, g \in k[t_1, \dots, t_m]$. Предположим, что $g \neq 0$, а f обращается в нуль на $k^m - \mathbf{V}(g)$. Докажите, что f — нулевой полином. Указание: рассмотрите произведение fg.
   (b) Докажите теорему 2, используя схему доказательства, рассмотренную в тексте параграфа.

12. Рассмотрим параметризацию (5). Пусть $k = \mathbb{C}$, и пусть $I = \langle vx - u^2, uy - v^2, z - u \rangle$ — идеал, полученный «избавлением от знаменателей».
   (a) Докажите, что $I_2 = \langle z(x^2y - z^3) \rangle$.
   (b) Докажите, что наименьшим многообразием в $\mathbb{C}^5$, содержащим $i(\mathbb{C}^2 - W)$ (см. диаграмму (7)) является $\mathbf{V}(vx - u^2, yu - v^2, z - u, x^2y - z^3, vz - xy)$. Указание: докажите, что $i(\mathbb{C}^2 - W) = \pi_1(\mathbf{V}(J))$, а затем примените теорему о замыкании.

(c) Докажите, что $\{(0,0,x,y,0) : x, y \text{ любые}\} \subset \mathbf{V}(I)$, и выведите отсюда, что $\mathbf{V}(I)$ *не* является наименьшим многообразием, содержащим $i(\mathbb{C}^2 - W)$.

(d) Определите, какая именно часть многообразия $\mathbf{V}(x^2y - z^3)$ параметризована системой (5).

13. Рассмотрим рациональную параметризацию вида (6). Существует один случай, когда «наивный» идеал $I = \langle g_1x_1 - f_1, \ldots, g_nx_n - f_n\rangle$, полученный «избавлением от знаменателей», дает правильный ответ в задаче неявного представления. Пусть t — единственный параметр, $x_i = f_i(t)/g_i(t)$. Предположим, что f_i и g_i взаимно просты в $k[t]$ для каждого i (в частности, не имеют общих корней). Пусть $I \subset k[t, x_1, \ldots, x_n]$ определен, как выше. Докажите, что $\mathbf{V}(I_1)$ является наименьшим многообразием, содержащим $F(k - W)$. Как обычно, $g = g_1 \ldots g_n \in k[t]$ и $W = \mathbf{V}(g) \subset k$. Указание: докажите, что в диаграмме (7) $i(k^m - W) = \mathbf{V}(I)$, а затем используйте доказательство теоремы 1.

14. *Декартов лист* задан следующей параметрической системой:

$$x = \frac{3t}{1+t^3},$$
$$y = \frac{3t^2}{1+t^3}.$$

(a) Найдите уравнение декартова листа. Указание: используйте упр. 13.

(b) Докажите, что и над $\mathbb{C}$, и над $\mathbb{R}$ параметризованное множество совпадает со всей кривой.

15. В упр. 16 к § 3 гл. 1 мы рассматривали параметрические уравнения над $\mathbb{R}$

$$x = \frac{(1-t)^2x_1 + 2t(1-t)wx_2 + t^2x_3}{(1-t)^2 + 2t(1-t)w + t^2},$$
$$y = \frac{(1-t)^2y_1 + 2t(1-t)wy_2 + t^2y_3}{(1-t)^2 + 2t(1-t)w + t^2},$$

где $w, x_1, y_1, x_2, y_2x_3, y_3$ — константы и $w > 0$. Исключая t, покажите, что эти уравнения описывают часть некоторого конического сечения. Напомним, что коническое сечение задается уравнением вида

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Указание: в большинстве систем компьютерной алгебры базис Грёбнера можно вычислять, когда коэффициенты полиномов зависят от параметров, таких, как $w, x_1, y_1, x_2, y_2, x_3, y_3$. Так как мы работаем над $\mathbb{R}$ и, следовательно, знаменатели не обращаются в нуль, то можно использовать результат упр. 13.

§ 4. Особые точки и огибающие

В этом параграфе будут рассмотрены две темы геометрии:

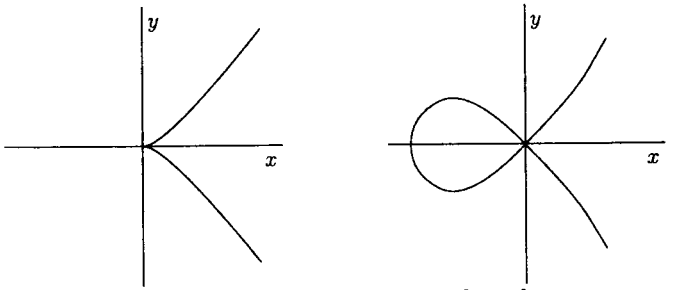
- *особые точки* на кривой,
- *огибающая* семейства кривых.

Мы хотим показать, как геометрические задачи приводят к интересным уравнениям, которые могут быть решены с использованием техники, развитой в §§ 1 и 2.

Мы изложим основы теории особых точек и огибающих, но далеко не в полном объеме. На эти темы можно написать целую книгу (см., например, BRUCE, GIBLIN (1992)). Кроме того, теория огибающих будет излагаться не вполне строго. Чтобы обосновать наши рассмотрения, мы будем опираться на некоторые идеи из математического анализа, чтобы сделать наши рассуждения полностью корректными.

Особые точки

Пусть дана кривая на плоскости k^2, определенная уравнением $f(x,y) = 0$, где $f \in k[x,y]$. Мы ожидаем, что многообразие $\mathbf{V}(f)$ будет иметь корректно определенную касательную в большинстве точек, но касательной может не быть в точках самопересечения или излома. Вот два примера:



$y^2 = x^3$ $\qquad$ $y^2 = x^2(1+x)$

Если мы потребуем, чтобы касательная была единственной и «примыкала» к кривой по обе стороны от точки касания, то каждая из кривых на рисунке содержит точку, в которой касательной нет. Интуитивно *особая точка* многообразия $\mathbf{V}(f)$ — это такая точка, в которой касательная отсутствует.

Прежде чем давать строгое определение, дадим алгебраическое определение касательной. Поступим следующим образом. Рассмотрим точку $(a,b) \in \mathbf{V}(f)$ и прямую L, проходящую через эту точку

и заданную параметрически:

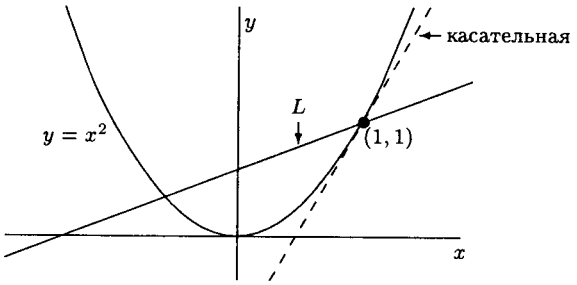
$$\begin{aligned} x &= a + ct, \\ y &= b + dt. \end{aligned} \tag{1}$$

Эта прямая проходит через (a, b) при $t = 0$. Отметим, что $(c, d) \neq (0, 0)$ — это вектор, параллельный указанной прямой. Меняя (c, d), мы можем получить все прямые, проходящие через (a, b). Но как выделить среди них *касательную* к $\mathbf{V}(f)$? Можем ли мы сделать это, не используя аналитических соображений?

Рассмотрим пример. Пусть дана прямая L, заданная параметрическими уравнениями

$$\begin{aligned} x &= 1 + ct, \\ y &= 1 + dt \end{aligned} \tag{2}$$

и проходящая через точку $(1, 1)$ на параболе $y = x^2$:



Из анализа мы знаем, что касательная имеет тангенс наклона 2, т. е. $d = 2c$. Чтобы найти эту прямую из алгебраических соображений, мы будем исследовать *полином*, описывающий пересечение прямой и параболы. Подставим (2) в уравнение $y - x^2 = 0$. Получаем

$$g(t) = 1 + dt - (1 + ct)^2 = -c^2t^2 + (d - 2c)t = t(-c^2t + d - 2c). \tag{3}$$

Его корни описывают точки пересечения прямой и параболы (уясните себе этот важный момент). Если $d \neq 2c$, то g имеет два различных корня при $c \neq 0$ и один корень при $c = 0$. Но если $d = 2c$, то g имеет один корень кратности 2. Другими словами, прямая (2) является касательной к параболе, если g имеет *кратный корень*.

Теперь можно дать определение.

Определение 1. Пусть l — натуральное число. Рассмотрим точку $(a, b) \in \mathbf{V}(f)$ и прямую L, проходящую через эту точку. Мы говорим, что L *пересекает* $\mathbf{V}(f)$ *с кратностью* l *в* (a, b), если L допускает параметризацию вида (1), такую, что $t = 0$ является корнем кратности l полинома $g(t) = f(a + ct, b + dt)$.

Отметим, что $g(0) = f(a, b) = 0$, т. е. $t = 0$ — корень полинома g. Напомним, что $t = 0$ называется корнем кратности l, если $g = t^l h$, где $h(0) \neq 0$. Это определение, однако, содержит одну неясность: прямая имеет много разных параметризаций, т. е. надо проверить, что кратность не зависит от параметризации. Этот вопрос будет рассмотрен в упражнениях.

Вернемся к прямой (2). Из (3) следует, что она пересекает параболу $y = x^2$ в точке $(1, 1)$ с кратностью 1, если $d \neq 2c$, и с кратностью 2, если $d = 2c$. Другие примеры будут рассмотрены в упражнениях.

Мы будем применять понятие кратности для того, чтобы строить касательные. Для этого нам потребуется *градиент* полинома f, т. е. вектор, определенный следующим равенством:

$$\nabla f = \left(\frac{\partial}{\partial x} f, \frac{\partial}{\partial y} f \right).$$

Теперь мы можем сформулировать утверждение.

Предложение 2. *Пусть* $f \in k[x, y]$ *и* $(a, b) \in \mathbf{V}(f)$.

(i) *Если* $\nabla f(a, b) \neq (0, 0)$, *то существует единственная прямая, проходящая через* (a, b), *которая пересекает* $\mathbf{V}(f)$ *с кратностью, большей или равной* 2.

(ii) *Если* $\nabla f(a, b) = (0, 0)$, *то любая прямая, проходящая через* (a, b), *пересекает* $\mathbf{V}(f)$ *с кратностью* ≥ 2.

Доказательство. Пусть прямая L, проходящая через (a, b), параметризована уравнениями (1), и пусть $g(t) = f(a + ct, b + dt)$. Так как $(a, b) \in \mathbf{V}(f)$, то $t = 0$ является корнем полинома g. Следующее утверждение будет доказано в упражнениях:

$$t = 0 \text{ является корнем полинома } g \text{ кратности } \geq 2 \iff g'(0) = 0. \tag{4}$$

Имеем по правилу дифференцирования

$$g'(t) = \frac{\partial}{\partial x} f(a + ct, b + dt) \cdot c + \frac{\partial}{\partial y} f(a + ct, b + dt) \cdot d,$$

т. е.

$$g'(0) = \frac{\partial}{\partial x} f(a, b) \cdot c + \frac{\partial}{\partial y} f(a, b) \cdot d.$$

Отсюда следует, что если $\nabla f(a, b) = (0, 0)$, то и $g'(0) = 0$. По (4) из этого следует, что L пересекает $\mathbf{V}(f)$ с кратностью ≥ 2. Это доказывает вторую часть предложения. Докажем первую часть. Пусть $\nabla f(a, b) \neq (0, 0)$. Мы знаем, что $g'(0) = 0$ в том и только том случае,

когда

$$\frac{\partial}{\partial x}f(a,b)\cdot c+\frac{\partial}{\partial y}f(a,b)\cdot d=0. \tag{5}$$

Это линейное уравнение с неизвестными c и d. Так как коэффициенты $\frac{\partial}{\partial x}f(a,b)$ и $\frac{\partial}{\partial y}f(a,b)$ не обращаются одновременно в нуль, то пространство решений одномерно, т. е. существует решение $(c_0,d_0)\neq(0,0)$, такое, что (c,d) является решением в том и только том случае, когда $(c,d)=\lambda(c_0,d_0)$ для некоторого $\lambda\in k$. Значит, решения (c,d) параметризуют одну и ту же прямую. Это доказывает единственность прямой, пересекающей $\mathbf{V}(f)$ с кратностью ≥ 2. Предложение 2 доказано. □

Предложение 2 позволяет дать строгое определение касательной. Вторая часть предложения объясняет, что такое особая точка.

Определение 3. Пусть $f\in k[x,y]$ и $(a,b)\in\mathbf{V}(f)$.

(i) Если $\nabla f(a,b)\neq(0,0)$, то *касательной* к $\mathbf{V}(f)$ в точке (a,b) называется единственная прямая, проходящая через (a,b) и пересекающая $\mathbf{V}(f)$ с кратностью ≥ 2. В этом случае мы скажем, что точка (a,b) является *неособой точкой* многообразия $\mathbf{V}(f)$.

(ii) Если $\nabla f(a,b)=(0,0)$, то (a,b) называется *особой точкой* многообразия $\mathbf{V}(f)$.

Над $\mathbb{R}$ касательная и градиент имеют следующую геометрическую интерпретацию. Если касательная к $\mathbf{V}(f)$ в точке (a,b) параметризована уравнениями (1), то вектор (c,d) параллелен касательной. Уравнение (5) означает, что скалярное произведение $(\nabla f(a,b),(c,d))$ равно нулю, т. е. градиент перпендикулярен вектору (c,d). Таким образом, мы получили алгебраическое доказательство теоремы из анализа, утверждающей, что *градиент* $\nabla f(a,b)$ *перпендикулярен касательной к* $\mathbf{V}(f)$ *в точке* (a,b).

Если задана кривая $\mathbf{V}(f)$, то ее особые точки можно найти следующим образом. Равенство нулю градиента ∇f означает, что обе частные производные $\frac{\partial}{\partial x}f$ и $\frac{\partial}{\partial y}f$ равны нулю одновременно. Так как особая точка принадлежит кривой $\mathbf{V}(f)$, то равенство $f=0$ также выполняется. Отсюда следует, что особые точки многообразия $\mathbf{V}(f)$ — это решения системы уравнений

$$f=\frac{\partial}{\partial x}f=\frac{\partial}{\partial y}f=0.$$

Рассмотрим, например, кривую $y^2=x^2(1+x)$ (представленную на рисунке выше). Чтобы найти ее особые точки, нужно решить

систему

$$f=y^2-x^2-x^3=0,$$
$$\frac{\partial}{\partial x}f=-2x-3x^2=0,$$
$$\frac{\partial}{\partial y}f=2y=0.$$

Легко видеть, что эта система имеет единственное решение $(0,0)$, т. е. $(0,0)$ — единственная особая точка многообразия $\mathbf{V}(y^2-x^2-x^3)$, что согласуется с графиком кривой на рисунке.

Используя методы, развитые в §§ 1 и 2, мы можем решать и более сложные задачи. Например, немного позже в этом параграфе мы найдем особые точки кривой, заданной уравнениями шестого порядка

$$\begin{aligned}0=&-1156+688x^2-191x^4+16x^6+544y+30x^2y-40x^4y\\&+225y^2-96x^2y^2+16x^4y^2-136y^3-32x^2y^3+16y^4.\end{aligned}$$

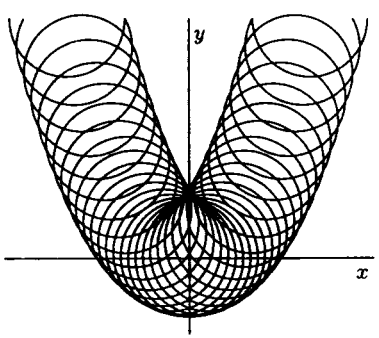
В упражнениях будут рассмотрены другие задачи, связанные с особыми точками. В гл. 9 мы будем изучать особые и неособые точки на произвольном аффинном многообразии.

Огибающие

Огибающие мы будем рассматривать над основным полем $\mathbb{R}$, чтобы геометрический аспект этой теории был наглядным. Лучший способ объяснить, что такое огибающая, — это рассмотреть пример. Пусть $t\in\mathbb{R}$. Рассмотрим окружность в $\mathbb{R}^2$, заданную уравнением

$$(x-t)^2+(y-t^2)^2=4. \tag{6}$$

Так как формула (t,t^2) параметризует параболу, мы можем считать, что уравнение (6) описывает *семейство* окружностей радиуса 4, центры которых лежат на параболе $y=x^2$. Выглядит это так:



Семейство окружностей на плоскости

Заметим, что «граничная» кривая *одновременно касается* всех окружностей семейства. Это пример *огибающей* семейства кривых. Основная идея состоит в том, что огибающая — это кривая, которая касается всех кривых некоторого семейства. Мы хотим изучить свойства огибающих и научиться находить их уравнения, в частности, найти уравнение огибающей только что рассмотренного семейства.

Прежде чем дать определение огибающей, нам нужно разобраться с понятием *семейства* кривых в $\mathbb{R}^2$.

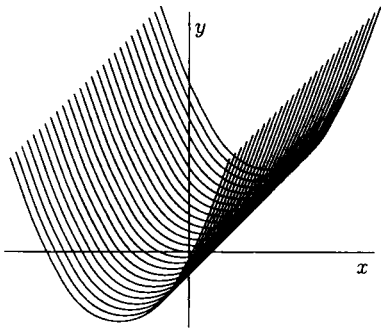
Определение 4. Рассмотрим полином $F \in \mathbb{R}[x, y, t]$ и зафиксируем $t \in \mathbb{R}$. Тогда многообразие в $\mathbb{R}^2$, заданное уравнением $F(x, y, t) = 0$, будет обозначаться через $\mathbf{V}(F_t)$. *Семейство кривых*, определенное полиномом F, состоит из многообразий $\mathbf{V}(F_t)$, где t пробегает вещественную ось.

В этом определении t играет роль *параметра*, который указывает, какая именно кривая в семействе рассматривается в данный момент. Строго говоря, нам следовало бы говорить о «семействе многообразий», а не о «семействе кривых», но мы будем использовать второй термин, чтобы подчеркнуть геометрический аспект.

Рассмотрим еще один пример семейства и его огибающей. Пусть множество кривых задано уравнением

$$F(x, y, t) = (x - t)^2 - y + t = 0. \tag{7}$$

Перепишем это уравнение в виде $y - t = (x - t)^2$. Теперь видно (см. следующий рисунок), что (7) задает семейство $\mathbf{V}(F_t)$ парабол, которые получены из стандартной параболы $y = x^2$ сдвигом вдоль прямой $y = x$. Здесь очевидно, что огибающая — это прямая, касающаяся каждой параболы семейства. Эта прямая задается уравнением $y = x - 1/4$ (подробности мы оставляем в качестве упражнения).



Семейство парабол на плоскости

Как правило, найти огибающую довольно трудно, и тем более замечательным является тот факт, что мы можем охарактеризовать огибающую следующим чисто алгебраическим образом.

Определение 5. Пусть дано семейство $\mathbf{V}(F_t)$ кривых в $\mathbb{R}^2$. Тогда *огибающая* семейства состоит из тех точек $(x, y) \in \mathbb{R}^2$, где имеют место равенства

$$F(x, y, t) = 0,$$
$$\frac{\partial}{\partial t} F(x, y, t) = 0$$

для некоторого t.

Сначала объясним, почему это определение соответствует интуитивному понятию огибающей. Наша аргументация не является строгой, но по крайней мере мы объясним, откуда возникает условие $\frac{\partial}{\partial t} F = 0$. Строгое рассмотрение теории огибающих требует применения серьезной техники. Заинтересованный читатель может обратиться к гл. 5 книги Bruce, Giblin (1992).

Пусть дано семейство $\mathbf{V}(F_t)$. Под огибающей мы понимаем кривую C, которая в каждой своей точке касается одной из кривых семейства. Пусть C задана параметрически:

$$x = f(t),$$
$$y = g(t),$$

причем для каждого t точка $(f(t), g(t))$ принадлежит кривой $\mathbf{V}(F_t)$. Таким образом, C пересекается со всеми кривыми семейства. Алгебраически это условие означает, что

$$F(f(t), g(t), t) = 0 \quad \text{для всех} \quad t \in \mathbb{R}. \tag{8}$$

Но C должна *касаться* многообразия $\mathbf{V}(F_t)$ в точке $(f(t), g(t))$. Мы знаем из анализа, что $(f'(t), g'(t))$ является касательным вектором к C; кроме того, градиент $\nabla F = (\frac{\partial}{\partial x} F, \frac{\partial}{\partial y} F)$ перпендикулярен касательной к $\mathbf{V}(F_t)$. Так как C касается $\mathbf{V}(F_t)$, то градиент ∇F перпендикулярен вектору $(f'(t), g'(t))$, т. е. $(\nabla F, (f'(t), g'(t))) = 0$ или, что эквивалентно,

$$\frac{\partial}{\partial x} F(f(t), g(t), t) \cdot f'(t) + \frac{\partial}{\partial y} F(f(t), g(t), t) \cdot g'(t) = 0. \tag{9}$$

Мы показали, что огибающая определяется условиями (8) и (9). Продифференцируем (8) по t. Имеем

$$\frac{\partial}{\partial x} F(f(t), g(t), t) \cdot f'(t) + \frac{\partial}{\partial y} F(f(t), g(t), t) \cdot g'(t) + \frac{\partial}{\partial t} F(f(t), g(t), t) = 0.$$

Если мы вычтем (9) из этого уравнения, то получим равенство

$$\frac{\partial}{\partial t}F(f(t),g(t),t)=0. \tag{10}$$

Таким образом, равенства (8) и (10) показывают, что $(x,y)=(f(t),g(t))$ удовлетворяет условиям определения 5.

Позже в этом параграфе мы увидим, что наш подход является слишком наивным. Однако для нас главным следствием определения 5 является то, что огибающая задается системой

$$\begin{aligned} F(x,y,t)&=0,\\ \frac{\partial}{\partial t}F(x,y,t)&=0. \end{aligned}$$

Переменные x и y определяют точку на огибающей, а t говорит нам, какой кривой семейства огибающая касается в этой точке. Так как уравнения зависят от x,y и t, то нам нужно исключить t, чтобы найти уравнение огибающей. Для этого мы применим результаты, полученные в §§ 1 и 2.

Рассмотрим семейство, заданное уравнением (6). Здесь $F=(x-t)^2+(y-t^2)^2-4$; поэтому огибающая задается системой

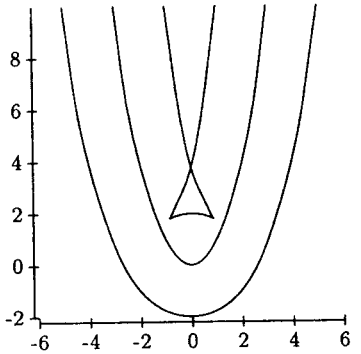
$$\begin{aligned} F&=(x-t)^2+(y-t^2)^2-4=0,\\ \frac{\partial}{\partial t}F&=-2(x-t)-4t(y-t^2)=0. \end{aligned} \tag{11}$$

Найдем базис Грёбнера по отношению к lex-упорядочению с $t>x>y$:

$$\begin{aligned} g_1 &= -1156+688x^2-191x^4+16x^6+544y+30x^2y-40x^4y\\ &\quad +225y^2-96x^2y^2+16x^4y^2-136y^3-32x^2y^3+16y^4,\\ g_2 &= (7327-1928y-768y^2-896y^3+256y^4)t+6929x-2946x^3\\ &\quad +224x^5+2922xy-1480x^3y+128x^5y-792xy^2-224x^3y^2\\ &\quad -544xy^3+128x^3y^3-384xy^4,\\ g_3 &= (431x-12xy-48xy^2-64xy^3)t+952-159x^2-16x^4+320y\\ &\quad -214x^2y+32x^4y-366y^2-32x^2y^2-80y^3+32x^2y^3+32y^4,\\ g_4 &= (697-288x^2+108y-336y^2+64y^3)t+23x-174x^3\\ &\quad +32x^5+322xy-112x^3y+32xy^2+32x^3y^2-96xy^3,\\ g_5 &= 135t^2+(26x+40xy+32xy^2)t-128+111x^2\\ &\quad -16x^4+64y+8x^2y+32y^2-16x^2y^2-16y^3. \end{aligned}$$

Элементы базиса Грёбнера представлены как полиномы от t с коэффициентами в $\mathbb{R}[x,y]$. По теореме об исключении g_1 порождает

первый исключающий идеал, т. е. огибающая принадлежит кривой $g_1=0$. Вот рисунок этой кривой вместе с параболой $y=x^2$:



Некоторым сюрпризом является «треугольная» часть графика огибающей. Эта часть не была ясно видна на рисунке семейства выше. Но рассмотрение окружностей с центрами вблизи вершины параболы показывает, что треугольник действительно является частью огибающей.

Мы доказали, что огибающая принадлежит многообразию $\mathbf{V}(g_1)$, но совпадает ли она с этим многообразием? На самом деле здесь можно задать два вопроса:

- Каждая ли точка многообразия $\mathbf{V}(g_1)$ принадлежит огибающей? Это то же самое, что спросить, каждое ли частичное решение (x,y) системы (11) продолжается до полного решения (x,y,t)?
- Пусть дана точка на огибающей. Сколько кривых семейства касаются огибающей в этой точке? Это все равно, что спросить, сколько существует полных решений (x,y,t) для данного частичного решения (x,y).

Так как старший коэффициент по t в g_5 является константой 135, то теорема о продолжении (в форме следствия 4 из § 1) гарантирует, что *каждое* частное решение продолжается, *если* мы работаем над полем $\mathbb{C}$. Значит, t существует, но может оказаться комплексным. Этот факт демонстрирует и силу, и слабость теоремы о продолжении: она гарантирует существование решения, но оно может принадлежать «неправильному» полю.

Однако уравнение g_5 дает нам кое-какую полезную информацию: g_5 квадратично по t, т. е. данное частичное решение (x,y) не более, чем *двумя* способами может быть продолжено до полного. Таким образом, *точка на огибающей семейства* (6) *может касаться не более чем двух окружностей семейства*. Можете ли вы

указать точки, в которых есть две касательные окружности к огибающей?

Рассмотрим теперь другие элементы базиса Грёбнера. Отметим, что g_2, g_3 и g_4 содержат t только в первой степени. Запишем их в виде

$$g_i = A_i(x,y)t + B_i(x,y), \quad i = 2,3,4.$$

Если A_i не обращается в нуль в точке (x,y) для какого-нибудь $i = 2,3,4$, то уравнение $A_i t + B_i = 0$ можно разрешить относительно t:

$$t = -\frac{B_i(x,y)}{A_i(x,y)}.$$

Таким образом, t вещественно, если вещественны x и y. Более того, эта формула показывает, что t определено однозначно, если $A_i(x,y) \neq 0$. Другими словами, *точка на огибающей семейства* (6), *не принадлежащая многообразию* $\mathbf{V}(A_2, A_3, A_4)$, *касается в точности одной окружности семейства.*

Осталось понять, когда A_2, A_3 и A_4 одновременно обращаются в нуль. Эти полиномы выглядят довольно сложными, но методы § 1 позволяют справиться с этой задачей: вещественными решениями системы $A_2 = A_3 = A_4 = 0$ являются

$$(x,y) = (0, 17/4) \quad \text{и} \quad (\pm 0.936845, 1.63999). \tag{12}$$

На рисунке, изображающем многообразие $\mathbf{V}(g_1)$, показаны особые точки этого многообразия. Постарайтесь увидеть две окружности, которые касаются огибающей в этих точках.

Мы уже знаем, что особые точки многообразия $\mathbf{V}(g_1)$ определяются уравнениями $g_1 = \frac{\partial}{\partial x} g_1 = \frac{\partial}{\partial y} g_1 = 0$. Если все особые точки перечислены в списке (12), то

$$\mathbf{V}(A_2, A_3, A_4) = \mathbf{V}(g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1). \tag{13}$$

Для того чтобы доказать это, достаточно проверить, что

$$\begin{aligned} g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1 &\in \langle A_2, A_3, A_4 \rangle, \\ A_2^2, A_3^2, A_4^2 &\in \langle g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1 \rangle. \end{aligned} \tag{14}$$

Прямое применение алгоритма принадлежности идеалу (гл. 2) позволяет сделать это. Сначала мы находим базис Грёбнера идеала $\langle A_2, A_3, A_4 \rangle$ и затем проверяем принадлежность идеалу каждого из полиномов $g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1$ (см. § 7 гл. 2). Аналогично проверяется и обратное включение. Детали будут рассмотрены в упражнениях.

Так как равенство (13) следует из включений (14), то мы доказали, что *неособые точки многообразия* $\mathbf{V}(g_1)$ *принадлежат огибающей семейства* (6), *и в каждой такой точке огибающая касается ровно одной окружности семейства.* Особые точки многообразия $\mathbf{V}(g_1)$ — это самые интересные точки огибающей: здесь огибающая касается двух окружностей. Это показывает, что наличие особых точек может быть полезным указанием на то, что происходит что-то необычное. Изучению особых точек посвящен важный раздел алгебраической геометрии.

В только что разобранном примере уравнения огибающей (11) легко выписать. Но анализ этих уравнений требует использования базисов Грёбнера, теоремы об исключении и теоремы о продолжении. Хотя базис Грёбнера и является довольно сложным, с его помощью удается точно установить, в каких точках огибающая касается более чем одной окружности. Все это демонстрирует возможности развитой нами теории.

Как уже упоминалось выше, наше рассмотрение огибающих проводилось на нестрогом уровне. Это видно и из предыдущего примера, где оказалось, что огибающая имеет особенности. Как огибающая может «касаться» кривой семейства в особой точке? В упражнениях мы отметим еще одну причину, по которой наше рассмотрение огибающих является слишком упрощенным. Мы также не обратили внимание на связь между семейством кривых $\mathbf{V}(F_t) \subset \mathbb{R}^2$ и поверхностью $\mathbf{V}(F) \subset \mathbb{R}^3$, определенной уравнением $F(x,y,t) = 0$. Мы отсылаем читателя к гл. 5 книги Bruce, Giblin (1992), где теория огибающих рассмотрена более полно.

Упражнения к § 4

1. Пусть кривая C в k^2 задана уравнением $x^3 - xy + y^2 = 1$. Отметим, что $(1,1) \in C$. Рассмотрим прямую, параметризованную уравнениями

$$\begin{aligned} x &= 1 + ct, \\ y &= 1 + dt. \end{aligned}$$

Найдите кратность пересечения этой прямой и кривой C в точке $(1,1)$. Что вы можете сказать о касательной в этой точке? Указание: нужно рассмотреть два случая.

2. Чтобы сделать определение 1 корректным, необходимо доказать, что кратность не зависит от параметризации.
(а) Докажите, что две параметризации

$$\begin{aligned} x &= a + ct, & x &= a + c't, \\ y &= b + dt, & y &= b + d't, \end{aligned}$$

описывают одну и ту же прямую в том и только том случае, когда существует ненулевое вещественное λ, такое, что $(c,d) = \lambda(c',d')$. Указание: если $x = a + ct, y = b + dt$ является параметризацией прямой L, то вектор (c,d) параллелен L.

(b) Пусть две параметризации п. (a) описывают одну и ту же прямую L, которая пересекает многообразие $\mathbf{V}(f)$ в точке (a,b). Докажите, что $t = 0$ является для полиномов $g(t) = f(a + ct, b + dt)$ и $h(t) = f(a + c't, b + d't)$ корнем одинаковой кратности. Указание: используйте п. (a) и найдите связь между g и h. Это утверждение докажет, что кратность пересечения прямой L и многообразия $\mathbf{V}(f)$ в точке (a,b) корректно определена.

3. Рассмотрим семейство прямых

$$x = t,$$
$$y = b + t.$$

Все эти прямые имеют тангенс наклона 1. Для какого b прямая из семейства касается окружности $x^2 + y^2 = 2$? Постройте график. Указание: рассмотрите полином $g(t) = t^2 + (b + t)^2 - 2$. Его корни определяют значения t, при которых прямая пересекает окружность.

4. Пусть $(a,b) \in \mathbf{V}(f)$ и $\nabla f(a,b) \neq (0,0)$. Докажите, что касательная к $\mathbf{V}(f)$ в точке (a,b) определена уравнением

$$\frac{\partial}{\partial x} f(a,b) \cdot (x - a) + \frac{\partial}{\partial y} f(a,b) \cdot (y - b) = 0.$$

5. Пусть $g \in k[t]$ и $g(0) = 0$.
   (a) Докажите, что $t = 0$ является корнем полинома g кратности ≥ 2 в том и только том случае, когда $g'(0) = 0$. Указание: представьте g как $g(t) = th(t)$ и продифференцируйте.
   (b) Докажите более общее утверждение: $t = 0$ является корнем кратности $\geq l$ в том и только том случае, когда $g'(0) = g''(0) = \ldots = g^{(l-1)}(0) = 0$.

6. Пусть прямая L параметризована уравнениями (1), где $(a,b) \in \mathbf{V}(f)$, и пусть $g(t) = f(a + ct, b + dt)$. Докажите, что L пересекает $\mathbf{V}(f)$ с кратностью l в том и только том случае, когда $g'(0) = g''(0) = \ldots = g^{(l-1)}(0) = 0$, но $g^{(l)}(0) \neq 0$. Указание: используйте предыдущее упражнение.

7. В этом упражнении мы рассмотрим, когда касательная пересекает кривую с кратностью, *большей* двух. Пусть C — кривая, определенная уравнением $y = f(x)$, где $f \in k[x]$, т. е. C — это график полинома f.

(a) Дайте алгебраическое доказательство того, что касательная к C в точке (a,b) имеет следующую параметризацию:

$$x = a + t,$$
$$y = f(a) + f'(a)t.$$

Указание: рассмотрите функцию $g(t) = f(a) + f'(a)t - f(a + t)$.

(b) Докажите, что касательная в точке $(a, f(a))$ пересекает кривую с кратностью ≥ 3 в том и только том случае, когда $f''(a) = 0$. Указание: примените предыдущее упражнение.

(c) Докажите, что кратность пересечения равна 3 в том и только том случае, когда $f''(a) = 0$, но $f'''(a) \neq 0$.

(d) *Точкой перегиба* (над $\mathbb{R}$) называется точка, в которой $f''(x)$ меняет знак. Докажите, что если кратность пересечения равна 3, то $(a, f(a))$ является точкой перегиба.

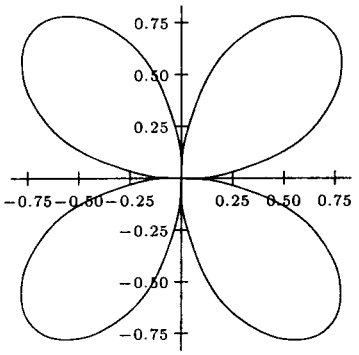
8. В этом упражнении мы будем искать особые точки.
   (a) Докажите, что $(0,0)$ является *единственной* особой точкой кривой $y^2 = x^3$.
   (b) В упр. 8 к § 3 гл. 1 мы изучали кривую $y^2 = cx^2 - x^3$, где c — некоторая константа. Найдите все особые точки этой кривой и объясните, как ваш ответ связан с изображением этой кривой, приведенным в гл. 1.
   (c) Докажите, что окружность $x^2 + y^2 = a^2$ не имеет особых точек.

9. Кратности могут использоваться в доказательстве того, что одна особенность «хуже» другой.
   (a) Докажите, что большинство прямых, проходящих через начало координат, пересекает кривую $y^2 = x^3$ с кратностью 2.
   (b) Докажите, что все прямые, проходящие через начало координат, пересекают кривую $x^4 + 2xy^2 + y^3 = 0$ с кратностью ≥ 3.

Отсюда следует, что особенность в нуле у второй кривой «хуже», чем у первой. Идея, заложенная в этом упражнении, показывает, как можно определить *кратность* особой точки.

10. В тексте параграфа было доказано, что $(0,0)$ является особой точкой кривой C, заданной уравнением $y^2 = x^2(1 + x)$. Но график этой кривой заставляет думать, что C имеет в нуле две «касательные». Можно ли использовать кратности, чтобы найти их?
    (a) Докажите, что все прямые, проходящие через начало координат, кроме двух, пересекают C с кратностью 2. Какие прямые имеют кратность пересечения 3?
    (b) Объясните, как ваш ответ связан с графиком кривой C, приведенным в тексте. Почему «касательные» должны иметь большую кратность пересечения?

11. Четырехлепестковая роза определена в полярных координатах уравнением $r = \sin(2\theta)$:



Эта же кривая имеет в декартовых координатах уравнение $(x^2 + y^2)^3 = 4x^2y^2$.

(a) Докажите, что большинство прямых, проходящих через начало координат, пересекают розу с кратностью 4 в этой точке. Можете ли вы дать этому геометрическое объяснение?

(b) Найдите прямые, проходящие через начало координат и пересекающие в этой точке розу с кратностью > 4. Дайте геометрическое объяснение полученным числам.

12. Рассмотрим поверхность $\mathbf{V}(f) \subset k^3$, где $f \in k[x, y, z]$.

(a) Попытайтесь дать определение особой точки $(a, b, c) \in \mathbf{V}(f)$.

(b) Найдите все особые точки на сфере $x^2 + y^2 + z^2 = 1$. Имеет ли ответ смысл?

(c) Найдите все особые точки на поверхности $\mathbf{V}(x^2 - y^2z^2 + z^3)$. Как ответ связан с изображением поверхности, приведенным в § 2 гл. 1?

13. Рассмотрим семейство кривых $F = xy - t \in \mathbb{R}[x, y, t]$. Нарисуйте графики различных кривых $\mathbf{V}(F_t)$ семейства и обязательно график кривой $\mathbf{V}(F_0)$.

14. В этом упражнении мы будем изучать огибающую семейства $F = (x - t)^2 - y + t$ (см. (7)).

(a) Очевидно, что огибающей является прямая с тангенсом наклона 1. Докажите аналитически, что эта прямая задается уравнением $y = x - 1/4$.

(b) Найдите огибающую алгебраически, используя определение 5.

(c) Найдите такую параметризацию огибающей, чтобы точка $(f(t), g(t))$ принадлежала параболе $\mathbf{V}(F_t)$. Отметим, что именно о такой параметризации шла речь при обсуждении определения 5.

15. В этом упражнении рассматривается огибающая семейства (6).

(a) На изображении семейства найдите пары окружностей, касательных к огибающей в точках, перечисленных в (12).

(b) Для точки $(0, 4.25) = (0, 17/4)$ найдите точные значения параметра t, которые определяют две касательные окружности.

(c) Докажите, что точные координаты точек (12) могут быть заданы формулами

$$\left(0, \frac{17}{4}\right) \quad \text{и} \quad \left(\pm\frac{1}{2}\sqrt{15 + 6\sqrt[3]{2} - 12\sqrt[3]{4}}, \frac{1}{4}(-1 + 6\sqrt[3]{2})\right).$$

Указание: большинство систем компьютерной алгебры могут разлагать полиномы на множители и решать кубические уравнения.

16. Рассмотрим семейство кривых $F = (x - t)^2 + y^2 - (1/2)t^2$.

(a) Найдите его огибающую.

(b) Поясните свой ответ рисунком.

17. Рассмотрим семейство окружностей $(x - t)^2 + (y - t^2)^2 = t^2$ в $\mathbb{R}^2$.

(a) Найдите уравнение огибающей и докажите, что огибающая представляет собой объединение двух многообразий.

(b) Используйте базис Грёбнера и теорему о продолжении, чтобы определить, сколько окружностей семейства касаются огибающей в данной точке. Поясните свой ответ рисунком. Указание: для каждой компоненты огибающей придется проводить свои рассуждения.

18. Докажите (14), используя указания, данные в тексте параграфа. Докажите также, что $A_2 \notin \langle g_1, \frac{\partial}{\partial x}g_1, \frac{\partial}{\partial y}g_1\rangle$. Это показывает, что идеалы $\langle g_1, \frac{\partial}{\partial x}g_1, \frac{\partial}{\partial y}g_1\rangle$ и $\langle A_2, A_3, A_4\rangle$ не совпадают, хотя и определяют одно и то же многообразие.

19. В этом упражнении мы покажем, что наше определение огибающей слишком упрощено.

(a) Рассмотрим семейство окружностей радиуса 1 с центрами на оси x. Используйте рисунок, чтобы показать что огибающая состоит из двух прямых $y = \pm 1$.

(b) Используя определение 5, вычислите уравнение огибающей для семейства $F = (x - t)^2 + y^2 - 1$. Результат не должен вас удивить.

(c) Используя определение 5, найдите огибающую семейства $F = (x - t^3)^2 + y^2 - 1$. Отметьте, что одна из кривых семейства является компонентой огибающей. Причина состоит в том, что t^3 позволяет окружностям «скапливаться» при $t = 0$, что и заставляет окружность $\mathbf{V}(F_0)$ быть частью огибающей.

В нашем неформальном обсуждении огибающей мы предполагали, что можем параметризовать ее так, чтобы точка $(f(t), g(t))$ при-

надлежала многообразию $\mathbf{V}(F_t)$ в момент t. Это предполагает, что огибающая касается *разных* кривых семейства. Однако в примере п. (c) компонента огибающей совпадает с *одной из* кривых семейства, т. е. мы трактовали огибающую слишком упрощенно.

20. Рассмотрим семейство кривых в $\mathbb{R}^2$, заданное полиномом $F(x,y,t) \in \mathbb{R}[x,y,t]$. Некоторые из кривых этого семейства могут иметь особенности, а другие — нет. Как определить, какие из кривых имеют особые точки?
   (a) Рассмотрим систему уравнений $F = \frac{\partial}{\partial x}F = \frac{\partial}{\partial y}F = 0$. Используйте теорию исключения и опишите процедуру, позволяющую найти значения параметра t, соответствующие кривым с особенностями.
   (b) Примените метод п. (a) к семейству из упр. 13.

§ 5. Единственность разложения на множители и результанты

Нашей главной (и пока не выполненной) задачей в гл. 3 было доказать теорему о продолжении. Для этого нам придется изучить новые разделы алгебры, относящиеся к *единственности разложения на множители* и к *результантам*. Оба эти понятия будут использованы в § 6 для доказательства теоремы о продолжении. Единственностью разложения на множители мы будем часто пользоваться и в последующих главах.

Неприводимые полиномы и единственность разложения на множители

Начнем с определения.

Определение 1. Полином $f \in k[x_1,\dots,x_n]$, где k — некоторое поле, называется *неприводимым над* k, если он не постоянен и не является произведением двух непостоянных полиномов из $k[x_1,\dots,x_n]$.

Это определение говорит, что если непостоянный полином f неприводим, то, с точностью до постоянного множителя, его делителем может быть только он сам. Сразу отметим, что неприводимость зависит от поля определения. Полином x^2+1, например, неприводим над $\mathbb{Q}$ и $\mathbb{R}$, но над $\mathbb{C}$ он разлагается на множители: $x^2+1 = (x+i)(x-i)$.

Справедливо следующее предложение.

Предложение 2. *Каждый непостоянный полином $f \in k[x_1,\dots,x_n]$ является произведением неприводимых над k полиномов.*

Доказательство. Если f неприводим, то утверждение справедливо, если нет, то f можно представить в виде $f = gh$, где g и h — непостоянные полиномы из $k[x_1,\dots,x_n]$. Однако и полная степень g, и полная степень h меньше, чем полная степень полинома f. К g и h применимо то же рассуждение, что и к f: если они приводимы, то они могут быть разложены в произведение непостоянных множителей с меньшими степенями. Полная степень уменьшается каждый раз, когда мы переходим к множителям. Но этот процесс не может продолжаться бесконечно, т. е. f является произведением неприводимых полиномов. □

В теореме 5 будет доказано, что это разложение на неприводимые множители по существу единственно. Однако сначала мы докажем следующее важное свойство неприводимых полиномов.

Теорема 3. *Пусть $f \in k[x_1,\dots,x_n]$ неприводим над k. Предположим, что произведение gh, где $g,h \in k[x_1,\dots,x_n]$, делится на f; тогда f делит g или h.*

Доказательство. Мы будем использовать индукцию по числу переменных. Если $n=1$, то можно использовать понятие наибольшего общего делителя (см. § 5 гл. 1). Пусть f делит gh. Рассмотрим $p = \mathrm{GCD}(f,g)$. Если степень полинома p больше нуля, то, с точностью до постоянного множителя, $f = p$ (так как f неприводим). Но тогда f делит g. Если же p — константа, то, положив $p=1$, мы можем найти полиномы $A, B \in k[x_1]$, такие, что $Af + Bg = 1$ (предложение 6 из § 5 гл. 1). Умножая это равенство на h, получим

$$h = h(Af+Bg) = Ahf + Bgh.$$

Так как f делит gh, то $gh = fs$ и, следовательно, $h = f(Ah+Bs)$, т. е. f делит h. Утверждение доказано при $n=1$.

Пусть теорема справедлива для $n-1$. Сначала мы рассмотрим случай, когда неприводимый полином не зависит от x_1:

$$\left\{\begin{array}{c} u \in k[x_2,\dots,x_n] \quad \text{неприводим и} \\ \text{делит} \quad gh \in k[x_1,\dots,x_n] \end{array}\right\} \Rightarrow u \text{ делит } g \text{ или } h. \qquad (1)$$

Имеем $g = \sum_{i=0}^{l} a_i x_1^i$ и $h = \sum_{i=0}^{m} b_i x_1^i$, где $a_i, b_j \in k[x_2,\dots,x_n]$. Если u делит каждый полином a_i, то u делит и g. Аналогично, если u делит каждый полином b_i, то u делит и h. Пусть ни одно, ни другое условие не выполнено. Тогда существуют такие $i,j \geq 0$, что u не делит a_i и не делит b_j. Мы будем считать, что i и j — это наименьшие числа с этими свойствами (т. е. u делит a_r, если $r<i$, и u делит b_s, если $s<j$). Рассмотрим полином

$$\begin{aligned} c_{i+j} =& (a_0 b_{i+j} + a_1 b_{i+j-1} + \dots + a_{i-1} b_{j+1}) + \\ &+ a_i b_j + (a_{i+1} b_{j-1} + \dots + a_{i+j} b_0). \end{aligned}$$

Мы выбрали i так, что u делит каждое слагаемое в первой скобке, и j так, что u делит каждое слагаемое во второй скобке. Но u не делит a_i и не делит b_j; следовательно, по предположению индукции, u не делит a_ib_j. Так как u делит все слагаемые, кроме одного, то u не делит c_{i+j}. Легко показать, что c_{i+j} является коэффициентом при x_1^{i+j} в gh. Значит, u не может делить gh. Противоречие. Утверждение (1) доказано.

Теперь рассмотрим общий случай. Пусть f делит g. Если f не зависит от x_1, то все доказано. Если f зависит от x_1, то рассмотрим кольцо $k(x_2,\dots,x_n)[x_1]$ — это кольцо полиномов от одной переменной над *полем* $k(x_2,\dots,x_n)$. Напомним, что элементами поля $k(x_2,\dots,x_n)$ являются отношения полиномов из $k[x_2,\dots,x_n]$. Кольцо $k[x_1,\dots,x_n]$ будет рассматриваться как подкольцо в $k(x_2,\dots,x_n)[x_1]$. Основная идея состоит в том, чтобы работать в большем кольце, где теорема справедлива, а затем вернуться в меньшее.

Мы утверждаем, что f неприводим и в $k(x_2,\dots,x_n)[x_1]$. Пусть f приводим: $f=AB$, где A,B — полиномы от x_1 с коэффициентами в $k(x_2,\dots,x_n)$. Нам нужно показать, что или A, или B имеет степень 0 по x_1. Пусть $d\in k[x_2,\dots,x_n]$ — это произведение всех знаменателей в A и B. Тогда $\widetilde{A}=dA$ и $\widetilde{B}=dB$ — полиномы из $k[x_1,\dots,x_n]$ и

$$d^2f=\widetilde{A}\widetilde{B} \tag{2}$$

в $k[x_1,\dots,x_n]$. Запишем d^2 как произведение неприводимых множителей из $k[x_2,\dots,x_n]$, что возможно в силу предложения 2; тогда по (1) каждый из них делит $\widetilde{A}$ или $\widetilde{B}$. Поделим обе части равенства на эти множители и получим, что

$$f=\widetilde{A}_1\widetilde{B}_1$$

в $k[x_1,\dots,x_n]$. Так как f неприводим в $k[x_1,\dots,x_n]$, то $\widetilde{A}_1$ или $\widetilde{B}_1$ — константа. Но эти полиномы были получены из A и B при помощи умножения и деления на полиномы из $k[x_2,\dots,x_n]$. Это показывает, что или A, или B не зависит от x_1. Это и требовалось доказать.

Таким образом, f неприводим в $k(x_2,\dots,x_n)[x_1]$ и, следовательно, делит g или h в $k(x_2,\dots,x_n)[x_1]$. Пусть, например, $g=Af$, где $A\in k(x_2,\dots,x_n)[x_1]$. Избавляясь от знаменателей, получаем

$$dg=\widetilde{A}f \tag{3}$$

в $k[x_1,\dots,x_n]$, где $d\in k[x_2,\dots,x_n]$. По (1) каждый неприводимый делитель полинома d делит $\widetilde{A}$ или f. Но f он делить не может, так как f неприводим и имеет положительную степень по x_1. Значит, каждый неприводимый делитель полинома d делит $\widetilde{A}$. Проводя

сокращения в (3), получаем, что f делит g в $k[x_1,\dots,x_n]$. Это завершает доказательство теоремы. □

В § 6 нам понадобится такое следствие теоремы 3.

Следствие 4. *Пусть полиномы $f,g\in k[x_1,\dots,x_n]$ имеют положительные степени по x_1. Тогда f и g имеют общий делитель в $k[x_1,\dots,x_n]$ положительной степени по x_1 в том и только том случае, когда они имеют общий делитель в $k(x_2,\dots,x_n)[x_1]$.*

Доказательство. Если f и g имеют общий делитель в $k[x_1,\dots,x_n]$ положительной степени по x_1, то они, конечно, имеют его и в большем кольце $k(x_2,\dots,x_n)[x_1]$. Пусть теперь f и g имеют общий делитель $\tilde{h}\in k(x_2,\dots,x_n)[x_1]$. Имеем

$$\begin{aligned} f&=\tilde{h}\tilde{f}_1, \quad \tilde{f}_1\in k(x_2,\dots,x_n)[x_1],\\ g&=\tilde{h}\tilde{g}_1, \quad \tilde{g}_1\in k(x_2,\dots,x_n)[x_1]. \end{aligned}$$

Разумеется, $\tilde{h},\tilde{f}_1$ и $\tilde{g}_1$ могут иметь знаменатели — полиномы из $k[x_2,\dots,x_n]$. Пусть $d\in k[x_2,\dots,x_n]$ — общий знаменатель полиномов $\tilde{h},\tilde{f}_1,\tilde{g}_1$. Положим $h=d\tilde{h}$, $f_1=d\tilde{f}_1$ и $g_1=d\tilde{g}_1$. Тогда $h,f_1,g_1\in k[x_1,\dots,x_n]$. Имеем

$$\begin{aligned} d^2f&=hf_1,\\ d^2g&=hg_1 \end{aligned}$$

в $k[x_1,\dots,x_n]$. Пусть h_1 — неприводимый делитель полинома h положительной степени по x_1. Так как $\tilde{h}=h/d$ имеет положительную степень по x_1, то такой делитель должен существовать. Тогда h_1 делит d^2 или f (по теореме 3). Но h_1 не может делить d^2, так как $d^2\in k[x_2,\dots,x_n]$; следовательно, h_1 делит f в $k[x_1,\dots,x_n]$. Рассуждая аналогично, получаем, что h_1 делит g, т. е. h_1 — требуемый общий делитель. Доказательство закончено □

Теорема 3 утверждает, что неприводимые полиномы ведут себя подобно простым числам в том смысле, что если простое число делит произведение двух чисел, то оно делит один из сомножителей. Это свойство простых чисел и лежит в основе однозначного разложения на простые множители. То же самое справедливо и для неприводимых полиномов.

Теорема 5. *Каждый непостоянный полином $f\in k[x_1,\dots,x_n]$ может быть записан как произведение неприводимых над k полиномов $f=f_1\cdot f_2\dots f_r$. Более того, если $f=g_1\cdot g_2\dots g_s$ — другое разложение в произведение неприводимых над k полиномов, то $r=s$ и, с точностью до перестановки и до постоянных множителей, $f_i=g_i$.*

Доказательство будет разобрано в упражнениях.

Для полиномов из $\mathbb{Q}[x_1, \ldots, x_n]$ существуют алгоритмы разложения в произведение неприводимых полиномов. Классический алгоритм, восходящий к Кронекеру, рассмотрен в книге MINES, RICHMAN, RUITENBURG (1993, Theorem 4.8). Существенно более эффективный метод изложен в работах DAVENPORT, SIRET, TOURNIER (1993) и MIGNOTTE (1992). Большинство систем компьютерной алгебры умеют разлагать на множители полиномы из $\mathbb{Q}[x_1, \ldots, x_n]$. Разложение на множители полиномов из $\mathbb{R}[x_1, \ldots, x_n]$ или $\mathbb{C}[x_1, \ldots, x_n]$ — это *существенно* более трудная задача.

Результанты

Хотя методы теории результантов заметно отличаются от всего, что мы рассматривали до сих пор, результанты играют важную роль в теории исключения. Понятие результанта возникает, когда мы задаем вопрос: при каких условиях два полинома из $k[x]$ имеют общий множитель? Эта задача кажется очень далекой от теории исключения, но в конце параграфа мы увидим, что здесь есть связь. В § 6 мы рассмотрим результант двух полиномов из $k[x_1, \ldots, x_n]$ и применим результанты для доказательства теоремы о продолжении.

Предположим, что мы хотим выяснить, имеют ли два полинома $f, g \in k[x]$ общий делитель (т. е. полином $h \in k[x]$ положительной степени, который делит и f и g). Можно, конечно, разложить f и g на неприводимые множители. К сожалению, разложение на множители — это весьма трудоемкий процесс. Более эффективный метод — это найти наибольший общий делитель полиномов f и g, используя алгоритм Евклида из гл. 1. К сожалению, алгоритм Евклида требует выполнения делений в поле k. Как мы увидим позже, в ходе процедуры исключения этого желательно избегать. Есть ли способ определить, существует ли общий делитель, не производя делений в k? Вот первый ответ.

Лемма 6. *Пусть $f, g \in k[x]$ — полиномы степеней $l > 0$ и $m > 0$ соответственно. Тогда f и g имеют общий делитель в том и только том случае, когда существуют полиномы $A, B \in k[x]$, такие, что*

(i) *A и B не равны нулю одновременно;*
(ii) *степень полинома A не больше $m-1$ и степень полинома B не больше $l-1$;*
(iii) $Af + Bg = 0$.

Доказательство. Предположим сначала, что f и g имеют общий делитель $h \in k[x]$. Тогда $f = hf_1, g = hg_1$, где $f_1, g_1 \in k[x]$. Отметим,

что степень полинома f_1 не больше $l-1$ и степень полинома g_1 не больше $m-1$. Тогда

$$g_1 \cdot f + (-f_1) \cdot g = g_1 \cdot hf_1 - f_1 \cdot hg_1 = 0,$$

т. е. $A = g_1$ и $B = -f_1$ обладают требуемыми свойствами.

Обратно, пусть A и B обладают указанными тремя свойствами. По (i) мы можем считать B не равным нулю. Если f и g не имеют общего делителя, то их наибольший общий делитель равен 1 и, следовательно, найдутся полиномы $\widetilde{A}, \widetilde{B} \in k[x]$, такие, что $\widetilde{A}f + \widetilde{B}g = 1$ (предложение 6 из § 5 гл. 1). Тогда, умножив это равенство на B, получаем, используя равенство $Bg = -Af$,

$$B = (\widetilde{A}f + \widetilde{B}g)B = \widetilde{A}Bf + \widetilde{B}Bg = \widetilde{A}Bf - \widetilde{B}Af = (\widetilde{A}B - \widetilde{B}A)f.$$

Так как $B \neq 0$, то это равенство показывает, что степень B не меньше l, что противоречит (ii). Отсюда следует, что f и g имеют общий делитель положительной степени. □

Процедура, описанная в лемме 6, не выглядит удовлетворительной: как найти (или доказать существование) требуемых A и B? Как это ни удивительно, *линейная алгебра* может дать ответ на этот вопрос. Для этого нужно превратить равенство $Af + Bg = 0$ в систему линейных уравнений. Пусть

$$A = c_0x^{m-1} + \ldots + c_{m-1},$$
$$B = d_0x^{l-1} + \ldots + d_{l-1},$$

где коэффициенты $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}$ (их $l+m$) считаются неизвестными. Мы должны найти $c_i, d_j \in k$, не все равные нулю, такие, что справедливо равенство

$$Af + Bg = 0. \tag{4}$$

Тогда условия леммы 6 будут выполнены.

Пусть

$$f = a_0x^l + \ldots + a_l, \quad a_0 \neq 0,$$
$$g = b_0x^m + \ldots + b_m, \quad b_0 \neq 0,$$

где $a_i, b_j \in k$. Подставим эти формулы для A, B, f, g в уравнение (4) и, сравнив коэффициенты при одинаковых степенях x, получим следующую систему:

$$\begin{aligned}
a_0c_0 \quad &+ \quad b_0d_0 \quad &&= 0 \ (\text{коэффициент при } x^{l+m-1}),\\
a_1c_0 + a_0c_1 \ &+ \ b_1d_0 + b_0d_1 \ &&= 0 \ (\text{коэффициент при } x^{l+m-2}),\\
\ddots \quad &\quad \ddots \quad &&\vdots\\
a_lc_{m-1} \quad &+ \quad b_md_{l-1} \quad &&= 0 \ (\text{коэффициент при } x^0).
\end{aligned} \tag{5}$$

Мы построили однородную систему из $l+m$ уравнений с $l+m$ неизвестными. Такая система имеет ненулевое решение в том и только том случае, когда определитель матрицы коэффициентов равен нулю. Таким образом, мы пришли к следующему определению.

Определение 7. Рассмотрим полиномы $f, g \in k[x]$ положительной степени

$$f = a_0x^l + \ldots + a_l, \quad a_0 \neq 0,$$
$$g = b_0x^m + \ldots + b_m, \quad b_0 \neq 0.$$

Матрицей Сильвестра $\mathrm{Syl}(f,g,x)$ полиномов f и g по отношению к x называется матрица коэффициентов системы (5). Таким образом, $\mathrm{Syl}(f,g,x)$ — это $(l+m)\times(l+m)$-матрица

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}.$$

Здесь m первых столбцов отведено a_i, оставшиеся l столбцов отведены b_j, а пустые места в матрице заняты нулями. *Результантом* $\mathrm{Res}(f,g,x)$ полиномов f и g по отношению к x называется определитель матрицы Сильвестра:

$$\mathrm{Res}(f,g,x) = \det(\mathrm{Syl}(f,g,x)).$$

Сформулируем основные свойства результантов. Напомним сначала, что полином называется *целочисленным*, если его коэффициенты — целые числа.

Предложение 8. *Пусть $f, g \in k[x]$ — полиномы положительной степени. Тогда $\mathrm{Res}(f,g,x)$ является целочисленным полиномом от коэффициентов полиномов f и g. Кроме того, f и g имеют общий делитель в $k[x]$ в том и только том случае, когда $\mathrm{Res}(f,g,x) = 0$.*

Доказательство. Напомним, что определитель $\det(A)$ матрицы $A = (a_{ij})_{1\le i,j\le s}$ размера $s\times s$ определяется формулой

$$\det(A) = \sum_\sigma \mathrm{sgn}(\sigma) a_{1\sigma(1)}\cdot a_{2\sigma(2)}\ldots a_{s\sigma(s)},$$

где σ пробегает все перестановки множества $\{1,\ldots,s\}$, а $\mathrm{sgn}(\sigma) = +1$, если σ — четная перестановка, и $\mathrm{sgn}(\sigma) = -1$, если нечетная (см. приложение А). Эта формула показывает, что определитель — целочисленный полином (на самом деле его коэффициенты равны ± 1).

Далее, результант равен нулю $\Leftrightarrow$ матрица коэффициентов системы (5) вырожденна $\Leftrightarrow$ система (5) имеет ненулевое решение. Мы отмечали раньше, что последнее эквивалентно существованию полиномов A и B со свойствами, перечисленными в лемме 6. Теперь лемма 6 заканчивает доказательство предложения. □

В качестве примера рассмотрим следующую задачу: имеют ли полиномы $f = 2x^2+3x+1$ и $g = 7x^2+x+3$ общий множитель? Вычисляем результант

$$\mathrm{Res}(f,g,x) = \det\begin{pmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{pmatrix} = 153 \neq 0$$

и получаем, что общего множителя нет.

Неудобство работы с результантами состоит в том, что приходится вычислять большие определители. В упражнениях мы рассмотрим другой метод вычисления результантов, аналогичный алгоритму Евклида. Большинство систем компьютерной алгебры умеет работать с результантами.

Теперь покажем, что существует связь между результантами и теорией исключения. Найдем результант полиномов $f = xy-1$ и $g = x^2+y^2-4$. Мы рассматриваем f и g как полиномы от x, коэффициенты которых являются полиномами от y. Имеем

$$\mathrm{Res}(f,g,x) = \det\begin{pmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2-4 \end{pmatrix} = y^4 - 4y^2 + 1.$$

Более общим образом, если f и g — *любые* полиномы из $k[x,y]$ положительной степени по x, то мы можем вычислить результант таким способом. Так как коэффициенты полиномов f и g являются полиномами от y, то, согласно предложению 8, $\mathrm{Res}(f,g,x)$ является полиномом от y. Таким образом, результант исключает x. Является

ли это исключением того же вида, что рассматривалось нами в §§ 1 и 2? В частности, принадлежит ли $\operatorname{Res}(f,g,x)$ первому исключающему идеалу $\langle f,g\rangle \cap k[y]$?

Предложение 9. *Пусть $f,g \in k[x]$ — полиномы положительной степени. Тогда существуют полиномы $A,B \in k[x]$, такие, что*

$$Af + Bg = \operatorname{Res}(f,g,x).$$

Более того, коэффициенты полиномов A и B являются целочисленными полиномами от коэффициентов полиномов f и g.

Доказательство. Определение результанта использует уравнение $Af+Bg=0$. Теперь те же самые методы мы применим для решения уравнения

$$\widetilde{A}f + \widetilde{B}g = 1. \tag{6}$$

Причина, почему мы работаем с $\widetilde{A}$, а не с A, сейчас станет ясна.

Предложение очевидным образом справедливо, если выполняется равенство $\operatorname{Res}(f,g,x)=0$ (положим $\widetilde{A}=\widetilde{B}=0$). Пусть теперь $\operatorname{Res}(f,g,x)\neq 0$ и

$$\begin{aligned} f &= a_0x^l + \ldots + a_l, \quad a_0 \neq 0,\\ g &= b_0x^m + \ldots + b_m, \quad b_0 \neq 0,\\ \widetilde{A} &= c_0x^{m-1} + \ldots + c_{m-1},\\ \widetilde{B} &= d_0x^{l-1} + \ldots + d_{l-1}, \end{aligned}$$

где коэффициенты $c_0,\ldots,c_{m-1},d_0,\ldots,d_{l-1}$ считаются неизвестными из поля k. Если мы подставим эти соотношения в (6) и сравним коэффициенты при одинаковых степенях x, то получим следующую систему с неизвестными c_i,d_j и коэффициентами a_i,b_j:

$$\begin{aligned} a_0c_0 \quad &+ \quad b_0d_0 \qquad &&= 0 \ (\text{коэффициент при } x^{l+m-1}),\\ a_1c_0 + a_0c_1 \ &+ \ b_1d_0 + b_0d_1 \qquad &&= 0 \ (\text{коэффициент при } x^{l+m-2}),\\ \ddots \quad &\quad \ddots \qquad &&\vdots\\ a_lc_{m-1} \quad &+ \quad b_md_{l-1} &&= 1 \ (\text{коэффициент при } x^0). \end{aligned} \tag{7}$$

Эта система есть система (5) за исключением того, что в правой части последнего уравнения стоит 1 (вместо 0). Значит, матрицей системы (7) является матрица Сильвестра, а условие $\operatorname{Res}(f,g,x)\neq 0$ гарантирует, что (7) имеет единственное решение в k.

В этом случае мы можем использовать *правило Крамера* для вычисления единственного решения. По этому правилу i-я неизвестная равна отношению двух определителей: в знаменателе стоит определитель матрицы системы, а в числителе — определитель матрицы, полученной из матрицы системы при замене i-го столбца столбцом свободных членов из правой части системы. Точную

формулировку правила Крамера читатель может найти в приложении A. В нашем случае правило Крамера позволяет найти c_i и d_j. Например,

$$c_0 = \frac{1}{\operatorname{Res}(f,g,x)} \det \begin{pmatrix} 0 & & & & b_0 & & \\ 0 & a_0 & & & \vdots & \ddots & \\ \vdots & \vdots & \ddots & & \vdots & & b_0 \\ 0 & a_l & & a_0 & b_m & & \vdots \\ \vdots & & \ddots & \vdots & & \ddots & \vdots \\ 1 & & & a_l & & & b_m \end{pmatrix}$$

Так как определитель является целочисленным полиномом от своих элементов, то

$$c_0 = \frac{\text{целочисленный полином от } a_i,b_j}{\operatorname{Res}(f,g,x)}.$$

Аналогичные формулы определяют остальные c_i, а также d_j. Теперь $\widetilde{A} = c_0x^{m-1} + \ldots + c_{m-1}$ может быть записано в виде

$$\widetilde{A} = \frac{1}{\operatorname{Res}(f,g,x)}A,$$

где $A \in k[x]$, а его коэффициенты являются целочисленными полиномами от a_i,b_j. Аналогично

$$\widetilde{B} = \frac{1}{\operatorname{Res}(f,g,x)}B,$$

где $B \in k[x]$ обладает теми же свойствами, что и A. Так как $\widetilde{A}f + \widetilde{B}g = 1$, то, умножая на $\operatorname{Res}(f,g,x)$, получаем

$$Af + Bg = \operatorname{Res}(f,g,x).$$

Предложение доказано. □

В большинстве курсов линейной алгебры правило Крамера не рассматривается, так как исключение по Гауссу — это гораздо более эффективная процедура (с вычислительной точки зрения). Но для нужд теории часто необходимо знать *форму* решения. И здесь правило Крамера оказывается весьма полезным.

Теперь мы можем объяснить связь между результантом и наибольшим общим делителем. Пусть $f,g \in k[x]$ и $\operatorname{Res}(f,g,x)\neq 0$; тогда f и g не имеют общих делителей, следовательно $\operatorname{GCD}(f,g)=1$. Но тогда по предложению 6 из § 5 гл. 1 существуют полиномы $\widetilde{A}$ и $\widetilde{B}$, такие, что $\widetilde{A}f + \widetilde{B}g = 1$. Выражения для $\widetilde{A}$ и $\widetilde{B}$, приведенные

выше, показывают, что коэффициенты полиномов $\widetilde{A}$ и $\widetilde{B}$ имеют общий знаменатель, равный результанту (хотя результант может и не быть наименьшим знаменателем). Теперь, умножая на результант, получаем $Af + Bg = \operatorname{Res}(f, g, x)$.

Вернемся к полиномам $f = xy - 1$ и $g = x^2 + y^2 - 4$. Рассматривая их как полиномы от x, вычислим результант $\operatorname{Res}(f, g, x) = y^4 - 4y^2 + 1 \neq 0$, т. е. $GCD(f, g) = 1$. Читатель может проверить, что

$$-\left(\frac{y}{y^4 - 4y^2 + 1}x + \frac{1}{y^4 - 4y^2 + 1}\right) f + \frac{y^2}{y^4 - 4y^2 + 1} g = 1.$$

Это равенство выполняется в кольце $k(y)[x]$, т. е. коэффициенты полиномов являются *рациональными функциями* от y. Причина состоит в том, что теория, лежащая в основе понятия наибольшего общего делителя, требует, чтобы коэффициенты полинома принадлежали *полю*. Если мы хотим работать в $k[x, y]$, то необходимо избавиться от знаменателей, и тогда мы получим следующее выражение:

$$-(xy + 1)f + y^2 g = y^4 - 4y^2 + 1. \tag{8}$$

То есть мы можем рассматривать результант как «свободный от знаменателей» аналог наибольшего общего делителя.

Мы также получили ответ на вопрос, сформулированный перед предложением 9, так как (8) показывает, что результант $y^4 - 4y^2 + 1$ принадлежит первому исключающему идеалу. Это утверждение носит общий характер: пусть $f, g \in k[x, y]$ — полиномы положительной степени по x; тогда их результант $\operatorname{Res}(f, g, x)$ принадлежит первому исключающему идеалу идеала $\langle f, g \rangle$. В § 6 мы увидим, как эти идеи можно обобщить на случай полиномов из $k[x_1, \ldots, x_n]$.

Можно определить результанты трех и более полиномов. Одно из возможных определений будет рассмотрено в § 6. Читатель, интересующийся *мультиполиномиальными результантами*, может ознакомиться с работами MACAULAY (1902) и VAN DER WAERDEN (1931). Современное введение в эту теорию можно найти в книге BAJAJ, GARRITY, WARREN (1988) и в работе CANNY, MANOCHA (1993). В последней работе имеется обширная библиография. Рассмотрение теории результантов с теоретических позиций имеется в работе JOUANOLOU (1991), а глубокое обобщение этой теории рассматривается в работе GELFAND, KAPRANOV, ZELEVINSKY (1994).

Упражнения к § 5

1. Рассмотрим несколько примеров неприводимых полиномов.
   (a) Докажите, что любой полином $f \in k[x]$ степени 1 неприводим над k.
   (b) Пусть $f \in k[x]$ имеет степень 2 или 3. Докажите, что f неприводим в том и только том случае, когда он не имеет корней в k.
   (c) Используя п. (b), докажите, что $x^2 - 2$ и $x^3 - 2$ неприводимы над $\mathbb{Q}$ (но не над $\mathbb{R}$).
   (d) Докажите неприводимость полинома $x^4 + 1$ над $\mathbb{Q}$ (но не над $\mathbb{R}$). Эта задача труднее предыдущей.
   (e) Используя п. (d), докажите, что утверждение (b) не выполняется для полиномов степени ≥ 4.
2. Докажите, что поле k алгебраически замкнуто в том и только том случае, когда любой неприводимый полином из $k[x]$ имеет степень 1.
3. В этом упражнении рассматривается доказательство теоремы 3. Пусть $f = \sum_i a_i x_1^i$ и $g = \sum_i b_i x_1^i$, где $a_i, b_i \in k[x_2, \ldots, x_n]$.
   (a) Пусть $u \in k[x_2, \ldots, x_n]$. Докажите, что u делит f в том и только том случае, когда u делит каждый a_i.
   (b) Пусть $fg = \sum_i c_i x_1^i$. Проверьте, что c_{i+j} задается формулой, приведенной в доказательстве теоремы 3.
4. Это упражнение посвящено доказательству теоремы 5.
   (a) Пусть f неприводим и делит произведение $h_1 \ldots h_s$. Докажите, что f делит некоторый полином h_i.
   (b) Существование разложения на неприводимые множители доказано в предложении 1. Докажите единственность (одно из утверждений теоремы 5). Указание: если $f = f_1 \ldots f_r = g_1 \ldots g_s$, где f_i и g_j неприводимы, то из п. (a) следует, что f_1 делит некоторый полином g_j. Тогда g_j совпадает с f_1 с точностью до постоянного множителя, и мы можем сократить обе части равенства на f_1. Теперь можно применить индукцию по полной степени полинома f.
5. Найдите результант полиномов $x^5 - 3x^4 - 2x^3 + 3x^2 + 7x + 6$ и $x^4 + x^2 + 1$. Имеют ли эти полиномы общий множитель в $\mathbb{Q}[x]$? Объясните ваш ответ.
6. В упр. 14 к § 5 гл. 1 мы доказали, что если $f = c(x - a_1)^{r_1} \ldots (x - a_l)^{r_l} \in \mathbb{C}[x]$, то

$$\operatorname{GCD}(f, f') = (x - a_1)^{r_1 - 1} \ldots (x - a_l)^{r_l - 1}.$$

Над произвольным полем k данный полином $f \in k[x]$ положительной степени не обязательно разлагается в произведение линейных множителей. Но по теореме о единственности разложения в произведение неприводимых полиномов имеем

$$f = f_1^{r_1} \ldots f_l^{r_l},$$

где $f_1, \ldots, f_l \in k[x]$ неприводимы, и ни один из f_i не совпадает с f_j даже с точностью до постоянного множителя при $i \neq j$. Пусть $\mathbb{Q} \subset k$. Докажите, что

$$\operatorname{GCD}(f, f') = f_1^{r_1 - 1} \ldots f_l^{r_l - 1}.$$

Указание: Доказательство аналогично доказательству упр. 14 к **§ 5** гл. 1. В доказательстве надо использовать единственность разложения. Условие $\mathbb{Q} \subset k$ гарантирует, что $f' \neq 0$.

7. Пусть $f, g \in \mathbb{C}[x]$ — полиномы положительной степени. Докажите, что f и g имеют общий корень в $\mathbb{C}$ в том и только том случае, когда $\operatorname{Res}(f, g, x) = 0$. Указание: используйте предложение 8 и тот факт, что $\mathbb{C}$ алгебраически замкнуто.

8. Пусть $f = a_0 x^l + \ldots + a_l \in k[x]$, где $a_0 \neq 0$ и $l > 0$. Определим его *дискриминант* следующим образом:

$$\operatorname{disc}(f) = \frac{(-1)^{l(l-1)/2}}{a_0} \operatorname{Res}(f, f', x).$$

Докажите, что f имеет кратный множитель (т. е. f делится на h^2, где $h \in k[x]$ — некоторый полином положительной степени) в том и только том случае, когда $\operatorname{disc}(f) = 0$. Указание: используйте предыдущее упражнение. Если $k = \mathbb{C}$, то из упр. 7 мы получаем, что полином имеет кратный корень в том и только том случае, когда его дискриминант равен нулю.

9. Используя предыдущее упражнение, определите, имеет ли полином $6x^4 - 23x^3 + 32x^2 - 19x + 4$ кратный корень в $\mathbb{C}$? Если да, то чему он равен?

10. Найдите дискриминант полинома второй степени $f = ax^2 + bx + c$. Объясните связь полученной формулы и стандартной формулы корней квадратного уравнения. Не используя упр. 8, докажите, что f имеет кратный корень в том и только том случае, когда дискриминант равен нулю.

11. Рассмотрим полиномы $f = 2x^2 + 3x + 1$ и $g = 7x^2 + x + 3$.
    (a) Используя алгоритм Евклида, найдите (вручную) $\operatorname{GCD}(f, g)$.
    (b) Найдите полиномы $A, B \in \mathbb{Q}[x]$, такие, что $Af + Bg = 1$. Указание: используйте вычисления из п. (a).
    (c) В уравнении, найденном в п. (b), избавьтесь от знаменателей. Объясните связь вашего ответа с результантом.

12. Объясните, почему если $f, g \in \mathbb{Z}[x]$, то $\operatorname{Res}(f, g, x) \in \mathbb{Z}$.

13. Пусть $f = xy - 1$ и $g = x^2 + y^2 - 4$. Эти полиномы будут рассматриваться как полиномы от x с коэффициентами в поле $k(y)$.
    (a) Составьте систему уравнений типа (7) для равенства $\widetilde{A}f + \widetilde{B}g = 1$ с этими f и g. Указание: $\widetilde{A}$ линеен, а $\widetilde{B}$ — константа, так что у вас должна получиться система из трех уравнений с тремя неизвестными.
    (b) Используйте правило Крамера и найдите решение системы, построенной в п. (a). Указание: результант является знаменателем.
    (c) Какое уравнение вы получите после избавления от знаменателей в уравнении из п. (b)? Указание: см. уравнение (8).

14. Результант $\operatorname{Res}(f, g, x)$ был определен для случая, когда оба полинома имеют положительную степень. В этом упражнении мы рассмотрим случай, когда один или оба полинома являются константами.
    (a) Пусть степень f равна $l > 0$, а $g = b_0$ — константа (возможно, нуль). Докажите, что матрица Сильвестра полиномов f и g — это диагональная $l \times l$-матрица с b_0 на главной диагонали. Выведите отсюда, что $\operatorname{Res}(f, g, x) = b_0^l$.
    (b) Докажите, что предложения 8 и 9 справедливы, если f и g такие, как в п. (a).
    (c) Чему равен $\operatorname{Res}(f, g, x)$, если $f = a_0$ — константа (возможно, нуль), а g — полином степени $m > 0$? Объясните ход ваших рассуждений.
    (d) Осталось разобрать последний случай, когда и $f = a_0$, и $g = b_0$ — константы. Здесь результант можно определить так:

$$\operatorname{Res}(a_0, b_0) = \begin{cases} 0, & \text{если } a_0 = 0 \quad \text{или} \quad b_0 = 0, \\ 1, & \text{если } a_0 \neq 0 \quad \text{и} \quad b_0 \neq 0. \end{cases}$$

Пусть $f = g = 2$ в $\mathbb{Q}[x]$. Покажите на этом примере, что предложения 8 и 9 оказываются неверными, если f и g — константы. Указание: вспомните, что некоторые объекты должны быть целочисленными полиномами от коэффициентов полиномов f и g.

15. Пусть степень полинома f равна l, а степень полинома g равна m. Докажите, что

$$\operatorname{Res}(f, g, x) = (-1)^{lm} \operatorname{Res}(g, f, x).$$

Указание: определитель меняет знак при перестановке двух столбцов.

16. Пусть $f = a_0 x^l + \ldots + a_l$ и $g = b_0 x^m + \ldots + b_m$ — полиномы из $k[x]$, и пусть $l \geq m$.
    (a) Рассмотрим полином $\tilde{f} = f - (a_0/b_0) x^{l-m} g$. Тогда $\deg(\tilde{f}) \leq l - 1$. Пусть $\deg(\tilde{f}) = l - 1$. Докажите, что

$$\operatorname{Res}(f, g, x) = (-1)^m b_0 \operatorname{Res}(\tilde{f}, g, x).$$

Указание: используйте элементарные преобразования столбцов матрицы Сильвестра. Нужно вычесть первые m столбцов из g-части матрицы, умноженных на a_0/b_0, из соответствующих столбцов f-части, а затем разложить определитель по первой строке. (В связи с этим см. теорему 5.7 из работы FINKBEINER (1978).)
    (b) Пусть $\tilde{f}$ такой же, как в п. (a), и пусть его степень может быть строго меньше $l - 1$. Докажите, что

$$\operatorname{Res}(f, g, x) = (-1)^{m(l-\deg(\tilde{f}))} b_0^{l-\deg(\tilde{f})} \operatorname{Res}(\tilde{f}, g, x).$$

Указание: показатель степени $l - \deg(\tilde{f})$ указывает, сколько раз нужно производить разложение по строке.

(c) Примените алгоритм деления и представьте f в виде $f = qg + r$, где $\deg(r) < \deg(g)$. Теперь, используя п. (b), докажите, что

$$\operatorname{Res}(f,g,x) = (-1)^{m(l-\deg(r))} b_0^{l-\deg(r)} \operatorname{Res}(r,g,x).$$

17. В этом упражнении на основе алгоритма Евклида будет построен алгоритм для вычисления результанта. Основная идея такова: для вычисления $\operatorname{GCD}(f,g)$ использовался алгоритм деления. Мы представляли f в виде $f = qg + r$, затем g в виде $g = q'r + r'$ и т. д. Формула (5) из § 5 гл. 1

$$\operatorname{GCD}(f,g) = \operatorname{GCD}(g,r) = \operatorname{GCD}(r,r') = \dots$$

позволяет найти наибольший общий делитель, так так степени полиномов уменьшаются. Теперь, используя упр. 15 и 16, мы можем дать «результантную» версию этих равенств:

$$\begin{aligned}
\operatorname{Res}(f,g,x) &= (-1)^{\deg(g)(\deg(f)-\deg(r))} b_0^{\deg(f)-\deg(r)} \operatorname{Res}(r,g,x) \\
&= (-1)^{\deg(f)\deg(g)} b_0^{\deg(f)-\deg(r)} \operatorname{Res}(g,r,x) \\
&= (-1)^{\deg(f)\deg(g)+\deg(r)(\deg(g)-\deg(r'))} b_0^{\deg(f)-\deg(r)} \\
&\quad \times {b_0'}^{\deg(g)-\deg(r')} \operatorname{Res}(r',r,x) \\
&= (-1)^{\deg(f)\deg(g)+\deg(g)\deg(r)} b_0^{\deg(f)-\deg(r)} \\
&\quad \times {b_0'}^{\deg(g)-\deg(r')} \operatorname{Res}(r,r',x),
\end{aligned}$$

где b_0 (соответственно b_0') — это старший коэффициент полинома g (соответственно r). Продолжая этот процесс, мы можем свести вычисление результанта к случаю, когда второй полином является константой, а затем применить упр. 14.

Запишем этот алгоритм в псевдокоде. Для этого нам понадобятся две переменные: r = остаток(f,g), т. е. остаток от деления f на g, и ст. коэфф.(f), т. е. старший коэффициент f. Вот этот алгоритм:

Вход: f, g
Выход: res
$h := f$
$s := g$
$res := 1$
WHILE $\deg(s) > 0$ DO
$\quad r :=$ остаток(h,s)
$\quad res := (-1)^{\deg(h)\deg(s)}$ ст. коэфф.$(s)^{\deg(h)-\deg(r)} res$
$\quad h := s$
$\quad s := r$
IF $h = 0$ OR $s = 0$ THEN $res := 0$ ELSE
IF $\deg(h) > 0$ THEN $res := s^{\deg(h)} res$

Докажите, что этот алгоритм вычисляет $\operatorname{Res}(f,g,x)$. Указание: используйте упр. 14, 15 и 16 и следуйте доказательству предложения 6 из § 5 гл. 1.

§ 6. Результанты и теорема о продолжении

В этом параграфе мы докажем теорему продолжения, используя результаты § 5. Наша первая задача — это обобщить теорию результантов на случай полиномов от нескольких переменных. Пусть нам даны полиномы $f, g \in k[x_1, \dots, x_n]$ положительной степени по x_1:

$$\begin{aligned}
f &= a_0 x_1^l + \dots + a_l, \quad a_0 \neq 0, \\
g &= b_0 x_1^m + \dots + b_m, \quad b_0 \neq 0,
\end{aligned} \tag{1}$$

где $a_i, b_j \in k[x_2, \dots, x_n]$. *Результантом* полиномов f и g по отношению к x_1 называется определитель

$$\operatorname{Res}(f,g,x_1) = \det \begin{pmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
 & a_1 & \ddots & & & b_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \dots & b_0 \\
 & \vdots & & a_1 & & \vdots & & b_1 \\
a_l & & & & b_m & & & \\
 & a_l & & \vdots & & b_m & & \vdots \\
 & & \ddots & & & & \ddots & \\
 & & & a_l & & & & b_m
\end{pmatrix}$$

порядка $l + m$. Здесь первые m столбцов заняты элементами a_i, а следующие l столбцов — элементами b_j, причем в пустых местах матрицы стоят нули.

Для полиномов от нескольких переменных результаты § 5 могут быть переформулированы следующим образом.

Предложение 1. *Пусть $f, g \in k[x_1, \dots, x_n]$ — полиномы положительной степени по x_1. Тогда*

(i) $\operatorname{Res}(f,g,x_1)$ *принадлежит первому исключающему идеалу* $\langle f,g\rangle \cap k[x_2, \dots, x_n]$.
(ii) $\operatorname{Res}(f,g,x_1) = 0$ *в том и только том случае, когда f и g имеют общий множитель в $k[x_1, \dots, x_n]$ положительной степени по x_1.*

Доказательство. Так как результант является целочисленным полиномом от коэффициентов полиномов f и g (предложение 8 из § 5), то $\operatorname{Res}(f,g,x_1) \in k[x_2, \dots, x_n]$. Мы также знаем, что

$$Af + Bg = \operatorname{Res}(f,g,x_1),$$

где A и B — полиномы от x_1, коэффициенты которых являются целочисленными полиномами от a_i, b_j (предложение 9 из § 5), т. е. $A, B \in k[x_2, \ldots, x_n][x_1] = k[x_1, \ldots, x_n]$. Значит, $\mathrm{Res}(f, g, x_1) \in \langle f, g \rangle$. Это доказывает (i).

Докажем (ii). Предложение 8 из § 5 поможет нам интерпретировать равенство результанта нулю в терминах общих делителей. В § 5 мы работали с полиномами от одной переменной с коэффициентами в некотором поле. Так как f и g — полиномы от x_1 с коэффициентами в $k[x_2, \ldots, x_n]$, то *полем* здесь является $k(x_2, \ldots, x_n)$. Предложение 8 из § 5 утверждает: если $f, g \in k(x_2, \ldots, x_n)[x_1]$, то $\mathrm{Res}(f, g, x_1) = 0$ в том и только том случае, когда f и g имеют общий делитель в $k(x_2, \ldots, x_n)[x_1]$ положительной степени по x_1. Но по следствию 4 из § 5 это эквивалентно тому, что f и g имеют общий делитель в $k[x_1, \ldots, x_n]$ положительной степени по x_1. Предложение доказано. □

Легко доказать, что два полинома из $\mathbb{C}[x]$ имеют общий делитель в том и только том случае, когда они имеют общий корень. Таким образом, мы имеем следующее утверждение.

Следствие 2. *Если $f, g \in \mathbb{C}[x]$, то $\mathrm{Res}(f, g, x) = 0$ в том и только том случае, когда f и g имеют общий корень в $\mathbb{C}$.*

Теперь мы покажем, как результанты применяются для продолжения частичных решений. Следующее предложение является ключевым в доказательстве теоремы о продолжении.

Предложение 3. *Пусть $f, g \in \mathbb{C}[x_1, \ldots, x_n]$, и пусть $a_i, b_j \in \mathbb{C}[x_2, \ldots, x_n]$, как в (1). Если $\mathrm{Res}(f, g, x_1) \in \mathbb{C}[x_2, \ldots, x_n]$ равен нулю в точке $(c_2, \ldots, c_n) \in \mathbb{C}^{n-1}$, то или*

(i) *a_0 или b_0 равно нулю в этой точке, или*
(ii) *существует $c_1 \in \mathbb{C}$, такое, что f и g равны нулю в точке $(c_1, \ldots, c_n) \in \mathbb{C}^n$.*

Доказательство. Для упрощения доказательства мы введем некоторые обозначения. Пусть $\mathbf{c} = (c_2, \ldots, c_n)$ и $f(x_1, \mathbf{c}) = f(x_1, c_2, \ldots, c_n)$. Нам нужно доказать, что полиномы от одной переменной $f(x_1, \mathbf{c})$ и $g(x_1, \mathbf{c})$ имеют общий корень, если $a_0(\mathbf{c})$ и $b_0(\mathbf{c})$ оба не равны нулю. Запишем

$$\begin{aligned} f(x_1, \mathbf{c}) &= a_0(\mathbf{c})x_1^l + \ldots + a_l(\mathbf{c}), \quad a_0(\mathbf{c}) \neq 0, \\ g(x_1, \mathbf{c}) &= b_0(\mathbf{c})x_1^m + \ldots + b_m(\mathbf{c}), \quad b_0(\mathbf{c}) \neq 0. \end{aligned} \tag{2}$$

По условию $h = \mathrm{Res}(f, g, x_1)$ равен нулю в $\mathbf{c}$. Таким образом,

$$0 = h(\mathbf{c}) = \det \begin{pmatrix} a_0(\mathbf{c}) & & & b_0(\mathbf{c}) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0(\mathbf{c}) & \vdots & & b_0(\mathbf{c}) \\ a_l(\mathbf{c}) & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix}. \tag{3}$$

Здесь m столбцов заняты элементами $a_i(\mathbf{c})$, а l столбцов — элементами $b_j(\mathbf{c})$. По (2) результант полиномов $f(x_1, \mathbf{c})$ и $g(x_1, \mathbf{c})$ — это в точности определитель (3), т. е.

$$0 = h(\mathbf{c}) = \mathit{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1).$$

Тогда по следствию 2 полиномы $f(x_1, \mathbf{c})$ и $g(x_1, \mathbf{c})$ имеют общий корень. Предложение доказано. □

Теперь у нас есть все необходимое для доказательства теоремы о продолжении. Но сначала мы рассмотрим частный случай, когда идеал порожден двумя полиномами.

Теорема 4 (теорема о продолжении для двух полиномов). *Пусть $I = \langle f, g \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$, и пусть I_1 — первый исключающий идеал идеала I, а a_0, b_0 такие же, как в (1). Предположим, что $(c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ — частичное решение. Тогда если $(c_2, \ldots, c_n) \notin \mathbf{V}(a_0, b_0)$, то существует $c_1 \in \mathbb{C}$, такое, что $(c_1, \ldots, c_n) \in \mathbf{V}(I)$.*

Доказательство. Как и в предложении 3, мы будем использовать обозначение $\mathbf{c} = (c_2, \ldots, c_n)$. Из предложения 1 мы знаем, что $\mathrm{Res}(f, g, x_1) \in I_1$; поэтому в точке $\mathbf{c}$ результант обращается в нуль. Если $a_0(\mathbf{c})$ и $b_0(\mathbf{c})$ оба не равны нулю, то требуемое c_1 существует по предложению 3.

К сожалению, условие теоремы требует, чтобы лишь одно (а не оба сразу) из чисел $a_0(\mathbf{c})$ и $b_0(\mathbf{c})$ было отлично от нуля. Пусть $a_0(\mathbf{c}) \neq 0$, а $b_0(\mathbf{c}) = 0$. Тогда степень полинома $g_1(x_1, \mathbf{c})$ по x_1 строго меньше m, т. е. определитель (3) порядка $(l+m) \times (l+m)$ *слишком велик*, чтобы быть результантом полиномов $f(x_1, \mathbf{c})$ и $g(x_1, \mathbf{c})$. Хотя между (3) и $\mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$ имеется связь (этот факт будет рассмотрен в упражнениях), мы применим другой подход.

Идея состоит в том, что $\mathbf{V}(f, g)$ зависит лишь от идеала $\langle f, g \rangle$ и не зависит от выбора его базиса. Поэтому в случае $a_0(\mathbf{c}) \neq 0$, $b_0(\mathbf{c}) = 0$ мы перейдем к другому базису. Пусть N — натуральное

число. Доказательство утверждения

$$\langle f, g\rangle = \langle f, g + x_1^N f\rangle \tag{4}$$

мы оставляем читателю в качестве упражнения. Выберем N так, чтобы степень полинома $x_1^N f$ по x_1 была больше, чем степень полинома g по x_1. Тогда старший коэффициент полинома $g + x_1^N f$ по x_1 равен $a_0 \neq 0$. Значит, существует $c_1 \in \mathbb{C}$, такое, что $(c_1, \mathbf{c}) \in \mathbf{V}(f, g + x_1^N f)$, т. е., согласно (4), $(c_1, \mathbf{c}) \in \mathbf{V}(f, g)$. Теорема доказана. □

Обратите внимание, что доказательство не проходит, если $a_0(\mathbf{c}) = b_0(\mathbf{c}) = 0$ для частичного решения $\mathbf{c}$. Главная причина здесь, разумеется, в том, что в этом случае частичное решение $\mathbf{c}$ *может не продолжаться*. Пример (4) из § 1 показывает, что это действительно может происходить.

Рассмотрим теперь, как процесс исключения связан с базисами Грёбнера и результантами. Если $f, g \in \mathbb{C}[x_1, \ldots, x_n]$, то базис Грёбнера и результант сообщают нам разные вещи о первом исключающем идеале I_1 идеала $\langle f, g\rangle$. Базис Грёбнера быстро *описывает* I_1, но не исключает возможности того, что $I_1 = \{0\}$. Наоборот, результант *предъявляет* элемент из I_1, который сразу позволяет делать выводы о существовании частичного решения. Так как теорема о продолжении по существу есть теорема *существования*, то нам нужно нечто большее, чем просто описание идеала I_1. Именно поэтому роль результантов в доказательстве так велика.

Теперь, наконец, нам нужно доказать теорему о продолжении для произвольного идеала $\langle f_1, \ldots, f_s\rangle \subset \mathbb{C}[x_1, \ldots, x_n]$. Однако мы определяли результант только двух полиномов. Что такое «результант» полиномов $f_1, \ldots, f_s$, если $s \geq 3$? Идея состоит в том, чтобы ввести новые переменные $u_2, \ldots, u_s$ и превратить набор $f_2, \ldots, f_n$ в один полином

$$u_2 f_2 + \ldots + u_s f_s \in \mathbb{C}[u_2, \ldots, u_s, x_1, \ldots, x_n].$$

Мы будем рассматривать полином f как элемент того же кольца. По предложению 1 результант полиномов f и $u_2 f_2 + \ldots + u_s f_s$ принадлежит $\mathbb{C}[u_2, \ldots, u_s, x_2, \ldots, x_n]$. Чтобы получить полиномы от $x_2, \ldots, x_n$, разложим результант по степеням $u_2, \ldots, u_s$:

$$\operatorname{Res}(f_1, u_2 f_2 + \ldots + u_s f_s, x_1) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) u^\alpha, \tag{5}$$

где u^α обозначает моном $u_2^{\alpha_2} \ldots u_s^{\alpha_s}$ (см. обозначение в гл. 1), а $h_\alpha \in \mathbb{C}[x_2, \ldots, x_n]$ для всех α. Полиномы h_α называются *обобщенными результантами* полиномов $f_1, \ldots, f_s$.

В качестве примера найдем обобщенные результанты полиномов

$$\begin{aligned} f_1 &= x^2 + y + z - 1, \\ f_2 &= x + y^2 + z - 1, \\ f_3 &= x + y + z^2 - 1 \end{aligned}$$

(см. пример (1) из § 1). Имеем

$$\begin{aligned} \operatorname{Res}(f_1, u_2 f_2 + u_3 f_3, x) =& (y^4 + 2y^2 z - 2y^2 + z^2 + y - z) u_2^2 \\ &+ 2(y^2 z^2 + y^3 + z^3 - y^2 - z^2 + yz) u_2 u_3 \\ &+ (z^4 + 2yz^2 + y^2 - 2z^2 - y + z) u_3^2. \end{aligned}$$

Таким образом, обобщенные результанты равны

$$\begin{aligned} h_{20} &= y^4 + 2y^2 z - 2y^2 + z^2 + y - z, \\ h_{11} &= 2(y^2 z^2 + y^3 + z^3 - y^2 - z^2 + yz), \\ h_{02} &= z^4 + 2yz^2 + y^2 - 2z^2 - y + z. \end{aligned}$$

Обратите внимание, что обобщенные результанты зависят от того, какой полином мы считаем первым. Обобщенные результанты набора f_2, f_1, f_3 будут другими.

На практике обобщенные результанты используются редко. Но они совершенно необходимы для доказательства теоремы о продолжении. Напомним ее формулировку.

Теорема 5 (теорема о продолжении). *Пусть* $I = \langle f_1, \ldots, f_s\rangle \subset \mathbb{C}[x_1, \ldots, x_n]$, *а* I_1 *— первый исключающий идеал. Для каждого* $i, 1 \leq i \leq s$, *запишем* f_i *в виде*

$$f_i = g_i(x_2, \ldots, x_n) x_1^{N_i} + \textit{члены, содержащие } x_1 \textit{ в степени } < N_i,$$

где $N_i \geq 0$, *а* $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ *— ненулевые полиномы. Пусть* $(c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ *— частичное решение. Тогда если* $(c_2, \ldots, c_n) \notin \mathbf{V}(g_1, \ldots, g_s)$, *то существует* $c_1 \in \mathbb{C}$, *такое, что* $(c_1, c_2, \ldots, c_n) \in \mathbf{V}(I)$.

Доказательство. Пусть $\mathbf{c} = (c_2, \ldots, c_n)$. Мы будем искать общий корень c_1 полиномов $f_1(x_1, \mathbf{c}), \ldots, f_s(x_1, \mathbf{c})$. Случай $s = 2$ рассмотрен в теореме 4; случай $s = 1$ сводится к случаю $s = 2$, так как $\mathbf{V}(f_1) = \mathbf{V}(f_1, f_1)$. Осталось доказать теорему при $s \geq 3$.

Так как $\mathbf{c} \notin \mathbf{V}(g_1, \ldots, g_s)$, то мы можем считать, что $g_1(\mathbf{c}) \neq 0$. Пусть $h_\alpha \in \mathbf{C}[x_2, \ldots, x_n]$ — обобщенные результанты полиномов $f_1, \ldots, f_s$, т. е.

$$\operatorname{Res}(f_1, u_2 f_2 + \ldots + u_s f_s, x_1) = \sum_\alpha h_\alpha u^\alpha. \tag{6}$$

Мы докажем, что h_α принадлежат первому исключающему идеалу I_1. Так как все вычисления мы проводим в кольце $\mathbb{C}[u_2,\dots,u_s,x_1,\dots,x_n]$, то из предложения 1 следует, что

$$Af_1 + B(u_2f_2 + \dots + u_sf_s) = \operatorname{Res}(f_1, u_2f_2 + \dots + u_sf_s, x_1) \qquad (7)$$

для некоторых полиномов $A, B \in \mathbb{C}[u_2,\dots,u_s,x_1,\dots,x_n]$. Пусть $A = \sum_\alpha A_\alpha u^\alpha$ и $B = \sum_\beta B_\beta u^\beta$, где $A_\alpha, B_\beta \in \mathbb{C}[x_1,\dots,x_n]$. Мы докажем, что $h_\alpha \in \langle f_1,\dots,f_s\rangle = I$, сравнивая коэффициенты при u^α в (7). Так как нам известно, что $h_\alpha \in \mathbb{C}[x_2,\dots,x_n]$, то из этого будет следовать, что $h_\alpha \in I_1$.

Для сравнения коэффициентов мы будем использовать обозначения из гл. 1. Положим $e_2 = (1,0,\dots,0),\dots,e_s = (0,\dots,0,1)$, так что $u_2f_2 + \dots + u_sf_s = \sum_{i\ge 2} u^{e_i}f_i$. Теперь (7) может быть записано в виде

$$\begin{aligned}
\sum_\alpha h_\alpha u^\alpha &= \left(\sum_\alpha A_\alpha u^\alpha\right) f_1 + \left(\sum_\beta B_\beta u^\beta\right)\left(\sum_{i\ge 2} u^{e_i} f_i\right) \\
&= \sum_\alpha (A_\alpha f_1)u^\alpha + \sum_{i\ge 2,\beta} B_\beta f_i u^{\beta+e_i} \\
&= \sum_\alpha (A_\alpha f_1)u^\alpha + \sum_\alpha \left(\sum_{\substack{i\ge 2,\beta\\ \beta+e_i=\alpha}} B_\beta f_i\right) u^\alpha \\
&= \sum_\alpha \left(A_\alpha f_1 + \sum_{\substack{i\ge 2,\beta\\ \beta+e_i=\alpha}} B_\beta f_i\right) u^\alpha.
\end{aligned}$$

Приравнивая коэффициенты при u^α, получаем

$$h_\alpha = A_\alpha f_1 + \sum_{\substack{i\ge 2,\beta\\ \beta+e_i=\alpha}} B_\beta f_i,$$

что и доказывает принадлежность $h_\alpha \in I$. Как мы видели выше, из этого следует, что $h_\alpha \in I_1$ для всех α.

Так как $\mathbf{c} \in \mathbf{V}(I_1)$, то $h_\alpha(\mathbf{c}) = 0$ для всех α. Теперь из (6) следует, что результант $h = \operatorname{Res}(f_1, u_2f_2 + \dots + u_sf_s, x_1)$ обращается в нуль в $\mathbf{c}$. Обозначим через $h(\mathbf{c}, u_2,\dots,u_s)$ полином в $\mathbb{C}[x_1,u_2,\dots,u_s]$, полученный при подстановке $\mathbf{c} = (c_2,\dots,c_n)$ вместо $(x_2,\dots,x_n)$. Имеем

$$h(\mathbf{c}, u_2,\dots,u_n) = 0. \qquad (8)$$

Предположим теперь, что

$$\begin{aligned}
&g_2(\mathbf{c}) \ne 0 \text{ и степень полиномов } f_2 \text{ по } x_1 \\
&\text{больше степеней полиномов } f_3,\dots,f_s.
\end{aligned} \qquad (9)$$

Мы утверждаем, что из этого следует равенство

$$h(\mathbf{c}, u_2,\dots,u_s) = \operatorname{Res}(f_1(x_1,\mathbf{c}), u_2f_2(x_1,\mathbf{c}) + \dots + u_sf_s(x_1,\mathbf{c}), x_1). \qquad (10)$$

Его доказательство аналогично доказательству равенства (3). А именно, если мы вычислим определитель, задающий $h = \operatorname{Res}(f_1, u_2f_2 + \dots + u_sf_s, x_1)$, в $\mathbf{c}$, то увидим, что $h(\mathbf{c}, u_2,\dots,u_s)$ задано некоторым определителем. Более того, этот определитель есть результант из (10), *но при условии*, что старшие коэффициенты полиномов f_1 и $u_2f_2 + \dots + u_sf_s$ не равны нулю в $\mathbf{c}$. Это справедливо для f_1, так как $g_1(\mathbf{c}) \ne 0$. Но по условию (9) старший коэффициент по x_1 в $u_2f_2 + \dots + u_sf_s$ равен u_2g_2, а $g_2(\mathbf{c}) \ne 0$. Равенство (10) доказано.

Объединяя (8) и (10), получаем

$$\operatorname{Res}(f_1(x_1,\mathbf{c}), u_2f_2(x_1,\mathbf{c}) + \dots + u_sf_s(x_1,\mathbf{c}), x_1) = 0.$$

Полиномы $f_1(x_1,\mathbf{c})$ и $u_2f_2(x_1,\mathbf{c}) + \dots + u_sf_s(x_1,\mathbf{c})$ принадлежат кольцу $\mathbb{C}[x_1,\dots,u_2,\dots,u_s]$. По предложению 1 из равенства нулю их результанта следует, что эти два полинома имеют общий множитель F положительной степени по x_1. Так как F делит $f_1(x_1,\mathbf{c})$, то $F \in \mathbb{C}[x_1]$. Мы утверждаем, что F делит каждый из полиномов $f_2(x_1,\mathbf{c}),\dots,f_s(x_1,\mathbf{c})$. В самом деле,

$$F(x_1)A(x_1,u_2,\dots,u_s) = u_2f_2(x_1,\mathbf{c}) + \dots + u_sf_s(x_1,\mathbf{c}) \qquad (11)$$

для некоторого полинома $A \in \mathbb{C}[x_1,u_2,\dots,u_s]$. Из сравнения коэффициентов при $u_2,\dots,u_s$ следует, что полином F делит $f_2(x_1,\mathbf{c})$, $\dots, f_s(x_1,\mathbf{c})$. Детали доказательства мы оставляем читателю в качестве упражнения.

Так как F делит также и $f_1(x_1,\mathbf{c})$, то мы видим, что F является общим делителем положительной степени *всех* $f_i(x_1,\mathbf{c})$. Пусть c_1 — корень полинома F (корень существует, так как мы работаем над $\mathbb{C}$). Тогда c_1 автоматически является общим корнем *всех* $f_i(x_1,\mathbf{c})$. Таким образом, теорема о продолжении доказана, если (9) имеет место.

Если (9) не выполняется для $f_1,\dots,f_s$, то нетрудно найти новый базис, для которого (9) имеет место. Нужно заменить f_2 на $f_2 + x_1^N f_1$, где N — натуральное число. Читатель должен проверить, что

$$I = \langle f_1, f_2 + x_1^N f_1, f_3,\dots,f_s\rangle.$$

Если N достаточно велико, то старшим коэффициентом полинома $f_2 + x_1^N f_1$ будет g_1, который не равен нулю в $\mathbf{c}$. Аналогично, при достаточно большом N мы можем предполагать, что $f_2 + x_1^N f_1$ имеет бóльшую степень по x_1, чем $f_3, \dots, f_s$. Теперь существует общий корень c_1 полиномов $f_1(x_1, \mathbf{c}), f_2(x_1, \mathbf{c}) + x_1^N f_1(x_1, \mathbf{c}), f_3(x_1, \mathbf{c}), \dots, f_s(x_1, \mathbf{c})$. Отсюда следует, что c_1 является общим корнем всех $f_i(x_1, \mathbf{c})$. Доказательство теоремы о продолжении закончено. □

Отметим, наконец, что теорема о продолжении справедлива над любым алгебраически замкнутым полем. Мы формулировали теорему только над $\mathbb{C}$, но анализ доказательства показывает, что требуемое c_1 существует именно потому, что любой непостоянный полином из $\mathbb{C}[x_1]$ имеет корень в $\mathbb{C}$. Так как это имеет место для любого алгебраически замкнутого поля, то, следовательно, и теорема о продолжении выполняется над такими полями (см. упр. 14).

Упражнения к § 6

1. Рассмотрим в $k[x, y]$ два полинома

$$f = x^2y - 3xy^2 + x^2 - 3xy,$$
$$g = x^3y + x^3 - 4y^2 - 3y + 1.$$

   (a) Найдите $\operatorname{Res}(f, g, x)$.
   (b) Найдите $\operatorname{Res}(f, g, y)$.
   (c) Что говорит результат п. (b) о f и g?

2. Пусть $f, g \in \mathbb{C}[x, y]$. В этом упражнении мы докажем, что

$$\mathbf{V}(f, g) \text{ бесконечно} \Leftrightarrow f \text{ и } g \text{ имеют непостоянный общий делитель в } \mathbb{C}[x, y].$$

   (a) Докажите, что $\mathbf{V}(f)$ бесконечно, если f — непостоянный полином. Указание: если f имеет положительную степень по x, то его старший коэффициент по x может обращаться в нуль только в конечном числе значений y. Теперь воспользуйтесь алгебраической замкнутостью поля $\mathbb{C}$.
   (b) Пусть f и g имеют непостоянный общий делитель $h \in \mathbb{C}[x, y]$. Используя п. (a), докажите, что в этом случае $\mathbf{V}(f, g)$ бесконечно.
   (c) Пусть f и g не имеют общих делителей положительной степени. Докажите, что $\operatorname{Res}(f, g, x)$ и $\operatorname{Res}(f, g, y)$ не равны нулю. Докажите, что из этого следует конечность многообразия $\mathbf{V}(f, g)$.

3. Пусть $f, g \in k[x, y]$. Тогда по предложению 1 $\operatorname{Res}(f, g, x) \in I_1 = \langle f, g \rangle \cap k[y]$. Оказывается, результант *не всегда* порождает I_1.
   (a) Докажите, что $\operatorname{Res}(f, g, x)$ порождает I_1, если $f = xy - 1$ и $g = x^2 + y^2 - 4$.

   (b) Докажите, что $\operatorname{Res}(f, g, x)$ не порождает I_1, если $f = xy - 1$, а $g = yx^2 + y^2 - 4$.
   Существует ли связь между п. (b) и теоремой о продолжении?

4. Пусть $f, g \in \mathbb{C}[x]$ — полиномы положительной степени. В этом упражнении мы сконструируем полином, корни которого суть все суммы корня полинома f и корня полинома g.
   (a) Докажите, что число $\gamma \in \mathbb{C}$ имеет вид $\gamma = \alpha + \beta$, где $f(\alpha) = g(\beta) = 0$, в том и только том случае, когда уравнения $f(x) = g(y - x) = 0$ имеют общее решение при $y = \gamma$.
   (b) Используя теорему 3, докажите, что γ является корнем полинома $\operatorname{Res}(f(x), g(y - x), x)$ в том и только том случае, когда $\gamma = \alpha + \beta$, где $f(\alpha) = g(\beta) = 0$.
   (c) Постройте полином с рациональными коэффициентами, имеющий корень $\sqrt{2} + \sqrt{3}$. Указание: чему равны f и g в этом случае?
   (d) Модифицируйте вашу конструкцию и постройте полином, корни которого являются разностями: корень полинома f минус корень полинома g.

5. Пусть $f, g \in \mathbb{C}[x]$ — полиномы положительной степени, и пусть все корни полинома f отличны от нуля. Используя конструкцию упр. 4, постройте полином, корни которого являются произведениями корня полинома f и корня полинома g.

6. Пусть $f, g \in \mathbb{Q}[x]$ — полиномы положительной степени.
   (a) Большинство систем компьютерной алгебры умеет разлагать полиномы над $\mathbb{Q}$ на неприводимые (над $\mathbb{Q}$) множители. В частности, можно определить, имеет ли данный полином целый корень. Используя п. (d) упр. 4, постройте алгоритм, проверяющий, имеют ли полиномы f и g корни α и β соответственно, такие, что разность $\alpha - \beta$ есть целое число?
   (b) Докажите, что полиномы $f = x^5 - 2x^3 - 2x^2 + 4$ и $g = x^5 + 5x^4 + 8x^3 + 2x^2 - 5x + 1$ имеют корни α и β соответственно, такие, что разность $\alpha - \beta$ — целое число. Чему оно равно?

7. В § 3 было упомянуто, что результанты бывают полезны при решении задач неявного описания. Рассмотрим параметрическую кривую

$$u = \frac{t^2}{1 + t^2}, \quad v = \frac{t^3}{1 + t^2}.$$

Сначала избавимся от знаменателей:

$$u(1 + t^2) - t^2 = 0, \quad v(1 + t^2) - t^3 = 0,$$

а потом исключим t с помощью результанта. Сравните ваш ответ с ответом, полученным в § 3 другими методами. (Обратите внимание на упр. 13 к § 3.)

8. В доказательстве теоремы 3 мы вычислили в точке $\mathbf{c}$ результант $h = \operatorname{Res}(f, g, x_1)$ и использовали тот факт, что полученное выражение также является результантом. Но так бывает не всегда.
   (a) Пусть $f = x^2y + 3x - 1$ и $g = 6x^2 + y^2 - 4$. Вычислите результант $h = \operatorname{Res}(f, g, x)$ и покажите, что $h(0) = -180$. Теперь положим $y = 0$ в f и g, т. е. получим полиномы $3x - 1$ и $6x^2 - 4$. Имеем $\operatorname{Res}(3x - 1, 6x^2 - 4, x) = -30$. Таким образом, $h(0)$ *не является* результантом — ошибка в 6 раз. Обратите внимание на причину: h — это определитель 4-го порядка, а $\operatorname{Res}(3x - 1, 6x^2 - 4, x)$ — это определитель 3-го порядка.
   (b) Пусть $f = x^2y + 3xy - 1$ и $g = 6x^2 + y^2 - 4$. Вычислите $h = \operatorname{Res}(f, g, x)$ и проверьте, что $h(0) = 36$. Подставив $y = 0$ в f и g, получим полиномы -1 и $x^2 - 4$. Используя упр. 14 к § 5, докажите, что результант этих полиномов равен 1 — ошибка в 36 раз.

   Когда степень f уменьшается на 1 (как в п. (a)), то возникает множитель 6, когда эта степень уменьшается на 2 (как в п. (b)), то возникает множитель $36 = 6^2$. Но старший коэффициент по x в g равен 6. В упр. 11 мы увидим, что это не случайность.

9. Пусть $f = x^2y + x - 1$ и $g = x^2y + x + y^2 - 4$. Вычислите $h = \operatorname{Res}(f, g, x) \in \mathbb{C}[y]$ и докажите, что $h(0) = 0$. Но если мы подставим $y = 0$ в f и g, то получим полиномы $x - 1$ и $x - 4$. Результант этих двух полиномов не равен нулю, т. е. $h(0)$ *не* результант.

10. В упр. 8 и 9 мы показали, что подстановка в результант может привести к ошибке. Во всех рассмотренных примерах степень одного из полиномов уменьшалась после подстановки. В этом упражнении мы докажем, что подстановка работает, если степени не уменьшаются. Дадим строгую формулировку этого утверждения. Пусть $f, g \in k[x_1, \dots, x_n]$, а $\mathbf{c} = (c_{i+1}, \dots, c_n) \in k^{n-i}$, $i \geq 2$. Через $f(x_1, \dots, x_i, \mathbf{c})$ будет обозначаться результат подстановки. Запишем f и g в виде (1), т. е. $a_0, b_0 \in k[x_2, \dots, x_n]$ — старшие коэффициенты по x_1 в f и g соответственно. Пусть $h = \operatorname{Res}(f, g, x_1) \in k[x_2, \dots, x_n]$.
    (a) Пусть $a_0(x_2, \dots, x_i, \mathbf{c}) \neq 0$ и $b_0(x_2, \dots, x_i, \mathbf{c}) \neq 0$. Докажите, что
    $$h(x_2, \dots, x_i, \mathbf{c}) = \operatorname{Res}(f(x_1, \dots, x_i, \mathbf{c}), g(x_1, \dots, x_i, \mathbf{c}), x_1)$$
    в $k[x_2, \dots, x_i]$. Указание: используйте доказательство теоремы 3, равенство (3) особенно важно.
    (b) Обратите внимание, что в доказательстве теоремы 3 используется частный случай ($i = 1$) утверждения, доказанного в п. (a). Объясните, какую роль этот результат играет в доказательстве теоремы о продолжении в общем случае. Указание: обратите внимание на уравнение (10).

11. В этом упражнении мы рассмотрим, что происходит с результантом, если при подстановке степень одного из полиномов уменьшается. Пусть $f, g \in k[x_1, \dots, x_n]$ и $h = \operatorname{Res}(f, g, x_1)$. Пусть $\mathbf{c} = (c_2, \dots, c_n) \in k^{n-1}$ и $f(x_1, \mathbf{c}) \in k[x_1]$ — результат подстановки $\mathbf{c}$ в полином f. Пусть, как в (1), $a_0, b_0 \in k[x_2, \dots, x_n]$ — старшие коэффициенты по x_1 полиномов f и g соответственно. Предположим, что $a_0(\mathbf{c}) \neq 0$, а $b_0(\mathbf{c}) = 0$. Наша цель — установить зависимость между $h(\mathbf{c})$ и $\operatorname{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$.
    (a) Предположим сначала, что степень полинома g по x_1 уменьшилась ровно на 1, т. е. $b_1(\mathbf{c}) \neq 0$. Докажите, что
    $$h(\mathbf{c}) = a_0(\mathbf{c}) \cdot \operatorname{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1).$$
    Указание: $h(\mathbf{c})$ задается следующим определителем:
    $$h(\mathbf{c}) = \det \begin{pmatrix} a_0(\mathbf{c}) & & & & 0 & & & \\ a_1(\mathbf{c}) & a_0(\mathbf{c}) & & & b_1(\mathbf{c}) & 0 & & \\ & a_1(\mathbf{c}) & \ddots & & & b_1(\mathbf{c}) & \ddots & \\ \vdots & & \ddots & a_0(\mathbf{c}) & \vdots & & \ddots & 0 \\ & \vdots & & a_1(\mathbf{c}) & & \vdots & & b_1(\mathbf{c}) \\ a_l(\mathbf{c}) & & & & b_m(\mathbf{c}) & & & \\ & a_l(\mathbf{c}) & & \vdots & & b_m(\mathbf{c}) & & \\ & & \ddots & & & & \ddots & \\ & & & a_l(\mathbf{c}) & & & & b_m(\mathbf{c}) \end{pmatrix}.$$
    Здесь m столбцов заняты элементами a_i и l столбцов — элементами b_j. Этот определитель не равен результанту полиномов $f(x_1, \mathbf{c})$ и $g(x_1, \mathbf{c})$ — у него неправильный размер. Но если мы разложим его по первой строке, то получим требуемый результат (см. теорему 5.7 работы FINKBEINER (1978)).
    (b) Вернемся к общему случаю. Пусть степень полинома $g(x_1, \mathbf{c})$ равна $m - p$, где $p \geq 1$. Докажите, что
    $$h(\mathbf{c}) = a_0(\mathbf{c})^p \cdot \operatorname{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1).$$
    Указание: разложите определитель p раз. Обратите внимание, что это утверждение объясняет результаты упр. 8.

12. Пусть $I = \langle f_1, f_2, f_3 \rangle \subset k[w, x, y, z]$, где
    $$f_1 = x^4 - 2xy^2 + zw,$$
    $$f_2 = wx^2 - w^2z + y,$$
    $$f_3 = x^3 + 3w.$$
    (a) Вычислите обобщенные результанты полиномов f_1, f_2, f_3 по отношению к w. Вы должны получить два полинома $h_{10}, h_{01} \in k[x, y, z]$.
    (b) Покажите, что обобщенные результанты не порождают идеал $I_1 = I \cap k[x, y, z]$. Указание: используйте lex-упорядочение с $w > z > y > x$.

13. Пусть $f, g_1, \ldots, g_s \in k[x]$. Докажите, что f является общим дел
лем $g_1, \ldots, g_s$ в том и только том случае, когда f делит пол
$u_1 g_1 + \ldots + u_s g_s$ в $k[x, u_1, \ldots, u_s]$. Указание: обратите вниман
рассуждения, следующие за формулой (11) в тексте параграфа.

14. Докажите справедливость теоремы о продолжении над любы
гебраически замкнутым полем. Указание: вы должны понять,
именно доказательства следствия 2, предложения 3 и теорем 4
используют свойства поля $\mathbb{C}$.

4
Алгебро-геометрический «словарь»

В этой главе мы рассмотрим соответствие между идеалами и многообразиями. В §§ 1 и 2 мы докажем знаменитую теорему Гильберта о нулях, которая устанавливает, какие именно идеалы соответствуют многообразиям. Это позволит нам составить алгебро-геометрический «словарь» для перевода утверждений о многообразиях на язык идеалов (и обратно). Эти же вопросы будут рассматриваться в §§ 3 и 4, где мы определим ряд естественных алгебраических операций на множестве идеалов и будем изучать их геометрические аналоги. Поддерживая вычислительную направленность книги, мы опишем алгоритмы, реализующие эти алгебраические операции. В §§ 5 и 6 мы рассмотрим более важные алгебраические и геометрические идеи и понятия, возникающие в связи с теоремой Гильберта о базисе, а именно возможность разложения многообразия в объединение более простых многообразий и отвечающее ему в алгебре представление идеала в виде пересечения более простых идеалов.

§ 1. Теорема Гильберта о нулях

В гл. 1 было показано, что свойства многообразия $V \in k^n$ связаны со свойствами идеала

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \text{ для всех } x \in V\}$$

всех полиномов, обращающихся в нуль на V. Таким образом, мы имеем отображение

$$\begin{array}{ccc} \text{аффинные многообразия} & & \text{идеалы} \\ V & \longrightarrow & \mathbf{I}(V). \end{array}$$

Обратно, по данному идеалу $I \subset k[x_1, \ldots, x_n]$ мы можем определить множество

$$\mathbf{V}(I) = \{x \in k^n : f(x) = 0 \text{ для всех } f \in I\}.$$

Теорема Гильберта о базисе утверждает, что $\mathbf{V}(I)$ является аффинным многообразием, так как существует конечный набор полиномов

$f_1, \ldots, f_s \in I$, такой, что $I = \langle f_1, \ldots, f_s \rangle$, а в предложении 9 из § гл. 2 доказано, что $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$. Таким образом, мы име отображение

$$\begin{array}{ccc} \text{идеалы} & & \text{аффинные многообразия} \\ I & \longrightarrow & \mathbf{V}(I). \end{array}$$

Эти два отображения описывают соответствие между идеалами многообразиями, природа которого и будет изучаться в этой гла

Отметим сначала, что указанное соответствие (точнее, отобр жение $\mathbf{V}$) не является взаимно однозначным: одному и тому м многообразию могут соответствовать различные идеалы. Напр мер, $\langle x \rangle$ и $\langle x^2 \rangle$ — это различные идеалы в $k[x]$, но они определя одно и то же многообразие $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$. Еще более трудн проблемы возникают в случае, когда основное поле k не являет алгебраически замкнутым. Рассмотрим, например, три полинома $1 + x^2$ и $1 + x^2 + x^4$ в $\mathbb{R}[x]$. Эти полиномы порождают различн идеалы

$$I_1 = \langle 1 \rangle = \mathbb{R}[x], \quad I_2 = \langle 1 + x^2 \rangle, \quad I_3 = \langle 1 + x^2 + x^4 \rangle,$$

но ни один из этих полиномов не имеет вещественных корней; п этому соответствующие многообразия пусты:

$$\mathbf{V}(I_1) = \mathbf{V}(I_2) = \mathbf{V}(I_3) = \varnothing.$$

Полиномы от двух переменных $1 + x^2 + y^2$ и $1 + x^2 + y^4$ также имеют вещественных корней. Они порождают различные идеалы $\mathbb{R}[x, y]$, но соответствующие многообразия пусты.

Возникает вопрос, могут ли какие-либо идеалы определить п стое многообразие, если поле k алгебраически замкнуто. В случ одной переменной каждый идеал кольца $k[x]$ порождается одн полиномом, так как $k[x]$ — это область главных идеалов (см. § гл. 1). Таким образом, $I = \langle f \rangle$ для некоторого полинома $f \in k[$ Тогда $\mathbf{V}(I)$ — это множество корней полинома f. Но так как k алге раически замкнуто, то каждый непостоянный полином в $k[x]$ име корень. Поэтому $\mathbf{V}(I) = \varnothing$ в том и только том случае, когда f ненулевая константа. Но тогда $1/f \in k$; значит, $1 = (1/f) \cdot f \in I$, т $g = g \cdot 1 \in I$ для любого g. Таким образом, только в случае $I = k[$ многообразие $\mathbf{V}(I)$ пусто.

Удивительным образом это же справедливо и в случае нескол ких переменных: если k алгебраически замкнуто, то $\mathbf{V}(I) = \varnothing$ в т и только том случае, когда $I = k[x_1, \ldots, x_n]$. Это утверждение наз вается *слабой теоремой о нулях*. Слабая теорема о нулях являет основой (на самом деле она ему эквивалентна) одного из сам значительных математических результатов конца девятнадцат

века — теоремы Гильберта о нулях. Влияние этого результата таково, что и сегодня немецкое название этой теоремы *Nullstellensatz* является общеупотребительным. Этот термин образован способом, обычным для немецкого языка, из трех слов: Null (=нуль), Stellen (=точки), Satz (=теорема).

Теорема 1 (слабая теорема о нулях). *Пусть k алгебраически замкнуто, и пусть $I \subset k[x_1, \ldots, x_n]$ — идеал, такой, что $\mathbf{V}(I) = \varnothing$. Тогда $I = k[x_1, \ldots, x_n]$.*

Доказательство. Обычная стратегия доказательства того, что идеал I совпадает с полиномиальным кольцом $k[x_1, \ldots, x_n]$, состоит в том, чтобы убедиться, что $1 \in I$. В самом деле, если $1 \in I$, то $f = f \cdot 1 \in I$ для любого полинома $f \in k[x_1, \ldots, x_n]$.

Мы будем проводить индукцию по n — числу переменных. Если $n = 1$, то $I \subset k[x]$, и мы уже доказали выше справедливость теоремы в этом случае.

Пусть теорема справедлива для полиномиального кольца $k[x_2, \ldots, x_n]$ от $n - 1$ переменных. Рассмотрим произвольный идеал $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$, и пусть $\mathbf{V}(I) = \varnothing$. Мы можем считать, что f_1 не константа — иначе нечего и доказывать. Пусть полная степень полинома f_1 равна $N \geq 1$. Мы произведем замену координат, чтобы преобразовать f_1 к удобному виду. А именно, рассмотрим линейную замену

$$\begin{aligned} x_1 &= \tilde{x}_1, \\ x_2 &= \tilde{x}_2 + a_2 \tilde{x}_1, \\ &\vdots \\ x_n &= \tilde{x}_n + a_n \tilde{x}_1, \end{aligned} \tag{1}$$

где a_i — это константы из k, которые мы определим позже. В новых координатах f_1 имеет вид

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2 \tilde{x}_1, \ldots, \tilde{x}_n + a_n \tilde{x}_1) \\ &= c(a_2, \ldots, a_n) \tilde{x}_1^N + \text{члены, где } \tilde{x}_1 \text{ имеет степень } < N. \end{aligned}$$

Мы оставляем читателю как упражнение доказательство того факта, что $c(a_2, \ldots, a_n)$ — ненулевой полином от переменных $a_2, \ldots, a_n$. В упражнениях мы докажем, что алгебраически замкнутое поле бесконечно, т. е. мы можем найти такие $a_2, \ldots, a_n$, что $c(a_2, \ldots, a_n) \neq 0$ (см. предложение 5 из § 1 гл. 1).

Выбрав $a_2, \ldots, a_n$, мы преобразуем теперь с помощью замены (1) каждый полином $f \in k[x_1, \ldots, x_n]$ в полином $\tilde{f} \in k[\tilde{x}_1, \ldots, \tilde{x}_n]$. В упражнениях мы докажем, что множество $\tilde{I} = \{\tilde{f} : f \in I\}$ является

идеалом в $k[\tilde{x}_1, \ldots, \tilde{x}_n]$. Отметим, что $\mathbf{V}(\widetilde{I}) = \varnothing$, так как если пр образованные уравнения имеют решение, то и исходные уравнен тоже. Более того, если мы докажем, что $1 \in \widetilde{I}$, то $1 \in I$, потому ч константы не меняются при замене переменных.

Таким образом, нужно доказать, что $1 \in \widetilde{I}$. Мы знаем, что имеет вид

$$\tilde{f}_1(\tilde{x}_1, \ldots, \tilde{x}_n) = \\ = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{члены, где } \tilde{x}_1 \text{ имеет степень } < N,$$

причем $c(a_2, \ldots, a_n) \neq 0$. Теперь мы можем применить следств геометрической теоремы о продолжении (следствие 4 из § 2 гл. чтобы связать многообразие $\mathbf{V}(\widetilde{I})$ и его проекцию на подпростра ство с координатами $\tilde{x}_2, \ldots, \tilde{x}_n$. Как указывалось в гл. 3, теорема продолжении и ее следствие справедливы над любым алгебраиче ки замкнутым полем. Пусть

$$\pi_1 : k^n \longrightarrow k^{n-1}$$

— проекция на последние $n-1$ координат. Положим, как обы но, $\widetilde{I}_1 = \widetilde{I} \cap k[\tilde{x}_2, \ldots, \tilde{x}_n]$. Тогда указанное следствие утвержда что все частичные решения в k^{n-1} продолжаются до полных, т. $\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I}))$. Значит, $\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I})) = \pi_1(\varnothing) = \varnothing$. То да по предположению индукции $\widetilde{I}_1 = k[x_2, \ldots, x_n]$. Следовательн $1 \in \widetilde{I}_1 \subset \widetilde{I}$. Доказательство закончено.

В случае $k = \mathbb{C}$ слабую теорему о нулях можно назвать «осно ной теоремой алгебры для полиномов от нескольких переменных каждая система полиномов, которая порождает идеал, меньши чем $\mathbb{C}[x_1, \ldots, x_n]$, имеет общий нуль в $\mathbb{C}^n$.

Слабая теорема о нулях позволяет решить *задачу совмест сти* из § 2 гл. 1. Напомним, что эта задача состоит в том, что определить, имеет ли система полиномиальных уравнений

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

решение в $\mathbb{C}^n$. Система не имеет решения в том и только том сл чае, когда $\mathbf{V}(f_1, \ldots, f_s) = \varnothing$. По слабой теореме о нулях последн выполняется в том и только том случае, когда $1 \in \langle f_1, \ldots, f_s \rangle$. Таки образом, для решения задачи совместности мы должны уметь опр делять, принадлежит ли единица данному идеалу. Это несложи

если заметить, что для любого мономиального упорядочения $\{1\}$ — *это единственный редуцированный базис Грёбнера идеала* $\langle 1 \rangle$.

Докажем это. Пусть $\{g_1, \ldots, g_t\}$ — базис Грёбнера идеала $I = \langle 1 \rangle$. Таким образом, $1 \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Согласно лемме 2 из § 4 гл. 2, 1 делится на какой-то $\mathrm{LT}(g_i)$, например на $\mathrm{LT}(g_1)$. Значит, $\mathrm{LT}(g_1)$ — константа. Но тогда $\mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)$ делятся на $\mathrm{LT}(g_1)$ и по лемме 3 из § 7 гл. 2 $g_2, \ldots, g_t$ могут быть удалены из базиса. Наконец, так как $\mathrm{LT}(g_1)$ — константа, то g_1 — константа, потому что любой непостоянный моном > 1 (следствие 6 из § 4 гл. 2). Умножив на подходящую константу, мы можем сделать так, чтобы $g_1 = 1$; таким образом, редуцированный базис Грёбнера идеала $\langle 1 \rangle$ состоит из одного элемента, т. е. это $\{1\}$.

Подведем итоги. Мы построили следующий *алгоритм проверки совместности*: пусть нам даны полиномы $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$. Мы находим редуцированный базис Грёбнера идеала, порожденного этими полиномами, по отношению к любому упорядочению. Если этот базис есть $\{1\}$, то система $f_1 = \ldots = f_s = 0$ не имеет решения; в противном случае эта система имеет решение в $\mathbb{C}^n$. Этот алгоритм работает над любым алгебраически замкнутым полем.

Если поле k не является алгебраически замкнутым, то алгоритм работает в одну сторону: если $\{1\}$ — редуцированный базис Грёбнера идеала $\langle f_1, \ldots, f_s \rangle$, то система $f_1 = \ldots = f_s = 0$ не имеет решений. Примеры, рассмотренные в начале параграфа, показывают, что обратное не имеет места.

Слабая теорема о нулях позволяет надеяться, что если поле k алгебраически замкнуто, то существует взаимно однозначное соответствие между аффинными многообразиями и идеалами. К сожалению, пример $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$) работает над *любым* полем. Аналогично, идеалы $\langle x^2, y \rangle$ и $\langle x, y \rangle$ (и вообще $\langle x^m, y^n \rangle$ при $m \geq 1, n \geq 1$) различны, но определяют одно и то же многообразие: точку $\{(0,0)\} \subset k^2$. Эти примеры демонстрируют основную причину, почему различные идеалы определяют одно и то же многообразие: степень полинома равна нулю на том же множестве, на котором равен нулю исходный полином. Теорема Гильберта о нулях утверждает, что над алгебраически замкнутым полем это *единственная* причина того, что разные идеалы определяют одно многообразие: если полином f равен нулю во всех точках многообразия $\mathbf{V}(I)$, то некоторая его степень принадлежит I.

Теорема 2 (теорема Гильберта о нулях). *Пусть k — алгебраически замкнутое поле. Если $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ таковы, что $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, то существует натуральное число $m \geq 1$,*

такое, что

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

(*и обратно*).

Доказательство. Пусть полином f обращается в нуль на мно образии $\mathbf{V}(f_1, \ldots, f_s)$. Мы должны доказать, что существует нату ральное $m \geq 1$ и полиномы $A_1, \ldots, A_s$, такие, что

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Самое простое доказательство использует следующий неожида ный прием[1]). Рассмотрим идеал

$$\widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y],$$

где y — новая переменная. Мы утверждаем, что

$$\mathbf{V}(\widetilde{I}) = \varnothing.$$

Докажем это. Пусть $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$; тогда или

- $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$, или
- $(a_1, \ldots, a_n) \notin \mathbf{V}(f_1, \ldots, f_s)$.

В первом случае $f(a_1, \ldots, a_n) = 0$, так как f обращается в нул на $\mathbf{V}(f_1, \ldots, f_s)$. Значит, полином $1 - yf$ равен 1 в точке $(a_1, \ldots$ $a_n, a_{n+1})$, т. е. $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\widetilde{I})$. Во втором случае для нек торого $i, 1 \leq i \leq s$, имеем $f_i(a_1, \ldots, a_n) \neq 0$. Мы будем рассматри вать f_i как функцию от $n+1$ переменных, которая не зависит о a_{n+1}, т. е. $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. В частности, отсюда следует, чт $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\widetilde{I})$.

Так как точка $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$ была выбрана произволь но, то получаем, что $\mathbf{V}(\widetilde{I}) = \varnothing$.

Теперь применение слабой теоремы о нулях показывает, что $1 \in \widetilde{I}$. Значит,

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf) \qquad (2)$$

для некоторых полиномов $p_i, q \in k[x_1, \ldots, x_n, y]$. Положим в равен стве (2) $y = 1/f(x_1, \ldots, x_n)$. Тогда

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i. \qquad (3)$$

[1])Принадлежащий Рабиновичу (см. Rabinovisch S. Zum Hilbertschen Nullstellensatz, Math. Ann., **102**, 1929, 520). — *Прим. ред.*

Умножим теперь (3) на подходящую степень полинома f^m так, что бы освободиться от знаменателей в правой части. Это даст нам равенство

$$f^m = \sum_{i=1}^{s} A_i f_i$$

для некоторых полиномов $A_i \in k[x_1, \ldots, x_n]$, что и требовалось до казать. □

Упражнения к § 1

1. Напомним, что многообразие $\mathbf{V}(y - x^2, z - x^3)$ — это скрученная ку бика в $\mathbb{R}^3$.
   (a) Докажите, что $\mathbf{V}((y-x^2)^2+(z-x^3)^2)$ — также скрученная кубика.
   (b) Докажите, что любое многообразие $\mathbf{V}(I) \subset \mathbb{R}^n, I \subset \mathbb{R}[x_1, \ldots, x_n]$, может быть задано одним уравнением (и, следовательно, глав ным идеалом).
2. Пусть $J = \langle x^2 + y^2 - 1, y - 1 \rangle$. Найдите $f \in \mathbf{I}(\mathbf{V}(J))$, такой, что $f \notin J$.
3. При замене переменных (1) полином $f(x_1, \ldots, x_n)$ полной степени N преобразуется в полином вида

   $$\tilde{f} = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{члены, содержащие } \tilde{x}_1 \text{ в степени } < N.$$

   Мы хотим доказать, что $c(a_2, \ldots, a_n)$ — ненулевой полином от пере менных a_i.
   (a) Пусть $f = h_N + h_{N-1} + \ldots + h_0$, где $h_i, 0 \leq i \leq N$, однородны степени i (т. е. каждый моном в h_i имеет полную степень i). Докажите, что $c(a_2, \ldots, a_n) = h_N(1, a_2, \ldots, a_n)$.
   (b) Пусть $h(x_1, \ldots, x_n)$ — однородный полином. Докажите, что h равен нулю в $k[x_1, \ldots, x_n]$ в том и только том случае, когда полином $h(1, x_2, \ldots, x_n)$ равен нулю в $k[x_2, \ldots, x_n]$.
   (c) Используя пп. (a) и (b), докажите, что $c(a_2, \ldots, a_n)$ не является нулевым полиномом от переменных $a_2, \ldots, a_n$.
4. Докажите, что алгебраически замкнутое поле k бесконечно. Указа ние: если $a_1, \ldots, a_n \in k$, можете ли вы построить полином $f \in k[x]$, такой, что $f(a_i) = 1$ для всех i?
5. Докажите, что множество $\widetilde{I}$, определенное в доказательстве слабой теоремы о нулях, является идеалом в $k[\tilde{x}_1, \ldots, \tilde{x}_n]$.
6. При выводе теоремы Гильберта о нулях из слабой теоремы о нулях мы использовали подстановку $y = 1/f(x_1, \ldots, x_n)$. Докажите кор ректность этой процедуры. Указание: в каком множестве содержится $1/f$?
7. В этом упражнении мы докажем следующий факт: если поле k не является алгебраически замкнутым, то любое многообразие $V \subset k^n$ может быть задано одним уравнением.

(a) Пусть $f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ — полином степени n от переменной x. Определим по f его гомогенизацию[1] — однородный полином f^h, построенный с помощью дополнительной переменной y: $f^h = a_0x^n + a_1x^{n-1}y + \ldots + a_{n-1}xy^{n-1} + a_ny^n$. Докажите, что f имеет корень в k в том и только том случае, когда найдется точка $(a,b) \in k^2, (a,b) \neq (0,0)$, такая, что $f^h(a,b) = 0$. Указание: докажите, что $f^h(a,b) = b^n f^h(a/b, 1)$, если $b \neq 0$.

(b) Пусть поле k не является алгебраически замкнутым. Докажите, что существует полином $f \in k[x,y]$, такой, что многообразие $\mathbf{V}(f)$ состоит только из одной точки $(0,0) \in k^2$. Указание: найдите полином в $k[x]$, не имеющий корней в k, и рассмотрите его гомогенизацию.

(c) Пусть поле k не является алгебраически замкнутым. Докажите, что для каждого натурального $s > 0$, существует $f \in k[x_1, \ldots, x_s]$, такой, что уравнение $f = 0$ имеет ровно одно решение $(0, \ldots, 0) \in k^s$. Указание: используйте результат п. (b) и проведите индукцию по s. См. также упр. 1.

(d) Пусть $W = \mathbf{V}(g_1, \ldots, g_s)$ — некоторое многообразие в k^n и поле k не является алгебраически замкнутым. Докажите, что W может быть задано одним уравнением. Указание: рассмотрите полином $f(g_1, \ldots, g_s)$, где f — полином, найденный в п. (c).

8. Пусть k — произвольное поле. Рассмотрим множество S всех полиномов из $k[x_1, \ldots, x_n]$, не равных нулю ни в одной точке из k^n. Пусть $I \subset k[x_1, \ldots, x_n]$ — идеал, такой, что $I \cap S = \varnothing$. Докажите, что $\mathbf{V}(I) \neq \varnothing$. Указание: если k не является алгебраически замкнутым, то используйте результат предыдущего упражнения.

9. (Обобщение упр. 5.) Пусть A есть $n \times n$-матрица с элементами из k. Пусть x и $\tilde{x}$ — векторы-столбцы, такие, что $x = A\tilde{x}$. Определим отображение

$$\alpha_A : k[x_1, \ldots, x_n] \to k[\tilde{x}_1, \ldots, \tilde{x}_n]$$

следующим образом: полином $f \in k[x_1, \ldots, x_n]$ отображается в полином $\tilde{f} \in k[\tilde{x}_1, \ldots, \tilde{x}_n]$, где $\tilde{f}(\tilde{x}) = f(A\tilde{x})$.

(a) Докажите, что отображение α_A k-линейно, т. е. $\alpha_A(rf + sg) = r\alpha_A f + s\alpha_A g$ для всех $r, s \in k$ и всех $f, g \in k[x_1, \ldots, x_n]$.

(b) Докажите, что $\alpha_A(f \cdot g) = \alpha_A(f) \cdot \alpha_A(g)$ для всех $f, g \in k[x_1, \ldots, x_n]$. ($k$-линейное отображение, обладающее этим свойством, а также переводящее постоянный полином 1 в постоянный полином 1, называется *кольцевым гомоморфизмом*. Так как $\alpha_A(1) = 1$, то α_A — кольцевой гомоморфизм.)

(c) Какими свойствами должна обладать матрица A, чтобы отображение α_A было взаимно однозначным?

[1] От английского «homogeneous» — однородный. — *Прим. ред.*

(d) Является ли образ $\{\alpha_A(f) : f \in I\}$ идеала $I \subset k[x_1, \ldots, x_n]$ идеалом в $k[\tilde{x}_1, \ldots, \tilde{x}_n]$? Докажите этот факт или приведите контрпример.

(e) Является ли прообраз $\{f \in k[x_1, \ldots, x_n] : \alpha_A(f) \in \tilde{I}\}$ идеала $\tilde{I} \subset k[\tilde{x}_1, \ldots, \tilde{x}_n]$ идеалом в $k[x_1, \ldots, x_n]$? Докажите или приведите контрпример.

(f) Изменятся ли заключения упражнений (a)–(e), если мы позволим элементам матрицы A быть полиномами из $k[x_1, \ldots, x_n]$?

10. В упр. 1 мы рассматривали два идеала из $\mathbb{R}[x,y]$, которые определяют одно и то же непустое многообразие. Докажите, что один из этих идеалов содержится в другом. Можете ли вы найти два идеала в $\mathbb{R}[x,y]$, из которых ни один не содержится в другом, но многообразия, определяемые ими, непусты и совпадают? Можете ли вы выполнить ту же задачу в $\mathbb{R}[x]$?

§ 2. Радикальные идеалы и соответствие идеал—многообразие

Чтобы дальше изучать соответствие между идеалами и многообразиями, мы переформулируем теорему Гильберта о нулях в терминах идеалов. Как охарактеризовать идеал, который является идеалом некоторого многообразия? Другими словами, как описать идеалы, состоящие из всех полиномов обращающихся в нуль на некотором многообразии V? Ключевым утверждением является следующая лемма.

Лемма 1. *Пусть V — многообразие. Если $f^m \in \mathbf{I}(V)$, то $f \in \mathbf{I}(V)$.*

Доказательство. Пусть $x \in V$. Если $f^m \in \mathbf{I}(V)$, то $(f(x))^m = 0$. Следовательно, $f(x) = 0$. Так как точка $x \in V$ была выбрана произвольно, то $f \in \mathbf{I}(V)$.

Таким образом идеал *всех* полиномов, равных нулю на некотором многообразии V, обладает следующим свойством: если степень полинома принадлежит идеалу, то и сам полином должен ему принадлежать. Дадим определение.

Определение 2. Идеал I называется *радикальным*, если из включения $f^m \in I$ для некоторого $m \geq 1$ следует, что $f \in I$.

Переформулируем лемму 1.

Следствие 3. *$\mathbf{I}(V)$ является радикальным идеалом.*

С другой стороны, теорема Гильберта о нулях утверждает, что идеал I не является идеалом всех полиномов, равных нулю на $\mathbf{V}(I)$,

только в том случае, когда он содержит некоторую степень f^m полинома f, причем $f \notin I$, другими словами, когда он не радикален. Это замечание наводит на мысль, что существует взаимно однозначное соответствие между аффинными многообразиями и радикальными идеалами. Чтобы прояснить ситуацию и четко сформулировать результат, мы введем операцию взятия радикала произвольного идеала.

Определение 4. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. *Радикалом* $\sqrt{I}$ идеала I называется множество

$$\{f : f^m \in I \quad \text{для некоторого целого} \quad m \geq 1\}.$$

Отметим, что $I \subset \sqrt{I}$, поскольку если $f \in I$, то $f^1 \in I$, а следовательно, $f \in \sqrt{I}$. Очевидно, что идеал I радикален в том и только том случае, когда $I = \sqrt{I}$. Менее очевиден тот факт, что радикал идеала — тоже идеал. Чтобы убедиться в нетривиальности этого утверждения, рассмотрим, например, $J = \langle x^2, y^3 \rangle \subset k[x, y]$. Хотя ни x, ни y не принадлежат J, они принадлежат $\sqrt{J}$. Кроме того, $(x \cdot y)^2 = x^2 y^2 \in J$, так как $x^2 \in J$, т. е. $x \cdot y \in \sqrt{J}$. Сложнее показать, что $x + y \in \sqrt{J}$. Для этого заметим, что

$$(x + y)^4 = x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4 \in J,$$

поскольку полиномы $x^4, 4x^3 y, 6x^2 y^2$ делятся на x^2, а полиномы $4xy^3, y^4$ делятся на y^3. Таким образом, $x + y \in \sqrt{J}$. При этом $xy \notin J$ и $x + y \notin J$.

Лемма 5. *Если I является идеалом в $k[x_1, \ldots, x_n]$, то $\sqrt{I} \supset I$ — также идеал. Более того, $\sqrt{I}$ — радикальный идеал.*

Доказательство. Мы уже доказали, что $I \subset \sqrt{I}$. Докажем теперь, что $\sqrt{I}$ — идеал. Пусть $f, g \in \sqrt{I}$; тогда существуют натуральные числа m и l, такие, что $f^m, g^l \in I$. Рассмотрим биномиальное разложение $(f + g)^{m+l-1}$. Каждый член этого разложения содержит произведение $f^i g^j$, $i + j = m + l - 1$. Так как или $i \geq m$, или $j \geq l$, то или f^i, или g^j принадлежит I, а следовательно, $f^i g^j \in I$; значит, каждый член этого разложения принадлежит I и потому $(f + g)^{m+l-1} \in I$ и $f + g \in \sqrt{I}$. Пусть теперь $f \in \sqrt{I}$ и $h \in k[x_1, \ldots, x_n]$. Тогда $f^m \in I$ для некоторого целого $m \geq 1$. Так как I — идеал, то $(h \cdot f)^m = h^m f^m \in I$. Следовательно, $hf \in \sqrt{I}$. Мы доказали, что $\sqrt{I}$ — идеал. В упр. 4 будет доказано, что $\sqrt{I}$ — радикальный идеал. □

Теперь мы можем доказать теорему о нулях в терминах идеалов.

Теорема 6 (сильная теорема о нулях). *Пусть k — алгебраически замкнутое поле и I — идеал в $k[x_1, \ldots, x_n]$. Тогда*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Доказательство. Очевидно, что $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$, потому что $f \in \sqrt{I}$ означает, что $f^m \in I$ для некоторого m. Значит, f^m обращается в нуль на $\mathbf{V}(I)$, а следовательно, f обращается в нуль на $\mathbf{V}(I)$. Таким образом, $f \in \mathbf{I}(\mathbf{V}(I))$.

С другой стороны, предположим, что $f \in \mathbf{I}(\mathbf{V}(I))$, т. е. f обращается в нуль на $\mathbf{V}(I)$. По теореме Гильберта о нулях существует целое $m \geq 1$, такое, что $f^m \in I$. Но это означает, что $f \in \sqrt{I}$. Поскольку полином f был выбран произвольно, $\mathbf{I}(\mathbf{V}(I)) \subset \sqrt{I}$. Теорема доказана. □

Именно теорему 6 обычно называют теоремой о нулях, и мы также будем следовать этой традиции. Самым важным следствием теоремы о нулях является возможность построить алгебро-геометрический «словарь». Основные правила пользования им формулируются в следующей теореме.

Теорема 7 (соответствие идеал—многообразие). *Пусть k — произвольное поле.*

(i) *Отображения*

$$\textit{аффинные многообразия} \xrightarrow{\mathbf{I}} \textit{идеалы}$$

и

$$\textit{идеалы} \xrightarrow{\mathbf{V}} \textit{аффинные многообразия}$$

обращают включение, т. е. если $I_1 \subset I_2$ — идеалы, то $\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$, и аналогично, если $V_1 \subset V_2$ — многообразия, то $\mathbf{I}(V_1) \supset \mathbf{I}(V_2)$. Кроме того, равенство

$$\mathbf{V}(\mathbf{I}(\mathbf{V})) = V$$

справедливо для любого многообразия V, т. е. отображение $\mathbf{I}$ взаимно однозначно.

(ii) *Если k алгебраически замкнуто и мы ограничиваемся радикальными идеалами, то отображения*

$$\textit{аффинные многообразия} \xrightarrow{\mathbf{I}} \textit{радикальные идеалы}$$

и

$$\textit{радикальные идеалы} \xrightarrow{\mathbf{V}} \textit{аффинные многообразия}$$

являются взаимно обратными биекциями, которые обращают включение.

Доказательство. (i) Тот факт, что $\mathbf{I}$ и $\mathbf{V}$ обращают включение, будет доказан в упражнениях. Докажем, что $\mathbf{V}(\mathbf{I}(V)) = V$, где $V = \mathbf{V}(f_1, \ldots, f_s)$ — некоторое подмногообразие в k^n. Так как любой полином $f \in \mathbf{I}(V)$ обращается в нуль на V, то $V \subset \mathbf{V}(\mathbf{I}(V))$ по определению многообразия $\mathbf{V}$. С другой стороны, заметим, что $f_1, \ldots, f_s \in \mathbf{I}(V)$ по определению идеала $\mathbf{I}(V)$; значит, $\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(V)$. Так как $\mathbf{V}$ обращает включение, то $\mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(\langle f_1, \ldots, f_s \rangle = V$. Равенство $\mathbf{V}(\mathbf{I}(V)) = V$ доказано. Кроме того, доказано, что $\mathbf{I}$ — взаимно однозначное отображение, так как оно имеет левое обратное.

(ii) По следствию 3 идеал $\mathbf{I}(V)$ радикален; следовательно, мы можем рассматривать $\mathbf{I}$ как отображение множества многообразий в множество радикальных идеалов. Мы знаем, что равенство $\mathbf{V}(\mathbf{I}(V)) = V$ справедливо над любым полем. Нам осталось доказать, что $\mathbf{I}(\mathbf{V}(I)) = I$, если I — радикальный идеал. По теореме о нулях $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$, но если I радикален, то $I = \sqrt{I}$ (см. упр. 4). Следовательно, отображения $\mathbf{V}$ и $\mathbf{I}$ взаимно обратны и определяют биекции между множеством радикальных идеалов и множеством аффинных многообразий. Теорема доказана. □

Эта теорема позволяет переформулировать любое утверждение о многообразиях как утверждение об идеалах (и обратно) (если основное поле алгебраически замкнуто). Возможность перехода от алгебры к геометрии весьма полезна.

В свете теоремы о нулях и важности того, что в соответствие ставятся радикальные идеалы, возникает естественный вопрос, как найти множество образующих радикала $\sqrt{I}$, если мы знаем множество образующих самого идеала I. На самом деле возникают три вопроса об идеале $I = \langle f_1, \ldots, f_s \rangle$:

- (Образующие радикала) Существует ли алгоритм, вычисляющий набор полиномов $g_1, \ldots, g_m$, такой, что $\sqrt{I} = \langle g_1, \ldots, g_m \rangle$?
- (Радикальный идеал) Существует ли алгоритм, позволяющий выяснить, радикален ли данный идеал I?
- (Принадлежность радикальному идеалу) Для заданной функции $f \in k[x_1, \ldots, x_n]$ существует ли алгоритм, позволяющий выяснить, верно ли, что $f \in \sqrt{I}$?

Существование подобных алгоритмов обосновано в работе HERMANN (1926) (современное рассмотрение этих вопросов см. в работах MINES, RICHMAN, RUITENBURG (1988) и SEIDENBERG

(1974, 1984)). К сожалению, алгоритмы, решающие первые два вопроса, малоэффективны и трудно реализуемы на компьютере. Однако недавняя работа GIANNI, TRAGER, ZACHARIAS (1988) привела к созданию алгоритма нахождения радикала. Этот алгоритм реализован в системах AXIOM и REDUCE и детально описан в работе BECKER, WEISPFENNING (1993), Theorem 8.99. Другой алгоритм нахождения радикала предложен в работе EISENBUD, HUNEKE, VASCONCELOS (1992) и реализован в системе Macaulay.

Сейчас мы займемся более простой третьей задачей — *задачей о принадлежности радикальному идеалу.* Для проверки принадлежности $f \in \sqrt{I}$ мы могли бы использовать алгоритм принадлежности идеалу, чтобы выяснить, принадлежит ли f^m идеалу I для произвольного натурального m. Это малоэффективный способ, потому что мы можем дойти до очень больших чисел, не приобретя уверенности, что $f \notin \sqrt{I}$. К счастью, доказательство теоремы Гильберта о нулях позволяет сконструировать алгоритм, решающий задачу о принадлежности идеалу $\sqrt{\langle f_1, \ldots, f_s \rangle}$.

Предложение 8 (принадлежность радикальному идеалу). *Пусть k — произвольное поле и $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Тогда $f \in \sqrt{I}$ в том и только том случае, когда постоянный полином 1 принадлежит идеалу $\widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$ (и, значит, $\widetilde{I} = k[x_1, \ldots, x_n, y]$).*

Доказательство. Пусть $1 \in \widetilde{I}$; тогда из равенств (2)–(4) из § 1 следует, что $f^m \in I$ для некоторого m, т. е. $f \in \sqrt{I}$. С другой стороны, пусть $f \in \sqrt{I}$. Тогда $f^m \in I \subset \widetilde{I}$ для некоторого m. Кроме того, $1 - yf \in \widetilde{I}$, и, следовательно

$$1 = y^m f^m + (1 - y^m f^m) =$$
$$= y^m \cdot f^m + (1 - yf) \cdot (1 + yf + \ldots + y^{m-1} f^{m-1}) \in \widetilde{I}.$$

Предложение доказано. □

Предложение 8 и замечания выше о том, как определить принадлежность 1 идеалу (см. обсуждение вопроса о совместности в § 1), дают возможность построить *алгоритм принадлежности радикальному идеалу.* А именно, чтобы определить, принадлежит ли f идеалу $\sqrt{\langle f_1, \ldots, f_s \rangle} \subset k[x_1, \ldots, x_n]$, мы находим редуцированный базис Грёбнера идеала $\langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$ по отношению к любому упорядочению. Если этот базис есть $\{1\}$, то $f \in \sqrt{I}$. В противном случае $f \notin \sqrt{I}$.

В качестве примера рассмотрим идеал $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle \subset k[x, y]$. Мы хотим узнать, принадлежит ли полином $f = y - x^2 + 1$

идеалу $\sqrt{I}$. Используя lex-упорядочение на $k[x,y,z]$, мы получае
что редуцированный базис Грёбнера идеала

$$\widetilde{I} = \langle xy^2+2y^2, x^4-2x^2+1, 1-z(y-x^2+1)\rangle \subset k[x,y,z]$$

есть $\{1\}$. Значит, $y-x^2+1 \in \sqrt{I}$.

В самом деле, используя алгоритм деления, мы можем убедить
ся, что

$$\overline{y-x^2+1}^{G} = y-x^2+1,$$
$$\overline{(y-x^2+1)^2}^{G} = -2x^2y+2y,$$
$$\overline{(y-x^2+1)^3}^{G} = 0,$$

где $G=\{x^4-2x^2+1, y^2\}$ — базис Грёбнера идеала I относительн
lex-упорядочения, а $\bar{p}^G$ — остаток от деления p на G. Таким обра
зом, $(y-x^2+1)^3 \in I$, но меньшие степени полинома f идеалу
не принадлежат.

Какова же геометрия этого примера? Как множество $\mathbf{V}(I)$
$\{(\pm 1,0)\}$, но (нестрого говоря) каждый полином из I имеет нул
порядка не менее двух в каждой из двух его точек. Это становитс
очевидным, если разложить образующие идеала I:

$$xy^2+2y^2 = y^2(x+2) \quad \text{и} \quad x^4-2x^2+1 = (x^2-1)^2.$$

Хотя $f = y-x^2+1$ и равен нулю в $(\pm 1,0)$, но имеет нуль порядк
один в этих точках. Следовательно, нужно возвести f в степен
большую единицы, чтобы получить элемент из I.

Мы завершим этот параграф обсуждением случая, когда оп
сать радикал идеала довольно просто, а именно когда мы имее
дело с главным идеалом $I=\langle f\rangle$. Напомним, что полином f назы
вается *неприводимым*, если он не может быть разложен в произве
дение двух полиномов положительной степени. В § 5 гл. 3 мы до
казали, что любой полином является произведением неприводимы
полиномов. Собирая вместе неприводимые полиномы, отличающ
еся на постоянный множитель, мы можем записать f в виде

$$f = f_1^{a_1} f_2^{a_2} \dots f_r^{a_r},$$

где $f_i, 1 \le i \le r$, — *различные* неприводимые полиномы, т. е. f_i нельз
получить из f_j при $i \ne j$ умножением на ненулевую константу. Боле
того, это представление полинома f единственно с точностью до пе
рестановки сомножителей и до постоянных множителей. (Здесь м
просто повторили формулировку теоремы 5 из § 5 гл. 3.) Если м
знаем представление полинома f в виде произведения неприводи
мых полиномов, то легко дать явное описание радикала главног
идеала I.

Предложение 9. *Пусть $f \in k[x_1,\dots,x_n]$, и пусть $I=\langle f\rangle$ — главный идеал, порожденный полиномом f. Если $f = f_1^{a_1} f_2^{a_2}\dots f_r^{a_r}$ — представление f в виде произведения неприводимых полиномов, то*

$$\sqrt{I} = \sqrt{\langle f\rangle} = \langle f_1 f_2 \dots f_r\rangle.$$

Доказательство. Легко показать, что $f_1 f_2 \dots f_r \in \sqrt{I}$. Пусть $N > \max(a_1,\dots,a_r)$. Тогда

$$(f_1 f_2 \dots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \dots f_r^{N-a_r} f \in I.$$

Так как $(f_1 f_2 \dots f_r)^N \in I$, то $f_1 f_2 \dots f_r \in \sqrt{I}$, т. е. $\langle f_1 f_2 \dots f_r\rangle \subset \sqrt{I}$.

Пусть теперь $g \in \sqrt{I}$. Тогда существует натуральное число M, такое, что $g^M \in I$, т. е. $g^M = h\cdot f$ для некоторого полинома h. Пусть $g = g_1^{b_1} g_2^{b_2} \dots g_s^{b_s}$ — разложение полинома g в произведение различных неприводимых полиномов. Тогда $g^M = g_1^{b_1 M} g_2^{b_2 M} \dots g_s^{b_s M}$ — разложение полинома g^M в произведение различных неприводимых полиномов. Таким образом,

$$g_1^{b_1 M} g_2^{b_2 M} \dots g_s^{b_s M} = h \cdot f_1^{a_1} f_2^{a_2} \dots f_r^{a_r}.$$

Но разложение на неприводимые множители единственно; значит, каждый полином f_i равен (с точностью до постоянного множителя) некоторому полиному g_j. Поэтому g делится на $f_1 f_2 \dots f_r$; следовательно, $g \in \langle f_1 f_2 \dots f_r\rangle$. Предложение доказано. □

Предложение 9 приводит нас к следующему определению.

Определение 10. Пусть $f \in k[x_1,\dots,x_n]$. *Редукцией полинома f* называется такой полином f_{red}, что $\langle f_{\text{red}}\rangle = \sqrt{\langle f\rangle}$. Полином называется *редуцированным* (или *свободным от квадратов*), если $f = f_{\text{red}}$.

Другими словами, f_{red} получается из f «удалением» повторяющихся неприводимых множителей. Пусть, например, $f=(x+y^2)^3(x-y)$; тогда $f_{\text{red}} = (x+y^2)(x-y)$. Отметим, что f_{red} определен однозначно с точностью до постоянного множителя.

Однако алгоритм, реализующий утверждение предложения 9, неэффективен, так как предложение 9 требует разложения полинома f в произведение неприводимых множителей. Возникает вопрос, существует ли алгоритм, позволяющий вычислять f_{red}, не производя разложения полинома f. Оказывается, что такой алгоритм есть.

Прежде чем дать его описание, определим наибольший общий делитель двух полиномов.

Определение 11. Пусть $f, g \in k[x_1,\dots,x_n]$; тогда $h \in k[x_1,\dots,x_n]$ называется *наибольшим общим делителем полиномов f и g* и обозначается $h = \text{GCD}(f,g)$, если

(i) h делит и f и g;
(ii) если полином p делит и f, и g, то p делит h.

Легко показать, что $\mathrm{GCD}(f,g)$ существует и определен однозначно с точностью до постоянного множителя (упр. 9). К сожалению, алгоритм вычисления GCD для случая одной переменной (алгоритм Евклида) не работает в случае нескольких переменных. Рассмотрим, например, полиномы $xy, xz \in k[x,y,z]$. Очевидно, что $\mathrm{GCD}(xy,xz) = x$. Однако при любом упорядочении деление xy на xz дает 0 и xy в остатке, а деление xz на xy дает 0 и xz в остатке. В результате ни один полином «не уменьшается», и следующий шаг аналога алгоритма Евклида невозможен.

Тем не менее алгоритм, вычисляющий GCD двух полиномов от нескольких переменных, существует. Его рассмотрение будет отложено до следующего параграфа — сначала мы должны изучить пересечение идеалов. Предположим, однако, что такой алгоритм у нас есть. Тогда мы можем определить $\mathrm{GCD}(f_1,\dots,f_s)$, где $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ так же, как в случае одной переменной. Существует и алгоритм для вычисления $\mathrm{GCD}(f_1,f_2,\dots,f_s)$.

Теперь, используя понятие наибольшего общего делителя, мы можем дать формулу для вычисления радикала главного идеала.

Предложение 12. *Пусть поле k содержит поле рациональных чисел $\mathbb{Q}$, и пусть $I = \langle f\rangle$ — главный идеал в $k[x_1,\dots,x_n]$. Тогда $\sqrt{I} = \langle f_{\mathrm{red}}\rangle$, где*

$$f_{\mathrm{red}} = \frac{f}{\mathrm{GCD}\left(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \dots, \frac{\partial f}{\partial x_n}\right)}.$$

Доказательство. Запишем f в таком же виде, как в предложении 9. Тогда $\sqrt{I} = \langle f_1 f_2 \dots f_r\rangle$. Таким образом, нам достаточно доказать, что

$$\mathrm{GCD}\left(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1-1} f_2^{a_2-1} \dots f_r^{a_r-1}. \qquad (1)$$

Имеем

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \dots f_r^{a_r-1}\left(a_1 \frac{\partial f_1}{\partial x_j} f_2 \dots f_r + \dots + a_r f_1 \dots f_{r-1} \frac{\partial f_r}{\partial x_j}\right).$$

Это доказывает, что $f_1^{a_1-1} f_2^{a_2-1} \dots f_r^{a_r-1}$ делит GCD. Осталось доказать, что для каждого i найдется $\frac{\partial f}{\partial x_j}$, не делящийся на $f_i^{a_i}$.

Запишем $f = f_i^{a_i} h_i$, где h_i не делится на f_i. Так как f_i имеет положительную степень, то некоторая переменная x_j встречается

в f_i. Тогда

$$\frac{\partial f}{\partial x_j} = f_i^{a_i-1}\left(a_i \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j}\right).$$

Если $\frac{\partial f}{\partial x_j}$ делится на $f_i^{a_i}$, то $\frac{\partial f_i}{\partial x_j} h_i$ делится на f_i. Так как f_i неприводим и h_i не делится на f_i, то f_i делит $\frac{\partial f_i}{\partial x_j}$. В упр. 13 будет доказано, что $\frac{\partial f_i}{\partial x_j}$ — ненулевой полином, потому что $\mathbb{Q} \subset k$ и x_j встречается в f_i. Но полная степень полинома $\frac{\partial f_i}{\partial x_j}$ меньше, чем полная степень полинома f_i; поэтому f_i не может делить $\frac{\partial f_i}{\partial x_j}$, а значит, $f_i^{a_i}$ не может делить $\frac{\partial f}{\partial x_j}$, что и доказывает (1). Предложение доказано. □

Следует отметить, что для полей, не содержащих $\mathbb{Q}$, приведенная выше формула для f_{red} может быть ошибочной (см. упр. 13).

Упражнения к § 2

1. Докажите, что $\sqrt{\langle x^2, y^2\rangle} = \langle x, y\rangle$ для произвольного поля k и что, более общим образом, $\sqrt{\langle x^n, y^m\rangle} = \langle x, y\rangle$ для натуральных m, n.
2. Пусть f и g — различные непостоянные полиномы в $k[x,y]$, и пусть $I = \langle f^2, g^3\rangle$. Верно ли, что $\sqrt{I} = \langle f, g\rangle$? Объясните ваш ответ.
3. Докажите, что $\langle x^2+1\rangle \subset \mathbb{R}[x]$ — радикальный идеал, но что многообразие $\mathbf{V}(x^2+1)$ пусто.
4. Пусть I — идеал в $k[x_1,\dots,x_n]$, а k — произвольное поле.
   (a) Докажите, что $\sqrt{I}$ — радикальный идеал.
   (b) Докажите, что I радикален в том и только том случае, когда $I = \sqrt{I}$.
   (c) Докажите, что $\sqrt{\sqrt{I}} = \sqrt{I}$.
5. Докажите, что отображения $\mathbf{I}$ и $\mathbf{V}$ обращают включения.
6. Пусть I — идеал в $k[x_1,\dots,x_n]$.
   (a) Докажите, что в частном случае, когда $\sqrt{I} = \langle f_1, f_2\rangle$, где $f_i^{m_i} \in I$, $f^{m_1+m_2-1} \in I$ для всех $f \in \sqrt{I}$.
   (b) Теперь докажите, что для любого I найдется m_0, такое, что $f^{m_0} \in I$ для всех $f \in \sqrt{I}$. Указание: $\sqrt{I} = \langle f_1,\dots,f_s\rangle$.
7. Определите, принадлежат ли указанные полиномы указанным радикалам. Если да, то найдите наименьшую степень полинома, принадлежащую исходному идеалу.
   (a) Верно ли, что $x+y \in \sqrt{\langle x^3, y^3, xy(x+y)\rangle}$?
   (b) Верно ли, что $x^2+3xz \in \sqrt{\langle x+z, x^2y, x-z^2\rangle}$?
8. Пусть f_m и f_{m+1} — однородные полиномы, степеней m и $m+1$ соответственно без общих делителей (т. е. $\mathrm{GCD}(f_m, f_{m+1}) = 1$). Докажите, что полином $h = f_m + f_{m+1}$ неприводим.

9. Пусть $f, g \in k[x_1, \ldots, x_n]$. Используя теорему о единственности разложения на множители, докажите существование $\mathrm{GCD}(f, g)$. Докажите, что $\mathrm{GCD}(f, g)$ определен однозначно с точностью до умножения на ненулевую константу.
10. В этом упражнении мы охарактеризуем $\mathrm{GCD}(f, g)$ с точки зрения теории идеалов. Пусть $f, g, h \in k[x_1, \ldots, x_n]$; тогда $h = \mathrm{GCD}(f, g)$ в том и только том случае, когда h является образующей наименьшего главного идеала, содержащего $\langle f, g\rangle$ (т. е. $\langle h\rangle \subset J$, где J — главный идеал, такой, что $\langle f, g\rangle \subset J$).
11. Найдите базис идеала.
$$\sqrt{\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1\rangle}.$$
См. упр. 17 к § 5 гл. 1.
12. Пусть $f = x^5 + 3x^4y + 3x^3y^2 - 2x^4y^2 + x^2y^3 - 6x^3y^3 - 6x^2y^4 + x^3y^4 - 2xy^5 + 3x^2y^5 + 3xy^6 + y^7 \in \mathbb{Q}[x, y]$. Найдите $\sqrt{\langle f\rangle}$.
13. Поле k имеет *характеристику нуль*, если оно содержит поле $\mathbb{Q}$, и *положительную характеристику* в противном случае.
    (a) Пусть k есть поле $\mathbb{F}_2$ из упр. 1 к § 1 гл. 1, и пусть $f = x_1^2 + \ldots + x_n^2 \in \mathbb{F}_2[x_1, \ldots, x_n]$. Докажите, что $\frac{\partial f}{\partial x_i} = 0$ для всех i. Выведите отсюда, что формула из предложения 12 может не выполняться в случае поля $\mathbb{F}_2$.
    (b) Пусть k — поле характеристики нуль и $f \in k[x_1, \ldots, x_n]$ — ненулевой полином. Докажите, что $\frac{\partial f}{\partial x_j} \neq 0$, если переменная x_j встречается в f. Объясните, почему полная степень полинома $\frac{\partial f}{\partial x_j}$ меньше, чем полная степень полинома f.
14. Пусть $J = \langle xy, (x - y)x\rangle$. Найдите $\mathbf{V}(J)$ и докажите, что $\sqrt{J} = \langle x\rangle$.
15. Докажите, что $I = \langle xy, xz, yz\rangle$ — радикальный идеал. Указание: что из себя представляет остаток от деления полинома $f \in k[x, y, z]$ на xy, xz, yz? Как выглядит полином f^m?

§ 3. Суммы, произведения и пересечения идеалов

Идеалы являются алгебраическими объектами. Следовательно, на них можно определить естественные алгебраические операции. В этом параграфе мы рассмотрим три операции: сумму, пересечение и произведение. Это бинарные операции: каждой паре идеалов они ставят в соответствие новый идеал. В связи с каждой из этих операций нас будут интересовать два вопроса. Первый: как найти множество образующих идеала, являющегося результатом операции над некоторыми двумя идеалами, если их образующие нам известны? Второй: какова геометрическая интерпретация этой операции? Таким образом, первый вопрос отвечает вычислительному направлению в этой книге, а второй — общему направлению этой главы. Мы рассмотрим операции по очереди.

Суммы идеалов

Определение 1. Пусть I и J — идеалы кольца $k[x_1, \ldots, x_n]$. *Сумма* $I + J$ идеалов I и J — это множество
$$I + J = \{f + g : \quad f \in I \quad \text{и} \quad g \in J\}.$$

Предложение 2. *Если I и J — идеалы в $k[x_1, \ldots, x_n]$, то $I + J$ также идеал в $k[x_1, \ldots, x_n]$, причем $I + J$ — это наименьший идеал, содержащий I и J. Кроме того, если $I = \langle f_1, \ldots, f_r\rangle$ и $J = \langle g_1 \ldots, g_s\rangle$, то $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s\rangle$.*

Доказательство. Прежде всего, $0 = 0 + 0 \in I + J$. Далее, пусть $h_1, h_2 \in I + J$. Тогда $h_1 = p_1 + q_1$, $h_2 = p_2 + q_2$, где $p_1, p_2 \in I$ и $q_1, q_2 \in J$. Имеем $h_1 + h_2 = (p_1 + q_1) + (p_2 + q_2) = (p_1 + p_2) + (q_1 + q_2) \in I + J$, так как $p_1 + p_2 \in I$ и $q_1 + q_2 \in J$ по определению идеала. Пусть теперь $h \in I + J$, а $l \in k[x_1, \ldots, x_n]$ — произвольный полином. Тогда $h = f + g$, где $f \in I, g \in J$. Имеем $l \cdot h = l \cdot (f + g) = l \cdot f + l \cdot g \in I + J$, так как $l \cdot f \in I$ и $l \cdot g \in J$ по определению идеала. Таким образом, $I + J$ — идеал.

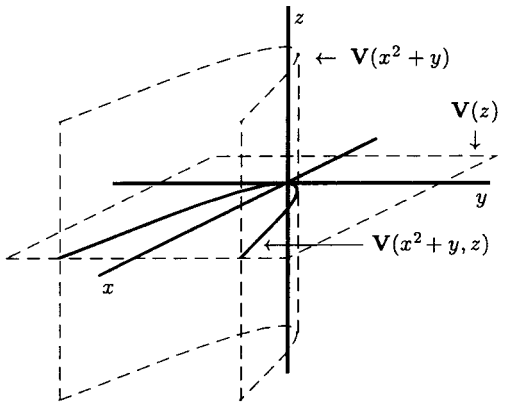
Если H — некоторый идеал, содержащий I и J, то H содержит все элементы $f \in I$ и все элементы $g \in J$. Так как H — идеал, то он содержит все суммы $f + g$, где $f \in I$ и $g \in J$. Значит, $I + J \subset H$. Таким образом, каждый идеал, содержащий I и J, обязан содержать и $I + J$, т. е. $I + J$ — наименьший из идеалов с этим свойством. Наконец, если $I = \langle f_1, \ldots, f_r\rangle$ и $J = \langle g_1, \ldots, g_s\rangle$, то идеал $\langle f_1, \ldots, f_r, g_1, \ldots, g_s\rangle$ содержит I и J. Поэтому $I + J \subset \langle f_1, \ldots, f_r, g_1, \ldots, g_s\rangle$. Обратное включение очевидно. Значит, $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s\rangle$. □

Следующее утверждение является прямым следствием предложения 2.

Следствие 3. *Пусть $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. Тогда*
$$\langle f_1, \ldots, f_r\rangle = \langle f_1\rangle + \ldots + \langle f_r\rangle.$$

Чтобы понять геометрический смысл суммы идеалов, рассмотрим в качестве примера идеалы $I = \langle x^2 + y\rangle$ и $J = \langle z\rangle$ в $\mathbb{R}[x, y, z]$. Многообразия $\mathbf{V}(I)$ и $\mathbf{V}(J)$ приведены на следующем рисунке. Идеал $I + J = \langle x^2 + y, z\rangle$ содержит полиномы $x^2 + y$ и z. Значит, многообразие $\mathbf{V}(I + J)$ состоит из тех точек, где оба полинома $x^2 + y$

и z обращаются в нуль, т. е. это пересечение многообразий $\mathbf{V}(I)$ и $\mathbf{V}(J)$.



Приведенные рассуждения нетрудно обобщить, чтобы показать, что сложение идеалов соответствует в геометрии пересечению многообразий.

Теорема 4. *Пусть I и J — идеалы в $k[x_1, \ldots, x_n]$. Тогда* $\mathbf{V}(I+J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.

Доказательство. Если $x \in \mathbf{V}(I+J)$, то $x \in \mathbf{V}(I)$, так как $I \subset I+J$. Аналогично, $x \in \mathbf{V}(J)$; значит, $x \in \mathbf{V}(I) \cap \mathbf{V}(J)$, т. е. $\mathbf{V}(I+J) \subset \mathbf{V}(I) \cap \mathbf{V}(J)$.

С другой стороны, пусть $x \in \mathbf{V}(I) \cap \mathbf{V}(J)$. Пусть h — произвольный полином из $I+J$. Тогда $h = f+g$, где $f \in I$ и $g \in J$. Далее, $f(x) = 0$, так как $x \in \mathbf{V}(I)$, и $g(x) = 0$, так как $x \in \mathbf{V}(J)$. Значит, $h(x) = f(x) + g(x) = 0 + 0 = 0$. Так как h — произвольный полином из $I+J$, то $x \in \mathbf{V}(I+J)$, т. е. $\mathbf{V}(I+J) \supset \mathbf{V}(I) \cap \mathbf{V}(J)$.

Аналог теоремы 4, сформулированный в терминах образующих, содержится в лемме 2 из § 2 гл. 1.

Произведение идеалов

В лемме 2 из § 2 гл. 1 мы обнаружили, что идеал, порожденный произведениями образующих двух других идеалов, соответствует объединению многообразий:

$$\mathbf{V}(f_1, \ldots, f_r) \cup \mathbf{V}(g_1, \ldots, g_s) = \mathbf{V}(f_i g_j : 1 \le i \le r, 1 \le j \le s).$$

Так, например, многообразие $\mathbf{V}(xz, yz)$, отвечающее идеалу, порожденному произведениями образующих идеалов $\langle x, y\rangle$ и $\langle z\rangle$ в $k[x, y, z]$, является объединением многообразия $\mathbf{V}(x, y)$ (ось z) и $\mathbf{V}(z)$ (плоскость xy). Это наблюдение приводит к следующему определению.

Определение 5. Пусть I и J — идеалы в $k[x_1, \ldots, x_n]$. Тогда их *произведение* $I \cdot J$ — это идеал, порожденный всеми полиномами вида $f \cdot g$, где $f \in I$ и $g \in J$.

Таким образом, произведение идеалов I и J — это множество

$$I \cdot J = \{f_1 g_1 + \ldots + f_m g_m : f_1, \ldots, f_m \in I, g_1, \ldots, g_m \in J, m \ge 1\}.$$

Докажем, что это множество является идеалом. В самом деле, $0 = 0 \cdot 0 \in I \cdot J$. Очевидно, что если $h_1, h_2 \in I \cdot J$, то и $h_1 + h_2 \in I \cdot J$. Наконец, если $h = f_1 g_1 + \ldots + f_m g_m \in I \cdot J$ и p — произвольный полином, то

$$ph = (pf_1)g_1 + \ldots + (pf_m)g_m \in I \cdot J,$$

так как $pf_i \in I$ для всех i, $1 \le i \le m$. Отметим, что множество произведений не является идеалом — оно не замкнуто относительно сложения. Следующее предложение показывает, что определение множества образующих идеала $I \cdot J$, когда известны образующие идеалов I и J, не вызывает трудностей.

Предложение 6. *Пусть $I = \langle f_1, \ldots, f_r\rangle$ и $J = \langle g_1, \ldots, g_s\rangle$. Тогда $I \cdot J$ порождается множеством всех произведений образующих идеалов I и J:*

$$I \cdot J = \langle f_i g_j : 1 \le i \le r, 1 \le j \le s\rangle.$$

Доказательство. Очевидно, что идеал, порожденный произведениями $f_i g_j$, содержится в $I \cdot J$. Докажем обратное включение. Любой полином из $I \cdot J$ является суммой полиномов вида fg, где $f \in I$ и $g \in J$. Но f и g могут быть выражены через образующие:

$$f = a_1 f_1 + \ldots + a_r f_r, \quad g = b_1 g_1 + \ldots + b_s g_s,$$

где a_i, b_j — некоторые полиномы. Тогда fg и любая сумма полиномов этого вида есть сумма $\sum c_{ij} f_i g_j$, где $c_{ij} \in k[x_1, \ldots, x_n]$. □

Следующее утверждение показывает, что произведение идеалов соответствует в геометрии операции взятия объединения многообразий.

Теорема 7. *Пусть I и J — идеалы в $k[x_1, \ldots, x_n]$. Тогда* $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

Доказательство. Пусть $x \in \mathbf{V}(I \cdot J)$. Тогда $f(x)g(x) = 0$ для всех $f \in I$ и всех $g \in J$. Если $f(x) = 0$ для всех $f \in I$, то $x \in \mathbf{V}(I)$. Если

$f(x) \neq 0$ для некоторого $f \in I$, то $g(x) = 0$ для всех $g \in J$. Значит, $x \in \mathbf{V}(J)$. В обоих случаях $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$.

Пусть теперь $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Тогда или $f(x) = 0$ для всех $f \in I$, или $g(x) = 0$ для всех $g \in J$. Таким образом, равенство $f(x)g(x) = 0$ выполняется для всех $f \in I$ и $g \in J$. Значит, $h(x) = 0$ для всех $h \in I \cdot J$, т. е. $x \in \mathbf{V}(I \cdot J)$. □

В дальнейшем мы часто будем обозначать произведение $I \cdot J$ просто через IJ.

Пересечение идеалов

В некотором смысле пересечение идеалов — это более простая операция, чем сложение или умножение идеалов.

Определение 8. *Пересечение* $I \cap J$ двух идеалов $I, J \in k[x_1, \ldots, x_n]$ — это множество полиномов, принадлежащих и I, и J.

Справедливо следующее утверждение.

Предложение 9. *Пусть I и J — идеалы в $k[x_1, \ldots, x_m]$. Тогда $I \cap J$ — тоже идеал.*

Доказательство. Прежде всего, $0 \in I \cap J$, так как $0 \in I$ и $0 \in J$. Далее, пусть $f, g \in I \cap J$. Тогда $f+g \in I$, так как $f, g \in I$. Аналогично, $f + g \in J$, откуда $f + g \in I \cap J$. Пусть теперь $f \in I \cap J$ и h — произвольный полином из $k[x_1, \ldots, x_n]$. Тогда $h \cdot f \in I$, так как $f \in I$ и I — идеал. Аналогично, $h \cdot f \in J$. Значит, $h \cdot f \in I \cap J$. □

Отметим, что $IJ \subset I \cap J$, потому что элементы из IJ — это суммы произведений вида fg, где $f \in I$ и $g \in J$. Но fg принадлежит I (так как $f \in I$) и принадлежит J (так как $g \in J$), т. е. $fg \in I \cap J$. Идеал IJ, однако, может строго содержаться в $I \cap J$. Пусть, например $I = J = \langle x, y \rangle$. Тогда $IJ = \langle x^2, xy, y^2 \rangle$ строго содержится в $I \cap J = I = \langle x, y \rangle$ ($x \in I \cap J$, но $x \notin IJ$).

Если мы знаем множество образующих идеала I и множество образующих идеала J, то как найти множество образующих пересечения $I \cap J$? Это существенно более тонкая задача, чем аналогичные задачи для суммы и произведения. Пусть, например, $I \subset k[x, y]$ — идеал, порожденный полиномом $f = (x+y)^4(x^2+y)^2(x-5y)$, а J — идеал, порожденный полиномом $g = (x+y)(x^2+y)^3(x+3y)$. Мы оставляем читателю в качестве нетрудного упражнения проверку того, что

$$I \cap J = \langle (x+y)^4(x^2+y)^3(x-5y)(x+3y) \rangle.$$

Это легко проделать лишь потому, что разложения полиномов f и g в произведение неприводимых нам известны. В общем случае мы можем не располагать подобными разложениями. Поэтому алгоритм, вычисляющий пересечения, должен быть достаточно мощным, чтобы преодолеть эту трудность.

Тем не менее существует удобный прием, позволяющий свести вычисление пересечения к вычислению пересечения идеала с подкольцом (т. е. к исключению переменных) — к задаче, уже решенной нами.

Прежде чем привести описание алгоритма, мы введем некоторые обозначения. Пусть I — идеал в $k[x_1, \ldots, x_n]$, а $f(t) \in k[t]$ — полином от одной переменной t. Тогда fI обозначает идеал в $k[x_1, \ldots, x_n, t]$, порожденный множеством полиномов $\{f \cdot h : h \in I\}$. Это определение отличается от обычного определения произведения, так как I и $f(t)$ лежат в разных кольцах и на самом деле идеал $I \subset k[x_1, \ldots, x_n]$ *не* является идеалом в $k[x_1, \ldots, x_n, t]$, так как он не замкнут относительно умножения на t. Когда мы хотим подчеркнуть, что f является полиномом только от t, мы пишем $f = f(t)$. Аналогично, подчеркивая, что полином $h \in k[x_1, \ldots, x_n]$ зависит только от переменных $x_1, \ldots, x_n$, мы пишем $h = h(x)$. В том же духе, рассматривая полином $g \in k[x_1, \ldots, x_n, t]$, зависящий как от $x_1, \ldots, x_n$, так и от t, мы будем писать $g = g(x, t)$. В этих обозначениях $fI = f(t)I = \langle f(t)h(x) \colon h(x) \in I \rangle$. Пусть, например, $f(t) = t^2 - t$, а $I = \langle x, y \rangle$. Тогда идеал $f(t)I \subset k[x, y, t]$ содержит полиномы $(t^2 - t)x$ и $(t^2 - t)y$. На самом деле несложно доказать, что $fI = \langle (t^2 - t)x, (t^2 - t)y \rangle$. Этот пример является частным случаем следующего утверждения.

Лемма 10.

(i) *Если I порожден как идеал кольца $k[x_1, \ldots, x_n]$ полиномами $p_1(x), \ldots, p_r(x)$, то $f(t)I$ порожден как идеал кольца $k[x_1, \ldots, x_n, t]$ полиномами $f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)$.*

(ii) *Если $g(x, t) \in f(t)I$ и a — произвольный элемент из поля k, то $g(x, a) \in I$.*

Доказательство. Отметим сначала, что любой полином $g(x, t) \in f(t)I$ может быть представлен как сумма полиномов вида $h(x, t) \cdot f(t) \cdot p(x)$, где $h \in k[x_1, \ldots, x_n, t]$, а $p \in I$. Но так как I порожден полиномами $p_1, \ldots, p_r$, то $p(x)$ может быть представлен как сумма полиномов вида $q_i(x)p_i(x)$, $1 \leq i \leq r$, т. е.

$$p(x) = \sum_{i=1}^{r} q_i(x)p_i(x).$$

Следовательно,

$$h(x,t)\cdot f(t)\cdot p(x)=\sum_{i=1}^{r}h(x,t)q_i(x)f(t)p_i(x).$$

Так как для любого i, $1\le i\le r$, $h(x,t)\cdot q_i(x)\in k[x_1,\dots,x_n,t]$, то полином $h(x,t)\cdot f(t)\cdot p(x)$ принадлежит идеалу, порожденному $f(t)\cdot p_1(x),\dots,f(t)\cdot p_r(x)$. Поэтому

$$g(x,t)\in\langle f(t)\cdot p_1(x),\dots,f(t)\cdot p_r(x)\rangle.$$

Пункт (i) доказан. Второе утверждение следует из первого при подстановке $a\in k$ вместо t. □

Теорема 11. *Пусть I,J — идеалы из $k[x_1,\dots,x_n]$. Тогда*

$$I\cap J=(tI+(1-t)J)\cap k[x_1,\dots,x_n].$$

Доказательство. Напомним, что $tI+(1-t)J$ — это идеал в $k[x_1,\dots,x_n,t]$. Как обычно, чтобы доказать совпадение двух множеств, докажем, что каждое из них содержится в другом.

Пусть $f\in I\cap J$. Тогда $f\in I$ и, значит, $t\cdot f\in tI$. Аналогично, $f\in J$ и, следовательно, $(1-t)\cdot f\in(1-t)J$. Тогда $f=t\cdot f+(1-t)\cdot f\in tI+(1-t)J$. Так как $I,J\subset k[x_1,\dots,x_n]$, то $f\in(tI+(1-t)J)\cap k[x_1,\dots,x_n]$. Значит, $I\cap J\subset(tI+(1-t)J)\cap k[x_1,\dots,x_n]$.

С другой стороны, пусть $f\in(tI+(1-t)J)\cap k[x_1,\dots,x_n]$. Тогда $f(x)=g(x,t)+h(x,t)$, где $g(x,t)\in tI$ и $h(x,t)\in(1-t)J$. Положим $t=0$. Так как каждый полином в tI делится на t, то $g(x,0)=0$. Поэтому $f(x)=h(x,0)$; следовательно, $f(x)\in J$ по лемме 10. Теперь положим $t=1$. Так как каждый полином в $(1-t)J$ делится на $1-t$, то $h(x,1)=0$. Следовательно, $f(x)=g(x,1)$ и $f(x)\in I$ по лемме 10. Отсюда вытекает, что $f\in I\cap J$ и $I\cap J\supset(tI+(1-t)J)\cap k[x_1,\dots,x_n]$. Доказательство закончено. □

Этот результат и теорема об исключении (теорема 2 из § 1 гл. 3) позволяют построить следующий *алгоритм для вычисления пересечения идеалов*: если $I=\langle f_1,\dots,f_r\rangle$ и $J=\langle g_1,\dots,g_s\rangle$ — идеалы из $k[x_1,\dots,x_n]$, то мы рассматриваем идеал

$$\langle tf_1,\dots,tf_r,(1-t)g_1,\dots,(1-t)g_s\rangle\subset k[x_1,\dots,x_n,t]$$

и находим его базис Грёбнера по отношению к lex-упорядочению, в котором t больше любого x_i. Тогда элементы этого базиса, не зависящие от t, образуют базис (на самом деле базис Грёбнера) идеала $I\cap J$. Вычисления можно сделать более эффективными, если использовать упорядочения, определенные в упр. 5 и 6 к § 1 гл. 3. Алгоритм, вычисляющий пересечение трех и более идеалов, описан в книге BECKER, WEISPFENNING (1993), Proposition 6.19.

Рассмотрим пример. Мы хотим вычислить пересечение идеалов $I=\langle x^2y\rangle$ и $J=\langle xy^2\rangle$ кольца $k[x,y]$. Рассмотрим идеал

$$tI+(1-t)J=\langle tx^2y,(1-t)xy^2\rangle=\langle tx^2y,txy^2-xy^2\rangle$$

в $k[t,x,y]$. Вычисляя S-полином от образующих, мы получаем $tx^2y^2-(tx^2y^2-x^2y^2)=x^2y^2$. Легко проверить, что $\{tx^2y,txy^2-xy^2,x^2y^2\}$ — базис Грёбнера идеала $tI+(1-t)J$ по отношению к lex-упорядочению с $t>x>y$. По теореме об исключении $\{x^2y^2\}$ есть базис Грёбнера идеала $(tI+(1-t)J)\cap k[x,y]$. Таким образом,

$$I\cap J=\langle x^2y^2\rangle.$$

В следующем примере мы предлагаем читателю убедиться в том, что алгоритм для вычисления пересечения идеалов дает другое доказательство того, что пересечение $I\cap J$ идеалов

$$I=\langle(x+y)^4(x^2+y)^2(x-5y)\rangle\quad\text{и}\quad J=\langle(x+y)(x^2+y)^3(x+3y)\rangle$$

в $k[x,y]$ равно

$$\langle(x+y)^4(x^2+y)^3(x-5y)(x+3y)\rangle.$$

Эти примеры достаточно просты — мы рассматривали пересечения только главных идеалов, хотя алгоритм может работать и в общем случае. Более трудные примеры будут рассмотрены в упражнениях.

Следующее определение обобщает сделанные нами наблюдения.

Определение 12. Полином $h\in k[x_1,\dots,x_n]$ называется *наименьшим общим кратным* полиномов $f,g\in k[x_1,\dots,x_n]$ (обозначение: $h=\mathrm{LCM}(f,g)$), если

(i) f делит h и g делит h;

(ii) h делит любой полином, который делится и на f, и на g.

Например,

$$\mathrm{LCM}(x^2y,xy^2)=x^2y^2$$

и

$$\mathrm{LCM}((x+y)^4(x^2+y)^2(x-5y),(x+y)(x^2+y)^3(x+3y))=(x+y)^4(x^2+y)^3(x-5y)(x+3y).$$

Обобщим эти примеры. Пусть $f,g\in k[x_1,\dots,x_n]$, и пусть $f=f_1^{a_1}\dots f_r^{a_r}$ и $g=g_1^{b_1}\dots g_s^{b_s}$ — разложения полиномов f и g в произведения различных неприводимых полиномов. Может случиться

так, что некоторые неприводимые сомножители полинома f являются также сомножителями полинома g. В этом случае упорядочим сомножители полиномов f и g так, чтобы f_i был равен g_i (с точностью до постоянного множителя) при $i \le l$ для некоторого l, $1 \le l \le \min(r,s)$, а при $i,j > l$ полиномы f_i и g_j не были равны даже с точностью до постоянного множителя. Тогда из единственности разложения следует, что

$$\mathrm{LCM}(f,g) = f_1^{\max(a_1,b_1)} \dots f_l^{\max(a_l,b_l)} \cdot f_{l+1}^{a_{l+1}} \dots f_r^{a_r} \cdot g_{l+1}^{b_{l+1}} \dots g_s^{b_s}. \quad (1)$$

Отметим, что если f и g не имеют общих делителей, то $\mathrm{LCM}(f,g) = f \cdot g$. Все это приводит к следующему утверждению.

Предложение 13.
(i) *Пересечение $I \cap J$ двух главных идеалов $I, J \subset k[x_1,\dots,x_n]$ является главным идеалом.*
(ii) *Если $I = \langle f \rangle$ и $J = \langle g \rangle$, то $I \cap J = \langle h \rangle$, где*

$$h = \mathrm{LCM}(f,g).$$

Доказательство. Доказательство этого утверждения будет рассмотрено в упражнениях. □

Этот результат и алгоритм для вычисления пересечения двух идеалов немедленно дают нам *алгоритм для вычисления наименьшего общего кратного* двух полиномов. А именно, пусть даны полиномы $f, g \in k[x_1,\dots,x_n]$. Мы находим пересечение $\langle f \rangle \cap \langle g \rangle$. По предложению 13 пересечение является главным идеалом и его образующий элемент и есть наименьшее общее кратное полиномов f и g.

Теперь мы можем решить задачу, не завершенную в § 2, — вычислить наибольший общий делитель двух полиномов f и g.

Предложение 14. *Пусть $f, g \in k[x_1,\dots,x_n]$. Тогда*

$$\mathrm{LCM}(f,g) \cdot \mathrm{GCD}(f,g) = fg.$$

Доказательство. Доказательство мы оставляем читателю в качестве упражнения. Нужно представить f и g в виде произведений неприводимых сомножителей и использовать равенство (1). □

Из предложения 14 следует, что

$$\mathrm{GCD}(f,g) = \frac{fg}{\mathrm{LCM}(f,g)}. \quad (2)$$

Это дает нам *алгоритм для вычисления наибольшего общего делителя* двух полиномов f и g. А именно, мы вычисляем $\mathrm{LCM}(f,g)$, используя алгоритм для вычисления наименьшего общего кратного, а

затем делим произведение fg на $\mathrm{LCM}(f,g)$, используя алгоритм деления. Следует отметить, что только что описанный GCD-алгоритм мало эффективен. На практике применяются более эффективные алгоритмы (см. DAVENPORT, SIRET, TOURNIER (1993)).

Теперь пришло время выяснить, какова геометрическая интерпретация операции пересечения идеалов.

Теорема 15. *Пусть I и J — идеалы в $k[x_1,\dots,x_n]$. Тогда $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

Доказательство. Пусть $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Тогда $x \in \mathbf{V}(I)$ или $x \in \mathbf{V}(J)$. Это означает, что или $f(x) = 0$ для всех $f \in I$, или $f(x) = 0$ для всех $f \in J$. Но тогда $f(x) = 0$ для всех $f \in I \cap J$. Значит, $x \in \mathbf{V}(I \cap J)$ и $\mathbf{V}(I) \cup \mathbf{V}(J) \subset \mathbf{V}(I \cap J)$.

С другой стороны, так как $IJ \subset I \cap J$, то $\mathbf{V}(I \cap J) \subset \mathbf{V}(IJ)$. Но $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ по теореме 7. Отсюда следует, что $\mathbf{V}(I \cap J) \subset \mathbf{V}(I) \cup \mathbf{V}(J)$. Теорема доказана. □

Другими словами, пересечению двух идеалов соответствует то же многообразие, что и их произведению. Так как пересечение находить гораздо труднее, чем произведение, то возникает естественный вопрос, стоит ли вообще изучать пересечение идеалов. Причина интереса к пересечениям состоит в том, что пересечение обладает хорошими свойствами по отношению к операции взятия радикала: произведение радикальных идеалов может не быть радикальным идеалом (например, когда $I = J$), но пересечение радикальных идеалов — всегда радикальный идеал. Этот факт вытекает из следующего предложения.

Предложение 16. *Пусть I, J — произвольные идеалы. Тогда*

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Доказательство. Если $f \in \sqrt{I \cap J}$, то $f^m \in I \cap J$ для некоторого натурального m. Тогда $f^m \in I$ и, значит, $f \in \sqrt{I}$. Аналогично, $f^m \in J$ и $f \in \sqrt{J}$. Таким образом, $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

С другой стороны, пусть $f \in \sqrt{I} \cap \sqrt{J}$. Тогда существуют натуральные m и p, такие, что $f^m \in I$ и $f^p \in J$. Таким образом, $f^m f^p = f^{m+p} \in I \cap J$, т. е. $f \in \sqrt{I \cap J}$. □

Упражнения к § 3

1. Докажите, что

$$\langle (x+y)^4 (x^2+y)^2 (x-5y) \rangle \cap \langle (x+y)(x^2+y)^3 (x+3y) \rangle = \langle (x+y)^4 (x^2+y)^3 (x-5y)(x+3y) \rangle.$$

2. Докажите формулу (1) для наименьшего общего кратного двух полиномов f и g.
3. Докажите утверждение (i) предложения 13, т. е. докажите, что пересечение двух главных идеалов является главным идеалом.
4. Докажите утверждение (ii) предложения 13, т. е. докажите, что наименьшее общее кратное двух полиномов $f, g \in k[x_1, \ldots, x_n]$ является образующим идеала $\langle f \rangle \cap \langle g \rangle$.
5. Докажите предложение 14, т. е. докажите, что наименьшее общее кратное двух полиномов, умноженное на их наибольший общий делитель, равно произведению этих полиномов. Указание: воспользуйтесь замечаниями в тексте после предложения 14.
6. Пусть $I_1, \ldots, I_r, J$ — идеалы кольца $k[x_1, \ldots, x_n]$. Докажите, что
   (a) $(I_1 + I_2)J = I_1 J + I_2 J$;
   (b) $(I_1 \ldots I_r)^m = I_1^m \ldots I_r^m$.
7. Пусть I и J — идеалы в $k[x_1, \ldots, x_n]$, где k — произвольное поле. Тогда
   (a) если $I^m \subset J$ для некоторого натурального m, то $\sqrt{I} \subset \sqrt{J}$;
   (b) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
8. Пусть
$$f = x^4 + x^3y + x^3z^2 - x^2y^2 + x^2yz^2 - xy^3 - xy^2z^2 - y^3z^2$$
и
$$g = x^4 + 2x^3z^2 - x^2y^2 + x^2z^4 - 2xy^2z^2 - y^2z^4.$$
   (a) Найдите, используя какую-нибудь систему компьютерной алгебры, образующие идеалов $\langle f \rangle \cap \langle g \rangle$ и $\sqrt{\langle f \rangle \langle g \rangle}$.
   (b) Найдите, используя какую-нибудь систему компьютерной алгебры, $\mathrm{GCD}(f, g)$.
   (c) Пусть $p = x^2 + xy + xz + yz$ и $q = x^2 - xy - xz + yz$. Найдите, используя систему компьютерной алгебры, $\langle f, g \rangle \cap \langle p, q \rangle$.
9. Докажите, что $\sqrt{IJ} = \sqrt{I \cap J}$ (этот результат верен над произвольным полем). Приведите пример, показывающий, что произведение радикальных идеалов может не быть радикальным идеалом. Приведите пример, показывающий, что равенство $\sqrt{IJ} = \sqrt{I}\sqrt{J}$ может не выполняться.
10. Пусть I — идеал в $k[x_1, \ldots, x_n]$, а $\langle f(t) \rangle$ — идеал в $k[t]$. Докажите, что идеал $f(t)I$, определенный в тексте параграфа, является произведением идеала $\widetilde{I}$, порожденного всеми элементами из I в $k[x_1, \ldots, x_n, t]$, и идеала $\langle f(t) \rangle$, порожденного $f(t)$ в $k[x_1, \ldots, x_n, t]$.
11. Два идеала $I, J \subset k[x_1, \ldots, x_n]$ называются *комаксимальными*, если $I + J = k[x_1, \ldots, x_n]$.
   (a) Пусть $k = \mathbb{C}$. Докажите, что I и J комаксимальны в том и только том случае, когда $\mathbf{V}(I) \cap \mathbf{V}(J) = \varnothing$. Приведите пример, показывающий, что это утверждение не выполняется над произвольным полем.

   (b) Докажите, что если I и J комаксимальны, то $IJ = I \cap J$.
   (c) Верно ли утверждение, обратное утверждению п. (b)? То есть вытекает ли из равенства $IJ = I \cap J$ комаксимальность идеалов I и J? Докажите это или приведите контрпример.
   (d) Пусть I и J комаксимальны. Докажите, что I и J^2 тоже комаксимальны. Докажите, что I^r и J^s комаксимальны для всех натуральных r и s.
   (e) Пусть $I_1, \ldots, I_r$ — идеалы в $k[x_1, \ldots, x_n]$, и пусть I_i и $J_i = \bigcap_{j \neq i} I_j$ комаксимальны для всех целых i. Докажите, что для всех целых $m > 0$
$$I_1^m \cap \cdots \cap I_r^m = (I_1 \ldots I_r)^m = (I_1 \cap \cdots \cap I_r)^m.$$
12. Пусть I — идеал в $k[x_1, \ldots, x_n]$, и пусть $I \subset \sqrt{J}$. Докажите, что $I^m \subset J$ для некоторого натурального m. Указание: воспользуйтесь теоремой Гильберта о базисе.
13. Пусть A есть $m \times n$-матрица с элементами из k, а $x \in k^m$ и $y \in k^n$ — векторы-столбцы, такие, что $x = Ay$. В упр. 9 к § 1 было определено отображение
$$\alpha_A : k[x_1, \ldots, x_m] \longrightarrow k[y_1, \ldots, y_n],$$
которое переводит полином $f \in k[x_1, \ldots, x_m]$ в полином $\alpha_A f \in k[y_1, \ldots, y_n]$, определяемое формулой $\alpha_A f(y) = f(Ay)$.
   (a) Докажите, что множество $\{f \in k[x_1, \ldots, x_m] : \alpha_A f = 0\}$ является идеалом в $k[x_1, \ldots, x_m]$ (это множество называется *ядром отображения* α_A и обозначается $\ker(\alpha_A)$).
   (b) Пусть I — идеал в $k[x_1, \ldots, x_m]$. Докажите, что множество $\alpha_A(I) = \{\alpha_A f : f \in I\}$ может не быть идеалом в $k[y_1, \ldots, y_n]$ (через $\langle \alpha_A(I) \rangle$ мы будем обозначать идеал в $k[y_1, \ldots, y_n]$, порожденный множеством $\alpha_A(I)$, и будем называть его *расширением идеала* I в кольцо $k[y_1, \ldots, y_n]$). Пусть I' — идеал в $k[y_1, \ldots, y_n]$. Докажите, что множество $\alpha_A^{-1}(I') = \{f \in k[x_1, \ldots, x_m] : \alpha_A f \in I'\}$ является идеалом в $k[x_1, \ldots, x_m]$ (этот идеал называется *сжатием* I').
14. Пусть A и α_A такие же, как в упр. 13, и $K = \ker(\alpha_A)$. Пусть I и J — идеалы в $k[x_1, \ldots, x_m]$. Докажите, что
   (a) если $I \subset J$, то $\langle \alpha_A(I) \rangle \subset \langle \alpha_A(J) \rangle$;
   (b) $\langle \alpha_A(I + J) \rangle = \langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle$;
   (c) $\langle \alpha_A(IJ) \rangle = \langle \alpha_A(I) \rangle \langle \alpha_A(J) \rangle$;
   (d) $\langle \alpha_A(I \cap J) \rangle \subset \langle \alpha_A(I) \rangle \cap \langle \alpha_A(J) \rangle$, причем включение превращается в равенство, если $K \subset I$ или $K \subset J$;
   (e) $\langle \alpha_A(\sqrt{I}) \rangle \subset \sqrt{\langle \alpha_A(I) \rangle}$, причем включение превращается в равенство, если $K \subset I$.
15. Пусть A, α_A и K такие же, как выше. Пусть I' и J' — идеалы в $k[y_1, \ldots, y_n]$. Докажите, что
   (a) если $I' \subset J'$, то $\alpha_A^{-1}(I') \subset \alpha_A^{-1}(J')$;
   (b) $\alpha_A^{-1}(I' + J') = \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$;

(c) $\alpha_A^{-1}(I'J') \supset (\alpha_A^{-1}(I'))(\alpha_A^{-1}(J'))$, причем включение превращается в равенство, если правая часть содержит K;
(d) $\alpha_A^{-1}(I' \cap J') = \alpha_A^{-1}(I') \cap \alpha_A^{-1}(J')$;
(e) $\alpha_A^{-1}(\sqrt{I'}) = \sqrt{\alpha_A^{-1}(I')}$.

§ 4. Замыкание Зарисского и частные идеалов

Нам уже встречались множества, которые не являлись многообразиями. Они очень естественно возникли в гл. 3, где мы обнаружили, что такие обычные множества, как проекции многообразий, могут не быть многообразиями. А в упражнениях в гл. 1 мы видели, что теоретико-множественная разность многообразий также может не быть многообразием.

Пусть $S \subset k^n$ — произвольное множество (не обязательно многообразие). Тогда множество

$$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \quad \text{для всех} \quad a \in S\}$$

является идеалом (проверьте это!). Более того, этот идеал радикален. Согласно установленному выше соответствию между идеалами и многообразиями, $\mathbf{V}(\mathbf{I}(S))$ — многообразие.

Предложение 1. *Пусть $S \subset k^n$. Тогда $\mathbf{V}(\mathbf{I}(S))$ — наименьшее многообразие, содержащее S (в том смысле, что если $W \subset k^n$ — некоторое многообразие, содержащее S, то $\mathbf{V}(\mathbf{I}(S)) \subset W$).*

Доказательство. Если $W \supset S$, то $\mathbf{I}(W) \subset \mathbf{I}(S)$ (потому что $\mathbf{I}$ обращает включение). Но тогда $\mathbf{V}(\mathbf{I}(W)) \supset \mathbf{V}(\mathbf{I}(S))$ (потому что $\mathbf{V}$ обращает включение). Так как W — аффинное многообразие, то $\mathbf{V}(\mathbf{I}(W)) = W$ по теореме 7 из § 2, и предложение доказано. □

Теперь можно дать следующее определение.

Определение 2. *Замыканием Зарисского* подмножества аффинного пространства называется наименьшее аффинное алгебраическое многообразие, содержащее это подмножество. Если $S \subset k^n$, то замыкание Зарисского множества S обозначается через $\bar{S}$, и оно равно $\mathbf{V}(\mathbf{I}(S))$.

Многообразия, определенные исключающими идеалами, являются естественным примером замыкания Зарисского. Теперь мы можем доказать первое утверждение теоремы о замыкании (теорема 3 из § 2 гл. 3).

Теорема 3. *Пусть поле k алгебраически замкнуто, $V = \mathbf{V}(f_1, \ldots, f_s) \subset k^n$, а $\pi_l : k^n \to k^{n-l}$ — проекция на последние $n - l$ компонент. Если I_l есть l-й исключающий идеал, $I_l = \langle f_1, \ldots, f_s \rangle \cap k[x_{l+1}, \ldots, x_n]$, то $\mathbf{V}(I_l)$ является замыканием Зарисского множества $\pi_l(V)$.*

Доказательство. Согласно предложению 1, мы должны доказать, что $\mathbf{V}(I_l) = \mathbf{V}(\mathbf{I}(\pi_l(V)))$. По лемме 1 из § 2 гл. 3 $\pi_l(V) \subset \mathbf{V}(I_l)$. Так как $\mathbf{V}(\mathbf{I}(\pi_l(V)))$ — это наименьшее многообразие, содержащее $\pi_l(V)$, то $\mathbf{V}(\mathbf{I}(\pi_l(V))) \subset \mathbf{V}(I_l)$.

С другой стороны, пусть $f \in \mathbf{I}(\pi_l(V))$, т. е. $f(a_{l+1}, \ldots, a_n) = 0$ для всех $(a_{l+1}, \ldots, a_n) \in \pi_l(V)$. Мы будем рассматривать f как элемент кольца $k[x_1, \ldots, x_n]$. Тогда $f(a_1, \ldots, a_n) = 0$ для всех $(a_1, \ldots, a_n) \in V$. По теореме Гильберта о нулях $f^N \in \langle f_1, \ldots, f_s \rangle$ для некоторого натурального N. Так как f не зависит от переменных $x_1, \ldots, x_l$, то и f^N также от них не зависит, т. е. $f^N \in \langle f_1, \ldots, f_s \rangle \cap k[x_{l+1}, \ldots, x_n] = I_l$. Значит, $f \in \sqrt{I_l}$, откуда $\mathbf{I}(\pi_l(V)) \subset \sqrt{I_l}$. Но тогда $\mathbf{V}(I_l) = \mathbf{V}(\sqrt{I_l}) \subset \mathbf{V}(\mathbf{I}(\pi_l(V)))$. Теорема доказана. □

Вторая ситуация, когда мы обнаружили множества, не являющиеся многообразиями — это взятие теоретико-множественной разности многообразий. Пусть, например, $W = \mathbf{V}(K)$, где $K = \langle xz, yz \rangle \subset k[x, y, z]$, и $V = \mathbf{V}(I)$, где $I = \langle z \rangle$. Мы знаем, что W — это объединение плоскости xy и оси z. Так как V — плоскость xy, то $W - V$ — это ось z без начала координат (потому что начало координат принадлежит плоскости xy). В гл. 1 было доказано, что это множество не является многообразием. Ось z $(= \mathbf{V}(x, y))$ — это наименьшее многообразие, содержащее $W - V$.

Существует ли общий способ находить идеал, отвечающий замыканию Зарисского $\overline{W - V}$ разности двух многообразий W и V? Ответ здесь утвердительный, но нам потребуется новая алгебраическая конструкция.

Сначала докажем следующий факт.

Предложение 4. *Пусть V и W — многообразия и $V \subset W$. Тогда $W = V \cup (\overline{W - V})$.*

Доказательство. Так как $W - V \subset W$ и W — многообразие, то $\overline{W - V} \subset W$. А так как $V \subset W$ по предположению, то $V \cup (\overline{W - V}) \subset W$.

С другой стороны, из включения $V \subset W$ следует, что $W = V \cup (W - V)$. Так как $W - V \subset \overline{W - V}$, то $W \subset V \cup (\overline{W - V})$. □

Наша задача — определить аналог замыкания $\overline{W - V}$ в теории идеалов.

Определение 5. Пусть I, J — идеалы в $k[x_1, \ldots, x_n]$. Тогда через $I : J$ обозначается множество

$$\{f \in k[x_1, \ldots, x_n] : fg \in I \quad \text{для всех} \quad g \in J\}.$$

Это множество называется *частным идеала* I по J.

Например, в $k[x, y, z]$ имеем

$$\begin{aligned}\langle xz, yz\rangle : \langle z\rangle &= \{f \in k[x,y,z] : f \cdot z \in \langle xz, yz\rangle\} \\ &= \{f \in k[x,y,z] : f \cdot z = Axz + Byz\} \\ &= \{f \in k[x,y,z] : f = Ax + By\} \\ &= \langle x, y\rangle.\end{aligned}$$

Предложение 6. *Пусть I, J — идеалы в $k[x_1, \ldots, x_n]$. Тогда $I : J$ также идеал в $k[x_1, \ldots, x_n]$ и $I : J$ содержит I.*

Доказательство. Пусть $f \in I$. Тогда $fg \in I$ для всех $g \in k[x_1, \ldots, x_n]$ и, значит, для всех $g \in J$, т. е. $f \in I : J$. Теперь докажем, что $I : J$ является идеалом. Прежде всего, $0 \in I : J$, так как $0 \in I$. Пусть $f_1, f_2 \in I : J$. Тогда $f_1 g$ и $f_2 g$ принадлежат I для всех $g \in J$. Значит, $(f_1 + f_2)g = f_1 g + f_2 g \in I$, так как I — идеал. Поэтому $f_1 + f_2 \in I : J$. Если $f \in I : J$ и $h \in k[x_1, \ldots, x_n]$, то $fg \in I$ и $hfg \in I$ для всех $g \in J$; значит, $hf \in I : J$. □

Следующая теорема показывает, что частное идеалов является алгебраическим аналогом замыкания Зарисского разности многообразий.

Теорема 7. *Пусть I, J — идеалы в $k[x_1, \ldots, x_n]$. Тогда*

$$\mathbf{V}(I : J) \supset \overline{\mathbf{V}(I) - \mathbf{V}(J)}.$$

Если k алгебраически замкнуто, а I — радикальный идеал, то

$$\mathbf{V}(I : J) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}.$$

Доказательство. Мы утверждаем, что $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Пусть $f \in I : J$ и $x \in \mathbf{V}(I) - \mathbf{V}(J)$. Тогда $fg \in I$ для всех $g \in J$. Так как $x \in \mathbf{V}(I)$, то $f(x)g(x) = 0$ для всех $g \in J$. Поскольку $x \notin \mathbf{V}(J)$, найдется $g \in J$, такой, что $g(x) \neq 0$. Следовательно, $f(x) = 0$ для любого $x \in \mathbf{V}(I) - \mathbf{V}(J)$. Значит, $f \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Утверждение доказано. Так как $\mathbf{V}$ обращает включения, то $\mathbf{V}(I : J) \supset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$, что и доказывает первую часть теоремы.

Пусть теперь k алгебраически замкнуто и $I = \sqrt{I}$. Пусть $x \in \mathbf{V}(I : J)$. Это означает, что

$$\text{если } hg \in I \text{ для всех } g \in J, \text{ то } \quad h(x) = 0. \tag{1}$$

Пусть теперь $h \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Если $g \in J$, то hg обращается в нуль на $\mathbf{V}(I)$, потому что h обращается в нуль на $\mathbf{V}(I) - \mathbf{V}(J)$, а g обращается в нуль на $\mathbf{V}(J)$. По теореме Гильберта о нулях $hg \in \sqrt{I}$, но по предположению $\sqrt{I} = I$; следовательно, $hg \in I$ для всех g. Тогда по (1) $h(x) = 0$, т. е. $x \in \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$. Значит,

$$\mathbf{V}(I : J) \subset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))),$$

что и завершает доказательство. □

Следующее утверждение справедливо над любым полем.

Следствие 8. *Пусть V и W являются многообразиями в k^n. Тогда*

$$\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V - W).$$

Доказательство. В теореме 7 было доказано, что $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Пусть $I = \mathbf{I}(V)$ и $J = \mathbf{I}(W)$; тогда $\mathbf{I}(V) : \mathbf{I}(W) \subset \mathbf{I}(V - W)$. Противоположное включение следует из определения частного идеалов. □

В следующем предложении перечислены основные свойства частных идеалов. Мы рекомендуем читателю переформулировать их в терминах многообразий (тогда они становятся очевидными).

Предложение 9. *Пусть I, J и K — идеалы в $k[x_1, \ldots, x_n]$. Тогда*

(i) $I : k[x_1, \ldots, x_n] = I$;
(ii) $IJ \subset K$ *в том и только том случае, когда* $I \subset K : J$;
(iii) $J \subset I$ *в том и только том случае, когда* $I : J = k[x_1, \ldots, x_n]$.

Доказательство этого утверждения мы оставляем читателю в качестве упражнения. □

В следующем предложении мы изучаем связи операции взятия частного с ранее введенными операциями на множестве идеалов.

Предложение 10. *Пусть I, I_i, J, J_i и K — идеалы в $k[x_1, \ldots, x_n]$, где $1 \leq i \leq r$. Тогда*

$$\left(\bigcap_{i=1}^{r} I_i\right) : J = \bigcap_{i=1}^{r} (I_i : J), \tag{2}$$

$$I : \left(\sum_{i=1}^{r} J_i\right) = \bigcap_{i=1}^{r} (I : J_i), \tag{3}$$

$$(I : J) : K = I : JK. \tag{4}$$

Доказательство мы снова оставляем читателю в качестве упражнения. □

Если f — полином, а I — идеал, то мы будем писать $I : f$ вместо $I : \langle f \rangle$. Следующее равенство является частным случаем равенства (3):

$$I : \langle f_1, \ldots, f_r \rangle = \bigcap_{i=1}^{r} (I : f_i). \tag{5}$$

Теперь мы ответим на вопрос, как найти образующие идеала $I : J$, если образующие идеалов I и J нам известны. Основной шаг в решении этой задачи делается в следующей теореме.

Теорема 11. *Пусть I — идеал, а g — некоторый полином из $k[x_1, \ldots, x_n]$. Если множество $\{h_1, \ldots, h_p\}$ образует базис идеала $I \cap \langle g \rangle$, то множество $\{h_1/g, \ldots, h_p/g\}$ образует базис идеала $I : g$.*

Доказательство. Пусть $a \in \langle g \rangle$. Тогда $a = bg$ для некоторого полинома b. Поэтому если $f \in \langle h_1/g, \ldots, h_p/g \rangle$, то

$$af = bgf \in \langle h_1, \ldots, h_p \rangle = I \cap \langle g \rangle \subset I.$$

Таким образом, $f \in I : g$. Обратно, пусть $f \in I : g$. Тогда $fg \in I$. Так как $fg \in \langle g \rangle$, то $fg \in I \cap \langle g \rangle$. Если $I \cap \langle g \rangle = \langle h_1, \ldots, h_p \rangle$, то $fg = \sum r_i h_i$, где r_i — некоторые полиномы. Так как каждый полином h_i лежит в $\langle g \rangle$, то частное h_i/g является полиномом; значит, $f = \sum r_i (h_i/g)$, т. е. $f \in \langle h_1/g, \ldots, h_p/g \rangle$. □

Эта теорема, процедура вычисления пересечения идеалов и равенство (5) позволяют построить *алгоритм для вычисления базиса частного идеалов*. А именно, пусть $I = \langle f_1, \ldots, f_r \rangle$ и $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \ldots + \langle g_s \rangle$. Для того чтобы найти базис идеала $I : J$, мы сначала строим базис каждого идеала $I : g_i$. В силу теоремы 11 нужно сначала найти базис пересечения $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$. Напоминаем, что для этого надо найти базис Грёбнера идеала $\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$ по отношению к lex-упорядочению, где t больше всех x_j, и исключить все элементы базиса, зависящие от t. Теперь с помощью алгоритма деления делим каждый элемент построенного базиса пересечения на g_i и получаем базис идеала $I : g_i$. Наконец, мы находим базис идеала $I : J$, применяя алгоритм пересечения $s-1$ раз, т. е. вычисляя сначала базис идеала $I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$, затем базис идеала $I : \langle g_1, g_2, g_3 \rangle = (I : g_1) \cap (I : g_2) \cap (I : g_3)$ и т. д.

Упражнения к § 4

1. Найдите замыкание Зарисского следующих множеств:
   (a) проекции гиперболы $\mathbf{V}(xy-1)$ в $\mathbb{R}^2$ на ось x;
   (b) границы первого квадранта в $\mathbb{R}^2$;
   (c) множества $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$.
2. Пусть $f = (x+y)^2(y-x)(x+z^2)$ и $g = (x+z^2)^3(x-y)(z+y)$. Найдите базис идеала $\langle f \rangle : \langle g \rangle$.
3. Рассмотрим идеалы I и J и предположим, что I радикален. Докажите, что $I : J$ — радикальный идеал и $I : J = I : \sqrt{J}$.
4. Покажите на примере, что требование радикальности идеала I необходимо для справедливости теоремы 7. Указание: проанализируйте доказательство теоремы и найдите то место, где используется радикальность идеала I.
5. Докажите предложение 9 и найдите геометрическую интерпретацию каждого его утверждения.
6. Докажите предложение 10 и найдите геометрическую интерпретацию каждого из его утверждений.
7. Пусть A есть $m \times n$-матрица с элементами из k, а $x \in k^m$ и $y \in k^n$ — векторы-столбцы, причем $x = Ay$. В упр. 9 из § 1 и 13 из § 3 мы определили отображение
   $$\alpha_A : k[x_1, \ldots, x_m] \longrightarrow k[y_1, \ldots, y_n],$$
   полагая $\alpha_A f(y) = f(Ay)$ для $f \in k[x_1, \ldots, x_m]$.
   (a) Докажите, что $\alpha_A(I : J) \subset \alpha_A(I) : \alpha_A(J)$, причем равенство достигается, когда $K \subset I$, где $K = \ker(\alpha_A)$.
   (b) Докажите, что $\alpha_A^{-1}(I' : J') = \alpha_A^{-1}(I') : \alpha_A^{-1}(J')$.
8. Пусть $I \subset k[x_1, \ldots, x_n]$ — идеал и $f \in k[x_1, \ldots, x_n]$. Тогда *насыщением идеала* I по отношению к f называется множество
   $$I : f^\infty = \{g \in k[x_1, \ldots, x_n] : f^m g \in I \quad \text{для некоторого} \quad m > 0\}.$$
   (a) Докажите, что $I : f^\infty$ является идеалом.
   (b) Докажите, что мы имеем возрастающую цепь идеалов $I : f \subset I : f^2 \subset I : f^3 \subset \ldots$.
   (c) Из п. (b) и теоремы об обрыве возрастающих цепей (теорема 7 из § 5 гл. 2) мы знаем, что, начиная с некоторого N, $I : f^N = I : f^{N+1} = \ldots$. Докажите, что $I : f^\infty = I : f^N$.
   (d) Докажите, что $I : f^\infty = I : f^m$ в том и только том случае, когда $I : f^m = I : f^{m+1}$.
   (e) Используя п. (d), постройте алгоритм, вычисляющий насыщение $I : f^\infty$.
9. Пусть $I = \langle f_1, \ldots, f_s \rangle$ — идеал в $k[x_1, \ldots, x_n]$ и $f \in k[x_1, \ldots, x_n]$ — некоторый полином. Введем новую переменную y и положим
   $$\widetilde{I} = \langle f_1, \ldots, f_s, 1 - fy \rangle \subset k[x_1, \ldots, x_n, y].$$

(a) Докажите, что $I : f^\infty = \widetilde{I} \cap k[x_1, \ldots, x_n]$. Указание: см. доказательство предложения 8 из § 2.
(b) Используя п. (a), постройте еще один алгоритм, вычисляющий $I : f^\infty$.

10. Докажите, что $I : f^\infty = k[x_1, \ldots, x_n]$ в том и только том случае, когда $f \in \sqrt{I}$. Отметим, что предложение 8 является прямым следствием упр. 9 и 10.

§ 5. Неприводимые многообразия и простые идеалы

Мы знаем, что объединение двух многообразий является многообразием. Например, в гл. 1 и в предыдущем параграфе мы рассматривали многообразие $\mathbf{V}(xz, yz)$, которое представляет собой объединение прямой и плоскости. На неформальном уровне можно считать, что прямая и плоскость «более фундаментальны», чем $\mathbf{V}(xz, yz)$. Интуиция подсказывает нам, что прямая и плоскость «неприводимы» или «неразложимы» в том смысле, что они не могут быть представлены в виде конечных объединений более простых многообразий. Дадим строгое определение.

Определение 1. Аффинное многообразие $V \subset k^n$ называется *неприводимым*, если оно может быть представлено в виде $V = V_1 \cup V_2$, где V_1 и V_2 — аффинные многообразия, в том и только том случае, когда или $V_1 = V$, или $V_2 = V$.

Таким образом, многообразие $\mathbf{V}(xz, yz)$ не является приводимым. Однако не совсем ясно, какие именно многообразия являются неприводимыми. Если это определение соответствует нашей геометрической интуиции, то кажется очевидным, что точка, прямая и плоскость должны быть неприводимыми. Скрученная кубика $\mathbf{V}(y - x^2, z - x^3)$ в $\mathbb{R}^3$ тоже кажется неприводимой. Но как доказать это? Для этого нужно переформулировать определение алгебраически: охарактеризовать идеалы, соответствующие неприводимым многообразиям. Тогда, возможно, нам удастся доказать неприводимость некоторых многообразий.

Введем следующее определение.

Определение 2. Идеал $I \subset k[x_1, \ldots, x_n]$ называется *простым*, если для любых $f, g \in k[x_1, \ldots, x_n]$ из $fg \in I$ следует, что или $f \in I$, или $g \in I$.

Теперь нужно убедиться в том, что неприводимым многообразиям соответствуют простые идеалы и обратно. Следующая теорема утверждает, что это действительно так.

Предложение 3. *Пусть $V \subset k^n$ — аффинное многообразие. Тогда оно неприводимо в том и только том случае, когда идеал $\mathbf{I}(V)$ прост.*

Доказательство. Пусть V неприводимо и $fg \in \mathbf{I}(V)$. Положим $V_1 = V \cap \mathbf{V}(f)$ и $V_2 = V \cap \mathbf{V}(g)$. И V_1, и V_2 — это пересечения аффинных многообразий; значит, сами они также являются аффинными многообразиями. Так как $fg \in \mathbf{I}(V)$, то $V = V_1 \cup V_2$. Но V неприводимо; следовательно, или $V_1 = V$, или $V_2 = V$. Пусть $V = V_1 = V \cap \mathbf{V}(f)$. Но тогда f равен нулю на V, т. е. $f \in \mathbf{I}(V)$ и идеал $\mathbf{I}(V)$ прост.

Пусть теперь идеал $\mathbf{I}(V)$ прост, и пусть $V = V_1 \cup V_2$. Предположим, что $V_1 \neq V$. Мы утверждаем, что тогда $\mathbf{I}(V) = \mathbf{I}(V_2)$. Докажем это. Так как $V_2 \subset V$, то $\mathbf{I}(V) \subset \mathbf{I}(V_2)$. Однако $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$, так как $V_1 \subsetneq V$. Значит, существует полином $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$. Пусть теперь g — произвольный полином из $\mathbf{I}(V_2)$. Так как $V = V_1 \cup V_2$, то fg равен нулю на V; следовательно, $fg \in \mathbf{I}(V)$. Но идеал $\mathbf{I}(V)$ простой, т. е. или f, или g принадлежит $\mathbf{I}(V)$. Однако мы знаем, что $f \notin \mathbf{I}(V)$. Следовательно, $g \in \mathbf{I}(V)$. Отсюда вытекает, что $\mathbf{I}(V) = \mathbf{I}(V_2)$ и, значит, $V = V_2$, потому что отображение $\mathbf{I}$ инъективно. Таким образом, V неприводимо. □

Легко показать, что каждый простой идеал радикален. Тогда, используя соответствие идеал—многообразие между радикальными идеалами и аффинными многообразиями, получаем такое следствие предложения 3:

Следствие 4. *Пусть поле k алгебраически замкнуто. Тогда отображения $\mathbf{I}$ и $\mathbf{V}$ задают взаимно однозначное соответствие между неприводимыми многообразиями в k^n и простыми идеалами в $k[x_1, \ldots, x_n]$.*

В качестве примера применения предложения 3 докажем, что скрученная кубика неприводима, т. е. что идеал $\mathbf{I}(V)$ скрученной кубики V прост. Предположим, что $fg \in \mathbf{I}(V)$. Так как параметризация (t, t^2, t^3) кубики нам известна, то для всех t

$$f(t, t^2, t^3)g(t, t^2, t^3) = 0.$$

Отсюда вытекает, что либо $f(t, t^2, t^3)$, либо $g(t, t^2, t^3)$ является нулевым полиномом, т. е. или f, или g равен нулю на V. Следовательно, или f, или g принадлежит $\mathbf{I}(V)$, что и доказывает простоту идеала $\mathbf{I}(V)$. Значит, V — неприводимое многообразие в $\mathbb{R}^3$. Неприводимость прямой доказывается аналогично: сначала она параметризуется, а затем используется примененное выше рассуждение.

Этот пример легко может быть обобщен.

Предложение 5. *Пусть поле k бесконечно, а многообразие $V \subset k^n$ задано параметрически уравнениями*

$$\begin{aligned} x_1 &= f_1(t_1, \dots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \dots, t_m), \end{aligned}$$

где $f_1, \dots, f_n \in k[t_1, \dots, t_m]$. Тогда V неприводимо.

Доказательство. Как и в § 3 гл. 3, пусть $F : k^m \to k^n$ — отображение, заданное формулой

$$F(t_1, \dots, t_m) = (f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)).$$

Так как V задано параметрически указанными выше уравнениями, то оно есть замыкание Зарисского множества $F(k^m)$. В частности, $\mathbf{I}(V) = \mathbf{I}(F(k^m))$.

Для любого полинома $g \in k[x_1, \dots, x_n]$ функция $g \circ F$ является полиномом из $k[t_1, \dots, t_m]$, т. е. $g \circ F$ — полином, полученный «подстановкой» полиномов $f_1, \dots, f_n$ в g,

$$g \circ F = g(f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)).$$

Так как k бесконечно, то $\mathbf{I}(V) = \mathbf{I}(F(k^m))$ — это множество полиномов в $k[x_1, \dots, x_n]$, композиция которых с F является нулевым полиномом в $k[t_1, \dots, t_m]$:

$$\mathbf{I}(V) = \{g \in k[x_1, \dots, x_n] : g \circ F = 0\}.$$

Пусть теперь $gh \in \mathbf{I}(V)$. Тогда $(gh) \circ F = (g \circ F)(h \circ F) = 0$. (Убедитесь, что поняли это рассуждение.) Но если произведение двух полиномов из $k[t_1, \dots, t_m]$ является нулевым полиномом, то один из них нулевой. Следовательно, либо $g \circ F = 0$, либо $h \circ F = 0$. Это означает, что или $g \in \mathbf{I}(V)$, или $h \in \mathbf{I}(V)$. Таким образом, $\mathbf{I}(V)$ — простой идеал и V неприводимо. □

С небольшими изменениями приведенные рассуждения могут быть применены для доказательства того, что многообразие, заданное *рациональной* параметризацией, неприводимо.

Предложение 6. *Пусть поле k бесконечно, а многообразие V задано рациональной параметризацией*

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \end{aligned}$$

где $f_1, \dots, f_n, g_1, \dots, g_n \in k[t_1, \dots, t_m]$. Тогда V неприводимо.

Доказательство. Пусть $W = \mathbf{V}(g_1 \dots g_n)$, а $F : k^m - W \to k^n$ — отображение, определенное формулой

$$F(t_1, \dots, t_m) = \left(\frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \dots, \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)}\right).$$

Тогда V — замыкание Зарисского множества $F(k^m - W)$, и, следовательно, $\mathbf{I}(V)$ — это множество полиномов $h \in k[x_1, \dots, x_n]$, таких, что функция $h \circ F$ равна нулю для всех $(t_1, \dots, t_m) \in k^m - W$. Здесь мы сталкиваемся с трудностью: $h \circ F$ может не быть полиномом, поэтому схема доказательства предложения 5 не проходит.

Мы справимся с этой трудностью следующим образом. Пусть $h \in k[x_1, \dots, x_n]$. Так как

$$g_1(t_1, \dots, t_m) g_2(t_1, \dots, t_m) \dots g_n(t_1, \dots, t_m) \neq 0$$

для любой точки $(t_1, \dots, t_m) \in k^m - W$, то функция $(g_1 \dots g_n)^N (h \circ F)$ обращается в нуль в точности в тех точках из $k^m - W$, в которых обращается в нуль функция $h \circ F$. Более того, пусть N — полная степень полинома $h \in k[x_1, \dots, x_n]$; тогда $(g_1 \dots g_n)^N (h \circ F) \in k[t_1, \dots, t_m]$ (докажите это самостоятельно). Таким образом, $h \in \mathbf{I}(V)$ в том и только том случае, когда $(g_1 \dots g_n)^N (h \circ F)$ равен нулю для всех точек $t \in k^m - W$. В упр. 11 к § 3 гл. 3 было доказано, что это возможно в том и только том случае, когда $(g_1 \dots g_n)^N (h \circ F)$ является нулевым полиномом в $k[t_1, \dots, t_m]$. Таким образом, мы доказали, что

$h \in \mathbf{I}(V)$ в том и только том случае, когда

$$(g_1 \dots g_n)^N (h \circ F) = 0 \in k[t_1, \dots, t_m].$$

Теперь докажем, что $\mathbf{I}(V)$ прост. Пусть $p, q \in k[x_1, \dots, x_n]$ и $pq \in \mathbf{I}(V)$. Если полная степень полинома p равна M, а полная степень полинома q равна N, то полная степень полинома pq равна $M + N$. Таким образом, $(g_1 \dots g_n)^{M+N} (p \circ F)(q \circ F) = 0$. Но этот полином есть произведение полиномов $(g_1 \dots g_n)^M (p \circ F)$ и $(g_1 \dots g_n)^N (q \circ F)$ из $k[t_1, \dots, t_m]$. Следовательно, один из них должен быть нулевым полиномом. В частности, или $p \in \mathbf{I}(V)$, или $q \in \mathbf{I}(V)$. Значит, идеал $\mathbf{I}(V)$ прост и многообразие V неприводимо. □

Простейшее многообразие в k^n, задаваемое с помощью параметризации, — это точка $\{(a_1, \dots, a_n)\}$. Это многообразие задается параметрически полиномами $f_i(t_1, \dots, t_m) = a_i$, $1 \leq i \leq n$. Ясно, что оно неприводимо; легко проверить, что идеал $\mathbf{I}(\{(a_1, \dots, a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ (см. упр. 7) прост. Идеал $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ обладает еще одним замечательным свойством: он максимален в том смысле, что любой другой идеал, строго содержащий его, совпадает со всем кольцом $k[x_1, \dots, x_n]$. Такие идеалы достаточно важны и требуют отдельного рассмотрения.

Определение 7. Идеал $I \subset k[x_1, \ldots, x_n]$ называется *максимальным*, если $I \neq k[x_1, \ldots, x_n]$ и любой идеал J, содержащий I, равен либо I, либо $k[x_1, \ldots, x_n]$.

Чтобы упростить формулировки, мы дадим еще одно полезное определение.

Определение 8. Идеал $I \subset k[x_1, \ldots, x_n]$ называется *собственным*, если он не совпадает с $k[x_1, \ldots, x_n]$.

Таким образом, идеал I максимален, если он собственный и не может строго содержаться в другом собственном идеале. Теперь мы докажем, что идеал I вида $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ максимален.

Предложение 9. *Пусть k — произвольное поле, а $a_1, \ldots, a_n \in k$. Тогда идеал I вида $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ максимален.*

Доказательство. Предположим, что идеал J строго содержит I. Тогда существует полином $f \in J$, такой, что $f \notin I$. Используя алгоритм деления, запишем f в виде $A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) + b$, где $b \in k$. Так как $A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) \in I$ и $f \notin I$, то $b \neq 0$. Но $f \in J$ и $I \subset J$; значит,

$$b = f - (A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n)) \in J.$$

Так как $b \neq 0$, то $1/b \cdot b = 1 \in J$; следовательно, $J = k[x_1, \ldots, x_n]$. □

Поскольку

$$\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\},$$

любая точка $(a_1, \ldots, a_n) \in k^n$ соответствует максимальному идеалу в $k[x_1, \ldots, x_n]$, а именно идеалу $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Если k не является алгебраически замкнутым, то обратное утверждение неверно. В упражнениях мы докажем, что идеал $\langle x^2 + 1 \rangle$ максимален в $\mathbb{R}[x]$. Этому идеалу не отвечает никакая точка в $\mathbb{R}$. Однако следующее утверждение справедливо в любом полиномиальном кольце.

Предложение 10. *Пусть k — произвольное поле. Тогда любой максимальный идеал в $k[x_1, \ldots, x_n]$ прост.*

Доказательство. Пусть I — собственный идеал, не являющийся простым. Тогда найдутся полиномы $f, g \notin I$, такие, что $fg \in I$. Рассмотрим идеал $\langle f \rangle + I$. Этот идеал строго содержит I, потому что $f \notin I$. Более того, если $\langle f \rangle + I = k[x_1, \ldots, x_n]$, то $1 = cf + h$ для некоторого полинома c и некоторого $h \in I$. Умножая это равенство на g, получим $g = cfg + hg \in I$, что противоречит выбору g. Значит, $\langle f \rangle + I$ — это собственный идеал, строго содержащий I, т. е. I не максимален. □

Отметим, что в силу предложений 9 и 10 идеал $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ прост в $k[x_1, \ldots, x_n]$, даже если k конечно. Над алгебраически замкнутым полем любой максимальный идеал соответствует точке из k^n.

Теорема 11. *Пусть k алгебраически замкнуто. Тогда любой максимальный идеал в $k[x_1, \ldots, x_n]$ имеет вид $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$, где $a_1, \ldots, a_n \in k$.*

Доказательство. Пусть $I \subset k[x_1, \ldots, x_n]$ — максимальный идеал. Так как $I \neq k[x_1, \ldots, x_n]$, то по слабой теореме о нулях (теорема 1 из § 1) $\mathbf{V}(I) \neq \varnothing$. Значит, некоторая точка $(a_1, \ldots, a_n)$ лежит в $\mathbf{V}(I)$. Переходя к идеалам, получаем

$$\mathbf{I}(\mathbf{V}(I)) \subset \mathbf{I}(\{(a_1, \ldots, a_n)\}).$$

Но $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ по сильной теореме о нулях (теорема 6 из § 1). Так как I максимален, то он прост (по предложению 10) и, следовательно, радикален, $\sqrt{I} = I$ (см. замечание после предложения 3). Поэтому

$$I \subset \mathbf{I}(\{(a_1, \ldots, a_n)\}).$$

Мы уже упоминали, что $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ (см. упр. 7); поэтому

$$I \subset \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subsetneq k[x_1, \ldots, x_n].$$

Так как I максимален, то $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

Обратите внимание, что доказательство теоремы 11 существенно опирается на теорему о нулях. Нетрудно доказать, что она на самом деле равносильна теореме о нулях.

Вот простое следствие теоремы 11.

Следствие 12. *Пусть поле k алгебраически замкнуто. Тогда существует взаимно однозначное соответствие между точками в k^n и максимальными идеалами кольца $k[x_1, \ldots, x_n]$.*

Наш алгебро-геометрический словарь значительно расширен. Мы узнали, что над алгебраически замкнутым полем непустое неприводимое многообразие соответствует собственному простому идеалу, и обратно. Каждая точка соответствует максимальному идеалу, и обратно.

Упражнения к § 5

1. Пусть полином $h \in k[x_1, \ldots, x_n]$ имеет полную степень N, а F определено, как в предложении 6. Докажите, что $(g_1 \ldots g_n)^N (h \circ F) \in k[t_1, \ldots, t_m]$.

2. Докажите, что простой идеал радикален.
3. Докажите, что идеал I прост в том и только том случае, когда для любых двух идеалов J и K, таких, что $JK \subset I$, либо $J \subset I$, либо $K \subset I$.
4. Пусть $I_1, \ldots, I_n$ — конечное множество идеалов, идеал P прост и $\bigcap_{i=1}^n I_i \subset P$. Докажите, что $I_i \subset P$ для некоторого i и, более того, если $P = \bigcap_{i=1}^n I_i$, то $P = I_i$ для некоторого i.
5. Представьте полином $f = x^2z - 6y^4 + 2xy^3z$ в виде $f = f_1(x,y,z)(x+3) + f_2(x,y,z)(y-1) + f_3(x,y,z)(z-2)$, где $f_1, f_2, f_3 \in k[x,y,z]$.
6. Пусть k — бесконечное поле.
   (a) Докажите, что прямая в k^n является неприводимым многообразием.
   (b) Докажите, что любое линейное подпространство в k^n является неприводимым многообразием. Указание: параметризуйте его и примените предложение 5.
7. Докажите, что
$$\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$
8. Докажите следующие утверждения.
   (a) Идеал $\langle x^2 + 1 \rangle$ максимален в $\mathbb{R}[x]$.
   (b) Если идеал $I \subset \mathbb{R}[x_1, \ldots, x_n]$ максимален, то или $\mathbf{V}(I) = \varnothing$, или $\mathbf{V}(I)$ — это точка из $\mathbb{R}^n$. Указание: проанализируйте доказательство теоремы 11.
   (c) Приведите пример максимального идеала $I \subset \mathbb{R}[x_1, \ldots, x_n]$, такого, что $\mathbf{V}(I) = \varnothing$. Указание: рассмотрите идеал $\langle x_1^2 + 1, x_2, \ldots, x_n \rangle$.
9. Предположим, что поле k не является алгебраически замкнутым.
   (a) Докажите, что если $I \subset k[x_1, \ldots, x_n]$ — максимальный идеал, то или $\mathbf{V}(I) = \varnothing$, или $\mathbf{V}(I)$ — это точка в k^n. Указание: проанализируйте доказательство теоремы 11.
   (b) Докажите, что существует максимальный идеал $I \subset k[x_1, \ldots, x_n]$, такой, что $\mathbf{V}(I) = \varnothing$. Указание: см. предыдущее упражнение.
   (c) Покажите, что всегда существует максимальный идеал в $k[x_1, \ldots, x_n]$, не равный ни одному из идеалов вида $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$.
10. Докажите, что слабая теорема о нулях является следствием теоремы 11.
11. Пусть полином $f \in \mathbb{C}[x_1, \ldots, x_n]$ неприводим. Докажите, что многообразие $\mathbf{V}(f)$ неприводимо.
12. Пусть $I \subset \mathbb{C}[x_1, \ldots, x_n]$ — собственный идеал. Тогда $\sqrt{I}$ является пересечением всех максимальных идеалов, содержащих I. Указание: используйте теорему 11.

§ 6. Разложение многообразия в объединение неприводимых

В предыдущем параграфе мы видели, что неприводимые многообразия естественно возникают во многих задачах. Встает вопрос: верно ли, что произвольное многообразие может быть построено из неприводимых? В этом параграфе мы изучим эту проблему и близкие вопросы.

Мы начнем с перевода *условия обрыва возрастающих цепей* для идеалов (см. § 5 из гл. 2) на язык многообразий.

Предложение 1 (условие обрыва убывающих цепей). *Любая убывающая цепь многообразий*
$$V_1 \supset V_2 \supset V_3 \supset \ldots$$
в k^n стабилизируется, т. е. существует натуральное N, такое, что $V_N = V_{N+1} = V_{N+2} = \ldots$.

Доказательство. Переходя к идеалам, получаем возрастающую цепь
$$\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \mathbf{I}(V_3) \subset \ldots.$$
По условию обрыва возрастающих цепей (теорема 7 из § 5 гл. 2) существует N, такое, что $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \ldots$. Так как $\mathbf{V}(\mathbf{I}(V)) = V$ для любого многообразия V, то $V_N = V_{N+1} = \ldots$. □

Теперь мы можем доказать следующее основное структурное свойство аффинных многообразий.

Теорема 2. *Пусть $V \subset k^n$ — аффинное многообразие. Тогда V может быть представлено в виде конечного объединения неприводимых многообразий V_i:*
$$V = V_1 \cup \ldots \cup V_m.$$

Доказательство. Пусть V — аффинное многообразие, которое нельзя представить в виде конечного объединения неприводимых многообразий. Тогда V не является неприводимым, а значит, $V = V_1 \cup V_1'$, где $V \neq V_1$ и $V \neq V_1'$. Хотя бы одно из многообразий V_1 и V_1' не является объединением конечного числа неприводимых, иначе V можно было бы представить в этом виде. Пусть, например, V_1 не есть конечное объединение неприводимых многообразий. Аналогичное рассуждение показывает, что $V_1 = V_2 \cup V_2'$, где $V_1 \neq V_2$, $V_1 \neq V_2'$ и V_2 не есть объединение конечного числа неприводимых многообразий. Продолжая построение, мы получим бесконечную последовательность многообразий
$$V \supset V_1 \supset V_2 \supset \ldots,$$

причем

$$V \neq V_1 \neq V_2 \neq \dots.$$

Это противоречит предложению 1. □

В качестве простого примера рассмотрим многообразие $\mathbf{V}(xz, yz)$, которое является объединением прямой (ось z) и плоскости (плоскость xy). Оба эти многообразия неприводимы (см. упр. 6 к § 5). В качестве более сложного примера рассмотрим многообразие

$$V = \mathbf{V}(xz - y^2, x^3 - yz).$$

Изобразим это многообразие:

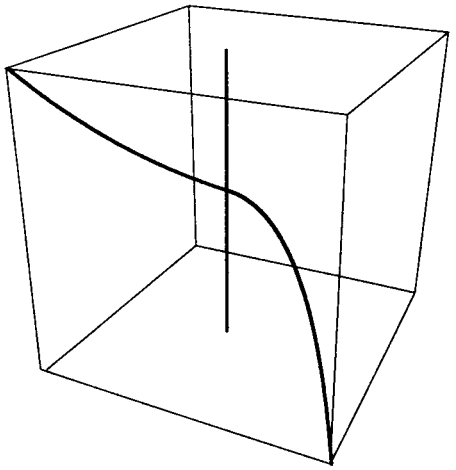


Рисунок подсказывает, что V не является неприводимым: оно есть объединение двух кривых. В самом деле, так как функции $xz - y^2$ и $x^3 - yz$ равны нулю на оси z, то ось z, т. е. многообразие $\mathbf{V}(x, y)$, содержится в V. Что можно сказать о другой кривой $V - \mathbf{V}(x, y)$?

Теорема 7 из § 4 наводит на мысль рассмотреть частное идеалов

$$\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle.$$

(В конце параграфа мы докажем, что идеал $\langle xz - y^2, x^3 - yz\rangle$ радикален.) Воспользуемся алгоритмом для вычисления частного двух идеалов (восстановите его в памяти). В соответствии с равенством (5) из § 4 это частное равно

$$(I : x) \cap (I : y),$$

где $I = \langle xz - y^2, x^3 - yz\rangle$. Для нахождения $I : x$ сначала вычислим пересечение идеалов $I \cap \langle x\rangle$, используя алгоритм для вычисления

пересечений и lex-упорядочение с $z > y > x$. Имеем

$$I \cap \langle x\rangle = \langle x^2 z - xy^2, x^4 - xyz, x^3 y - xz^2, x^5 - xy^3\rangle.$$

Полином $x^5 - xy^3$ есть комбинация первого и второго элементов базиса; следовательно, его можно исключить. Получаем

$$\begin{aligned} I : x &= \left\langle \frac{x^2 z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3 y - xz^2}{x} \right\rangle \\ &= \langle xz - y^2, x^3 - yz, x^2 y - z^2\rangle \\ &= I + \langle x^2 y - z^2\rangle. \end{aligned} \tag{1}$$

Теперь, чтобы найти $I : y$, вычислим

$$I \cap \langle y\rangle = \langle xyz - y^3, x^3 y - y^2 z, x^2 y^2 - yz^2\rangle.$$

Следовательно,

$$\begin{aligned} I : y &= \left\langle \frac{xyz - y^3}{y}, \frac{x^3 y - y^2 z}{y}, \frac{x^2 y^2 - yz^2}{y} \right\rangle \\ &= \langle xz - y^2, x^3 - yz, x^2 y - z^2\rangle \\ &= I + \langle x^2 y - z^2\rangle \\ &= I : x. \end{aligned}$$

(Проделайте эти вычисления, используя систему компьютерной алгебры.) Так как $I : x = I : y$, то

$$I : \langle x, y\rangle = \langle xz - y^2, x^3 - yz, x^2 y - z^2\rangle.$$

Многообразие $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2 y - z^2)$ — это неприводимая кривая, потому что оно имеет параметризацию (t^3, t^4, t^5) (очевидно, что $(t^3, t^4, t^5) \in W$ для любого t, а доказательство того факта, что таким образом параметризованное множество совпадает с W, мы оставляем читателю в качестве упражнения). Следовательно, W неприводимо (по предложению 5 из предыдущего параграфа). Значит,

$$V = \mathbf{V}(x, y) \cup W,$$

(см. упр. 8), что и дает нам требуемое разложение многообразия V.

В предыдущем примере и в случае $\mathbf{V}(xz, yz)$ разложение многообразия на неприводимые многообразия было единственным. Естественно спросить, всегда ли это верно? Очевидно, что мы должны исключить из рассмотрения такие тривиальные случаи, как появление одной и той же неприводимой компоненты несколько раз или включение одной неприводимой компоненты в другую как подмножества. Это и является целью следующего определения.

Определение 3. Пусть $V \subset k^n$ — аффинное многообразие. Разложение

$$V = V_1 \cup \ldots \cup V_m,$$

где многообразия V_i неприводимы, называется *минимальным разложением* (или *неизбыточным объединением*), если V_i не принадлежит V_j при $i \neq j$.

Теперь мы можем сформулировать теорему единственности.

Теорема 4. *Пусть $V \subset k^n$ — аффинное многообразие. Тогда существует минимальное разложение*

$$V = V_1 \cup \ldots \cup V_m$$

(т. е. каждое V_i — неприводимое многообразие и $V_i \not\subset V_j$ при $i \neq j$). Более того, это разложение единственно с точностью до порядка, в котором записаны многообразия $V_1, \ldots, V_m$.

Доказательство. По теореме 2 V может быть представлено в виде $V = V_1 \cup \ldots \cup V_m$, где V_i неприводимы. Предположим, что некоторое V_i лежит в каком-то $V_j, i \neq j$. Тогда мы можем исключить V_i из разложения, и тогда V будет объединением V_l при $l \neq i$. Продолжая этот процесс, мы придем к минимальному разложению.

Докажем единственность. Пусть $V = V_1' \cup \ldots \cup V_l'$ — другое минимальное разложение многообразия V. Тогда

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \ldots \cup V_l') = (V_i \cap V_1') \cup \ldots \cup (V_i \cap V_l').$$

Так как V_i неприводимо, то $V_i = V_i \cap V_j'$ для некоторого j, т. е. $V_i \subset V_j'$. Проводя аналогичные рассуждения для V_j', получаем, что $V_j' \subset V_s$ для некоторого s. Значит,

$$V_i \subset V_j' \subset V_s.$$

Но из минимальности разложения следует, что $i = s$, т. е. $V_i = V_j'$. Значит, каждое V_i содержится в разложении $V = V_1' \cup \ldots \cup V_l'$, откуда следует, что $m \leq l$. Но точно так же можно доказать, что $l \leq m$. Таким образом, $l = m$ и набор V_j' — это просто перестановка набора V_i. □

Отметим, что утверждение о единственности неверно, если отказаться от требования конечности разложения (плоскость есть объединение всех ее точек и одновременно объединение прямой и точек вне этой прямой, а таких прямых на ней бесконечно много). Это должно показать читателю, что хотя теорема 4 имеет простое доказательство, но она вовсе не тривиальна: свойство конечности используется существенно (а конечность есть следствие теоремы Гильберта о базисе).

Взаимно однозначное соответствие между многообразиями и радикальными идеалами позволяет получить алгебраическую переформулировку теорем 2 и 4.

Теорема 5. *Пусть поле k алгебраически замкнуто. Тогда каждый радикальный идеал $I \subset k[x_1, \ldots, x_n]$ может быть однозначно записан в виде пересечения простых идеалов, $I = P_1 \cap \ldots \cap P_r$, где $P_i \not\subset P_j$ при $i \neq j$. (Как и в случае многообразий, такое представление радикального идеала мы называем* минимальным разложением *или* неизбыточным пересечением.)

Доказательство. Теорема 5 является прямым следствием теорем 2 и 4 и соответствия идеал—многообразие. □

Частные идеалов помогают описать простые идеалы, участвующие в минимальном разложении радикального идеала.

Теорема 6. *Пусть поле k алгебраически замкнуто, I — собственный радикальный идеал и*

$$I = \bigcap_{i=1}^{r} P_i$$

— его минимальное разложение. Тогда P_i — это в точности те простые собственные идеалы, которые имеют вид $I : f$, где $f \in k[x_1, \ldots, x_n]$.

Доказательство. Отметим сначала, что если идеал I собственный, то и идеалы P_i собственные (это следует из минимальности).

Для любого $f \in k[x_1, \ldots, x_n]$ имеем

$$I : f = \left(\bigcap_{i=1}^{r} P_i\right) : f = \bigcap_{i=1}^{r} (P_i : f)$$

(формула (2) из § 4). Отметим также, что для любого простого идеала P или $f \in P$ и тогда $P : f = \langle 1 \rangle$, или $f \notin P$ и тогда $P : f = P$ (см. упр. 3).

Пусть теперь $I : f$ — собственный простой идеал. Из упр. 4 к § 5 и приведенной выше формулы следует, что $I : f = P_i : f$ для некоторого i. Так как $P_i : f$ равен P_i или $\langle 1 \rangle$, то $I : f = P_i$.

Чтобы убедиться, что любой P_i получается таким образом, зафиксируем i и возьмем полином

$$f \in \left(\bigcap_{j \neq i}^{r} P_j\right) - P_i.$$

Такой полином существует, потому что разложение $\bigcap_{j=1}^{r} P_j$ минимально. Тогда $P_i : f = P_i$ и $P_j : f = \langle 1 \rangle$ при $j \neq i$. Отсюда вытекает с учетом приведенной выше формулы для $I : f$, что $P_i = I : f$. □

Следует упомянуть, что теоремы 5 и 6 справедливы над любым полем k, хотя метод доказательства в общем случае другой (см. следствие 10 из § 7).

Рассмотрим в качестве примера идеал $I = \langle xz - y^2, x^3 - yz \rangle$. С многообразием $V = \mathbf{V}(I)$ мы уже встречались в этом параграфе. Предположим, что I радикален (мы скоро увидим, что это так). Как найти его представление в виде пересечения простых идеалов?

Начнем с геометрического разложения

$$V = \mathbf{V}(x, y) \cup W,$$

найденного ранее, где $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$. Это разложение приводит к формуле

$$I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle,$$

доказать которую сравнительно нетрудно (см. упр. 4). Кроме того, в силу формулы (1) $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$. Таким образом,

$$I = \langle x, y \rangle \cap (I : x).$$

Идеал $\langle x, y \rangle$ также можно представить, как частное идеала I. Геометрические соображения подсказывают, что для этого надо вычесть W из V. Из трех уравнений, определяющих W, первые два определяют V. Поэтому кажется разумным использовать третье уравнение $x^2y - z^2$. В самом деле, легко проверить, что $I : (x^2y - z^2) = \langle x, y \rangle$ (см. упр. 4). Таким образом,

$$I = (I : (x^2y - z^2)) \cap (I : x). \tag{2}$$

Осталось доказать, что $I : (x^2y - z^2)$ и $I : x$ — простые идеалы. Доказать первое утверждение совсем не сложно, так как идеал $I : (x^2y - z^2) = \langle x, y \rangle$, очевидно, прост. Что касается второго, то мы уже знаем, что $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ неприводимо, а в упражнениях мы докажем, что $\mathbf{I}(W) = \langle xz - y^2, x^3 - yz, x^2y - x^2 \rangle = I : x$. Теперь из предложения 3 § 5 следует, что идеал $I : x$ прост. Это и завершает доказательство того факта, что (2) является минимальным разложением идеала I. Наконец, так как I является пересечением простых идеалов, он радикален (см. упр. 1).

Все эти рассуждения связаны со спецификой идеала $I = \langle xz - y^2, x^3 - yz \rangle$. Желательно, однако, построить методы, применимые в общем случае для разложения любого идеала. В теоремах 2, 4, 5 и 6 утверждается, что разложение есть, но не даются указания на то, как его найти. Дело здесь в том, что доказательства опираются на теорему Гильберта о базисе, которая неконструктивна. Поэтому совершенно естественно возникают также вопросы:

- (Простота) Существует ли алгоритм, позволяющий узнать, прост ли данный идеал?
- (Неприводимость) Существует ли алгоритм, позволяющий узнать, неприводимо ли данное многообразие?
- (Разложение) Существует ли алгоритм, позволяющий построить минимальное разложение данного многообразия или радикального идеала?

Ответ на все эти три вопроса *положительный*. Описания алгоритмов можно найти в работах HERMANN (1926), MINES, RICHMAN, RUITENBURG (1988) и SEIDENBERG (1974, 1984). Как и алгоритм в § 2, алгоритмы, предложенные в этих работах, мало эффективны. Однако недавняя работа GIANNI, TRAGER, ZACHARIAS (1988) привела к созданию алгоритмов, реализованных в системах AXIOM и REDUCE, которые позволяют решить сформулированные выше вопросы. См. также гл. 8 книги BECKER, WEISPFENNING (1993). Еще один алгоритм простоты описан в § 4.4 книги ADAMS, LOUSTAUNAU (1994). Наконец, алгоритм, основанный на идеях из работы EISENBUD, HUNEKE, VASCONCELOS (1992), был реализован в системе Macaulay.

Упражнения к § 6

1. Докажите, что пересечение любого множества простых идеалов является радикальным идеалом.
2. Докажите, что неизбыточное пересечение даже двух простых идеалов не может быть простым.
3. Пусть $P \subset k[x_1, \ldots, x_n]$ — простой идеал. Докажите, что $P : f = P$, если $f \notin P$, и $P : f = \langle 1 \rangle$, если $f \in P$.
4. Пусть $I = \langle xz - y^2, x^3 - yz \rangle$.
   (a) Докажите, что $I : (x^2y - z^2) = \langle x, y \rangle$.
   (b) Докажите, что идеал $I : (x^2y - z^2)$ прост.
   (c) Докажите, что $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y \rangle$.
5. Пусть $J = \langle xz - y^2, x^3 - yz, z^2 - x^2y \rangle$.
   (a) Докажите, что каждая точка в $W = \mathbf{V}(J)$ имеет вид (t^3, t^4, t^5) для некоторого $t \in k$.
   (b) Докажите, что $J = \mathbf{I}(W)$. Указание: найдите базис Грёбнера идеала J для lex-упорядочения с $z > y > x$ и докажите, что любой полином $f \in k[x_1, \ldots, x_n]$ может быть представлен в виде
   $$f = g + a + bz + A(x) + yB(x) + y^2C(x),$$
   где $g \in J, a, b \in k$ и $A, B, C \in k[x]$.

6. Переведите теорему 6 и ее доказательство на язык геометрии.
7. Пусть $I = \langle xz - y^2, z^3 - x^5 \rangle$.
   (a) Найдите представление многообразия $\mathbf{V}(I)$ в виде конечного объединения неприводимых многообразий. Указание: используйте параметризации (t^3, t^4, t^5) и $(t^3, -t^4, t^5)$.
   (b) Представьте I в виде пересечения простых идеалов — частных идеала I — и докажите, что I радикален.
8. Пусть V, W — многообразия в k^n и $V \subset W$. Докажите, что каждая неприводимая компонента многообразия V содержится в некоторой неприводимой компоненте многообразия W.
9. Пусть $f \in \mathbb{C}[x_1, \ldots, x_n]$, и пусть $f = f_1^{a_1} \ldots f_s^{a_s}$ — разложение полинома f на неприводимые множители. Докажите, что $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_s)$ является разложением многообразия $\mathbf{V}(f)$ на неприводимые компоненты и что $\mathbf{I}(\mathbf{V}(f)) = \langle f_1 \ldots f_s \rangle$. Указание: см. упр. 11 к § 5.

§ 7. Дополнение. Примарное разложение идеалов

В свете теоремы о разложении радикальных идеалов, которая была доказана в § 6, естественно спросить, верно ли, что произвольный идеал (не обязательно радикальный) может быть представлен в виде пересечения более простых идеалов. В этом параграфе будет доказана теорема о разложении Ласкера—Нётер, которая детально описывает структуру произвольного идеала.

Представить произвольный идеал в виде пересечения простых нельзя, так как пересечение простых идеалов всегда радикально. Возникает мысль, что можно его представить как пересечение степеней простых идеалов. Она тоже неверна: рассмотрим идеал $I = \langle x, y^2 \rangle \subset \mathbb{C}[x, y]$. Любой простой идеал, содержащий I, должен содержать x и y; значит, он равен $\langle x, y \rangle$ (так как $\langle x, y \rangle$ — максимальный идеал). Таким образом, если бы I был пересечением степеней простых идеалов, то он совпадал бы с некоторой степенью идеала $\langle x, y \rangle$. Но $\langle x, y \rangle^2 \subsetneq I \subsetneq \langle x, y \rangle$ (см. упр. 1).

Поэтому нам необходимо более тонкое понятие.

Определение 1. Идеал $I \subset k[x_1, \ldots, x_n]$ называется *примарным*, если из $fg \in I$ следует, что или $f \in I$, или $g^m \in I$ для некоторого целого $m > 0$.

Очевидно, что простой идеал примарен. Нетрудно доказать примарность рассматривавшегося выше идеала $I = \langle x, y^2 \rangle$ (см. упр. 1).

Лемма 2. *Если идеал I примарен, то идеал $\sqrt{I}$ прост и является наименьшим простым идеалом, содержащим I.*

Доказательство. См. упр. 2. □

Благодаря этой лемме мы можем дать следующее определение.

Определение 3. Пусть I примарен и $\sqrt{I} = P$. Тогда I называется *P-примарным.*

Теперь мы докажем, что каждый идеал является пересечением примарных.

Теорема 4. *Любой идеал $I \subset k[x_1, \ldots, x_n]$ может быть представлен в виде конечного пересечения примарных идеалов.*

Доказательство. Мы назовем идеал I *неприводимым*, если из равенства $I = I_1 \cap I_2$ следует, что или $I = I_1$, или $I = I_2$. Мы утверждаем, что каждый идеал является пересечением конечного числа неприводимых. Доказательство этого утверждения — это перевод на язык идеалов доказательства теоремы 2 из § 6 (используется условие обрыва возрастающих цепей). Мы оставляем его читателю в качестве упражнения.

Теперь мы докажем, что неприводимый идеал примарен. Это и докажет теорему. Пусть I неприводим и $fg \in I$, причем $f \notin I$. Нам нужно доказать, что некоторая степень идеала g принадлежит I. Рассмотрим идеалы $I : g^n$ при $n \geq 1$. В упражнениях мы докажем, что $I : g^n \subset I : g^{n+1}$ для всех n. Значит, мы получаем возрастающую цепь идеалов

$$I : g \subset I : g^2 \subset \ldots.$$

По условию обрыва возрастающих цепей существует $N \geq 1$, такое, что $I : g^N = I : g^{N+1}$. Мы оставляем читателю в качестве упражнения доказательство того, что $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Так как I неприводим, то или $I = I + \langle g^N \rangle$, или $I = I + \langle f \rangle$. Но последнее невозможно, так как $f \notin I$ по условию. Значит, $I = I + \langle g^N \rangle$, т. е. $g^N \in I$. □

Как и в случае многообразий, мы можем определить минимальное разложение.

Определение 5. *Примарным разложением* идеала I называется его представление в виде конечного пересечения примарных идеалов: $I = \bigcap_{i=1}^{r} Q_i$. Разложение называется *минимальным* или *неизбыточным*, если идеалы $\sqrt{Q_i}$ различны и $\bigcap_{j \neq i} Q_j$ не лежит в Q_i ни для какого i.

Для доказательства существования минимального разложения нам понадобится следующая лемма. Ее доказательство мы оставляем читателю в качестве упражнения.

Лемма 6. *Пусть I, J — примарные идеалы и $\sqrt{I} = \sqrt{J}$. Тогда идеал $I \cap J$ примарен.*

Теперь мы докажем первую часть теоремы о разложении Ласкера—Нётер.

Теорема 7 (Ласкер—Нётер). *Для каждого идеала $I \subset k[x_1, \ldots, x_n]$ существует минимальное примарное разложение.*

Доказательство. По теореме 4 существует примарное разложение $I = \bigcap_{i=1}^{r} Q_i$. Предположим, что $\sqrt{Q_i} = \sqrt{Q_j}$ при $i \neq j$. Тогда по лемме 6 идеал $Q = Q_i \bigcap Q_j$ примарен и в разложении идеала I мы можем заменить два идеала Q_i и Q_j одним идеалом Q. Продолжая этот процесс, мы добьемся того, чтобы все примарные идеалы в разложении идеала I имели различные радикалы.

Пусть теперь $\bigcap_{j \neq i} Q_j \subset Q_i$. Тогда мы можем исключить Q_i из разложения. Продолжая этот процесс, мы добьемся того, чтобы условие $Q_i \not\supset \bigcap_{j \neq i} Q_j$ было выполнено для всех i. □

В отличие от случая многообразий (или радикальных идеалов) минимальное примарное разложение не единственно. В упражнениях мы проверим, что идеал $\langle x^2, xy \rangle \subset k[x, y]$ имеет два различных минимальных разложения:

$$\langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x^2, y \rangle.$$

Хотя идеалы $\langle x^2, xy, y^2 \rangle$ и $\langle x^2, y \rangle$ различны, но их радикалы совпадают. Чтобы доказать, что это имеет место и в общем случае, нам понадобятся частные идеалов из § 4. Мы начнем с вычисления частных примарного идеала.

Лемма 8. *Пусть идеал I примарен, $\sqrt{I} = P$ и $f \in k[x_1, \ldots, x_n]$. Тогда*

если $f \in I$, *то* $I : f = \langle 1 \rangle$,
если $f \notin I$, *то* $I : f$ *P-примарен,*
если $f \notin P$, *то* $I : f = I$.

□

Доказательство. См. упр. 7.

Вторая часть теоремы Ласкера—Нётер утверждает, что *радикалы* примарных компонент минимального разложения определены однозначно.

Теорема 9 (Ласкер—Нётер). *Пусть $I = \bigcap_{i=1}^{r} Q_i$ — минимальное примарное разложение собственного идеала $I \subset k[x_1, \ldots, x_n]$, и пусть $P_i = \sqrt{Q_i}$. Тогда P_i — это в точности те собственные простые идеалы, которые содержатся в множестве идеалов $\{\sqrt{I : f} : f \in k[x_1, \ldots, x_n]\}$.*

Замечание. В частности, идеалы P_i не зависят от примарного разложения идеала I. Мы будем говорить, что P_i *принадлежат* I.

Доказательство. Доказательство аналогично доказательству теоремы 6 из § 6. Детали будут рассмотрены в упр. 8–10. □

В § 6 мы доказали теорему разложения для радикальных идеалов над алгебраически замкнутым полем. Теперь, используя теорему Ласкера—Нётер, мы можем доказать ее справедливость для любого поля k.

Следствие 10. *Пусть $I = \bigcap_{i=1}^{r} Q_i$ — минимальное примарное разложение собственного радикального идеала $I \subset k[x_1, \ldots, x_n]$. Тогда идеалы Q_i просты и являются в точности простыми собственными идеалами, которые имеют вид $I : f$, где $f \in k[x_1, \ldots, x_n]$.*

Доказательство. См. упр. 12. □

Теория минимальных примарных разложений не исчерпывается теоремами Ласкера—Нётер. Пусть, например, идеал P_i минимален в том смысле, что никакой идеал P_j не содержится строго в P_i. Тогда Q_i однозначно определен. Таким образом, имеет место теорема единственности для *некоторых* Q_i (см. гл. 4 из книги ATIYAH, MACDONALD (1969)). Следует упомянуть, что теорема 9 может быть усилена: можно доказать, что P_i — это в точности те простые собственные идеалы, которые имеют вид $I : f$, где $f \in k[x_1, \ldots, x_n]$ (см. гл. 7 книги ATIYAH, MACDONALD (1969)).

Наконец, естественно задать вопрос, можно ли описать примарное разложение конструктивно. Точнее, пусть задан идеал $I = \langle f_1, \ldots, f_s \rangle$.

- (Примарное разложение) Существует ли алгоритм, позволяющий найти базисы примарных идеалов Q_i, участвующих в разложении идеала I?
- (Ассоциированные простые идеалы) Можем ли мы найти базисы ассоциированных простых идеалов $P_i = \sqrt{Q_i}$?

Если вы еще раз прочтете библиографические комментарии в конце § 6, то увидите, что ответ положителен. Алгоритмы примарного разложения реализованы в системах AXIOM и REDUCE.

Упражнения к § 7

1. Рассмотрим идеал $I = \langle x, y^2 \rangle \subset \mathbb{C}[x, y]$.
   (a) Докажите, что $\langle x, y \rangle^2 \subsetneq I \subsetneq \langle x, y \rangle$. Выведите отсюда, что I не является степенью простого идеала.
   (b) Докажите, что I примарен.
2. Докажите лемму 2.
3. В этом упражнении мы рассмотрим доказательство теоремы 4. Пусть $I \subset k[x_1, \ldots, x_n]$ — идеал.
   (a) Используя указания, данные в тексте параграфа, докажите, что I является конечным пересечением неприводимых идеалов.
   (b) Пусть $g \in k[x_1, \ldots, x_n]$. Докажите, что $I : g^n \subset I : g^{n+1}$ для всех $n \geq 1$.
   (c) Пусть $fg \in I$ и $I : g^N = I : g^{N+1}$. Докажите, что $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Указание: элементы идеала $(I + \langle g^N \rangle) \cap (I + \langle f \rangle)$ могут быть записаны в виде $a + bg^N = c + df$, где $a, c \in I$, а $b, d \in k[x_1, \ldots, x_n]$. Теперь умножьте это равенство на g.
4. В ходе доказательства теоремы 4 мы показали, что каждый неприводимый идеал примарен. Удивительно, но обратное неверно. Пусть $I = \langle x^2, xy, y^2 \rangle \subset k[x, y]$.
   (a) Докажите, что I примарен.
   (b) Докажите, что $I = \langle x^2, y \rangle \cap \langle x, y^2 \rangle$ и убедитесь, что I не является неприводимым.
5. Докажите лемму 6. Указание: воспользуйтесь предложением 16 из § 3.
6. Пусть $I = \langle x^2, xy \rangle \subset \mathbb{Q}[x, y]$.
   (a) Докажите, что
   $$I = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x^2, y \rangle$$
   — два различных минимальных примарных разложения идеала I.
   (b) Докажите, что для любого $a \in \mathbb{Q}$
   $$I = \langle x \rangle \cap \langle x^2, y - ax \rangle$$
   является минимальным примарным разложением идеала I, т. е. I имеет бесконечно много различных минимальных примарных разложений.
7. Докажите лемму 8.
8. Докажите, что идеал является собственным тогда и только тогда, когда собствен его радикал.
9. Пусть I — собственный идеал. Докажите, что простые идеалы, принадлежащие I, также являются собственными. Указание: используйте упр. 8.

10. Докажите теорему 9. Указание: используйте доказательство теоремы 6 из § 6. Вам также придется переходить к радикалам. Здесь будет полезным предложение 16 из § 3. Также используйте упр. 9 и лемму 8.
11. Пусть $P_1, \ldots, P_r$ — простые идеалы, принадлежащие I.
    (a) Докажите, что $\sqrt{I} = \bigcap_{i=1}^{r} P_i$. Указание: используйте предложение 16 из § 3.
    (b) Рассмотрите идеал из упр. 4 и покажите, что $\sqrt{I} = \bigcap_{i=1}^{r} P_i$ не обязательно является минимальным разложением идеала $\sqrt{I}$.
12. Докажите следствие 10. Указание: докажите, что идеал $I : f$ всегда радикален.

§ 8. Сводка результатов

В следующей таблице сведены воедино результаты этой главы. Мы считаем все идеалы радикальными, а поле алгебраически замкнутым.

АЛГЕБРА		ГЕОМЕТРИЯ
радикальные идеалы		многообразия
I	$\longrightarrow$	$\mathbf{V}(I)$
$\mathbf{I}(V)$	$\longleftarrow$	V
суммы идеалов		пересечения многообразий
$I + J$	$\longrightarrow$	$\mathbf{V}(I) \cap \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V) + \mathbf{I}(W)}$	$\longleftarrow$	$V \cap W$
произведения идеалов		объединение многообразий
IJ	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V)\mathbf{I}(W)}$	$\longleftarrow$	$V \cup W$
пересечения идеалов		объединение многообразий
$I \cap J$	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\mathbf{I}(V) \cap \mathbf{I}(W)$	$\longleftarrow$	$V \cup W$
частные идеалов		разность многообразий
$I : J$	$\longrightarrow$	$\overline{\mathbf{V}(I) - \mathbf{V}(J)}$
$\mathbf{I}(V) : \mathbf{I}(W)$	$\longleftarrow$	$\overline{V - W}$
исключение переменных		проекция многообразий
$\sqrt{I \cap k[x_{l+1}, \ldots, x_n]}$	$\longleftrightarrow$	$\overline{\pi_l(\mathbf{V}(I))}$
простой идеал		неприводимое многообразие
максимальный идеал		точка аффинного пространства
обрыв возрастающих цепей		обрыв убывающих цепей

5

Полиномиальные и рациональные функции на многообразии

Одна из идей, проходящих через всю современную математику, состоит в следующем: чтобы понять некоторый класс математических объектов, необходимо также изучить *отображения* между этими объектами и в особенности те из них, которые сохраняют некоторое исследуемое свойство объектов. Например, линейная алгебра изучает векторные пространства, но также и свойства *линейных отображений* векторных пространств, т. е. таких отображений, которые сохраняют операции сложения векторов и умножения вектора на скаляр.

В этой главе мы будем рассматривать отображения многообразий, в результате чего получим следующий раздел алгебро-геометрического «словаря», который мы начали создавать в гл. 4. Алгебраические свойства полиномиальных и рациональных функций на многообразии помогают понять геометрические свойства самого многообразия. Эта глава также является введением в теорию факторколец (и объяснением ее важности).

§ 1. Полиномиальные отображения

Изучение отображений многообразий мы начнем с рассмотрения двух примеров, с которыми уже встречались раньше. Напомним, что касательная поверхность скрученной кубики в $\mathbb{R}^3$ (§ 3 гл. 3) задается параметрически следующим образом:

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned} \tag{1}$$

На языке функций параметризация (1) задает отображение

$$\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$$

формулой

$$\phi(t, u) = (t + u, t^2 + 2tu, t^3 + 3t^2u). \tag{2}$$

Область определения этого отображения — аффинное многообразие $V = \mathbb{R}^2$, а образ — касательная поверхность S.

В § 3 гл. 3 было доказано, что S является аффинным многообразием $W = \mathbf{V}(x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2)$. Таким образом, наша параметризация определяет то, что мы будем называть *полиномиальным отображением многообразия* V в W. Слово «полиномиальный» здесь указывает на то, что компоненты отображения ϕ являются полиномами от t и u.

Далее, когда мы изучали (§ 2 гл. 3) исключение переменных из систем уравнений, то рассматривали отображение проекции

$$\pi_l : \mathbb{C}^n \longrightarrow \mathbb{C}^{n-l},$$

определенное формулой

$$\pi_l(a_1, \ldots, a_n) = (a_{l+1}, \ldots, a_n).$$

Если мы работаем с многообразием $V = \mathbf{V}(I) \subset \mathbb{C}^n$, то можем ограничить π_l на V. Тогда, как мы знаем, $\pi_l(V)$ содержится в аффинном многообразии $W = \mathbf{V}(I_l)$, где $I_l = I \cap \mathbb{C}[x_{l+1}, \ldots, x_n]$ есть l-й исключающий идеал идеала I. Таким образом, мы можем рассматривать π_l как отображение многообразий. В этом случае мы также можем в силу определения отображения π_l рассматривать его компоненты как полиномы от координат области определения.

Определение 1. Пусть $V \subset k^m$ и $W \subset k^n$ — многообразия. Функция $\phi : V \to W$ называется *полиномиальным* или *регулярным отображением*, если существуют полиномы $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$, такие, что

$$\phi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$$

для всех $(a_1, \ldots, a_m) \in V$. Мы будем говорить, что n-набор полиномов

$$(f_1, \ldots, f_n) \in (k[x_1, \ldots, x_m])^n$$

представляет ϕ.

Утверждение, что ϕ — полиномиальное отображение многообразия $V \subset k^m$ в многообразие $W \subset k^n$, представленное набором $(f_1, \ldots, f_n)$, означает, что полиномы, определяющие W, равны нулю в точках $(f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$ для всех $(a_1, \ldots, a_m) \in V$. Рассмотрим, например, многообразия $V = \mathbf{V}(y - x^2, z - x^3) \subset k^3$ (скрученная кубика) и $W = \mathbf{V}(y^3 - z^2) \subset k^2$. Проекция $\pi_1 : k^3 \to k^2, \pi_1(x, y, z) = (y, z)$, задает полиномиальное отображение $\pi_1 : V \to W$. В самом деле, каждая точка в $\pi_1(V) = \{(x^2, x^3) : x \in k\}$ удовлетворяет уравнению, определяющему W.

Случай $W = k$ особенно интересен. Здесь ϕ является скалярной полиномиальной функцией, заданной на многообразии V. Полиномиальные функции из V в k следует изучать, в частности, и потому, что общее полиномиальное отображение $\phi : V \to k^n$ построено из n полиномиальных функций $\phi_i : V \to k$ — компонент отображения ϕ. Другими словами, если мы изучим функции $\phi : V \to k$, то поймем, как строить отображения $\phi : V \to k^n$.

Рассмотрение полиномиальных функций мы начнем со следующего замечания: если $V \subset k^m$, то $\phi : V \to k$ по определению 1 является полиномиальной функцией, когда *существует* полином $f \in k[x_1, \ldots, x_m]$, представляющий ϕ. Обычно мы задаем полиномиальную функцию, явно указав полиномиальное представление. Таким образом, поиск представителя не вызывает трудностей. Но только в редких случаях полиномиальное представление определено однозначно. Рассмотрим, например, многообразие $V = (y - x^2) \subset \mathbb{R}^2$. Полином $f = x^3 + y^3$ представляет полиномиальную функцию из V в $\mathbb{R}$. Но $g = x^3 + y^3 + (y - x^2), h = x^3 + y^3 + (x^4 y - x^6)$ и $F = x^3 + y^3 + A(x, y)(y - x^2)$ для любого $A(x, y)$ определяют *ту же самую полиномиальную функцию* на V. В самом деле, если мы прибавим к f любой полином из $\mathbf{I}(V)$, то это не изменит значения f в точках из V. То же самое происходит и в общем случае.

Предложение 2. *Пусть $V \subset k^m$ — аффинное многообразие. Тогда*

(i) *f и $g \in k[x_1, \ldots, x_m]$ представляют одну и ту же полиномиальную функцию на V в том и только том случае, когда $f - g \in \mathbf{I}(V)$.*

(ii) *$(f_1, \ldots, f_n)$ и $(g_1, \ldots, g_n)$ представляют одно и то же полиномиальное отображение из V в k^n в том и только том случае, когда $f_i - g_i \in \mathbf{I}(V)$ для всех $i, 1 \leq i \leq n$.*

Доказательство. (i) Если $f - g = h \in \mathbf{I}(V)$, то $f(p) - g(p) = h(p) = 0$ для любой точки $p = (a_1, \ldots, a_m) \in V$. Следовательно, f и g представляют одну и ту же функцию на V. Обратно, если f и g представляют одну и ту же функцию на V, то $f(p) - g(p) = 0$ в каждой точке $p \in V$. Таким образом, $f - g \in \mathbf{I}(V)$. Пункт (ii) является прямым следствием п. (i). □

Другими словами, соответствие между полиномами из $k[x_1, \ldots, x_m]$ и полиномиальными функциями является взаимно однозначным только в случае $\mathbf{I}(V) = \{0\}$. В упр. 7 будет доказано, что если k бесконечно, то $\mathbf{I}(V) = \{0\}$ в том и только том случае, когда $V = k^m$.

Есть два способа справляться с неоднозначностью представления полиномиальных функций на многообразии:

- Грубо говоря, мы можем «собрать вместе» *все* полиномы $f \in k[x_1, \ldots, x_m]$, представляющие одну и ту же функцию на V, и объявить это множество «новым объектом». Тогда мы можем рассматривать такое множество полиномов как описание функции на V.
- С другой стороны, мы можем выбрать полином самого простого вида среди тех, которые представляют некоторую функцию на V, и работать только с этими «стандартными представителями».

Оба подхода имеют свои преимущества, и мы рассмотрим их подробно в следующих параграфах. А сейчас мы рассмотрим еще два примера, которые демонстрируют, какого типа свойства многообразий отражены в полиномиальных функциях.

Определение 3. Через $k[V]$ мы будем обозначать множество полиномиальных функций $\phi : V \to k$.

Так как k — поле, то можно определить сумму и произведение любых двух функций $\phi, \psi \in k[V]$, складывая и умножая их значения. Для любого $p \in V$

$$(\phi + \psi)(p) = \phi(p) + \psi(p),$$
$$(\phi \cdot \psi)(p) = \phi(p) \cdot \psi(p).$$

Более того, если мы выберем представители $f, g \in k[x_1, \ldots, x_m]$ для ϕ, ψ соответственно, то сумма $f + g$ представляет $\phi + \psi$ и произведение $f \cdot g$ представляет $\phi \cdot \psi$. Значит, $\phi + \psi$ и $\phi \cdot \psi$ являются полиномиальными функциями на V.

Таким образом, в $k[V]$ можно определить операции сложения и умножения, используя соответствующие операции в $k[x_1, \ldots, x_m]$. Все обычные свойства этих операций имеют место в $k[V]$. Следовательно, $k[V]$ является ***коммутативным кольцом*** (см. приложение A, где дано точное определение). Мы вернемся к этому вопросу в § 2.

Теперь мы готовы к выяснению того, что $k[V]$ может сказать нам о геометрии многообразия V. Напомним, что в § 5 гл. 4 многообразие $V \subset k^m$ было названо ***приводимым***, если оно может быть представлено в виде объединения двух непустых собственных подмногообразий: $V = V_1 \cup V_2$, где $V_1 \neq V$ и $V_2 \neq V$. Например, многообразие $V = \mathbf{V}(x^3 + xy^2 - xz, yx^2 + y^3 - yz) \subset k^3$ приводимо, потому что, разлагая на множители определяющие уравнения, мы получаем разложение $V = \mathbf{V}(x^2 + y^2 - z) \cup \mathbf{V}(x, y)$. Мы хотим показать, что такие геометрические свойства, как приводимость, могут

быть «вычитаны» из достаточно хорошего алгебраического описания кольца $k[V]$. Пусть, например,

$$f = x^2 + y^2 - z, \quad g = 2x^2 - 3y^4 z \in k[x, y, z], \tag{3}$$

и пусть ϕ и ψ — соответствующие элементы из $k[V]$.

Заметим, что ни ϕ, ни ψ не обращаются тождественно в нуль на V: $(0,0,5) \in V$, а $\phi(0,0,5) = f(0,0,5) = -5 \neq 0$. Аналогично, $(1,1,2) \in V$, а $\psi(1,1,2) = g(1,1,2) = -4 \neq 0$. Но произведение $\phi \cdot \psi$ этих функций равно нулю в каждой точке из V. Причина состоит в том, что

$$\begin{aligned} f \cdot g &= (x^2 + y^2 - z)(2x^2 - 3y^4 z) \\ &= 2x(x^3 + xy^2 - xz) - 3y^3 z(x^2 y + y^3 - yz) \\ &\in \langle x^3 + xy^2 - xz, x^2 y + y^3 - yz \rangle. \end{aligned}$$

Следовательно $f \cdot g \in \mathbf{I}(V)$; поэтому соответствующая полиномиальная функция $\phi \cdot \psi$ тождественно равна нулю на V.

Произведение двух ненулевых элементов поля или двух ненулевых полиномов из $k[x_1, \ldots, x_n]$ не может равняться нулю. В общем случае коммутативное кольцо R называется *областью целостности*, если из $a \cdot b = 0$ в R следует, что или $a = 0$, или $b = 0$. Таким образом, для нашего многообразия V кольцо $k[V]$ не является областью целостности. Более того, существование функций $\phi \neq 0$ и $\psi \neq 0$ в $k[V]$, таких, что $\phi \cdot \psi = 0$, является прямым следствием приводимости многообразия V: полином f в (3) равен нулю на $V_1 = \mathbf{V}(x^2 + y^2 - z)$, но не на $V_2 = \mathbf{V}(x, y)$; аналогично, g равен нулю на V_2, но не на V_1. Именно поэтому $f \cdot g = 0$ в каждой точке $V = V_1 \cup V_2$. Мы продемонстрировали наличие связи между геометрическими свойствами многообразия V и алгебраическими свойствами кольца $k[V]$.

В общем случае справедливо следующее утверждение.

Предложение 4. *Пусть $V \subset k^n$ — аффинное многообразие. Следующие утверждения эквивалентны:*

(i) *V неприводимо;*
(ii) *идеал $\mathbf{I}(V)$ прост;*
(iii) *$k[V]$ является областью целостности.*

Доказательство. (i)⇔(ii) — это предложение 3 из § 5 гл. 5.

Докажем, что (iii)⇒(i). Предположим, что $k[V]$ является областью целостности, но V приводимо. Это означает, согласно определению 1 § 5 гл. 5, что $V = V_1 \cup V_2$, где V_1 и V_2 — непустые собственные подмногообразия многообразия V. Рассмотрим полиномы $f_1, f_2 \in k[x_1, \ldots, x_n]$, такие, что f_1 равен нулю на V_1, но не обращается тождественно в нуль на V_2, а f_2 равен нулю на V_2, но не обращается тождественно в нуль на V_1. (Такие полиномы существуют, потому что V_1 не содержит V_2, а V_2 не содержит V_1.) Таким образом, ни f_1, ни f_2 не представляет нуль в $k[V]$. Однако $f_1 \cdot f_2$ обращается в нуль во всех точках из $V_1 \cup V_2 = V$. Следовательно, это произведение равно нулю в $k[V]$, что противоречит целостности кольца $k[V]$. Значит, V неприводимо.

Докажем, наконец, что (i)⇒(iii). Предположим, что $k[V]$ не является областью целостности. Тогда найдутся два полинома $f, g \in k[x_1, \ldots, x_n]$, такие, что ни f, ни g не равен нулю тождественно на V, но их произведение равно нулю в каждой точке из V. В упр. 9 будет доказано, что тогда существует разложение многообразия V в объединение подмногообразий:

$$V = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g)).$$

В упр. 9 также будет показано, что при этих предположениях $V \cap \mathbf{V}(f) \neq V$ и $V \cap \mathbf{V}(g) \neq V$. Это противоречит неприводимости многообразия V. □

Рассмотрим еще один пример, показывающий, какого рода информацию о многообразиях можно обнаружить, изучая полиномиальные отображения. Пусть многообразие $V \subset \mathbb{C}^3$ определено как пересечение трех квадрик:

$$\begin{aligned} x^2 + 2xz + 2y^2 + 3y &= 0, \\ xy + 2x + z &= 0, \\ xz + y^2 + 2y &= 0. \end{aligned} \tag{4}$$

Чтобы изучить многообразия V, мы находим базис Грёбнера идеала, порожденного полиномами (4), по отношению к lex-упорядочению с $y > z > x$. Этот базис состоит из двух полиномов

$$\begin{aligned} g_1 &= y - x^2, \\ g_2 &= z + x^3 + 2x. \end{aligned} \tag{5}$$

Геометрически это означает, что проекция многообразия V на ось x является отображением «на», так как полиномы (5) имеют постоянные старшие коэффициенты (§ 2 гл. 3). Более того, для каждого значения $x \in \mathbb{C}$ найдется ровно одно y и ровно одно z, такие, что $(x, y, z) \in V$.

Другими словами, существуют отображения

$$\begin{aligned} &\pi : V \longrightarrow \mathbb{C}, \quad (x, y, z) \mapsto x, \\ &\phi : \mathbb{C} \longrightarrow V, \quad x \mapsto (x, x^2, -x^3 - 2x). \end{aligned}$$

Отметим, что в силу (5) образ отображения ϕ принадлежит V. Очевидно, что и π, и ϕ являются полиномиальными отображениями.

Мы утверждаем, что эти отображения определяют взаимно однозначное соответствие между точками многообразия V и точками многообразия $\mathbb{C}$.

Утверждение будет доказано, если мы покажем, что π и ϕ взаимно обратны. Докажем сначала, что $\pi \circ \phi = \mathrm{id}_{\mathbb{C}}$. Это очевидно, так как

$$(\pi \circ \phi)(x) = \pi(x, x^2, -x^3 - 2x) = x.$$

С другой стороны, пусть $(x, y, z) \in V$; тогда

$$(\phi \circ \pi)(x, y, z) = (x, x^2, -x^3 - 2x).$$

Согласно (5), $y - x^2, z + x^3 + 2x \in \mathbf{I}(V)$. Значит, $\phi \circ \pi$ определяет *то же самое* отображение на V, что и $\mathrm{id}_V(x, y, z) = (x, y, z)$.

Из этих рассмотрений мы сделаем вывод, что $V \subset \mathbb{C}^3$ и $\mathbb{C}$ являются «изоморфными» многообразиями в том смысле, что существует полиномиальная биекция многообразия V на $\mathbb{C}$, причем обратное отображение также полиномиально. Хотя эти два многообразия определены разными уравнениями и лежат в различных объемлющих пространствах, они в некотором смысле «одинаковы». Кроме того, вычисление базиса Грёбнера (5) показывает, что $\mathbb{C}[V] = \mathbb{C}[x]$ в том смысле, что любой элемент $\psi \in \mathbb{C}[V]$ может быть однозначно преобразован подстановкой выражений для y и z из (5) в полином от x. Разумеется, если x используется как координата на многообразии $W = \mathbb{C}$, то, кроме того, $\mathbb{C}[W] = \mathbb{C}[x]$. Следовательно, множества полиномиальных функций на изоморфных многообразиях совпадают.

Итак, мы установили, что изучение множества полиномиальных функций на аффинном многообразии позволяет обнаружить его приводимость или неприводимость. Кроме того, структура кольца $k[V]$ содержит информацию, позволяющую приступить к *классификации* многообразий. Этой темы мы до сих пор не касались. Мы вернемся к этим вопросам позже, после того как рассмотрим различные методы анализа алгебраических свойств кольца $k[V]$.

Упражнения к § 1

1. Пусть V — скрученная кубика в $\mathbb{R}^3$, а $W = \mathbf{V}(v - u - u^2) \subset \mathbb{R}^2$. Докажите, что отображение $\phi(x, y, z) = (xy, z + x^2y^2)$ является полиномиальным отображением из V в W. Указание: воспользуйтесь параметризацией многообразия V.

2. Пусть $V = \mathbf{V}(y - x) \subset \mathbb{R}^2$, а $\phi : \mathbb{R}^2 \to \mathbb{R}^3$ — полиномиальное отображение, определяемое формулой $\phi(x, y) = (x^2 - y, y^2, x - 3y^2)$. Докажите, что образ многообразия V является аффинным многообразием в $\mathbb{R}^3$. Найдите систему уравнений, определяющую это многообразие.

3. Пусть $\phi : V \to k$ — полиномиальная функция. Ее *множеством уровня* называется множество

$$\phi^{-1}(c) = \{(a_1, \ldots, a_m) \in V : \phi(a_1, \ldots, a_m) = c\},$$

где $c \in k$ фиксировано. В этом упражнении мы рассмотрим, как множества уровня можно использовать в анализе и реконструкции многообразия. Пусть $k = \mathbb{R}$ и мы работаем с поверхностью

$$\mathbf{V}(x^2 - y^2z^2 + z^3) \subset \mathbb{R}^3.$$

   (a) Пусть $f(x, y, z) = z$ представляет полиномиальную функцию ϕ. Тогда образом функции ϕ является $\mathbb{R}$. Объясните, почему множество уровня $\phi^{-1}(c)$ для любого $c \in \mathbb{R}$ является аффинным многообразием, которое задается уравнениями

$$x^2 - y^2z^2 + z^3 = 0,$$
$$z - c = 0.$$

   (b) Исключите z из этих уравнений и найдите уравнение пересечения многообразия V с плоскостью $z = c$. Объясните, почему ваше уравнение определяет гиперболу на плоскости $z = c$ при $c \neq 0$ и ось y при $c = 0$. (Обратитесь к изображению многообразия V в § 3 гл. 1 и постарайтесь понять, как гиперболы лежат на V.)
   (c) Пусть полиномиальное отображение $\pi : V \to \mathbb{R}$ задано формулой $\pi(x, y, z) = x$. Геометрически опишите множества уровня $\pi^{-1}(c) \subset V$ для $c = -1, 0, 1$.
   (d) Решите ту же задачу для отображения $\sigma : V \to \mathbb{R}$, где $\sigma(x, y, z) = y$.
   (e) Постройте полиномиальное отображение $\psi : \mathbb{R} \to V$ и опишите его образ как подмногообразие в V.

4. Пусть $V = \mathbf{V}(z^2 - (x^2 + y^2 - 1)(4 - x^2 - y^2)) \subset \mathbb{R}^3$, а $\pi : V \to \mathbb{R}^2$ — вертикальная проекция $\pi(x, y, z) = (x, y)$.
   (a) Каково максимальное количество точек в множестве $\pi^{-1}(a, b)$, где $(a, b) \in \mathbb{R}^2$.
   (b) Каковы те множества $R \subset \mathbb{R}^2$, для которых множество $\pi^{-1}(a, b)$, $(a, b) \in \mathbb{R}$, состоит из двух точек, из одной точки, пусто?
   (c) Используя п. (b), нарисуйте V.

5. Докажите, что $\phi_1(x, y, z) = (2x^2 + y^2, z^3 - y^3 + 3xz)$ и $\phi_2(x, y, z) = (2y + xz, 3y^2)$ представляют одно и то же полиномиальное отображение скрученной кубики из $\mathbb{R}^3$ в $\mathbb{R}^2$.

6. Рассмотрим отображение $\phi : \mathbb{R}^2 \to \mathbb{R}^5$, где $\phi(u, v) = (u, v, u^2, uv, v^2)$.
   (a) Его образом является многообразие S, называемое поверхностью Веронезе. Найдите неявное представление для S.

(b) Докажите, что проекция $\pi : S \to \mathbb{R}^2$, $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2)$, обратна отображению ϕ: $\mathbb{R}^2 \to S$. Что этот факт говорит об S и $\mathbb{R}^2$?

7. В этой задаче мы опишем многообразия, для которых $\mathbf{I}(V) = \{0\}$.
   (a) Пусть поле k бесконечно и $V \subset k^n$ — многообразие. Тогда $\mathbf{I}(V) = \{0\}$ в том и только том случае, когда $V = k^n$.
   (b) Пусть теперь k конечно. Докажите, что в этом случае $\mathbf{I}(V)$ не может быть равно $\{0\}$. Указание: см. упр. 4 к § 1 гл. 1.

8. Пусть $V = \mathbf{V}(xy, xz) \subset \mathbb{R}^3$.
   (a) Докажите, что ни одна из двух функций $f = y^2 + z^3, g = x^2 - x$ не обращается тождественно в нуль на V, но их произведение *является* тождественным нулем на V.
   (b) Найдите $V_1 = V \cap \mathbf{V}(f)$ и $V_2 = V \cap \mathbf{V}(g)$ и докажите, что $V = V_1 \cup V_2$.

9. Пусть V — неприводимое многообразие и ϕ, ψ — функции из $k[V]$, представленные полиномами f, g соответственно. Пусть $\phi \cdot \psi = 0$ в $k[V]$, но ни ϕ, ни ψ не являются нулевыми функциями на V.
   (a) Докажите, что $V = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g))$.
   (b) Докажите, что $V \neq (V \cap \mathbf{V}(f))$ и $V \neq (V \cap \mathbf{V}(g))$, и выведите отсюда противоречие.

10. В этой задаче мы покажем, что не существует непостоянных полиномиальных отображений из $V = \mathbb{R}$ в $W = \mathbf{V}(y^2 - x^3 + x) \subset \mathbb{R}^2$. Таким образом, эти многообразия не изоморфны (т. е. они не «одинаковы» в том смысле, который обсуждался в тексте параграфа).
    (a) Пусть $\phi : \mathbb{R} \to W$ — полиномиальное отображение с представлением $\phi(t) = (a(t), b(t))$, где $a(t), b(t) \in \mathbb{R}[t]$. Докажите, что $b(t)^2 = a(t)(a(t)^2 - 1)$.
    (b) Объясните, почему два множителя в правой части равенства в п. (a) должны быть взаимно просты в $\mathbb{R}[t]$.
    (c) Используя однозначность разложения полиномов a и b на неприводимые множители, докажите, что $b^2 = ac^2$ для некоторого полинома $c(t) \in \mathbb{R}[t]$, причем c взаимно прост с a.
    (d) Из п. (c) вытекает, что $c^2 = a^2 - 1$. Докажите, что в этом случае c, a и, следовательно, b — константы.

§ 2. Факторкольца полиномиальных колец

Кольцо $k[V]$, построенное в § 1, является частным случаем так называемого факторкольца кольца $k[x_1, \ldots, x_n]$ по идеалу I. Переход к факторкольцу — это то «собирание» полиномов в один элемент, которое упоминалось в § 1, когда описывались элементы $\phi \in k[V]$. Переход к факторможеству — это одна из основополагающих конструкций в коммутативной алгебре и алгебраической геометрии.

Поэтому прежде чем двигаться дальше, мы ознакомимся с теорией факторколец.

Сначала дадим необходимые определения.

Определение 1. Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Полиномы $f, g \in k[x_1, \ldots, x_n]$ называются *сравнимыми по модулю* I, $f \equiv g \bmod I$, если $f - g \in I$.

Пусть, например, $I = \langle x^2 - y^2, x + y^3 + 1 \rangle \subset k[x, y]$. Тогда полиномы $f = x^4 - y^4 + x$ и $g = x + x^5 + x^4 y^3 + x^4$ сравнимы по модулю I, потому что

$$\begin{aligned} f - g &= x^4 - y^4 - x^5 - x^4 y^3 - x^4 \\ &= (x^2 + y^2)(x^2 - y^2) - (x^4)(x + y^3 + 1) \in I. \end{aligned}$$

Самое важное свойство отношения сравнимости описано в следующем предложении.

Предложение 2. *Пусть $I \subset k[x_1, \ldots, x_n]$ — идеал. Тогда сравнимость по модулю I является отношением эквивалентности на множестве $k[x_1, \ldots, x_n]$.*

Доказательство. Сравнимость по модулю I рефлексивна, так как $f - f = 0 \in I$ для всех $f \in k[x_1, \ldots, x_n]$. Докажем симметричность. Пусть $f \equiv g \bmod I$. Тогда $f - g \in I$, а значит, $g - f = (-1)(f - g) \in I$, т. е. $g \equiv f \bmod I$. Теперь докажем транзитивность. Пусть $f \equiv g \bmod I$ и $g \equiv h \bmod I$. Тогда $f - g \in I$ и $g - h \in I$. Но так как I замкнут относительно сложения, $f - g + g - h = f - h \in I$; следовательно, $f \equiv h \bmod I$. □

Отношение эквивалентности на множестве S разбивает это множество на непересекающиеся подмножества, которые называются классами эквивалентности. Для любого $f \in k[x_1, \ldots, x_n]$ его класс эквивалентности — это множество

$$[f] = \{g \in k[x_1, \ldots, x_n] : g \equiv f \bmod I\}.$$

Определение сравнимости по модулю I и предложение 2 справедливы *для любого* идеала $I \subset k[x_1, \ldots, x_n]$. В том частном случае, когда $I = \mathbf{I}(V)$, выражение $f \equiv g \bmod \mathbf{I}(V)$ в силу предложения 2 § 1 означает, что f и g определяют одну и ту же функцию на многообразии V. Другими словами, «собирание» полиномов, которые определяют одну и ту же функцию на V, осуществляется с помощью перехода к классам эквивалентности по отношению сравнимости по модулю $\mathbf{I}(V)$. Придадим этому замечанию строгую формулировку.

Предложение 3. *Множество попарно различных полиномиальных функций $\phi : V \to k$ находится во взаимно однозначном соответствии с множеством классов эквивалентности полиномов по отношению сравнимости по модулю $\mathbf{I}(V)$.*

Доказательство. Это утверждение есть следствие предложения 2 из § 1, и его (простое) доказательство мы оставляем читателю в качестве упражнения. □

Теперь мы готовы определить факторкольцо — предмет рассмотрения этого параграфа.

Определение 4. *Факторкольцом* $k[x_1, \ldots, x_n]/I$ кольца $k[x_1, \ldots, x_n]$ по идеалу I называется множество классов эквивалентности по отношению сравнимости по модулю I:

$$k[x_1, \ldots, x_n]/I = \{[f] : f \in k[x_1, \ldots, x_n]\}.$$

Пусть, например, $k = \mathbb{R}$, а $I = \langle x^2 - 2\rangle$. Существует ли способ описать все классы эквивалентности по модулю I? Используя алгоритм деления, любой полином $f \in \mathbb{R}[x]$ можно записать в виде $f = q \cdot (x^2 - 2) + r$, где $r = ax + b$, $a, b \in \mathbb{R}$. По определению $f \equiv r \bmod I$, так как $f - r = q \cdot (x^2 - 2) \in I$. Таким образом, любой полином из $\mathbb{R}[x]$ принадлежит единственному из классов эквивалентности вида $[ax + b]$, и $\mathbb{R}[x]/I = \{[ax + b] : a, b \in \mathbb{R}\}$. В § 3 мы обобщим использованную в этом примере идею на случай $k[x_1, \ldots, x_n]/I$ для произвольного идеала I.

Так как $k[x_1, \ldots, x_n]$ — это кольцо, можно попытаться определить операции сложения и умножения *для классов* $[f], [g] \in k[x_1, \ldots, x_n]/I$, используя соответствующие операции для полиномов. Другими словами, мы хотим, чтобы операции на классах выглядели так:

$$\begin{aligned} [f] + [g] &= [f + g] \quad (\text{сумма в } k[x_1, \ldots, x_n]/I), \\ [f] \cdot [g] &= [f \cdot g] \quad (\text{произведение в } k[x_1, \ldots, x_n]/I). \end{aligned} \tag{1}$$

Мы должны проверить корректность этих формул, т. е. должны доказать, что если мы выберем другие полиномы из этих же классов, $f' \in [f]$ и $g' \in [g]$, то класс $[f' + g']$ совпадет с классом $[f + g]$. Аналогично, мы должны доказать, что $[f' \cdot g'] = [f \cdot g]$.

Предложение 5. *Операции сложения и умножения классов* корректно определены *равенствами* (1), *т. е. класс* $[f' + g']$ *и класс* $[f' \cdot g']$ *не зависят от выбора полиномов* $f' \in [f]$ *и* $g' \in [g]$.

Доказательство. Пусть $f' \in [f]$ и $g' \in [g]$. Тогда $f' = f + a$ и $g' = g + b$, где $a, b \in I$. Имеем

$$f' + g' = (f + a) + (g + b) = (f + g) + (a + b).$$

Так как $a + b \in I$, то $f' + g' \equiv f + g \bmod I$; значит, $[f' + g'] = [f + g]$. Аналогично,

$$f' \cdot g' = (f + a) \cdot (g + b) = fg + ag + fb + ab.$$

Так как $ag + fb + ab \in I$, то $f' \cdot g' \equiv f \cdot g \bmod I$, а значит, $[f' \cdot g'] = [f \cdot g]$. □

В качестве примера рассмотрим операции сложения и умножения в факторкольце $\mathbb{R}[x]/\langle x^2 - 2\rangle$. Мы знаем, что классы $[ax + b]$, $a, b \in \mathbb{R}$, составляют полное множество элементов из $\mathbb{R}[x]/\langle x^2 - 2\rangle$. Сумма классов определяется формулой $[ax + b] + [cx + d] = [(a + c)x + (b + d)]$. Отметим, что это обычная векторная (покомпонентная) сумма упорядоченных пар вещественных чисел. Произведение классов также несложно определить:

$$\begin{aligned} [ax + b] \cdot [cx + d] &= [acx^2 + (ad + bc)x + bd] \\ &= [(ad + bc)x + (bd + 2ac)]. \end{aligned}$$

Для этого нужно полином второй степени в первой строчке равенства справа поделить на $x^2 - 2$ и найти остаток от деления.

Так как операции (1) определены корректно, то аксиомы коммутативного кольца выполнены в $k[x_1, \ldots, x_n]/I$, потому что операции на классах определены в терминах соответствующих операций в кольце $k[x_1, \ldots, x_n]$, где эти аксиомы выполнены. Например, чтобы доказать ассоциативность сложения в $k[x_1, \ldots, x_n]/I$, можно рассуждать следующим образом:

$$\begin{aligned} ([f] + [g]) + [h] &= [f + g] + [h] \\ &= [(f + g) + h] \ (\text{по (1)}) \\ &= [f + (g + h)] \ (\text{в силу ассоциативности кольца } k[x_1, \ldots, x_n]) \\ &= [f] + [g + h] \\ &= [f] + ([g] + [h]). \end{aligned}$$

Аналогично доказывается коммутативность сложения и умножения, ассоциативность умножения и законы дистрибутивности. Аддитивной единицей в $k[x_1, \ldots, x_n]/I$ является $[0]$, а мультипликативной служит $[1]$. Таким образом, мы дали набросок доказательства следующей теоремы.

Теорема 6. *Пусть I — идеал в $k[x_1, \ldots, x_n]$. Тогда факторкольцо $k[x_1, \ldots, x_n]/I$ является коммутативным кольцом, операции в котором заданы равенствами* (1).

Пусть теперь дано многообразие V. Что можно сказать о связи между факторкольцом $k[x_1, \ldots, x_n]/\mathbf{I}(V)$ и кольцом $k[V]$ полиномиальных функций на V? Оказывается эти кольца «одинаковы» в следующем смысле.

Теорема 7. *Взаимно однозначное соответствие между элементами кольца $k[V]$ и элементами кольца $k[x_1,\dots,x_n]/\mathbf{I}(V)$, определенное в предложении 3, сохраняет суммы и произведения.*

Доказательство. Определим отображение $\Phi : k[x_1,\dots,x_n]/\mathbf{I}(V) \to k[V]$ следующим образом: $\Phi([f]) = \phi$, где ϕ — полиномиальная функция, представленная полиномом f. Так как каждый элемент из $k[V]$ представлен некоторым полиномом, то Φ — это отображение «на». Докажем его инъективность. Пусть $\Phi([f]) = \Phi([g])$. По предложению 3 тогда $f \equiv g \bmod \mathbf{I}(V)$; следовательно, $[f] = [g]$ в $[x_1,\dots,x_n]/\mathbf{I}(V)$.

Рассмотрим теперь суммы и произведения. Пусть $[f],[g] \in k[x_1,\dots,x_n]/\mathbf{I}(V)$. Тогда $\Phi([f]+[g]) = \Phi([f+g])$ по определению суммы в факторкольце. Если f представляет полиномиальную функцию ϕ, а g представляет ψ, то $f+g$ представляет $\phi+\psi$. Следовательно,

$$\Phi([f+g]) = \phi + \psi = \Phi([f]) + \Phi([g]).$$

Таким образом, Φ сохраняет суммы. Аналогично,

$$\Phi([f]\cdot[g]) = \Phi([f\cdot g]) = \phi\cdot\psi = \Phi([f])\cdot\Phi([g]),$$

т. е. Φ сохраняет также произведения. Аналогичные рассуждения показывают, что обратное соответствие Ψ также сохраняет суммы и произведения. Теорема доказана. □

Теорема 7 иллюстрирует одно из основных понятий общей алгебры. Следующее определение объясняет, что значит, что два кольца в сущности одинаковы.

Определение 8. Пусть R, S — коммутативные кольца.

(i) Отображение $\phi : R \to S$ называется *кольцевым изоморфизмом*, если
   (a) ϕ сохраняет суммы, т. е. $\phi(r+r') = \phi(r) + \phi(r')$ для всех $r, r' \in R$;
   (b) ϕ сохраняет произведения, т. е. $\phi(r\cdot r') = \phi(r)\cdot\phi(r')$ для всех $r, r' \in R$;
   (c) ϕ является инъективным отображением «на».

(ii) Кольца R, S называются *изоморфными*, если существует изоморфизм $\phi : R \to S$. Если R изоморфно S, то мы будем писать $R \cong S$.

(iii) Отображение $\phi : R \to S$ называется *кольцевым гомоморфизмом*[1)], если ϕ удовлетворяет условиям (a) и (b) п. (i), но не обязательно условию (c) и, кроме того, переводит мультипликативную единицу $1 \in R$ в мультипликативную единицу $1 \in S$.

[1)] Читатель легко проверит, что кольцевой изоморфизм является кольцевым гомоморфизмом (см. упр. 8). — *Прим. ред.*

Вообще, «гомоморфизм» — это отображение, сохраняющее алгебраическую структуру. Кольцевой гомоморфизм $\phi : R \to S$ сохраняет операции сложения и умножения в кольце R.

Таким образом, теорема 7 определяет кольцевой изоморфизм $k[V] \cong k[x_1,\dots,x_n]/\mathbf{I}(V)$. Можно спросить, а что получится, если мы заменим идеал $\mathbf{I}(V)$ каким-либо другим идеалом, определяющим V? (Из гл. 4 мы знаем, что существует *много* идеалов I, таких, что $\mathbf{V}(I) = V$.) Верно ли, что *все* факторкольца $k[x_1,\dots,x_n]/I$ изоморфны $k[V]$? Следующий пример показывает, что ответ отрицательный. Пусть $V = \{(0,0)\}$. В § 4 гл. 1 было показано, что $\mathbf{I}(V) = \mathbf{I}(\{(0,0)\}) = \langle x, y\rangle$. Из теоремы 7 следует, что $k[x,y]/\mathbf{I}(V) \cong k[V]$.

Прежде всего, отметим, что $k[x,y]/\mathbf{I}(V) \cong k$, потому что полиномиальная функция на множестве, состоящем из одной точки $\{(0,0)\}$, может быть представлена константой, так как ее множество значений состоит из одного числа. Мы можем также доказать это утверждение алгебраически, построив отображение

$$\Phi : k[x,y]/\mathbf{I}(V) \longrightarrow k,$$

где $\Phi([f]) = f(0,0)$ (постоянный член полинома). Доказательство того, что Φ является кольцевым изоморфизмом, мы оставляем читателю.

Пусть теперь $I = \langle x^3 + y^2, 3y^4\rangle \subset k[x,y]$. Легко проверить, что $\mathbf{V}(I) = \{(0,0)\} = V$. Верно ли, что $k[x,y]/I \cong k$? Чтобы убедиться, что неверно, рассмотрим класс $[y] \in k[x,y]/I$. Отметим, что $y \notin I$ (это легко проверить, построив базис Грёбнера идеала I, используя упорядочение, и вычислив остаток). Значит, $[y] \neq [0]$ в кольце $k[x,y]/I$. Но $[y]^4 = [y^4] = [0]$, так как $y^4 \in I$. Таким образом, в $k[x,y]/I$ существует ненулевой элемент, четвертая степень которого равна нулю. Но в поле такой элемент существовать не может. Следовательно, $k[x,y]/I$ не является полем. Значит, кольца $k[x,y]/\mathbf{I}(V)$ и $k[x,y]/I$ не изоморфны, потому что одно из них является полем, а другое — нет. (См. также упр. 8.)

Элемент a в коммутативном кольце R называется *нильпотентным элементом*, если $a^n = 0$ для некоторого $n \geq 1$. Только что разобранный пример достаточно точно показывает, что происходит, когда мы сравниваем факторкольца $k[x_1,\dots,x_n]/\mathbf{I}(V)$ и $k[x_1,\dots,x_n]/I$, где I — некоторый другой идеал, такой, что $\mathbf{V}(I) = V$. Если I не радикален, то существует полином $f \in \sqrt{I}$, такой, что $f \notin I$. Тогда $[f] \neq [0]$ в $k[x_1,\dots,x_n]/I$, но $[f]^n = [0]$, так как $f^n \in I$ для некоторого $n > 1$. Факторкольцо $k[x_1,\dots,x_n]/I$ *будет* иметь

ненулевые нильпотентные элементы, в то время как факторкольцо $k[x_1,\dots,x_n]/\mathbf{I}(V)$ их иметь не может: $\mathbf{I}(V)$ является радикальным идеалом и потому $[f]^n = 0$ в том и только том случае, когда $[f] = 0$.

Так как факторкольцо $k[x_1,\dots,x_n]/I$ само является коммутативным кольцом, мы можем изучать также другие грани его кольцевой структуры, в частности, изучать идеалы в $k[x_1,\dots,x_n]/I$. Идеал в коммутативном кольце определяется так же, как в кольце полиномов.

Определение 9. Подмножество I коммутативного кольца R называется *идеалом*, если

(i) $0 \in I$, где 0 — нулевой элемент кольца R;
(ii) если $a, b \in I$, то $a + b \in I$;
(iii) если $a \in I$, а $r \in R$, то $r \cdot a \in I$.

Между идеалами в факторкольце $k[x_1,\dots,x_n]/I$ и идеалами в кольце $k[x_1,\dots,x_n]$ существует тесная связь.

Предложение 10. *Пусть I — идеал в $k[x_1,\dots,x_n]$. Тогда идеалы в факторкольце $k[x_1,\dots,x_n]/I$ находятся во взаимно однозначном соответствии с идеалами в $k[x_1,\dots,x_n]$, содержащими I (т. е. с идеалами J, такими, что $I \subset J \subset k[x_1,\dots,x_n]$).*

Доказательство. Сначала покажем, как построить идеал в $k[x_1,\dots,x_n]/I$, соответствующий идеалу J, $I \subset J \subset k[x_1,\dots,x_n]$. Если идеал J содержит I, то через J/I будет обозначаться множество $\{[j] \in k[x_1,\dots,x_n]/I : j \in J\}$. Мы утверждаем, что J/I является идеалом в $k[x_1,\dots,x_n]/I$. Докажем это. Прежде всего, $[0] \in J/I$, так как $0 \in J$. Далее, пусть $[j], [h] \in J/I$; тогда $[j] + [h] = [j + h]$ по определению суммы в факторкольце. Так как $j + h \in J$, то $[j] + [h] \in J/I$. Наконец, если $[j] \in J/I$ и $[r] \in k[x_1,\dots,x_n]/I$, то $[r] \cdot [j] = [r \cdot j]$ по определению умножения в факторкольце. Так как $r \cdot j \in J$ в силу того, что J — идеал, то $[r] \cdot [j] \in J/I$. Таким образом, J/I — идеал в $k[x_1,\dots,x_n]/I$.

Пусть теперь $\widetilde{J} \subset k[x_1,\dots,x_n]/I$ — некоторый идеал. Мы сейчас покажем, как построить по $\widetilde{J}$ идеал J в $k[x_1,\dots,x_n]$, содержащий I. Пусть $J = \{j \in k[x_1,\dots,x_n] : [j] \in \widetilde{J}\}$. Имеем $I \subset J$, так как $[i] = [0] \in \widetilde{J}$ для любого $i \in I$. Осталось показать, что J — идеал. Во-первых, $0 \in I \subset J$. Далее, если $j, h \in J$, то $[j], [h] \in \widetilde{J}$. Тогда $[j] + [h] = [j + h] \in \widetilde{J}$. Следовательно, $j + h \in J$. Наконец, пусть $j \in J$ и $r \in k[x_1,\dots,x_n]$. Тогда $[j] \in \widetilde{J}$ и потому $[r][j] = [rj] \in \widetilde{J}$. Следовательно, $rj \in J$, т. е. J — идеал в $k[x_1,\dots,x_n]$.

Мы доказали, таким образом, что существует соответствие между двумя множествами идеалов:

$$\begin{array}{ccc} \{J : I \subset J \subset k[x_1,\dots,x_n]\} & & \{\widetilde{J} \subset k[x_1,\dots,x_n]/I\} \\ J & \longrightarrow & J/I = \{[j] : j \in J\} \\ J = \{j : [j] \in \widetilde{J}\} & \longleftarrow & \widetilde{J}. \end{array} \tag{2}$$

Доказательство того факта, что отображения, показанные стрелками, взаимно обратны, мы оставляем читателю в качестве упражнения. Это показывает, что установленное соответствие взаимно однозначно. □

Рассмотрим, например, идеал $I = \langle x^2 - 4x + 3\rangle \subset R = \mathbb{R}[x]$. Мы знаем, что R является областью главных идеалов (см. гл. 1), т. е. каждый идеал в R порожден одним полиномом. Идеалы, содержащие I, — это в точности те идеалы, образующие которых *делят* $x^2 - 4x + 3$. Следовательно, факторкольцо R/I содержит в точности четыре идеала:

идеалы в R/I	идеалы в R, содержащие I
$\{[0]\}$,	I,
$\langle [x-1]\rangle$,	$\langle x-1\rangle$,
$\langle [x-3]\rangle$,	$\langle x-3\rangle$,
R/I,	R.

Как в уже разобранном ранее примере, мы можем описать операции в R/I, вычисляя остатки от деления на $x^2 - 4x + 3$.

Следствием предложения 10 является утверждение об идеалах в факторкольцах, аналогичное теореме Гильберта о базисе (гл. 2).

Следствие 11. *Каждый идеал в факторкольце $k[x_1,\dots,x_n]/I$ конечно порожден.*

Доказательство. Пусть $\widetilde{J}$ — некоторый идеал в $k[x_1,\dots,x_n]/I$. По предложению 10 существует идеал $J \subset k[x_1,\dots,x_n]$, такой, что $I \subset J$ и $\widetilde{J} = \{[j] : j \in J\}$. По теореме Гильберта о базисе идеал J конечно порожден, $J = \langle f_1,\dots,f_s\rangle$. Значит, любой элемент $j \in J$ может быть представлен в виде $j = h_1 f_1 + \dots + h_s f_s$, где $h_i \in k[x_1,\dots,x_n]$. Тогда

$$[j] = [h_1 f_1 + \dots + h_s f_s] = [h_1][f_1] + \dots + [h_s][f_s].$$

Таким образом, классы $[f_1],\dots,[f_s]$ порождают идеал $\widetilde{J}$ в $k[x_1,\dots,x_n]/I$. □

В следующем параграфе мы обсудим более конструктивный метод изучения факторколец $k[x_1,\dots,x_n]/I$ и их алгебраических свойств.

Упражнения к § 2

1. Пусть $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$. Используя методы гл. 2, опишите алгоритм, позволяющий выяснить, справедливо ли соотношение $f \equiv g \bmod I$.
2. Докажите предложение 3.
3. Докажите теорему 6, т. е. докажите, что в $k[x_1, \ldots, x_n]/I$ выполнены аксиомы коммутативного кольца.
4. В этом упражнении мы приведем алгебраическое построение поля, содержащего $\mathbb{Q}$, в котором число 2 является полным квадратом. Наше построение не использует *предельного перехода*, необходимого для придания смысла бесконечному десятичному представлению типа $\sqrt{2} = 1.414\ldots$. Вместо этого мы будем работать с полиномом $x^2 - 2$.
   (a) Докажите, что любой полином $f \in \mathbb{Q}[x]$ сравним по модулю идеала $I = \langle x^2 - 2 \rangle \subset \mathbb{Q}[x]$ с единственным полиномом вида $ax + b$, где $a, b \in \mathbb{Q}$.
   (b) Докажите, что класс $[x]$ в $\mathbb{Q}[x]/I$ является квадратным корнем из 2 в том смысле, что $[x]^2 = [2]$.
   (c) Докажите, что $F = \mathbb{Q}[x]/I$ является полем. Указание: по теореме 6 F является коммутативным кольцом; следовательно, осталось доказать, что каждый ненулевой элемент из F имеет мультипликативный обратный по умножению в F.
   (d) Найдите подполе в F, изоморфное $\mathbb{Q}$.
5. В этом упражнении мы рассмотрим операции сложения и умножения в факторкольце $\mathbb{R}/\langle x^2 + 1 \rangle$.
   (a) Докажите, что каждый полином $f \in \mathbb{R}[x]$ сравним по модулю $I = \langle x^2 + 1 \rangle$ с единственным полиномом вида $ax + b$, где $a, b \in \mathbb{R}$.
   (b) Найдите формулы для сложения и умножения в $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, используя полиномы $ax + b$ как стандартные представители классов.
   (c) Есть ли другой способ описать кольцо $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ (т. е. существует ли хорошо известное кольцо, изоморфное ему)? Указание: чему равен $[x]^2$?
6. Докажите, что факторкольцо $\mathbb{R}[x]/\langle x^2 - 4x + 3 \rangle$ не является областью целостности.
7. Для любого коммутативного кольца R и любого идеала I в нем можно определить факторкольцо R/I. Факторкольцо строится точно так же, как и факторкольцо $k[x_1, \ldots, x_n]/I$. Вот простой пример.
   (a) Пусть $I = \langle p \rangle \subset R = \mathbb{Z}$, где p — простое число. Докажите, что сравнимость по модулю p, задаваемая правилом

$$m \equiv n \bmod p \iff p \text{ делит } m - n,$$

   является отношением эквивалентности на $\mathbb{Z}$, и опишите его классы эквивалентности. Множество этих классов эквивалентности мы будем обозначать $\mathbb{Z}/\langle p \rangle$.

   (b) Постройте операции сложения и умножения в $\mathbb{Z}/\langle p \rangle$ по аналогии с равенствами (1) и, используя технику предложения 5, докажите, что они корректно определены.
   (c) Докажите, что $\mathbb{Z}/\langle p \rangle$ является коммутативным кольцом относительно операций из п. (b).
   (d) Докажите, что конечное поле $\mathbb{F}_p$, определенное в гл. 1, изоморфно (как кольцо) $\mathbb{Z}/\langle p \rangle$.
8. В этом упражнении мы рассмотрим образы мультипликативных обратных при гомоморфизмах колец.
   (a) Докажите, что любой кольцевой изоморфизм $\phi : R \to S$ переводит мультипликативную единицу в R в мультипликативную единицу в S, т. е. $\phi(1) = 1$.
   (b) Пусть элемент $r \in R$ имеет мультипликативный обратный. Докажите, что $\phi(r^{-1})$ является мультипликативным обратным для элемента $\phi(r)$, где $\phi : R \to S$ — кольцевой гомоморфизм.
   (c) Пусть R и S — изоморфные кольца и, кроме того, R является полем. Докажите, что S также является полем.
9. Докажите, что отображение $f \mapsto f(0, 0)$ задает кольцевой изоморфизм $k[x, y]/\langle x, y \rangle \cong k$. Указание: воспользуйтесь упр. 16.
10. В этом упражнении мы рассмотрим одно важное свойство нильпотентных элементов в кольцах. Пусть $R = k[x]$ и $I = \langle x^2 \rangle$.
    (a) Докажите, что $[x]$ является нильпотентным элементом в R/I, и найдите наименьшую степень элемента $[x]$, равную нулю.
    (b) Докажите, что каждый класс в R/I имеет единственный представитель вида $b + a\epsilon$, где $a, b \in k$, а через ϵ мы обозначили $[x]$.
    (c) Зафиксировав $b + a\epsilon \in R/I$, мы можем определить отображение $R \to R/I$, заменяя x на $b + a\epsilon$ в каждом полиноме $f(x) \in R$. Например, если $b + a\epsilon = 2 + \epsilon$ и $f(x) = x^2$, то $x^2 \to (2 + \epsilon)^2 = 4 + 4\epsilon + \epsilon^2 = 4 + 4\epsilon$. Докажите, что

$$f(b + a\epsilon) = f(b) + a \cdot f'(b)\epsilon, \tag{3}$$

    где f' — формальная производная полинома f (т. е. производная, построенная чисто алгебраическим путем).
    (d) Пусть $\epsilon = [x] \in k[x]/\langle x^3 \rangle$. Найдите формулу для $f(b + a\epsilon)$, аналогичную формуле (3).
11. Пусть R — коммутативное кольцо. Докажите, что множество всех нильпотентных элементов в R образует идеал. Указание: чтобы доказать, что сумма двух нильпотентных элементов также нильпотентна, нужно рассмотреть подходящую степень $(a + b)^k$ и воспользоваться формулой бинома.
12. В этом упражнении мы докажем, что отображения в (2) обратны друг другу.

(a) Пусть J — идеал в $k[x_1,\dots,x_n]$ и $I \subset J$. Докажите, что $J = \{f \in k[x_1,\dots,x_n] : [f] \in J/I\}$, где $J/I = \{[j] : j \in J\}$. Объясните, где доказательство использует включение $I \subset J$.

(b) Пусть $\widetilde{J}$ — идеал в $k[x_1,\dots,x_n]/I$. Докажите, что $\widetilde{J} = \{[f] \in k[x_1,\dots,x_n]/I : f \in J\}$, где $J = \{j : [j] \in \widetilde{J}\}$.

13. Пусть R и S — коммутативные кольца и $\phi : R \to S$ — кольцевой гомоморфизм.
(a) Докажите, что $\phi^{-1}(J)$ является идеалом в R, если J — идеал в S.
(b) Пусть ϕ — изоморфизм колец. Докажите, что существует взаимно однозначное сохраняющее включение соответствие между множеством идеалов в S и множеством идеалов в R.

14. В этом упражнении мы рассмотрим идеалы в некоторых факторкольцах.
(a) Пусть $I = \langle x^3 - x\rangle \subset R = \mathbb{R}[x]$. Найдите все идеалы факторкольца R/I, используя предложение 10. Нарисуйте диаграмму, иллюстрирующую включения идеалов.
(b) Как изменится ваш ответ, если $I = \langle x^3 + x\rangle$?

15. В этом упражнении мы рассмотрим некоторые факторкольца $\mathbb{R}[x,y]/I$.
(a) Пусть $I = \langle x^2, y^2\rangle \subset \mathbb{R}[x,y]$. Опишите идеалы в $\mathbb{R}[x,y]/I$. Указание: воспользуйтесь предложением 10.
(b) Верно ли, что $\mathbb{R}[x,y]/\langle x^3, y\rangle$ изоморфно $\mathbb{R}[x,y]/\langle x^2, y^2\rangle$?

16. Пусть $\phi : k[x_1,\dots,x_n] \to S$ — гомоморфизм колец. Множество $\{r \in k[x_1,\dots,x_n] : \phi(r) = 0 \in S\}$ называется *ядром* гомоморфизма ϕ и обозначается $\ker(\phi)$.
(a) Докажите, что $\ker(\phi)$ является идеалом в $k[x_1,\dots,x_n]$.
(b) Докажите, что отображение v из $k[x_1,\dots,x_n]/\ker(\phi)$ в S, определенное формулой $v([r]) = \phi(r)$, корректно определено в том смысле, что $v([r]) = v([r'])$, если $r \equiv r' \bmod \ker(\phi)$.
(c) Докажите, что v является кольцевым гомоморфизмом.
(d) (Теорема об изоморфизме) Предположим, что ϕ является отображением «на». Докажите, что v является взаимно однозначным отображением кольца $k[x_1,\dots,x_n]/\ker(\phi)$ на S, т. е. $S \cong k[x_1,\dots,x_n]/\ker(\phi)$, если ϕ является отображением «на».

17. Используя упр. 16, дайте краткое доказательство теоремы 7. Рассмотрите отображение $\phi : k[x_1,\dots,x_n] \to k[V]$, которое переводит полином в элемент из $k[V]$, который этот полином представляет. Указание: что является его ядром?

§ 3. Алгоритмические вычисления в $k[x_1,\dots,x_n]/I$

В этом параграфе, используя алгоритм деления, мы найдем простые представители классов эквивалентности по модулю идеала $I \subset k[x_1,\dots,x_n]$. Знание этих представителей позволит нам разработать явный метод вычисления сумм и произведений в факторкольце $k[x_1,\dots,x_n]/I$. Кроме того, мы получим простой критерий *конечности числа решений* полиномиальной системы над $\mathbb{C}$.

Основная идея состоит в том, что остаток от деления полинома f на *базис Грёбнера* G идеала I определен однозначно (предложение 1 из § 6 гл. 2). Следующие важные утверждения интерпретируют результаты деления и вид остатка в терминах факторколец.

Предложение 1. *Зафиксируем мономиальное упорядочение в* $k[x_1,\dots,x_n]$. *Пусть* I — *идеал в* $k[x_1,\dots,x_n]$. *Через* $\langle \mathrm{LT}(I)\rangle$ *мы будем обозначать (как и в* § 5 *гл.* 2) *идеал, порожденный старшими членами полиномов из* I.

(i) *Каждый полином* $f \in k[x_1,\dots,x_n]$ *сравним по модулю* I *с единственным полиномом* r, *который является* k-*линейной комбинацией мономов из дополнения к* $\langle \mathrm{LT}(I)\rangle$.

(ii) *Элементы* $\{x^\alpha : x^\alpha \notin \langle \mathrm{LT}(I)\rangle\}$ *«линейно независимы по модулю* I», *т. е. если*

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \bmod I,$$

где x^α *принадлежат дополнению* $\langle \mathrm{LT}(I)\rangle$, *то* $c_\alpha = 0$ *для всех* α.

Доказательство. (i) Пусть G — базис Грёбнера идеала I и $f \in k[x_1,\dots,x_n]$. Тогда $f = q + r$, где $q \in I$, а $r = \bar{f}^G$ — остаток от деления. Таким образом, $f - r = q \in I$, т. е. $f \equiv r \bmod I$. Алгоритм деления вычисляет остаток так, что r есть k-линейная комбинация мономов $x^\alpha \notin \langle \mathrm{LT}(I)\rangle$. Единственность остатка r доказана в предложении 1 из § 6 гл. 2.

(ii) Доказательство этого пункта аналогично доказательству единственности остатка в предложении 1 из § 6 гл. 2. Детали мы оставляем читателю. □

Исторически именно это и было первым применением базисов Грёбнера. Диссертация Бухбергера была посвящена нахождению «стандартного множества представителей» классов в факторкольце. Заметим также, что если $I = \mathbf{I}(V)$ для некоторого многообразия V, то в предложении 1 определены и стандартные представители полиномиальных функций $\phi \in k[V]$.

Пример 2. Пусть $I = \langle xy^3 - x^2, x^3y^2 - y\rangle \subset \mathbb{R}[x,y]$ и используется grlex-упорядочение. Тогда

$$G = \{x^3y^2 - y, x^4 - y^2, xy^3 - x^2, y^4 - xy\}$$

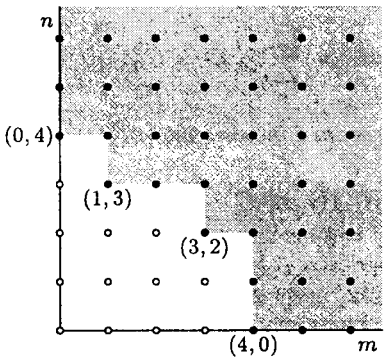
является базисом Грёбнера идеала I. Следовательно, $\langle \mathrm{LT}(I)\rangle = \langle x^3y^2, x^4, xy^3, y^4\rangle$. Как в § 4 гл. 2, построим диаграмму в $\mathbb{Z}^2_{\geq 0}$, на которой представлены векторы — показатели степеней мономов из $\langle \mathrm{LT}(I)\rangle$ и дополнения к $\langle \mathrm{LT}(I)\rangle$. А именно, векторы

$$\begin{aligned}\alpha(1) &= (3,2),\\ \alpha(2) &= (4,0),\\ \alpha(3) &= (1,3),\\ \alpha(4) &= (0,4)\end{aligned}$$

являются векторами — показателями степеней порождающих элементов идеала $\langle \mathrm{LT}(I)\rangle$. Таким образом, множество

$$((3,2) + \mathbb{Z}^2_{\geq 0}) \cup ((4,0) + \mathbb{Z}^2_{\geq 0}) \cup ((1,3) + \mathbb{Z}^2_{\geq 0}) \cup ((0,4) + \mathbb{Z}^2_{\geq 0})$$

и есть множество показателей степеней мономов из $\langle \mathrm{LT}(I)\rangle$. Это множество состоит из точек целочисленной решетки, лежащих в выделенной области на рисунке:



$(m,n) \leftrightarrow x^m y^n$

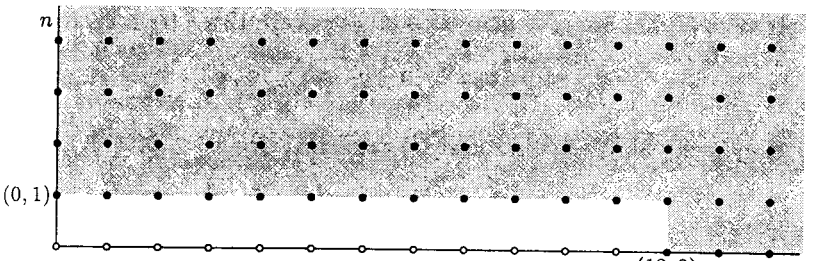
Мы видим, что для заданного $f \in \mathbb{R}[x,y]$ остаток $\bar{f}^G$ является $\mathbb{R}$-линейной комбинацией 12 мономов $1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^3$, которые *не содержатся* в выделенной области в силу предложения 1. Отметим, что в этом случае все остатки принадлежат конечномерному векторному подпространству в $\mathbb{R}[x,y]$.

Можно спросить, а что же случится, если используется другое мономиальное упорядочение. Если мы используем lex- вместо grlex-упорядочения с $y > x$, то базис Грёбнера G в этом случае состоит

из двух полиномов:

$$G = \{y - x^7, x^{12} - x^2\}.$$

Следовательно, $\langle \mathrm{LT}(I)\rangle = \langle y, x^{12}\rangle$ и $\langle \mathrm{LT}(I)\rangle$ содержит все мономы, показатели степеней которых принадлежат выделенной области на рисунке ниже. Таким образом, $\bar{f}^G$ является линейной комбинацией мономов $\{1, x, x^2, \ldots, x^{11}\}$ для любого $f \in \mathbb{R}[x,y]$.



$(m,n) \leftrightarrow x^m y^n$

Обратите внимание, что $\langle \mathrm{LT}(I)\rangle$ и остатки меняются при переходе к другому упорядочению. В обоих случаях, однако, остатки принадлежат 12-мерному пространству. Как мы вскоре увидим, эти пространства имеют одну размерность не случайно. Для данного идеала I *число* мономов в дополнении к $\langle \mathrm{LT}(I)\rangle$ не зависит от используемого упорядочения (в том случае, если это число конечно).

Пример 3. В примере 2 в дополнении к $\langle \mathrm{LT}(I)\rangle$ содержится только конечное число мономов. На самом деле это особый случай. Рассмотрим, например, идеал $I = \langle x - z^2, y - z^3\rangle \subset k[x,y,z]$. В случае lex-упорядочения указанные порождающие элементы образуют также и базис Грёбнера, т. е. $\langle \mathrm{LT}(I)\rangle = \langle x, y\rangle$. Множество остатков по модулю I — это множество k-линейных комбинаций степеней z. Идеал I в этом случае является идеалом скрученной кубики в k^3. Отсюда следует по предложению 1, что каждая полиномиальная функция на скрученной кубике может быть однозначно представлена полиномом из $k[z]$. Значит, пространство остатков бесконечномерно и $\mathbf{V}(I)$ — это кривая. Что можно сказать о $\mathbf{V}(I)$ для I из примера 2?

В любом случае мы можем использовать предложение 1 для частичного описания алгебраической структуры факторкольца $k[x_1, \ldots, x_n]/I$.

Предложение 4. *Пусть I — идеал в $k[x_1, \ldots, x_n]$. Тогда факторкольцо $k[x_1, \ldots, x_n]/I$ как векторное пространство изоморфно пространству $S = \mathrm{Span}(x^\alpha : x^\alpha \notin \langle \mathrm{LT}(I)\rangle)$ (где* Span *обозначает линейную оболочку).*

Доказательство. По предложению 1 отображение $\Phi : k[x_1, \ldots, x_n]/I \to S$, определенное формулой $\Phi[f] = \bar{f}^G$, устанавливает взаимно однозначное соответствие между классами эквивалентности в $k[x_1, \ldots, x_n]/I$ и элементами из S. Осталось доказать, что Φ линейно. Рассмотрим операцию сложения в $k[x_1, \ldots, x_n]/I$, определенную в § 2. Пусть $[f], [g] \in k[x_1, \ldots, x_n]/I$. По предложению 1 определены «стандартные» представители — остатки от деления на базис Грёбнера G. Так как $\overline{f+g}^G = \bar{f}^G + \bar{g}^G$ (см. упр. 12 к § 6 гл. 2), то если

$$\bar{f}^G = \sum_\alpha c_\alpha x^\alpha \quad \text{и} \quad \bar{g}^G = \sum_\alpha d_\alpha x^\alpha$$

(где суммирование происходит по таким α, что $x^\alpha \notin \langle \mathrm{LT}(I) \rangle$), то

$$\overline{f+g}^G = \sum_\alpha (c_\alpha + d_\alpha) x^\alpha. \tag{1}$$

Таким образом, для стандартных представителей операция сложения в $[x_1, \ldots, x_n]/I$ совпадает с операцией сложения в k-векторном пространстве $S = \mathrm{Span}(x^\alpha : x^\alpha \notin \langle \mathrm{LT}(I) \rangle)$. Далее, мы оставляем читателю в качестве упражнения доказательство того, что если $c \in k$, то $\overline{c \cdot f}^G = c \cdot \bar{f}^G$ (это следствие единственности, доказанной в предложении 1). Тогда

$$\overline{c \cdot f}^G = \sum_\alpha c c_\alpha x^\alpha.$$

Значит, умножение на c в $k[x_1, \ldots, x_n]/I$ совпадает со скалярным умножением в S. Поэтому отображение Φ линейно и является изоморфизмом векторных пространств. □

С произведением в $k[x_1, \ldots, x_n]/I$ справиться не так легко. Мы рассмотрим пример, который демонстрирует возникающие здесь трудности. Рассмотрим идеал

$$I = \langle y + x^2 - 1, xy - 2y^2 + 2y \rangle \subset \mathbb{R}[x, y].$$

Его базис Грёбнера для lex-упорядочения с $x > y$ имеет вид

$$G = \{x^2 + y - 1, xy - 2y^2 + 2y, y^3 - (7/4)y^2 + (3/4)y\}. \tag{2}$$

Таким образом, $\langle LT(I) \rangle = \langle x^2, xy, y^3 \rangle$; следовательно, $\{1, x, y, y^2\}$ является базисом пространства остатков по модулю I. Рассмотрим классы эквивалентности полиномов $f = 3y^2 + x$ и $g = x - y$ в $\mathbb{R}[x, y]/I$. Произведение классов $[f]$ и $[g]$ представлено полиномом $f \cdot g = 3xy^2 + x^2 - 3y^3 - xy$. Но этот полином не является стандартным представителем, потому что он содержит мономы, *лежащие* в $\langle \mathrm{LT}(I) \rangle$. Однако мы можем *поделить* этот полином на G, и тогда остаток $\overline{f \cdot g}^G$ и будет стандартным представителем произведения. Имеем

$$\overline{3xy^2 + x^2 - 3y^3 - xy}^G = (-11/4)y^2 - (5/4)y + 1,$$

и этот полином принадлежит $\mathrm{Span}(1, x, y, y^2)$, как мы и ожидали.

Этот пример показывает, как алгоритмически проводить вычисления в $k[x_1, \ldots, x_n]/I$. Другими словами, мы доказали следующее утверждение.

Предложение 5. *Пусть I — идеал в $k[x_1, \ldots, x_n]$, и пусть G — его базис Грёбнера по отношению к некоторому мономиальному упорядочению. Для каждого $[f] \in k[x_1, \ldots, x_n]/I$ найдем стандартный представитель $\bar{f} = \bar{f}^G \in S = \mathrm{Span}(x^\alpha : x^\alpha \notin \langle LT(I) \rangle)$. Тогда*

(i) *$\bar{f} + \bar{g}$ представляет $[f] + [g]$;*
(ii) *$\overline{\bar{f} \cdot \bar{g}}^G$ представляет $[f] \cdot [g]$.*

Рассмотренные выше методы дают возможность построить алгоритм, позволяющий определить, состоит многообразие в $\mathbb{C}^n$ из конечного числа точек или нет, или, что эквивалентно, определить, конечно или бесконечно число решений полиномиальной системы над $\mathbb{C}$. (Как и в гл. 3, необходимо работать над алгебраически замкнутым полем, чтобы быть уверенным, что «не пропущены» решения с координатами, принадлежащими большему полю $K \supset k$.)

Теорема 6. *Пусть $V = \mathbf{V}(I)$ — аффинное многообразие в $\mathbb{C}^n$. Зафиксируем мономиальное упорядочение в $\mathbb{C}[x_1, \ldots, x_n]$. Следующие условия эквивалентны:*

(i) *V — конечное множество;*
(ii) *для каждого $i, 1 \le i \le n$, найдется $m_i \ge 0$, такое, что $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$;*
(iii) *если G — базис Грёбнера идеала I, то для каждого $i, 1 \le i \le n$, найдется $m_i \ge 0$, такое, что $x_i^{m_i} = \mathrm{LM}(g)$ для некоторого $g \in G$;*
(iv) *$\mathbb{C}$-векторное пространство $S = \mathrm{Span}(x^\alpha : x^\alpha \notin \langle \mathrm{LT}(I) \rangle)$ конечномерно;*
(v) *$\mathbb{C}$-векторное пространство $\mathbb{C}[x_1, \ldots, x_n]/I$ конечномерно.*

Доказательство. (i)⇒(ii). Если $V = \varnothing$, то $1 \in I$ по слабой теореме о нулях. В этом случае положим $m_i = 0$ для всех i. Если V непусто, то зафиксируем i, и пусть $a_j, j = 1, \ldots, l$, — различные комплексные числа, являющиеся i-ми координатами точек из V. Рассмотрим по-

лином от одной переменной

$$f(x_i) = \prod_{j=1}^{l} (x_i - a_j).$$

По построению f равен нулю в каждой точке из V; значит, $f \in \mathbf{I}(V)$. По теореме о нулях найдется $m \geq 1$, такое, что $f^m \in I$. Но это значит, что старший член полинома f^m принадлежит $\langle \mathrm{LT}(I) \rangle$, т. е. $x_i^{lm} \in \langle \mathrm{LT}(I) \rangle$.

(ii)$\Leftrightarrow$(iii). Пусть $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$. Так как G — это базис Грёбнера, то $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$. Но это значит (см. лемму 2 из § 4 гл. 2), что найдется $g \in G$, такой, что $\mathrm{LT}(g)$ делит $x_i^{m_i}$. Значит, $\mathrm{LT}(g)$ является степенью x_i. Обратное утверждение очевидно.

(ii)$\Rightarrow$(iv). Предположим, что некоторая степень $x_i^{m_i}$ принадлежит $\langle \mathrm{LT}(I) \rangle$ для каждого i. Тогда мономы $x_1^{\alpha_1} \dots x_n^{\alpha_n}$, где $\alpha_i \geq m_i$ хотя бы для одного i, принадлежат $\langle \mathrm{LT}(I) \rangle$. У мономов, принадлежащих дополнению к $\langle \mathrm{LT}(I) \rangle$, $\alpha_i < m_i$ для всех i. Следовательно, число мономов в дополнении к $\langle \mathrm{LT}(I) \rangle$ не превышает $m_1 \cdot \ldots \cdot m_n$.

(iv)$\Leftrightarrow$(v) следует из предложения 4.

(v)$\Rightarrow$(i). Для доказательства конечности многообразия V достаточно доказать, что для каждого i множество i-х координат точек из V конечно. Зафиксируем i и рассмотрим классы $[x_i^j] \in \mathbb{C}[x_1, \dots, x_n]/I, j = 0, 1, 2, \dots$. Так как $\mathbb{C}[x_1, \dots, x_n]/I$ конечномерно, то элементы множества $[x_i^j]$ *линейно зависимы* в $\mathbb{C}[x_1, \dots, x_n]/I$, т. е. существуют константы c_j (не все равные нулю) и натуральное m, такие, что

$$\sum_{j=0}^{m} c_j [x_i^j] = \left[\sum_{j=0}^{m} c_j x_i^j \right] = [0].$$

Значит, $\sum_{j=0}^{m} c_j x_i^j \in I$. Этот полином обращается в нуль в точках из V, но так как ненулевой полином имеет лишь конечное число корней в $\mathbb{C}$, то i-я координата точек из V имеет лишь конечное число значений.

Отметим, что условие $k = \mathbb{C}$ понадобилось нам только для доказательства импликации (i)$\Rightarrow$(ii). Все другие справедливы, даже когда поле не является алгебраически замкнутым. □

Правильный выбор мономиального упорядочения иногда значительно облегчает доказательство конечности многообразия. Рассмотрим, например, идеал

$$I = \langle x^5 + y^3 + z^2 - 1, x^2 + y^3 + z - 1, x^4 + y^5 + z^6 - 1 \rangle.$$

Используя grlex-упорядочение, мы получаем, что x^5, y^3, z^6 принадлежат $\langle \mathrm{LT}(I) \rangle$, так как это старшие мономы образующих. Тогда (теорема 6, п. (ii)) $\mathbf{V}(I)$ конечно (нам даже не понадобилось вычислять базис Грёбнера). Но если мы хотим найти точки многообразия $\mathbf{V}(I)$, то нам придется исключать переменные с помощью базиса Грёбнера для lex-упорядочения. Это трудное вычисление даже для системы компьютерной алгебры.

Анализ доказательства этой теоремы приводит к следующей оценке числа решений системы, если нам известно, что множество решений конечно.

Следствие 7. *Пусть I — идеал в $\mathbb{C}[x_1, \dots, x_n]$, такой, что некоторая степень $x_i^{m_i}$ лежит в $\langle \mathrm{LT}(I) \rangle$ для каждого i. Тогда число точек многообразия $\mathbf{V}(I)$ не превышает $m_1 \cdot \ldots \cdot m_n$.*

Доказательство. Доказательство этого утверждения мы оставляем читателю. □

Вот несколько примеров, иллюстрирующих следствие 7. Рассмотрим многообразие $V = \mathbf{V}(y - x^7, x^{12} - x) \subset \mathbb{C}^2$. Базис Грёбнера для lex-упорядочения с $y > x$ имеет вид $G = \{y - x^7, x^{12} - x\}$. Следовательно, в обозначениях теоремы 6 $m_1 = 12$, $m_2 = 1$ — наименьшие степени переменных, принадлежащие $\langle \mathrm{LT}(I) \rangle$. Решая уравнения $y - x^7 = x - x^{12} = 0$, мы получаем, что V действительно состоит из $12 = m_1 \cdot m_2$ точек:

$$V = \{(0,0)\} \cup \{(\zeta, \zeta^7) : \zeta^{11} = 1\}.$$

(Напомним, что в $\mathbb{C}$ существует 11 различных корней одиннадцатой степени из 1.)

Теперь рассмотрим многообразие $V = \mathbf{V}(x^2 + y - 1, xy - 2y^2 + 2y) \subset \mathbb{C}^2$. Базис Грёбнера для этого идеала по отношению к lex-упорядочению приведен в (2). Мы видим, что $m_1 = 2, m_2 = 3$ — наименьшие степени x и y, содержащиеся в $\langle \mathrm{LT}(I) \rangle$. Однако V содержит только $4 < 2 \cdot 3$ точки из $\mathbb{C}^2$:

$$V = \{(\pm 1, 0), (0, 1), (-1/2, 3/4)\}.$$

Можете ли вы объяснить причину этого явления?

Мы можем улучшить оценку из следствия 7 следующим образом.

Предложение 8. *Пусть I — идеал $\mathbb{C}[x_1, \dots, x_n]$, такой, что многообразие $V = \mathbf{V}(I)$ конечно.*

(i) *Число точек многообразия V не превышает размерности* $\dim(\mathbb{C}[x_1, \dots, x_n]/I)$ («dim» *обозначает размерность как векторного пространства над* $\mathbb{C}$).

(ii) *Если I — радикальный идеал, то число точек многообразия V равно* $\dim(\mathbb{C}[x_1,\dots,x_n]/I)$.

Доказательство. Докажем сначала, что для данных различных точек $p_1,\dots,p_m \in \mathbb{C}^n$ существует полином $f_1 \in \mathbb{C}[x_1,\dots,x_n]$, такой, что $f_1(p_1) = 1$ и $f_1(p_2) = \dots = f_1(p_m) = 0$. Если $a \neq b \in \mathbb{C}^n$, то хотя бы одной координатой, например j-й, a и b различаются. Тогда полином $g = (x_j - b_j)/(a_j - b_j)$ обладает тем свойством, что $g(a) = 1, g(b) = 0$. Применяя это соображение к каждой паре $p_1 \neq p_i$, $i \geq 2$, мы получаем полиномы $g_i, i \geq 2$, такие, что $g_i(p_1) = 1$ и $g_i(p_i) = 0$ для $i \geq 2$. Тогда полином $f_1 = g_2 \cdot g_3 \cdot \dots \cdot g_m$ обладает требуемым свойством.

Поскольку в точке p_1 нет ничего специфического, мы можем построить полиномы $f_2, f_3, \dots, f_m$, такие, что $f_i(p_i) = 1$ и $f_i(p_j) = 0$, если $i \neq j$.

Теперь перейдем к доказательству предложения 8. Пусть $V = \{p_1,\dots,p_m\}$, где точки p_i различны. Построим полиномы $f_1,\dots,f_m$, как выше. Если мы докажем, что $[f_1],\dots,[f_m] \in \mathbb{C}[x_1,\dots,x_n]/I$ линейно независимы, то неравенство

$$m \leq \dim(\mathbb{C}[x_1,\dots,x_n]/I) \tag{3}$$

будет доказано, что завершит доказательство п. (i).

Предположим, что классы $[f_1],\dots,[f_m]$ линейно зависимы. Тогда $\sum_{i=1}^m a_i[f_i] = [0]$ для некоторых $a_i \in \mathbb{C}$. Это означает, что $g = \sum_{i=1}^m a_i f_i \in I$. Поэтому g обращается в нуль во всех точках многообразия $V = \{p_1,\dots,p_m\}$. Но тогда для всех $j, 1 \leq j \leq m$, имеем

$$0 = g(p_j) = \sum_{i=1}^m a_i f_i(p_j) = 0 + a_j f_j(p_j) = a_j,$$

откуда и следует линейная независимость.

Пусть теперь I радикален. Если мы докажем, что $[f_1],\dots,[f_m]$ образуют базис в $\mathbb{C}[x_1,\dots,x_n]/I$, то тем самым докажем, что (3) становится равенством. Линейная независимость уже доказана, осталось доказать, что линейная оболочка классов $[f_i]$ содержит все факторкольцо. Пусть $[g] \in \mathbb{C}[x_1,\dots,x_n]/I$ — произвольный элемент и $a_i = g(p_i)$. Рассмотрим полином $h = g - \sum_{i=1}^m a_i f_i$. Тогда $h(p_j) = 0$ для всех j; следовательно, $h \in \mathbf{I}(V)$. По теореме о нулях $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ в силу алгебраической замкнутости поля $\mathbb{C}$. Но I радикален; следовательно, $h \in I$, т. е. $[h] = [0]$ в $\mathbb{C}[x_1,\dots,x_n]/I$. Значит, $[g] = \sum_{i=1}^m a_i[f_i]$. Предложение доказано. □

Покажем на примере, что предложение 8 улучшает оценку следствия 7. Рассмотрим идеал из примера 2. Используя grlex-упорядочение, мы показали, что $x^4, y^4 \in \langle \mathrm{LT}(I)\rangle$; поэтому по следствию 7 $\mathbf{V}(I)$ содержит $\leq 4 \cdot 4 = 16$ точек. Но в том же примере 2 показано, что $\dim(\mathbb{C}[x,y]/I) = 12$. Таким образом, предложение 8 дает лучшую оценку, а именно 12.

Для любого идеала I имеем $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$. Поэтому если $\mathbf{V}(I)$ конечно, то предложение 8 показывает, как можно точно найти число точек $\mathbf{V}(I)$ над $\mathbb{C}$, если нам известен радикал $\sqrt{I}$. Хотя нахождение радикала в общем случае — трудная задача, при выполнении условий из теоремы 6 это сравнительно легко сделать. Описание алгоритма дано в книге BECKER, WEISPFENNING (1993), Theorem 8.20. Этот же вопрос (и его связи с решением уравнений) рассматривается в работе COX, LITTLE, O'SHEA (1998).

Теорема 6 показывает, как можно охарактеризовать «нульмерные» многообразия (т. е. многообразия, содержащие лишь конечное множество точек), используя свойства кольца $\mathbb{C}[x_1,\dots,x_n]/I$. В гл. 9, когда мы будем рассматривать весьма общий вопрос о *размерности* многообразия, идеи и методы этого параграфа будут нам полезны.

Упражнения к § 3

1. Завершите доказательство п. (ii) предложения 1.
2. В предложении 5 был описан метод вычисления произведений $[f]\cdot[g]$ в $k[x_1,\dots,x_n]/I$. Могли бы мы просто вычислить $\overline{f\cdot g}^G$, не находя сначала остатки полиномов f и g?
3. Рассмотрим идеал $I = \langle x^4y - z^6, x^2 - y^3z, x^3z^2 - y^3\rangle \subset k[x,y,z]$.
   (a) Используя lex-упорядочение, найдите базис Грёбнера G для I и множество мономов, линейной оболочкой которого является пространство остатков от деления на G.
   (b) Сделайте то же самое для grlex-упорядочения. Сравните множества мономов.
4. Используя алгоритм деления и утверждение о единственности из предложения 1, докажите, что $\overline{c\cdot f}^G = c\cdot\bar{f}^G$, если $f \in k[x_1,\dots,x_n]$ и $c \in k$.
5. Пусть $I = \langle y + x^2 - 1, xy - 2y^2 + 2y\rangle \subset \mathbb{R}[x,y]$. (Этот идеал рассматривался в примере после предложения 4.)
   (a) Постройте изоморфизм векторных пространств $\mathbb{R}[x,y]/I \cong \mathbb{R}^4$.
   (b) Используя базис Грёбнера по отношению к lex-упорядочению, приведенный в (2), постройте «таблицу умножения» для элементов $\{[1],[x],[y],[y^2]\}$ в $\mathbb{R}[x,y]/I$. (Представьте каждое произведение как линейную комбинацию этих четырех классов.)
   (c) Верно ли, что $\mathbb{R}[x,y]/I$ является полем? Почему да или почему нет?

6. Пусть $V = \mathbf{V}(x_3 - x_1^2, x_4 - x_1x_2, x_2x_4 - x_1x_5, x_4^2 - x_3x_5) \subset \mathbb{C}^5$.
   (a) Используя любое удобное мономиальное упорядочение, найдите множество мономов, линейная оболочка которого совпадает с пространством остатков от деления на базис Грёбнера идеала, порожденного определяющими уравнениями многообразия V.
   (b) Для каких i найдется $m_i \geq 0$, такое, что $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$?
   (c) Верно ли, что V конечно? Почему да или почему нет?

7. Пусть I — некоторый идеал в $k[x_1, \ldots, x_n]$.
   (a) Предположим, что $S = \mathrm{Span}(x^\alpha : x^\alpha \notin \langle \mathrm{LT}(I) \rangle)$ является k-векторным пространством размерности d (для некоторого мономиального упорядочения). Докажите, что $k[x_1, \ldots, x_n]/I$ является k-векторным пространством размерности d.
   (b) Используя (a), докажите, что количество мономов в дополнении к $\langle \mathrm{LT}(I) \rangle$ не зависит от выбора мономиального упорядочения, если их конечное число.

8. Докажите следствие 7. Указание: используйте предложение 4 и п. (iii) теоремы 6.

9. Пусть $I \subset k[x_1, \ldots, x_n]$ — идеал, и пусть для каждого i найдется m_i, такое, что $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$. Сформулируйте и докажите критерий того, что $\mathbf{V}(I)$ содержит *ровно* $m_1 \cdot \ldots \cdot m_n$ точек из $\mathbb{C}^n$. Учитывает ли ваш критерий кратности корней?

10. Большинство систем компьютерной алгебры может упрощать выражения, содержащие радикалы. Например, вместо того чтобы работать с выражением
$$r = \frac{1}{x + \sqrt{2} + \sqrt{3}},$$
система позволит вам избавиться от иррациональностей в знаменателе и записать r как частное полиномов от x, где $\sqrt{2}$ и $\sqrt{3}$ встречаются в коэффициентах только в числителе. Один из методов, позволяющих делать такие преобразования, использует следующую идею.
   (a) Объясните, почему r можно рассматривать, как рациональную функцию от x с коэффициентами в факторкольце $R = \mathbb{Q}[y_1, y_2]/\langle y_1^2 - 2, y_2^2 - 3 \rangle$. Указание: см. упр. 4 к § 2.
   (b) Найдите базис Грёбнера G идеала $I = \langle y_1^2 - 2, y_2^2 - 3 \rangle$ и постройте таблицу умножения классов мономов, порождающих пространство остатков от деления на G (это будут $\{[1], [y_1], [y_2], [y_1y_2]\}$).
   (c) Для того чтобы избавиться от иррациональностей в знаменателе функции r, можно попробовать решить следующее уравнение:
$$(x[1] + [y_1] + [y_2]) \cdot (a_0[1] + a_1[y_1] + a_2[y_2] + a_3[y_1y_2]) = [1], \quad (3)$$
   где a_0, a_1, a_2, a_3 — рациональные функции от x с коэффициентами из $\mathbb{Q}$. Для этого надо раскрыть скобки в (3), воспользовавшись таблицей умножения из п. (b), и решить полученную линейную систему относительно a_0, a_1, a_2, a_3. Тогда
$$a_0[1] + a_1[y_1] + a_2[y_2] + a_3[y_1y_2]$$
   и является тем представлением для r, которое мы ищем.

11. В этой задаче мы найдем число различных мономов полной степени $\leq d$ в $k[x_1, \ldots, x_n]$ и установим связь этого числа с размерностью (понимаемой интуитивно) многообразия $V = k^n$.
   (a) Объясните, почему каждый моном из $k[x_1, \ldots, x_n]$ принадлежит дополнению к $\langle \mathrm{LT}(\mathbf{I}(V)) \rangle$, если $V = k^n$.
   (b) Докажите, что для всех $d, n \geq 0$, число различных мономов полной степени $\leq d$ в $k[x_1, \ldots, x_n]$ равно биномиальному коэффициенту $\binom{n+d}{n}$. (Это утверждение обобщает п. (a) из упр. 5 к § 1 гл. 2.)
   (c) Пусть n фиксировано. Докажите, что число мономов степени $\leq d$ растет как d^n при $d \to \infty$. Обратите внимание, что *показатель степени* n совпадает с интуитивной размерностью многообразия $V = k^n$, для которого $k[V] = k[x_1, \ldots, x_n]$.

12. В этом упражнении мы сравним, что происходит с мономами, принадлежащими дополнению к $\langle \mathrm{LT}(I) \rangle$, в двух примерах, когда $\mathbf{V}(I)$ бесконечно, и в одном, когда $\mathbf{V}(I)$ конечно.
   (a) Рассмотрим многообразие $\mathbf{V}(I) \subset \mathbb{C}^3$, где $I = \langle x^2 + y, x - y^2 + z^2, xy - z \rangle$. Найдите базис Грёбнера для I по отношению к lex-упорядочению и для $1 \leq d \leq 10$ найдите число мономов степени $\leq d$, не принадлежащих $\langle \mathrm{LT}(I) \rangle$. Отметим, что, согласно теореме 6, $\mathbf{V}(I)$ конечно в $\mathbb{C}^3$. Указание: попытайтесь нарисовать для этого идеала трехмерный аналог диаграмм из примера 2.
   (b) Повторите вычисления п. (a) для идеала $J = \langle x^2 + y, x - y^2 + z^2 \rangle$. Здесь $\mathbf{V}(J)$ бесконечно. Как отличается поведение числа мономов степени $\leq d$ (как функции от d), не принадлежащих $\langle \mathrm{LT}(J) \rangle$, от поведения аналогичной функции из п. (a)?
   (c) Обозначим через $H_J(d)$ число мономов степени $\leq d$, не принадлежащих $\langle \mathrm{LT}(J) \rangle$. Можете ли вы приблизительно определить число l, такое, что $H_J(d)$ растет как d^l.
   (d) Повторите вычисления пп. (b) и (c) для идеала $K = \langle x^2 + y \rangle$.
   (e) Можете ли вы усмотреть здесь некоторую зависимость, используя интуитивное понятие размерности, о котором шла речь в гл. 1? Мы вернемся к этим вопросам в гл. 9.

13. Пусть k — произвольное поле, I — идеал в кольце $k[x_1, \ldots, x_n]$ и $\dim(k[x_1, \ldots, x_n]/I) < \infty$.
   (a) Докажите, что $\dim(k[x_1, \ldots, x_n]/\sqrt{I}) \leq \dim(k[x_1, \ldots, x_n]/I)$. Указание: докажите, что включение $I \subset \sqrt{I}$ индуцирует отображение факторколец $k[x_1, \ldots, x_n]/I \to k[x_1, \ldots, x_n]/\sqrt{I}$, которое является отображением «на».

(b) Докажите, что число точек многообразия $\mathbf{V}(I)$ не превосходит $\dim(k[x_1,\dots,x_n]/\sqrt{I})$.

(c) Приведите пример, показывающий, что неравенство в п. (b) может быть строгим, если k не является алгебраически замкнутым.

§ 4. Координатное кольцо аффинного многообразия

В этом параграфе мы используем алгебраические методы, разработанные в §§ 2 и 3, для изучения кольца $k[V]$ полиномиальных функций на аффинном многообразии $V \subset k^n$. Изоморфизм $k[V] \cong k[x_1,\dots,x_n]/\mathbf{I}(V)$ из § 2 позволяет нам отождествить $k[V]$ с факторкольцом $k[x_1,\dots,x_n]/\mathbf{I}(V)$. Поэтому мы будем обозначать полиномиальную функцию из $k[V]$, представленную полиномом $f \in k[x_1,\dots,x_n]$, через $[f]$.

В частности, каждая переменная x_i определяет полиномиальную функцию $[x_i] : V \to k$, значение которой в точке $p \in V$ есть i-я координата этой точки. Мы будем $[x_i]$ называть *i-й координатной функцией* на V. Так как $k[V] \cong k[x_1,\dots,x_n]/\mathbf{I}(V)$, то координатные функции порождают $k[V]$ в том смысле, что любая функция из $k[V]$ является k-линейной комбинацией произведений полиномиальных функций $[x_i]$. Это объясняет происхождение следующего термина.

Определение 1. Пусть $V \subset k^n$ — аффинное многообразие. Тогда кольцо $k[V]$ называется *координатным кольцом* многообразия V.

Многие результаты из предыдущих параграфов могут быть переформулированы в терминах координатного кольца. Например:

- Предложение 4 из § 1: многообразие неприводимо в том и только том случае, когда его координатное кольцо является областью целостности.
- Теорема 6 из § 3: многообразие над $\mathbb{C}$ конечно в том и только том случае, когда его координатное кольцо конечномерно как векторное пространство над $\mathbb{C}$.

В алгебро-геометрическом «словаре» из гл. 4 мы связали многообразия из k^n с идеалами из $k[x_1,\dots,x_n]$. В этой главе мы хотим показать, что этот словарь сохраняет свое значение, если заменить k^n и $k[x_1,\dots,x_n]$ на некоторое многообразие V и его координатное кольцо $k[V]$. Но сначала дадим определения.

Определение 2. Рассмотрим аффинное многообразие $V \subset k^n$.

(i) Для произвольного идеала $J = \langle \phi_1,\dots,\phi_s\rangle$ в $k[V]$ определим множество
$$\mathbf{V}_V(J) = \{(a_1,\dots,a_n) \in V : \phi(a_1,\dots,a_n) = 0 \quad \text{для всех} \quad \phi \in J\},$$
которое называется *подмногообразием* многообразия V.

(ii) Для каждого подмножества $W \subset V$ положим
$$\mathbf{I}_V(W) = \{\phi \in k[V] : \phi(a_1,\dots,a_n) = 0 \text{ для всех } (a_1,\dots,a_n) \in W\}.$$

Пусть, например, $V = \mathbf{V}(z - x^2 - y^2) \subset \mathbb{R}^3$ и $J = \langle [x]\rangle \subset \mathbb{R}[V]$. Тогда
$$W = \mathbf{V}_V(J) = \{(0,y,y^2) : y \in \mathbb{R}\} \subset V$$
является подмногообразием в V. Отметим, что $W = \mathbf{V}(z - x^2 - y^2, x) \subset \mathbb{R}^3$. Аналогично, если $W = \{(1,1,2)\} \subset V$, то
$$\mathbf{I}_V(W) = \langle [x-1],[y-1]\rangle$$
(мы оставляем читателю в качестве упражнения доказательство этого равенства). Если аффинное многообразие V зафиксировано, то отображения $\mathbf{V}_V$ и $\mathbf{I}_V$ задают связи между подмногообразиями в V и идеалами в $k[V]$. Следующее предложение описывает характер этих связей.

Предложение 3. *Пусть $V \subset k^n$ — аффинное многообразие.*

(i) *Пусть J — идеал в $k[V]$. Тогда $W = \mathbf{V}_V(J)$ является аффинным многообразием в k^n, которое лежит в V.*

(ii) *Пусть $W \subset V$ — некоторое подмножество. Тогда $\mathbf{I}_V(W)$ является идеалом в $k[V]$.*

(iii) *Если $J \subset k[V]$ — некоторый идеал, то $J \subset \sqrt{J} \subset \mathbf{I}_V(\mathbf{V}_V(J))$.*

(iv) *Если $W \subset V$ — некоторое подмногообразие, то W совпадает с $\mathbf{V}_V(\mathbf{I}_V(W))$.*

Доказательство. Для доказательства п. (i) мы воспользуемся взаимно однозначным соответствием между идеалами в $k[V]$ и идеалами в $k[x_1,\dots,x_n]$, содержащими $\mathbf{I}(V)$ (предложение 10 из § 2). Пусть $\widetilde{J} = \{f \in k[x_1,\dots,x_n] : [f] \in J\} \subset k[x_1,\dots,x_n]$ — идеал, соответствующий идеалу $J \subset k[V]$. Тогда $\mathbf{V}(\widetilde{J}) \subset V$, потому что $\mathbf{I}(V) \subset \widetilde{J}$. Но вместе с тем $\mathbf{V}(\widetilde{J}) = \mathbf{V}_V(J)$, так как элементы из $\widetilde{J}$ представляют полиномиальные функции из J. Таким образом, W (рассматриваемое как подмножество в k^n) само является аффинным многообразием.

Доказательство утверждений (ii), (iii) и (iv) не вызывает трудностей, и мы оставляем его читателю в качестве упражнения. Отметим только, что определение радикала идеала одинаково в $k[V]$ и в $k[x_1,\dots,x_n]$. □

Можно доказать, что радикальные идеалы в $k[V]$ соответствуют радикальным идеалам в $k[x_1,\dots,x_n]$, содержащим $\mathbf{I}(V)$.

Предложение 4. *Идеал $J \subset k[V]$ радикален в том и только том случае, когда радикальным является идеал $\widetilde{J} = \{f \in k[x_1, \ldots, x_n] : [f] \in J\}$.*

Доказательство. Пусть J радикален и полином $f \in k[x_1, \ldots, x_n]$ таков, что $f^m \in \widetilde{J}$ для некоторого $m \geq 1$. Тогда $[f^m] = [f]^m \in J$. Но J радикален. Значит, $[f] \in J$. Следовательно, $f \in \widetilde{J}$ по определению, т. е. $\widetilde{J}$ тоже радикален. Пусть теперь $\widetilde{J}$ радикален и $[f]^m \in J$. Тогда $f^m \in \widetilde{J}$, а значит, $f \in \widetilde{J}$. Поэтому $[f] \in J$, т. е. J радикален. □

Вместо того чтобы детально обсуждать соответствие «идеал—многообразие» (что мы делали в гл. 4), мы ограничимся доказательством следующего результата, который определяет ряд важных черт этого соответствия.

Теорема 5. *Пусть k алгебраически замкнуто и $V \subset k^n$ — аффинное многообразие.*

(i) (*Теорема о нулях в $k[V]$*) *Если J — некоторый идеал в $k[V]$, то*

$$\mathbf{I}_V(\mathbf{V}_V(J)) = \sqrt{J} = \{[f] \in k[V] : [f]^m \in J\}.$$

(ii) *Отображения*

$$\left\{\begin{array}{c}\text{аффинные подмногообразия}\\ W \subset V\end{array}\right\} \underset{\mathbf{V}_V}{\overset{\mathbf{I}_V}{\rightleftarrows}} \left\{\begin{array}{c}\text{радикальные идеалы}\\ J \subset k[V]\end{array}\right\}$$

являются биекциями, обращающими включение, и взаимно обратны.

(iii) *При отображениях, определенных в п.* (ii), *точки многообразия V соответствуют максимальным идеалам в $k[V]$.*

Доказательство.

(i) Пусть J — идеал в $k[V]$. Тогда идеалу J соответствует (предложение 10 из § 2) идеал $\widetilde{J} \subset k[x_1, \ldots, x_n]$. Кроме того, $\mathbf{V}(\widetilde{J}) = \mathbf{V}_V(J)$ (доказательство предложения 3). Тогда, если $[f] \in \mathbf{I}_V(\mathbf{V}_V(\widetilde{J}))$, то $f \in \mathbf{I}(\mathbf{V}(\widetilde{J}))$. Согласно теореме о нулях для k^n, $\mathbf{I}(\mathbf{V}(\widetilde{J})) = \sqrt{\widetilde{J}}$; поэтому $f^m \in \widetilde{J}$ для некоторого $m \geq 1$. Но тогда $[f^m] = [f]^m \in J$, так что $[f] \in \sqrt{J}$ в $k[V]$. Таким образом, $\mathbf{I}_V(\mathbf{V}_V(J)) \subset \sqrt{J}$. Противоположное включение имеет место для любого идеала. Теорема о нулях для $k[V]$ доказана.

(ii) следует из (i), как в гл. 4.

(iii) доказывается так же, как теорема 11 из § 5 гл. 4. □

Теперь мы возвращаемся к вопросу о *классификации* многообразий, сформулированному в § 1. Что означает, что два аффинных многообразия «изоморфны»? Разумный ответ дает следующее определение.

Определение 6. Пусть $V \subset k^m$ и $W \subset k^n$ — аффинные многообразия. Они называются *изоморфными*, если существуют полиномиальные отображения $\alpha : V \to W$ и $\beta : W \to V$, такие, что $\alpha \circ \beta = \mathrm{id}_W$ и $\beta \circ \alpha = \mathrm{id}_V$. (Для любого многообразия V через id_V обозначается тождественное отображение V на себя. Это отображение всегда полиномиально.)

На интуитивном уровне очевидно, что если многообразия *изоморфны*, то они одновременно приводимы или неприводимы, имеют одинаковую размерность и т. д. Кроме того, должно существовать соответствие между подмногообразиями в V и подмногообразиями в W. Например, если $W \subset k^n$ изоморфно $V = k^m$, то существует взаимно однозначное полиномиальное отображение $\alpha : k^m \to W$, у которого есть полиномиальное обратное, т. е. в этом случае существует полиномиальная *параметризация* многообразия W с хорошими свойствами! Вот пример, подсказанный методами геометрического моделирования, который иллюстрирует пользу этого понятия.

Пример 7. Рассмотрим две поверхности

$$Q_1 = \mathbf{V}(x^2 - xy + y^2 + z^2) = \mathbf{V}(f_1),$$
$$Q_2 = \mathbf{V}(x^2 - y^2 + z^2 - z) = \mathbf{V}(f_2)$$

в $\mathbb{R}^3$. (Эти поверхности могут, например, ограничивать тело, форму которого мы проектируем.) Как описать *кривую пересечения* $C = \mathbf{V}(f_1, f_2)$ этих поверхностей? Непосредственно сделать это затруднительно. Но, как обычно, *не обязательно* использовать именно полиномы f_1 и f_2 для описания кривой. Легко видеть, что $C = \mathbf{V}(f_1, f_1 + cf_2)$, где $c \in \mathbb{R}$ — ненулевая константа. Следовательно, поверхности $F_c = \mathbf{V}(f_1, f_1 + cf_2)$ также содержат C. Это множество поверхностей вместе с Q_2 называется *пучком* поверхностей, определенным поверхностями Q_1 и Q_2. (Пучок многообразий — это однопараметрическое семейство многообразий, параметризованное элементами поля k. В нашем случае параметр — это $c \in \mathbb{R}$.)

Теперь надо найти значение c, такое, при котором поверхность F_c особенно проста. Тогда задача описания кривой C также упростится. Если $c = -1$, то поверхность F_{-1} определена уравнениями

$$0 = f_1 - f_2 = z - xy.$$

Поверхность $Q = F_{-1}$ легко себе представить, потому что она *изоморфна $\mathbb{R}^2$ как многообразие* (это верно для любого *графика* полиномиальной функции $f(x, y)$). Чтобы доказать это, отметим, что

существуют полиномиальные отображения

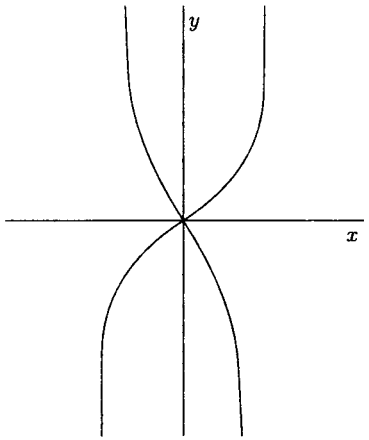
$$\begin{aligned} \alpha : \mathbb{R}^2 &\longrightarrow Q, \\ (x, y) &\mapsto (x, y, xy), \\ \pi : Q &\longrightarrow \mathbb{R}^2, \\ (x, y, z) &\mapsto (x, y), \end{aligned}$$

удовлетворяющие соотношениям $\alpha \circ \pi = \mathrm{id}_Q$ и $\pi \circ \alpha = \mathrm{id}_{\mathbb{R}^2}$.

Следовательно, изучение кривой на Q, в частности C, можно свести к изучению плоской кривой. А именно, мы рассматриваем вместо C ее проекцию $\pi(C) \subset \mathbb{R}^2$. Уравнение проекции

$$x^2y^2 + x^2 - xy - y^2 = 0$$

может быть получено из f_1 или f_2 с помощью подстановки $z = xy$. Отметим, что π и α (ограниченные на C и $\pi(C)$ соответственно) задают изоморфизм между C и $\pi(C)$, так что мы ничего не теряем, переходя к проекции.



В частности, каждой точке $(a, b) \in \pi(C)$ соответствует ровно одна точка $(a, b, ab) \in C$. В упражнениях будет доказано, что $\pi(C)$ имеет следующую параметризацию:

$$\begin{aligned} x &= \frac{-t^2 + t + 1}{t^2 + 1}, \\ y &= \frac{-t^2 + t + 1}{t(t + 2)}. \end{aligned} \tag{1}$$

Эти формулы позволяют построить параметризацию кривой C, используя изоморфизм α.

Имея в виду предыдущий пример, естественно спросить, как можно доказать изоморфность двух многообразий? Один из способов — это сравнить их координатные кольца

$$k[V] = k[x_1, \ldots, x_n]/\mathbf{I}(V) \quad \text{и} \quad k[W] = k[y_1, \ldots, y_n]/\mathbf{I}(W).$$

Основу здесь составляет тот факт, что если задано полиномиальное отображение $\alpha : V \to W$, то каждой полиномиальной функции $\phi : W \to k$ из $k[W]$ сопоставляется другая полиномиальная функция $\phi \circ \alpha : V \to k$ из $k[V]$. Таким образом, мы получаем отображение из $k[W]$ в $k[V]$ со следующими свойствами.

Предложение 8. *Пусть V и W — многообразия (возможно, принадлежащие различным аффинным пространствам).*

(i) *Пусть $\alpha : V \to W$ — полиномиальное отображение. Тогда для каждой полиномиальной функции $\phi : W \to k$ композиция $\phi \circ \alpha : V \to k$ также является полиномиальной функцией. Более того, отображение $\alpha^* : k[W] \to k[V]$, определенное формулой $\alpha^*(\phi) = \phi \circ \alpha$, является кольцевым гомоморфизмом, тождественным на постоянных функциях. (Отметим, что α^* «действует в противоположном направлении» по сравнению с α, так как отображает функции на W в функции на V. По этой причине α^* называется* отображением обратного образа *на функциях.)*

(ii) *Обратно, пусть $f : k[W] \to k[V]$ — кольцевой гомоморфизм, тождественный на постоянных функциях. Тогда существует единственное полиномиальное отображение $\alpha : V \to W$, такое, что $f = \alpha^*$.*

Доказательство. (i) Пусть $x_1, \ldots, x_m$ — координаты в $k^m \supset V$, а $y_1, \ldots, y_n$ — координаты в $k^n \supset W$. Тогда полиномиальная функция $\phi : W \to k$ может быть представлена полиномом $f(y_1, \ldots, y_n)$, а полиномиальное отображение $\alpha : V \to W$ может быть представлено n-набором полиномов:

$$\alpha(x_1, \ldots, x_m) = (a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)).$$

Найдем $\phi \circ \alpha$, подставляя $\alpha(x_1, \ldots, x_m)$ в ϕ:

$$(\phi \circ \alpha)(x_1, \ldots, x_m) = f(a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)).$$

Очевидно, что $\phi \circ \alpha$ является полиномом от $x_1, \ldots, x_n$. Таким образом, $\phi \circ \alpha \in k[V]$.

Значит, мы можем определить $\alpha^* : k[W] \to k[V]$ формулой $\alpha^*(\phi) = \phi \circ \alpha$. Покажем, что α^* — кольцевой гомоморфизм. Пусть ψ — другая полиномиальная функция из $k[W]$, представленная по-

линомом $g(y_1,\dots,y_n)$. Тогда

$$\begin{aligned}(\alpha^*(\phi+\psi))(x_1,\dots,x_m) &= f(a_1(x_1,\dots,x_m),\dots,a_n(x_1,\dots,x_m))\\ &\quad + g(a_1,(x_1,\dots,x_m),\dots,a_n(x_1,\dots,x_m))\\ &= \alpha^*(\phi)(x_1,\dots,x_m)+\alpha^*(\psi)(x_1,\dots,x_m).\end{aligned}$$

Следовательно, $\alpha^*(\phi+\psi)=\alpha^*(\phi)+\alpha^*(\psi)$. Равенство $\alpha^*(\phi\cdot\psi)=\alpha^*(\phi)\cdot\alpha^*(\psi)$ доказывается аналогично. Значит, α^* — это кольцевой гомоморфизм.

Рассмотрим теперь постоянную функцию $[a]\in k[W], a\in k$, на W со значением a. Тогда $\alpha^*([a])=[a]\circ\alpha$ является постоянной функцией на V с тем же значением a. Таким образом, отображение α^* тождественно на константах.

(ii) Пусть теперь $f: k[W]\to k[V]$ — кольцевой гомоморфизм, тождественный на константах. Нам нужно доказать, что существует полиномиальное отображение $\alpha: V\to W$, такое, что $f=\alpha^*$. Рассмотрим координатные функции $[y_1],\dots,[y_n]\in k[W]$. Тогда $f([y_i])\in k[V]$, а так как $x_1,\dots,x_m$ — это координаты на $k^m\supset V$, то $f([y_i])=[a_i(x_1,\dots,x_m)]\in k[V]$ для некоторых полиномов $a_i\in k[x_1,\dots,x_m]$. Теперь рассмотрим полиномиальное отображение

$$\alpha=(a_1(x_1,\dots,x_m),\dots,a_n(x_1,\dots,x_m)).$$

Мы докажем, что α отображает V в W и что $f=\alpha^*$.

Пусть $F\in k[y_1,\dots,y_n]$. Тогда

$$[F\circ\alpha]=f([F]) \tag{2}$$

в $k[V]$. Чтобы это доказать, отметим, что

$$[F\circ\alpha]=[F(a_1,\dots,a_n)]=F([a_1],\dots,[a_n])=F(f([y_1]),\dots,f([y_n])),$$

где второе равенство следует из определения операций в $k[V]$, а третье — из равенств $[a_i]=f([y_i])$. Но $[F]$ — это k-линейная комбинация произведений $[y_i]$; поэтому

$$F(f([y_1]),\dots,f([y_n]))=f([F(y_1,\dots,y_n)])=f([F]),$$

так как f является кольцевым гомоморфизмом, тождественным на постоянных функциях (см. упр. 10). Отсюда следует (2).

Теперь мы докажем, что α отображает V в W. Пусть $(c_1,\dots,c_m)\in V$. Нам нужно доказать, что $\alpha(c_1,\dots,c_m)\in W$. Если $F\in\mathbf{I}(W)$, то $[F]=0$ в $k[W]$. Тогда $f([F])=0$ в $k[V]$, потому что f — кольцевой гомоморфизм. По (2) отсюда следует, что $[F\circ\alpha]$ — нулевая функция на V. В частности,

$$[F\circ\alpha](c_1,\dots.c_m)=F(\alpha(c_1,\dots,c_m))=0.$$

В силу произвольности выбора F из $\mathbf{I}(W)$ получаем, что $\alpha(c_1,\dots,c_m)\in W$.

Теперь мы знаем, что α отображает V в W. Поэтому из равенства (2) следует, что $[F]\circ\alpha=f([F])$ для любой полиномиальной функции $[F]\in k[W]$. Так как $\alpha^*([F])=[F]\circ\alpha$, то $f=\alpha^*$. Осталось показать, что отображение α определено однозначно. Пусть существует отображение $\beta: V\to W$, такое, что $f=\beta^*$, и пусть

$$\beta(x_1,\dots,x_m)=(b_1(x_1,\dots,x_m),\dots,b_n(x_1,\dots,x_m)).$$

Тогда $\beta^*([y_i])=[y_i]\circ\beta=[b_i(x_1,\dots,x_m)]$. Однако $\alpha^*([y_i])=[a_i(x_1,\dots,x_m)]$, а так как $\alpha^*=f=\beta^*$, то $[a_i]=[b_i]$ для всех i. Таким образом, a_i и b_i определяют одну и ту же функцию на V и, следовательно, $\alpha=(a_1,\dots,a_n)$ и $\beta=(b_1,\dots,b_n)$ определяют одно и то же отображение из V в W. Значит, $\alpha=\beta$ и единственность доказана. □

Пусть теперь $\alpha: V\to W$ и $\beta: W\to V$ — взаимно обратные полиномиальные отображения. Тогда $\alpha\circ\beta=\mathrm{id}_W$. Но это означает, что $(\alpha\circ\beta)^*(\phi)=\mathrm{id}_W^*(\phi)=(\phi)\circ\mathrm{id}_W=\phi$ для всех $\phi\in k[W]$. С другой стороны,

$$\begin{aligned}(\alpha\circ\beta)^*(\phi)=\phi\circ(\alpha\circ\beta)&=(\phi\circ\alpha)\circ\beta\\ &=\alpha^*(\phi)\circ\beta=\beta^*(\alpha^*(\phi))=(\beta^*\circ\alpha^*)(\phi).\end{aligned} \tag{3}$$

Следовательно, $(\alpha\circ\beta)^*=\beta^*\circ\alpha^*=\mathrm{id}_{k[W]}$ как отображение из $k[W]$ в себя. Аналогично, $(\beta\circ\alpha)^*=\alpha^*\circ\beta^*=\mathrm{id}_{k[V]}$. Это доказывает первую часть следующего утверждения.

Теорема 9. *Два аффинных многообразия $V\subset k^m$ и $W\subset k^n$ изоморфны в том и только том случае, когда существует изоморфизм $k[V]\cong k[W]$ их координатных колец, тождественный на константах.*

Доказательство. Мы уже доказали, что если V и W изоморфны, то $k[V]\cong k[W]$ как кольца. По предложению 8 этот изоморфизм тождествен на константах.

Пусть теперь существует кольцевой изоморфизм $f: k[W]\to k[V]$, тождественный на константах. Тогда f и f^{-1} «задаются» полиномиальными отображениями из V в W и из W в V соответственно, т. е. $f=\alpha^*$ для некоторого $\alpha: V\to W$ и $f^{-1}=\beta^*$ для некоторого $\beta: W\to V$ в силу п. (ii) предложения 8. Нам нужно показать, что отображения α и β взаимно обратны. Рассмотрим композицию $\alpha\circ\beta: W\to W$. Очевидно, что это полиномиальное отображение, и по (3)

$$(\alpha\circ\beta)^*(\phi)=\beta^*(\alpha^*(\phi))=f^{-1}(f(\phi))=\phi \tag{4}$$

для любой полиномиальной функции $\phi\in k[W]$. Но $\mathrm{id}_W: W\to W$ — это полиномиальное отображение, и $\mathrm{id}_W^*(\phi)=\phi$ для всех $\phi\in k[W]$.

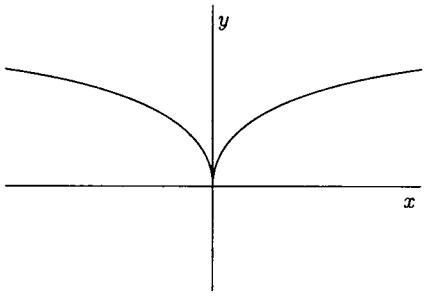
Согласно (4), $(\alpha \circ \beta)^* = \mathrm{id}_W^*$, а значит, $\alpha \circ \beta = \mathrm{id}_W$ по утверждению о единственности из п. (ii) предложения 8. Аналогично получаем, что $\beta \circ \alpha = \mathrm{id}_V$; следовательно, α и β взаимно обратны. Теорема доказана. □

В заключение мы рассмотрим несколько примеров изоморфизмов многообразий и соответствующих изоморфизмов их координатных колец.

Пусть A — невырожденная $n \times n$-матрица с элементами из k. Рассмотрим линейное отображение $L_A : k^n \to k^n$, определенное формулой $L_A(x) = Ax$, где Ax — произведение матрицы на вектор-столбец. Из упр. 9 к § 1 гл. 4 мы знаем, что L_A^* — кольцевой изоморфизм из $k[x_1, \ldots, x_n]$ на себя. Следовательно, L_A — это изоморфизм многообразия k^n на себя. (Такие изоморфизмы называются *автоморфизмами* многообразий.) В упр. 9 будет доказано, что если V — многообразие в k^n, то $L_A(V)$ — также многообразие в k^n, причем $L_A(V)$ изоморфно V (ограничение L_A на V и является изоморфизмом этого многообразия V на $L_A(V)$). Например, кривая, которую мы рассматривали в последнем примере в § 1, получена из «стандартной» скрученной кубики в $\mathbb{C}^3$ с помощью обратимого линейного преобразования. Проанализируйте уравнение (5) из § 1 и постарайтесь определить отображение L_A.

Пусть теперь $f(x, y) \in k[x, y]$. Рассмотрим *график* полиномиальной функции f, т. е. многообразие $V = \mathbf{V}(z - f(x, y)) \subset k^3$. Обобщая то, что мы говорили о многообразии $\mathbf{V}(z - xy)$ в примере 7, мы можем сказать, что V изоморфно k^2 как многообразие. Дело в том, что проекция $\pi : V \to k^2$ и параметризация V, заданная формулой $\alpha : k^2 \to V$, $\alpha(x, y) = (x, y, f(x, y))$, являются взаимно обратными отображениями. Изоморфизм координатных колец α^* состоит в подстановке $z = f(x, y)$ в любую полиномиальную функцию $F(x, y, z)$ на V.

Рассмотрим, наконец, кривую $V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$.



Мы утверждаем, что V *не* изоморфно $\mathbb{R}$ как многообразие, хотя существует взаимно однозначное полиномиальное отображение из V на $\mathbb{R}$ — проекция многообразия V на ось x. Причина в структуре координатного кольца $\mathbb{R}[V] = \mathbb{R}[x, y]/\langle y^5 - x^2 \rangle$. Если бы существовал изоморфизм $\alpha : \mathbb{R} \to V$, то $\alpha^* : \mathbb{R}[V] \to \mathbb{R}[u]$ было бы кольцевым изоморфизмом. Пусть

$$\alpha^*([x]) = c(u),$$
$$\alpha^*([y]) = d(u),$$

где $c(u), d(u) \in \mathbb{R}[u]$. Так как $y^5 - x^2$ представляет нуль в $\mathbb{R}[V]$, то $\alpha^*(y^5 - x^2) = (d(u))^5 - (c(u))^2 = 0$ в $\mathbb{R}[u]$.

Мы можем считать, что $c(0) = d(0) = 0$, — в противном случае сделаем замену переменной u так, чтобы $\alpha(0) = (0, 0) \in V$. Рассмотрим полиномиальное уравнение $(c(u))^2 = (d(u))^5$, и пусть

$$c(u) = c_1 u + c_2 u^2 + \ldots, \quad d(u) = d_1 u + d_2 u^2 + \ldots$$

— его решение. Разложение полинома $(d(u))^5$ по степеням u не содержит степеней, меньших u^5; поэтому то же самое справедливо относительно $(c(u))^2$. Но

$$(c(u))^2 = c_1^2 u^2 + 2c_1 c_2 u^3 + (c_2^2 + 2c_1 c_3) u^4 + \ldots.$$

Следовательно, $c_1 = 0$. Но коэффициент при u^4 также должен быть равен нулю; значит, и $c_2 = 0$. Если $c_1 = c_2 = 0$, то коэффициент при u^5 в $(c(u))^2$ равен нулю. Значит, разложение полинома $(c(u))^2$ начинается со степени 6. Но тогда $d_1 = 0$.

Из этого следует, что полином u не может принадлежать образу отображения α^*, так как последний состоит из полиномов от $c(u)$ и $d(u)$. Но если α^* — изоморфизм, то его образ должен совпадать со *всем* кольцом $\mathbb{R}[u]$. Значит, мы получили противоречие и эти два многообразия не изоморфны. Из упражнений с помощью методов § 3 можно получить дополнительные сведения о структуре $\mathbb{R}[V]$. Это и позволит дать другое доказательство того, что $\mathbb{R}[V]$ не изоморфно кольцу полиномов от одной переменной.

Упражнения к § 4

1. Пусть C — скрученная кубика в k^3.
   (a) Докажите, что C является подмногообразием поверхности $S = \mathbf{V}(xz - y^2)$.
   (b) Найдите идеал $J \subset k[S]$, такой, что $C = \mathbf{V}_S(J)$.
2. Пусть $V \subset \mathbb{C}^n$ — непустое аффинное многообразие.
   (a) Пусть $\phi \in \mathbb{C}[V]$. Докажите, что $\mathbf{V}_V(\phi) = \varnothing$ в том и только том случае, когда ϕ обратима в $\mathbb{C}[V]$ (т. е. когда существует функция $\psi \in \mathbb{C}[V]$, такая, что $\phi\psi = [1] \in \mathbb{C}[V]$).

(b) Останется ли утверждение п. (a) верным при замене $\mathbb{C}$ на $\mathbf{R}$? Если да, то докажите это, если нет, то приведите контрпример.

3. Докажите пп. (ii), (iii) и (iv) предложения 3.

4. Пусть $V = \mathbf{V}(y - x^n, z - x^m)$, где m, n — натуральные числа. Докажите, что V изоморфно k как многообразие, построив взаимно обратные полиномиальные отображения $\alpha : k \to V$ и $\beta : V \to k$.

5. Докажите, что любая поверхность в k^3, определенная уравнением вида $x - f(y, z) = 0$ или $y - g(x, z) = 0$, изоморфна k^2 как многообразие.

6. Пусть V — многообразие в k^n, заданное уравнением вида $x_n - f(x_1, \ldots, x_{n-1}) = 0$. Докажите, что V изоморфно k^{n-1} как многообразие.

7. В этом упражнении мы выведем параметризацию (1) проекции $\pi(C)$ из примера 7.
   (a) Докажите, что любая гипербола в $\mathbb{R}^2$ с горизонтальной и вертикальной асимптотами, которая проходит через точки $(0, 0)$ и $(1, 1)$, определена уравнением вида
   $$xy + tx - (t + 1)y = 0$$
   для некоторого t.
   (b) Используя систему компьютерной алгебры, найдите базис Грёбнера идеала, порожденного уравнениями кривой $\pi(C)$ и уравнением гиперболы. Используйте lex-упорядочение с $x > y > t$.
   (c) Базис Грёбнера будет содержать только один полином, не зависящий от x. Рассматривая его как полином от y, покажите, что $y = 0$ является его двойным корнем, $y = 1$ — простым корнем и что у него имеется еще один корень, зависящий от t, $y = \frac{-t^2+t+1}{t(t+2)}$.
   (d) Теперь, рассмотрев другие элементы базиса Грёбнера, докажите, что «непостоянному» корню, найденному в п. (c), отвечает единственное значение x, которое можно найти по первой формуле из (1).

   Создается впечатление, что метод, рассмотренный в этом упражнении, приспособлен для решения исключительно этой конкретной задачи. Но на самом деле это пример техники, нацеленной на решение задач об алгебраических кривых. С использованием комплексной проективной плоскости в гл. 8 будет показано, что $\pi(C)$ содержится в проективной алгебраической кривой с *тремя* особыми точками (аналогичными точке $(0, 0)$ на рисунке). С помощью семейства коник, проходящих через эти три точки и еще одну точку, мы можем построить рациональную параметризацию *любой* неприводимой квартики (т. е. кривой четвертого порядка) с тремя особенностями. *Неособые* квартики не имеют рациональной параметризации.

8. Пусть $Q_1 = \mathbf{V}(x^2 + y^2 + z^2 - 1)$ и $Q_2 = \mathbf{V}((x - 1/2)^2 - 3y^2 - 2z^2)$ в $\mathbb{R}^3$.

   (a) Используя метод примера 7 и упр. 5, в пучке, определенном многообразиями Q_1 и Q_2, найдите поверхность, изоморфную $\mathbb{R}^2$ (как многообразие).
   (b) Опишите и/или нарисуйте кривую $Q_1 \cap Q_2$.

9. Пусть $\alpha : V \to W$ и $\beta : W \to V$ — взаимно обратные полиномиальные отображения двух изоморфных многообразий V и W. Пусть $U = \mathbf{V}_V(I)$, где I — некоторый идеал в $k[V]$. Докажите, что $\alpha(U)$ является подмногообразием в W, и объясните, как найти идеал $J \subset k[W]$, такой, что $\alpha(U) = \mathbf{V}_W(J)$.

10. Пусть $f : k[V] \to k[W]$ — изоморфизм координатных колец, тождественный на константах. Пусть $V \subset k^m$ и $x_1, \ldots, x_m$ — координаты в k^m. Докажите, что $f([F]) = F(f([x_1]), \ldots, f([x_m]))$, где $F \in k[x_1, \ldots, x_m]$. Указание: представьте F как k-линейную комбинацию произведений $[x_i]$.

11. В этом упражнении мы займемся поверхностью V, рассмотренной после определения 2, $V = \mathbf{V}(z - x^2 - y^2) \subset \mathbb{R}^3$.
   (a) Докажите, что подмногообразие $W = \{(1, 1, 2)\} \subset V$ равно $\mathbf{V}_V([x - 1], [y - 1])$. Объясните, почему из этого следует, что $\langle [x - 1], [y - 1] \rangle \subset \mathbf{I}_V(W)$.
   (b) Докажите, что $\langle [x - 1], [y - 1] \rangle = \mathbf{I}_V(W)$. Указание: докажите, что V изоморфно $\mathbb{R}^2$ и примените упр. 9.

12. Пусть $V = \mathbf{V}(y^2 - 3x^2z + 2) \subset \mathbb{R}^3$, и пусть L_A — линейное преобразование на $\mathbb{R}^3$, заданное матрицей
   $$A = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$
   (a) Проверьте, что L_A является изоморфизмом из $\mathbb{R}^3$ на $\mathbb{R}^3$.
   (b) Найдите уравнение образа многообразия V при L_A.

13. В этом упражнении мы изучим вращения скрученной кубики.
   (a) Найдите матрицу вращения в $\mathbb{R}^3$ против часовой стрелки на угол $\pi/6$ вокруг оси z.
   (b) Найдите уравнение образа стандартной скрученной кубики при этом вращении.

14. В этом упражнении мы рассмотрим другое доказательство того факта, что кривая $V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$ не изоморфна $\mathbb{R}$. В этом доказательстве будет использована алгебраическая структура кольца $\mathbb{R}[V]$. Мы докажем, что не существует изоморфизма между кольцами $\mathbb{R}[V]$ и $\mathbb{R}[t]$ ($\mathbb{R}[t]$ — это координатное кольцо многообразия $\mathbb{R}$).
   (a) Используя методы § 3, докажите, что каждый элемент из $\mathbb{R}[V]$ представлен единственным полиномом вида $a(y) + b(y)x$, где $a, b \in \mathbb{R}[y]$.
   (b) Найдите такое же представление для произведения $(a + bx)(a' + b'x) \in \mathbb{R}[V]$.

(c) Предположим, что, напротив, существует кольцевой изоморфизм $\alpha : \mathbb{R}[t] \to \mathbb{R}[V]$. Так как α — это отображение «на», то $x = \alpha(f(t))$ и $y = \alpha(g(t))$ для некоторых полиномов f, g. Используя однозначность разложения f и g на множители и формулу для произведения из п. (b), получите противоречие.

15. Пусть $V \subset \mathbb{R}^3$ — касательная поверхность скрученной кубики.
   (a) Докажите, что обычная параметризация многообразия V является взаимно однозначным соответствием между точками этого многообразия и точками из $\mathbb{R}^2$. Указание: вернитесь к рассмотрению поверхности в § 3 гл. 3. Естественно спросить, верно ли, что V *изоморфно* $\mathbb{R}^2$. Мы покажем, что *нет*.
   (b) Используя метод упр. 12 к § 4 гл. 3, докажите, что каждая точка скрученной кубики является особой точкой многообразия V. (Касательная поверхность имеет так называемое «каспидальное ребро» вдоль кубики.)
   (c) Пусть $\alpha : \mathbb{R}^2 \to V$ — *произвольная* полиномиальная параметризация многообразия V и точка $\alpha(a, b)$ принадлежит кубике. Тогда матрица производных отображения α имеет ранг меньше 2 в точке (a, b) (другими словами, столбцы матрицы производных линейно зависимы). (Обратите внимание, что α не обязательно является стандартной параметризацией, хотя утверждение верно и в стандартном случае тоже.)
   (d) Предположим теперь, что полиномиальное отображение α имеет полиномиальное обратное $\beta : V \to \mathbb{R}^2$. Докажите, что мы придем к противоречию с п. (c), если вычислим матрицу производных в точке (a, b), такой, что $\alpha(a, b)$ принадлежит кубике.

§ 5. Рациональные функции на многообразии

Многие поля содержат кольцо целых чисел. *Наименьшим* из таких полей является поле рациональных чисел $\mathbb{Q}$, потому что $\mathbb{Q}$ строится из дробей $\frac{m}{n}, m, n \in \mathbb{Z}$. Для построения $\mathbb{Q}$ используются только целые числа. Аналогично, полиномиальное кольцо $k[x_1, \ldots, x_n]$ является подкольцом поля *рациональных функций*

$$k(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : f, g \in k[x_1, \ldots, x_n], g \neq 0 \right\}.$$

Обобщим эти примеры. Пусть R — некоторая область целостности. Тогда мы можем построить ее *поле частных*, которое обозначается $QF(R)$. Его элементами являются «дроби» r/s, где $r, s \in R$ и $s \neq 0$[1]. Мы складываем и умножаем элементы из $QF(R)$ как числовые дроби или рациональные функции:

$$r/s + t/u = (ru + ts)/su \quad \text{и} \quad r/s \cdot t/u = rt/su.$$

Обратите внимание, что так как R — область целостности, то знаменатели и суммы, и произведения не равны нулю. Далее, две дроби r/s и r'/s' равны в $QF(R)$, если $rs' = r's$. Легко проверить, что все аксиомы поля в $QF(R)$ выполнены (см. упр. 1). Более того, $QF(R)$ содержит подмножество $\{r/1 : r \in R\}$, которое является подкольцом, изоморфным R. Это и объясняет смысл термина «поле частных кольца R».

Пусть $V \subset k^n$ — *неприводимое* многообразие. Тогда (см. § 1) координатное кольцо $k[V]$ является областью целостности. Поле частных $QF(k[V])$ имеет особое название.

Определение 1. Пусть V — неприводимое аффинное многообразие в k^n. Тогда поле $QF(k[V])$ называется *полем функций* или *полем рациональных функций* на V и обозначается $k(V)$.

Обратите внимание на соблюдение стиля обозначений: $k[x_1, \ldots, x_n]$ обозначает кольцо полиномов, а $k[V]$ — координатное кольцо многообразия V; аналогично, $k(x_1, \ldots, x_n)$ обозначает поле рациональных функций, а $k(V)$ — поле функций на V.

Явно поле функций $k(V), V \subset k^n$, можно задать так:

$$\begin{aligned} k(V) &= \{\phi/\psi : \phi, \psi \in k[V], \psi \neq 0\} \\ &= \{[f]/[g] : f, g \in k[x_1, \ldots, x_n], g \notin \mathbf{I}(V)\}. \end{aligned}$$

Как и при работе с рациональными функциями, мы должны следить за необращением в нуль знаменателя. Таким образом, элемент $\phi/\psi \in k(V)$ определяет функцию только на дополнении к $\mathbf{V}_V(\psi)$.

Многообразие $V = k^n$ дает основной пример поля функций. Здесь $k[V] = k[x_1, \ldots, x_n]$ и, следовательно,

$$k(V) = k(x_1, \ldots, x_n).$$

Рассмотрим более сложные примеры.

Пример 2. В § 4 мы доказали, что кривая

$$V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$$

не изоморфна $\mathbb{R}$, потому что координатные кольца многообразий $\mathbb{R}$ и V не изоморфны. Что можно сказать о поле функций? Отметим сначала, что метод § 2 предлагает представлять элементы из $\mathbb{R}[V]$ остатками по модулю $G = \{y^5 - x^2\}$ (G является базисом Грёбнера идеала $\mathbf{I}(V)$ по отношению к lex-упорядочению с $x > y$ в $\mathbb{R}[x, y]$). Тогда $\mathbb{R}[V] = \{a(y) + b(y)x \colon a, b \in \mathbb{R}[y]\}$ как векторное пространство

[1] Точнее говоря, элементами поля $QF(R)$ являются классы равных дробей; равенство определено двумя фразами ниже. — *Прим. ред.*

над $\mathbb{R}$, а умножение задано следующей формулой:

$$(a+bx)\cdot(c+dx) = (ac+y^5\cdot bd) + x(ad+bc). \tag{1}$$

В упр. 2 будет доказана неприводимость многообразия V; следовательно, $\mathbb{R}[V]$ является областью целостности.

Теперь, используя описание $\mathbb{R}[V]$, мы можем описать и поле функций $\mathbb{R}(V)$ следующим образом. Если $c+dx \neq 0$ в $\mathbb{R}[V]$, то элемент из $\mathbb{R}(V)$

$$\begin{aligned}\frac{a+bx}{c+dx} &= \frac{a+bx}{c+dx}\cdot\frac{c-dx}{c-dx}\\ &= \frac{(ac-y^5bd)+x(bc-ad)}{c^2-y^5d^2}\\ &= \frac{ac-y^5bd}{c^2-y^5d^2} + x\frac{bc-ad}{c^2-y^5d^2}\end{aligned}$$

принадлежит $\mathbb{R}(y) + x\mathbb{R}(y)$. Обратно, каждый элемент из $\mathbb{R}(y) + x\mathbb{R}(y)$ определяет элемент из $\mathbb{R}(V)$. Таким образом, поле $\mathbb{R}(V)$ может быть отождествлено с множеством функций $\mathbb{R}(y) + x\mathbb{R}(y)$, где сложение и умножение определены, как в $\mathbb{R}[V]$, только вместо полиномов используются рациональные функции от y.

Рассмотрим отображения

$$\begin{aligned}&\alpha : V \longrightarrow \mathbb{R}, \quad (x,y)\mapsto x/y^2,\\ &\beta : \mathbb{R} \longrightarrow V, \quad u \mapsto (u^5,u^2).\end{aligned}$$

Обратите внимание, что α определено всюду, кроме точки $(0,0)$ на V, в то время как β является полиномиальной параметризацией многообразия V. Как и в § 4, по α и β мы определим отображения функций, «действующие в противоположном направлении». Но так как α определено как рациональная функция, то его композиция с функцией из $\mathbb{R}[u]$ не будет элементом из $\mathbb{R}[V]$. Рассмотрим отображения

$$\begin{aligned}&\alpha^* : \mathbb{R}(u) \longrightarrow \mathbb{R}(V), \quad f(u)\mapsto f(x/y^2),\\ &\beta^* : \mathbb{R}(V) \longrightarrow \mathbb{R}(u), \quad a(y)+xb(y)\mapsto a(u^2)+u^5b(u^2).\end{aligned}$$

Мы утверждаем, что α^* и β^* — взаимно обратные кольцевые изоморфизмы. Тот факт, что α^* и β^* сохраняют суммы и произведения, доказывается так же, как аналогичный факт в предложении 8 из § 4. Проверим, что α^* и β^* взаимно обратны. Если $f(u)\in\mathbb{R}(u)$, то $\alpha^*(f) = f(x/y^2)$. Следовательно, $\beta^*(\alpha^*(f)) = f(u^5/(u^2)^2) = f(u)$. Поэтому $\beta^*\circ\alpha^*$ тождественно на $\mathbb{R}(u)$. Пусть теперь $a(y)+xb(y)\in\mathbb{R}(V)$. Тогда $\beta^*(a+xb) = a(u^2)+u^5b(u^2)$, так что

$$\begin{aligned}\alpha^*(\beta^*(a+xb)) &= a((x/y^2)^2) + (x/y^2)^5 b((x/y^2)^2)\\ &= a(x^2/y^4) + (x^5/y^{10})b(x^2/y^4).\end{aligned}$$

Но $x^2 = y^5$ в $\mathbb{R}(V)$; поэтому $x^2/y^4 = y$ и $x^5/y^{10} = xy^{10}/y^{10} = x$. Таким образом, отображение $\alpha^*\circ\beta^*$ тождественно на $\mathbb{R}(V)$. Поэтому α^*, β^* являются кольцевыми изоморфизмами *полей функций* $\mathbb{R}(V)$ и $\mathbb{R}(u)$.

Этот пример показывает, что неизоморфные многообразия могут иметь изоморфные поля функций. Здесь же приведен пример рационального отображения многообразий. Прежде чем давать точное определение рационального отображения, разберем еще один пример.

Пример 3. Рассмотрим однополостный гиперболоид $Q = \mathbf{V}(x^2+y^2-z^2-1)$ в $\mathbb{R}^3$, и пусть $W = \mathbf{V}(x+1)$ — плоскость $x=-1$. Рассмотрим точку $p = (1,0,0)\in Q$. Для любой точки $q\in Q-\{p\}$ построим прямую L_q, соединяющую p и q, и определим отображение ϕ поверхности Q в W, положив

$$\phi(q) = L_q \cap W,$$

если L_q пересекает W. (Если прямая не пересекает W, то $\phi(q)$ не определено.) Найдем алгебраическое выражение для ϕ. Если $q = (x_0,y_0,z_0)\in Q$, то L_q параметризована уравнениями

$$\begin{aligned}x &= 1+t(x_0-1),\\ y &= ty_0,\\ z &= tz_0.\end{aligned} \tag{2}$$

В точке $\phi(q) = L_q\cap W$ мы имеем $1+t(x_0-1) = -1$, т. е. $t = \frac{-2}{x_0-1}$. Тогда из (2) вытекает, что

$$\phi(q) = \left(-1, \frac{-2y_0}{x_0-1}, \frac{-2z_0}{x_0-1}\right). \tag{3}$$

Это показывает, что ϕ определено всюду на Q, кроме точек на двух прямых

$$Q\cap\mathbf{V}(x-1) = \{(1,t,t) : t\in\mathbb{R}\}\cup\{(1,t,-t) : t\in\mathbb{R}\}.$$

Мы будем называть $\phi : Q - \mathbf{V}_Q(x-1)\to W$ *рациональным отображением*, потому что его компоненты являются рациональными функциями. (Мы можем считать их также элементами из $\mathbb{R}(Q)$.)

С другой стороны, если $(-1, a, b) \in W$, то прямая L, проходящая через $p = (1, 0, 0)$ и $(-1, a, b)$, параметризуется уравнениями

$$\begin{aligned} x &= 1 - 2t, \\ y &= ta, \\ z &= tb. \end{aligned}$$

Тогда пересечение прямой L с Q состоит из двух точек

$$L \cap Q = \left\{ (1,0,0,), \left(\frac{a^2 - b^2 - 4}{a^2 - b^2 + 4}, \frac{4a}{a^2 - b^2 + 4}, \frac{4b}{a^2 - b^2 + 4} \right) \right\}.$$

Если мы обозначим через H гиперболу $\mathbf{V}_W(a^2 - b^2 + 4)$, то можем определить другое рациональное отображение

$$\psi : W - H \longrightarrow Q,$$

формулой

$$\psi(-1, a, b) = \left(\frac{a^2 - b^2 - 4}{a^2 - b^2 + 4}, \frac{4a}{a^2 - b^2 + 4}, \frac{4b}{a^2 - b^2 + 4} \right). \qquad (4)$$

Из описания отображений ϕ и ψ следует, что $\phi \circ \psi$ — тождественное отображение множества $W - H$ на себя. Аналогично, $\psi \circ \phi$ — это тождественное отображение $Q - \mathbf{V}_Q(x - 1)$ на себя. С помощью формул (3) и (4) можно показать, что $\phi^* \circ \psi^*$ и $\psi^* \circ \phi^*$ — тождественные отображения полей функций. (Следует упомянуть, что, как и во втором примере, Q и W *не* изоморфны как многообразия. Однако доказать это с использованием знакомой нам техники непросто.)

Сейчас мы дадим строгое определение тех понятий, которыми мы пользовались в предыдущих примерах.

Определение 4. Пусть $V \subset k^m$ и $W \subset k^n$ — неприводимые аффинные многообразия. *Рациональным отображением* многообразия V на W называется функция ϕ, представленная следующим образом:

$$\phi(x_1, \ldots, x_m) = \left(\frac{f_1(x_1, \ldots, x_m)}{g_1(x_1, \ldots, x_m)}, \ldots, \frac{f_n(x_1, \ldots, x_m)}{g_n(x_1, \ldots, x_m)} \right), \qquad (5)$$

где $f_i/g_i \in k(x_1, \ldots, x_m)$, и удовлетворяющая следующим условиям:

(i) ϕ определена хотя бы в одной точке из V;
(ii) для любой точки $(a_1, \ldots, a_m) \in V$, в которой ϕ определена, $\phi(a_1, \ldots, a_m) \in W$.

Обратите внимание, что рациональное отображение $\phi : V \to W$ может *не* быть функцией из V в W в обычном смысле, потому что, как мы уже видели в примерах выше, она не обязательно определена всюду на V. По этой причине некоторые авторы используют специальное обозначение для рационального отображения:

$$\phi : V - - \to W,$$

которого мы также будем придерживаться. По условию (i) множество точек, где рациональное отображение ϕ, заданное формулой (5), не определено, есть $\mathbf{V}_V(g_1, \ldots, g_n)$ — собственное подмногообразие многообразия V.

Так как рациональные отображения определены не всюду, то работа с ними требует некоторой осторожности. В частности, нам понадобится строгое определение того, что значит, что два рациональных отображения равны.

Определение 5. Пусть $\phi, \psi : V - - \to W$ — рациональные отображения, представленные формулами

$$\phi = \left(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n} \right) \quad \text{и} \quad \psi = \left(\frac{h_1}{l_1}, \ldots, \frac{h_n}{l_n} \right).$$

Тогда ϕ и ψ называются *равными*, если для любого i, $1 \le i \le n$,

$$f_i l_i - h_i g_i \in \mathbf{I}(V).$$

Рассмотрим геометрический критерий равенства рациональных отображений.

Предложение 6. *Два рациональных отображения $\phi, \psi : V - - \to W$ равны в том и только том случае, когда существует собственное подмногообразие $V' \subset V$, такое, что ϕ и ψ определены на $V - V'$ и $\phi(p) = \psi(p)$ для всех точек $p \in V - V'$.*

Доказательство. Пусть $\phi = (f_1/g_1, \ldots, f_n/g_n)$ и $\psi = (h_1/l_1, \ldots, h_n/l_n)$. Предположим, что ϕ и ψ равны в смысле определения 5, и пусть $V_1 = \mathbf{V}_V(g_1, \ldots, g_n)$ и $V_2 = \mathbf{V}_V(l_1, \ldots, l_n)$. По условию V_1 и V_2 — собственные подмногообразия многообразия V, а так как V неприводимо, то и $V' = V_1 \cup V_2$ также собственное подмногообразие в V. Тогда ϕ и ψ определены на $V - V'$, а так как $f_i l_i - h_i g_i \in \mathbf{I}(V)$, то f_i/g_i и h_i/l_i представляют одну и ту же функцию на $V - V'$. Значит, то же самое верно для ϕ и ψ.

С другой стороны, пусть ϕ и ψ определены и равны (как функции) на $V - V'$. Это означает, что $f_i/g_i = h_i/l_i$ на $V - V'$ для каждого i. Но тогда $f_i l_i - h_i g_i$ равны нулю на $V - V'$; значит, $V = \mathbf{V}_V(f_i l_i - h_i g_i) \cup V'$. Так как V неприводимо, а V' — собственное подмногообразие, то $V = \mathbf{V}_V(f_i l_i - h_i g_i)$. Таким образом, $f_i l_i - h_i g_i \in \mathbf{I}(V)$. □

В примере 3 мы определили рациональные отображения $\phi : Q \dashrightarrow W$ и $\psi : W \dashrightarrow Q$, такие, что $\psi \circ \phi$ тождественно на $W - H \subset W$. По предложению 6 это доказывает, что $\psi \circ \phi$ равно id_W в смысле определения 5.

Надо также соблюдать осторожность при определении композиции рациональных отображений.

Определение 7. Пусть даны отображения $\phi : V \dashrightarrow W$ и $\psi : W \dashrightarrow Z$. Мы говорим, что *композиция* $\psi \circ \phi$ *определена*, если существует точка $p \in V$, такая, что ϕ определено в p и ψ определено в $\phi(p)$.

Если композиция $\psi \circ \phi$ определена, то она является рациональным отображением, как показывает следующее утверждение:

Предложение 8. *Пусть $\phi : V \dashrightarrow W$ и $\psi : W \dashrightarrow Z$ — рациональные отображения, такие, что композиция $\psi \circ \phi$ определена. Тогда существует собственное подмногообразие $V' \subset V$, такое, что*

(i) *ϕ определено на $V - V'$ и ψ определено на $\phi(V - V')$;*
(ii) *$\psi \circ \phi : V \dashrightarrow Z$ — рациональное отображение, определенное на $V - V'$.*

Доказательство. Пусть ϕ и ψ имеют следующие представления:

$$\phi(x_1, \ldots, x_m) = \left(\frac{f_1(x_1, \ldots, x_m)}{g_1(x_1, \ldots, x_m)}, \ldots, \frac{f_n(x_1, \ldots, x_m)}{g_n(x_1, \ldots, x_m)} \right),$$

$$\psi(y_1, \ldots, y_n) = \left(\frac{h_1(y_1, \ldots, y_n)}{l_1(y_1, \ldots, y_n)}, \ldots, \frac{h_s(y_1, \ldots, y_n)}{l_s(y_1, \ldots, y_n)} \right).$$

Тогда j-я координата отображения $\psi \circ \phi$ равна

$$\frac{h_j(f_1/g_1, \ldots, f_n/g_n)}{l_j(f_1/g_1, \ldots, f_n/g_n)}$$

и, очевидно, является рациональной функцией от $x_1, \ldots, x_m$. Чтобы представить ее в виде частного полиномов, мы должны записать ее в виде

$$\frac{P_j}{Q_j} = \frac{(g_1 \ldots g_n)^M h_j(f_1/g_1, \ldots, f_n/g_n)}{(g_1 \ldots g_n)^M l_j(f_1/g_1, \ldots, f_n/g_n)},$$

где M достаточно велико.

Положим

$$V' = \mathbf{V}_V([Q_1], \ldots, [Q_s], [g_1 \ldots g_n]) \subset V.$$

Очевидно, что ϕ определена на $V - V'$ и ψ определена на $\phi(V - V')$. Осталось доказать, что $V \neq V'$. По условию существует точка $p \in V$,

такая, что ϕ определено в p, а ψ определено в $\phi(p)$. Это означает, что $g_i(p) \neq 0$ при $1 \leq i \leq n$ и

$$l_j(f_1(p)/g_1(p), \ldots, f_n(p)/g_n(p)) \neq 0$$

для всех $1 \leq j \leq s$. Но тогда $Q_j(p) \neq 0$ и, следовательно, $p \in V - V'$. □

В упражнениях мы рассмотрим пример, когда композиция $\psi \circ \phi$ не определена. Это происходит в тех случаях, когда область определения отображения ψ не пересекается с образом отображения ϕ.

Примеры 2 и 3 продемонстрировали нам, что есть альтернатива понятию *изоморфизма* многообразий.

Определение 9.

(i) Два неприводимых многообразия $V \subset k^m$ и $W \subset k^n$ называются *бирационально эквивалентными*, если существуют рациональные отображения $\phi : V \dashrightarrow W$ и $\psi : W \dashrightarrow V$, такие, что композиции $\psi \circ \phi$ и $\phi \circ \psi$ определены (в смысле определения 7) и равны (в смысле определения 5) тождественным отображениям id_V и id_W соответственно.
(ii) Многообразие называется *рациональным многообразием*, если оно бирационально эквивалентно пространству k^n для некоторого n.

Рассмотрение координатных колец может помочь при доказательстве изоморфности многообразий. Точно так же рассмотрение полей функций может помочь при доказательстве их бирациональной эквивалентности.

Теорема 10. *Два неприводимых многообразия V и W бирационально эквивалентны в том и только том случае, когда существует изоморфизм $k(V) \cong k(W)$ их полей функций, тождественный на константах. (По определению два поля изоморфны, если они изоморфны как коммутативные кольца.)*

Доказательство. Доказательство этой теоремы аналогично доказательству теоремы 8 из § 4. Предположим, что V и W бирационально эквивалентны и $\phi : V \dashrightarrow W$ и $\psi : W \dashrightarrow V$ — соответствующие отображения. Определим отображение $\phi^* : k(W) \to k(V)$ формулой $\phi^*(f) = f \circ \phi$ и докажем, что это изоморфизм. В отличие от полиномиального случая здесь не очевидно, что $\phi^*(f) = f \circ \phi$ существует для всех $f \in k(W)$ — нам нужно доказать, что функция $f \circ \phi$ определена в некоторой точке многообразия V.

Сначала мы докажем, что из условия $\phi \circ \psi = \mathrm{id}_W$ вытекает существование собственного подмногообразия $W' \subset W$, такого, что

$$\begin{aligned} &\psi \text{ определено на } W - W', \\ &\phi \text{ определено на } \psi(W - W'), \\ &\phi \circ \psi \text{ тождественно на } W - W'. \end{aligned} \tag{6}$$

Для этого мы найдем собственное подмногообразие $W_1 \subset W$, такое, что ψ определено на $W - W_1$, а ϕ определено на $\psi(W - W_1)$ (предложение 8). По предложению 6 существует собственное подмногообразие $W_2 \subset W$, такое, что $\phi \circ \psi$ тождественно на $W - W_2$. Так как W неприводимо, то $W' = W_1 \cup W_2$ — собственное подмногообразие, которое и удовлетворяет условиям (6).

Пусть $f \in k(W)$. Теперь мы можем доказать, что композиция $f \circ \phi$ определена. Если f определена на $W - W'' \subset W$, то $W' \cup W'' \neq W$, потому что W неприводимо. Пусть $q \in W - (W' \cup W'')$. Тогда по (6) отображение ϕ определено в точке $p = \psi(q) \in V$, а так как $\phi(p) = q \notin W''$, то f определена в $\phi(p)$. Значит, по определению 5 функция $\phi^*(f) = f \circ \phi$ существует как элемент из $k(V)$.

Это рассуждение доказывает существование отображения $\phi^* : k(W) \to k(V)$. Кроме того, из доказательства предложения 8 из § 4 вытекает, что ϕ^* является кольцевым гомоморфизмом. Аналогично может быть построен и кольцевой гомоморфизм $\psi^* : k(V) \to k(W)$. Покажем, что эти отображения взаимно обратны. Рассмотрим функцию

$$(\psi^* \circ \phi^*)(f) = f \circ \phi \circ \psi,$$

где $f \in k(W)$. В наших обозначениях функция $f \circ \phi \circ \psi$ равна f как функция на множестве $W - (W' \cup W'')$; поэтому $f \circ \phi \circ \psi = f$ в $k(W)$ по предложению 6. Это показывает, что $\psi^* \circ \phi^* = \mathrm{id}_{k(W)}$. Аналогично доказывается равенство $\phi^* \circ \psi^* = \mathrm{id}_{k(V)}$. Таким образом, $\phi^* : k(W) \to k(V)$ является изоморфизмом полей. Мы оставляем читателю в качестве упражнения доказательство того, что ϕ^* тождественно на постоянных функциях $k \subset k(W)$.

Доказательство обратного утверждения мы оставляем читателю в качестве упражнения. Отметим только, что это доказательство аналогично доказательству теоремы 9 из § 4. □

В упражнениях мы докажем, что два неприводимых многообразия бирационально эквивалентны, если существуют «большие» подмножества (дополнения до собственных подмногообразий), между которыми можно установить взаимно однозначное соответствие с помощью рациональных отображений. Например, кривая $V = \mathbf{V}(y^5 - x^2)$ из примера 2 бирационально эквивалентна многообразию $W = \mathbb{R}$. Следует проверить, что рациональные отображения f и g из (1) устанавливают взаимно однозначное соответствие между множествами $V - \{(0,0)\}$ и $W - \{0\}$. Аналогично устанавливается бирациональная эквивалентность между гиперболоидом и плоскостью из примера 3. Эти примеры показывают, что вне указанных «больших» подмножеств бирационально эквивалентные многообразия могут быть совсем непохожи (см. упр. 14).

Как видно из примеров, бирациональная эквивалентность неприводимых многообразий — это *более слабое* отношение эквивалентности, чем изоморфизм. Под этим мы понимаем следующее: класс бирационально эквивалентных многообразий может содержать много неизоморфных многообразий. Тем не менее в истории алгебраической геометрии именно классификация многообразий с точностью до бирациональной эквивалентности привлекала большее внимание, возможно, потому, что строить рациональные функции на многообразии проще, чем полиномиальные[1]. Существует почти полная классификация многообразий в размерностях 1 и 2 с точностью до бирациональной эквивалентности. И недавно значительный прогресс был достигнут в размерности 3. Однако классификация неприводимых многообразий размерности ≥ 4 с точностью до бирациональной эквивалентности неполна и является областью активных исследований.

Упражнения к § 5

1. Пусть R — область целостности, а $QF(R)$ — ее поле частных.
   (a) Докажите, что сложение корректно определено в $QF(R)$. Это означает, что если $r/s = r'/s'$ и $t/u = t'/u'$, то $(ru+ts)/su = (r'u' + t's')/s'u'$. Указание: вспомните, как определяется равенство двух элементов из $QF(R)$.
   (b) Докажите, что умножение в $QF(R)$ определено корректно.
   (c) Докажите, что в $QF(R)$ выполнены аксиомы поля.
2. Пусть $V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$, как в примере 2.
   (a) Докажите, что полином $y^5 - x^2$ неприводим в $R[x, y]$ и что $\mathbf{I}(V) = \langle y^5 - x^2 \rangle$.
   (b) Выведите из этого, что $\mathbb{R}[V]$ является областью целостности.

[1] Исторические истоки можно усмотреть в том, что алгебраическая геометрия возникла как теория алгебраических кривых, мощным стимулом для развития которой послужила та ветвь анализа, в которой изучались интегралы от рациональных функций (на эллиптических кривых). См. Клейн Ф. Лекции о развитии математики в XIX столетии, т. I. — М.: Наука, 1989, и исторический очерк в книге: Shafarevich (1974) (см. список литературы). — *Прим. ред.*

3. Используя рассуждения из примера 2, докажите, что особая кубическая кривая $\mathbf{V}(y^2 - x^3)$ является рациональным многообразием (бирационально эквивалентным k).
4. Рассмотрим особую кубическую кривую $V_c = \mathbf{V}(y^2 - cx^2 + x^3)$ (см. упр. 8 к § 3 гл. 1). Используя параметризацию, приведенную в этом упражнении, докажите, что V_c — рациональное многообразие, и найдите подмногообразия $V_c' \subset V_c$ и $W \subset k$, такие, что найденные вами рациональные отображения определяют взаимно однозначное соответствие между $V_c - V_c'$ и $k - W$. Указания: напомним, что t в параметризации кривой V_c является коэффициентом наклона некоторой прямой, проходящей через точку $(0, 0)$.
5. Докажите, что кривая $\pi(C)$ из упр. 7 к § 4 — рациональное многообразие. Указание: для того чтобы найти рациональное отображение, обратное параметризации, полученной в этом выражении, нужно выразить t как функцию от координат x и y на кривой. Здесь следует использовать уравнение гиперболы.
6. В примере 3 проверьте непосредственно, что (3) и (4) являются взаимно обратными рациональными отображениями однополостного гиперболоида и плоскости друг в друга.
7. Пусть $S = \mathbf{V}(x^2 + y^2 + z^2 - 1) \subset \mathbb{R}^3$ и $W = \mathbf{V}(z)$ — плоскость xy. В этом упражнении мы докажем, что S и W бирационально эквивалентны, явно построив отображение, называемое стереографической проекцией. См. также упр. 6 к § 3 гл. 1.
   (a) Найдите параметрические уравнения (как в (2)) прямой L_q в $\mathbb{R}^3$, соединяющей северный полюс сферы — точку $(0, 0, 1)$ — и произвольную точку $q = (x_0, y_0, z_0) \in S, q \neq (0, 0, 1)$.
   (b) Теперь определите рациональное отображение $\phi : S - - \to W$, положив $\phi(q) = L_q \cap W$. Это и есть отображение стереографической проекции.
   (c) Докажите, что рациональная параметризация многообразия S, приведенная в упр. 6 к § 3 гл. 1, представляет собой отображение ψ, обратное к ϕ.
   (d) Докажите, что S и W бирационально эквивалентны, и найдите подмногообразия $S' \subset S$ и $W' \subset W$, такие, что отображения ϕ и ψ определяют взаимно однозначное соответствие между $S - S'$ и $W - W'$.
8. В упр. 10 к § 1 мы доказали, что не существует непостоянных полиномиальных отображений из $\mathbb{R}$ в $V = \mathbf{V}(y^2 - x^3 + x)$. Существуют ли непостоянные *рациональные* отображения? Является ли V бирационально эквивалентным $\mathbb{R}$?
9. Пусть V — неприводимое многообразие и $f \in k(V)$. Если $f = \phi/\psi$, где $\phi, \psi \in k[V]$, то f определена на $V - \mathbf{V}_V(\psi)$. Интересно отметить, что иногда f можно определить и на большем множестве. В этом упражнении мы рассмотрим, как это может происходить на многообразии $V = \mathbf{V}(xz - yw) \subset \mathbb{C}^4$.

   (a) Докажите, что полином $xz - yw \in \mathbb{C}[x, y, z, w]$ неприводим. Указание: обратите внимание на полные степени возможных делителей.
   (b) Используя единственность разложения на множители в $\mathbb{C}[x, y, z, w]$, докажите, что $\langle xz - yw \rangle$ является простым идеалом.
   (c) Докажите, что V неприводимо и $\mathbf{I}(V) = \langle xz - yw \rangle$.
   (d) Пусть $f = [x]/[y] \in \mathbb{C}[V]$, так что функция f определена на $V - \mathbf{V}_V([y])$. Докажите, что $\mathbf{V}_V([y])$ является объединением плоскостей $\{(0, 0, z, w) : z, w \in \mathbb{C}\} \cup \{(x, 0, 0, w) : x, w \in \mathbb{C}\}$.
   (e) Докажите, что $f = [w]/[x]$ и покажите, что тем самым f определена везде в дополнении к плоскости $\{(x, 0, 0, w) : x, w \in \mathbb{C}\}$.

   Отметим, что это оказалось возможным, потому что существуют два совершенно различных представления рациональной функции f. Это также объясняет, почему работа с рациональными функциями требует осторожности.
10. Рассмотрим рациональные отображения $\phi : \mathbb{R} - - \to \mathbb{R}^3$ и $\psi : \mathbb{R}^3 - - \to \mathbb{R}$, определенные формулами

$$\phi(t) = (t, 1/t, t^2) \qquad \text{и} \qquad \psi(x, y, z) = \frac{x + yz}{x - yz}.$$

    Докажите, что композиция $\psi \circ \phi$ не определена.
11. Завершите доказательство теоремы 10, показав, что если V и W — неприводимые многообразия и существует изоморфизм $k(V) \cong k(W)$ их полей функций, тождественный на константах, то также существуют взаимно обратные рациональные отображения $\phi : V - - \to W$ и $\psi : W - - \to V$. Указание: следуйте доказательству теоремы 9 из § 4.
12. Пусть $\phi : V - - \to W$ — рациональное отображение, определенное на $V - V'$. Рассмотрим подмногообразие $W' \subset W$. Докажите, что

$$V'' = V' \cup \{p \in V - V' : \phi(p) \in W'\}$$

    является подмногообразием в V. Указание: найдите уравнения, определяющие V'', следующим образом: подставьте рациональные функции, представляющие ϕ, в уравнения, определяющие W', и приравняйте нулю числители получившихся функций.
13. Пусть рациональные отображения $\phi : V - - \to W$ и $\psi : W - - \to V$ определяют бирациональную эквивалентность многообразий V и W. Как отмечалось в тексте параграфа после доказательства теоремы 10, это означает, что существуют «большие» подмножества в V и W, которые «одинаковы». Точнее, существуют собственные подмногообразия $V_1 \subset V$ и $W_1 \subset W$, такие, что ϕ и ψ определяют взаимно обратные биекции между подмногообразиями $V - V_1$ и $W - W_1$ друг на друга. Отметим, что в упр. 4 и 7 рассматривались частные случаи этого утверждения.
    (a) Пусть $V' \subset V$ — подмногообразие, удовлетворяющее условиям (6) для отображения $\phi \circ \psi$. Аналогично, пусть $W' \subset W$ удовлетворяет

условиям (6) для $\psi \circ \phi$. Пусть

$$\mathcal{V} = \{p \in V - V' : \phi(p) \in W - W'\},$$
$$\mathcal{W} = \{q \in W - W' : \psi(q) \in V - V'\}.$$

Докажите, что $\phi : \mathcal{V} \to \mathcal{W}$ и $\psi : \mathcal{W} \to \mathcal{V}$ являются взаимно обратными биекциями.

(b) Используя упр. 12, докажите, что $\mathcal{V} = V - V_1$ и $\mathcal{W} = W - W_1$, где V_1 и W_1 — собственные подмногообразия.

Пункты (a) и (b) и определяют требуемую биекцию между «большими» подмножествами многообразий V и W.

14. В примере 3 мы рассматривали рациональные отображения $\phi : Q - - \to W$ и $\psi : W - - \to Q$.

(a) Докажите, что ϕ и ψ определяют взаимно обратные биекции $\phi : Q - \mathbf{V}_Q(x-1) \to W - H$ и $\psi : W - H \to Q - \mathbf{V}_Q(x-1)$, где $H = \mathbf{V}_W(a^2 - b^2 + 4)$.

(b) Докажите, что многообразия H и $\mathbf{V}_Q(x-1)$ совершенно различны: они не изоморфны и не бирационально эквивалентны.

§ 6. Дополнение. Доказательство теоремы о замыкании

В этом параграфе мы завершим доказательство теоремы о замыкании, которое было начато в § 2 гл. 3. Мы будем использовать понятия и методы, введенные в гл. 4 и 5, в том числе неприводимые многообразия, простые идеалы, факторкольца и поля частных.

Напомним, о чем, собственно, идет речь. Пусть поле k алгебраически замкнуто, а $\pi_l : k^n \to k^{n-l}$ — проекция на последние $n-l$ компонент. Пусть $V = \mathbf{V}(I)$ — аффинное многообразие в k^n и $I_l = I \cap k[x_{l+1}, \ldots, x_n]$ — его l-й исключающий идеал. В § 4 гл.4 мы доказали первую часть теоремы о замыкании, которая утверждает, что $\mathbf{V}(I_l)$ является наименьшим многообразием в k^{n-l}, содержащим $\pi_l(V)$. На языке гл. 4 это означает, что $\mathbf{V}(I_l)$ является замыканием Зарисского множества $\pi_l(V)$.

Последняя часть теоремы о замыкании утверждает, что $\pi_l(V)$ составляет «бóльшую часть» многообразия $\mathbf{V}(I_l)$ в следующем смысле.

Теорема 1 (теорема о замыкании, вторая часть). *Пусть k алгебраически замкнуто, а $V = \mathbf{V}(I) \subset k^n$. Если $V \neq \varnothing$, то существует аффинное многообразие W, строго содержащееся в $\mathbf{V}(I_l)$, такое, что*

$$\mathbf{V}(I_l) - W \subset \pi_l(V).$$

Доказательство. В гл. 3 мы доказали это утверждение в случае $l = 1$ с помощью результантов. Прежде чем приступать к доказательству общего утверждения, отметим, что $\mathbf{V}(I_l)$ зависит только от V, так как является замыканием Зарисского множества $\pi_l(V)$. Это означает, что для *любого* идеала, определяющего V, многообразие $\mathbf{V}(I_l)$ одно и то же. В частности, так как $V = \mathbf{V}(\mathbf{I}(V))$, то мы можем взять $\mathbf{I}(V)$ вместо I. Следовательно, если V неприводимо, то мы можем считать идеал I простым.

Мы начнем доказательство с рассмотрения неприводимого случая. Следующие факты нам будут полезны:

$$\begin{aligned} I \text{ прост} &\implies I_l \text{ прост}, \\ V \text{ неприводимо} &\implies \mathbf{V}(I_l) \text{ неприводимо}. \end{aligned} \tag{1}$$

Доказательство первого утверждения несложно, и мы оставляем его читателю. Докажем второе. Мы можем считать, что $I = \mathbf{I}(V)$, а следовательно, считать I простым. Тогда I_l также прост. Значит (см. алгебро-геометрический словарь в следствии 4 из § 5 гл. 4), $\mathbf{V}(I_l)$ неприводимо.

Пусть V неприводимо. Индукцией по l мы докажем более сильное утверждение, чем утверждение теоремы. Если $W_0 \subsetneq V$ — собственное подмногообразие, то существует собственное подмногообразие $W_l \subsetneq \mathbf{V}(I_l)$, такое, что

$$\mathbf{V}(I_l) - W_l \subset \pi_l(V - W_0). \tag{2}$$

(Утверждение теоремы соответствует случаю $W_0 = \varnothing$.) Начнем со случая $l = 1$. Так как $W_0 \neq V$, то найдется точка $(a_1, \ldots, a_n) \in V - W_0$. Тогда существует полином $f \in \mathbf{I}(W_0)$, такой, что $f(a_1, \ldots, a_n) \neq 0$. Полином f будет играть решающую роль в дальнейшем доказательстве. Теперь надо рассмотреть два случая.

Случай I. Предположим, что *для всех* $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ имеет место включение $(b_1, b_2, \ldots, b_n) \in V$ *для всех* $b_1 \in k$. Запишем f как полином от x_1:

$$f = \sum_{i=0}^{m} g_i(x_2, \ldots, x_n) x_1^i.$$

Пусть $W_1 = \mathbf{V}(I_1) \cap \mathbf{V}(g_0, \ldots, g_m)$. Это многообразие строго меньше, чем $\mathbf{V}(I_1)$, потому что из условия $f(a_1, \ldots, a_n) \neq 0$ следует, что $g_i(a_2, \ldots, a_n) \neq 0$ для некоторого i. Тогда $(a_2, \ldots, a_n) \in \mathbf{V}(I_1) - W_1$, так что $W_1 \neq \mathbf{V}(I_1)$.

Теперь покажем, что (2) выполнено. Если $(c_2, \ldots, c_n) \in \mathbf{V}(I_1) - W_1$, то некоторый полином g_i не равен нулю в точке $(c_2, \ldots, c_n)$; поэтому $f(x_1, c_2, \ldots, c_n)$ — ненулевой полином. Так как k бесконечно

(упр. 4 к § 1 гл. 4), то найдется $c_1 \in k$, такое, что $f(c_1, c_2, \ldots, c_n) \neq 0$. Но по условию $(c_1, \ldots, c_n) \in V$. Однако эта точка не принадлежит W_0, так как $f \in \mathbf{I}(W_0)$. Значит, $(c_2, \ldots, c_n) \in \pi_1(V - W_0)$, что и доказывает (2) в случае I.

Случай II. Предположим, что *существует* точка $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ и *существует* $b_1 \in k$, такие, что $(b_1, b_2, \ldots, b_n) \notin V$. Тогда мы можем найти полином $h \in I$, такой, что $h(b_1, \ldots, b_n) \neq 0$ (h существует, потому что $I = \mathbf{I}(V)$). Запишем h как полином от x_1:

$$h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n) x_1^i. \tag{3}$$

Так как $h(b_1, \ldots, b_n) \neq 0$, то $u_i(b_2, \ldots, b_n) \neq 0$ для некоторого i. Тогда $u_i \notin I_1$. Более того, если $u_r \in I_1$, то полином $h - u_r x_1^r$ не равен нулю в точке $(b_2, \ldots, b_n)$. Поэтому мы можем заменить h на $h - u_r x_1^r$. Повторяя эту процедуру, мы можем добиться того, что $u_r \notin I_1$ в (3).

Теперь мы хотим доказать следующее утверждение:

$$\text{существуют } v_i \in k[x_2, \ldots, x_n], \text{ такие, что } \sum_{i=0}^{r} v_i f^i \in I \text{ и } v_0 \notin I_1. \tag{4}$$

Для этого, рассматривая f и h как полиномы от x_1, поделим f на h. Но вместо того чтобы прямо использовать алгоритм деления из § 5 гл. 1, мы сначала заменим f на $u_r^{N_1} f$, где N_1 — натуральное число. Мы утверждаем, что если N_1 достаточно велико, то мы можем поделить $u_r^{N_1} f$ на h, не прибегая к дробям. Другими словами,

$$u_r^{N_1} f = qh + v_{10} + v_{11} x_1 + \ldots + v_{1,r-1} x_1^{r-1},$$

где $q \in k[x_1, \ldots, x_n]$ и $v_{1i} \in k[x_2, \ldots, x_n]$. Доказательство этого факта мы оставляем читателю (упр. 2). Читатель может также ознакомиться с результатами § 5 гл. 6, где этот процесс *псевдоделения* изучается подробнее. Теперь проведем этот процесс «деления» не только для f, но и для всех степеней $1, f, f^2, \ldots, f^r$. Тогда мы получим уравнения вида

$$u_r^{N_j} f^j = q_j h + v_{j0} + v_{j1} x_1 + \ldots + v_{j.r-1} x_1^{r-1} \tag{5}$$

для всех $0 \leq j \leq r$.

Перейдем к факторкольцам и полям частных. Так как $I_1 = \mathbf{I}(\mathbf{V}(I_1))$, то (см. § 2) факторкольцо $k[x_2, \ldots, x_n]/I_1$ естественно изоморфно координатному кольцу $k[\mathbf{V}(I_1)]$. Это кольцо является областью целостности, так как многообразие $\mathbf{V}(I_1)$ неприводимо. Следовательно, мы можем построить его поле частных, которое обозначим через K. Факторкольцо $k[x_2, \ldots, x_n]/I_1$ мы будем считать

вложенным в K, так что полиному $v \in k[x_2, \ldots, x_n]$ отвечает элемент $[v] \in k[x_2, \ldots, x_n]/I_1 \subset K$. В частности, нулевой элемент в K есть $[0]$, где $0 \in k[x_2, \ldots, x_n]$ — нулевой полином.

Полиномы v_{ij} из (5) задают элементы $(r+1) \times r$-матрицы

$$\begin{pmatrix} [v_{00}] & \ldots & [v_{0.r-1}] \\ \vdots & & \vdots \\ [v_{r0}] & \ldots & [v_{r.r-1}] \end{pmatrix}$$

с элементами из K. Строки этой матрицы (их $r+1$) можно рассматривать как векторы в r-мерном пространстве K^r. Следовательно, строки линейно зависимы над K. Таким образом, существуют элементы $\phi_0, \ldots, \phi_r \in K$, не все равные нулю, такие, что $\sum_{j=0}^{r} \phi_j [v_{ji}] = [0]$ в K для всех $0 \leq i \leq r-1$. Запишем каждое ϕ_j как частное элементов из $k[x_2, \ldots, x_n]/I_1$, умножим на общий знаменатель и будем считать, что $\phi_j = [w_j]$, где $w_j \in k[x_2, \ldots, x_n]$. Так как не все ϕ_j равны нулю в $k[x_2, \ldots, x_n]/I_1 \subset K$, то найдется $w_j \notin I_1$. Имеем

$$\sum_{j=0}^{r} [w_j][v_{ji}] = [0],$$

а это означает, что

$$\sum_{j=0}^{r} w_j v_{ji} \in I_1. \tag{6}$$

Наконец, если мы умножим каждое из уравнений (5) на соответствующий элемент w_j и сложим их, то, учитывая (6) и принадлежность $h \in I$, получим, что

$$\sum_{j=0}^{r} w_j u_r^{N_j} f^j \in I.$$

Положим $v_j = w_j u_r^{N_j}$. Так как $u_r \notin I_1$ и $w_j \notin I_1$ для некоторых j, то $v_j \notin I_1$ для некоторых j, потому что по (1) идеал I_1 прост.

Осталось добиться того, чтобы $v_0 \notin I_1$. Предположим, что $v_0, \ldots, v_{t-1} \in I_1$, но $v_t \notin I_1$. Тогда

$$f^t \sum_{j=t}^{r} v_j f^{j-t} \in I.$$

Так как идеал I прост и $f \notin I$, то $\sum_{j=t}^{r} v_j f^{j-t} \in I$. Теперь мы можем считать, что индекс меняется от 0 до $r-t$ и v_t играет роль v_0, и тем самым получаем формулу (4).

Важным следствием условия (4) является такой решающий факт:

$$\pi_1(V) \cap (k^{n-1} - \mathbf{V}(v_0)) \subset \pi_1(V - W_0). \tag{7}$$

Докажем это. Так как $\sum_{i=0}^{r} v_i f^i \in I$, то для любой точки $(c_1, \ldots, c_n) \in V$ имеем

$$v_0(c_2, \ldots, c_n) + f(c_1, \ldots, c_n) \sum_{i=1}^{r} v_i(c_2, \ldots, c_n) f(c_1, \ldots, c_n)^{i-1} = 0.$$

Если $v_0(c_2, \ldots, c_n) \neq 0$, то $f(c_1, \ldots, c_n) \neq 0$, а следовательно, $(c_1, \ldots, c_n) \notin W_0$ (так как f обращается в нуль на W_0). Отсюда вытекает (7).

Теперь мы можем доказать (2) в случае II. Так как $u_r, v_0 \notin I_1$ и I_1 прост, то $g = u_r v_0 \notin I_1$. Тогда $W_1 = \mathbf{V}(g) \cap \mathbf{V}(I_1) \subsetneqq \mathbf{V}(I_1)$. Пусть $(c_2, \ldots, c_n) \in \mathbf{V}(I_1) - W_1$. Это означает, что и u_r, и v_0 не равны нулю в этой точке.

Пусть $I = \langle f_1, \ldots, f_s \rangle$ и $h \in I$. Тогда $I = \langle h, f_1, \ldots, f_s \rangle$. Так как $u_r(c_2, \ldots, c_n) \neq 0$, то по теореме о замыкании, доказанной в гл. 3 для случая $l = 1$, существует точка $(c_1, c_2, \ldots, c_n) \in V$. Тогда в силу (7) и того, что $v_0(c_2, \ldots, c_n) \neq 0$, имеет место включение $(c_2, \ldots, c_n) \in \pi_1(V - W_0)$. Таким образом, утверждение (2) доказано для случая $l = 1$. В упражнениях будет прояснен геометрический смысл случаев I и II.

Пусть теперь (2) выполнено для $l - 1$. Докажем, что это утверждение выполняется для l. Рассмотрим многообразие W_0, строго содержащееся в V, и найдем W_1, строго содержащееся в $\mathbf{V}(I_1)$, такое, что

$$\mathbf{V}(I_1) - W_1 \subset \pi_1(V - W_0).$$

Но I_l является $(l-1)$-м исключающим идеалом идеала I_1. Кроме того, многообразие $\mathbf{V}(I_1)$ неприводимо по (1). Следовательно, по предположению индукции, примененному к $W_1 \subsetneqq \mathbf{V}(I_1)$, существует $W_l \subsetneqq \mathbf{V}(I_l)$, такое, что

$$\mathbf{V}(I_l) - W_l \subset \tilde{\pi}_{l-1}(\mathbf{V}(I_1) - W_1),$$

где $\tilde{\pi}_{l-1} : k^{n-1} \to k^{n-l}$ — проекция на последние $(n-1)-(l-1) = n-l$ компонент. Но так как $\pi_l = \tilde{\pi}_{l-1} \circ \pi_1$ (см. упр. 4), то

$$\mathbf{V}(I_l) - W_l \subset \tilde{\pi}_{l-1}(\mathbf{V}(I_1) - W_1) \subset \tilde{\pi}_{l-1}(\pi_1(V - W_0)) = \pi_l(V - W_0),$$

что и завершает доказательство утверждения (2) для неприводимых многообразий.

Теперь рассмотрим общий случай. Пусть $V \subset k^n$ — произвольное многообразие. Представим V в виде объединения неприводимых

компонент (теорема 2 из § 6 гл. 4):

$$V = V_1 \cup \ldots \cup V_m.$$

Обозначим через V_i' замыкание Зарисского множества $\pi_l(V_i) \subset k^{n-l}$. Мы утверждаем, что

$$\mathbf{V}(I_l) = V_1' \cup \ldots \cup V_m'. \tag{8}$$

Для доказательства заметим, что $V_1' \cup \ldots \cup V_m'$ — многообразие, содержащее множество $\pi_l(V_1) \cup \ldots \cup \pi_l(V_m) = \pi_l(V)$. Так как $\mathbf{V}(I_l)$ — это замыкание Зарисского множества $\pi_l(V)$, то $\mathbf{V}(I_l) \subset V_1' \cup \ldots \cup V_m'$. С другой стороны, заметим, что $\pi_l(V_i) \subset \pi_l(V) \subset \mathbf{V}(I_l)$ для каждого i. Следовательно, $V_i' \subset \mathbf{V}(I_l)$, так как V_i' — замыкание Зарисского множества $\pi_l(V_i)$. Таким образом, (8) доказано.

Из (1) мы знаем, что многообразия V_i' неприводимы; значит, (8) — это разложение многообразия $\mathbf{V}(I_l)$ в объединение неприводимых. Это разложение не обязательно является минимальным, но все-таки мы можем найти одно из этих многообразий, не принадлежащее никакому другому. Мы можем считать, что V_1' не принадлежит никакому V_i' при $2 \leq i \leq m$.

Тогда по формуле (2), примененной к неприводимому многообразию V_1 (здесь $W_0 = \varnothing$), существует неприводимое многообразие $W_1 \subsetneqq V_1'$, такое, что

$$V_1' - W_1 \subset \pi_l(V_1)$$

(так как V_1' является замыканием Зарисского множества $\pi_l(V_1)$). Пусть $W = W_1 \cup V_2' \cup \ldots \cup V_m'$. Тогда $W \subset \mathbf{V}(I_l)$ и

$$\begin{aligned} \mathbf{V}(I_l) - W &= V_1' \cup \ldots \cup V_m' - (W_1 \cup V_2' \cup \ldots \cup V_m') \\ &\subset V_1' - (W \cup V_2' \cup \ldots \cup V_m') \\ &\subset V_1' - W_1 \subset \pi_l(V_1) \subset \pi_l(V). \end{aligned}$$

Осталось показать, что $W \neq \mathbf{V}(I_l)$. Но если $W = \mathbf{V}(I_l)$, то $V_1' \subset W_1 \cup V_2' \cup \ldots \cup V_m'$. Так как V_1' неприводимо, то V_1' принадлежит одному из многообразий $W_1, V_2', \ldots, V_m'$ (см. упр. 5). Но это противоречит выбору V_1' и W_1. Мы пришли к противоречию, и теорема доказана. □

Теорема о замыкании позволяет дать точное описание проекции $\pi_l(V)$.

Следствие 2. *Пусть поле k алгебраически замкнуто и $V \subset k^n$ — аффинное многообразие. Тогда существуют аффинные многообразия $Z_i \subset W_i \subset k^{n-l}, 1 \leq i \leq p$, такие, что*

$$\pi_l(V) = \bigcup_{i=1}^{p} (W_i - Z_i).$$

Доказательство. Положим $W_1 = \mathbf{V}(I_l)$. По теореме о замыкании существует подмногообразие $Z_1 \subsetneqq W_1$, такое, что $W_1 - Z_1 \subset \pi_l(V)$. Теперь в k^n определим множество

$$V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n : (a_{l+1}, \ldots, a_n) \in Z_1\}.$$

Легко проверить, что V_1 — аффинное многообразие (см. упр. 7), более того, $V_1 \subsetneqq V$, потому что иначе $\pi_l(V) \subset Z_1$, откуда $W_1 \subset Z_1$, так как W_1 — это замыкание Зарисского. Кроме того, имеем

$$\pi_l(V) = (W_1 - Z_1) \cup \pi_l(V_1) \tag{9}$$

(см. упр. 7).

Если $V_1 = \varnothing$, то утверждение доказано. Если V_1 непусто, то пусть W_2 — замыкание Зарисского множества $\pi_l(V_1)$. По теореме о замыкании существует $Z_2 \subsetneqq W_2$, такое, что $W_2 - Z_2 \subset \pi_l(V_1)$. Рассуждая, как выше, мы получаем многообразие

$$V_2 = V_1 \cap \{(a_1, \ldots, a_n) \in k^n : (a_{l+1}, \ldots, a_n) \in Z_2\}.$$

Имеем $V_2 \subsetneqq V_1$ и

$$\pi_l(V) = (W_1 - Z_1) \cup (W_2 - Z_2) \cup \pi_l(V_2).$$

Если $V_2 = \varnothing$, то утверждение доказано. В противном случае мы строим многообразия W_3, Z_3 и $V_3 \subsetneqq V_2$. Продолжая этот процесс, мы в конце концов получим $V_N = \varnothing$ для некоторого N — в противном случае будет построена бесконечная убывающая цепь многообразий

$$V \supsetneqq V_1 \supsetneqq V_2 \supsetneqq \ldots.$$

Однако существование такой цепи противоречит предложению 1 из § 6 гл. 4. Следовательно, $V_N = \varnothing$ для некоторого N, и структурная формула для $\pi_l(V)$ доказана. □

Множества типа, описанного в следствии 2, называются *конструктивными*.

Упражнения к § 6

1. В этом упражнении рассматриваются утверждения (1) из доказательства теоремы 1.
   (a) Пусть идеал I прост. Докажите, что I_l также прост. Ваше доказательство должно быть справедливым для любого поля.
   (b) В ходе доказательства теоремы 1 было показано, что если k алгебраически замкнуто и V неприводимо, то $\mathbf{V}(I_l)$ также неприводимо. Дайте доказательство этого утверждения, которое годится для любого поля.

2. Пусть $g, h \in k[x_1, \ldots, x_n]$ и h имеет степень $r > 0$ по x_1, т. е. $h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n)x_1^i$. Индукцией по степени полинома g по отношению к переменной x_1 докажите, что существует N, такое, что $u_r^N g = qh + g'$, где $q, g' \in k[x_1, \ldots, x_n]$ и g' имеет степень $< r$ по x_1.

3. В этом упражнении мы рассмотрим геометрический смысл случаев I и II в доказательстве теоремы 1. Мы будем считать, что $k = \mathbb{C}$. Напомним, что мы рассматриваем неприводимое многообразие $V \subset \mathbb{C}^n$ и его проекцию $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$. Пусть $y \in \mathbb{C}^{n-1}$. Определим множество

$$V_y = \{x \in V : \pi_1(x) = y\},$$

которое называется *слоем над* y проекции π_1.
   (a) Докажите, что $V_y \subset \mathbb{C} \times \{y\}$, так что $V_y \neq \varnothing$ в том и только том случае, когда $y \in \pi_1(V)$.
   (b) Докажите, что в случае I $\pi_1(V) = \mathbf{V}(I_1)$ и $V_y = \mathbb{C} \times \{y\}$ для всех $y \in \pi_1(V)$, т. е. в этом случае все непустые слои — наибольшие из возможных.
   (c) Докажите, что в случае II существует многообразие $\widetilde{W} \subset \mathbb{C}^{n-1}$, такое, что $\pi_1(V)$ не принадлежит $\widetilde{W}$ и каждый непустой слой над точкой $y \notin \widetilde{W}$ конечен, т. е. в этом случае «большинство» непустых слоев конечно. Указание: если h такое, как в (3), и $u_r \notin I_1$, то можно положить $\widetilde{W} = \mathbf{V}(u_r)$.
   (d) Пусть $V = \mathbf{V}(x_2 - x_1x_3) \subset \mathbb{C}^3$. Докажите, что «большинство» слоев V_y состоят из единственной точки. Существует ли бесконечный слой?

4. Пусть $\pi_1 : k^n \to k^{n-1}, \pi_l : k^n \to k^{n-l}$ и $\tilde{\pi}_{l-1} : k^{n-1} \to k^{n-l}$ такие же, как в доказательстве теоремы 1. Докажите, что $\pi_l = \tilde{\pi}_{l-1} \circ \pi_1$.

5. Пусть $V \subset k^n$ — неприводимое многообразие. Докажите следующие утверждения.
   (a) Если $V_1, V_2 \subset k^n$ — многообразия, такие, что $V \subset V_1 \cup V_2$, то или $V \subset V_1$, или $V \subset V_2$.
   (b) Более общее утверждение формулируется так: если $V_1, \ldots, V_m \subset k^n$ — многообразия и $V \subset V_1 \cup \ldots \cup V_m$, то $V \subset V_i$ для некоторого i.

6. Многообразие W, построенное в доказательстве теоремы 1, довольно велико — оно содержит все, кроме одной, неприводимые компоненты многообразия $\mathbf{V}(I_l)$. Докажите, что существует многообразие $W \subset \mathbf{V}(I_l)$, которое не содержит неприводимых компонент многообразия $\mathbf{V}(I_l)$ и удовлетворяет условию $\mathbf{V}(I_l) - W \subset \pi_l(V)$. Указание: сначала объясните, почему каждая неприводимая компонента многообразия $\mathbf{V}(I_l)$ есть V_j' для некоторого j. Затем построение, проведенное для V_1', проведите для каждого V_j'.

7. В этом упражнении мы рассмотрим доказательство следствия 2.

(a) Проверьте, что $V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n : (a_{l+1}, \ldots, a_n) \in Z_1\}$ является аффинным многообразием.
(b) Проверьте, что $\pi_l(V) = (W_1 - Z_1) \cup \pi_l(V_1)$.

8. Пусть $V = \mathbf{V}(y - xz) \subset \mathbb{C}^3$. Следствие 2 утверждает, что $\pi_1(V) \subset \mathbb{C}^2$ является конструктивным множеством. Постройте явное разложение $\pi_1(V)$ в форме, приведенной в следствии 2. Указание: в разложении будут участвовать W_1, Z_1 и W_2.

9. При работе с аффинными многообразиями иногда бывает полезен *принцип минимума*, который утверждает, что в любом множестве многообразий из k^n есть минимальное по отношению включения. Точнее, пусть даны многообразия $V_\alpha, \alpha \in \mathcal{A}$, где $\mathcal{A}$ — произвольное множество индексов. Тогда существует $\beta \in \mathcal{A}$, такой, что из $V_\alpha \subset V_\beta$ следует, что $V_\alpha = V_\beta$.
(a) Докажите принцип минимума. Указание: используйте предложение 1 из § 6 гл. 4.
(b) Сформулируйте и докажите аналогичный *принцип максимума* для идеалов из $k[x_1, \ldots, x_n]$.

10. Как пример применения принципа минимума из упр. 9, мы дадим другое доказательство следствия 2. А именно, рассмотрим множество всех многообразий $V \subset k^n$, для которых $\pi_l(V)$ не конструктивно. По принципу минимума найдется многообразие V, такое, что $\pi_l(V)$ не конструктивно, но $\pi_l(W)$ конструктивно для любого $W \subsetneq V$. Покажите, как доказательство следствия 2 до равенства (9) дает возможность получить противоречие и тем самым доказать следствие.

11. В этом упражнении мы обобщим следствие 2 и докажем, что если k алгебраически замкнуто, то $\pi_l(C)$ конструктивно для любого конструктивного подмножества $C \subset k^n$.
(a) Сведите доказательство к случаю $\pi_l(V - W)$, где V — неприводимое многообразие, а W — его собственное подмногообразие.
(b) Если V неприводимо, а W_1 — замыкание Зарисского множества $\pi_l(V)$, то из (2) следует, что существует $Z_1 \subsetneq W_1$, такое, что $W_1 - Z_1 \subset \pi_l(V - W)$. Положим $V_1 = \{x \in V : \pi_l(x) \in Z_1\}$. Докажите, что $V_1 \neq V$ и что $\pi_l(V - W) = (W_1 - Z_1) \cup \pi_l(V_1 - W)$.
(c) Примените принцип минимума и завершите доказательство (как в упр. 10).

6

Роботика и автоматическое доказательство геометрических теорем

В этой главе мы рассмотрим два недавно возникших приложения понятий и методов алгебраической геометрии. Прежде всего, в продолжение нескольких примеров, приведенных в гл.1, мы разовьем систематический подход, который позволяет использовать алгебраические многообразия для описания пространства возможных конфигураций механических соединений, таких, как «рука» робота. Мы также применим этот подход для решения прямой и обратной кинематических задач роботики для некоторых типов роботов.

Далее, алгоритмы, разработанные в предыдущих главах, мы применим к изучению автоматического доказательства геометрических теорем — тема, важная для специалистов в области искусственного интеллекта. Если предположения геометрической теоремы могут быть представлены в виде полиномиальных уравнений от декартовых координат точек евклидовой плоскости, то геометрические утверждения, выводимые из этих предположений, представляются полиномами из идеала, порожденного предположениями.

§ 1. Геометрическое описание роботов

Прежде чем дать геометрическое описание пространства конфигураций робота, необходимо дать формальное (упрощенное) описание компонент робота и их механических свойств. Нас не будет интересовать техническая сторона конструкции реальных роботов (например, какие типы двигателей и механических соединений используются для реализации движения и управления движением). Другими словами, мы ограничимся рассмотрением идеальных «формальных» роботов. Однако и при таких ограничениях можно указать типы задач, реально возникающих при описании и планировании движения роботов.

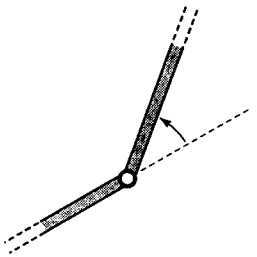
Под роботом мы будем понимать конструкцию из жестких сегментов и сочленений разного типа. Для простоты мы будем рассматривать только те роботы, где сегменты соединены *последовательно*, как в человеческой руке. Один конец «руки» робота будет

обычно жестко закреплен. Другой конец, который мы будем называть *кистью* или *эффектором*, будет рассматриваться как конечный сегмент робота. В реальных роботах «кисть» снабжается механизмами захвата или инструментами для выполнения некоторой работы. Наша главная цель — описать пространство положений и ориентаций «кисти».

Так как сегменты робота жесткие, то возможные движения всей конструкции определяются движениями в сочленениях. Мы будем рассматривать сочленения двух типов (многие реальные роботы именно из таких сочленений и сконструированы):

- плоские шарнирные соединения (шарниры) и
- призматические соединения.

Плоские шарниры позволяют «поворачивать» один сегмент относительно другого. Мы будем предполагать, что оба сегмента лежат в одной плоскости и движения в шарнирном соединении не выводят их из этой плоскости. (Другими словами, ось вращения перпендикулярна плоскости сегментов.)



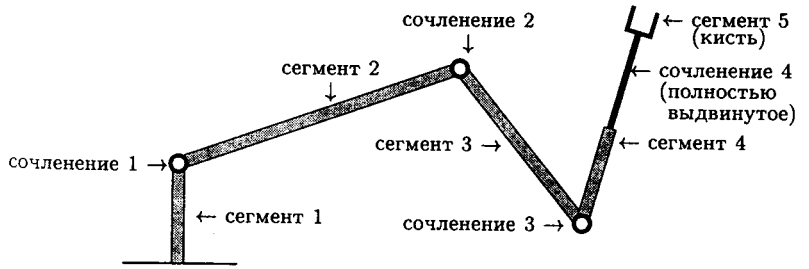
шарнирное соединение

Призматическое соединение позволяет сегменту робота перемещаться (выдвигаться или вдвигаться) вдоль оси. На рисунке ниже представлена схема призматического соединения двух сегментов, находящихся в одной плоскости. Такое сочленение осуществляет скользящее движение вдоль прямой на плоскости.

призматическое соединение

Если робот содержит несколько сочленений, то мы будем предполагать (для простоты), что все они лежат в одной плоскости, оси вращения перпендикулярны этой плоскости, а оси сдвига призматических соединений лежат в плоскости сочленений. Таким образом, все движения происходят в одной плоскости. Конечно, мы рассматриваем весьма ограниченный класс роботов. Реальные роботы способны двигаться в трехмерном пространстве. Для этого используются другие типы и комбинации сочленений. Это шаровые шарниры, позволяющие производить вращения относительно любой оси в $\mathbb{R}^3$ и спиральные или винтовые соединения, позволяющие комбинировать вращение и перемещение вдоль оси вращения в $\mathbb{R}^3$. Можно также связывать сегменты плоскими шарнирами с *непараллельными* осями вращения. Пространство конфигураций в этих случаях может быть описано теми же методами, которые мы здесь будем рассматривать, но мы этим заниматься не будем. Наша цель — показать, как аффинные многообразия могут помочь при описании движения робота, а не создать учебник практической роботики. Плоские роботы представляют собой класс относительно простых, но достаточно показательных примеров.

Пример 1. Рассмотрим руку плоского робота с тремя шарнирными соединениями и одним призматическим соединением. Все движения происходят в плоскости листа бумаги.



Пронумеруем сегменты и сочленения робота, начиная с закрепленного конца и до кисти. Таким образом, сегмент 2 соединяет сочленения 1 и 2 и т. д. Сочленение 4 является призматическим соединением, и мы будем считать, что сегмент 4 имеет переменную длину, которая зависит от состояния призматического соединения. Кисть этого робота является пятым сегментом.

В общем случае состояние шарнирного соединения между сегментами i и $i+1$ может быть описано величиной θ угла поворота (против часовой стрелки) от сегмента i к сегменту $i+1$, т. е. множество состояний сочленения параметризуется *окружностью* S^1

или интервалом $[0, 2\pi]$ с отождествленными концами. (В некоторых случаях шарнирное соединение может не допускать всех поворотов; тогда множество состояний параметризуется подмножеством окружности S^1.)

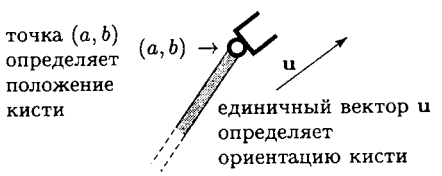
Аналогично, состояние призматического соединения описывается величиной выдвинутого сегмента или, как в примере 1, длиной сегмента (т. е. расстоянием между концом соединения и предыдущим сочленением). В любом случае пространство состояний призматического соединения параметризуется конечным интервалом вещественной оси.

Если состояния сочленений робота независимы, то полное пространство состояний плоского робота с r шарнирными соединениями и p призматическими соединение параметризуется декартовым произведением

$$\mathcal{J} = S^1 \times \ldots \times S^1 \times I_1 \times \ldots \times I_p,$$

куда входит по одному сомножителю S^1 на каждое шарнирное соединение, а I_j задает состояние j-го призматического соединения. Мы будем называть $\mathcal{J}$ *пространством сочленений* робота.

Пространство возможных конфигураций кисти плоского робота может быть описано следующим образом. Зададим декартову систему координат на плоскости. Тогда положение кисти задается точками (a, b) из некоторой области $U \subset \mathbb{R}^2$. Аналогично, ориентация кисти задается единичным вектором, связанным с какой-либо специфической ее частью. Другими словами, пространство ориентаций параметризуется векторами $\mathbf{u}$ из $V = S^1$. Если, например, кисть присоединена шарнирным соединением, то мы имеем следующую картину ее конфигурации:



Множество $\mathcal{C} = U \times V$ мы будем называть *конфигурационным пространством* или *операционным пространством* кисти робота.

Так как сегменты робота жесткие, то, задав состояния сочленений, мы однозначно определим состояние кисти как в смысле положения, так и в смысле ориентации. Таким образом, задано отображение

$$f : \mathcal{J} \longrightarrow \mathcal{C},$$

которое указывает, как по заданному набору состояний сочленений определить конфигурацию кисти.

Две основные задачи, которые мы будем рассматривать, описываются в терминах отображения $f : \mathcal{J} \to \mathcal{C}$:

- (Прямая кинематическая задача) Можно ли дать явное описание или формулу для f в терминах состояний сочленений (координат на $\mathcal{J}$) и длин сегментов «руки» робота?
- (Обратная кинематическая задача) Для данного $c \in \mathcal{C}$ можем ли мы найти одно или все $j \in \mathcal{J}$, такие, что $f(j) = c$?

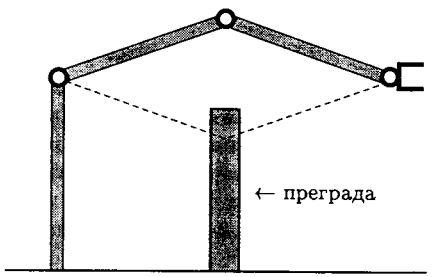
В § 2 мы увидим, что прямая задача решается сравнительно легко. Определение положения и ориентации кисти по состояниям сочленений руки сводится к систематическому описанию относительных положений сегментов по обе стороны от сочленения. Таким образом, прямая задача представляет интерес только как первый шаг к обратной задаче. Мы покажем, что отображение $f : \mathcal{J} \to \mathcal{C}$, задающее конфигурацию «кисти» как функцию состояний сочленений, может быть записано как полиномиальное отображение (см. § 1 гл. 5).

Обратная задача более трудна, так как наши явные формулы будут нелинейными, если имеются шарнирные соединения. Таким образом, чтобы решить уравнение

$$f(j) = c, \tag{1}$$

нам понадобятся общие результаты о системах полиномиальных уравнений.

Одним из свойств нелинейных систем уравнений является то, что решений может быть несколько, даже если общее пространство решений конечно. Мы увидим в § 3, что это так для руки плоского робота с тремя и более шарнирными соединениями. На практике потенциальная неоднозначность решения системы (1) иногда весьма желательна. Пусть, например, робот работает в пространстве с преградами для движения в некоторых направлениях. Тогда некоторые решения системы (1) могут соответствовать физически невозможным состояниям:



Чтобы понять, можно ли получить определенное положение кисти, возможно, будет необходимо найти *все* решения системы (1) и выбрать из них то (или те), которое удовлетворяет имеющимся ограничениям.

Упражнения к § 1

1. Опишите пространство сочленений $\mathcal{J}$ и конфигурационное пространство C для плоского робота, изображенного на рисунке к примеру 1. Для описания пространства C определите ограниченную область $U \subset \mathbb{R}^2$, содержащую все возможные положения кисти. Указание: описание области U должно учитывать длины сегментов.
2. Рассмотрим отображение $f : \mathcal{J} \to C$ для примера 1. Является ли f *инъективным* отображением с геометрической точки зрения? Можете ли вы найти два способа поместить кисть в заданное место с заданной ориентацией? Можно ли это сделать более чем двумя способами?

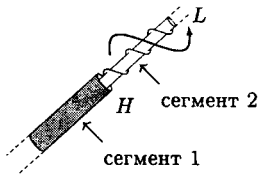
В тексте параграфа рассматривались пространство сочленений $\mathcal{J}$ и конфигурационное пространство C плоского робота. В следующих задачах мы рассмотрим, что можно сказать о $\mathcal{J}$ и C для роботов, способных двигаться в трехмерном пространстве.

3. Как можно описать конфигурационное пространство трехмерного робота? В частности, как описать возможные ориентации кисти?
4. Шаровой шарнир в точке B позволяет сегменту 2 на приведенном ниже рисунке поворачиваться на любой угол вокруг любой оси в $\mathbb{R}^3$, проходящей через B. (Замечание: движения в этом сочленении аналогичны движениям джойстика в компьютерных играх.)

шаровой шарнир

(a) Математически опишите пространство возможных состояний сочленения в этом случае. Указание: состояние сочленения определяется вектором, направленным вдоль сегмента 2.
(b) Постройте взаимно однозначное соответствие между пространством состояний сочленения из п. (a) и единичной сферой $S^2 \subset \mathbb{R}^3$. Указание: это можно сделать с помощью сферических координат ϕ, θ на сфере S^2.

5. Спиральное, или винтовое соединение в точке H позволяет сегменту 2 на рисунке ниже выдвигаться из H вдоль прямой L в направлении сегмента 1, вращаясь в то же время вокруг оси L.



спиральное, или винтовое соединение

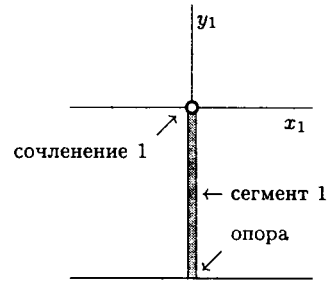
Угол вращения θ (измеренный от начального, «убранного» положения сегмента 2) равен $l \cdot \alpha$, где $l \in [0, m]$ — длина выдвинутой части сегмента 2, а α — заданная угловая константа. Дайте математическое описание пространства состояний сочленения в этом случае.

6. Дайте математическое описание пространства сочленений $\mathcal{J}$ для трехмерного робота с двумя шаровыми шарнирами и одним спиральным соединением.

§ 2. Прямая кинематическая задача

В этом параграфе мы рассмотрим стандартный метод решения прямой кинематической задачи для руки данного робота. Как и в § 1, мы будем иметь дело только с роботами в $\mathbb{R}^2$, т. е. «кисть» не выходит за пределы плоскости. Другие случаи будут рассмотрены в упражнениях.

У всех рассматриваемых роботов первый сегмент руки считается закрепленным. Другими словами, в начале сегмента 1 нет подвижного сочленения. Учитывая это условие, мы будем использовать обычную прямоугольную систему координат на плоскости для описания положения и ориентации «кисти». Начало системы координат будет помещено в сочленение 1, которое не меняет своего положения (как и весь сегмент 1). Например:

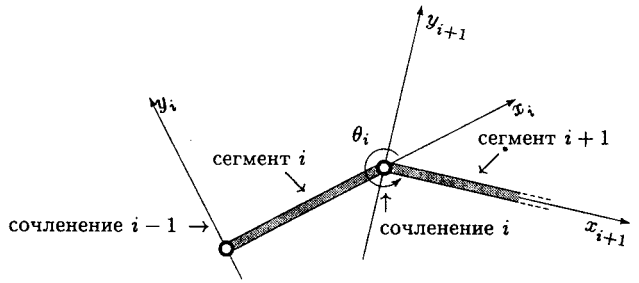


Глобальная система координат (x_1, y_1)

Кроме глобальной системы координат (x_1, y_1) мы определим локальные прямоугольные системы координат в каждом *шарнирном соединении* для описания относительного положения сегментов, сходящихся в этом сочленении. Естественно, эти системы координат *меняются* при изменении состояния руки.

В i-м шарнирном соединении мы зададим систему координат (x_{i+1}, y_{i+1}) следующим образом. Начало системы помещаем в сочленение i. За положительное направление оси x_{i+1} выбираем направление $(i+1)$-го сегмента (в текущем состоянии руки робота). Положительное направление оси y_{i+1} выбираем так, чтобы система координат была обычной правой прямоугольной системой. Обратите внимание, что для каждого $i \geq 2$ пара $(l_i, 0)$ — это (x_i, y_i)-координаты сочленения i, где l_i — длина i-го сегмента.

Наша первая задача — связать (x_{i+1}, y_{i+1})-координаты некоторой точки с ее же (x_i, y_i)-координатами. Пусть θ_i — это угол, отсчитанный против часовой стрелки, между осью x_i и осью x_{i+1}.



Локальная система координат в i-м шарнирном соединении

Этот угол равен углу, определяющему состояние сочленения i, из § 1. Пусть точка q имеет в системе координат (x_{i+1}, y_{i+1}) (см. рисунок выше) координаты (a_{i+1}, b_{i+1}); тогда для вычисления ее (x_i, y_i)-координат (a_i, b_i) мы должны осуществить поворот на угол θ_i (совместить оси x_i и x_{i+1}), а потом параллельный перенос на вектор $(l_i, 0)$ (совместить начала систем координат). В упражнениях мы докажем, что поворот на угол θ_i — это умножение на матрицу поворота

$$\begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}.$$

Легко проверить, что параллельный перенос — это сложение с вектором $(l_i, 0)$. Таким образом, мы имеем следующее соотношение:

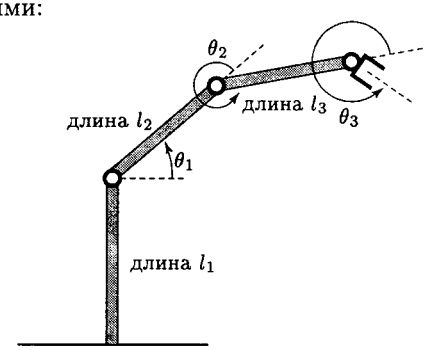
$$\begin{pmatrix} a_i \\ b_i \end{pmatrix} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \cdot \begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} + \begin{pmatrix} l_i \\ 0 \end{pmatrix}.$$

Это преобразование координат удобно представлять с помощью 3×3-матрицы и трехкомпонентного вектора:

$$\begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i & l_i \\ \sin\theta_i & \cos\theta_i & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{pmatrix} = A_i \cdot \begin{pmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{pmatrix}. \quad (1)$$

Эта запись позволяет объединить поворот и параллельный перенос в одну 3×3-матрицу A_i.

Пример 1. Рассмотрим руку плоского робота с тремя шарнирными соединениями:



Кисть мы будем рассматривать как четвертый сегмент, соединенный шарниром 3 с сегментом 3. Как и выше, через l_i обозначается длина сегмента i. Имеем

$$A_1 = \begin{pmatrix} \cos\theta_1 & -\sin\theta_1 & 0 \\ \sin\theta_1 & \cos\theta_1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

так как начало системы координат (x_2, y_2) также находится в сочленении 1. Мы можем найти матрицы A_2 и A_3, как в формуле (1). Основное наблюдение состоит в том, что глобальные координаты любой точки мы можем найти, зная ее координаты в системе (x_4, y_4) и последовательно вычисляя координаты в системах (x_3, y_3), (x_2, y_2) и, наконец, (x_1, y_1):

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = A_1 A_2 A_3 \begin{pmatrix} x_4 \\ y_4 \\ 1 \end{pmatrix}.$$

Тригонометрические формулы для суммы углов позволяют записать это уравнение в следующем виде:

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = \begin{pmatrix} \cos(\theta_1+\theta_2+\theta_3) & -\sin(\theta_1+\theta_2+\theta_3) & l_3\cos(\theta_1+\theta_2)+l_2\cos\theta_1 \\ \sin(\theta_1+\theta_2+\theta_3) & \cos(\theta_1+\theta_2+\theta_3) & l_3\sin(\theta_1+\theta_2)+l_2\sin\theta_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_4 \\ y_4 \\ 1 \end{pmatrix}.$$

Так как (x_4, y_4)-координаты кисти равны $(0,0)$ (кисть непосредственно закреплена в сочленении 3), то (x_1, y_1)-координаты кисти могут быть получены при подстановке $x_4 = y_4 = 0$ в матричное произведение:

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = \begin{pmatrix} l_3\cos(\theta_1+\theta_2) + l_2\cos\theta_1 \\ l_3\sin(\theta_1+\theta_2) + l_2\sin\theta_1 \\ 1 \end{pmatrix}. \tag{2}$$

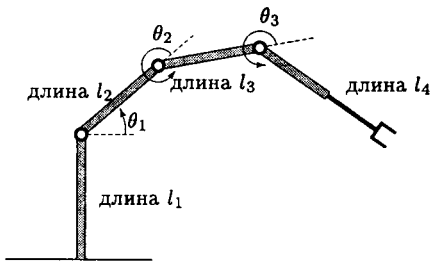
Ориентация кисти определена, если мы знаем угол между осью x_4 и направлением кисти. Например, мы можем просто использовать направление оси x_4 как ориентацию. Но мы знаем, что угол между осью x_1 и осью x_4 равен $\theta_1 + \theta_2 + \theta_3$, так что найти ориентацию несложно.

Объединяя эти замечания об ориентации кисти и формулу (2), мы получаем явное описание отображения $f : \mathcal{J} \to \mathcal{C}$, определенного в § 1. Конфигурация кисти как функция углов θ_i равна

$$f(\theta_1,\theta_2,\theta_3) = \begin{pmatrix} l_3\cos(\theta_1+\theta_2) + l_2\cos\theta_1 \\ l_3\sin(\theta_1+\theta_2) + l_2\sin\theta_1 \\ \theta_1+\theta_2+\theta_3 \end{pmatrix}. \tag{3}$$

Аналогично может быть найдена функция f для любого количества плоских шарнирных соединений. Детали см. в упр. 7.

Пример 2. В рамках этого подхода могут быть описаны и призматические соединения. Рассмотрим, например, руку плоского робота, первые три сегмента и сочленения которой такие же, как у робота в примере 1, но у которого есть дополнительное призматическое соединение между сегментом 4 и кистью. Другими словами, сегмент 4 имеет переменную длину, а кисть будет сегментом 5.



Ось перемещения призматического соединения совпадает с направлением сегмента 4. Этот робот может быть описан следующим образом. Три шарнирных соединения действуют так же, как в примере 1, но призматическое соединение позволяет менять длину l_4 сегмента 4 от m_1, когда сегмент вдвинут, до m_2, когда он полностью выдвинут. Рассуждая, как в примере 1, получаем, что положение кисти можно найти, умножая матрицу $A_1A_2A_3$ на координатный вектор кисти в системе (x_4, y_4), т. е. на вектор $(l_4, 0)$. Таким образом, конфигурация кисти задается формулой

$$g(\theta_1,\theta_2,\theta_3,l_4) = \begin{pmatrix} l_4\cos(\theta_1+\theta_2+\theta_3) + l_3\cos(\theta_1+\theta_2) + l_2\cos\theta_1 \\ l_4\sin(\theta_1+\theta_2+\theta_3) + l_3\sin(\theta_1+\theta_2) + l_2\sin\theta_1 \\ \theta_1+\theta_2+\theta_3 \end{pmatrix}. \tag{4}$$

Как и выше, l_2 и l_3 — константы, но $l_4 \in [m_1, m_2]$ — это новая переменная. Ориентация кисти определяется углом $\theta_1 + \theta_2 + \theta_3$, как в примере 1, потому что призматическое соединение не влияет на ее направление.

Теперь мы рассмотрим, как формулы, подобные (3) и (4), могут быть преобразованы в полиномиальные или рациональные представления для f и g (в соответствующих переменных). Шарнирные соединения и призматические соединения требуют различного подхода. Как преобразовать тригонометрические выражения в полиномиальные, мы знаем (см., например, упр. 8 к § 8 гл. 2). Хотя $\cos\theta$ и $\sin\theta$ — трансцендентные функции, но они дают параметризацию

$$\begin{aligned} x &= \cos\theta, \\ y &= \sin\theta \end{aligned}$$

единичной окружности — многообразия $\mathbf{V}(x^2+y^2-1)$. Таким образом, компоненты правой части равенства (3), т. е. элементы матрицы $A_1A_2A_3$ в последней формуле на с. 347, мы можем считать функциями от переменных $c_i = \cos\theta_i, s_i = \sin\theta_i$, на которые наложены условия

$$c_i^2 + s_i^2 - 1 = 0, \tag{5}$$

$i = 1, 2, 3$. Обратите внимание, что многообразие в $\mathbb{R}^6$, определенное этими тремя уравнениями, и есть реализация пространства сочленений $\mathcal{J}$ для этого робота. С геометрической точки зрения это многообразие — просто декартово произведение трех окружностей.

Из (3) мы можем получить явное полиномиальное выражение для положения кисти в переменных $c_1, s_1, c_2, s_2, c_3, s_3$. Имеем

$$\cos(\theta_1+\theta_2) = \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 = c_1c_2 - s_1s_2.$$

Аналогично,

$$\sin(\theta_1+\theta_2) = \sin\theta_1\cos\theta_2 + \sin\theta_2\cos\theta_1 = s_1c_2 + s_2c_1.$$

Таким образом, (x_1, y_1)-координаты кисти равны

$$\begin{pmatrix} l_3(c_1c_2 - s_1s_2) + l_2c_1 \\ l_3(s_1c_2 + s_2c_1) + l_2s_1 \end{pmatrix}. \tag{6}$$

В терминологии гл. 5 мы определили полиномиальное отображение многообразия $\mathcal{J} = \mathbf{V}(x_1^2+y_1^2-1, x_2^2+y_2^2-1, x_3^2+y_3^2-1)$ в $\mathbb{R}^2$. Обратите внимание, что *положение* кисти не зависит от θ_3. Этот угол влияет только на ее ориентацию.

Так как ориентация кисти зависит непосредственно от углов θ_i, то *невозможно* представить ориентацию как полином от $c_i = \cos\theta_i$ и $s_i = \sin\theta_i$. Однако есть способ и ориентацию представить в полиномиальном виде. См. упр. 3.

Аналогично может быть получена полиномиальная форма в (x_1, y_1)-координатах отображения g из примера 2. Это

$$\begin{pmatrix} l_4(c_1(c_2c_3 - s_2s_3) - s_1(c_2s_3 + c_3s_2)) + l_3(c_1c_2 - s_1s_2) + l_2c_1 \\ l_4(s_1(c_2c_3 - s_2s_3) + c_1(c_2s_3 + c_3s_2)) + l_3(s_1c_2 + s_2c_1) + l_2s_1 \end{pmatrix}. \quad (7)$$

Здесь $\mathcal{J}$ является подмножеством $V \times [m_1, m_2]$ многообразия $V \times \mathbb{R}$, где $V = \mathbf{V}(x_1^2 + y_1^2 - 1, x_2^2 + y_2^2 - 1, x_3^2 + y_3^2 - 1)$. Длина l_4 в (7) рассматривается как переменная; поэтому компоненты отображения являются полиномами от l_4 и c_i, s_i.

Второй способ преобразования формул (3) и (4) использует *рациональную* параметризацию окружности

$$x = \frac{1-t^2}{1+t^2}, \qquad y = \frac{2t}{1+t^2} \quad (8)$$

(см. § 3 гл. 1). Следует отметить, что в терминах тригонометрической параметризации $t = \operatorname{tg}(\theta/2)$. Эта параметризация позволяет выразить отображение (3) как рациональную функцию от трех переменных $t_i = \operatorname{tg}(\theta_i/2)$. Мы оставляем читателю в качестве упражнения вывод явной формы отображения $f : \mathcal{J} \to C$ для примера 1 в этих переменных. В терминологии гл. 5 многообразие $\mathcal{J}$ для робота из примера 1 бирационально эквивалентно $\mathbb{R}^3$. Рациональная параметризация $\rho : \mathbb{R}^3 \to \mathcal{J}$ конструируется с помощью трех экземпляров параметризации (8). Таким образом, мы получили рациональное отображение $\mathbb{R}^3 \to \mathbb{R}^2$, которое представляет координаты кисти робота как функции от t_1, t_2, t_3 и которое является композицией ρ с отображением f в форме (6). Оба эти представления имеют свои преимущества и недостатки. Для робота из примера 1 явное преимущество рационального представления с помощью (8) состоит в том, что используются только три переменные t_1, t_2, t_3 вместо шести $c_i, s_i, i = 1, 2, 3$ (см. упр. 3). Кроме того, нам не нужны условия (5). Однако если θ_i близко к π, то соответствующее t_i очень велико, и, кроме того, значение $\theta_i = \pi$ не параметризовано. Другими словами, описываются не все возможные положения кисти в образе f. Разумеется, если робот сконструирован так, что сегмент $i+1$ не может совмещаться с сегментом i, то этой проблемы не возникает (в этом случае θ_i не может принимать значение π). Полиномиальная форма (6) не столь удобна в работе, но так как она основана на тригонометрической параметризации единичной окружности, то недостатки рационального представления здесь не возникают. Эта форма более удобна при работе с шарнирными соединениями, допускающими свободные повороты на любой угол.

Упражнения к § 2

1. Рассмотрим плоскость $\mathbb{R}^2$ с обычной ортогональной системой координат (x_1, y_1). Пусть система координат (x_2, y_2) является результатом поворота системы (x_1, y_1) на угол θ против часовой стрелки относительно начала координат. Предположим, что точка q имеет координаты (a_1, b_1) в системе (x_1, y_1) и координаты (a_2, b_2) в системе (x_2, y_2). Докажите, что
$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}.$$
Для доказательства перейдите от (x_1, y_1)-координат точки q к полярным:
$$q = (a_1, b_1) = (r\cos\alpha, r\sin\alpha).$$
   (a) Докажите, что
   $$q = (a_2, b_2) = (r\cos(\alpha+\theta), r\sin(\alpha+\theta)).$$
   (b) Теперь используйте тригонометрические тождества для вывода доказываемой формулы.
2. В примерах 1 и 2 мы использовали 3×3-матрицу A для представления преобразования координат при переходе от одной локальной системы к другой. Эти преобразования включали повороты и параллельные переносы. Такие преобразования называются *аффинными преобразованиями*.
   (a) Докажите, что любое аффинное преобразование плоскости
   $$x' = ax + by + e,$$
   $$y' = cx + dy + f$$
   может быть представлено в том же виде:
   $$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.$$
   (b) Найдите аналогичное представление для аффинных преобразований в $\mathbb{R}^3$ с использованием 4×4-матриц.
3. В этом упражнении мы снова рассмотрим задачу об ориентации кисти робота из примеров 1 и 2. А именно, пусть $\alpha = \theta_1 + \theta_2 + \theta_3$ — угол, задающий ориентацию кисти в системе (x_1, y_1).

(a) Используя тригонометрические формулы, докажите, что переменные

$$c = \cos\alpha, \qquad s = \sin\alpha$$

являются полиномами от $c_i = \cos\theta_i$ и $s_i = \sin\theta_i$. Таким образом, мы можем представить отображение f в полиномиальной форме за счет введения еще одной координатной функции в $\mathcal{C}$.

(b) Найдите рациональное представление для c и s, используя формулы (8).

4. Пусть плоский робот имеет шарнирное соединение 1, сегмент 2 длины l_2, призматическое соединение 2 с состоянием $l_3 \in [0, m_3]$ и шарнирное соединение 3 с сегментом 4 — кистью робота.
   (a) Что представляют собой пространство сочленений $\mathcal{J}$ и конфигурационное пространство $\mathcal{C}$ в этом случае?
   (b) Используя методы примеров 1 и 2, постройте явную формулу для отображения $f\colon \mathcal{J} \to \mathcal{C}$ в тригонометрической форме.
   (c) Преобразуйте f к полиномиальному виду, используя удобные новые координаты.
5. Преобразуйте формулы отображений f и g в примерах 1 и 2 соответственно к рациональному виду, используя параметризацию (8) для каждого шарнирного соединения. Покажите, что в обоих случаях и положение кисти, и ее ориентация задаются рациональными функциями на $\mathbb{R}^n$ (значение n в этих двух примерах различно).
6. Формулу для отображения f из упр. 4 преобразуйте к рациональному виду, используя параметризацию (8) для каждого шарнирного соединения.
7. Пусть дан плоский робот с закрепленным сегментом 1 (как и во всех примерах этого параграфа) и с n шарнирными соединениями, связывающими сегменты с длинами $l_2, \dots, l_n$. Кисть — сегмент $n+1$ — связана с сегментом n шарнирным соединением n.
   (a) Что представляют собой пространство сочленений и конфигурационное пространство в этом случае?
   (b) Докажите, что отображение $f : \mathcal{J} \to \mathcal{C}$ в этом случае имеет вид

$$f(\theta_1, \dots, \theta_n) = \begin{pmatrix} \sum_{i=1}^{n-1} l_{i+1} \cos\left(\sum_{j=1}^{i} \theta_j\right) \\ \sum_{i=1}^{n-1} l_{i+1} \sin\left(\sum_{j=1}^{i} \theta_j\right) \\ \sum_{i=1}^{n} \theta_i \end{pmatrix}.$$

   Указание: индукция по n.
8. Еще одним типом трехмерного соединения является «круг» или неплоское шарнирное соединение, которое дает возможность сегменту вращаться в плоскости, перпендикулярной предыдущему сегменту. В этом упражнении мы рассмотрим прямую кинематическую задачу для трехмерного робота, содержащего два «круговых» сочленения. Как обычно, первый сегмент считается закрепленным. Глобальная система координат (x_1, y_1, z_1) выбрана так, что ее начало находится в первом сочленении, а сегмент 1 лежит на оси z_1. Вращение в сочленении 1 — это вращение вокруг оси z_1 в плоскости (x_1, y_1). Сегмент 2 имеет длину l_2, а сочленение 2 — это второй «круг», соединяющий сегмент 2 с сегментом 3. Ось вращения сочленения 2 направлена по сегменту 2, так что сегмент 3 вращается в плоскости, перпендикулярной сегменту 2.
   (a) Постройте локальную прямоугольную правую систему координат (x_2, y_2, z_2) с началом в сочленении 1, ось x_2 которой направлена вдоль сегмента 2, а ось y_2 лежит в плоскости (x_1, y_1). Найдите явные формулы, выражающие (x_1, y_1, z_1)-координаты некоторой точки через ее (x_2, y_2, z_2)-координаты и угол поворота θ_1.
   (b) Представьте ваши формулы в матричном виде, используя 4×4-матрицы аффинных преобразований из п. (b) упр. 2.
   (c) Теперь постройте локальную прямоугольную систему координат (x_3, y_3, z_3) с началом в сочленении 2, ось x_3 которой направлена вдоль сегмента 3, а ось z_3 — вдоль сегмента 2. Найдите явные формулы, выражающие (x_2, y_2, z_2)-координаты некоторой точки через ее (x_3, y_3, z_3)-координаты и угол поворота θ_2.
   (d) Представьте формулы из п. (c) в матричном виде.
   (e) Найдите матрицу преобразования от (x_3, y_3, z_3)-координат точки к ее (x_1, y_1, z_1)-координатам. Указание: для этого надо перемножить матрицы из пп. (b) и (d).
9. Рассмотрим робот из упражнения 8.
   (a) Используя формулы из п. (c) упр. 8, найдите явную формулу отображения $f : \mathcal{J} \to \mathcal{C}$.
   (b) Опишите положение кисти полиномиальной функцией от переменных $c_i = \cos\theta_i$ и $s_i = \sin\theta_i$.
   (c) Ориентация кисти (т. е. конца сегмента 3) задается единичным вектором, направленным вдоль сегмента 3 в координатах (x_1, y_1, z_1). Опишите этот вектор.

§ 3. Обратная кинематическая задача и планирование движения

В этом параграфе мы продолжим рассмотрение кинематических задач, сформулированных в § 1. Сначала мы рассмотрим обратную кинематическую задачу для плоского робота из примера 1 § 2. Для заданной точки $(x_1, y_1) = (a, b) \in \mathbb{R}^2$ и некоторой ориентации мы хотим определить, можно ли поместить кисть робота в эту точку с заданной ориентацией. Если да, то мы хотим определить все состояния сочленений, при которых это осуществляется. Другими словами, мы хотим найти *образ* отображения $f : \mathcal{J} \to \mathcal{C}$ и для каждой точки c из этого образа найти ее *прообраз* $f^{-1}(c)$.

Легко видеть, что если $l_3 = l_2 = l$, то кисть робота может быть помещена в любую точку замкнутого круга радиуса $2l$ с центром в сочленении 1 — начале координат системы (x_1, y_1). Если же $l_3 \neq l_2$,

то возможные положения кисти принадлежат замкнутому кольцу с центром в сочленении 1 (см. упр. 14 к § 2 гл. 1). Мы докажем это, используя решение прямой кинематической задачи в форме (6) из § 2. Кроме того, мы выведем *явные формулы* для состояний сочленений, которые обеспечивают заданное положение кисти. Такие формулы можно использовать в управляющих программах робота.

В нашем случае задача управления ориентацией кисти решается легко. Так как состояния сочленений независимы друг от друга, то ориентацию кисти $\alpha = \theta_1 + \theta_2 + \theta_3$ мы можем получить, положив $\theta_3 = \alpha - (\theta_1 + \theta_2)$.

Чтобы упростить проблему, в дальнейшем рассмотрении обратной задачи ориентацию кисти мы будем игнорировать. Мы будем изучать только ее положение, которое является функцией лишь углов θ_1 и θ_2. Из формулы (6) § 2 получаем, что все возможные способы поместить кисть в заданную точку $(x_1, y_1) = (a, b)$ описываются следующей полиномиальной системой:

$$\begin{aligned} a &= l_3(c_1c_2 - s_1s_2) + l_2c_1, \\ b &= l_3(c_1s_2 + c_2s_1) + l_2s_1, \\ 0 &= c_1^2 + s_1^2 - 1, \\ 0 &= c_2^2 + s_2^2 - 1. \end{aligned} \tag{1}$$

Чтобы решить эту систему, найдем базис Грёбнера, используя lex-упорядочение с

$$c_2 > s_2 > c_1 > s_1.$$

Получаем

$$\begin{aligned} & c_2 - \frac{a^2 + b^2 - l_2^2 - l_3^2}{2l_2l_3}, \\ & s_2 + \frac{a^2 + b^2}{al_3}s_1 - \frac{a^2b + b^3 + b(l_2^2 - l_3^2)}{2al_2l_3}, \\ & c_1 + \frac{b}{a}s_1 - \frac{a^2 + b^2 + l_2^2 - l_3^2}{2al_2}, \\ & s_1^2 + \frac{a^2b + b^3 + b(l_2^2 - l_3^2)}{l_2(a^2 + b^2)}s_1 \\ & \quad + \frac{(a^2 + b^2)^2 + (l_2^2 - l_3^2)^2 - 2a^2(l_2^2 + l_3^2) + 2b^2(l_2^2 - l_3^2)}{4l_2^2(a^2 + b^2)}. \end{aligned} \tag{2}$$

В алгебраических терминах это редуцированный базис Грёбнера идеала I, порожденного полиномами (1) в кольце $\mathbb{R}(a, b, l_2, l_3)[s_1, c_1, s_2, c_2]$, где знаменатели содержат только параметры a, b, l_2, l_3.

Здесь мы впервые вычислили базис Грёбнера над полем рациональных функций, и интерпретировать формулы (2) надо с осторожностью. Работа над $\mathbb{R}(a, b, l_2, l_3)$ означает, что a, b, l_2, l_3 рассматриваются как абстрактные переменные над $\mathbb{R}$, в частности, они считаются алгебраически независимыми (т. е. если $p(a, b, l_2, l_3) = 0$, где p — полином с вещественными коэффициентами, то p — нулевой полином). Но в нашей задаче a, b, l_2, l_3 — заданные вещественные числа. Когда мы делаем подстановку в (1), заменяя параметры их конкретными значениями, то получаем идеал $\bar{I} \subset \mathbb{R}[c_1, s_1, c_2, s_2]$, соответствующий данному положению кисти руки робота с данными длинами сегментов. Теперь возникает вопрос, остается ли (2) базисом Грёбнера $\bar{I}$? В общем случае замена переменных их конкретными значениями из поля называется *специализацией*, так что вопрос можно сформулировать так: как ведет себя базис Грёбнера при специализации?

Отметим, во-первых, что трудности могут возникать, если при специализации знаменатели в (2) обращаются в нуль. При специализации обычно никаких трудностей не возникает для большинства (но не для всех!) значений переменных. В упражнениях будет доказано, что существует собственное подмногообразие $W \subset \mathbb{R}^4$, такое, что (2) остается базисом Грёбнера идеала $\bar{I}$ при специализации, если $(a, b, l_2, l_3) \in \mathbb{R}^4 - W$. Мы также покажем, что существует алгоритм определения W. Следует отметить, что в общем случае не только обращение знаменателей в нуль может вызвать трудности (примеры будут разобраны в упражнениях). К счастью, в нашей задаче W определяется только обращением в нуль знаменателей. Это означает, что если $l_2 \neq 0, l_3 \neq 0, a \neq 0$ и $a^2 + b^2 \neq 0$, то (2) является базисом Грёбнера идеала (1). Подробнее этот факт будет доказан в упр. 9.

Пусть задана некоторая «хорошая» специализация. Старшие члены элементов базиса Грёбнера (2) таковы, что, во-первых, любой корень s_1 последнего полинома однозначно продолжается до полного решения системы. Во-вторых, множество решений системы (1) *конечно* при таком выборе a, b, l_2, l_3. В самом деле, последний полином в (2) имеет вторую степень по s_1; следовательно, он может иметь не более *двух* различных корней. Осталось понять, при каких значениях параметров соответствующие решения s_1 *вещественны* (только вещественные решения имеют смысл при описании геометрии робота).

Чтобы упростить формулы, рассмотрим специализацию $l_2 = l_3 = 1$. В упр. 1 будет показано, что и подстановка $l_2 = l_3 = 1$ в (2), и подстановка $l_2 = l_3 = 1$ в (1) с последующим вычислением ба-

зиса Грёбнера в $\mathbb{R}(a,b)[s_1,c_1,s_2,c_2]$ дают один и тот же результат:

$$\begin{aligned} &c_2 - \frac{a^2+b^2-2}{2}, \\ &s_2 + \frac{a^2+b^2}{a}s_1 - \frac{a^2b+b^3}{2a}, \\ &c_1 + \frac{b}{a}s_1 - \frac{a^2+b^2}{2a}, \\ &s_1^2 + \frac{a^2b+b^3}{a^2+b^2}s_1 + \frac{(a^2+b^2)^2-4a^2}{4(a^2+b^2)}. \end{aligned} \tag{3}$$

Другие выборы значений для l_2 и l_3 будут рассмотрены в упр. 4. (Хотя (2) остается базисом Грёбнера для всех ненулевых значений l_2 и l_3, геометрия робота меняется радикально, если $l_2 \neq l_3$.)

Как уже упоминалось выше, (3) является базисом Грёбнера для всех значений a и b, если $a \neq 0$ и $a^2+b^2 \neq 0$. Другими словами, положение кисти в $(0,b)$ или в $(0,0)$ обладает какими-то особыми свойствами. Рассмотрим сначала общий случай $a \neq 0$. Тогда и $a^2+b^2 \neq 0$ (так как $a,b \in \mathbb{R}$). Решая последнее уравнение в (3), получаем

$$s_1 = \frac{b \pm |a|\sqrt{4-(a^2+b^2)}}{2\sqrt{a^2+b^2}}.$$

Корни вещественны в том и только том случае, когда $0 < a^2+b^2 \leq 4$, причем, когда $a^2+b^2=4$, мы имеем двойной корень. С геометрической точки зрения этот результат очевиден. Расстояние от сочленения 1 до сочленения 3 не превышает $l_2+l_3=2$, причем это расстояние равно 2, только когда $\theta_2=0$, т. е. когда сегменты 2 и 3 направлены в одну сторону.

По данному s_1 остальные переменные c_1, s_2, c_2 определяются однозначно с помощью других элементов базиса Грёбнера (при $a \neq 0$). (В действительности значение c_2 не зависит от s_1 — см. упр. 2.) Так как полиномы $c_1^2+s_1^2-1$ и $c_2^2+s_2^2-1$ принадлежат идеалу, порожденному полиномами (3), то полученное нами решение s_1, c_1, s_2, c_2 однозначно определяет углы θ_1 и θ_2. Таким образом, случай $a \neq 0$ сравнительно прост.

Перейдем к случаю $a=b=0$. Геометрически это означает, что сочленение 3 расположено в начале координат системы (x_1,y_1) — в той же точке, где сочленение 1. Это тот случай, когда специализация (2) некорректна — последний полином в (2) не определен. Причину этого нетрудно понять с геометрической точки зрения. В действительности существует *бесконечно много* способов поместить сочленение 3 в начало координат, когда $l_1=l_2$: угол θ_1 может быть выбран произвольно, а положив $\theta_2=\pi$, мы совмещаем сегмент 3 с сегментом 2, помещая сочленение 3 в $(0,0)$. Только так можно

поместить кисть в точку $(a,b)=(0,0)$. В упр. 3 тот же результат будет получен другими методами.

Наконец, выясним, что происходит, когда $a=0, b \neq 0$. Геометрические соображения не позволяют увидеть что-либо особенное в этом положении кисти. В самом деле, этот случай сводится к общему повороту, который делает первую координату отличной от нуля. Тем не менее *алгебраическая* проблема остается, так как знаменатели в (2) обращаются в нуль при $a=0$. Специализация (2) в этом случае некорректна. Нам ничего не остается, как подставить $a=0$ (и $l_2=l_3=1$) в (1) и вычислить базис Грёбнера заново. Имеем

$$\begin{aligned} &c_2 - \frac{b^2-2}{2}, \\ &s_2 - bc_1, \\ &c_1^2 + \frac{b^2-4}{4}, \\ &s_1 - \frac{b}{2}. \end{aligned} \tag{4}$$

Обратите внимание, что *форма* базиса Грёбнера изменилась при этой специализации: уравнение, определяющее s_1, теперь имеет степень 1, а уравнение для c_1 — степень 2. Таким образом, есть два вещественных значения c_1, если $|b|<2$, и одно, если $|b|=2$. Как и в случае $a \neq 0$, мы имеем не более двух различных решений системы, причем решения совпадают, если точка находится на границе круга радиуса 2. В упр. 2 будет проанализирован геометрический смысл условия $a=0$ и будет объяснено, почему s_1 имеет только одно значение.

Это завершает анализ поведения руки робота. Подведем итоги. Пусть задана точка (a,b) в системе координат (x_1,y_1). Тогда поместить сочленение 3 в эту точку

- можно бесконечным количеством способов, если $a^2+b^2=0$,
- можно двумя способами, если $0<a^2+b^2<4$,
- можно одним способом, если $a^2+b^2=4$,
- нельзя, если $a^2+b^2>4$.

Случаи $a^2+b^2=0,4$ (но *не* специальный случай $a=0, b \neq 0$) являются примерами того, что называется *кинематическими особенностями* робота. Мы дадим точное определение этого понятия и обсудим его смысл ниже.

В упражнениях мы рассмотрим робот с тремя шарнирными соединениями и одним призматическим соединением (см. пример 2 из § 2). В этом случае на ориентацию кисти наложено больше ограничений. Например, если $l_4 \in [0,1]$, то кисть может быть помещена в любую точку замкнутого круга радиуса 3 с центром в

$(x_1, y_1) = (0, 0)$. Но на границе этого круга ориентация кисти определена однозначно.

Прежде чем продолжить изучение роботики, сделаем несколько замечаний о специализации. В примере, рассмотренном выше, мы предполагали, что можем вычислять базис Грёбнера над полем функций. Однако не все компьютерные системы могут проводить такие вычисления — некоторые из них не работают с коэффициентами из поля функций. Стандартный метод справиться с этой трудностью рассмотрен в упр. 10. Другой вопрос — как найти «плохие» специализации. Этот вопрос рассмотрен в упр. 8. Наконец, следует упомянуть, что существует особый класс базисов Грёбнера, называемых *исчерпывающими базисами Грёбнера*. Эти базисы остаются базисами Грёбнера при *любой* специализации. Этот класс базисов рассмотрен в приложении в книге BECKER, WEISPFENNING (1993).

Мы закончим обсуждение геометрии роботов рассмотрением кинематических особенностей и тех проблем, которые они создают при планировании движения. При этом мы будем использовать аппарат математического анализа функций нескольких переменных.

Пусть $f : \mathcal{J} \to \mathcal{C}$ — отображение, описывающее конфигурацию кисти как функцию состояния сочленений. В той явной параметризации пространства $\mathcal{J}$, которая использовалась ранее, каждая компонента отображения f является дифференцируемой функцией переменных θ_i. Например, для робота с тремя шарнирными сочленениями это очевидно:

$$f(\theta_1, \theta_2, \theta_3) = \begin{pmatrix} l_3 \cos(\theta_1 + \theta_2) + l_2 \cos\theta_1 \\ l_3 \sin(\theta_1 + \theta_2) + l_2 \sin\theta_1 \\ \theta_1 + \theta_2 + \theta_3 \end{pmatrix}. \tag{5}$$

Следовательно, мы можем найти матрицу Якоби (т. е. матрицу частных производных) отображения f по отношению к переменным $\theta_1, \theta_2, \theta_3$. Пусть f_i есть i-я компонента отображения f. Тогда матрица Якоби — это

$$J_f(\theta_1, \theta_2, \theta_3) = \begin{pmatrix} \frac{\partial f_1}{\partial \theta_1} & \frac{\partial f_1}{\partial \theta_2} & \frac{\partial f_1}{\partial \theta_3} \\ \frac{\partial f_2}{\partial \theta_1} & \frac{\partial f_2}{\partial \theta_2} & \frac{\partial f_2}{\partial \theta_3} \\ \frac{\partial f_3}{\partial \theta_1} & \frac{\partial f_3}{\partial \theta_2} & \frac{\partial f_3}{\partial \theta_3} \end{pmatrix}.$$

Например, для отображения f из (5) имеем

$$J_f(\theta_1,\theta_2,\theta_3) = \begin{pmatrix} -l_3\sin(\theta_1+\theta_2) - l_2\sin\theta_1 & -l_3\sin(\theta_1+\theta_2) & 0 \\ l_3\cos(\theta_1+\theta_2) + l_2\cos\theta_1 & l_3\cos(\theta_1+\theta_2) & 0 \\ 1 & 1 & 1 \end{pmatrix}. \tag{6}$$

Из функциональной матрицы J_f мы можем получить числовую, подставляя значения переменных $j = (\theta_1, \theta_2, \theta_3)$. Через $J_f(j)$ мы будем обозначать полученную таким образом числовую матрицу. Она играет важную роль в анализе. Самым важным свойством матрицы $J_f(j)$ является то, что она задает линейное отображение, которое является *наилучшим линейным приближением* отображения f в точке $j \in \mathcal{J}$. Это означает, что в малой окрестности значения j отображение f и линейное отображение $J_f(j)$ ведут себя примерно одинаково. Другими словами, $J_f(j)$ представляет собой *производную* отображения f в точке $j \in \mathcal{J}$.

Прежде чем рассматривать кинематические особенности, определим (на интуитивном уровне) *размерности* пространства сочленений $\mathcal{J}$ и конфигурационного пространства $\mathcal{C}$. Они будут обозначаться $\dim(\mathcal{J})$ и $\dim(\mathcal{C})$ соответственно. Под размерностью пространства $\mathcal{J}$, например, мы будем понимать количество независимых «степеней свободы» при задании состояния сочленений. Каждое плоское соединение (шарнирное или призматическое) добавляет одну размерность в $\dim(\mathcal{J})$. Таким образом, пространство сочленений плоского робота с тремя шарнирными соединениями имеет размерность 3. Аналогично, $\dim(\mathcal{C})$ — это количество независимых степеней свободы при определении конфигурации (положения и ориентации) кисти. Для нашего плоского робота эта размерность также равна 3.

Пусть дан робот, у которого $\dim(\mathcal{J}) = m$ и $\dim(\mathcal{C}) = n$. Тогда якобиан отображения f является $n \times m$-функциональной матрицей. Если мы рассмотрим значение этой матрицы в точке $j \in \mathcal{J}$, то получим линейное отображение $J_f(j) : \mathbb{R}^m \to \mathbb{R}^n$, которое наилучшим образом приближает f в окрестности точки j. Важным инвариантом матрицы является ее *ранг*, который равен максимальному числу ее линейно независимых строк (или столбцов). В упражнениях будут рассмотрены некоторые свойства ранга. Так как $J_f(j)$ — это $n \times m$-матрица, то ее ранг не больше, чем $\min(m, n)$. Рассмотрим плоский робот с тремя шарнирными соединениями, у которого $l_2 = l_3 = 1$. Пусть $j = (0, \pi/2, \pi/3)$; тогда из (6) следует, что

$$J_f\left(0, \frac{\pi}{2}, \frac{\pi}{3}\right) = \begin{pmatrix} -1 & -1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Эта матрица имеет ранг 3 (максимально возможный в этом случае).

Мы говорим, что $J_f(j)$ имеет *максимальный ранг*, если ее ранг равен $\min(m, n)$ (максимальное возможное значение). В противном случае $J_f(j)$ называется матрицей *неполного ранга*. Если матрица имеет неполный ранг, то ее ядро больше, а образ меньше, чем можно было бы ожидать (см. упр. 14). Так как $J_f(j)$ является приближением для f, то неполнота ранга матрицы $J_f(j)$ указывает на

особое, или «сингулярное», поведение отображения f в окрестности точки j. Теперь дадим определение.

Определение 1. Точка $j \in \mathcal{J}$ называется *кинематической особенностью* робота, если ранг матрицы $J_f(j)$ строго меньше, чем $\min(\dim(\mathcal{J}), \dim(\mathcal{C}))$.

Например, кинематические особенности робота с тремя шарнирными соединениями — это те точки, в которых матрица (6) имеет ранг ≤ 2. Для квадратной $n \times n$-матрицы неполнота ранга означает, что ее определитель равен нулю. Имеем

$$\begin{aligned} 0 = \det(J_f) &= \sin(\theta_1 + \theta_2)\cos\theta_1 - \cos(\theta_1 + \theta_2)\sin\theta_1 \\ &= \sin\theta_2 \end{aligned}$$

в том и только том случае, когда $\theta_2 = 0, \pi$. Случай $\theta_2 = 0$ — это состояние, когда сегмент 3 направлен в ту же сторону, что и сегмент 2. Случай $\theta_2 = \pi$ — это состояние, когда сегмент 3 накладывается на сегмент 2. Это как раз те два случая, рассмотренные ранее, когда количество состояний пространства сочленений, отвечающих данной конфигурации для кисти, не равно двум.

Робот с тремя и более шарнирными соединениями обязательно имеет кинематические особенности.

Предложение 2. *Пусть $f : \mathcal{J} \to \mathcal{C}$ — конфигурационное отображение для плоского робота с $n \geq 3$ шарнирными соединениями. Тогда робот имеет кинематические особенности $j \in \mathcal{J}$.*

Доказательство. В упр. 7 к § 2 отображение f было явно определено формулой

$$f(\theta_1, \ldots, \theta_n) = \begin{pmatrix} \sum_{i=1}^{n-1} l_{i+1} \cos\left(\sum_{j=1}^{i} \theta_j\right) \\ \sum_{i=1}^{n-1} l_{i+1} \sin\left(\sum_{j=1}^{i} \theta_j\right) \\ \sum_{i=1}^{n} \theta_i \end{pmatrix}.$$

Следовательно, его матрица Якоби — это $3 \times n$-матрица вида

$$\begin{pmatrix} -\sum_{i=1}^{n-1} l_{i+1} \sin\left(\sum_{j=1}^{i} \theta_j\right) & -\sum_{i=2}^{n-1} l_{i+1} \sin\left(\sum_{j=1}^{i} \theta_j\right) & \ldots & -l_n \sin(\theta_{n-1}) & 0 \\ \sum_{i=1}^{n-1} l_{i+1} \cos\left(\sum_{j=1}^{i} \theta_j\right) & \sum_{i=2}^{n-1} l_{i+1} \cos\left(\sum_{j=1}^{i} \theta_j\right) & \ldots & l_n \cos(\theta_{n-1}) & 0 \\ 1 & 1 & \ldots & 1 & 1 \end{pmatrix}$$

Так как $n \geq 3$, то кинематической особенностью является точка, в которой ранг якобиана J_f не превосходит 2. Пусть в точке $j \in \mathcal{J}$ все θ_i — это 0 или π. Тогда каждый элемент первой строки матрицы $J_f(j)$ равен нулю. Следовательно, в этой точке ранг матрицы J_f не превышает двух.

Описание возможных движений робота, подобное тому, что мы дали выше, используется для *планирования* его движений, необходимых для выполнения поставленных перед ним задач. Методы, использованные нами, применимы (хотя бы теоретически) для создания программ автоматического управления роботом. Назначение таких программ — «проинструктировать» робота, какие изменения нужно сделать в состоянии сочленений, чтобы переместить кисть из одного положения в другое. Здесь возникают две основные проблемы: первая — найти *параметризованный путь* $c(t) \in \mathcal{C}$ от начальной точки в конфигурационном пространстве до требуемого положения, вторая — найти соответствующий путь $j(t) \in \mathcal{J}$, такой, что $f(j(t)) = c(t)$ для всех t. Кроме того, мы можем вводить дополнительные условия типа указанных ниже.

(i) Если путь $c(t)$ в конфигурационном пространстве замкнут (т. е. начальная и конечная конфигурации совпадают), то можно потребовать, чтобы путь $j(t)$ тоже был замкнут. Это требование важно для роботов, выполняющих *повторяющиеся* операции (например, сварку деталей автомобиля). Если путь в пространстве сочленений замкнут, то состояние сочленений возобновляется, и робот может просто повторить выполнение задания.

(ii) Для реального робота необходимо ограничить *скорости движения* сочленений. Слишком быстрые (или резкие) движения могут испортить механизм.

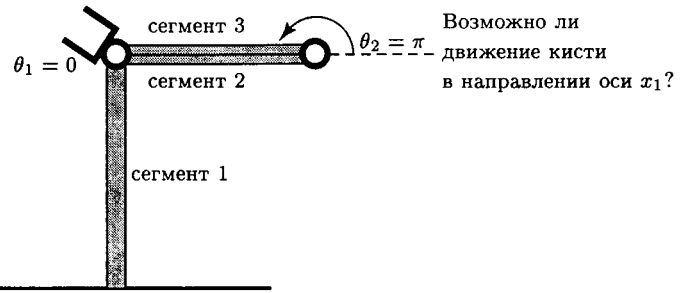
(iii) Суммарное движение желательно минимизировать.

Кинематические особенности играют важную роль в планировании движения. Посмотрим, где могут возникать осложнения. Пусть путь $c(t)$ в конфигурационном пространстве таков, что соответствующий путь $j(t)$ в пространстве сочленений проходит вблизи или через особенность. Имеем

$$c'(t) = J_f(j(t)) \cdot j'(t). \tag{7}$$

Мы можем интерпретировать $c'(t)$ как *скорость* движения по пути *в конфигурационном пространстве*, а $j'(t)$ — как соответствующую *скорость движения в пространстве сочленений*. Если в момент t_0 путь в пространстве сочленений проходит *через* особенность, то уравнение (7) может *не* иметь решения $j'(t_0)$ (потому что матрица $J_f(j(t_0))$ имеет неполный ранг). Это означает, что может *не* существовать гладкого пути $j(t)$, который соответствовал бы пути $c(t)$ в

конфигурационном пространстве. Рассмотрим, например, кинематическую особенность с $\theta_2 = \pi$ плоского робота с тремя шарнирными соединениями. Если $\theta_1 = 0$, то сегменты 2 и 3 направлены вдоль оси x_1:



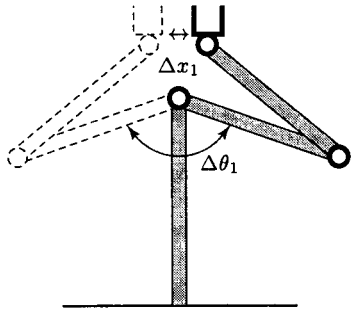
Кинематическая особенность

Если направления сегментов 2 и 3 противоположны, как на рисунке, то кисть не может двигаться в направлении оси x_1. Точнее, пусть путь в конфигурационном пространстве таков, что $c'(t_0)$ — вектор в направлении оси x_1. Используя формулу (6), преобразуем (7) к виду

$$c'(t_0) = J_f(j(t_0)) \cdot j'(t_0) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \cdot j'(t_0).$$

Так как первая строка матрицы $J_f(j(t_0))$ состоит из одних нулей, то это уравнение не может быть разрешено относительно $j'(t_0)$, если x_1-компонента вектора $c'(t_0)$ не равна нулю. Другими словами, в пространстве сочленений нет гладкого пути, соответствующего пути $c(t)$. Это типичный пример того, какие трудности здесь могут возникать.

Если $j(t_0)$ находится *вблизи* особенности, трудности все равно остаются, потому что $J_f(j(t_0))$ мало отличается от матрицы неполного ранга. Численная техника линейной алгебры показывает, что если матрица $J_f(j(t_0))$ близка к матрице неполного ранга, то очень большая скорость в пространстве сочленений соответствует малой скорости в конфигурационном пространстве. В качестве примера опять рассмотрим плоский робот с тремя шарнирными соединениями и с $\theta_2 = \pi$. Как показывает рисунок, перемещение из положения A в положение B (обе эти точки находятся вблизи начала координат) требует большого изменения угла θ_1, хотя кисть перемещается на короткое расстояние.



Вблизи кинематической особенности

Чтобы избежать этих нежелательных ситуаций, мы должны аккуратно задавать путь $c(t)$ в конфигурационном пространстве. Методы определения таких «правильных» путей активно изучаются в настоящее время. К сожалению, эта область исследований находится за пределами нашей книги. Если читатель хочет ознакомиться с этой областью подробнее, он может обратиться к книге PAUL (1981) — стандартному введению в роботику. В обзоре BUCHBERGER (1985) рассматриваются возможности применения базисов Грёбнера для решения обратной кинематической задачи. Несложное введение в недавние исследования обратной кинематической задачи и управления движением, содержащее ссылки на оригинальные работы, имеется в книге BAILLIEUL ET AL. (1990).

Упражнения к § 3

1. Рассмотрим специализацию базиса Грёбнера (2) к случаю $l_2 = l_3 = 1$.
   (a) Подставьте $l_2 = l_3 = 1$ непосредственно в (2) и упростите.
   (b) Положите $l_2 = l_3 = 1$ в (1) и вычислите базис Грёбнера «специализированного» идеала, порожденного полиномами из (1), опять-таки используя lex-упорядочение с $c_2 > s_2 > c_1 > s_1$. Сравните результаты пп. (a) и (b). Они должны совпасть.
2. В этом упражнении будет рассмотрена геометрия плоского робота с тремя шарнирными соединениями и длинами сегментов $l_2 = l_3 = 1$.
   (a) Постройте рисунок, демонстрирующий два решения обратной кинематической задачи при $a \neq 0, a^2 + b^2 \neq 4$. Почему в этом случае c_2 не зависит от s_1? Указание: какой четырехугольник образуют сегменты робота для двух возможных состояний с положением кисти в точке (a, b)? Как связаны два соответствующих значения θ_2?

(b) С помощью рисунка или другим способом объясните геометрический смысл двух решений системы (4) в случае $a = 0$. В частности, объясните, почему s_1 должно иметь только одно значение. Указание: как связаны два значения θ_1 на вашем рисунке?

3. Рассмотрим робот с $l_2 = l_3 = 1$. Положим $a = b = 0$ в (1) и вычислим базис Грёбнера соответствующего идеала. Отличается ли этот базис от базисов (3) и (4)? Как это отличие объясняет свойства кинематической особенности в $(0, 0)$?

4. В этом упражнении будет рассмотрена геометрия того же робота при $l_2 \neq l_3$.
   (a) Положим $l_2 = 1, l_3 = 2$. Решите систему (2) относительно s_1, c_1, s_2, c_2. Объясните геометрический смысл решения, выявите и интерпретируйте все специальные случаи. Чем этот случай отличается от случая $l_2 = l_3 = 1$, разобранного в тексте параграфа?
   (b) Проведите аналогичное исследование случая $l_2 = 2, l_3 = 1$.

Мы уже убедились на примерах, что вид базиса Грёбнера некоторого идеала может измениться при специализации параметров. В упр. 5–9 мы рассмотрим еще ряд примеров и докажем некоторые утверждения о специализации базисов Грёбнера.

5. Рассмотрим на примере, как знаменатели элементов базиса Грёбнера могут создавать трудности при специализации. Пусть $I = \langle f, g \rangle$, где $f = x^2 - y, g = (y - tx)(y - t) = -txy + t^2x + y^2 - ty$, а t — параметр. Мы будем использовать lex-упорядочение с $x > y$.
   (a) Найдите редуцированный базис Грёбнера для I в $\mathbb{R}(t)[x, y]$. Что из себя представляют знаменатели элементов базиса?
   (b) Положим $t = 0$ в f и g и вычислим базис Грёбнера заново. Чем это базис отличается от базиса из п. (a)? Что получится, если мы освободимся от знаменателей в базисе из (a) и положим $t = 0$?
   (c) Как многообразие $\mathbf{V}(I) \subset \mathbb{R}^2$ зависит от выбора $t \in \mathbb{R}$? Является ли случай $t = 0$ особым с геометрической точки зрения?
   (d) Первый шаг алгоритма Бухбергера для нахождения базиса Грёбнера состоит в вычислении S-полинома $S(f, g)$. Вычислите этот полином вручную в $\mathbb{R}(t)[x, y]$. Обратите внимание, что отличия случая $t = 0$ проявляются уже на этом шаге.

6. В этом упражнении мы рассмотрим более тонкий пример того, какие неприятности могут происходить при специализации. Пусть $I = \langle x + ty, x + y \rangle \subset \mathbb{R}(t)[x, y]$, где t — параметр. Мы будем использовать lex-упорядочение с $x > y$.
   (a) Докажите, что $\{x, y\}$ является редуцированным базисом Грёбнера идеала I. Обратите внимание, что ни исходный базис, ни базис Грёбнера не имеют знаменателей.
   (b) Положим $t = 1$. Докажите, что $\{x+y\}$ является базисом Грёбнера специализированного идеала $\bar{I} \subset \mathbb{R}[x, y]$.
   (c) Чтобы увидеть, почему значение $t = 1$ является особым, выразите элементы базиса Грёбнера $\{x, y\}$ через элементы исходного базиса $\{x + ty, x + y\}$. Какие знаменатели появились? В следующем упражнении мы объясним в общем случае, что при этом происходит.

7. В этом упражнении мы выведем условия, при которых вид базиса Грёбнера *не* меняется при специализации. Рассмотрим идеал

$$I = \langle f_i(t_1, \ldots, t_m, x_1, \ldots, x_n) : 1 \leq i \leq s \rangle$$

в $k(t_1, \ldots, t_m)[x_1, \ldots, x_n]$ и зафиксируем некоторое мономиальное упорядочение. Мы будем считать $t_1, \ldots, t_m$ параметрами из коэффициентов полиномов $f_1, \ldots, f_s$. Поделим каждый f_i на его старший коэффициент (принадлежащий полю $k(t_1, \ldots, t_m)$) и будем считать все старшие коэффициенты полиномов f_i равными 1. Пусть теперь $\{g_1, \ldots, g_t\}$ — редуцированный базис Грёбнера идеала I, т. е. старшие коэффициенты полиномов g_i также равны 1. Пусть, наконец, $(t_1, \ldots, t_m) \mapsto (a_1, \ldots, a_m) \in k^m$ — такая специализация параметров, что ни один из знаменателей в f_i и g_i не обращается в нуль в $(a_1, \ldots, a_m)$.
   (a) Используя алгоритм деления, мы можем найти такие $A_{ij} \in k(t_1, \ldots, t_m)[x_1, \ldots, x_n]$, что

$$f_i = \sum_{j=1}^{t} A_{ij} g_j.$$

   Докажите, что ни один из знаменателей в A_{ij} не обращается в нуль в точке $(a_1, \ldots, a_m)$.
   (b) Мы можем представить g_j в виде

$$g_j = \sum_{i=1}^{s} B_{ji} f_i,$$

   для некоторых $B_{ji} \in k(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. Упражнение 6 показывает, что в B_{ji} могут появиться «новые» знаменатели. Предположим теперь, что ни один из знаменателей в B_{ji} не обращается в нуль при специализации $(t_1, \ldots, t_m) \mapsto (a_1, \ldots, a_m)$. Обозначим через $\bar{I}$ идеал в $k[x_1, \ldots, x_n]$, порожденный специализированными полиномами f_i. Докажите в этих предположениях, что специализированные полиномы g_j образуют базис идеала $\bar{I}$.
   (c) Докажите, что специализированные полиномы g_j образуют базис Грёбнера для $\bar{I}$. Указание: мономиальное упорядочение, использованное для вычисления базиса, учитывает только переменные x_i. Параметры t_j этим упорядочением рассматриваются как «константы».
   (d) Пусть $d_1, \ldots, d_M \in k[t_1, \ldots, t_m]$ — все знаменатели, которые встречаются в f_i, g_j и B_{ji}, и пусть $W = \mathbf{V}(d_1, \ldots, d_M) \subset k^m$. Докажите, что $\{g_1, \ldots, g_t\}$ остается базисом Грёбнера идеала $\langle f_1, \ldots, f_s \rangle$ при специализации $(t_1, \ldots, t_m) \mapsto (a_1, \ldots, a_m) \in k^m - W$.

8. Опишем алгоритм для нахождения всех специализаций, сохраняющих базис Грёбнера. Мы будем использовать обозначения предыдущего упражнения. Другими словами, алгоритм должен найти все знаменатели $d_1, \dots, d_M$, появляющиеся в f_i, g_j и B_{ji}. Это легко сделать для f_i и g_j, но для B_{ji} — это более трудная задача. Проблема состоит в том, что f_i не образуют базис Грёбнера и потому мы не можем использовать алгоритм деления для вычисления B_{ji}. К счастью, нас интересуют только знаменатели. Мы будем работать в кольце $k[t_1, \dots, t_m, x_1, \dots, x_n]$. Умножая f_i и g_j на подходящие полиномы из $k[t_1, \dots, t_m]$, мы получим полиномы

$$\tilde{f}_i, \tilde{g}_j \in k[t_1, \dots, t_m, x_1, \dots, x_n].$$

Пусть $\widetilde{I} \subset k[t_1, \dots, t_m, x_1, \dots, x_n]$ — идеал, порожденный всеми $\tilde{f}_i$.

(a) Пусть $g_j = \sum_{i=1}^{s} B_{ji} f_i$ в $k(t_1, \dots, t_m)[x_1, \dots, x_n]$, и пусть полином $d \in k[t_1, \dots, t_m]$ делится на все знаменатели коэффициентов полиномов f_i, g_j и B_{ji}. Докажите, что

$$d \in (\widetilde{I} : \tilde{g}_j) \cap k[t_1, \dots, t_m],$$

где $\widetilde{I} : \tilde{g}_j$ — частное идеалов, определенное в § 4 гл. 4.

(b) Постройте алгоритм, вычисляющий $(\widetilde{I} : \tilde{g}_j) \cap k[t_1, \dots, t_m]$, и с его помощью постройте алгоритм, описывающий подмножество $W \subset k^m$, определенное в п. (d) упр. 7.

9. Вычисления, требуемые описанным выше алгоритмом, могут оказаться слишком сложными для некоторых систем компьютерной алгебры. К счастью, есть более быстрые методы, применимые в некоторых случаях. Пусть $f_i, g_j \in k(t_1, \dots, t_m)[x_1, \dots, x_n]$ такие же, как в упр. 7 и 8. Как быстро проверить, что полиномы g_j образуют базис Грёбнера при всех специализациях, при которых знаменатели в f_i и g_j не обращаются в нуль?

(a) Пусть $d \in k[t_1, \dots, t_m]$ — наименьшее общее кратное всех знаменателей коэффициентов полиномов f_i и g_j, и пусть $\tilde{f}_i = df_i$, $\tilde{g}_j = dg_j$. Тогда $\tilde{f}_i, \tilde{g}_j \in k[t_1, \dots, t_m, x_1, \dots, x_n]$. Рассмотрим идеал $\widetilde{I} \subset k[t_1, \dots, t_m, x_1, \dots, x_n]$, порожденный всеми $\tilde{f}_i$. Предположим, что $d\tilde{g}_j \in \widetilde{I}$ для всех j. Докажите, что специализация $(t_1, \dots, t_m) \mapsto (a_1, \dots, a_m)$ корректна для всех $(a_1, \dots, a_m) \in k^m - \mathbf{V}(d)$.

(b) Опишите алгоритм, реализующий критерий из п. (a). Какое мономиальное упорядочение будет здесь наиболее эффективно?

(c) Примените алгоритм п. (b) для анализа системы (1) в тексте параграфа. Этим вы докажете, что (2) остается базисом Грёбнера для (1) при всех специализациях $l_2 \neq 0, l_3 \neq 0, a \neq 0$ и $a^2 + b^2 \neq 0$.

10. В этом упражнении мы научимся вычислять базис Грёбнера идеала в кольце $k(t_1, \dots, t_m)[x_1, \dots, x_n]$, работая в полиномиальном кольце $k[t_1, \dots, t_m, x_1, \dots, x_n]$. Это важно уметь, потому что система компьютерной алгебры может отказаться вычислять базис Грёбнера, если коэффициенты принадлежат полю функций. Сначала зададим мономиальное упорядочение так, чтобы моном, содержащий хотя бы один x_i, был больше всех мономов, содержащих только t_j. Например, мы можем взять lex-упорядочение с $x_1 > \dots > x_n > t_1 > \dots > t_m$.

(a) Пусть I — идеал в $k(t_1, \dots, t_m)[x_1, \dots, x_n]$. Докажите, что I может быть представлен в виде

$$I = \langle f_i(t_1, \dots, t_m, x_1, \dots, x_n) : 1 \leq i \leq s \rangle,$$

где $f_i \in k[t_1, \dots, t_m, x_1, \dots, x_n]$.

(b) Пусть $\widetilde{I}$ — идеал в $k[t_1, \dots, t_m, x_1, \dots, x_n]$, порожденный $f_1, \dots, f_s$, и пусть $g_1, \dots, g_t$ — редуцированный базис Грёбнера для $\widetilde{I}$ по отношению к определенному выше мономиальному упорядочению. Докажите, что если некоторый g_j лежит в $k[t_1, \dots, t_m]$, то $I = k(t_1, \dots, t_m)[x_1, \dots, x_n]$.

(c) Пусть $g_1, \dots, g_t$ — базис Грёбнера идеала $\widetilde{I}$ из п. (b), и предположим, что ни один g_j не принадлежит $k[t_1, \dots, t_m]$. Докажите, что $g_1, \dots, g_t$ составляют базис Грёбнера идеала I (по отношению к мономиальному упорядочению, определенному на мономах из $k[x_1, \dots, x_n]$).

11. Рассмотрим плоский робот с двумя шарнирными соединениями и одним призматическим соединением, описанный в упр. 4 к § 2.

(a) Пусть положение кисти и ее ориентация заданы. Составьте систему уравнений, подобную системе (1), решениями которой являются те состояния пространства сочленений, которые соответствуют заданной конфигурации кисти. Рассмотрите случай, когда $l_2 = 1$.

(b) Используя систему компьютерной алгебры, найдите решение этих уравнений, т. е. найдите базис Грёбнера соответствующего идеала для некоторого lex-упорядочения. Указание: возможно, вам потребуется несколько попыток, чтобы выбрать подходящее упорядочение.

(c) Что является решением обратной кинематической задачи для этого робота? Другими словами, какие положения и ориентация кисти возможны? Сколько различных состояний пространства сочленений соответствуют одной конфигурации? (Напомним, что пространство состояний призматического соединения является интервалом $[0, m_3] \subset \mathbb{R}$.)

(d) Имеет ли этот робот кинематические особенности? Если да, то опишите их.

12. Рассмотрим плоский робот с тремя шарнирными соединениями и одним призматическим соединением, рассмотренный в примере 2 из § 2.

(a) Пусть положение кисти и ее ориентация заданы. Составьте систему уравнений, подобную системе (1), решениями которой явля-

ются те состояния пространства сочленений, которые соответствуют заданной конфигурации. Пусть $l_2 = l_3 = 1$, а $l_4 \in [1, 2]$. Указание: ваша система *должна* учитывать ориентацию кисти.

(b) Решите вашу систему, вычислив базис Грёбнера соответствующего идеала при подходящем lex-упорядочении. Указание: возможно, вам потребуется несколько попыток, чтобы выбрать подходящее упорядочение. «Плохой» порядок переменных приводит к чрезмерно сложным вычислениям.

(c) Что является решением обратной кинематической задачи для этого робота? Другими словами, какие положения и ориентация кисти возможны? Изменяется ли множество возможных ориентаций при изменении положения кисти? (Не забудьте, что $l_4 \in [1, 2] \subset \mathbb{R}$.)

(d) Сколько различных состояний пространства сочленений соответствуют одной конфигурации кисти в общем случае? Есть ли особые случаи?

(e) Есть ли у этого робота кинематические особенности? Если да, то опишите соответствующие конфигурации кисти и свяжите их с особыми случаями из п. (d).

13. Рассмотрим трехмерный робот с двумя трехмерными «круговыми» соединениями из упр. 8 к § 2.

(a) Пусть заданы положение кисти и ее ориентация. Составьте систему уравнений, подобную системе (1), решениями которой являются все состояния пространства сочленений, соответствующие заданной конфигурации. Рассмотрите, например, случай, когда $l_2 = 4, l_3 = 2$.

(b) Решите эту систему, вычислив базис Грёбнера соответствующего идеала для подходящего lex-упорядочения. Указание: один из элементов базиса Грёбнера будет зависеть только от координат положения кисти. Что это значит с геометрической точки зрения? Является ли ответ осмысленным с точки зрения геометрии робота?

(c) Что является решением обратной кинематической задачи для этого робота? Другими словами, какие положения и ориентация кисти возможны?

(d) Сколько различных состояний пространства сочленений соответствует одной конфигурации кисти в общем случае? Есть ли особые случаи?

(e) Есть ли у этого робота кинематические особенности?

14. Рассмотрим вещественную $m \times n$-матрицу A. Нас будет интересовать ее ранг, т. е. максимальное количество линейно независимых столбцов (или строк) в ней. Эта матрица определяет линейное отображение $L_A : \mathbb{R}^n \to \mathbb{R}^m$, причем ее ранг равен размерности образа отображения L_A. Напомним, что A называется матрицей максимального ранга, если ее ранг равен $\min(m, n)$. Для того чтобы понять, что означает максимальность ранга, рассмотрим три случая.

(a) Пусть $m = n$. Докажите, что A является матрицей максимального ранга тогда и только тогда, когда $\det(A) \neq 0$, а это эквивалентно тому, что L_A является изоморфизмом векторных пространств.

(b) Пусть $m < n$. Докажите, что A является матрицей максимального ранга тогда и только тогда, когда уравнение $A \cdot \mathbf{x} = \mathbf{b}$ имеет решение для всех $\mathbf{b} \in \mathbb{R}^m$, а это эквивалентно тому, что L_A — сюръективное (т. е. «на») отображение.

(c) Пусть $m > n$. Докажите, что A является матрицей максимального ранга тогда и только тогда, когда уравнение $A \cdot \mathbf{x} = \mathbf{b}$ имеет не более одного решения для всех $\mathbf{b} \in \mathbb{R}^m$, а это эквивалентно тому, что L_A является инъективным отображением.

15. Робот называется *кинематически избыточным*, если размерность пространства сочленений $\mathcal{J}$ *больше*, чем размерность конфигурационного пространства $\mathcal{C}$.

(a) Какие роботы из числа рассмотренных в тексте параграфа и в упражнениях являются кинематически избыточными?

(b) (Это часть требует знания теоремы о неявной функции.) Пусть дан кинематически избыточный робот и $j \in \mathcal{J}$ не является кинематической особенностью. Что можно сказать о прообразе $f^{-1}(f(j))$? В частности, сколько различных состояний пространства сочленений соответствует конфигурации $f(j)$?

16. Докажите формулу (7) для плоского робота с тремя шарнирными соединениями. Указание: сделайте подстановку $\theta_i = \theta_i(t)$ и найдите производную пути $f(\theta_1(t), \theta_2(t), \theta_3(t))$ в конфигурационном пространстве по t.

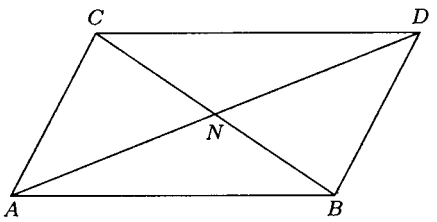
§ 4. Автоматическое доказательство геометрических теорем

Геометрическое описание робота и его движения (рассмотренное нами в первых трех параграфах этой главы) используется управляющей программой для планирования его движений с целью выполнить требуемую задачу. Управляющая программа «размышляет» о геометрических ограничениях, связанных как с конструкцией робота, так и с условиями его работы, и «находит» подходящее решение задачи движения. В этом параграфе и в следующем мы рассмотрим близкую задачу — автоматизацию геометрических рассуждений. Мы обсудим два алгоритмических метода проверки справедливости утверждений общего характера в евклидовой геометрии. Эти методы полезны в области искусственного интеллекта (ИИ) и геометрического моделирования, так как используются при создании программ проверки существования гипотетических связей между геометрическими объектами на плоскости или теорем о них.

Существует мнение, что такие программы демонстрируют понимание *смысла* геометрических утверждений, сравнимое с пониманием ученого-геометра. На самом деле вопрос о способности компьютера к интеллектуальному поведению совершенно неясен. Тем не менее интересно отметить, что несколько новых (т. е. до тех пор неизвестных) теорем было доказано этими методами. В некотором ограниченном смысле, эти «доказыватели теорем» способны «размышлять» о геометрических конфигурациях, т. е. делать то, что раньше считали уделом исключительно человеческого разума.

Основа этих методов состоит в том, что, как только заданы декартовы координаты на евклидовой плоскости, условия, а также заключения некоторых геометрических теорем могут быть заданы *полиномиальными уравнениями* от координат тех точек, о которых говорится в формулировках соответствующих утверждений[1]. Вот простой пример.

Пример 1. Пусть A, B, C, D — вершины параллелограмма на плоскости, представленного на рисунке:



Общеизвестная теорема утверждает, что диагонали $\overline{AD}$ и $\overline{BC}$ в точке пересечения N делятся пополам. Другими словами, $AN = ND$ и $BN = NC$, где через XY мы обозначаем длину сегмента $\overline{XY}$, соединяющего точки X и Y. Стандартное доказательство использует равенство треугольников $\triangle ANC$ и $\triangle BND$ (см. упр. 1).

Чтобы установить связь этой теоремы с алгебраической геометрией, мы покажем, как конфигурация параллелограмма и его диагоналей (условия теоремы), а также утверждение, что точка N делит диагонали пополам (заключение теоремы), могут быть записаны в полиномиальной форме.

[1] В действительности этот круг идей восходит к «Эрлангенской программе» Феликса Клейна (Klein F. Vergleichende Betrachtungen über neue geometrische Forschungen. — Erlangen, 1872 [имеется перевод: Клейн Ф. Сравнительное обозрение новейших геометрических исследований. — Изв. физ.-мат. о-ва при Казанском унив., 1896, т. 5] и Klein F. Elementarmathematik von höheren standpunkte aus. B. 2. Geometrie. — Berlin: Springer-Verlag, 1925 [имеется перевод: Клейн Ф. Элементарная математика с точки зрения высшей. Т. 2. Геометрия. — М.: Наука, 1987]). Современные исследования по «автоматическому доказательству геометрических теорем» можно рассматривать как техническую разработку алгебраического аспекта Эрлангенской программы. — *Прим. ред.*

Свойства параллелограмма не зависят от сдвигов и поворотов плоскости. Значит, мы можем сдвигами и поворотами придать параллелограмму желательное положение, или, что эквивалентно, выбрать систему координат удобным нам образом. Проще всего сделать это так: точку A мы помещаем в начало координат, а сторону $\overline{AB}$ совмещаем с горизонтальной осью. Другими словами, $A = (0, 0)$, а $B = (u_1, 0)$ для некоторого $u_1 \neq 0 \in \mathbb{R}$. Мы рассматриваем u_1 как неизвестную или переменную, значения которой могут быть выбраны произвольно в множестве $\mathbb{R} - \{0\}$. Точка C имеет координаты (u_2, u_3), где u_2, u_3 — новые переменные, не зависящие от u_1, и $u_3 \neq 0$. Координаты точки D полностью определены координатами точек A, B, C.

При построении геометрической конфигурации, описываемой теоремой, координаты некоторых точек будут *произвольными*, тогда как координаты остальных точек будут *определены* (с точностью до конечного числа возможностей) значениями «произвольных» координат. Произвольные координаты будут обозначаться через u_i, а другие координаты — через x_j. Следует отметить, что разделение координат на два подмножества не задается однозначно условиями задачи. Различные способы описания одной и той же конфигурации приводят к различным множествам произвольных переменных и к различным полиномиальным формулировкам условий теоремы.

Так как D определяется точками A, B, C, то запишем $D = (x_1, x_2)$. Одним из условий теоремы является то, что четырехугольник $ABDC$ — параллелограмм, т. е. его противоположные стороны параллельны, а следовательно, имеют одинаковые углы с осью абсцисс. Имеем:

$$\overline{AB}||\overline{CD}: \quad 0 = \frac{x_2 - u_3}{x_1 - u_2},$$
$$\overline{AC}||\overline{BD}: \quad \frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1}.$$

Освобождаясь от знаменателей, переходим к полиномиальным уравнениям

$$\begin{aligned} h_1 &= x_2 - u_3 = 0, \\ h_2 &= (x_1 - u_1)u_3 - x_2 u_2 = 0. \end{aligned} \tag{1}$$

(Ниже мы рассмотрим другой способ вывода уравнений для x_1 и x_2.)

Теперь мы должны построить точку пересечения диагоналей. Так как координаты этой точки N определены координатами вершин, то $N = (x_3, x_4)$. Утверждение, что N является пересечением

диагоналей, означает, что N принадлежит и прямой $\overline{AD}$, и прямой $\overline{BC}$. Другими словами, тройки точек A, N, D и B, N, C ***коллинеарны***. Это дает следующие соотношения:

$$A,N,D \text{ коллинеарны} : \frac{x_4}{x_3} = \frac{u_3}{x_1},$$
$$B,N,C \text{ коллинеарны} : \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}.$$

Освобождаясь от знаменателей, переходим к полиномиальным уравнениям

$$\begin{aligned} h_3 &= x_4x_1 - x_3u_3 = 0, \\ h_4 &= x_4(u_2 - u_1) - (x_3 - u_1)u_3 = 0. \end{aligned} \tag{2}$$

Система уравнений, составленная из уравнений (1) и (2), и является переводом условий теоремы на язык полиномов.

Заключения теоремы могут быть также записаны в полиномиальном виде (с помощью теоремы Пифагора):

$$AN = ND : x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2,$$
$$BN = NC : (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2.$$

Упрощая эти выражения, перепишем эти утверждения в следующем виде:

$$\begin{aligned} g_1 &= x_1^2 - 2x_1x_3 - 2x_2x_4 + x_2^2 = 0, \\ g_2 &= 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0. \end{aligned} \tag{3}$$

Алгебраическая формулировка теоремы такова: если выполнены условия (1) и (2), то (3) также имеет место.

Мы уже отмечали, что можно различными способами перевести условия и заключения теоремы на язык полиномов. В упр. 2, например, даны различные алгебраические формулировки теоремы о диагоналях, использующие различные конструкции параллелограмма (т. е. различные множества произвольных координат). Кроме того, имеются различные способы перевода геометрических условий на алгебраический язык. Например, способ, которым мы описали, что $ABDC$ — параллелограмм, в виде уравнений (1), есть демонстрация того, как ***компьютерная программа*** могла бы формализовать тот факт, что $\overline{AB}||\overline{CD}$. Другой метод перевода может использовать то, что D есть просто *сумма векторов* $B = (u_1, 0)$ и $C = (u_2, u_3)$. Тогда в этой формализации (напомним, что $D = (x_1, x_2)$)

$$\begin{aligned} h_1' &= x_1 - u_1 - u_2 = 0, \\ h_2' &= x_2 - u_3 = 0. \end{aligned} \tag{4}$$

Уравнения (4) значительно проще уравнений (1). Если мы хотим создать доказыватель геометрических теорем, который умел бы давать алгебраическую формулировку условия «$ABDC$ — параллелограмм» ***непосредственно*** (т. е. не делая дополнительной редукции к виду «$\overline{AB}||\overline{CD}$ и $\overline{AC}||\overline{BD}$»), то (4), конечно, предпочтительнее (1). Далее, h_2' можно использовать для ***исключения*** переменной x_2 из условий и заключений, что даст нам более простую систему уравнений. В реальных задачах, связанных со сложными геометрическими конструкциями, такие предварительные упрощения могут быть просто необходимы.

Следующее предложение представляет собой список наиболее часто встречающихся геометрических утверждений и методов их перевода на язык полиномов.

Предложение 2. *Пусть A, B, C, D, E, F — точки плоскости. Каждое из следующих утверждений может быть записано в виде одного или нескольких полиномиальных уравнений:*

(i) $\overline{AB}$ *параллелен* $\overline{CD}$;
(ii) $\overline{AB}$ *перпендикулярен* $\overline{CD}$;
(iii) A, B, C *коллинеарны;*
(iv) *расстояние от* A *до* B *равно расстоянию от* C *до* D : $AB = CD$;
(v) C *лежит на окружности с центром в* A *радиуса* AB;
(vi) C *— середина отрезка* $\overline{AB}$;
(vii) *острый угол* $\angle ABC$ *равен острому углу* $\angle DEF$;
(viii) $\overline{BD}$ *делит пополам угол* $\angle ABC$.

Доказательство. Метод перевода утверждений (i), (iii) и (iv) на язык полиномов рассмотрен в примере 1. Утверждение (v) эквивалентно утверждению $AC = AB$. Утверждение (vi) есть конъюнкция двух утверждений: A, B, C коллинеарны *и* $AC = CB$. Утверждения (ii), (vii) и (viii) будут рассмотрены в упр. 4.

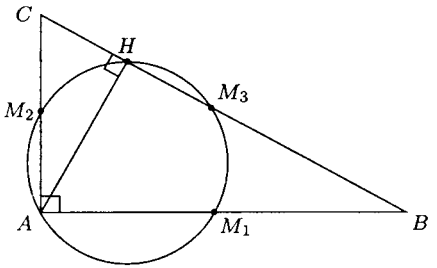
В упр. 3 предлагаются другие типы геометрических утверждений, которые также могут быть переформулированы с помощью полиномиальных уравнений. Геометрическую теорему мы назовем *допустимой*, если и ее условия, и ее заключения могут быть сформулированы на языке полиномов. Каждая допустимая теорема имеет много эквивалентных алгебраических формулировок: перевод всегда неоднозначен.

Адекватное преобразование условий теоремы в систему полиномиальных уравнений легче всего осуществить, если ***конструировать*** чертеж, иллюстрирующий рассматриваемую конфигурацию,

шаг за шагом. Это как раз то самое, что мы делали в примере 1 и что будем делать в следующем примере.

Пример 3. Предложение 2 будет применено для преобразования следующего красивого результата в систему уравнений.

Теорема (теорема Аполлония об окружности). *Рассмотрим на плоскости прямоугольный треугольник $\triangle ABC$ с прямым углом в вершине A. Тогда середины сторон и основание высоты, опущенной из A на $\overline{BC}$, лежат на одной окружности.*



Упражнение 1 посвящено стандартному геометрическому доказательству этой теоремы. А здесь мы преобразуем теорему в полиномиальную форму, доказав тем самым, что эта теорема допустима. Начнем с построения треугольника. Поместим точку A в $(0,0)$, а точку B в $(u_1,0)$; тогда так как угол $\angle CAB$ прямой, то $C=(0,u_2)$. (Разумеется, мы пропускаем некоторые этапы рассуждения: точку C можно было бы выбрать произвольно и добавить условие $CA \perp AB$, что привело бы к большему числу переменных и уравнений.)

Теперь мы построим середины сторон. Эти точки имеют следующие координаты: $M_1=(x_1,0), M_2=(0,x_2), M_3=(x_3,x_4)$. Как и в примере 1, переменные u_1,u_2 произвольны, а переменные x_j определены значениями переменных u_1,u_2. Используя п. (vi) предложения 2, получаем уравнения

$$\begin{aligned} h_1 &= 2x_1 - u_1 = 0,\\ h_2 &= 2x_2 - u_2 = 0,\\ h_3 &= 2x_3 - u_1 = 0,\\ h_4 &= 2x_4 - u_2 = 0. \end{aligned} \tag{5}$$

На следующем шаге мы построим точку $H=(x_5,x_6)$ — основание высоты, опущенной из A. Построение использует два условия:

$$\begin{aligned} AH \perp BC &: h_5 = x_5u_1 - x_6u_2 = 0,\\ B,H,C \text{ коллинеарны} &: h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0. \end{aligned} \tag{6}$$

Наконец, нужно записать алгебраически условие, что точки M_1,M_2,M_3,H лежат на одной окружности. В общем случае набор из четырех точек *не* лежит на окружности (поэтому утверждение этой теоремы и является интересным). Но *три* неколлинеарные точки всегда лежат на окружности (на *описанной* окружности треугольника, образованного этими точками). Следовательно, заключение теоремы может быть сформулировано так: если мы построим окружность, на которой лежат неколлинеарные точки M_1,M_2,M_3, то и точка H лежит на *этой* окружности. Для того чтобы применить п. (v) предложения 2, мы должны знать координаты центра окружности; поэтому нам нужно будет ввести дополнительную точку $O=(x_7,x_8)$ и дополнительные условия

$$\begin{aligned} M_1O=M_2O &: h_7=(x_1-x_7)^2+x_8^2-x_7^2-(x_8-x_2)^2=0,\\ M_1O=M_3O &: h_8=(x_1-x_7)^2+x_8^2-(x_3-x_7)^2-(x_4-x_8)^2=0. \end{aligned} \tag{7}$$

Теперь заключение теоремы — это $HO=M_1O$, и оно принимает вид

$$g=(x_5-x_7)^2+(x_6-x_8)^2-(x_1-x_7)^2-x_8^2=0. \tag{8}$$

Отметим, что и здесь, и в примере 1, количество условий *равно* количеству *зависимых* переменных. Так и должно быть для правильно поставленной геометрической задачи. Мы ожидаем, что при заданных u_i существует не более конечного числа различных комбинаций x_j, удовлетворяющих полученным уравнениям.

Рассмотрим типичную алгебраическую форму допустимой геометрической теоремы. Имеется некоторое число произвольных координат или независимых переменных, обозначаемых $u_1,\ldots,u_m$. Кроме того, имеется некоторое множество зависимых переменных $x_1,\ldots,x_n$. Условия теоремы представлены в виде системы полиномиальных уравнений от переменных u_i,x_j. Как мы отметили в примере 2, для правильно поставленной теоремы число условий равно числу зависимых переменных, т. е. мы запишем условия в следующем виде:

$$\begin{aligned} h_1(u_1,\ldots,u_m,x_1,\ldots,x_n)&=0,\\ &\vdots\\ h_n(u_1,\ldots,u_m,x_1,\ldots,x_n)&=0. \end{aligned} \tag{9}$$

Заключения теоремы также представлены полиномами от u_i,x_j. Достаточно рассмотреть случай *одного* заключения, потому что в противном случае мы можем просто рассматривать их по очереди. Запишем заключение в следующем виде:

$$g(u_1,\ldots,u_m,x_1,\ldots,x_n)=0.$$

Теперь вопрос может быть сформулирован так: как тот факт, что g следует из $h_1, \ldots, h_n$, может быть доказан *алгебраически*? Основная идея состоит в том, что g должен обращаться в нуль там, где равны нулю полиномы $h_1, \ldots, h_n$. Обратим внимание, что уравнения (9) определяют *многообразие*

$$V = \mathbf{V}(h_1, \ldots, h_n) \subset \mathbb{R}^{m+n}.$$

Это наблюдение приводит к следующему определению.

Определение 4. Утверждение g называется *строго следующим* из условий $h_1, \ldots, h_n$, если $g \in \mathbf{I}(V) \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, где $V = \mathbf{V}(h_1, \ldots, h_n)$.

Это определение кажется разумным, хотя мы увидим ниже, что оно слишком «жесткое». В большинстве геометрических теорем встречаются «вырожденные» случаи, которые определением 4 не учитываются. Но пока мы будем использовать введенное выше понятие «строгого следования».

Одним из недостатков определения 4 является то, что у нас нет эффективного метода для нахождения $I(V)$, поскольку мы работаем над $\mathbb{R}$. Однако мы располагаем следующими критериями:

Предложение 5. *Если* $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$, *то* g *строго следует из* $h_1, \ldots, h_n$.

Доказательство. Условие $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$ означает, что $g^s \in \langle h_1, \ldots, h_n \rangle$ для некоторого s. Тогда $g^s = \sum_{i=1}^{n} A_i h_i$, где $A_i \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, т. е. g^s, а значит, и g равны нулю в тех точках, где все h_i равны нулю. □

Обратите внимание, что обратное утверждение неверно, если идеал $\sqrt{\langle h_1, \ldots, h_n \rangle}$ строго содержится в идеале $\mathbf{I}(V)$, что вполне возможно над $\mathbb{R}$. Тем не менее предложение 5 полезно, потому что условие $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$ может быть проверено с помощью алгоритма принадлежности радикалу из § 2 гл. 4. Пусть $\bar{I} = \langle h_1, \ldots, h_n, 1 - gy \rangle \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n, y]$. Тогда по предложению 8 из § 2 гл. 4

$$g \in \sqrt{\langle h_1, \ldots, h_n \rangle} \iff \{1\} \text{ является редуцированным базисом Грёбнера для } \bar{I}.$$

Если это условие выполнено, то g строго следует из $h_1, \ldots, h_n$.

Если мы работаем над $\mathbb{C}$, то смысл условия $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$ более прозрачен. Здесь условия $h_1, \ldots, h_n$ определяют многообразие $V_{\mathbb{C}} \subset \mathbb{C}^{m+n}$. В упр. 9 с использованием сильной теоремы о нулях

будет доказано, что

$$g \in \sqrt{\langle h_1, \ldots, h_n \rangle} \subset \mathbb{R}[u_1, \ldots, u_m, x_1 \ldots, x_n] \iff g \in \mathbf{I}(V_{\mathbb{C}}) \subset \mathbb{C}[u_1, \ldots, u_m, x_1, \ldots, x_n].$$

Таким образом, условие $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$ означает, что g «строго следует над $\mathbb{C}$» из $h_1, \ldots, h_n$.

Рассмотрим пример, который в числе прочего объяснит, почему определение 4 слишком жесткое.

Пример 1 (продолжение). Чтобы увидеть, какие трудности могут возникать, вернемся к теореме о диагоналях параллелограмма из примера 1. Условиями здесь являются полиномы из (1) и (2):

$$\begin{aligned} h_1 &= x_2 - u_3, \\ h_2 &= (x_1 - u_1)u_3 - u_2 x_2, \\ h_3 &= x_4 x_1 - x_3 u_3, \\ h_4 &= x_4(u_2 - u_1) - (x_3 - u_1)u_3. \end{aligned}$$

Рассмотрим в качестве заключения *первый* полином из (3):

$$g = x_1^2 - 2x_1 x_3 - 2x_4 x_2 + x_2^2.$$

Для того чтобы применить предложение 5, найдем базис Грёбнера идеала

$$\bar{I} = \langle h_1, h_2, h_3, h_4, 1 - yg \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y].$$

Удивительно, но мы *не* обнаруживаем, что $\{1\}$ является базисом. (В упр. 10 мы проверим это с использованием системы компьютерной алгебры.) Так как рассматриваемое утверждение является верной геометрической теоремой, то необходимо понять, почему предложенный нами метод не сработал.

Найдем базис Грёбнера идеала

$$I = \langle h_1, h_2, h_3, h_4 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4],$$

используя lex-упорядочение с $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$. Имеем

$$\begin{aligned} f_1 &= x_1 x_4 + x_4 u_1 - x_4 u_2 - u_1 u_3, \\ f_2 &= x_1 u_3 - u_1 u_3 - u_2 u_3, \\ f_3 &= x_2 - u_3, \\ f_4 &= x_3 u_3 + x_4 u_1 - x_4 u_2 - x_4 u_3, \\ f_5 &= x_4 u_1^2 - x_4 u_1 u_2 - \frac{1}{2} u_1^2 u_3 + \frac{1}{2} u_1 u_2 u_3, \\ f_6 &= x_4 u_1 u_3 - \frac{1}{2} u_1 u_3^2. \end{aligned}$$

Мы видим, что многообразие $V = \mathbf{V}(h_1, h_2, h_3, h_4) = \mathbf{V}(f_1, \ldots, f_6) \subset \mathbb{R}^7$ *приводимо*. В самом деле, $f_2 = (x_1 - u_1 - u_2)u_3$, а следовательно,

$$V = \mathbf{V}(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6) \cup \mathbf{V}(f_1, u_3, f_3, f_4, f_5, f_6).$$

Так как f_5 и f_6 также приводимы, то процесс разложения многообразия на компоненты может быть продолжен. Однако ситуация резко упрощается, если на каждом шаге мы будем вычислять базис Грёбнера заново. В упражнениях мы проверим, что этот подход дает следующее разложение многообразия V в объединение неприводимых:

$$V = V' \cup U_1 \cup U_2 \cup U_3,$$

где

$$V' = \mathbf{V}(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}),$$
$$U_1 = \mathbf{V}(x_2, x_4, u_3),$$
$$U_2 = \mathbf{V}(x_1, x_2, u_1 - u_2, u_3),$$
$$U_3 = \mathbf{V}(x_1 - u_2, x_2 - u_3, x_3 u_3 - x_4 u_2, u_1).$$

Мы также докажем, что ни одно из этих многообразий не содержится в другом и что они являются неприводимыми компонентами многообразия V.

Ситуация проясняется, если мы постараемся понять геометрический смысл компонент $U_1, U_2, U_3 \subset V$ в терминах параллелограмма $ABDC$. На U_1 и U_2 координата u_3 равна 0. Это неприятно, так как переменная u_3 произвольна. Более того, если $u_3 = 0$, то вершина C лежит на $\overline{AB}$, а следовательно, здесь вообще нет параллелограмма. Это *вырожденный* случай нашей конфигурации, который должен быть *исключен* условием, что $ABDC$ — настоящий параллелограмм на плоскости. Аналогично, равенство $u_1 = 0$ на U_3 также приводит к вырожденной конфигурации.

Кроме того, на $U_1 = \mathbf{V}(x_2, x_4, u_3)$ заключение g записывается в виде $g = x_1^2 - 2x_1x_3$, что *не* равно нулю, так как x_1 и x_3 произвольны на U_1. Все это объясняет неудачу нашей первой попытки доказать теорему. Если мы исключим вырожденные случаи U_1, U_2, U_3, то легко показать, что g обращается в нуль на V'. Детали мы оставляем читателю.

Наша цель — создание общего метода, который бы позволял делать вывод о справедливости геометрических утверждений, учитывая и вырожденные случаи. Начнем с того, что представим многообразие $V = \mathbf{V}(h_1, \ldots, h_n) \subset \mathbb{R}^{m+n}$ в виде объединения неприводимых компонент (теорема 2 из § 6 гл. 4):

$$V = V_1 \cup \ldots \cup V_k. \tag{10}$$

Как мы видели выше (в продолжении примера 1), не исключено, что существуют полиномы, зависящие *только* от u_i, которые обращаются в нуль на некоторых компонентах. Так как переменные u_i могут принимать любые значения и независимы, то эти компоненты мы *исключим* из рассмотрения. Дадим определение.

Определение 6. Рассмотрим неприводимое многообразие W в аффинном пространстве $\mathbb{R}^{m+n}$ с координатами $u_1, \ldots, u_m, x_1, \ldots, x_n$. Функции $u_1, \ldots, u_m$ называются *алгебраически независимыми на* W, если не существует полинома от переменных u_i, который обращался бы тождественно в нуль на W.

Согласно определению 6, $u_1, \ldots, u_m$ алгебраически независимы на W, если $\mathbf{I}(W) \cap \mathbb{R}[u_1, \ldots, u_m] = \{0\}$.

Таким образом, в разложении (10) мы можем перегруппировать компоненты многообразия V следующим образом:

$$V = W_1 \cup \ldots \cup W_p \cup U_1 \cup \ldots \cup U_q, \tag{11}$$

где u_i алгебраически *независимы* на компонентах W_j и алгебраически *зависимы* на компонентах U_j. Таким образом, U_j представляют «вырожденные» случаи условий теоремы. Чтобы быть уверенными, что u_i в нашей геометрической конструкции произвольны, мы должны рассматривать *только* подмногообразие

$$V' = W_1 \cup \ldots \cup W_p \subset V.$$

Мы не интересуемся поведением заключения $g \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ в вырожденных случаях. Это приводит нас к следующему определению.

Определение 7. Заключение g *обобщенно следует* из условий $h_1, \ldots, h_n$, если $g \in \mathbf{I}(V') \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, где, как выше, $V' \subset \mathbb{R}^{m+n}$ является объединением тех компонент многообразия $V = \mathbf{V}(h_1, \ldots, h_n)$, на которых u_i алгебраически независимы.

Обычное высказывание, что геометрическая теорема «верна», означает в точности, что заключения этой теоремы обобщенно следует из условий. Теперь задача может быть сформулирована следующим образом: как выяснить, когда $g \in \mathbf{I}(V')$? То есть можем ли мы указать критерий, который выяснял бы, обращается ли g в нуль на тех компонентах многообразия V, где u_i *алгебраически независимы*, игнорируя в то же время «вырожденные» компоненты?

Задача разложения многообразия в объединение неприводимых достаточно сложна; поэтому нам бы хотелось найти метод, позволяющий доказать (или опровергнуть) обобщенное следование и *не требующий* знания разложения (11). Кроме того, даже если V' нам известно, то как найти $\mathbf{I}(V')$?

К счастью, найти такой метод возможно.

Предложение 8. *В ситуации, описанной выше, g обобщенно следует из $h_1, \dots, h_n$, если существует ненулевой полином $c(u_1, \dots, u_m) \in \mathbb{R}[u_1, \dots, u_m]$, такой, что*

$$c \cdot g \in \sqrt{H},$$

где $H = \langle h_1, \dots, h_n \rangle \subset \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$.

Доказательство. Пусть V_j — неприводимая компонента многообразия V'. Так как $c \cdot g \in \sqrt{H}$, то $c \cdot g$ обращается в нуль на V и, следовательно, на V_j. Таким образом, $c \cdot g \in \mathbf{I}(V_j)$. Но V_j неприводимо; следовательно, $\mathbf{I}(V_j)$ — простой идеал (предложение 3 из § 5 гл. 4). Значит, либо c, либо g принадлежит $\mathbf{I}(V_j)$. Но $c \notin \mathbf{I}(V_j)$, так как полином, зависящий только от u_i, не может обращаться в нуль на компоненте V_j. Следовательно, $g \in \mathbf{I}(V_j)$. А так как это верно для каждой компоненты многообразия V', то $g \in \mathbf{I}(V')$. □

Для того чтобы предложение 8 можно было применять в реальных задачах, надо найти метод, позволяющий установить существование ненулевого полинома c, такого, что $c \cdot g \in \sqrt{H}$. Это несложно. По определению радикала $c \cdot g \in \sqrt{H}$ в том и только том случае, когда

$$(c \cdot g)^s = \sum_{j=1}^{n} A_j h_j$$

для некоторых $A_j \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$. Поделим обе части уравнения на c^s и получим равенство

$$g^s = \sum_{j=1}^{n} \frac{A_j}{c^s} h_j,$$

из которого следует, что g принадлежит радикалу идеала $\widetilde{H}$, порожденного полиномами $h_1, \dots, h_n$ в кольце $\mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$. Обратно, если $g \in \sqrt{\widetilde{H}}$, то

$$g^s = \sum_{j=1}^{n} B_j h_j,$$

где $B_j \in \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$. Если c — наименьшее общее кратное всех знаменателей во всех членах полиномов B_j, то, умножая обе части равенства на c^s, получим

$$(c \cdot g)^s = \sum_{j=1}^{n} B'_j h_j,$$

где $B'_j \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$, а c зависит только от u_i. Таким образом, $c \cdot g \in \sqrt{H}$. Эти вычисления и алгоритм принадлежности радикалу (§ 2 гл. 4) дают нам следующее предложение.

Следствие 9. *В условиях предложения 8 следующие утверждения эквивалентны:*

(i) *существует ненулевой полином $c \in \mathbb{R}[u_1, \dots, u_m]$, такой, что $c \cdot g \in \sqrt{H}$;*

(ii) *$g \in \sqrt{\widetilde{H}}$, где $\widetilde{H}$ — это идеал, порожденный в $\mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$ полиномами h_j;*

(iii) *$\{1\}$ является редуцированным базисом Грёбнера идеала*

$$\langle h_1, \dots, h_n, 1 - yg \rangle \subset \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n, y].$$

Объединяя п. (iii) с предложением 8, мы получаем алгоритмический метод доказательства того, что заключение теоремы обобщенно следует из ее условий. Мы назовем этот подход методом базисов Грёбнера в доказательстве геометрических теорем.

Рассмотрим снова теорему о параллелограмме из примера 1. Вычисляя базис Грёбнера идеала $\langle h_1, h_2, h_3, h_4, 1 - yg \rangle \subset \mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4, y]$, убеждаемся, что $\{1\}$ *действительно* образует редуцированный базис (как и ожидалось). Переход к $\mathbb{R}(u_1, u_2, u_3)$, обеспечивающий обратимость переменных u_1, u_2, u_3, *исключает* вырожденные случаи, рассмотренные выше, и, следовательно, заключение обобщенно следует из условий. Более того, в упр. 12 будет доказано, что на самом деле g (а не его степень) принадлежит идеалу $\langle h_1, h_2, h_3, h_4 \rangle \subset \mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$.

Обратите внимание, что метод базисов Грёбнера не указывает, какие случаи являются вырожденными. Информация о них содержится в полиноме $c \in \mathbb{R}[u_1, \dots, u_m]$, потому что условие $c \cdot g \in \sqrt{H}$ означает, что g следует из $h_1, \dots, h_n$ там, где c не равен нулю (так как $c \cdot g$ является тождественным нулем на V). В упр. 14 будет описан алгоритм вычисления c.

Над $\mathbb{C}$ следствие 9 можно представить в терминах многообразия $V_{\mathbb{C}} = \mathbf{V}(h_1, \dots, h_n) \subset \mathbb{C}^{m+n}$. Разложим $V_{\mathbb{C}} = \mathbf{V}(h_1, \dots, h_n) \subset \mathbb{C}^{m+n}$ на компоненты, как в (11). Пусть $V'_{\mathbb{C}} \subset V_{\mathbb{C}}$ — объединение тех компонент, на которых u_i алгебраически независимы. В упражнении 15 с использованием теоремы о нулях будет доказано, что

$$\exists c \neq 0 \text{ в } \mathbb{R}[u_1, \dots, u_m], c \cdot g \in \sqrt{H} \subset \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$$
$$\iff g \in \mathbf{I}(V'_{\mathbb{C}}) \subset \mathbb{C}[u_1, \dots, u_m, x_1, \dots, x_n].$$

Другими словами, условия следствия 9 означают, что g «обобщенно следует над $\mathbb{C}$» из условий $h_1, \dots, h_n$.

Комплексная интерпретация указывает на, пожалуй, главный недостаток метода базисов Грёбнера: этот метод может доказывать только те теоремы, где утверждение обобщенно следует из условий над $\mathbb{C}$, в то время как мы интересуемся только тем, что происходит над $\mathbb{R}$. В частности, есть теоремы, справедливые над $\mathbb{R}$, но не над

$\mathbb{C}$ (см., например, работу STURMFELS (1989)). Подобные теоремы нельзя доказать этим методом.

Применение следствия 9 не всегда требует вычисления радикала идеала $\widetilde{H}$. Во многих случаях достаточно проверить просто принадлежность идеалу $\widetilde{H}$. Поэтому большинство программ автоматического доказательства теорем сначала используют алгоритм принадлежности g *идеалу* $\widetilde{H}$, и только если не получено утвердительного ответа, начинают проверять принадлежность радикалу.

Проиллюстрируем эти соображения на примере теоремы Аполлония из примера 3. Условия теоремы были представлены восемью полиномами (5)–(7). Вычисление базиса Грёбнера идеала $\widetilde{H}$ для lex-упорядочения дает

$$\begin{aligned}
f_1 &= x_1 - u_1/2,\\
f_2 &= x_2 - u_2/2,\\
f_3 &= x_3 - u_1/2,\\
f_4 &= x_4 - u_2/2,\\
f_5 &= x_5 - \frac{u_1u_2^2}{u_1^2+u_2^2},\\
f_6 &= x_6 - \frac{u_1^2u_2}{u_1^2+u_2^2},\\
f_7 &= x_7 - u_1/4,\\
f_8 &= x_8 - u_2/4.
\end{aligned} \tag{12}$$

Мы оставляем читателю в качестве упражнения показать, что остаток от деления заключения (8) на базис Грёбнера равен нулю. Таким образом, $g \in \widetilde{H}$, и, значит, g обобщенно следует из полиномов $h_1, \ldots, h_8$. Обратите внимание, что если $u_1 = u_2 = 0$, то мы не можем определить переменные x_5 и x_6. Уравнения $u_1 = 0$ и $u_2 = 0$ задают вырожденные прямоугольные «треугольники», у которых две вершины совпадают, и мы, конечно, не должны эти случаи рассматривать. Интересно отметить, что если $u_1 \neq 0$ или $u_2 \neq 0$, то заключение теоремы имеет место. Пусть, например, $u_1 \neq 0$, но $u_2 = 0$. Тогда вершины C и A совпадают. При этом точки M_1 и M_3 совпадают, M_2 совпадает с A и H также совпадает с A. В результате получаем, что *существует* окружность (на самом деле таких окружностей бесконечно много), содержащая M_1, M_2, M_3 и H. В упр. 16 будет рассмотрен случай $u_1 = u_2 = 0$.

Отметим, наконец, еще один тонкий момент в использовании этого метода. А именно, в ряде случаев формулировка теоремы подразумевает наличие дополнительных, не сформулированных явно условий. Эти дополнительные условия не будут записаны в полиномиальной форме при прямом переводе условий теоремы на алгебраический язык. Часто это приводит к ситуации, когда многообразие V' оказывается *приводимым*, т. е. $p > 1$ в (11). Тогда полином g может быть равным нулю *только* на некоторых компонентах многообразия V', и никакой метод, использующий следствие 9, не приведет к успеху. В упр. 17 будет рассмотрен такой пример. В этом случае мы должны переформулировать условия теоремы, чтобы исключить лишние, ненужные компоненты многообразия V'.

Упражнения к § 4

1. В этом упражнении мы предлагаем читателю дать геометрическое доказательство теорем из примеров 1 и 3.
   (a) Дайте стандартное геометрическое доказательство теоремы из примера 1. Указание: докажите, что $\triangle ANC \cong \triangle BND$.
   (b) Дайте стандартное геометрическое доказательство теоремы Аполлония об окружности из примера 3. Указание: сначала докажите, что $\overline{AB} \| \overline{M_2M_3}$.

2. В этом упражнении мы рассмотрим другой перевод теоремы о параллелограмме из примера 1 на алгебраический язык с использованием других координат в качестве произвольных переменных. Пусть вершина A параллелограмма $ABDC$ помещена в начало координат.
   (a) Объясните, почему обе координаты вершины D можно рассматривать как произвольные переменные, $D = (u_1, u_2)$.
   (b) Имея в виду п. (a), объясните, почему координаты вершины B можно задать как (u_3, x_1). Другими словами, x-координата точки B произвольна, а y-координата определена выбором значений u_1, u_2, u_3.
   (c) Завершите перевод теоремы на алгебраический язык, используя этот выбор переменных.

3. Пусть A, B, C, D, E, F, G, H — точки на плоскости.
   (a) Докажите, что утверждение о том, что отрезок $\overline{AB}$ касателен к окружности, проходящей через точки A, C, D, может быть сформулирован в виде полиномиальных уравнений. Указание: сначала постройте центр окружности. Что можно сказать о касательной и радиусе окружности в той же точке?
   (b) Докажите, что утверждение $AB \cdot CD = EF \cdot GH$ может быть выражено с помощью одного или нескольких полиномиальных уравнений.
   (c) Докажите, что утверждение $AB/CD = EF/GH$ может быть выражено с помощью одного или нескольких полиномиальных уравнений.
   (d) *Двойным отношением* упорядоченной четверки различных *коллинеарных* точек (A, B, C, D) называется число

$$\frac{AC \cdot BD}{AD \cdot BC}.$$

Докажите, что утверждение «двойное отношение четверки (A, B, C, D) равно $\rho \in \mathbb{R}$» может быть выражено с помощью одного или нескольких полиномиальных уравнений.

4. В этом упражнении будет завершено доказательство предложения 2.
   (a) Докажите п. (ii).
   (b) Пусть α, β — острые углы. Докажите, что $\alpha = \beta$ в том и только том случае, когда $\operatorname{tg}(\alpha) = \operatorname{tg}(\beta)$. Используя этот факт и п. (c) упр. 3, докажите п. (vii) предложения 2. Указание: чтобы вычислить тангенс угла, нужно построить соответствующий прямоугольный треугольник и найти отношение катетов.
   (c) Докажите п. (viii).

5. Рассмотрим треугольник $\triangle ABC$ на плоскости. Напомним, что *высотой*, проведенной из вершины A, называется отрезок перпендикуляра, опущенного из A на сторону $\overline{BC}$. (Основание перпендикуляра может принадлежать продолжению отрезка $\overline{BC}$.) Классическая геометрическая теорема утверждает, что высоты пересекаются в одной точке H, которая называется *ортоцентром* треугольника. Запишите условия теоремы и ее заключение в полиномиальном виде.

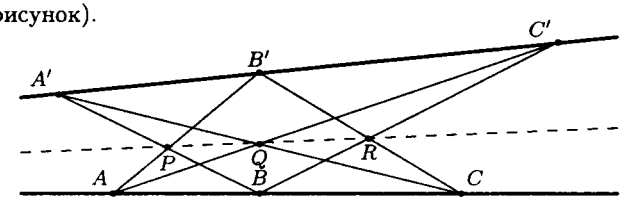
6. Рассмотрим треугольник $\triangle ABC$ на плоскости. Пусть M_1 — середина стороны $\overline{BC}$, M_2 — середина стороны $\overline{AC}$, а M_3 — середина стороны $\overline{AB}$. Классическая теорема утверждает, что отрезки $\overline{AM_1}, \overline{BM_2}$ и $\overline{CM_3}$ пересекаются в одной точке M, которая называется *центроидом* треугольника. Запишите условия теоремы и ее заключение в полиномиальном виде.

7. Рассмотрим треугольник $\triangle ABC$ на плоскости. Знаменитая теорема Эйлера утверждает, что *центр описанной окружности, ортоцентр* и *центроид* коллинеарны. Запишите условия теоремы и ее заключение в полиномиальном виде. (Прямая, на которой лежат эти три «центра» треугольника, называется его *прямой Эйлера*.)

8. Красивая теорема, принадлежащая Паппу, рассматривает две тройки коллинеарных точек A, B, C и A', B', C'. Пусть

$$P = \overline{AB'} \cap \overline{A'B},$$
$$Q = \overline{AC'} \cap \overline{A'C},$$
$$R = \overline{BC'} \cap \overline{B'C}$$

(см. рисунок).



Тогда P, Q, R коллинеарны. Запишите условия теоремы и ее заключение в полиномиальном виде.

9. Пусть $h_1, \ldots, h_n \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ и $V_{\mathbb{C}} = \mathbf{V}(h_1, \ldots, h_n) \subset \mathbb{C}^{m+n}$. Рассмотрим полином $g \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$. Мы хотим доказать следующее утверждение:

$$g \in \sqrt{\langle h_1, \ldots, h_n \rangle} \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$$
$$\iff g \in \mathbf{I}(V_{\mathbb{C}}) \subset \mathbb{C}[u_1, \ldots, u_m, x_1, \ldots, x_n].$$

   (a) Докажите справедливость импликации $\Rightarrow$.
   (b) Используя сильную теорему о нулях, докажите, что если $g \in \mathbf{I}(V_{\mathbb{C}})$, то найдутся полиномы $A_j \in \mathbb{C}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, такие, что $g^s = \sum_{j=1}^{n} A_j h_j$ для некоторого $s \geq 1$.
   (c) Объясните, почему каждый A_j может быть представлен в виде $A_j = A_j' + iA_j''$, где A_j', A_j'' — полиномы с вещественными коэффициентами. Используя это, докажите, что $g^s = \sum_{j=1}^{n} A_j' h_j$, а это завершает доказательство импликации $\Leftarrow$. Указание: $g, h_1, \ldots, h_n$ — полиномы с вещественными коэффициентами.

10. Докажите, что в условиях примера 1 $\{1\}$ не является единственным редуцированным базисом Грёбнера идеала $\widetilde{I} = \langle h_1, h_2, h_3, 1 - yg \rangle$.

11. В этом упражнении мы рассмотрим разложение на неприводимые компоненты многообразия, определенного условиями теоремы из примера 1.
   (a) Докажите, что (см. продолжение примера 1)
   $$V = \mathbf{V}(f_1, x_1 - u_1 - u_2, f_3, \ldots, f_6) \cup \mathbf{V}(f_1, u_3, f_3, \ldots, f_6) = V_1 \cup V_2.$$
   (b) Найдите базисы Грёбнера идеалов, порожденных определяющими уравнениями многообразий V_1 и V_2. Некоторые из базисных элементов будут приводимыми, что даст возможность разложить V_1 и V_2.
   (c) Продолжая этот процесс, покажите, что V является объединением многообразий V', U_1, U_2, U_3, определенных в тексте параграфа.
   (d) Докажите, что V', U_1, U_2, U_3 неприводимы и что ни одно из них не содержится в объединении остальных. Это доказывает, что V', U_1, U_2, U_3 являются неприводимыми компонентами многообразия V.
   (e) На какой неприводимой компоненте многообразия V заключение теоремы справедливо?
   (f) Пусть в качестве условий рассматриваются четыре полинома из (4) и (2). Является ли приводимым многообразие $W = \mathbf{V}(h_1', h_2', h_3, h_4)$? Сколько компонент оно имеет?

12. Докажите, что в примере 1 само заключение g (а не его степень) принадлежит идеалу, порожденному h_1, h_2, h_3, h_4 в кольце $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$.

13. Используя п. (iii) следствия 9, докажите, что g обобщенно следует из h_j в каждой из следующих теорем. Также найдите в каждом случае наименьшую степень полинома g, принадлежащую идеалу $\tilde{H}$.
   (a) Теорема об ортоцентре (упр. 5).
   (b) Теорема о центроиде (упр. 6).
   (c) Теорема о прямой Эйлера (упр. 7).
   (d) Теорема Паппа (упр. 8).

14. В этом упражнении мы рассмотрим алгоритм вычисления ненулевого $c \in \mathbb{R}[u_1, \ldots, u_m]$, такого, что $c \cdot g \in \sqrt{H}$ (в предположении, что такое c существует). Мы будем работать с идеалом
$$\tilde{H} = \langle h_1, \ldots, h_n, 1 - yg \rangle \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n, y].$$
   (a) Докажите, что условия следствия 9 эквивалентны условию $\tilde{H} \cap \mathbb{R}[u_1, \ldots, u_m] \neq \{0\}$. Указание: используйте п. (iii) следствия 9.
   (b) Пусть $c \in \tilde{H} \cap \mathbb{R}[u_1, \ldots, u_m]$. Докажите, что $c \cdot g \in \sqrt{H}$. Указание: используйте рассуждения, связанные с уравнениями (2)–(4) в доказательстве теоремы Гильберта о нулях (§ 1 гл. 4).
   (c) Опишите алгоритм вычисления идеала $\tilde{H} \cap \mathbb{R}[u_1, \ldots, u_m]$. Какое мономиальное упорядочение обеспечивает максимальную эффективность?

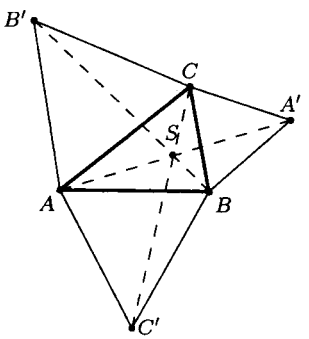
   Пункты (a)–(c) описывают алгоритм, определяющий существование ненулевого c, такого, что $c \cdot g \in \sqrt{H}$, и *одновременно* находящий требуемое c. В пп. (d) и (e) ниже будут рассмотрены некоторые интересные свойства идеала $\tilde{H} \cap \mathbb{R}[u_1, \ldots, u_m]$.
   (d) Предположим, что заключение g не имеет места для некоторых $u_1, \ldots, u_m$. Докажите, что тогда $(u_1, \ldots, u_m) \in W = \mathbf{V}(\tilde{H} \cap \mathbb{R}[u_1, \ldots, u_m]) \subset \mathbb{R}^m$. Таким образом, в W содержатся все вырожденные случаи, при которых g не имеет места.
   (e) Докажите, что условие $c \cdot g \in \sqrt{H}$ эквивалентно условию $c \in \sqrt{\tilde{H} \cap \mathbb{R}[u_1, \ldots, u_m]}$. Указание: в одну сторону это утверждение следует из п. (a); если же $c \cdot g \in \sqrt{H}$, то $\tilde{H}$ содержит $(c \cdot g)^s$ и $1 - gy$; далее, используя рассуждения из доказательства предложения 8 из § 2 гл. 4, докажите, что $c^s \in \tilde{H}$.

15. Пусть $h_1, \ldots, h_n \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ (как в упр. 9). Тогда $V_{\mathbf{C}} = \mathbf{V}(h_1, \ldots, h_n) \subset \mathbb{C}^{m+n}$, и пусть $V'_{\mathbf{C}}$ — объединение тех неприводимых компонент многообразия $V_{\mathbf{C}}$, на которых переменные $u_1, \ldots, u_m$ алгебраически независимы. Пусть $g \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$. Мы хотим доказать, что
$$\begin{aligned} &\exists c \neq 0 \text{ в } \mathbb{R}[u_1, \ldots, u_m], \text{ такое, что } c \cdot g \in \sqrt{\langle h_1, \ldots, h_n \rangle} \subset \\ &\qquad \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n] \\ &\iff g \in \mathbf{I}(V'_{\mathbf{C}}) \subset \mathbb{C}[u_1, \ldots, u_m, x_1, \ldots, x_n]. \end{aligned}$$
   (a) Докажите импликацию $\Rightarrow$. Указание: см. доказательство предложения 8.

   (b) Докажите, что если $g \in \mathbf{I}(V'_{\mathbf{C}})$, то существует ненулевой полином $c \in \mathbb{C}[u_1, \ldots, u_m]$, такой, что $c \cdot g \in \mathbf{I}(V_{\mathbf{C}})$. Указание: пусть $V_{\mathbf{C}} = V'_{\mathbf{C}} \cup U'_1 \cup \ldots \cup U'_q$, где $u_1, \ldots, u_m$ алгебраически зависимы на каждом U'_j. Это означает, что существует ненулевой полином $c_j \in \mathbb{C}[u_1, \ldots, u_m]$, равный нулю на U'_j.
   (c) Докажите, что можно выбрать полином c из п. (b) так, чтобы он имел вещественные коэффициенты. Указание: пусть $\bar{c}$ — полином, коэффициенты которого являются комплексно-сопряженными к коэффициентам полинома c. Докажите, что полином $c\bar{c}$ вещественен.
   (d) Пусть мы нашли полином $c \in \mathbb{R}[u_1, \ldots, u_m]$, такой, что $c \cdot g \in \mathbf{I}(V_{\mathbf{C}})$. Используйте упр. 9 для доказательства импликации $\Leftarrow$.

16. В этом упражнении мы рассмотрим теорему Аполлония об окружности из примера 3.
   (a) Докажите, что остаток от деления заключения (8) на базис Грёбнера (12) равен нулю.
   (b) Рассмотрите случай $u_1 = u_2 = 0$. Справедливо ли утверждение теоремы в этом вырожденном случае?
   (c) Обратите внимание, что на рисунке, иллюстрирующем теорему Аполлония, интересующая нас окружность проходит также через вершину A. Следует ли это заключение из условий теоремы?

17. В этом упражнении мы рассмотрим случай, когда прямой перевод условий «верной» теоремы на алгебраический язык приводит к появлению лишних компонент, на которых теорема просто неверна. Пусть $\triangle ABC$ — треугольник на плоскости. Построим три новые точки A', B', C' так, чтобы треугольники $\triangle A'BC, \triangle AB'C, \triangle ABC'$ были бы *равносторонними*. См. рисунок ниже.



Утверждение теоремы состоит в том, что три отрезка $\overline{AA'}, \overline{BB'}, \overline{CC'}$ пересекаются в одной точке S, которая называется *точкой Штейнера* треугольника. (Если углы исходного треугольника не превышают $2\pi/3$, то можно доказать, что три отрезка $\overline{AS}, \overline{BS}, \overline{CS}$ образуют

граф минимальной длины в множестве графов, соединяющих вершины A, B, C.)

(a) Дайте геометрическое доказательство этой теоремы для случая, изображенного на предыдущем рисунке.

(b) Найдите прямой перевод условий и заключения этой теоремы на полиномиальный язык.

(c) Примените следствие 9, чтобы выяснить, будет ли заключение обобщенно следовать из условий. Вы должны получить отрицательный ответ. Замечание: вы должны проявить *значительную* ловкость при проведении этого вычисления, иначе не всякая система компьютерной алгебры справится с ним: приходится работать с весьма сложной полиномиальной системой.

(d) (Основной этап) Покажите, что есть другие способы построить геометрическую конфигурацию, удовлетворяющую условиям в том виде, *как они сформулированы выше*, но совершенно не похожую на конфигурацию на рисунке. Указание: однозначно ли определены положения точек A', B', C' условиями теоремы? Справедлива ли теорема для других конфигураций? Используйте эти соображения для объяснения отрицательного результата п. (c). (Эти разные конфигурации соответствуют разным компонентам многообразия, определенного условиями.)

(e) Как нужно сформулировать теорему, чтобы исключить лишние компоненты?

§ 5. Метод Ву

В этом параграфе мы рассмотрим другой широко используемый метод алгоритмического доказательства теорем евклидовой геометрии, основанный на использовании систем полиномиальных уравнений. Он был разработан китайским математиком Ву Вень-Цунем *до* появления метода базисов Грёбнера из § 4. Этот метод эффективнее метода базисов Грёбнера и чаще применяется.

Как элементарная версия метода Ву (которую мы и будем рассматривать), так и и его усовершенствованные версии, используют интересный вариант алгоритма деления полиномов от нескольких переменных (§ 3 гл. 2). Идея этого варианта (он называется алгоритмом *псевдоделения*) состоит в том, что надо как можно точнее следовать алгоритму деления полиномов от одной переменной. Чтобы описать его первый шаг, рассмотрим два полинома из кольца $k[x_1, \dots, x_n, y]$, которые записаны в виде

$$\begin{aligned} f &= c_p y^p + \dots + c_1 y + c_0, \\ g &= d_m y^m + \dots + d_1 y + d_0, \end{aligned} \tag{1}$$

где коэффициенты c_i, d_j являются полиномами от $x_1, \dots, x_n$. Пусть $m \le p$. Действуя, как в случае полиномов от одной переменной (от

y), мы ликвидируем старший член $c_p y^p$ полинома f, вычитая подходящее кратное полинома g. Однако этого нельзя сделать, если d_m не делит c_p в $k[x_1, \dots, x_n]$. При псевдоделении мы сначала *умножаем* f на d_m, чтобы быть уверенными, что его старший коэффициент делится на d_m, и первый шаг мы можем проделать, как и в случае одной переменной. Дадим описание алгоритма.

Предложение 1. *Пусть* $f, g \in k[x_1, \dots, x_n, y]$ *такие же, как в* (1), $m \le p$ *и* $g \neq 0$.

(i) *Справедливо равенство*

$$d_m^s f = qg + r,$$

где $q, r \in k[x_1, \dots, x_n, y]$, $s > 0$ *и или полином* r *равен* 0, *или его степень по* y *меньше* m.

(ii) $r \in \langle f, g \rangle \subset k[x_1, \dots, x_n, y]$.

Доказательство. (i) Полиномы q, r, удовлетворяющие утверждению (i), могут быть построены с помощью следующего алгоритма, называемого алгоритмом *псевдоделения по переменной* y. Через $\deg(h, y)$ будет обозначаться степень полинома h по y, а через $\mathrm{LC}(h, y)$ будет обозначаться его старший коэффициент по y, т. е. коэффициент при $y^{\deg(h,y)}$.

Вход: f, g
Выход: q, r
$r := f; q := 0$
WHILE $r \neq 0$ AND $\deg(r, y) \ge m$ DO
$\quad r := d_m r - \mathrm{LC}(r, y) g y^{\deg(r,y)-m}$
$\quad q := d_m q + \mathrm{LC}(r, y) y^{\deg(r,y)-m}$

Обратите внимание, что при работе алгоритма цикл WHILE выполнится, самое большее, $p - m + 1$ раз. Таким образом, степень s в $d_m^s f = qg + r$ можно выбрать так, чтобы $s \le p - m + 1$. Остальные детали доказательства, включая вопрос о единственности полиномов q и r, мы оставляем читателю (упр. 1).

(ii) Из равенства $d_m^s f = qg + r$ следует, что $r = d_m^s f - qg \in \langle f, g \rangle$. □

Полиномы q, r называются *псевдочастным* и *псевдоостатком* при псевдоделении полинома f на g по переменной y. Мы будем использовать обозначение $\mathrm{Rem}(f, g, y)$ для псевдоостатка, вычисленного с использованием алгоритма из предложения 1. Например, псевдоделение полинома $f = x^2 y^3 - y$ на $g = x^3 y - 2$ дает нам равенство

$$(x^3)^3 f = (x^8 y^2 + 2x^5 y + 4x^2 - x^6) g + 8x^2 - 2x^6.$$

В частности, $\mathrm{Rem}(f, g, y) = 8x^2 - 2x^6$.

Отметим, что есть другой способ объяснить, как работает алгоритм: он использует ту же идею *перехода к частным*, которую мы использовали в § 4. А именно,

- это обычное деление полиномов от одной переменной y с коэффициентами в поле рациональных функций $K = k(x_1, \dots, x_n)$, но с
- последующей ликвидацией знаменателей. В упр. 2 это будет доказано с помощью того факта, что при делении в кольце $K[y]$ (K — любое поле) нам нужно находить обратный элемент только для *старшего коэффициента* d_m делителя g. Таким образом, все знаменатели, полученные в процессе деления, ликвидируются при умножении на некоторую степень d_m^s. Именно так мы и получаем равенство $d_m^s f = qg + r$.

В этой второй (прямой) форме псевдоделение легко может быть реализовано в системах компьютерной алгебры (и на самом деле этот алгоритм в ряде систем реализован как стандартная процедура).

Напомним, что в § 4 мы рассматривали вопрос о переводе условий и заключений геометрических теорем на язык полиномиальных уравнений. Полиномы $h_1, \dots, h_n \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$ представляли условия некоторой теоремы, а полином g от тех же переменных — ее заключение. В уравнении (11) из § 4 неприводимые компоненты многообразия $V = \mathbf{V}(h_1, \dots, h_n) \in \mathbb{R}^{m+n}$ мы объединяли в два класса,

$$V = V' \cup U,$$

где V' — это объединение тех компонент многообразия V, на которых переменные u_i алгебраически независимы. Доказать теорему — это доказать, что g обращается в нуль на V'.

Элементарная версия метода Ву, которую мы и будем рассматривать, работает только в том случае, когда V' *неприводимо*. Следует отметить, что усовершенствованный метод позволяет рассматривать и приводимый случай, однако необходимая алгебраическая техника (алгоритм разложения Ритта, использующий *характеристические множества* простых идеалов) слишком сложна, чтобы ее здесь рассматривать. Решая реальную задачу, мы заранее не знаем, приводимо V' или нет. Поэтому надежные «доказыватели теорем», использующие метод Ву, должны уметь использовать эту более сложную технику.

Упрощенная версия алгоритма Ву использует алгоритм псевдоделения *двумя* способами в процессе выяснения, следует ли равенство $g = 0$ из равенств $h_j = 0$.

- Шаг 1 метода Ву использует псевдоделение для приведения системы условий к системе полиномов f_j *треугольного вида* по переменным $x_1, \dots, x_n$. Другими словами, мы хотим найти систему полиномов

$$\begin{aligned} f_1 &= f_1(u_1, \dots, u_m, x_1), \\ f_2 &= f_2(u_1, \dots, u_m, x_1, x_2), \\ &\vdots \\ f_n &= f_n(u_1, \dots, u_m, x_1, \dots, x_n), \end{aligned} \tag{2}$$

такую, что $\mathbf{V}(f_1, \dots, f_n)$ снова содержит неприводимое многообразие V', на котором u_i алгебраически независимы.
- Шаг 2 метода Ву использует *последовательное* псевдоделение заключения g по каждой переменной x_j с целью узнать, принадлежит g идеалу $\mathbf{I}(V')$ или нет. Мы вычисляем

$$\begin{aligned} R_{n-1} &= \mathrm{Rem}(g, f_n, x_n), \\ R_{n-2} &= \mathrm{Rem}(R_{n-1}, f_{n-1}, x_{n-1}), \\ &\vdots \\ R_1 &= \mathrm{Rem}(R_2, f_2, x_2), \\ R_0 &= \mathrm{Rem}(R_1, f_1, x_1). \end{aligned} \tag{3}$$

- Теперь, если $R_0 = 0$, то g следует из условий h_j при одном дополнительном условии, которое будет сформулировано в теореме 4.

Объяснение принципов работы метода Ву требует последовательного объяснения всех трех шагов. Мы начнем с первого, с приведения к треугольному виду.

Шаг 1. Приведение к треугольному виду

На практике это приведение почти всегда может быть реализовано с помощью процедуры, похожей на метод исключения Гаусса для решения линейных систем. Мы не будем формулировать никаких общих теорем об этой процедуре, потому что есть случаи, в которых она не дает требуемого результата (см. замечания 3 и 4 ниже). Общий алгоритм такой редукции описан в книге Chou (1988).

Элементарная версия работает следующим образом. Переменные x_j рассматриваются по очереди, начиная с x_n.

1. Находим все полиномы h_j, содержащие x_n. Обозначим это множество полиномов через S. (Если таких полиномов нет, то это, скорее всего, означает, что наш перевод теоремы на алгебраический язык некорректен, так как x_n оказывается свободной переменной.)
2. Если S содержит только один полином, то мы переобозначим полиномы h_j символами f_i' так, чтобы наша система при-

обрела вид

$$\begin{aligned} f_1' &= f_1'(u_1,\dots,u_m,x_1,\dots,x_{n-1}),\\ &\vdots\\ f_{n-1}' &= f_{n-1}'(u_1,\dots,u_m,x_1,\dots,x_{n-1}),\\ f_n' &= f_n'(u_1,\dots,u_m,x_1,\dots,x_n). \end{aligned} \tag{4}$$

3. Если S содержит несколько полиномов, но один из них имеет степень 1 по x_n, то мы обозначим его через f_n' и заменим все остальные полиномы из S их псевдоостатками от деления на f_n' по x_n. (Может случиться так, что один из этих псевдоостатков окажется равным *нулю*. Но это означает, что f_n' делит $d^s h$, где h — одно из других условий, а $d = \mathrm{LC}(f_n', x_n)$, что маловероятно, так как V' предполагается неприводимым.) Таким образом, мы опять получаем систему вида (4). Из п. (ii) предложения 1 следует, что все полиномы f_j' принадлежат идеалу, порожденному полиномами h_j.
4. Если S содержит несколько полиномов и все они имеют степень по x_n, большую 1, то мы поступаем следующим образом:
   (a) находим $a, b \in S$, такие, что $0 < \deg(b, x_n) \le \deg(a, x_n)$;
   (b) вычисляем псевдоостаток $r = \mathrm{Rem}(a, b, x_n)$;
   (c) заменяем S на $(S - \{a\}) \cup \{r\}$ (полиномы, не входящие в S, не меняются).

   Шаги (a), (b), (c) повторяются до тех пор, пока мы не приведем систему полиномов к виду (4). Так как степень по x_n уменьшается при переходе к псевдоостатку, то в конце концов мы исключим x_n изо всех полиномов, кроме одного. Кроме того (п. (ii) предложения 1), все полученные нами полиномы содержатся в идеале, порожденном h_j. Опять-таки мы можем получить нулевой полином на каком-то шаге наших вычислений, но из этого, как правило (но не всегда!), следует приводимость многообразия V', так что это маловероятно. Теперь аналогичную процедуру мы применяем к полиномам $f_1', \dots, f_{n-1}'$ в (4), исключая x_{n-1} изо всех полиномов, кроме одного. Продолжая этот процесс, мы в конце концов получим систему уравнений треугольного вида (2).

Связь между треугольной системой и исходными полиномами — условиями теоремы, объясняется в следующем предложении.

Предложение 2. *Пусть $f_1 = \dots = f_n = 0$ — треугольная система, полученная из исходной системы $h_1 = \dots = h_n$ с помощью описанного выше алгоритма. Тогда*

$$V' \subset V \subset \mathbf{V}(f_1,\dots,f_n).$$

Доказательство. Как отмечалось выше, все f_j содержатся в идеале, порожденном h_j. Поэтому $\langle f_1,\dots,f_n\rangle \subset \langle h_1,\dots,h_n\rangle$. Следовательно, $V = \mathbf{V}(h_1,\dots,h_n) \subset \mathbf{V}(f_1,\dots,f_n)$. Так как $V' \subset V$, то предложение доказано. □

Пример 3. Проиллюстрируем процедуру приведения к треугольному виду на примере теоремы Аполлония об окружности из § 4 (см. уравнения (5)–(7) из § 4). Имеем

$$\begin{aligned} h_1 &= 2x_1 - u_1,\\ h_2 &= 2x_2 - u_2,\\ h_3 &= 2x_3 - u_1,\\ h_4 &= 2x_4 - u_2,\\ h_5 &= u_2x_5 + u_1x_6 - u_1u_2,\\ h_6 &= u_1x_5 - u_2x_6,\\ h_7 &= x_1^2 - x_2^2 - 2x_1x_7 + 2x_2x_8,\\ h_8 &= x_1^2 - 2x_1x_7 - x_3^2 + 2x_3x_7 - x_4^2 + 2x_4x_8. \end{aligned}$$

Обратите внимание, что эта система очень близка к треугольной по x_j. На самом деле это обычное явление, если мы строим геометрическую конфигурацию, добавляя на каждом шаге одну точку.

На первом шаге процедуры приведения к треугольному виду мы должны работать с h_7 и h_8 — только эти два полинома содержат x_8. Кроме того, h_8 имеет степень 1 по x_8. Таким образом, мы поступаем, как в шаге 3 треугольной процедуры, полагая $f_8 = h_8$ и заменяя h_7 на

$$\begin{aligned} f_7 &= \mathrm{Rem}(h_7, h_8, x_8)\\ &= (2x_1x_2 - 2x_2x_3 - 2x_1x_4)x_7 - x_1^2x_2 + x_2x_3^2 + x_1^2x_4 - x_2^2x_4 + x_2x_4^2. \end{aligned}$$

(Мы, как правило, игнорируем числовые множители при вычислении остатков.) Теперь только f_7 содержит x_7, поэтому мы сразу же переходим к x_6. Два полинома h_6 и h_5 содержат x_6, но оба имеют степень 1 по x_6, так что мы опять находимся в ситуации шага 3. Положим $f_6 = h_6$ и заменим h_5 на

$$f_5 = \mathrm{Rem}(h_5, h_6, x_6) = (u_1^2 + u_2^2)x_5 - u_1u_2^2.$$

Оставшиеся четыре полинома уже образуют треугольную систему; поэтому можно положить $f_i = h_i$ для $i = 1, 2, 3, 4$.

Шаг 2. Последовательное псевдоделение

Основной шаг метода Ву состоит в выполнении последовательного псевдоделения, описанного в (3), и в вычислении *последнего остат-*

ка R_0. Результативность этой процедуры описывается в следующей теореме.

Теорема 4. *Рассмотрим множество условий и заключение геометрической теоремы. Пусть* R_0 *— последний остаток, найденный при последовательном псевдоделении полинома* g *(как в* (3)*) с использованием системы полиномов* $f_1, \dots, f_n$ *треугольного вида* (2)*. Пусть* d_j *— старший коэффициент полинома* f_j *как полинома от* x_j *(т. е.* d_j *— полином от* $u_1, \dots, u_m, x_1, \dots, x_{j-1}$*). Тогда*

(i) *существуют неотрицательные целые числа* $s_1, \dots, s_n$ *и полиномы* $A_1, \dots, A_n$ *в кольце* $\mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$*, такие, что*

$$d_1^{s_1} \dots d_n^{s_n} g = A_1 f_1 + \dots + A_n f_n + R_0;$$

(ii) *если* $R_0 = 0$*, то* g *обращается в нуль в каждой точке множества* $V' - \mathbf{V}(d_1 d_2 \dots d_n) \subset \mathbb{R}^{m+n}$.

Доказательство. Пункт (i) доказывается последовательным применением предложения 1. Проводя псевдоделение полинома g на f_n по x_n, получаем

$$R_{n-1} = d_n^{s_n} g - q_n f_n.$$

На следующем шаге мы снова проводим псевдоделение, но по x_{n-1}:

$$\begin{aligned} R_{n-2} &= d_{n-1}^{s_{n-1}} (d_n^{s_n} g - q_n f_n) - q_{n-1} f_{n-1} \\ &= d_{n-1}^{s_{n-1}} d_n^{s_n} g - q_{n-1} f_{n-1} - d_{n-1}^{s_{n-1}} q_n f_n. \end{aligned}$$

Продолжая этот процесс, мы в конце концов придем к выражению вида

$$R_0 = d_1^{s_1} \dots d_n^{s_n} g - (A_1 f_1 + \dots + A_n f_n),$$

которое и требовалось получить.

(ii) Из п. (i) следует, что если $R_0 = 0$, то в каждой точке многообразия $W = \mathbf{V}(f_1, \dots, f_n)$ или g обращается в нуль, или один из $d_j^{s_j}$ обращается в нуль. Так как $V' \subset W$ (предложение 2), то это же справедливо и для V'. Теорема доказана. □

Хотя d_j зависят не только от u_i, уравнения $d_j = 0$, где d_j — старший коэффициент полинома f_j, могут быть интерпретированы как уравнения, определяющие *вырожденные специальные случаи* нашей геометрической конфигурации.

Пример 3 (продолжение). Закончим доказательство теоремы Аполлония с помощью метода Ву. Мы должны показать, что равенство

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0$$

является следствием условий $h_1 = \dots = h_8 = 0$ (см. (8) из § 4). Полиномы $f_1, \dots, f_8$ были найдены нами выше. Положим $R_8 = g$ и начнем последовательно вычислять остатки

$$R_{i-1} = \operatorname{Rem}(R_i, f_i, x_i)$$

при i, меняющемся от 8 до 1. При вычислении мы всегда будем брать минимально возможную степень s (см. предложение 1) и иногда игнорировать постоянные множители. Имеем

$$\begin{aligned}
R_7 =& x_4x_5^2 - 2x_4x_5x_7 + x_4x_6^2 - x_4x_1^2 + 2x_4x_1x_7 + x_6x_1^2 - 2x_6x_1x_7 \\
& - x_6x_3^2 + 2x_6x_3x_7 - x_6x_4^2, \\
R_6 =& x_4^2x_1x_5^2 - x_4^2x_1^2x_5 - x_4x_1x_6x_3^2 + x_4^2x_1x_6^2 - x_4^3x_1x_6 + x_4^2x_2^2x_5 \\
& - x_4^2x_2^2x_1 - x_2x_4^3x_5 + x_2x_4^3x_1 - x_2x_1x_4x_5^2 - x_2x_1x_4x_6^2 \\
& + x_2x_3x_4x_5^2 + x_2x_3x_4x_6^2 - x_2x_3x_4x_1^2 + x_4x_1^2x_6x_3 + x_4x_2^2x_6x_1 \\
& - x_4x_2^2x_6x_3 + x_2x_1^2x_4x_5 - x_2x_3^2x_4x_5 + x_2x_3^2x_4x_1, \\
R_5 =& u_2^2x_4^2x_1x_5^2 - u_2^2x_4^2x_1^2x_5 + u_2^2x_4^2x_2^2x_5 - u_2^2x_4^2x_2^2x_1 - u_2^2x_2x_4^3x_5 \\
& + u_2^2x_2x_4^3x_1 - x_4u_2^2x_2x_1x_5^2 + x_4u_2^2x_2x_3x_5^2 - x_4u_2^2x_2x_3x_1^2 \\
& + x_4u_2^2x_2x_1^2x_5 - x_4u_2^2x_2x_3^2x_5 + x_4u_2^2x_2x_3^2x_1 - u_1x_5u_2x_4^3x_1 \\
& + x_4u_1x_5u_2x_2^2x_1 - x_4u_1x_5u_2x_1x_3^2 - x_4u_1x_5u_2x_2^2x_3 \\
& + x_4u_1x_5u_2x_1^2x_3 + u_1^2x_5^2x_4^2x_1 - x_4u_1^2x_5^2x_2x_1 + x_4u_1^2x_5^2x_2x_3, \\
R_4 =& - u_2^4x_4x_2x_3x_1^2 - u_2^4x_4^2x_2^2x_1 + u_2^4x_4x_2x_3^2x_1 + u_2^4x_4^3x_2x_1 \\
& - u_2^2x_4u_1^2x_2x_3x_1^2 - u_2^2x_4^2u_1^2x_2^2x_1 + u_2^2x_4u_1^2x_2x_3^2x_1 \\
& + u_2^2x_4^3u_1^2x_2x_1 - u_2^4x_4^3u_1x_2 - u_2^3x_4^3u_1^2x_1 + u_2^4x_4^2u_1x_2^2 \\
& - u_2^4x_4^2u_1x_1^2 + u_2^3x_4u_1^2x_2^2x_1 - u_2^3x_4u_1^2x_1x_3^2 - u_2^4x_4u_1x_2x_3^2 \\
& + u_2^4x_4u_1x_2x_1^2 - u_2^3x_4u_1^2x_2^2x_3 + u_2^3x_4u_1^2x_1^2x_3 + u_2^4x_4^2u_1^2x_1 \\
& - u_2^4x_4u_1^2x_2x_1 + u_2^4x_4u_1^2x_2x_3, \\
R_3 =& 4u_2^5x_2x_3^2x_1 - 4u_2^5u_1x_2x_3^2 + 4u_2^5u_1x_2x_1^2 - 4u_2^5x_2x_3x_1^2 \\
& - 3u_2^5u_1^2x_2x_1 + 4u_2^5u_1^2x_2x_3 - 4u_2^4u_1^2x_1x_3^2 - 4u_2^4u_1^2x_2^2x_3 \\
& + 2u_2^4u_1^2x_2^2x_1 + 4u_2^4u_1^2x_1^2x_3 - 4u_2^3u_1^2x_2x_3x_1^2 + 4u_2^3u_1^2x_2x_3^2x_1 \\
& - 2u_2^6x_2^2x_1 - 2u_2^6u_1x_1^2 + 2u_2^6u_1x_2^2 + u_2^6u_1^2x_1 + u_2^7x_2x_1 \\
& - u_2^7u_1x_2, \\
R_2 =& 2u_2^5u_1x_2x_1^2 - 2u_2^5u_1^2x_2x_1 + 2u_2^4u_1^2x_2^2x_1 - 2u_2^6x_2^2x_1 \\
& - 2u_2^6u_1x_1^2 + 2u_2^6u_1x_2^2 + u_2^6u_1^2x_1 + u_2^7x_2x_1 - u_2^7u_1x_2 \\
& + u_2^5u_1^3x_2 - 2u_2^4u_1^3x_2^2 + 2u_2^4u_1^3x_1^2 - 2u_2^3u_1^3x_2x_1^2 + u_2^3u_1^4x_2x_1 \\
& - u_2^4u_1^4x_1, \\
R_1 =& - 2u_2^6u_1x_1^2 - u_2^4u_1^4x_1 + u_2^6u_1^2x_1 + 2u_2^4u_1^3x_1^2, \\
R_0 =& 0.
\end{aligned}$$

По теореме 4 это означает, что, если ни один из старших коэффициентов полиномов f_i не равен нулю, то теорема об окружности доказана методом Ву. Нетривиальные условия здесь таковы:

$$d_5 = u_1^2 + u_2^2 \neq 0,$$
$$d_6 = u_2 \neq 0,$$
$$d_7 = 2x_1x_2 - 2x_2x_3 - 2x_1x_4 \neq 0,$$
$$d_8 = -2x_4 \neq 0.$$

Второе условие $u_2 \neq 0$ означает, что вершины A и C прямоугольного треугольника $\triangle ABC$ различны. Напомним, что система координат выбрана так, что $A = (0,0)$ и $C = (0,u_2)$ (см. пример 3 из § 4). Из этого также следует справедливость первого условия, так как u_1 и u_2 вещественны. Условие $-2x_4 \neq 0$ эквивалентно условию $u_2 \neq 0$ (так как $h_4 = 2x_4 - u_2 = 0$). Наконец, условие $d_7 \neq 0$ означает, что вершины треугольника различны (см. упр. 5). Отсюда получаем, что заключение теоремы об окружности обобщенно следует из ее условий.

Элементарная версия метода Ву доказывает заключение $g = 0$ только при дополнительных условиях $d_j \neq 0$. В частности, в случае неприводимого многообразия V' не исключено, что некоторый d_j равен нулю на всем V' (так как V' состоит из одной компоненты). Если такой факт имеет место, то нельзя говорить о справедливости теоремы для конфигураций, соответствующих точкам из V'.

Но в случае, когда для заданного множества условий h многообразие V' неприводимо, существует гораздо более сильная версия теоремы 4. Достаточно сложная алгебраическая техника (алгоритм разложения Ритта) позволяет построить специальную треугольную систему полиномов f_j (которая называется характеристическим множеством), обладающую тем свойством, что $R_0 = 0$ тогда и только тогда, когда $g \in \mathbf{I}(V')$. В частности, старшие коэффициенты полинома f_j не могут обращаться в нуль на всем V'; поэтому из $R_0 = 0$ следует, что g должен обращаться в нуль на всем V'. Заинтересованный читатель может обратиться к книге CHOU (1988). Другое изложение теории характеристических множеств и алгоритма Ву—Ритта имеется в книгах MISHRA (1993) и WANG (1994b). Система Maple содержит пакет, называемый «charsets», в котором реализован метод характеристических множеств (см. WANG (1994a)).

Наконец, сделаем несколько сравнительных замечаний о методе базисов Грёбнера и методе Ву. Эти два метода имеют дело с одним и тем же классом геометрических теорем, и обычно результаты их применения одинаковы. Оба метода используют алгоритм деления, чтобы выяснить, принадлежит полином данному идеалу

или нет. Однако, как мы могли видеть из примера процедуры приведения к треугольному виду, метод Ву значительно эффективнее (в этой задаче). Причина состоит в том, что приводить к треугольному виду множество полиномов гораздо проще, чем найти базис Грёбнера идеала, который они порождают, или базис Грёбнера идеала $\widetilde{H} = \langle h_1, \ldots, h_n, 1 - yg \rangle$. Это особенно хорошо заметно, если исходная система полиномов уже имеет почти треугольную форму (а это часто бывает при переводе геометрических теорем на язык полиномов). В каком-то смысле превосходство метода Ву совершенно естественно, так как базис Грёбнера содержит гораздо больше информации об идеале, чем треугольная система. Обратите внимание, что мы даже не утверждаем, что треугольная система порождает тот же идеал, что и условия, как в $\mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, так и в $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$. На самом деле это неверно (упр. 4). Метод Ву является примером техники, нацеленной на решение одной конкретной задачи. Такая техника часто эффективнее общих методов (таких, как вычисление базиса Грёбнера), которые применимы для решения широкого круга задач.

Заинтересованный читатель может обратиться к книге CHOU (1988), во второй части которой приведен список из 512 геометрических теорем, доказанных программой, реализующей метод Ву. Работа WU (1983) является репринтом оригинальной работы, в которой и был изложен этот метод.

Упражнения к § 5

1. В этом упражнении рассматривается предложение 1.
   (a) Завершите доказательство п. (i).
   (b) Покажите, что q и r в равенстве $d_m^s f = qg + r$ *не* являются однозначно определенными, если на степень s не налагается никаких условий.
2. Докажите утверждение (сформулированное после предложения 1), что псевдоделение эквивалентно обычному делению полиномов в кольце $K[y]$, где $K = k(x_1, \ldots, x_n)$.
3. Покажите, что существует единственное минимальное $s \leq p - m + 1$ в предложении 1, для которого равенство $d_m^s f = qg + r$ имеет место. Докажите, что q и r определены для этого s однозначно. Указание: используйте единственность частного и остатка для деления при $k(x_1, \ldots, x_n)[y]$.
4. Приведите пример, показывающий, что применение процедуры приведения к треугольному виду к двум полиномам $h_1, h_2 \in k[x_1, x_2]$ может дать полиномы f_1, f_2, которые порождают идеал, строго меньший, чем $\langle h_1, h_2 \rangle$. То же самое справедливо и в случае большего числа переменных.

5. Докажите, что условие $d_7 \neq 0$ в теореме об окружности выполнено автоматически, если $u_1 \neq 0$ и $u_2 \neq 0$.
6. Примените метод Ву для проверки справедливости следующих теорем. В каждом случае рассмотрите условия $d_j \neq 0$, при которых теорема 4 гарантирует, что заключение g обобщенно следует из условий h_j. Если вы проделали соответствующие упражнения к § 4, то сравните эффективность (затраченное время и/или усилия, например) двух методов.
   (a) Теорема о диагоналях параллелограмма (упр. 1 к § 4).
   (b) Теорема об ортоцентре треугольника (упр. 5 к § 4).
   (c) Теорема о центроиде треугольника (упр. 6 к § 4).
   (d) Теорема о прямой Эйлера в треугольнике (упр. 7 к § 4).
   (e) Теорема Паппа (упр. 8 к § 4).
7. Рассмотрим теорему из упр. 17 к § 4 (где V' оказывается приводимым при прямом переводе условий теоремы на алгебраический язык).
   (a) Примените к ней метод Ву. (Последний остаток должен быть отличным от нуля.)
   (b) Приведет ли применение метода Ву к успеху для переформулированной теоремы из п. (e) упр. 17 к § 4.

7
Теория инвариантов конечных групп

Теория инвариантов оказала глубокое влияние на развитие алгебраической геометрии. Достаточно упомянуть, что теорема Гильберта о базисе и теорема Гильберта о нулях, которые играют центральную роль в первых главах этой книги, были доказаны Гильбертом в ходе его исследований в области теории инвариантов.

В этой главе мы будем изучать инварианты конечных групп. Основной целью является описание *всех* полиномов, не меняющихся при заменах переменных, определенных матрицами из некоторой конечной группы матриц. Наше рассмотрение этих вопросов будет вполне элементарным и, конечно, неполным. В частности, мы не предполагаем предварительного знакомства читателя с теорией групп.

§ 1. Симметрические полиномы

Симметрические полиномы естественно возникают при изучении корней полиномов. Рассмотрим, например, кубический полином $f = x^3+bx^2+cx+d$. Пусть его корнями являются числа $\alpha_1, \alpha_2, \alpha_3$. Тогда

$$x^3 + bx^2 + cx + d = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Если мы раскроем скобки в правой части этого равенства, то получим, что

$$\begin{aligned} &x^3 + bx^2 + cx + d \\ &\quad = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3. \end{aligned}$$

Таким образом,

$$\begin{aligned} b &= -(\alpha_1 + \alpha_2 + \alpha_3), \\ c &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\ d &= -\alpha_1\alpha_2\alpha_3. \end{aligned} \tag{1}$$

Мы видим, что коэффициенты полинома f являются полиномами от его корней. Кроме того, так как изменение порядка корней не

меняет f, то полиномы, выражающие b, c, d через $\alpha_1, \alpha_2, \alpha_3$, не меняются, если мы переставляем $\alpha_1, \alpha_2, \alpha_3$. Такие полиномы называются *симметрическими*. Дадим общее определение.

Определение 1. Полином $f \in k[x_1, \ldots, x_n]$ называется *симметрическим*, если

$$f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)$$

для любой перестановки $x_{i_1}, \ldots, x_{i_n}$ переменных $x_1, \ldots, x_n$.

Пусть, например, переменными являются x, y и z. Тогда $x^2+y^2+z^2$ и xyz — симметрические полиномы. Следующие симметрические полиномы играют важную роль в наших обсуждениях.

Определение 2. Пусть $x_1, \ldots, x_n$ — переменные. Определим полиномы $\sigma_1, \ldots, \sigma_n \in k[x_1, \ldots, x_n]$, называемые *элементарными симметрическими функциями*, следующим образом:

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n, \\
&\vdots \\
\sigma_r &= \sum_{i_1 < i_2 < \ldots < i_r} x_{i_1} x_{i_2} \ldots x_{i_r}, \\
&\vdots \\
\sigma_n &= x_1 x_2 \ldots x_n.
\end{aligned}$$

Другими словами, σ_r — это сумма всех произведений r различных переменных. В частности, каждый член в σ_r имеет полную степень r. Чтобы доказать, что эти полиномы симметрические, мы обобщим формулу (1). Введем новую переменную X и рассмотрим полином

$$f(X) = (X - x_1)(X - x_2)\ldots(X - x_n), \tag{2}$$

корнями которого являются $x_1, \ldots, x_n$. Раскроем скобки в правой части и получим

$$f(X) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \ldots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n$$

(детали доказательства мы оставляем читателю в качестве упражнения). Предположим теперь, что произведена перестановка переменных $x_1, \ldots, x_n$. Эта перестановка меняет порядок множителей в правой части формулы (2), но f при этом не меняется. Это и означает, что коэффициенты $(-1)^r\sigma_r$ полинома f являются симметрическими.

В качестве следствия получаем, что если старший коэффициент полинома равен 1, то остальные его коэффициенты являются элементарными симметрическими функциями от его корней (с точностью до умножения на ± 1). В упражнениях мы рассмотрим интересные следствия этого факта.

Из элементарных симметрических функций мы можем строить другие симметрические функции как полиномы от $\sigma_1, \ldots, \sigma_n$. Например,

$$\sigma_2^2 - \sigma_1\sigma_3 = x^2y^2 + x^2yz + x^2z^2 + xy^2z + xyz^2 + y^2z^2$$

является симметрическим полиномом. Удивительно, что *все* симметрические полиномы могут быть построены таким образом.

Теорема 3 (основное свойство симметрических полиномов). *Каждый симметрический полином из $k[x_1, \ldots, x_n]$ может быть однозначно представлен в виде полинома от элементарных симметрических функций $\sigma_1, \ldots, \sigma_n$.*

Доказательство. Мы будем использовать lex-упорядочение с $x_1 > x_2 > \ldots > x_n$. Пусть $f \in k[x_1, \ldots, x_n]$ — ненулевой симметрический полином и $\mathrm{LT}(f) = ax^\alpha$, где $\alpha = (\alpha_1, \ldots, \alpha_n)$. Мы утверждаем, что $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$. Предположим, что это не так. Тогда $\alpha_i < \alpha_{i+1}$ для некоторого i. Рассмотрим вектор степеней β, полученный из α перестановкой α_i и α_{i+1}: $\beta = (\ldots, \alpha_{i+1}, \alpha_i, \ldots)$. Так как ax^α является членом полинома f, то ax^β является членом полинома $f(\ldots, x_{i+1}, x_i, \ldots)$. Но f — симметрический полином. Значит, $f(\ldots, x_{i+1}, x_i, \ldots) = f$; поэтому ax^β также является членом полинома f, что невозможно, потому что $\beta > \alpha$.

Рассмотрим полином

$$h = \sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}.$$

Для того чтобы найти его старший член, отметим, что $\mathrm{LT}(\sigma_r) = x_1x_2\ldots x_r, 1 \leq r \leq n$. Следовательно,

$$\begin{aligned}
\mathrm{LT}(h) &= \mathrm{LT}(\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_n^{\alpha_n}) \\
&= \mathrm{LT}(\sigma_1)^{\alpha_1-\alpha_2}\,\mathrm{LT}(\sigma_2)^{\alpha_2-\alpha_3}\ldots\mathrm{LT}(\sigma_n)^{\alpha_n} \\
&= x_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3}\ldots(x_1\ldots x_n)^{\alpha_n} \\
&= x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n} = x^\alpha.
\end{aligned} \tag{3}$$

Значит, старшие члены полиномов f и ah совпадают; поэтому

$$\mathrm{multideg}(f - ah) < \mathrm{multideg}(f),$$

если $f - ah \neq 0$.

Положим теперь $f_1 = f - ah$. Тогда f_1 — симметрический полином, потому что f и ah симметрические. Если $f_1 \neq 0$, то мы можем повторить описанную выше процедуру и получить полином $f_2 = f_1 - a_1h_1$, где a_1 — константа, а h_1 — произведение функций $\sigma_1, \ldots, \sigma_n$ в некоторых степенях. Кроме того, нам известно, что

$\mathrm{LT}(f_2) < \mathrm{LT}(f_1)$, если $f_2 \neq 0$. Продолжая этот процесс, мы построим последовательность полиномов $f, f_1, f_2, \ldots$, таких, что

$$\mathrm{multideg}(f) > \mathrm{multideg}(f_1) > \mathrm{multideg}(f_2) > \ldots.$$

Так как lex-упорядочение является вполне упорядочением, то эта последовательность конечна. Но это может быть только в том случае, когда $f_{t+1} = 0$ для некоторого t. Тогда

$$f = ah + a_1h_1 + \ldots + a_th_t,$$

и, следовательно, f является полиномом от элементарных симметрических функций.

Теперь докажем единственность. Предположим, что f имеет два разных представления,

$$f = g_1(\sigma_1, \ldots, \sigma_n) = g_2(\sigma_1, \ldots, \sigma_n).$$

Здесь g_1 и g_2 — полиномы от n переменных, например, от $y_1, \ldots, y_n$. Мы хотим доказать, что $g_1 = g_2$ в $k[y_1, \ldots, y_n]$.

Положим $g = g_1 - g_2$. Тогда $g(\sigma_1, \ldots, \sigma_n) = 0$ в $k[x_1, \ldots, x_n]$. Единственность будет доказана, если мы докажем, что $g = 0$ в $k[y_1, \ldots, y_n]$. Предположим, что $g \neq 0, g = \sum_\beta a_\beta y^\beta$. Тогда $g(\sigma_1, \ldots, \sigma_n)$ является суммой полиномов вида $g_\beta = a_\beta \sigma_1^{\beta_1}\sigma_2^{\beta_2}\ldots\sigma_n^{\beta_n}$, где $\beta = (\beta_1, \ldots, \beta_n)$. Как и при выводе соотношения (3), получаем, что

$$\mathrm{LT}(g_\beta) = a_\beta x_1^{\beta_1+\ldots+\beta_n} x_2^{\beta_2+\ldots+\beta_n} \ldots x_n^{\beta_n}.$$

Легко показать, что отображение

$$(\beta_1, \ldots, \beta_n) \mapsto (\beta_1 + \ldots + \beta_n, \beta_2 + \ldots + \beta_n, \ldots, \beta_n)$$

является инъективным. Другими словами, полиномы g_β имеют различные старшие члены. В частности, если $\mathrm{LT}(g_\beta) > \mathrm{LT}(g_\gamma)$ для всех $\gamma \neq \beta$, то $\mathrm{LT}(g_\beta)$ больше *всех* членов полиномов g_γ. Следовательно, $\mathrm{LT}(g_\beta)$ не может сократиться и потому $g(\sigma_1, \ldots, \sigma_n) \neq 0$ в $k[y_1, \ldots, y_n]$. Теорема доказана. □

Только что изложенное доказательство принадлежит Гауссу, который использовал свойства симметрических полиномов в своем втором доказательстве (1816 г.) основной теоремы алгебры. Вот как Гаусс определял lex-упорядочение: «Тогда из двух членов

$$Ma^\alpha b^\beta c^\gamma \ldots \text{ и } Ma^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$$

старшим считается первый, а не второй, если

$$\text{или } \alpha > \alpha', \text{ или } \alpha = \alpha' \text{ и } \beta > \beta', \text{ или } \alpha = \alpha', \beta = \beta' \text{ и } \gamma > \gamma',$$
$$\text{или } \ldots \text{ и т. д.»}$$

(см. Gauss (1876, p. 36)). Это первое из известных явных определений lex-упорядочения.

Обратите внимание, что доказательство теоремы 3 дает алгоритм для преобразования симметрического полинома в полином от $\sigma_1, \ldots, \sigma_n$. Пусть, например,

$$f = x^3y + x^3z + xy^3 + xz^3 + y^3z + yz^3 \in k[x, y, z].$$

Старшим членом полинома f является $x^3y = \mathrm{LT}(\sigma_1^2\sigma_2)$. Переходим к полиному

$$f_1 = f - \sigma_1^2\sigma_2 = -2x^2y^2 - 5x^2yz - 2x^2z^2 - 5xy^2z - 5xyz^2 - 2y^2z^2.$$

Теперь $\mathrm{LT}(f_1) = -2x^2y^2 = -2\,\mathrm{LT}(\sigma_2^2)$; следовательно, переходим к полиному

$$f_2 = f - \sigma_1^2\sigma_2 + 2\sigma_2^2 = -x^2yz - xy^2z - xyz^2.$$

Тогда легко получить, что

$$f_3 = f - \sigma_1^2\sigma_2 + 2\sigma_2^2 + \sigma_1\sigma_3 = 0,$$

т. е.

$$f = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3$$

является единственным представлением полинома f через элементарные симметрические функции.

Удивительно, но нам на самом деле не нужен особый алгоритм для представления симметрического полинома в виде полинома от $\sigma_1, \ldots, \sigma_n$ — мы можем воспользоваться алгоритмом деления из гл. 2. Мы даже можем использовать алгоритм деления для проверки симметричности.

Предложение 4. *Зафиксируем в кольце $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ мономиальное упорядочение, такое, что любой моном, содержащий хотя бы один из x_i больше всех мономов из $k[y_1, \ldots, y_n]$. Пусть G — базис Грёбнера идеала $\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n\rangle \subset k[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Пусть $f \in k[x_1, \ldots, x_n]$ и $g = \bar{f}^G$ — остаток от деления полинома f на G. Тогда*

(i) *f симметричен в том и только том случае, когда $g \in k[y_1, \ldots, y_n]$;*

(ii) *если f симметричен, то $f = g(\sigma_1, \ldots, \sigma_n)$ — единственное представление f в виде полинома от элементарных симметрических функций $\sigma_1, \ldots, \sigma_n$.*

Доказательство. Пусть $f \in k[x_1, \ldots, x_n]$, а $g \in k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ — остаток от деления f на $G = \{g_1, \ldots, g_t\}$. Это означает, что

$$f = A_1g_1 + \ldots + A_tg_t + g,$$

где $A_1, \dots, A_t \in k[x_1, \dots, x_n, y_1, \dots, y_n]$. Мы можем считать, что $g_i \neq 0$ для всех i.

Докажем (i). Пусть сначала $g \in k[y_1, \dots, y_n]$. Подставим в формулу для f вместо каждого y_i соответствующее σ_i. При этой подстановке f не изменится, так как он не зависит от y_i, но каждый полином из идеала $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$ станет равным нулю. Так как полиномы $g_1, \dots, g_t$ принадлежат этому идеалу, то

$$f = g(\sigma_1, \dots, \sigma_n).$$

Следовательно, f симметричен.

Пусть теперь $f \in k[x_1, \dots, x_n]$ — симметрический полином. Тогда $f = g(\sigma_1, \dots, \sigma_n)$ для некоторого $g \in k[y_1, \dots, y_n]$. Мы хотим показать, что g является остатком от деления f на G. Отметим сначала, что в $k[x_1, \dots, x_n, y_1, \dots, y_n]$ моном от полиномов $\sigma_1, \dots, \sigma_n$ может быть представлен в следующем виде:

$$\begin{aligned}\sigma_1^{\alpha_1} \dots \sigma_n^{\alpha_n} &= (y_1 + (\sigma_1 - y_1))^{\alpha_1} \dots (y_n - (\sigma_n - y_n))^{\alpha_n} \\ &= y_1^{\alpha_1} \dots y_n^{\alpha_n} + B_1 \cdot (\sigma_1 - y_1) + \dots + B_n \cdot (\sigma_n - y_n),\end{aligned}$$

где $B_1, \dots, B_n \in k[x_1, \dots, x_n, y_1, \dots, y_n]$. Умножая на подходящие константы и суммируя эти равенства по всем мономам из g, получаем

$$g(\sigma_1, \dots, \sigma_n) = g(y_1, \dots, y_n) + C_1 \cdot (\sigma_1 - y_1) + \dots + C_n(\sigma_n - y_n),$$

где $C_1, \dots, C_n \in k[x_1, \dots, x_n, y_1, \dots, y_n]$. Так как $f = g(\sigma_1, \dots, \sigma_n)$, то

$$f = C_1 \cdot (\sigma_1 - y_1) + \dots + C_n \cdot (\sigma_n - y_n) + g(y_1, \dots, y_n). \quad (4)$$

Мы хотим показать, что g является остатком от деления f на G.

Докажем сначала, что ни один член полинома g не делится ни на один элемент из $\mathrm{LT}(G)$. Если это не так, то найдется $g_i \in G$, такой, что $\mathrm{LT}(g_i)$ делит некоторый член полинома g. Следовательно, $\mathrm{LT}(g_i)$ зависит только от $y_1, \dots, y_n$, так как $g \in k[y_1, \dots, y_n]$. Но наше упорядочение выбрано так, что из этого следует, что $g_i \in k[y_1, \dots, y_n]$. Теперь заменим каждое y_i соответствующим σ_i. Так как $g_i \in \langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$, то g_i становится равным нулю при такой замене. Но $g_i \in k[y_1, \dots, y_n]$; следовательно, $g_i(\sigma_1, \dots, \sigma_n) = 0$. По утверждению о единственности из теоремы 3 из этого следует, что $g_i = 0$, но по предположению $g_i \neq 0$. Мы пришли к противоречию, и утверждение доказано. Теперь в равенстве (4) ни один член полинома g не делится на элементы из $\mathrm{LT}(G)$. Так как G — базис Грёбнера, то по предложению 1 из § 6 гл. 2 g является остатком от деления полинома f на G. Это доказывает, что остаток принадлежит $k[y_1, \dots, y_n]$, если f — симметрический полином.

Пункт (ii) является прямым следствием приведенных выше рассуждений. □

Кажущимся неудобством этого предложения является необходимость вычислять базис Грёбнера идеала $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$. Однако в случае использования lex-упорядочения базис Грёбнера найти очень легко. Сначала введем обозначения. Если $u_1, \dots, u_s$ — переменные, то через

$$h_i(u_1, \dots, u_s) = \sum_{|\alpha| = i} u^\alpha$$

мы будем обозначать сумму *всех* мономов от $u_1, \dots, u_s$ полной степени i. Тогда базис Грёбнера определяется следующим образом.

Предложение 5. *Зафиксируем* lex*-упорядочение на* $k[x_1, \dots, x_n, y_1, \dots, y_n]$ *с* $x_1 > \dots > x_n > y_1 > \dots > y_n$. *Тогда полиномы*

$$g_m = h_m(x_m, \dots, x_n) + \sum_{i=1}^{m} (-1)^i h_{m-i}(x_m, \dots, x_n) y_i, \quad m = 1, \dots, n,$$

образуют базис Грёбнера идеала $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$.

Доказательство. Мы дадим набросок доказательства, детали будут рассмотрены в упражнениях. Будем использовать следующее полиномиальное тождество:

$$0 = h_m(x_m, \dots, x_n) + \sum_{i=1}^{m} (-1)^i h_{m-i}(x_m, \dots, x_n) \sigma_i. \quad (5)$$

Это тождество будет доказано в упр. 10 и 11.

Докажем, что $g_1, \dots, g_n$ образуют базис идеала $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$. Используя тождество (5), получаем

$$g_m = \sum_{i=1}^{m} (-1)^i h_{m-i}(x_m, \dots, x_n)(y_i - \sigma_i), \quad (6)$$

что доказывает включение $\langle g_1, \dots, g_n \rangle \subset \langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$. Чтобы доказать обратное включение, заметим, что так как $h_0 = 1$, то равенство (6) может быть записано в виде

$$g_m = (-1)^m (y_m - \sigma_m) + \sum_{i=1}^{m-1} (-1)^i h_{m-i}(x_m, \dots, x_n)(y_i - \sigma_i). \quad (7)$$

Теперь индукцией по m доказываем, что $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle \subset \langle g_1, \dots, g_n \rangle$ (см. упр. 12).

Нам осталось доказать, что $g_1, \dots, g_n$ образуют базис Грёбнера. В упр. 12 будет доказано, что

$$\mathrm{LT}(g_m) = x_m^m.$$

Именно в этом месте используется lex-упорядочение, определенное в условии предложения 5. Мы видим, что старшие члены полиномов

$g_1, \ldots, g_n$ взаимно просты. Теперь из результатов § 9 гл. 2 следует, что $g_1, \ldots, g_n$ образуют базис Грёбнера (детали доказательства рассматриваются в упр. 12).

При работе с симметрическими полиномами часто бывает удобным работать с *однородными* полиномами.

Определение 6. Полином $f \in k[x_1, \ldots, x_n]$ называется *однородным полной степени* m, если каждый член из f имеет полную степень m.

Обратите внимание, что i-я элементарная симметрическая функция однородна полной степени i. Важным фактом является то, что каждый полином имеет единственное представление в виде суммы однородных полиномов. А именно, пусть $f \in k[x_1, \ldots, x_n]$. Через f_m обозначим сумму всех членов полинома f полной степени m. Тогда f_m однородны и $f = \sum_m f_m$. Мы будем называть f_m *однородными компонентами* полинома f.

Предложение 7. *Полином $f \in k[x_1, \ldots, x_n]$ является симметрическим в том и только том случае, когда симметрическими являются все его однородные компоненты.*

Доказательство. Пусть f — симметрический полином, а $x_{i_1}, \ldots, x_{i_n}$ — некоторая перестановка переменных $x_1, \ldots, x_n$. Такая перестановка преобразует члены полной степени m в члены полной степени m. Так как $f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)$, то однородная компонента полной степени m также симметрическая. Обратное утверждение тривиально. □

Предложение 7 показывает, что при работе с симметрическим полиномом мы можем считать его однородным. В упражнениях мы рассмотрим, как однородность полинома f влияет на форму его представления в виде полинома от $\sigma_1, \ldots, \sigma_n$.

В заключение рассмотрим другие способы представления симметрических полиномов. Рассмотрим, в частности, *суммы степеней*

$$s_k = x_1^k + x_2^k + \ldots + x_n^k.$$

Обратите внимание, что полиномы s_k симметрические. Оказывается, что произвольный симметрический полином может быть выражен через $s_1, \ldots, s_n$ следующим образом.

Теорема 8. *Пусть поле k содержит поле рациональных чисел $\mathbb{Q}$. Тогда любой симметрический полином из $k[x_1, \ldots, x_n]$ может быть представлен как полином от $s_1, \ldots, s_n$.*

Доказательство. Так как каждый симметрический полином является полиномом от элементарных симметрических функций, то достаточно доказать, что $\sigma_1, \ldots, \sigma_n$ являются полиномами от $s_1, \ldots, s_n$. Для этого мы используем *тождества Ньютона*:

$$s_m - \sigma_1 s_{m-1} + \ldots + (-1)^{m-1}\sigma_{m-1}s_1 + (-1)^m m\sigma_m = 0, \quad 1 \le m \le n,$$

$$s_m - \sigma_1 s_{m-1} + \ldots + (-1)^{n-1}\sigma_{n-1}s_{m-n+1} + (-1)^n \sigma_n s_{m-n} = 0, \quad m > n.$$

Доказательство этих тождеств будет дано в упражнениях.

Теперь индукцией по m докажем, что σ_m является полиномом от $s_1, \ldots, s_n$. Это верно при $m = 1$, так как $\sigma_1 = s_1$. Предположим, что это верно для $1, 2, \ldots, m-1$. Тогда из тождеств Ньютона следует, что

$$\sigma_m = (-1)^{m-1}\frac{1}{m}(s_m - \sigma_1 s_{m-1} + \ldots + (-1)^{m-1}\sigma_{m-1}s_1).$$

Мы имеем право делить на m, так как $\mathbb{Q} \subset k$ (в упр. 16 рассмотрен пример того, что получается, если $\mathbb{Q}$ не принадлежит k). Теперь из нашего предположения индукции следует, что σ_m является полиномом от $s_1, \ldots, s_n$. □

Таким образом, элементарные симметрические функции выражаются через суммы степеней и наоборот. Например,

$$s_2 = \sigma_1^2 - 2\sigma_2 \quad \longleftrightarrow \quad \sigma_2 = \frac{1}{2}(s_1^2 - s_2),$$

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \quad \longleftrightarrow \quad \sigma_3 = \frac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3).$$

Суммы степеней неожиданно окажутся полезными в § 3, когда мы будем рассматривать алгоритм вычисления инвариантных полиномов для конечной группы.

Упражнения к § 1

1. Докажите, что полином $f \in k[x, y, z]$ симметрический в том и только том случае, когда $f(x, y, z) = f(y, x, z) = f(y, z, x)$.
2. (Это упражнение требует знания абстрактной алгебры.) Докажите, что полином $f \in k[x_1, \ldots, x_n]$ является симметрическим в том и только том случае, когда

$$f(x_1, x_2, x_3, \ldots, x_n) = f(x_2, x_1, x_3, \ldots, x_n) = f(x_2, x_3, \ldots, x_n, x_1).$$

Указание: докажите, что циклические перестановки $(1, 2)$ и $(1, 2, \ldots, n)$ порождают симметрическую группу S_n (см. упр. 11 в § 2.10 книги HERSTEIN (1975)).

3. Обозначим i-ю элементарную симметрическую функцию от переменных $x_1, \ldots, x_n$ через σ_i^n. Верхний индекс здесь обозначает количество переменных и не является степенью. Положим $\sigma_0^n = 1$ и $\sigma_i^n = 0$, если $i < 0$ или $i > n$. Докажите, что $\sigma_i^n = \sigma_i^{n-1} + x_n\sigma_{i-1}^{n-1}$ для всех $n > 1$ и всех i. Это тождество полезно при проведении индуктивных рассуждений, связанных с симметрическими функциями.
4. Пусть $f(X) = (X - x_1)\ldots(X - x_n)$ (как в (2)). Докажите, что $f = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \ldots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n$. Указание: используйте индукцию и тождества из упр. 3.
5. Рассмотрим полином

$$f = (x^2 + y^2)(x^2 + z^2)(y^2 + z^2) \in k[x, y, z].$$

   (a) Используя метод теоремы 3, представьте f в виде полинома от $\sigma_1, \sigma_2, \sigma_3$.
   (b) Используя метод предложения 4, представьте f в виде полинома от $\sigma_1, \sigma_2, \sigma_3$.

Для решения этого упражнения воспользуйтесь системой компьютерной алгебры. Обратите внимание на то, что, раскрывая скобки в произведении $(X - x)(X - y)(X - z)$, можно ввести в компьютер элементарные симметрические функции.

6. Пусть $x_1, \ldots, x_n$ — переменные. Докажите, что $\sum_{i \neq j} x_i^2 x_j = \sigma_1\sigma_2 - 3\sigma_3$. Указание: если у вас возникнут трудности, то обратитесь к упр. 13. Обратите внимание, что система компьютерной алгебры здесь не поможет.
7. Пусть полином $f = x^n + a_1x^{n-1} + \ldots + a_n \in k[x]$ имеет корни $\alpha_1, \ldots, \alpha_n$, принадлежащие полю $K \supset k$.
   (a) Докажите, что симметрический полином $g(\alpha_1, \ldots, \alpha_n)$ от корней полинома f может быть представлен в виде полинома от коэффициентов $a_1, \ldots, a_n$ полинома f.
   (b) Пусть коэффициенты симметрического полинома g принадлежат полю k. Тогда $g(\alpha_1, \ldots, \alpha_n) \in k$.
8. Пусть корни $\alpha_1, \ldots, \alpha_n$ полинома $f = x^n + a_1x^{n-1} + \ldots + a_n \in k[x]$ принадлежат полю $K \supset k$ (как в упр. 7). *Дискриминантом* полинома f называется следующее выражение:

$$D(f) = \prod_{i \neq j}(\alpha_i - \alpha_j).$$

   (a) Используя упр. 7, покажите, что $D(f)$ является полиномом от $a_1, \ldots, a_n$.
   (b) Найдите явное выражение для $D(f)$ в виде полинома от коэффициентов полинома f, если $n = 2$. Не знакома ли вам эта формула?
   (c) Найдите явное выражение для $D(f)$ в виде полинома от коэффициентов полинома f, если $n = 3$.

   (d) Докажите, что кубический полином $x^3 + a_1x^2 + a_2x + a_3$ имеет кратный корень в том и только том случае, когда $4a_1^3a_3 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2 = 0$.
9. Рассмотрим кубический полином $f = x^3 + a_1x^2 + a_2x + a_3$. Какому условию должны удовлетворять его коэффициенты, чтобы один его корень был равен среднему арифметическому двух других? Указание: если корень α_1 равен среднему арифметическому корней α_2 и α_3, то $2\alpha_1 - \alpha_2 - \alpha_3 = 0$, но, может быть, α_2 (или α_3) равен среднему арифметическому двух других корней; таким образом, условие упражнения эквивалентно тому, что произведение трех сомножителей типа $2\alpha_1 - \alpha_2 - \alpha_3$ равно нулю. Остается применить упр. 7.
10. Как и в предложении 5, пусть $h_i(x_1, \ldots, x_n)$ — сумма всех мономов полной степени i от переменных $x_1, \ldots, x_n$. Положим $\sigma_0 = 1$ и $\sigma_i = 0$ при $i > n$. В этом упражнении мы хотим доказать, что

$$0 = \sum_{i=0}^{m}(-1)^i h_{m-i}(x_1, \ldots, x_n)\sigma_i(x_1, \ldots, x_n).$$

    В упр. 11 это тождество будет использовано для доказательства тождества (5) из текста параграфа. Чтобы доказать его, мы найдем коэффициент при мономе x^α в произведении $h_{m-i}\sigma_i$. Так как каждый член в $h_{m-i}\sigma_i$ имеет полную степень m, то мы будем считать, что моном x^α имеет полную степень m. Через a мы обозначим число переменных, входящих в x^α.
    (a) Пусть x^α входит в $h_{m-i}\sigma_i$. Докажите, что $i \leq a$. Указание: сколько переменных содержит каждый член полинома σ_i?
    (b) Докажите, что если $i \leq a$, то в точности $\binom{a}{i}$ членов полинома σ_i содержат только те переменные, которые входят в x^α. Обратите внимание, что все члены полинома σ_i имеют полную степень i.
    (c) Докажите, что если $i \leq a$, то x^α входит в $h_{m-i}\sigma_i$ с коэффициентом $\binom{a}{i}$. Указание: это следует из п. (b), потому что h_{m-i} является суммой всех мономов полной степени $m - i$ и каждый моном входит в эту сумму с коэффициентом 1.
    (d) Докажите, что коэффициент при x^α в $\sum_{i=0}^{m}(-1)^i h_{m-i}\sigma_i$ равен $\sum_{i=0}^{a}(-1)^i\binom{a}{i}$. Но из формулы бинома следует, что этот коэффициент равен нулю, что и завершает доказательство тождества.
11. В этом упражнении мы докажем тождество

$$0 = h_m(x_m, \ldots, x_n) + \sum_{i=1}^{m}(-1)^i h_{m-i}(x_m, \ldots, x_n)\sigma_i(x_1, \ldots, x_n),$$

    которое использовалось при доказательстве предложения 5. Как и в упр. 10, положим $\sigma_0 = 1$. Тогда это тождество примет более компактный вид:

$$0 = \sum_{i=0}^{m}(-1)^i h_{m-i}(x_m, \ldots, x_n)\sigma_i(x_1, \ldots, x_n).$$

Идея состоит в том, чтобы отделить переменные $x_1, \dots, x_{m-1}$. Если $S \subset \{1, \dots, m-1\}$, то через x^S мы обозначим произведение соответствующих переменных, а через $|S|$ — число элементов в S.

(a) Докажите, что

$$\sigma_i(x_1, \dots, x_n) = \sum_{S \subset \{1,\dots,m-1\}} x^S \sigma_{i-|S|}(x_m, \dots, x_n),$$

где мы считаем, что $\sigma_j = 0$, если $j < 0$.

(b) Докажите, что

$$\sum_{i=0}^{m} (-1)^i h_{m-i}(x_m, \dots, x_n)\sigma_i(x_1, \dots, x_n)$$
$$= \sum_{S \subset \{1,\dots,m-1\}} x^S \left(\sum_{i=|S|}^{m} (-1)^i h_{m-i}(x_m, \dots, x_n)\sigma_{i-|S|}(x_m, \dots, x_n) \right).$$

(c) Используя упр. 10, докажите, что сумма внутри скобок равна нулю для каждого S. Это и докажет тождество. Указание: положите $j = i - |S|$.

12. В этом упражнении мы рассмотрим доказательство предложения 5. Пусть g_m такие же, как в формулировке предложения.
(a) Используя равенство (7), докажите, что $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle \subset \langle g_1, \dots, g_n \rangle$.
(b) Докажите, что $\mathrm{LT}(g_m) = x_m^m$.
(c) Используя п. (b) и результаты § 9 гл. 2 (особенно теорему 3 и предложение 4), докажите, что $g_1, \dots, g_m$ образуют базис Грёбнера.

13. Пусть f — однородный симметрический полином полной степени m.
(a) Докажите, что f может быть представлен в виде линейной комбинации (с коэффициентами в поле k) полиномов вида $\sigma_1^{i_1}\sigma_2^{i_2}\dots\sigma_n^{i_n}$, таких, что $m = i_1 + 2i_2 + \dots + ni_n$.
(b) Пусть l — максимальная степень переменной x_1 в f. Из симметричности следует, что l — это максимальная степень любой переменной в f. Пусть полином $\sigma_1^{i_1}\sigma_2^{i_2}\dots\sigma_n^{i_n}$ содержится в представлении полинома f, описанном в п. (a). Докажите, что $i_1 + i_2 + \dots + i_n \le l$.
(c) Докажите, что симметрический полином $\sum_{i \ne j} x_i^2 x_j$ может быть представлен в виде $a\sigma_1\sigma_2 + b\sigma_3$ для некоторых констант a и b. Найдите a и b. Сравните ваш результат с результатом упр. 6.

14. В этом упражнении мы докажем тождества Ньютона, использованные в доказательстве теоремы 8. Пусть переменными будут $x_1, \dots, x_n$.

(a) Как и в упр. 3, положим $\sigma_0 = 1$ и $\sigma_i = 0$, если или $i < 0$ или $i > n$. Докажите эквивалентность тождеств Ньютона тождествам

$$s_m - \sigma_1 s_{m-1} + \dots + (-1)^{m-1}\sigma_{m-1}s_1 + (-1)^m k\sigma_m = 0,$$

для *всех* $m \ge 1$.

(b) Докажите тождество п. (a) индукцией по n. Указание: обозначьте σ_i через σ_i^n и s_m через s_m^n, где верхний индекс — число переменных, учтите, что $s_m^n = s_m^{n-1} + x_n^m$, и используйте упр. 3.

15. В этом упражнении тождество (5) будет использовано для доказательства следующих *несимметрических тождеств Ньютона*

$$x_i^m - \sigma_1 x_i^{m-1} + \dots + (-1)^{m-1}\sigma_{m-1}x_i + (-1)^m\sigma_m = (-1)^m\hat{\sigma}_m^i, \quad 1 \le m \le n,$$
$$x_i^m - \sigma_1 x_i^{m-1} + \dots + (-1)^{n-1}\sigma_{n-1}x_i^{m-n+1} + (-1)^n\sigma_n x_i^{m-n} = 0, \quad m \ge n,$$

где $\hat{\sigma}_m^i = \sigma_m(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ есть m-я элементарная симметрическая функция от всех переменных, кроме x_i. Затем мы дадим второе доказательство тождеств Ньютона.

(a) Докажите, что несимметрическое тождество Ньютона при $m = n$ следует из (5). Затем докажите, что несимметрические тождества Ньютона при $m \ge n$ следуют из случая $m = n$. Указание: сначала рассмотрите случай $i = n$.

(b) Докажите, что несимметрическое тождество Ньютона для $m = n - 1$ следует из соответствующего тождества для $m = n$. Указание: $\sigma_n = x_i\hat{\sigma}_{n-1}^i$.

(c) Докажите несимметрические тождества Ньютона для $m < n$ индукцией по убыванию m. Указание: из упр. 3 следует, что $\sigma_m = \hat{\sigma}_m^i + x_i\hat{\sigma}_{m-1}^i$.

(d) Докажите, что $\sum_{i=1}^n \hat{\sigma}_m^i = (n-m)\sigma_m$. Указание: в скольких слагаемых $\hat{\sigma}_m^i$ содержится член $x_{i_1}\dots x_{i_m}$, где $1 \le i_1 < \dots < i_m \le n$?

(e) Докажите тождества Ньютона.

16. Рассмотрим поле $\mathbb{F}_2 = \{0, 1\}$ из двух элементов. Докажите, что симметрический полином $xy \in \mathbb{F}_2[x, y]$ невозможно представить в виде полинома от s_1 и s_2 с коэффициентами из $\mathbb{F}_2$. Указание: докажите, что $s_2 = s_1^2$.

17. Представьте s_4 в виде полинома от $\sigma_1, \dots, \sigma_4$ и σ_4 в виде полинома от $s_1, \dots, s_4$.

18. Алгоритм деления можно использовать для автоматизации процесса представления полинома $g(\sigma_1, \dots, \sigma_n)$ в виде полинома от $s_1, \dots, s_n$. А именно, рассмотрим $\sigma_1, \dots, \sigma_n, s_1, \dots, s_n$ как новые переменные, и пусть

$$g_m = s_m - \sigma_1 s_{m-1} + \dots + (-1)^{m-1}\sigma_{m-1}s_1 + (-1)^m k\sigma_m, 1 \le m \le n.$$

Докажите, что при «правильном» lex-упорядочении остаток от деления полинома $g(\sigma_1,\dots,\sigma_n)$ на $g_1,\dots,g_n$ будет полиномом $h(s_1,\dots,s_n)$, таким, что $g(\sigma_1,\dots,\sigma_n)=h(s_1,\dots,s_n)$. Указание: нужное lex-упорядочение *не* является упорядочением $\sigma_1>\dots>\sigma_n>s_1>\dots>s_n$.

§ 2. Конечные матричные группы и кольца инвариантов

В этом параграфе мы дадим определение инварианта конечной матричной группы и рассмотрим примеры тех задач, которыми занимается теория инвариантов. До конца этого параграфа под полем k мы понимаем поле, содержащее поле рациональных чисел $\mathbb{Q}$. Такие поля называются полями *характеристики нуль*.

Определение 1. Через $\mathrm{GL}(n,k)$ мы будем обозначать множество всех обратимых $n\times n$-матриц с элементами из k.

Если A и B — обратимые $n\times n$-матрицы, то из курса линейной алгебры известно, что их произведение AB обратимо и обратная матрица A^{-1} также обратима (упр. 1). Напомним, что единичная $n\times n$-матрица I_n обладает следующими свойствами: $A\cdot I_n=I_n\cdot A=A$ и $A\cdot A^{-1}=I_n$ для любой матрицы $A\in\mathrm{GL}(n,k)$. В терминологии приложения А это означает, что $\mathrm{GL}(n,k)$ является *группой*.

Отметим, что матрица $A\in\mathrm{GL}(n,k)$ задает обратимое линейное отображение $A:k^n\to k^n$ (умножением слева на эту матрицу вектор-столбцов). Так как каждое линейное отображение пространства k^n на себя может быть задано таким образом, то $\mathrm{GL}(n,k)$ обычно называют *общей линейной группой*.

Нас будут в основном интересовать следующие подмножества из $\mathrm{GL}(n,k)$.

Определение 2. Конечное подмножество $G\subset\mathrm{GL}(n,k)$ называется *конечной матричной группой*, если оно непусто и замкнуто относительно матричного умножения. Количество элементов в G называется *порядком* этой группы и обозначается $|G|$.

Рассмотрим примеры конечных матричных групп.

Пример 3. Пусть матрица $A\in\mathrm{GL}(n,k)$ такова, что $A^m=I_n$ для некоторого положительного m. Если m — наименьшее положительное число с таким свойством, то легко доказать, что множество

$$C_m=\{I_n,A,A^2,\dots,A^{m-1}\}\subset\mathrm{GL}(n,k)$$

замкнуто относительно умножения (упр. 2) и, следовательно, является конечной матричной группой. Мы будем называть C_m *циклической группой* порядка m. Пусть, например,

$$A=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\subset\mathrm{GL}(2,k).$$

Тогда $A^4=I_2$, а следовательно, $C_4=\{I_2,A,A^2,A^3\}$ — это циклическая группа порядка 4 в $\mathrm{GL}(2,k)$.

Пример 4. Важный пример конечной матричной группы связан с перестановками переменных, обсуждавшимися в § 1. Обозначим через τ перестановку $x_{i_1},\dots,x_{i_n}$ переменных $x_1,\dots,x_n$. Так как τ полностью определяется тем, как она действует на индексы, то положим $i_1=\tau(1),i_2=\tau(2),\dots,i_n=\tau(n)$. Теперь соответствующую перестановку переменных можно записать в виде $x_{\tau(1)},\dots,x_{\tau(n)}$.

Построим по τ матрицу следующим образом. Рассмотрим линейное отображение, которое переводит $(x_1,\dots,x_n)$ в $(x_{\tau(1)},\dots,x_{\tau(n)})$. Матрица, соответствующая этому линейному отображению, обозначается через M_τ и называется *матрицей перестановки*. Это означает, что

$$M_\tau\cdot\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}=\begin{pmatrix}x_{\tau(1)}\\\vdots\\x_{\tau(n)}\end{pmatrix}.$$

Мы оставляем читателю в качестве самостоятельного упражнения доказательство того факта, что M_τ может быть получена из единичной матрицы I_n перестановкой столбцов в соответствии с τ. Точнее, $\tau(i)$-й столбец матрицы M_τ равен i-му столбцу матрицы I_n. Рассмотрим, например, перестановку τ, которая (x,y,z) переводит в (y,z,x), т. е. $\tau(1)=2,\tau(2)=3$ и $\tau(3)=1$. Тогда

$$M_\tau\cdot\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}y\\z\\x\end{pmatrix}.$$

Так как количество перестановок n переменных равно $n!$, то имеется $n!$ матриц перестановок. Более того, множество матриц перестановок замкнуто относительно умножения: легко доказать, что

$$M_\tau\cdot M_\nu=M_{\nu\tau},$$

где $\nu\tau$ — это перестановка, переводящая i в $\nu(\tau(i))$ (см. упр. 4). Таким образом, множество матриц перестановок является конечной матричной группой в $\mathrm{GL}(n,k)$. Эту матричную группу мы будем обозначать через S_n. (Строго говоря, группа матриц перестановок только изоморфна S_n в смысле теории групп. Мы это различие будем игнорировать.)

Пример 5. Другой важный класс конечных матричных групп связан с симметриями правильных многогранников. Рассмотрим, например, куб в $\mathbb{R}^3$ с центром в начале координат. Множество вращений пространства $\mathbb{R}^3$, переводящих куб в себя, конечно и замкнуто относительно умножения, т. е. оно является конечной матричной группой в $\mathrm{GL}(3,\mathbb{R})$. Все конечные матричные группы в $\mathrm{GL}(3,\mathbb{R})$ описаны, и с этими группами связаны глубокие геометрические результаты (некоторые примеры см. в упр. 5–9). Заинтересованный читатель может обратиться к книгам BENSON, GROVE (1985), KLEIN (1884) или COXETER (1973).

Конечные матричные группы обладают целым рядом полезных свойств.

Предложение 6. *Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа. Тогда*

(i) $I_n \in G$;
(ii) *если $A \in G$, то $A^m = I_n$ для некоторого положительного m;*
(iii) *если $A \in G$, то $A^{-1} \in G$.*

Доказательство. Если $A \in G$, то $\{A, A^2, A^3, \dots\} \subset G$, так как G замкнута относительно умножения. Из конечности группы G следует, что $A^i = A^j$ для некоторых $i > j$, а так как A обратима, то, умножая обе части равенства на A^{-j}, получим, что $A^m = I_n$, где $m = i - j > 0$. Это доказывает (ii).

Докажем (iii). Из (ii) следует, что $I_n = A^m = A \cdot A^{m-1} = A^{m-1} \cdot A$. Отсюда следует, что $A^{-1} = A^{m-1} \in G$, поскольку G замкнута относительно умножения. Теперь докажем (i). Так как $G \neq \varnothing$, то мы можем взять некоторую матрицу $A \in G$. Тогда $I_n = A^m \in G$ по (ii). □

Рассмотрим теперь действие элементов из $\mathrm{GL}(n,k)$ на полиномы из $k[x_1,\dots,x_n]$. Пусть $A = (a_{ij}) \in \mathrm{GL}(n,k)$ и $f \in k[x_1,\dots,x_n]$. Тогда

$$g(x_1,\dots,x_n) = f(a_{11}x_1 + \dots + a_{1n}x_n, \dots, a_{n1}x_1 + \dots + a_{nn}x_n)) \quad (1)$$

также является полиномом из $k[x_1,\dots,x_n]$. Представим это равенство в более компактном виде. Для этого обозначим через $\mathbf{x}$ вектор-столбец переменных $x_1,\dots,x_n$, т. е.

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Тогда равенство (1) может быть записано в матричном виде:

$$g(\mathbf{x}) = f(A \cdot \mathbf{x}).$$

Если рассматривать A как матрицу перехода к новому базису, то g — это f в новых координатах.

Пусть, например, $f(x,y) = x^2 + xy + y^2 \in \mathbb{R}[x,y]$, а

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R}).$$

Тогда

$$\begin{aligned} g(x,y) = f(A \cdot \mathbf{x}) &= f\left(\frac{x-y}{\sqrt{2}}, \frac{x+y}{\sqrt{2}}\right) \\ &= \left(\frac{x-y}{\sqrt{2}}\right)^2 + \frac{x-y}{\sqrt{2}} \cdot \frac{x+y}{\sqrt{2}} + \left(\frac{x+y}{\sqrt{2}}\right)^2 \\ &= \frac{3}{2}x^2 + \frac{1}{2}y^2. \end{aligned}$$

С геометрической точки зрения этим преобразованием мы исключили член xy в f, повернув систему координат на 45°.

Замечательным фактом является то, что иногда такое преобразование не меняет полином. Если, например, $h(x,y) = x^2 + y^2$ и A — матрица, о которой шла речь выше, то

$$h(\mathbf{x}) = h(A \cdot \mathbf{x}).$$

Мы будем говорить, что полином h *инвариантен* относительно A. Эти наблюдения приводят нас к фундаментальному определению.

Определение 7. Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа. Полином $f(\mathbf{x}) \in k[x_1,\dots,x_n]$ называется *инвариантным* относительно группы G (или ее *инвариантом*), если

$$f(\mathbf{x}) = f(A \cdot \mathbf{x}),$$

для всех $A \in G$. Множество всех инвариантных относительно G полиномов обозначается $k[x_1,\dots,x_n]^G$.

Основной пример инвариантов дают симметрические полиномы.

Пример 8. Рассмотрим группу $S_n \subset \mathrm{GL}(n,k)$ всех матриц перестановок. Очевидно, что

$$k[x_1,\dots,x_n]^{S_n} = \{\text{все симметрические полиномы в } k[x_1,\dots,x_n]\}.$$

По теореме 3 из § 1 симметрические полиномы — это полиномы от элементарных симметрических функций с коэффициентами в k. Мы можем записать это следующим образом:

$$k[x_1,\dots,x_n]^{S_n} = k[\sigma_1,\dots,\sigma_n].$$

Таким образом, каждый инвариант является полиномом от конечного числа инвариантов (элементарных симметрических функций).

Кроме того, мы знаем, что такое представление единственно. Все это дает нам явное описание инвариантов группы S_n.

Одна из основных задач теории инвариантов — выяснить, можно ли множество инвариантов $k[x_1,\dots,x_n]^G$ описать так же хорошо, как множество $k[x_1,\dots,x_n]^{S_n}$ в примере 8. Докажем сначала, что множество $k[x_1,\dots,x_n]^G$ имеет следующую алгебраическую структуру.

Предложение 9. *Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа. Тогда множество $k[x_1,\dots,x_n]^G$ замкнуто относительно сложения и умножения, а также содержит все константы.*

Доказательство. (Легкое) доказательство этого предложения мы оставляем читателю. □

Сложение и умножение в $k[x_1,\dots,x_n]^G$ автоматически коммутативны, ассоциативны, дистрибутивны и т. п., потому что этими свойствами обладают операции в $k[x_1,\dots,x_n]$. В соответствии с терминологией гл. 5 $k[x_1,\dots,x_n]^G$ является *кольцом*. Более того, $k[x_1,\dots,x_n]^G$ является *подкольцом* кольца $k[x_1,\dots,x_n]$.

Теперь мы знаем три способа строить новые кольца. В гл. 5 мы научились строить факторкольцо $k[x_1,\dots,x_n]/I$ по идеалу $I \subset k[x_1,\dots,x_n]$ и координатное кольцо $k[V]$ аффинного многообразия $V \subset k^n$. А только что мы узнали, как строить кольцо инвариантов $k[x_1,\dots,x_n]^G$ конечной матричной группы $G \subset \mathrm{GL}(n,k)$. В § 4 мы увидим, что эти три конструкции тесно связаны.

В § 1 было доказано, что однородные компоненты симметрических полиномов также симметрические. То же самое справедливо для инвариантов любой матричной группы.

Предложение 10. *Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа. Тогда полином $f \in k[x_1,\dots,x_n]$ инвариантен относительно G в том и только том случае, когда инвариантны его однородные компоненты.*

Доказательство. См. упр. 11. □

Во многих ситуациях предложение 10 позволяет сводить рассмотрения к случаю однородных инвариантов. Это будет особенно полезно в доказательствах ряда утверждений в § 3.

В следующей лемме формулируется полезный критерий инвариантности.

Лемма 11. *Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа и матрицы $A_1,\dots,A_m \in G$ таковы, что любая матрица $A \in G$ может быть представлена в виде*

$$A = B_1 B_2 \dots B_t,$$

где $B_i \in \{A_1,\dots,A_m\}$ для любого i (другими словами, $A_1,\dots,A_m$ порождают G). Тогда полином $f \in k[x_1,\dots,x_n]$ инвариантен относительно G в том и только том случае, когда

$$f(\mathbf{x}) = f(A_1\cdot\mathbf{x}) = \dots = f(A_m\cdot\mathbf{x}).$$

Доказательство. Докажем сначала, что если f инвариантен относительно матриц $B_1,\dots,B_t$, то он инвариантен относительно их произведения. Это очевидно, если $t=1$. Предположим, что это верно для $t-1$. Тогда

$$\begin{aligned} f((B_1\dots B_t)\cdot\mathbf{x}) &= f((B_1\dots B_{t-1})\cdot B_t\mathbf{x}) \\ &= f(B_t\cdot x) \text{ (по предположению индукции)} \\ &= f(\mathbf{x}) \text{ (в силу инвариантности относительно } B_t). \end{aligned}$$

Пусть теперь f инвариантен относительно $A_1,\dots,A_m$. Так как каждый элемент $A \in G$ может быть записан в виде произведения $B_1\dots B_t$, где каждое B_i является одним из $A_1,\dots,A_m$, то $f \in k[x_1,\dots,x_n]^G$. Обратное утверждение очевидно. □

Теперь мы можем найти некоторые интересные примеры колец инвариантов.

Пример 12. Рассмотрим конечную матричную группу

$$V_4 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \subset \mathrm{GL}(2,k),$$

которая иногда называется *четверной группой Клейна*. Мы используем обозначение V_4, потому что «четыре» по немецки — это «vier». Легко проверить, что две матрицы

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

порождают V_4. По лемме 11 полином $f \in k[x,y]$ является инвариантом группы V_4 в том и только том случае, когда

$$f(x,y) = f(-x,y) = f(x,-y).$$

Пусть $f = \sum_{ij} a_{ij}x^iy^j$. Тогда

$$\begin{aligned} f(x,y) = f(-x,y) &\iff \sum_{ij} a_{ij}x^iy^j = \sum_{ij} a_{ij}(-x)^iy^j \\ &\iff \sum_{ij} a_{ij}x^iy^j = \sum_{ij}(-1)^i a_{ij}x^iy^j \\ &\iff a_{ij} = (-1)^i a_{ij} \text{ для всех } i,j \\ &\iff a_{ij} = 0, \text{ если } i \text{ нечетно.} \end{aligned}$$

Из этого следует, что f содержит переменную x только в четной степени. Аналогично, из условия $f(x,y) = f(x,-y)$ следует, что f содержит переменную y только в четной степени. Таким образом,

$$f(x,y) = g(x^2, y^2),$$

для некоторого однозначно определенного полинома $g \in k[x,y]$. С другой стороны, полином f такого вида, очевидно, инвариантен относительно V_4. Значит,

$$k[x,y]^{V_4} = k[x^2, y^2].$$

Таким образом, каждый инвариант группы V_4 может быть однозначно представлен в виде полинома от двух однородных инвариантов x^2 и y^2. Таким образом, инварианты группы Клейна похожи на симметрические полиномы.

Пример 13. Рассмотрим теперь пример, когда инварианты описываются не столь просто, а именно циклическую группу $C_2 = \{\pm I_2\} \subset \mathrm{GL}(2,k)$ второго порядка. В этом случае инвариантами являются полиномы $f \in k[x,y]$, такие, что $f(x,y) = f(-x,-y)$. Мы оставляем читателю в качестве упражнения доказательство того, что инвариантность f эквивалентна условию

$$f(x,y) = \sum_{ij} a_{ij} x^i y^j, \text{ где } a_{ij} = 0, \text{ если } i+j \text{ нечетно.}$$

Это означает, что f — инвариант группы C_2, если в каждом его члене степени переменных x и y имеют одинаковую четность (т. е. или обе четные, или обе нечетные). Таким образом, каждый моном $x^i y^j$, входящий в f, имеет вид

$$x^i y^j = \begin{cases} x^{2m} y^{2l} = (x^2)^m (y^2)^l, & \text{если } i,j \text{ четны,} \\ x^{2m+1} y^{2l+1} = (x^2)^m (y^2)^l xy, & \text{если } i,j \text{ нечетны.} \end{cases}$$

Следовательно, каждый моном в f, а значит, и сам f является полиномом от трех однородных инвариантов x^2, y^2 и xy. Другими словами,

$$k[x,y]^{C_2} = k[x^2, y^2, xy].$$

Обратите внимание, что все три эти инварианта необходимы для того, чтобы породить кольцо $k[x,y]^{C_2}$.

Кольцо $k[x^2, y^2, xy]$ резко отличается от колец инвариантов, рассмотренных ранее, потому что здесь отсутствует единственность: инвариант может иметь несколько представлений в виде полинома от x^2, y^2, xy. Например, полином x^4y^2, очевидно, является инвариантом группы C_2, но

$$x^4 y^2 = (x^2)^2 \cdot y^2 = x^2 \cdot (xy)^2.$$

В § 4 мы увидим, что это связано с существованием алгебраического соотношения $x^2 \cdot y^2 = (xy)^2$ между основными инвариантами. Вообще говоря, основная задача[1)] теории и состоит в определении всех алгебраических соотношений между инвариантами. Если такая информация имеется, то нетрудно понять, где и как нарушается единственность.

Эти примеры позволяют сформулировать две основные задачи в теории инвариантов конечных групп. Пусть G — конечная матричная группа и $k[x_1, \ldots, x_n]^G$ — ее кольцо инвариантов.

- (Конечная порожденность) Верно ли, что существует конечный набор однородных инвариантов $f_1, \ldots, f_m$, таких, что каждый инвариант является полиномом от $f_1, \ldots, f_m$?
- (Единственность) Сколькими способами инвариант f может быть представлен как полином от $f_1, \ldots, f_m$? В § 4 мы увидим, что эта задача сводится к задаче описания алгебраических соотношений между инвариантами $f_1, \ldots, f_m$.

В §§ 3 и 4 мы дадим полные ответы на эти вопросы. Мы также рассмотрим алгоритмы нахождения инвариантов и соотношений между ними.

Упражнения к § 2

1. Пусть $A, B \in \mathrm{GL}(n,k)$ — обратимые матрицы. Докажите обратимость матриц AB и A^{-1}.
2. Пусть $A \in \mathrm{GL}(n,k)$ и $A^m = I_n$ для некоторого положительного m. Докажите, что если m — наименьшее из таких чисел, то множество $\{I_n, A, A^2, \ldots, A^{m-1}\}$ содержит в точности m элементов и замкнуто относительно умножения.
3. Выпишите все шесть матриц перестановок из группы $\mathrm{GL}(3,k)$.
4. Пусть M_τ — матрица линейного преобразования, которое переводит $x_1, \ldots, x_n$ в $x_{\tau(1)}, \ldots, x_{\tau(n)}$. Это означает, что если $e_1, \ldots, e_n$ — стандартный базис в k^n, то $M_\tau \cdot (\sum_j x_j e_j) = \sum_j x_{\tau(j)} e_j$.
   (a) Докажите, что $M_\tau \cdot e_{\tau(i)} = e_i$. Указание: обратите внимание, что $\sum_j x_j e_j = \sum_j x_{\tau(j)} e_{\tau(j)}$.
   (b) Докажите, что $\tau(i)$-й столбец матрицы M_τ равняется i-му столбцу матрицы I_n.
   (c) Докажите, что $M_\tau \cdot M_\nu = M_{\nu\tau}$, где перестановка $\nu\tau$ переводит i в $\nu(\tau(i))$.
5. Рассмотрим куб в $\mathbb{R}^3$ с центром в начале координат, ребра которого параллельны координатным осям и имеют длину 2.

[1)] Точнее, одна из основных задач. — *Прим. ред.*

(a) Докажите, что существует только конечное число вращений пространства $\mathbb{R}^3$ с центром в начале координат, переводящих куб в себя, и что множество таких вращений замкнуто относительно композиции. Рассматривая матрицы этих вращений, мы получим конечную матричную группу $G \subset \mathrm{GL}(3,\mathbb{R})$.

(b) Докажите, что $|G| = 24$. Указание: каждое вращение является вращением относительно некоторой прямой, проходящей через начало координат, так что сначала нужно найти эти «линии симметрии» куба.

(c) Найдите в G матрицу вращения на угол $120°$ против часовой стрелки относительно диагонали, соединяющей вершины $(-1,-1,-1)$ и $(1,1,1)$.

(d) Найдите в G матрицу вращения на угол $90°$ против часовой стрелки вокруг оси z.

(e) Докажите геометрически, что G порождается двумя матрицами, из п. (c) и из п. (d).

6. В этом упражнении мы геометрическими методами найдем некоторые инварианты группы вращений куба G из упр. 5.

(a) Объясните, почему $x^2+y^2+z^2 \in \mathbb{R}[x,y,z]^G$. Указание: рассуждайте геометрически в терминах расстояния от начала координат.

(b) Докажите геометрически, что объединение трех координатных плоскостей $\mathbf{V}(xyz)$ сохраняется под действием вращений из группы G.

(c) Докажите, что $\mathbf{I}(\mathbf{V}(xyz)) = \langle xyz \rangle$, и убедитесь, что если $f = xyz$ и $A \in G$, то $f(A \cdot \mathbf{x}) = axyz$ для некоторого вещественного a.

(d) Докажите, что если $f = xyz$, то $f(A \cdot \mathbf{x}) = \pm xyz$ для всех $A \in G$ и что $x^2y^2z^2 \in k[x,y,z]^G$. Указание: используйте п. (c) и тот факт, что $A^m = I_3$ для некоторого натурального m.

(e) Используя аналогичные методы, докажите, что полиномы

$$((x+y+z)(x+y-z)(x-y+z)(x-y-z))^2,$$
$$\left((x^2-y^2)(x^2-z^2)(y^2-z^2)\right)^2$$

принадлежат $k[x,y,z]^G$. Указание: плоскость $x+y+z=0$ перпендикулярна диагонали куба.

7. В этом упражнении мы продолжим изучение инвариантов группы вращений куба, начатое в упр. 6.

(a) Докажите, что $f \in k[x,y,z]^G$ в том и только том случае, когда $f(x,y,z) = f(y,z,x) = f(-y,x,z)$. Указание: примените пп. (c), (d) и (e) упр. 5.

(b) Пусть

$$f = xyz,$$
$$g = (x+y+z)(x+y-z)(x-y+z)(x-y-z),$$
$$h = (x^2-y^2)(x^2-z^2)(y^2-z^2).$$

В упр. 6 было доказано, что $f^2, g^2, h^2 \in k[x,y,z]^G$. Докажите, что $f, h \notin k[x,y,z]^G$, но $g, fh \in k[x,y,z]^G$. Таким образом, учитывая результаты упр. 6, мы получаем инварианты $x^2+y^2+z^2, g, f^2, fh$ и h^2 группы G степеней $2,4,6,9$ и 12 соответственно. В § 3 будет доказано, что h^2 может быть выражен через другие инварианты.

8. В этом упражнении будет рассмотрена интересная «двойственность» правильных многогранников.

(a) Рассмотрим куб и октаэдр в $\mathbb{R}^3$ с центрами в начале координат. Пусть ребра куба параллельны координатным осям, а вершины октаэдра лежат на этих осях. Докажите, что группы вращений этих многогранников совпадают. Указание: поместите вершины октаэдра в центры граней куба.

(b) Докажите аналогичное утверждение для додекаэдра и икосаэдра. Указание: что получится, если соединить центры 12 граней додекаэдра?

(c) Пункты (a) и (b) показывают, что в некотором смысле октаэдр является «двойственным» кубу, а икосаэдр — додекаэдру. Какой многогранник «двойствен» тетраэдру?

9. (Это упражнение требует знания абстрактной алгебры.) В этом упражнении мы рассмотрим тетраэдр с центром в начале координат.

(a) Докажите, что вращения пространства $\mathbb{R}^3$ с центром в начале координат, переводящие тетраэдр в себя, образуют конечную матричную группу G порядка 12 в $\mathrm{GL}(3,\mathbb{R})$.

(b) Так как каждое вращение тетраэдра индуцирует перестановку четырех его вершин, то докажите существование группового гомоморфизма $\rho : G \to S_4$.

(c) Докажите, что ρ инъективен и что его образом является знакопеременная группа A_4. Это показывает, что группа вращений тетраэдра изоморфна A_4.

10. Докажите предложение 9.

11. Докажите предложение 10. Указание: пусть $A = (a_{ij}) \in \mathrm{GL}(n,k)$, и пусть $x_1^{i_1} \dots x_n^{i_n}$ — моном полной степени $m = i_1 + \dots + i_n$ в f. Тогда полином

$$(a_{11}x_1 + \dots + a_{1n}x_n)^{i_1} \dots (a_{n1}x_1 + \dots + a_{nn}x_n)^{i_n}$$

однороден полной степени m.

12. В примере 13 мы рассматривали полиномы $f \in k[x,y]$, такие, что $f(x,y) = f(-x,-y)$. Докажите, что если $f = \sum_{ij} a_{ij}x^iy^j$, то это условие эквивалентно условию, что $a_{ij} = 0$, если $i+j$ нечетно.

13. В примере 13 мы нашли алгебраическое соотношение $x^2 \cdot y^2 = (xy)^2$ между инвариантами x^2, y^2 и xy. Мы хотим доказать, что это соотношение является в некотором смысле единственным. Точнее, рассмотрим полином $g(u,v,w) \in k[u,v,w]$, такой, что $g(x^2,y^2,xy) = 0$. Мы хотим доказать, что $g(u,v,w)$ делится (в $k[u,v,w]$) на полином $uv - w^2$ (этот полином соответствует приведенному выше соотношению).

(a) Разделите g на $uv - w^2$, используя lex-упорядочение с $u > v > w$, и докажите, что остаток от деления может быть записан в виде $uA(u,w) + vB(v,w) + C(w)$.
(b) Докажите, что полином $r = uA(u,w) + vB(v,w) + C(w)$ удовлетворяет равенству $r(x^2, y^2, xy) = 0$ в том и только том случае, когда $r = 0$.

14. Рассмотрим конечную матричную группу $C_4 \subset \mathrm{GL}(2,\mathbb{C})$, порожденную матрицей

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in \mathrm{GL}(2,\mathbb{C}).$$

(a) Докажите, что C_4 — циклическая группа порядка 4.
(b) Используя метод упр. 13, найдите $\mathbb{C}[x,y]^{C_4}$.
(c) Существуют ли алгебраические соотношения между инвариантами, найденными в п. (b)? Можете ли вы привести пример нарушения единственности?
(d) Используя метод упр. 13, докажите, что соотношение, найденное в п. (c), является единственным соотношением между инвариантами.

15. Пусть

$$V_4 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \subset \mathrm{GL}(2,k).$$

(a) Докажите, что V_4 является конечной матричной группой порядка 4.
(b) Найдите $k[x,y]^{V_4}$.
(c) Докажите, что каждый инвариант имеет единственное представление через образующие инварианты, найденные в п. (b).

16. В примере 3 мы рассмотрели конечную матричную группу C_4 в $\mathrm{GL}(2,k)$, порожденную матрицей

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}(2,k).$$

Попытайтесь применить методы упр. 12 и 13 и найти $k[x,y]^{C_4}$. Если вы и не сможете найти все инварианты, то постарайтесь найти инварианты небольшой полной степени. В § 3 кольцо $k[x,y]^{C_4}$ будет описано полностью.

§ 3. Образующие кольца инвариантов

В этом параграфе мы алгоритмически определим кольцо инвариантов $k[x_1,\dots,x_n]^G$ конечной матричной группы $G \subset \mathrm{GL}(n,k)$. Как и в § 2, будем считать, что поле k имеет характеристику нуль. Мы начнем со строгого определения некоторых понятий, которыми неявно пользовались в § 2.

Определение 1. Пусть $f_1,\dots,f_m \in k[x_1,\dots,x_n]$. Через $k[f_1,\dots,f_m]$ будет обозначаться подмножество в $k[x_1,\dots,x_n]$, состоящее из

всех полиномиальных выражений от $f_1,\dots,f_m$ с коэффициентами из k.

Другими словами, $f \in k[f_1,\dots,f_m]$, если f может быть представлен в виде

$$f = g(f_1,\dots,f_m),$$

где g — полином от m переменных с коэффициентами из k.

Так как множество $k[f_1,\dots,f_m]$ замкнуто относительно сложения и умножения и содержит все константы, то оно является подкольцом в $k[x_1,\dots,x_n]$. Мы будем говорить, что $k[f_1,\dots,f_m]$ *порождено полиномами* $f_1,\dots,f_m$ *над* k. Здесь следует быть внимательным: подкольцо $k[f_1,\dots,f_m]$ и идеал $\langle f_1,\dots,f_m\rangle$ оба «порождены» полиномами $f_1,\dots,f_m$, но в выражение «порождены» мы вкладываем разный смысл. В упражнениях мы рассмотрим примеры, которые помогут понять это различие.

Важным инструментом изучения колец $k[x_1,\dots,x_n]^G$ является *оператор Рейнольдса*, который определяется следующим образом.

Определение 2. Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа. Ее *оператором Рейнольдса* называется отображение $R_G : k[x_1,\dots,x_n] \to k[x_1,\dots,x_n]$, заданное формулой

$$R_G(f)(\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} f(A \cdot \mathbf{x}),$$

где $f(\mathbf{x}) \in k[x_1,\dots,x_n]$.

$R_G(f)$ является усреднением полинома f под действием группы G. Отметим, что деление на $|G|$ корректно, так как характеристика поля k равна нулю. Оператор Рейнольдса обладает следующими важными свойствами.

Предложение 3. *Пусть R_G — оператор Рейнольдса конечной матричной группы G. Тогда*

(i) *R_G является k-линейным по f;*
(ii) *если $f \in k[x_1,\dots,x_n]$, то $R_G(f) \in k[x_1,\dots,x_n]^G$;*
(iii) *если $f \in k[x_1,\dots,x_n]^G$, то $R_G(f) = f$.*

Доказательство. Доказательство п. (i) мы оставляем читателю в качестве упражнения. Докажем п. (ii). Если $B \in G$, то

$$R_G(f)(B\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} f(A \cdot B\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} f(AB \cdot \mathbf{x}). \qquad (1)$$

Пусть $G = \{A_1,\dots,A_{|G|}\}$. Тогда $A_iB \neq A_jB$ при $i \neq j$ (в противном случае достаточно умножить это равенство на B^{-1} справа и получить, что $A_i = A_j$). Таким образом, подмножество

$\{A_1B, \ldots, A_{|G|}B\} \subset G$ состоит из $|G|$ различных элементов и, следовательно, совпадает с G, т. е.

$$G = \{AB : A \in G\}.$$

Значит, в последней сумме в (1) полиномы $f(AB \cdot \mathbf{x})$ — это полиномы $f(A \cdot \mathbf{x})$, но взятые в другом порядке. Тогда

$$\frac{1}{|G|}\sum_{A\in G} f(AB\cdot \mathbf{x}) = \frac{1}{|G|}\sum_{A\in G} f(A\cdot \mathbf{x}) = R_G(f)(\mathbf{x}).$$

Отсюда следует, что $R_G(f)(B \cdot \mathbf{x}) = R_G(f)(\mathbf{x})$ для всех $B \in G$, т. е. $R_G(f) \in k[x_1, \ldots, x_n]^G$.

Докажем п. (iii). Отметим, что если $f \in k[x_1, \ldots, x_n]^G$, то

$$R_G(f)(\mathbf{x}) = \frac{1}{|G|}\sum_{A\in G} f(A\cdot \mathbf{x}) = \frac{1}{|G|}\sum_{A\in G} f(\mathbf{x}) = f(\mathbf{x}),$$

так как f — инвариант. Доказательство закончено. □

Полезным следствием этого предложения является простой метод построения инвариантов. Приведем пример.

Пример 4. Рассмотрим циклическую матричную группу $C_4 \subset \mathrm{GL}(2, k)$ порядка 4, порожденную матрицей

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

По предложению 11 из § 2

$$k[x, y]^{C_4} = \{f \in k[x, y] : f(x, y) = f(-y, x)\}.$$

Легко проверить, что оператор Рейнольдса группы C_4 задается следующей формулой:

$$R_{C_4}(f)(x, y) = \frac{1}{4}(f(x, y) + f(-y, x) + f(-x, -y) + f(y, -x))$$

(см. упр. 3). Применяя предложение 3, легко построить следующие инварианты:

$$R_{C_4}(x^2) = \frac{1}{4}(x^2 + (-y)^2 + (-x)^2 + y^2) = \frac{1}{2}(x^2 + y^2),$$

$$R_{C_4}(xy) = \frac{1}{4}(xy + (-y)x + (-x)(-y) + y(-x)) = 0,$$

$$R_{C_4}(x^3y) = \frac{1}{4}(x^3y + (-y)^3x + (-x)^3(-y) + y^3(-x)) = \frac{1}{2}(x^3y - xy^3),$$

$$R_{C_4}(x^2y^2) = \frac{1}{4}(x^2y^2 + (-y)^2x^2 + (-x)^2(-y)^2 + y^2(-x)^2) = x^2y^2.$$

Таким образом, $x^2 + y^2, x^3y - xy^3, x^2y^2 \in k[x, y]^{C_4}$. Мы увидим, что эти инварианты порождают кольцо $k[x, y]^{C_4}$.

Легко доказать, что образ любого монома x^α при действии оператора Рейнольдса является однородным инвариантом $R_G(x^\alpha)$ полной степени $|\alpha|$ (если он не равен нулю). Следующая замечательная теорема, принадлежащая Эмми Нётер, утверждает, что с помощью оператора Рейнольдса мы всегда можем построить конечное число инвариантов, порождающих кольцо $k[x_1, \ldots, x_n]^G$.

Теорема 5. *Пусть $G \subset \mathrm{GL}(n, k)$ — конечная матричная группа. Тогда*

$$k[x_1, \ldots, x_n]^G = k[R_G(x^\beta) : |\beta| \le |G|].$$

В частности, кольцо $k[x_1, \ldots, x_n]^G$ порождено конечным числом однородных инвариантов.

Доказательство. Пусть $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]^G$. Тогда из предложения 3 вытекает, что

$$f = R_G(f) = R_G\left(\sum_\alpha c_\alpha x^\alpha\right) = \sum_\alpha c_\alpha R_G(x^\alpha).$$

Следовательно, любой инвариант является линейной комбинацией (над k) инвариантов вида $R_G(x^\alpha)$. Таким образом, достаточно доказать, что инвариант $R_G(x^\alpha)$ для любого α является полиномом от инвариантов $R_G(x^\beta), |\beta| \le |G|$.

Замечательная идея Нётер состоит в том, что нужно зафиксировать целое m и объединить *все* инварианты $R_G(x^\alpha)$ полной степени m в сумму степеней (как в § 1). Затем, используя теорию симметрических функций, эту сумму можно представить как полином от конечного числа сумм степеней.

На первом шаге выражение $(x_1 + \ldots + x_n)^m$ мы записываем (раскрывая скобки) в виде суммы мономов $x^\alpha, |\alpha| = m$:

$$(x_1 + \ldots + x_n)^m = \sum_{|\alpha|=m} a_\alpha x^\alpha. \tag{2}$$

В упр. 4 будет доказано, что коэффициенты a_α являются положительными целыми числами.

Введем некоторые обозначения. Если $A = (a_{ij}) \in G$, то через A_i мы будем обозначать i-ую строку матрицы A. Таким образом, $A_i \cdot \mathbf{x} = a_{i1}x_1 + \ldots + a_{in}x_n$. Пусть $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\ge 0}$. Положим

$$(A \cdot \mathbf{x})^\alpha = (A_1 \cdot \mathbf{x})^{\alpha_1} \ldots (A_n \cdot \mathbf{x})^{\alpha_n}.$$

В этих обозначениях

$$R_G(x^\alpha) = \frac{1}{|G|}\sum_{A\in G} (A\cdot \mathbf{x})^\alpha.$$

Введем новые переменные $u_1, \ldots, u_n$ и подставим выражения $u_i A_i \cdot \mathbf{x}$ вместо x_i в (2). В результате получим тождество

$$(u_1 A_1 \cdot \mathbf{x} + \ldots + u_n A_n \cdot \mathbf{x})^m = \sum_{|\alpha|=m} a_\alpha (A \cdot \mathbf{x})^\alpha u^\alpha.$$

Суммируя по всем $A \in G$, получаем

$$S_m = \sum_{A \in G} (u_1 A_1 \cdot \mathbf{x} + \ldots + u_n A_n \cdot \mathbf{x})^m = \sum_{|\alpha|=m} a_\alpha \left(\sum_{A \in G} (A \cdot \mathbf{x})^\alpha \right) u^\alpha = \sum_{|\alpha|=m} b_\alpha R_G(x^\alpha) u^\alpha, \tag{3}$$

где $b_\alpha = |G| a_\alpha$. Заметим, что в сумме в правой части равенства содержатся *все* $R_G(x^\alpha), |\alpha| = m$. Именно поэтому мы и используем переменные $u_1, \ldots, u_n$: они не дают сократиться подобным членам.

Левая часть равенства (3) — это сумма m-х степеней выражений

$$U_A = u_1 A_1 \cdot \mathbf{x} + \ldots + u_n A_n \cdot \mathbf{x},$$

индексированных элементами $A \in G$. Запишем это так: $S_m = S_m(U_A : A \in G)$. По теореме 8 из § 1 каждая симметрическая функция от $|G|$ выражений U_A является полиномом от $S_1, \ldots, S_{|G|}$. Так как S_m — симметрическая функция от U_A, то

$$S_m = F(S_1, \ldots, S_{|G|})$$

для некоторого полинома F с коэффициентами из k. Подставляя это в (3), получаем

$$\sum_{|\alpha|=m} b_\alpha R_G(x^\alpha) u^\alpha = F\left(\sum_{|\beta|=1} b_\beta R_G(x^\beta) u^\beta, \ldots, \sum_{|\beta|=|G|} b_\beta R_G(x^\beta) u^\beta \right).$$

Раскрывая скобки в правой части и приравнивая коэффициенты при u^α, получаем

$$b_\alpha R_G(x^\alpha) = \text{полином от } R_G(x^\beta), \quad |\beta| \le |G|.$$

Так как характеристика поля равна нулю, то коэффициент $b_\alpha = |G| a_\alpha$ не равен нулю в k; следовательно, $R_G(x^\alpha)$ имеет требуемое представление. □

Эта теорема решает задачу о *конечной порожденности*, которая была сформулирована в конце § 2. В упражнениях будет рассмотрено другое доказательство этой теоремы, опирающееся на теорему Гильберта о базисе.

Силу этой теоремы легко увидеть на примерах.

Пример 6. Вернемся к рассмотрению циклической группы $C_4 \subset \mathrm{GL}(2, k)$ порядка 4 из примера 4. Чтобы найти кольцо инвариантов, нам нужно найти все полиномы $R_{C_4}(x^i y^j), i + j \le 4$. Результаты вычислений сведены в следующей таблице:

$x^i y^j$	$R_{C_4}(x^i y^j)$	$x^i y^j$	$R_{C_4}(x^i y^j)$
x	0	xy^2	0
y	0	y^3	0
x^2	$(x^2+y^2)/2$	x^4	$(x^4+y^4)/2$
xy	0	x^3y	$(x^3y-xy^3)/2$
y^2	$(x^2+y^2)/2$	x^2y^2	x^2y^2
x^3	0	xy^3	$-(x^3y-xy^3)/2$
x^2y	0	y^4	$(x^4+y^4)/2$

Из теоремы 5 следует, что кольцо $k[x,y]^{C_4}$ порождено четырьмя инвариантами $x^2+y^2, x^4+y^4, x^3y-xy^3$ и x^2y^2. Легко видеть, что инвариант x^4+y^4 «лишний», он выражается через остальные:

$$x^4 + y^4 = (x^2+y^2)^2 - 2x^2y^2.$$

Таким образом,

$$k[x,y]^{C_4} = k[x^2+y^2, x^3y-xy^3, x^2y^2].$$

Главный недостаток теоремы 5 состоит в том, что если $|G|$ велико, то необходимо вычислить оператор Рейнольдса от *очень большого* числа мономов. Рассмотрим, например, циклическую группу $C_8 \subset \mathrm{GL}(2, \mathbb{R})$ порядка 8, порожденную вращением на угол 45°

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R}).$$

Тогда в теореме 5 утверждается, что кольцо $k[x,y]^{C_8}$ порождено 44 инвариантами $R_{C_8}(x^i y^j), i + j \le 8$. В действительности только 3 инварианта порождают все кольцо. Для больших матричных групп в многомерных пространствах ситуация может быть еще хуже. В упр. 10 рассмотрены некоторые примеры.

К счастью, существуют более эффективные методы вычисления порождающих инвариантов. Основой этих методов является *теорема Молина*, позволяющая предсказывать количество линейно независимых однородных инвариантов данной полной степени. Эта теорема изложена в гл. 7 книги BENSON, GROVE (1985) и в гл. 2 книги STURMFELS (1993). В последней книге рассмотрен также эффективный алгоритм вычисления порождающих инвариантов в кольце $k[x_1, \ldots, x_n]^G$, основанный на теореме Молина.

Если нам известно, что $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, то возникает вопрос, существует ли алгоритм, позволяющий для данного инварианта $f \in k[x_1,\dots,x_n]^G$ найти его представление через $f_1,\dots,f_m$. Легко проверить, например, что полином

$$f(x,y) = x^8 + 2x^6y^2 - x^5y^3 + 2x^4y^4 + x^3y^5 + 2x^2y^6 + y^8 \qquad (4)$$

удовлетворяет условию $f(x,y) = f(-y,x)$ и, следовательно, является инвариантом группы C_4 из примера 4. Из примера 6 следует, что $f \in k[x,y]^{C_4} = k[x^2+y^2, x^3y - xy^3, x^2y^2]$. Но как выразить f через эти три образующие? Для этого можно использовать метод, аналогичный тому, который мы использовали в предложении 4 из § 1.

Мы докажем даже более общий результат: $f_1,\dots,f_m$ будут *произвольными* полиномами из $k[x_1,\dots,x_n]$. В следующем предложении описан алгоритм, позволяющий проверить принадлежность данного полинома кольцу $k[f_1,\dots,f_m]$ и позволяющий найти его представление через $f_1,\dots,f_m$, если принадлежность доказана.

Предложение 7. *Пусть даны полиномы $f_1,\dots,f_m \in k[x_1,\dots,x_n]$. Рассмотрим мономиальное упорядочение в $k[x_1,\dots,x_n,y_1,\dots,y_m]$, такое, что любой моном, содержащий хотя бы одну из переменных x_i, больше всех мономов из $k[y_1,\dots,y_m]$. Пусть G — базис Грёбнера идеала*

$$\langle f_1 - y_1,\dots,f_m - y_m\rangle \subset k[x_1,\dots,x_n,y_1,\dots,y_m].$$

Рассмотрим полином $f \in k[x_1,\dots,x_n]$, и пусть $g = \bar{f}^G$ — его остаток от деления на G. Тогда

(i) *$f \in k[f_1,\dots,f_m]$ в том и только том случае, когда $g \in k[y_1,\dots,y_m]$;*
(ii) *если $f \in k[f_1,\dots,f_m]$, то $f = g(f_1,\dots,f_m)$.*

Доказательство. Доказательство аналогично доказательству предложения 4 из § 1 (с одним интересным отличием). Разделив f на $G = \{g_1,\dots,g_t\}$, мы получим равенство вида

$$f = A_1g_1 + \dots + A_tg_t + g,$$

где $A_1,\dots,A_t, g \in k[x_1,\dots,x_n,y_1,\dots,y_m]$.

Докажем п. (i). Пусть $g \in k[y_1,\dots,y_m]$. В предыдущем равенстве заменим каждую переменную y_i на f_i. Эта подстановка не меняет f, так как f не зависит от $y_1,\dots,y_m$, но каждый полином из $\langle f_1 - y_1,\dots,f_m - y_m\rangle$ она превращает в нуль. Так как $g_1,\dots,g_t$ принадлежат этому идеалу, то $f = g(f_1,\dots,f_m)$; следовательно, $f \in k[f_1,\dots,f_m]$.

Пусть теперь $f = g(f_1,\dots,f_m)$ для некоторого $g \in k[y_1,\dots,y_m]$. Рассуждая, как в § 1, мы видим, что

$$f = C_1\cdot(f_1 - y_1) + \dots + C_n\cdot(f_m - y_m) + g(y_1,\dots,y_m) \qquad (5)$$

(см. равенство (4) из § 1). В отличие от случая симметрических полиномов g не обязательно является остатком от деления полинома f на G, и нам потребуется еще кое-какая работа с g.

Рассмотрим множество $G' = G \cap k[y_1,\dots,y_m]$, состоящее из тех элементов базиса G, которые зависят только от переменных $y_1,\dots,y_m$. Изменяя порядок элементов в G, если это необходимо, мы можем считать, что $G' = \{g_1,\dots,g_s\}, s \le t$. Поделив g на G', мы получим равенство

$$g = B_1g_1 + \dots + B_sg_s + g', \qquad (6)$$

где $B_1,\dots,B_s,\ g' \in k[y_1,\dots,y_m]$. Объединяя равенства (5) и (6), запишем f в виде (напомним, что каждый полином g_i в (6) принадлежит идеалу $\langle f_1 - y_1,\dots,f_m - y_m\rangle$)

$$f = C_1'\cdot(f_1 - y_1) + \dots + C_m'\cdot(f_m - y_m) + g'(y_1,\dots,y_m).$$

Мы утверждаем, что g' является остатком от деления полинома f на G (что и докажет, что остаток принадлежит $k[y_1,\dots,y_m]$).

Так как G является базисом Грёбнера, то, согласно предложению 1 из § 6 гл. 2, g' является остатком от деления полинома f на G в том случае, если ни один член полинома g' не делится ни на один старший член из $\mathrm{LT}(G)$. Предположим противное, и пусть существует элемент $g_i \in G$, такой, что его старший член $\mathrm{LT}(g_i)$ делит некоторый член полинома g'. Тогда $\mathrm{LT}(g_i)$ содержит только переменные $y_1,\dots,y_m$, так как $g' \in k[y_1,\dots,y_m]$. Но наше мономиальное упорядочение выбрано так, что тогда $g_i \in k[y_1,\dots,y_m]$; следовательно, $g_i \in G'$. Но так как g' является остатком от деления полинома g на G', то $\mathrm{LT}(g_i)$ не может делить ни один из членов полинома g'. Противоречие. Значит, g' и является искомым остатком.

Пункт (ii) непосредственно следует из доказательства п. (i).

В упражнениях мы, используя это предложение, найдем выражение полинома

$$f(x,y) = x^8 + 2x^6y^2 - x^5y^3 + 2x^4y^4 + x^3y^5 + 2x^2y^6 + y^8$$

из (4) в виде полинома от образующих $x^2+y^2, x^3y - xy^3, x^2y^2$ кольца $k[x,y]^{C_4}$.

Задача построения порождающих элементов кольца инвариантов (и связанная с ней задача построения соотношений между ними — см. § 4) сыграла огромную роль в развитии теории инвариантов. Первоначально изучались инварианты группы всех обрати-

мых матриц над некоторым полем. Введение в классическую теорию инвариантов имеется в книгах HILBERT (1993) и STURMFELS (1993). Читателю, желающему подробнее ознакомиться с теорией инвариантов конечных групп, мы можем рекомендовать книги BENSON (1993), BENSON, GROVE (1985), SMITH (1995) и STURMFELS (1993)[1].

Упражнения к § 3

1. С помощью полиномов $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ можно «породить» два объекта:
   - Идеал $\langle f_1, \dots, f_m \rangle \subset k[x_1, \dots, x_n]$, порожденный полиномами $f_1, \dots, f_m$. Этот идеал состоит из всех полиномов вида $\sum_{i=1}^m h_i f_i$, где $h_1, \dots, h_m \in k[x_1, \dots, x_n]$.
   - Подкольцо $k[f_1, \dots, f_m] \subset k[x_1, \dots, x_n]$, порожденное полиномами $f_1, \dots, f_m$ над k. Оно состоит из всех полиномов вида $g(f_1, \dots, f_m)$, где g — полином от m переменных с коэффициентами из k.

   Чтобы продемонстрировать различие между этими двумя объектами, рассмотрим простой пример, где $f_1 = x^2 \in k[x]$.
   (a) Объясните, почему $1 \in k[x^2]$, но $1 \notin \langle x^2 \rangle$.
   (b) Объясните, почему $x^3 \notin k[x^2]$, но $x^3 \in \langle x^2 \rangle$.
2. Пусть G — конечная матричная группа в $\mathrm{GL}(n, k)$. Докажите, что оператор Рейнольдса R_G обладает следующими свойствами:
   (a) если $a, b \in k$ и $f, g \in k[x_1, \dots, x_n]$, то $R_G(af+bg) = aR_G(f)+bR_G(g)$;
   (b) R_G отображает $k[x_1, \dots, x_n]$ на все $k[x_1, \dots, x_n]^G$;
   (c) $R_G \circ R_G = R_G$;
   (d) если $f \in k[x_1, \dots, x_n]^G$ и $g \in k[x_1, \dots, x_n]$, то $R_G(fg) = f \cdot R_G(g)$.
3. В этом упражнении мы рассмотрим циклическую группу $C_4 \subset \mathrm{GL}(2, k)$ из примера 4.
   (a) Докажите, что оператор Рейнольдса для C_4 задается следующей формулой:
   $$R_{C_4}(f)(x, y) = \frac{1}{4}\left(f(x, y) + f(-y, x) + f(-x, -y) + f(y, -x)\right).$$
   (b) Найдите $R_{C_4}(x^i y^j)$ для $i + j \leq 4$. Некоторые из необходимых вычислений проделаны в примере 4. Сравните ваши результаты с таблицей из примера 6.

[1] См. также: Гильберт Д. Избранные труды, т. I.— М.: Факториал, 1998, с. 13–114; Вейль Г., Классические группы, их инварианты и представления.— М.: ИЛ, 1947; Дьедонне Ж., Керрол Дж., Мамфорд Д. Геометрическая теория инвариантов.— М.: Мир, 1974; Спрингер Т. Теория инвариантов.— М.: Мир, 1981; Крафт Х. Геометрические методы в теории инвариантов.— М.: Мир, 1987; Винберг Э. Б., Попов В. Л. Теория инвариантов.— Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 55, М.: ВИНИТИ, 1989, с. 137–314.— *Прим. ред.*

4. В этом упражнении мы рассмотрим тождество (2) из доказательства теоремы 5. Мы будем работать с *мультиномиальными коэффициентами*, которые сейчас определим. Пусть $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ и $|\alpha| = l$. Положим
   $$\binom{l}{\alpha} = \frac{l!}{\alpha_1!\alpha_2! \dots \alpha_n!}.$$
   (a) Докажите, что $\binom{l}{\alpha}$ — целое число. Указание: используйте индукцию по n и обратите внимание на то, что если $n = 2$, то $\binom{l}{\alpha}$ — биномиальный коэффициент.
   (b) Докажите, что
   $$(x_1 + \dots + x_n)^l = \sum_{|\alpha|=l} \binom{l}{\alpha} x^\alpha.$$
   В частности, коэффициенты a_α в (2) являются положительными целыми числами $\binom{l}{\alpha}$. Указание: используйте индукцию по n и обратите внимание на то, что при $n = 2$ это утверждение является обычной формулой бинома.
5. Пусть $G \subset \mathrm{GL}(n, k)$ — конечная матричная группа. В этом упражнении мы рассмотрим принадлежащее Гильберту доказательство конечной порожденности кольца $k[x_1, \dots, x_n]^G$. Пусть $I \subset k[x_1, \dots, x_n]$ — *идеал*, порожденный однородными инвариантами положительной полной степени.
   (a) Докажите, что существует конечное множество однородных инвариантов $f_1, \dots, f_m$, таких, что $I = \langle f_1, \dots, f_m \rangle$. Стратегия Гильберта состоит в доказательстве равенства $k[x_1, \dots, x_m]^G = k[f_1, \dots, f_m]$. Включение $k[f_1, \dots, f_m] \subset k[x_1, \dots, x_n]^G$ очевидно. Поэтому нам нужно привести к противоречию предположение о том, что $k[x_1, \dots, x_n]^G \not\subset k[f_1, \dots, f_m]$.
   (b) Докажите, что если $k[x_1, \dots, x_n]^G \not\subset k[f_1, \dots, f_m]$, то существует однородный инвариант f положительной степени, не принадлежащий $k[f_1, \dots, f_m]$.
   (c) Выберем инвариант f, как в п. (b), но *минимальной* полной степени l. По определению $f \in I$; следовательно, $f = \sum_{i=1}^m h_i f_i$, где $h_1, \dots, h_m \in k[x_1, \dots, x_n]$. Докажите, что мы можем считать каждое слагаемое $h_i f_i$ либо равным нулю, либо однородным полной степени l.
   (d) Докажите, что $f = \sum_{i=1}^m R_G(h_i) f_i$. Указание: используйте предложение 3 и упр. 2. Докажите также, что для каждого i полином $R_G(h_i) f_i$ или равен нулю, или однороден полной степени l.
   (e) Так как полиномы f_i имеют положительную полную степень, то, следовательно, $R_G(h_i)$ являются однородными инвариантами полной степени $< l$ (докажите это). Из минимальности l следует,

что $R_G(h_i) \in k[f_1, \ldots, f_m]$ для всех i. Докажите, что это противоречит предположению $f \notin k[f_1, \ldots, f_m]$.

Это доказательство является изящным следствием теоремы Гильберта о базисе. К сожалению, оно ничего не говорит нам о том, как искать образующие — оно совершенно неконструктивно. В этом отношении гораздо полезнее теорема Нётер.

6. Рассмотрим две конечные матричные группы G и H, такие, что $G \subset H \subset \mathrm{GL}(n,k)$. Докажите, что $k[x_1, \ldots, x_n]^H \subset k[x_1, \ldots, x_n]^G$.

7. Пусть дана матрица
$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}(2,k).$$
   (a) Докажите, что A порождает циклическую группу C_3 порядка 3.
   (b) Используя теорему 5, найдите конечное множество однородных инвариантов, порождающих $k[x,y]^{C_3}$.
   (c) Можно ли уменьшить множество образующих? Указание: если $f_1, \ldots, f_m$ — инварианты, то, воспользовавшись предложением 7, можно определить, принадлежит ли f_1 кольцу $k[f_2, \ldots, f_m]$.

8. Пусть A — матрица из упр. 7.
   (a) Докажите, что $-A$ порождает циклическую матричную группу C_6 порядка 6.
   (b) Докажите, что $-I_2 \in C_6$. Теперь, используя упр. 6 и результаты § 2, докажите, что $k[x,y]^{C_6} \subset k[x^2, y^2, xy]$. Выведите отсюда, что ненулевые однородные инварианты группы C_6 имеют четную полную степень.
   (c) Используя п. (b) и теорему 5, найдите кольцо $k[x,y]^{C_6}$. Указание: для этого надо вычислить очень много значений оператора Рейнольдса; воспользуйтесь системой компьютерной алгебры и напишите процедуру, вычисляющую $R_{C_6}(x^i y^j)$ по заданной паре i, j.

9. Рассмотрим матрицу
$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2,k).$$
   (a) Докажите, что A порождает циклическую матричную группу $C_8 \subset \mathrm{GL}(2,k)$ порядка 8.
   (b) Докажите геометрически, что $x^2 + y^2 \in k[x,y]^{C_8}$. Указание: A — это матрица оператора вращения.
   (c) Как и в упр. 8, докажите, что однородные инварианты C_8 имеют четную полную степень.
   (d) Найдите $k[x,y]^{C_8}$. Указание: не приступайте к этой задаче, пока не напишете процедуру, аналогичную процедуре из п. (c) упр. 8.

10. Рассмотрим конечную матричную группу
$$G = \left\{ \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \right\} \subset \mathrm{GL}(3,k).$$
Легко видеть, что $|G| = 8$.
   (a) Если воспользоваться теоремой 5 для вычисления $k[x,y,z]^G$, то для скольких мономов надо будет вычислить оператор Рейнольдса?
   (b) Используйте метод примера 12 из § 2 для вычисления $k[x,y,z]^G$.

11. Пусть f — полином из равенства (4).
   (a) Докажите, что $f \in k[x,y]^{C_4} = k[x^2+y^2, x^3y - xy^3, x^2y^2]$.
   (b) Используйте предложение 7 и найдите представление f в виде полинома от $x^2+y^2, x^3y - xy^3, x^2y^2$.

12. В упр. 5, 6 и 7 к § 2 мы изучали группу $G \subset \mathrm{GL}(3,\mathbb{R})$ вращений куба в $\mathbb{R}^3$ и обнаружили, что кольцо $k[x,y,z]^G$ содержит следующие полиномы:
$$\begin{aligned} f_1 &= x^2 + y^2 + z^2, \\ f_2 &= (x+y+z)(x+y-z)(x-y+z)(x-y-z), \\ f_3 &= x^2y^2z^2, \\ f_4 &= xyz(x^2-y^2)(x^2-z^2)(y^2-z^2). \end{aligned}$$
   (a) Придумайте элементарное рассуждение, оперирующее степенями и доказывающее, что $f_4 \notin k[f_1, f_2, f_3]$.
   (b) Используя предложение 7, докажите, что $f_3 \notin k[f_1, f_2]$.
   (c) В упр. 6 к § 2 мы доказали, что
$$\left((x^2-y^2)(x^2-z^2)(y^2-z^2)\right)^2 \in k[x,y,z]^G.$$
Докажите, что этот полином принадлежит кольцу $k[f_1, f_2, f_3]$. Почему мы здесь можем проигнорировать f_4? Используя теорему Молина и методы книги STURMFELS (1993), можно доказать, что $k[x,y,z]^G = k[f_1, f_2, f_3, f_4]$.

§ 4. Соотношения между образующими и геометрия орбит

Пусть дана конечная матричная группа $G \subset \mathrm{GL}(n,k)$. Тогда по теореме 5 из § 3 существует конечное число однородных инвариантов $f_1, \ldots, f_m$, таких, что
$$k[x_1, \ldots, x_n]^G = k[f_1, \ldots, f_m].$$
В этом параграфе мы научимся находить *алгебраические соотношения* между $f_1, \ldots, f_m$ и увидим, что эти соотношения обладают рядом удивительных алгебраических и геометрических свойств.

Напомним сначала *задачу единственности*, сформулированную в конце § 2. Если $f \in k[x_1,\dots,x_n]^{S_n} = k[\sigma_1,\dots,\sigma_n]$ является симметрическим полиномом, то он имеет единственное представление в виде полинома от $\sigma_1,\dots,\sigma_n$. Если $G \subset \mathrm{GL}(n,k)$ — произвольная конечная матричная группа и $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, то мы можем спросить, единственно ли представление произвольного инварианта $f \subset k[x_1,\dots,x_n]^G$ в виде полинома от $f_1,\dots,f_m$.

Если $g_1, g_2 \in k[y_1,\dots,y_m]$, то

$$g_1(f_1,\dots,f_m) = g_2(f_1,\dots,f_m) \iff h(f_1,\dots,f_m) = 0,$$

где $h = g_1 - g_2$. Поэтому единственность нарушается в том и только том случае, когда существует ненулевой полином $h \in k[y_1,\dots,y_m]$, для которого $h(f_1,\dots,f_m) = 0$. Такой полином называется *нетривиальным алгебраическим соотношением* между $f_1,\dots,f_m$ [1].

Положим $F = (f_1,\dots,f_m)$. Тогда множество

$$I_F = \{h \in k[y_1,\dots,y_m] : h(f_1,\dots,f_m) = 0 \text{ в } k[x_1,\dots,x_n]\} \qquad (1)$$

содержит *все* алгебраические соотношения между $f_1,\dots,f_m$. Это множество обладает следующими свойствами.

Предложение 1. *Пусть* $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$ *и множество* $I_F \subset k[y_1,\dots,y_m]$ *определено, как в* (1). *Тогда*

(i) I_F *является простым идеалом в* $k[y_1,\dots,y_m]$;

(ii) *если* $f \in k[x_1,\dots,x_n]^G$ *и* $f = g(f_1,\dots,f_m)$ *— одно из представлений* f *в виде полинома от* $f_1,\dots,f_m$, *то все такие представления имеют вид*

$$f = g(f_1,\dots,f_m) + h(f_1,\dots,f_m),$$

где h *— произвольный полином из* I_F.

Доказательство. Доказать, что I_F является идеалом, нетрудно. Докажем его простоту. Пусть $fg \in I_F$. Мы должны доказать, что $f \in I_F$ или $g \in I_F$ (см. определение 2 из § 5 гл. 4). Но если $fg \in I_F$, то $f(f_1,\dots,f_m)g(f_1,\dots,f_m) = 0$. Произведение двух полиномов в $k[x_1,\dots,x_n]$ равно нулю только в том случае, когда один из них нулевой. Следовательно, $f(f_1,\dots,f_m) = 0$ или $g(f_1,\dots,f_m) = 0$, т. е. $f \in I_F$ или $g \in I_F$.

Доказательство п. (ii) мы оставляем читателю в качестве упражнения.

Мы будем называть I_F *идеалом соотношений* для $F = (f_1,\dots,f_m)$. Этот идеал также называется иногда *идеалом сизигий*. Рассмотрим в качестве примера группу $C_2 = \{\pm I_2\} \subset \mathrm{GL}(2,k)$.

[1] Или *сизигией*. — *Прим. ред.*

Мы знаем из § 2, что $k[x,y]^{C_2} = k[x^2,y^2,xy]$. В примере 4 будет доказано, что $I_F = \langle uv - w^2\rangle \subset k[u,v,w]$. Рассмотрим полином $x^6 + x^3y^3 \in k[x,y]^{C_2}$. Из предложения 1 следует, что все способы представить $x^6 + x^3y^3$ в виде полинома от x^2, y^2, xy даются следующей формулой:

$$(x^2)^3 + (xy)^3 + (x^2\cdot y^2 - (xy)^2)\cdot b(x^2,y^2,xy),$$

так как элементы идеала $\langle uv - w^2\rangle$ имеют вид $(uv - w^2)\cdot b(u,v,w)$.

Идеал соотношений I_F может быть использован для описания кольца инвариантов.

Предложение 2. *Пусть* $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, *и пусть* $I_F \subset k[y_1,\dots,y_m]$ *— идеал соотношений. Тогда имеет место кольцевой изоморфизм*

$$k[y_1,\dots,y_m]/I_F \cong k[x_1,\dots,x_n]^G,$$

т. е. кольцо инвариантов изоморфно факторкольцу кольца полиномов по идеалу I_F.

Доказательство. Напомним (см. § 2 гл. 5), что элементы факторкольца $k[y_1,\dots,y_m]/I_F$ обозначаются $[g]$, где $g \in k[y_1,\dots,y_m]$, причем $[g_1] = [g_2]$ в том и только том случае, когда $g_1 - g_2 \in I_F$.

Определим отображение $\phi : k[y_1,\dots,y_m]/I_F \to k[x_1,\dots,x_n]^G$ следующим образом:

$$\phi([g]) = g(f_1,\dots,f_m).$$

Доказательство корректности определения отображения ϕ и доказательство того, что ϕ — гомоморфизм колец, мы оставляем читателю в качестве упражнения. Докажем, что ϕ — биективное отображение.

Так как $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, то сюръективность ϕ очевидна. Докажем его инъективность. Предположим, что $\phi([g_1]) = \phi([g_2])$. Тогда $g_1(f_1,\dots,f_m) = g_2(f_1,\dots,f_m)$, а следовательно, $g_1 - g_2 \in I_F$, откуда $[g_1] = [g_2]$, т. е. ϕ инъективно.

Мы знаем, что ϕ — биективное отображение и гомоморфизм колец; значит, обратное отображение существует и также является гомоморфизмом колец, т. е. ϕ — кольцевой изоморфизм.

Более короткое доказательство этого утверждения использует теорему об изоморфизме (упр. 16 к § 2 гл. 5).

Для нас особенно важным является то, что идеал I_F может быть явно описан с помощью теории исключения. А именно, рассмотрим

систему

$$y_1 = f_1(x_1, \dots, x_n),$$
$$\vdots$$
$$y_m = f_m(x_1, \dots, x_n).$$

Тогда определение I_F сводится к исключению $x_1, \dots, x_n$ из этой системы. Точнее, имеет место

Предложение 3. *Пусть* $k[x_1, \dots, x_n]^G = k[f_1, \dots, f_m]$. *Рассмотрим идеал*

$$J_F = \langle f_1 - y_1, \dots, f_m - y_m \rangle \subset k[x_1, \dots, x_n, y_1, \dots, y_m].$$

(i) I_F *является* n*-м исключающим идеалом идеала* J_F, *т. е.* $I_F = J_F \cap k[y_1, \dots, y_m]$.

(ii) *Зафиксируем мономиальное упорядочение в кольце* $k[x_1, \dots, x_n, y_1, \dots, y_m]$, *такое, что моном, содержащий хотя бы одну из переменных* $x_1, \dots, x_n$, *больше любого монома из* $k[y_1, \dots, y_m]$, *и пусть* G *— базис Грёбнера идеала* J_F. *Тогда* $G \cap k[y_1, \dots, y_m]$ *является базисом Грёбнера идеала* I_F *относительно индуцированного мономиального упорядочения в* $k[y_1, \dots, y_m]$.

Доказательство. Обратите внимание, что с идеалом J_F мы уже встречались в предложении 7 из § 3. Докажем сначала следующее свойство идеала J_F: если $p \in k[x_1, \dots, x_n, y_1, \dots, y_m]$, то

$$p \in J_F \iff p(x_1, \dots, x_n, f_1, \dots, f_m) = 0 \text{ в } k[x_1, \dots, x_n]. \qquad (2)$$

Импликация в одну сторону очевидна, так как подстановка $y_i \mapsto f_i$ переводит каждый элемент из идеала $J_F = \langle f_1 - y_1, \dots, f_m - y_m \rangle$ в нуль. Пусть теперь $p \in k[x_1, \dots, x_n, y_1, \dots, y_m]$. Заменим каждую переменную y_i в p на $f_i - (f_i - y_i)$ и раскроем скобки. Тогда

$$p(x_1, \dots, x_n, y_1, \dots, y_m) = p(x_1, \dots, x_n, f_1, \dots, f_m) + B_1 \cdot (f_1 - y_1) + \dots + B_m \cdot (f_m - y_m)$$

для некоторых полиномов $B_1, \dots, B_m \in k[x_1, \dots, x_n, y_1, \dots, y_m]$ (см. упр. 4). В частности, если $p(x_1, \dots, x_n, f_1, \dots, f_m) = 0$, то

$$p(x_1, \dots, x_n, y_1, \dots, y_m) = B_1 \cdot (f_1 - y_1) + \dots + B_m \cdot (f_m - y_m) \in J_F,$$

что и завершает доказательство утверждения (2).

Теперь рассмотрим правую и левую части утверждения (2) на пересечении с $k[y_1, \dots, y_m]$. Если $p \in k[y_1, \dots, y_m]$, то это дает

$$p \in J_F \cap k[y_1, \dots, y_m] \iff p(f_1, \dots, f_m) = 0 \text{ в } k[x_1, \dots, x_n],$$

т. е. $p \in I_F$, а значит, $J_F \cap k[y_1, \dots, y_m] = I_F$ по определению идеала I_F и (i) доказано, а (ii) является непосредственным следствием теоремы 2 из § 3 гл. 3 (см. также упр. 5 к § 1 гл. 3). □

Предложение 3 дает возможность описывать соотношения между образующими.

Пример 4. В § 2 мы показали, что инварианты группы $C_2 = \{\pm I_2\} \subset \mathrm{GL}(2, k)$ образуют кольцо $k[x, y]^{C_2} = k[x^2, y^2, xy]$. Пусть $F = (x^2, y^2, xy)$, и пусть u, v, w — новые переменные. Идеал соотношений определяется исключением x, y из системы

$$u = x^2,$$
$$v = y^2,$$
$$w = xy.$$

Зададим lex-упорядочение с $x > y > u > v > w$; тогда базис Грёбнера идеала $J_F = \langle u - x^2, v - y^2, w - xy \rangle$ состоит из полиномов

$$x^2 - u, xy - w, xv - yw, xw - yu, y^2 - v, uv - w^2.$$

Таким образом, согласно предложению 3,

$$I_F = \langle uv - w^2 \rangle,$$

т. е. все соотношения между образующими x^2, y^2 и xy порождаются очевидным соотношением $x^2 \cdot y^2 = (xy)^2$. Теперь из предложения 2 следует, что кольцо инвариантов является факторкольцом кольца всех полиномов:

$$k[x, y]^{C_2} \cong k[u, v, w]/\langle uv - w^2 \rangle.$$

Пример 5. В § 3 мы рассматривали циклическую матричную группу C_4, порожденную матрицей

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

и доказали, что

$$k[x, y]^{C_4} = k[x^2 + y^2, x^3 y - x y^3, x^2 y^2].$$

Положим $F = (x^2 + y^2, x^3 y - x y^3, x^2 y^2)$. Мы оставляем читателю в качестве упражнения доказательство того, что $I_F = \langle u^2 w - v^2 - 4w^2 \rangle \subset k[u, v, w]$, т. е. существует одно нетривиальное соотношение между образующими,

$$(x^2 + y^2)^2 \cdot x^2 y^2 = (x^3 y - x y^3)^2 + 4(x^2 y^2)^2.$$

Поэтому по предложению 2

$$k[x, y]^{C_4} \cong k[u, v, w]/\langle u^2 w - v^2 - 4w^2 \rangle.$$

Предложения 1, 2, 3 и теория, развитая в § 3 гл. 5, позволяют решить *задачу единственности*, сформулированную в конце § 2.

Пусть $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, и пусть $I_F \subset k[y_1,\dots,y_m]$ — идеал соотношений. Если $I_F \neq \{0\}$, то, как мы знаем, элемент $f \in k[x_1,\dots,x_n]^G$ может быть многими способами представлен в виде полинома от $f_1,\dots,f_m$. Существует ли стандартное представление полинома f?

Для решения этой задачи зафиксируем мономиальное упорядочение на $k[y_1,\dots,y_m]$ и найдем базис Грёбнера G идеала I_F с помощью предложения 3. Если $g \in k[y_1,\dots,y_m]$, то через $\bar{g}^G$ мы будем обозначать остаток от деления полинома g на G. В гл. 5 мы показали, что остатки $\bar{g}^G$ являются однозначно определенными представителями элементов факторкольца $k[y_1,\dots,y_m]/I_F$ (предложение 1 из § 3 гл. 5). Этот факт и изоморфизм

$$k[y_1,\dots,y_m]/I_F \cong k[x_1,\dots,x_n]^G$$

из предложения 2 позволяют определить стандартное представление элементов из $k[x_1,\dots,x_n]^G$ в виде полиномов от $f_1,\dots,f_m$. Так базисы Грёбнера помогают восстановить единственность представления, нарушенную при $I_F \neq \{0\}$.

До сих пор мы рассматривали алгебраические свойства идеала I_F. Теперь перейдем к геометрии. Геометрический объект, ассоциированный с идеалом, — это многообразие.

Определение 6. Пусть $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, и пусть $I_F \subset k[y_1,\dots,y_m]$ — идеал соотношений для $F = (f_1,\dots,f_m)$. Тогда можно определить аффинное многообразие

$$V_F = \mathbf{V}(I_F) \subset k^m.$$

Многообразие V_F обладает следующими свойствами.

Предложение 7. *Пусть I_F и V_F такие же, как в определении* 6.

(i) *V_F — это наименьшее многообразие в k^m, содержащее параметризованное множество*

$$\begin{aligned} y_1 &= f_1(x_1,\dots,x_n),\\ &\vdots\\ y_m &= f_m(x_1,\dots,x_n). \end{aligned}$$

(ii) *$I_F = \mathbf{I}(V_F)$, так что I_F — идеал полиномов, обращающихся в нуль на V_F.*

(iii) *V_F — неприводимое многообразие.*

(iv) *Пусть $k[V_F]$ — координатное кольцо многообразия V_F (см. § 4 гл. 5). Тогда*

$$k[V_F] \cong k[x_1,\dots,x_n]^G.$$

Доказательство. По предложению 3 I_F является n-м исключающим идеалом идеала $J_F = \langle f_1 - y_1,\dots,f_m - y_m\rangle$. Пункт (i) является прямым следствием теоремы о полиномиальном неявном представлении (теорема 1 из § 3 гл. 3).

Докажем (ii). Включение $I_F \subset \mathbf{I}(\mathbf{V}(I_F)) = \mathbf{I}(V_F)$ всегда имеет место. Докажем обратное включение. Пусть $h \in \mathbf{I}(V_F)$. Если $(a_1,\dots,a_n) \in k^n$, то из (i) следует, что

$$(f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n)) \in V_F.$$

Так как h обращается в нуль на V_F, то

$$h(f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n)) = 0$$

для всех $(a_1,\dots,a_n) \in k^n$. Но k имеет характеристику нуль и, следовательно, бесконечно; поэтому (см. предложение 5 из § 1 гл. 1) $h(f_1,\dots,f_m) = 0$, т. е. $h \in I_F$.

Из (ii) и предложения 1 следует, что $\mathbf{I}(V_F) = I_F$ — простой идеал. Значит, многообразие V_F неприводимо (предложение 4 из § 1 гл. 5). (Мы также можем использовать наличие параметризации и предложение 5 из § 5 гл. 5, чтобы получить второе доказательство неприводимости многообразия V_F.)

Наконец, в гл. 5 было показано, что координатное кольцо $k[V_F]$ изоморфно факторкольцу кольца $k[y_1,\dots,y_m]$

$$k[V_F] \cong k[y_1,\dots,y_m]/\mathbf{I}(V_F)$$

(теорема 7 из § 2 гл. 5). Так как $\mathbf{I}(V_F) = I_F$ по п. (ii), то (см. предложение 2)

$$k[V_F] \cong k[y_1,\dots,y_m]/I_F \cong k[x_1,\dots,x_n]^G. \tag{3}$$

Предложение доказано. □

Обратите внимание, как изоморфизмы в (3) объединяют три метода образования новых колец: построение координатного кольца, переход к факторкольцу и построение кольца инвариантов.

В равенстве $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$ полиномы $f_1,\dots,f_m$ однозначно не определены. Возникает естественный вопрос: как меняется многообразие V_F при переходе к другому множеству образующих?

Следствие 8. *Пусть $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m] = k[f'_1,\dots,f'_{m'}]$. Положим $F = (f_1,\dots,f_m)$ и $F' = (f'_1,\dots,f'_{m'})$. Тогда многообразия $V_F \subset k^m$ и $V_{F'} \subset k^{m'}$ изоморфны (в смысле определения из* § 4 *гл.* 5).

Доказательство. Из предложения 7 следует, что $k[V_F] \cong k[x_1,\dots,x_n]^G \cong k[V_{F'}]$. Легко видеть, что эти изоморфизмы тождественны на константах. Но тогда по теореме 9 из § 4 гл. 5 многообразия V_F и $V_{F'}$ также изоморфны. □

Из гл. 4 мы вынесли важный опыт: алгебро-геометрическое соответствие лучше всего работает над алгебраически замкнутыми полями. Поэтому до конца этого параграфа мы будем предполагать поле k алгебраически замкнутым.

Чтобы понять геометрию многообразия V_F, нам нужно рассмотреть группу $G \subset \mathrm{GL}(n,k)$ с геометрической точки зрения. Пока что мы изучали только ее действие на полиномы: если $f(\mathbf{x}) \in k[x_1,\dots,x_n]$, то с помощью матрицы $A \in G$ мы строили новый полином $g(\mathbf{x}) = f(A\cdot\mathbf{x})$. Но G также действует и на векторы из пространства k^n. Точку $(a_1,\dots,a_n) \in k^n$ мы будем записывать в виде вектора-столбца

$$\mathbf{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Тогда умножение на матрицу $A \in G$ вектор-столбца $\mathbf{a}$ дает нам новую точку $A\cdot\mathbf{a}$ в k^n.

Группа G определяет на k^n следующее отношение эквивалентности: векторы $\mathbf{a}$ и $\mathbf{b}$ из k^n эквивалентны, $\mathbf{a} \sim_G \mathbf{b}$, если $\mathbf{b} = A\cdot\mathbf{a}$ для некоторой матрицы $A \in G$. Проверку того, что $\sim_G$ в самом деле является отношением эквивалентности, мы оставляем читателю в качестве упражнения. Также легко доказать, что класс эквивалентности вектора $\mathbf{a} \in k^n$ — это множество

$$\{\mathbf{b} \in k^n : \mathbf{b} \sim_G \mathbf{a}\} = \{A\cdot\mathbf{a} : A \in G\}.$$

Подобные классы эквивалентности имеют специальное название.

Определение 9. Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа и $\mathbf{a} \in k^n$. Тогда *G-орбитой* вектора $\mathbf{a}$ называется множество

$$G\cdot\mathbf{a} = \{A\cdot\mathbf{a} : A \in G\}.$$

Множество всех G-орбит в k^n обозначается через k^n/G и называется *пространством орбит.*

Отметим, что орбита $G\cdot\mathbf{a}$ содержит не более $|G|$ точек. В упражнениях мы докажем, что число точек в орбите всегда является делителем числа $|G|$.

Так как орбиты — это классы эквивалентности, то пространство орбит — это множество классов эквивалентности по отношению $\sim_G$. Мы определили k^n/G как множество, но нас интересуют главным образом аффинные многообразия. Поэтому естественно спросить: можно ли задать на k^n/G структуру аффинного многообразия?

Теорема 10. *Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа и поле k алгебраически замкнуто. Пусть $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$.*

(i) *Полиномиальное отображение $F : k^n \to V_F, F(\mathbf{a}) = (f_1(\mathbf{a}),\dots,f_m(\mathbf{a}))$ сюръективно. Геометрически это означает, что при параметризации $y_i = f_i(x_1,\dots,x_n)$ каждая точка из V_F является параметризованной.*

(ii) *Отображение, сопоставляющее G-орбите $G\cdot\mathbf{a}$ точку $F(\mathbf{a}) \in V_F$, индуцирует взаимно однозначное соответствие*

$$k^n/G \cong V_F.$$

Доказательство. Пункт (i) мы докажем с помощью теории исключения. Рассмотрим идеал $J_F = \langle f_1 - y_1,\dots,f_m - y_m\rangle$, определенный в предложении 3. Так как $I_F = J_F \cap k[y_1,\dots,y_m]$ является исключающим идеалом для J_F, то точка $(b_1,\dots,b_m) \in V_F = \mathbf{V}(I_F)$ — это частичное решение системы уравнений

$$\begin{aligned} y_1 &= f_1(x_1,\dots,x_n), \\ &\vdots \\ y_m &= f_m(x_1,\dots,x_n). \end{aligned}$$

Если мы докажем, что решение $(b_1,\dots,b_m) \in \mathbf{V}(I_F)$ продолжается до полного решения $(a_1,\dots,a_n,b_1,\dots,b_m) \in \mathbf{V}(J_F)$, то $F(a_1,\dots,a_n) = (b_1,\dots,b_m)$ и сюръективность отображения $F : k^n \to V_F$ будет доказана.

Мы утверждаем, что для каждого i существует полином $p_i \in J_F \cap k[x_i,\dots,x_n,y_1,\dots,y_m]$, такой, что

$$p_i = x_i^N + \text{ члены, содержащие } x_i \text{ в степенях } < N, \tag{4}$$

где $N = |G|$. Доказательство этого утверждения мы дадим чуть позже, а пока будем считать его доказанным.

Предположим, что существует продолжение частичного решения $(b_1,\dots,b_m)$ до частичного решения

$$(a_{i+1},\dots,a_n,b_1,\dots,b_m) \in \mathbf{V}(J_F) \cap k[x_{i+1},\dots,x_n,y_1,\dots,y_m].$$

Так как k алгебраически замкнуто, то по теореме о продолжении из § 1 гл. 3 мы можем продолжить это частичное решение до $(a_i,a_{i+1},\dots,a_n,b_1,\dots,b_m)$, если старший коэффициент при x_i у одного из порождающих элементов идеала $J_F \cap k[x_i,\dots,x_n,y_1,\dots,y_m]$ не обращается в нуль на этом частичном решении. По нашему предположению идеал содержит элемент p_i с таким свойством (его старший коэффициент — 1), и мы можем считать p_i образующим (просто добавим его к множеству порождающих элементов). Таким образом, требуемое продолжение существует (см. следствие 4 из § 1 гл. 3).

Теперь нужно доказать существование таких p_i. Нам понадобится следующая лемма.

Лемма 11. *Пусть $G \subset \mathrm{GL}(n,k)$ — конечная матричная группа, $|G| = N$ и $f \in k[x_1,\dots,x_n]$. Тогда найдутся инварианты $g_1,\dots,g_N \in k[x_1,\dots,x_n]^G$, такие, что*

$$f^N + g_1 f^{N-1} + \dots + g_N = 0.$$

Доказательство леммы. Рассмотрим полином $\prod_{A\in G}(X - f(A\cdot\mathbf{x}))$. Раскрывая скобки, получим

$$\prod_{A\in G}(X - f(A\cdot\mathbf{x})) = X^N + g_1(\mathbf{x})X^{N-1} + \dots + g_N(\mathbf{x}),$$

где коэффициенты $g_1,\dots,g_N$ принадлежат $k[x_1,\dots,x_n]$. Мы утверждаем, что $g_1,\dots,g_N$ являются инвариантами группы G. Чтобы доказать это, предположим, что $B \in G$. В доказательстве предложения 3 из § 3 мы показали, что множество полиномов $f(AB\cdot\mathbf{x})$ совпадает с множеством полиномов $f(A\cdot\mathbf{x})$. Таким образом,

$$\prod_{A\in G}(X - f(AB\cdot\mathbf{x})) = \prod_{A\in G}(X - f(A\cdot\mathbf{x})).$$

Раскрывая скобки в этом равенстве, получим, что

$$x^N + g_1(B\cdot\mathbf{x})X^{N-1} + \dots + g_N(B\cdot\mathbf{x}) = X^N + g_1(\mathbf{x})X^{N-1} + \dots + g_N(\mathbf{x})$$

для любого $B \in G$. Это и доказывает инвариантность полиномов $g_1,\dots,g_N$.

Одним из сомножителей в этом произведении является $X - f(I_n\cdot\mathbf{x}) = X - f(\mathbf{x})$. Значит, при $X = f(\mathbf{x})$ произведение равно нулю и $f^N + g_1 f^{N-1} + \dots + g_N = 0$. □

Теперь мы можем доказать утверждение о полиноме p_i. Положим в лемме 11 $f = x_i$. Тогда

$$x_i^N + g_1 x_i^{N-1} + \dots + g_N = 0, \qquad (5)$$

где $N = |G|$ и $g_1,\dots,g_N \in k[x_1,\dots,x_n]^G$. Так как $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$, то $g_j = h_j(f_1,\dots,f_m), j = 1,\dots N$. Пусть

$$p_i(x_i,y_1,\dots,y_m) = x_i^N + h_1(y_1,\dots,y_m)x_i^{N-1} + \dots + h_N(y_1,\dots,y_m) \in k[x_i,y_1,\dots,y_m].$$

Из (5) следует, что $p_i(x_i,f_1,\dots,f_m) = 0$; следовательно, по (2) $p_i \in J_F$. Осталось заметить, что $p_i \in J_F \cap k[x_i,\dots,x_n,y_1,\dots,y_m]$.

Докажем (ii). Отображение

$$\widetilde{F} : k^n/G \longrightarrow V_F, \quad G\cdot\mathbf{a} \mapsto F(\mathbf{a}) = (f_1(\mathbf{a}),\dots,f_m(\mathbf{a})),$$

корректно определено, так как каждый полином f_i инвариантен и, следовательно, принимает одно и то же значение в каждой точке

орбиты $G\cdot\mathbf{a}$. По (i) отображение F сюръективно; значит, $\widetilde{F}$ также сюръективно.

Осталось доказать, что $\widetilde{F}$ инъективно. Пусть $G\cdot\mathbf{a}$ и $G\cdot\mathbf{b}$ — различные орбиты. Так как $\sim_G$ — отношение эквивалентности, то эти две орбиты не имеют общих точек. Построим инвариант $g \in k[x_1,\dots,x_n]^G$, такой, что $g(\mathbf{a}) \neq g(\mathbf{b})$. Чтобы сделать это, сначала отметим, что $S = G\cdot\mathbf{b} \cup G\cdot\mathbf{a} - \{\mathbf{a}\}$ — конечное множество точек в k^n и, следовательно, S является аффинным многообразием. Так как $\mathbf{a} \notin S$, то найдется полином f, равный нулю на S, но отличный от нуля в точке $\mathbf{a}$. Поэтому

$$f(A\cdot\mathbf{b}) = 0 \quad \text{и} \quad f(A\cdot\mathbf{a}) = \begin{cases} 0, & \text{если } A\cdot\mathbf{a} \neq \mathbf{a}, \\ f(\mathbf{a}) \neq 0, & \text{если } A\cdot\mathbf{a} = \mathbf{a}. \end{cases}$$

Пусть теперь $g = R_G(f)$. Мы оставляем читателю в качестве упражнения доказательство того, что

$$g(\mathbf{b}) = 0 \text{ и } g(\mathbf{a}) = \frac{M}{|G|}f(\mathbf{a}) \neq 0,$$

где M — это число элементов $A \in G$, таких, что $A\cdot\mathbf{a} = \mathbf{a}$. Таким образом, мы нашли инвариант $g \in k[x_1,\dots,x_n]^G$, такой, что $g(\mathbf{a}) \neq g(\mathbf{b})$.

Но g может быть записан в виде полинома от $f_1,\dots,f_m$. Значит, из условия $g(\mathbf{a}) \neq g(\mathbf{b})$ следует, что $f_i(\mathbf{a}) \neq f_i(\mathbf{b})$ для некоторого i, т. е. $\widetilde{F}$ имеет разные значения на орбитах $G\cdot\mathbf{a}$ и $G\cdot\mathbf{b}$. Теорема доказана. □

Теорема 10 показывает, что существует биекция *множества* k^n/G на *многообразие* V_F. Именно это мы и подразумеваем, когда говорим, что пространство орбит имеет структуру аффинного многообразия. Хотя I_F зависит от выбора образующих кольца $k[x_1,\dots,x_n]^G$, но многообразие V_F определено однозначно с точностью до изоморфизма (следствие 8). Это означает, что структура многообразия на пространстве орбит определена однозначно с точностью до изоморфизма.

Из теоремы 10 и предложения 7 вытекает такой приятный результат: «полиномиальные функции» на пространстве орбит k^n/G — это функции из координатного кольца

$$k[V_F] \cong k[x_1,\dots,x_n]^G.$$

Отметим естественность этого утверждения: инвариантный полином принимает одно и то же значение в точках G-орбиты; следовательно, он определяет функцию на пространстве орбит. Таким

образом, естественно ожидать, что $k[x_1, \ldots, x_n]^G$ является «координатным кольцом» вне зависимости от структуры многообразия на k^n/G.

Однако существование биекции $k^n/G \cong V_F$ — это удивительный факт, если взглянуть с несколько иной позиции. Предположим, что мы начали с геометрического действия группы G на k^n: $\mathbf{a} \mapsto A \cdot \mathbf{a}, A \in G$. Затем мы строим пространство орбит k^n/G (как множество). Чтобы задать на нем структуру аффинного многообразия, мы сделали следующие вещи:

- придали этому действию алгебраическую форму, определив действие группы G на полиномах;
- определили инвариантные полиномы и доказали конечную порожденность кольца инвариантов;
- построили идеал соотношений между образующими.

Уравнения, получающиеся из этого идеала, и задают требуемую структуру V_F на k^n/G.

В общем случае задание структуры аффинного (или проективного — см. гл. 8) многообразия на каком-либо множестве интересующих нас объектов (G-орбит, касательных и пр.) является важной задачей алгебраической геометрии. Некоторые примеры будут рассмотрены в упражнениях.

Упражнения к § 4

1. Пусть $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ и $I = \{g \in k[y_1, \ldots, y_m] : g(f_1, \ldots, f_m) = 0\}$.
   (a) Докажите, что I является идеалом в $k[y_1, \ldots, y_m]$.
   (b) Пусть $f = k[f_1, \ldots, f_m]$ и $f = g(f_1, \ldots, f_m)$ — представление f в виде полинома от $f_1, \ldots, f_m$. Докажите, что все такие представления задаются формулой $f = g(f_1, \ldots, f_m) + h(f_1, \ldots, f_m)$, где $h \in I$.

2. Пусть $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ и $I \subset k[y_1, \ldots, y_m]$ — идеал соотношений, определенный в упр. 1.
   (a) Докажите, что отображение, переводящее $[g]$ в $g(f_1, \ldots, f_m)$, корректно определено и является гомоморфизмом колец
   $$\phi : k[y_1, \ldots, y_m]/I \longrightarrow k[f_1, \ldots, f_m].$$
   (b) Докажите, что ϕ — взаимно однозначное отображение «на», т. е. ϕ — изоморфизм колец.
   (c) Используя упр. 13 к § 2 гл. 5, дайте другое доказательство изоморфности колец $k[y_1, \ldots, y_m]/I$ и $k[f_1, \ldots, f_m]$. Указание: рассмотрите гомоморфизм $\Phi : k[y_1, \ldots, y_m] \to k[f_1, \ldots, f_m]$, $\Phi(y_i) = f_i$.

3. Хотя в предложениях 1 и 2 речь идет о кольце $k[x_1, \ldots, x_n]^G$, из упр. 1 и 2 следует, что эти результаты справедливы для любого подкольца вида $k[f_1, \ldots, f_m] \subset k[x_1, \ldots, x_n]$. Обобщите аналогичным образом предложение 3. Нужны ли для этого изменения в его доказательстве?

4. Пусть $p \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Докажите, что
   $$\begin{aligned} p(x_1, \ldots, x_n, y_1, \ldots, y_m) = & p(x_1, \ldots, x_n, f_1, \ldots, f_m) \\ & + B_1 \cdot (f_1 - y_1) + \ldots + B_m \cdot (f_m - y_m), \end{aligned}$$
   где $B_1, \ldots, B_m \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Указание: в p замените каждую переменную y_i на $f_i - (f_i - y_i)$. Доказательство аналогично доказательству равенства (4) в § 1.

5. Завершите рассмотрение примера 5, доказав, что идеал $I_F \subset k[u, v, w]$ задается формулой $I_F = \langle u^2 w - v^2 - 4w^2 \rangle$ (здесь $F = (x^2 + y^2, x^3 y - xy^3, x^2 y^2)$).

6. В упр. 7 к § 3 мы искали инварианты циклической группы $C_3 \subset \mathrm{GL}(2, k)$ порядка 3. Укажите соотношения между найденными вами образующими кольца $k[x, y]^{C_3}$.

7. Сделайте то же самое для циклической группы $C_6 \subset \mathrm{GL}(2, k)$ порядка 6, рассмотренной в упр. 8 к § 3.

8. В упр. 12 к § 3 мы нашли четыре инварианта f_1, f_2, f_3, f_4 группы вращений куба в $\mathbb{R}^3$.
   (a) С помощью полинома $(f_4/xyz)^2$ и п. (c) упр. 12 к § 3 найдите алгебраическое соотношение между f_1, f_2, f_3, f_4.
   (b) Докажите, что между f_1, f_2, f_3 нет нетривиальных алгебраических соотношений.
   (c) Докажите, что соотношение из п. (a) порождает идеал всех соотношений между f_1, f_2, f_3, f_4. Указание: это большая задача, вашему компьютеру может не хватить памяти, а вам — времени.

9. Пусть $G \subset \mathrm{GL}(n, k)$ — конечная матричная группа. Мы определили отношение $\sim_G$ на k^n, положив $\mathbf{a} \sim_G \mathbf{b}$, если $\mathbf{b} = A \cdot \mathbf{a}$ для некоторой матрицы $A \in G$.
   (a) Докажите, что $\sim_G$ является отношением эквивалентности.
   (b) Докажите, что классом эквивалентности вектора $\mathbf{a}$ является множество $G \cdot \mathbf{a}$, определенное в тексте параграфа.

10. Рассмотрим группу вращений куба в $\mathbb{R}^3$. Мы изучали эту группу в упр. 5 к § 2 и знаем, что она состоит из 24 элементов.
    (a) Нарисуйте куб и укажите на нем орбиты, состоящие из 1, 6, 8, 12 и 24 точек.
    (b) Докажите геометрически, что орбит из четырех точек нет.

11. (Это упражнение требует знания абстрактной алгебры.) Пусть $G \subset \mathrm{GL}(n, k)$ — конечная матричная группа. В этом упражнении мы докажем, что число точек орбиты $G \cdot \mathbf{a}$ делит $|G|$.

(a) Зафиксируем $\mathbf{a} \in k^n$, и пусть $H = \{A \in G : A \cdot \mathbf{a} = \mathbf{a}\}$. Докажите, что H — подгруппа в G. Она называется *подгруппой изотропии* или *стабилизатором* вектора $\mathbf{a}$.

(b) Пусть $A \in G$. Тогда его *левым смежным классом* называется подмножество $AH = \{AB : B \in H\} \subset G$. Через G/H обозначается множество всех левых смежных классов (обратите внимание, что G/H является группой только в том случае, когда H — нормальный делитель). Докажите, что отображение $AH \mapsto A \cdot \mathbf{a}$ индуцирует биекцию $G/H \cong G \cdot \mathbf{a}$. Указание: сначала необходимо доказать, что это отображение корректно определено. Напомним, что два смежных класса AH и BH равны в том и только том случае, когда $B^{-1}A \in H$.

(c) Используя п. (b), докажите, что число точек орбиты $G \cdot \mathbf{a}$ делит $|G|$.

12. Рассмотрим две непересекающиеся орбиты $G \cdot \mathbf{a}$ и $G \cdot \mathbf{b}$ (как в доказательстве теоремы 10). Пусть $S = G \cdot \mathbf{b} \cup G \cdot \mathbf{a} - \{\mathbf{a}\}$. Найдем полином $f \in k[x_1, \dots, x_n]$, такой, что f равен нулю во всех точках множества S, но $f(\mathbf{a}) \neq 0$. Пусть $g = R_G(f)$, где R_G — оператор Рейнольдса группы G.

(a) Докажите, что $g(\mathbf{b}) = 0$.

(b) Объясните, почему $g(\mathbf{a}) = \frac{M}{|G|} f(\mathbf{a}) \neq 0$, где M — число элементов $A \in G$, таких, что $A \cdot \mathbf{a} = \mathbf{a}$.

13. В этом упражнении мы покажем, что теорема 10 может оказаться неверной, если основное поле не является алгебраически замкнутым. Рассмотрим группу матриц перестановки $S_2 \subset \mathrm{GL}(2, \mathbb{R})$.

(a) Мы знаем, что $\mathbb{R}[x, y]^{S_2} = \mathbb{R}[\sigma_1, \sigma_2]$. Докажите, что $I_F = \{0\}$ для $F = (\sigma_1, \sigma_2)$, т. е. $V_F = \mathbb{R}^2$. Таким образом, в теореме 10 в данном случае рассматривается отображение $\widetilde{F} : \mathbb{R}^2/S_2 \to \mathbb{R}^2, S_2 \cdot (x, y) \mapsto (y_1, y_2) = (x + y, xy)$.

(b) Докажите, что образом отображения $\widetilde{F}$ является множество $\{(y_1, y_2) \in \mathbb{R}^2 : y_1^2 \geq 4y_2\} \subset \mathbb{R}^2$ (т. е. область, лежащая ниже параболы $y_1^2 = 4y_2$). Указание: рассмотрите y_1 и y_2 как коэффициенты полинома $X^2 - y_1 X + y_2$. Когда этот полином имеет вещественные корни?

14. Во многих случаях в математике рассматриваются классы эквивалентности по некоторому отношению и на них задается алгебраическая структура. Покажите, что конструкция факторкольца является таким примером. Указание: см. § 2 из гл. 5.

15. В этом упражнении мы рассмотрим примеры множеств, которые при внимательном изучении оказываются многообразиями. Сначала обратим внимание на то, что множество невертикальных прямых на плоскости k^2 имеет естественную геометрическую структуру. А именно, каждая такая прямая L единственным образом задается уравнением вида $y = mx + b$, так что прямой L может быть сопоставлена точка (m, b) в другом двумерном аффинном пространстве $k^{2\vee}$. (Включение в рассмотрение вертикальных прямых требует перехода к проективному пространству, которым мы и займемся в следующей главе.)

Рассмотрим теперь кривую C на плоскости и множество прямых, касательных к C. Этому множеству сопоставляется подмножество $C^\vee \subset k^{2\vee}$. Мы найдем это множество в некоторых простых случаях и покажем, что оно является аффинным многообразием.

(a) Пусть C — парабола $y = x^2$. Покажите, что касательная в точке $(x_0, y_0) \in C$ имеет уравнение $y = 2x_0 x - x_0^2$. Покажите, что $C^\vee$ задается уравнением $m^2 + 4b = 0$ в $k^{2\vee}$.

(b) Докажите, что $C^\vee$ является аффинным многообразием, если C — кубическая кривая $y = x^3$.

В общем случае изучение множества $C^\vee$ требует некоторых усилий. В частности, метод, рассмотренный в пп. (a) и (b), не работает, если у кривой есть вертикальные касательные или особые точки. Тем не менее удается построить удовлетворительную теорию *двойственных кривых* $C^\vee$ к кривым $C \subset k_2$. Для данного неприводимого многообразия $V \subset k^n$ также можно определить *двойственное многообразие* $V^\vee$.

8

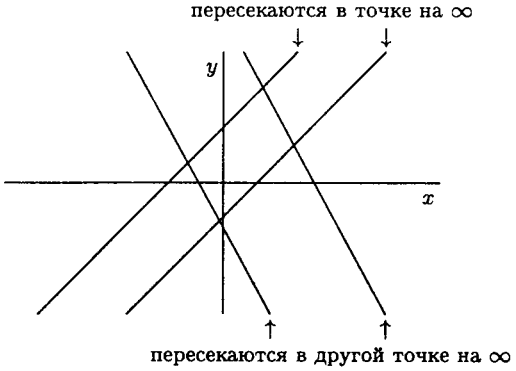
Проективная алгебраическая геометрия

Все многообразия, которые мы до сих пор рассматривали, были подмножествами аффинного пространства k^n. В этой главе мы расширим k^n, добавляя «точки на бесконечности», и построим проективное пространство $\mathbb{P}^n(k)$. Мы определим проективные многообразия в $\mathbb{P}^n(k)$ и рассмотрим проективную версию алгебро-геометрического соответствия. Связи между аффинными и проективными многообразиями будут рассмотрены в § 4, а в § 5 мы будем изучать теорию исключения с проективной точки зрения. Проективная точка зрения помогает лучше понять смысл теоремы о продолжении из гл. 3. В конце главы мы обсудим геометрию квадрик и теорему Безу.

§ 1. Проективная плоскость

В этом параграфе мы рассмотрим проективную плоскость $\mathbb{P}^2(\mathbb{R})$ над полем вещественных чисел $\mathbb{R}$. Мы увидим, что, в некотором смысле, на обычной аффинной плоскости $\mathbb{R}^2$ «недостает точек на бесконечности» и что, добавляя эти точки, мы и получаем проективную плоскость $\mathbb{P}^2(\mathbb{R})$. Мы также введем *однородные координаты*, которые помогут нам провести систематическое исследование проективной плоскости $\mathbb{P}^2(\mathbb{R})$.

Мы начнем с замечания, что две прямые на $\mathbb{R}^2$ пересекаются в точке, *если только* они не параллельны. Однако мы можем включить это исключение в общую схему, если будем считать, что параллельные прямые пересекаются в некой точке на ∞. Рисунок ниже подсказывает, что точка пересечения на бесконечности двух параллельных прямых зависит от их направления.



Чтобы формализовать эти соображения, определим отношение эквивалентности на множестве прямых, полагая $L_1 \sim L_2$, если L_1 и L_2 параллельны. Тогда класс эквивалентности $[L]$ состоит из всех прямых, параллельных L. Предыдущие рассуждения подсказывают, как нам следует определить точку на бесконечности, соответствующую классу $[L]$. Дадим строгое определение.

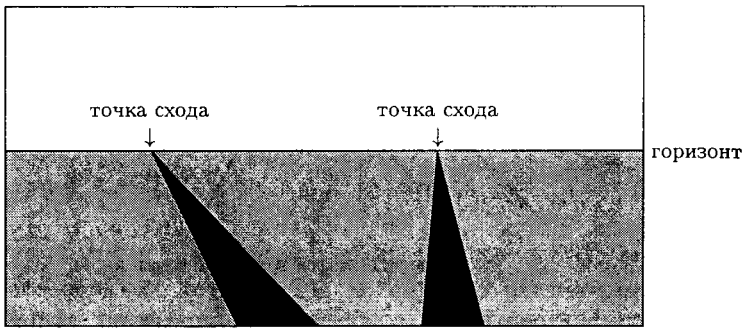
Определение 1. *Проективной плоскостью* $(\mathbb{R})$ называется множество

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \{\text{одна точка на } \infty \text{ для каждого класса параллельных прямых}\}.$$

Обозначим через $[L]_\infty$ общую точку на ∞ для всех прямых, параллельных прямой L. Множество $\bar{L} = L \cup [L]_\infty \subset \mathbb{P}^2(\mathbb{R})$ называется *проективной прямой*, соответствующей прямой L. Обратите внимание, что две проективные прямые всегда пересекаются в одной точке: если они не параллельны (как аффинные прямые), то пересекаются в какой-то точке из $\mathbb{R}^2$, а если параллельны, то они пересекаются в их общей точке на бесконечности.

На первый взгляд, следует ожидать, что прямая на плоскости должна иметь две точки на ∞, соответствующие двум направлениям движения на этой прямой. Но тогда в силу изложенного в предыдущем абзаце две параллельные прямые пересекались бы в двух точках, а не в одной, так что если мы параметризуем прямую $x = y$ с помощью формулы $(x, y) = (t, t)$, то к точке на бесконечности мы можем приближаться как при $t \to \infty$, так и при $t \to -\infty$.

Обычный способ визуализации точек на ∞ — использовать перспективу. Пусть на рисунке изображена плоская равнина и две дороги, идущие в разных направлениях:



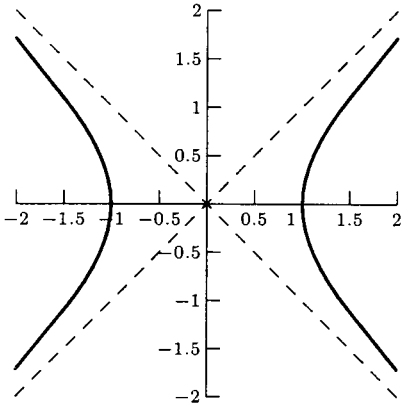
Два края каждой дороги (они параллельны) кажутся сходящимися в некоторой точке горизонта, которую теория перспективы называет *точкой схода*. Более того, каждая прямая, параллельная одной из дорог, приходит в ту же точку схода, т. е. точка схода соответствует точке на ∞ для этих прямых. Точки горизонта на этом рисунке представляют точки на ∞. (Обратите внимание, что горизонт содержит не все точки на ∞, в нем отсутствует точка на ∞ для прямых, параллельных горизонту.)

Этот рисунок демонстрирует еще одно интересное свойство проективной плоскости: точки на ∞ (мы часто будем называть их *бесконечно удаленными* точками) образуют особую проективную прямую, которая называется *бесконечно удаленной прямой* или прямой на ∞. Таким образом, прямые на $\mathbb{P}^2(\mathbb{R})$ — это проективные прямые $\bar{L} = L \cup [L]_\infty$, где L — это обычная прямая на $\mathbb{R}^2$, плюс прямая на ∞. В упражнениях мы докажем, что две различные проективные прямые в $\mathbb{P}^2(\mathbb{R})$ определяют единственную точку (их точку пересечения) и две различные точки в $\mathbb{P}^2(\mathbb{R})$ определяют единственную проективную прямую. Обратите внимание на симметрию этих утверждений: заменяя друг на друга «точки» и «проективные прямые» в одном утверждении, мы получаем другое. Это пример *принципа двойственности*, одного из оснований проективной геометрии.

Точки на ∞ появляются и в других задачах. Рассмотрим, например, параметризацию гиперболы $x^2 - y^2 = 1$, заданную уравнениями

$$x = \frac{1+t^2}{1-t^2},$$
$$y = \frac{2t}{1-t^2}.$$

При $t \neq \pm 1$ на гиперболе параметризованы все точки, кроме $(-1, 0)$. Но что происходит при $t = \pm 1$? Посмотрим на рисунок.



Пусть $t \to 1^-$; тогда соответствующая точка (x, y) движется по ветви гиперболы в первой четверти, все больше приближаясь к асимптоте $x = y$. Аналогично, при $t \to 1^+$ точка приближается к асимптоте $x = y$, но двигаясь по ветви гиперболы в третьей четверти. Таким образом, $t = 1$ соответствует точке на ∞ прямой $x = y$. Аналогично, $t = -1$ соответствует точке на ∞ другой асимптоты, $x = -y$. (В упражнениях мы рассмотрим ту же задачу с другой точки зрения.)

Хотя наше рассмотрение проективной плоскости и обогатило нас новыми идеями, но оно не является вполне удовлетворительным. Например, неясно, почему прямая на ∞ должна называться проективной прямой. Более серьезный недостаток состоит в том, что у нас нет единого подхода к точкам проективной плоскости: мы определили точки двух типов — обычные, заданные координатами в $\mathbb{R}^2$, и бесконечно удаленные, заданные прямыми. Чтобы исправить эту асимметрию, мы введем *однородные координаты* на $\mathbb{P}^2(\mathbb{R})$.

Введение однородных координат требует нового определения проективного пространства. Сначала мы определим отношение эквивалентности на точках из $\mathbb{R}^3$, отличных от начала координат, следующим образом:

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2),$$

если существует ненулевое вещественное λ, такое, что $(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$. Легко проверить, что $\sim$ в самом деле является отношением эквивалентности на $\mathbb{R}^3 - \{0\}$ (здесь 0 обозначает точку $(0, 0, 0) \in \mathbb{R}^3$). Теперь мы можем дать новое определение проективной плоскости.

Определение 2. *Проективная плоскость* $\mathbb{P}^2(\mathbb{R})$ — это множество классов эквивалентности по отношению $\sim$ на $\mathbb{R}^3 - \{0\}$, т. е.

$$\mathbb{P}^2(\mathbb{R}) = (\mathbb{R}^3 - \{0\})/\sim .$$

Если тройка чисел $(x, y, z) \in \mathbb{R}^3 - \{0\}$ соответствует точке $p \in \mathbb{P}^2(\mathbb{R})$, то (x, y, z) называются *однородными координатами* этой точки.

Не очевидно, что определения 1 и 2 описывают один и тот же объект, но мы вскоре увидим, что это так.

Однородные координаты отличаются от обычных координат тем, что они не единственны. Например, тройки $(1,1,1), (2,2,2), (\pi,\pi,\pi)$ и $(\sqrt{2},\sqrt{2},\sqrt{2})$ — это координаты одной и той же точки проективной плоскости. Но неединственность координат не является большой помехой, так как эти тройки пропорциональны друг другу.

Примером использования однородных координат является определение прямой.

Определение 3. Пусть $A, B, C \in \mathbb{R}$ и $A^2 + B^2 + C^2 > 0$. Тогда множество

$$\{p \in \mathbb{P}^2(\mathbb{R}) : Ax + By + Cz = 0, \text{ где } (x, y, z) \text{ — однородные координаты точки } p\}$$

называется *проективной прямой* в $\mathbb{P}^2(\mathbb{R})$.

Здесь необходимо отметить, что если равенство $Ax+By+Cz=0$ выполнено для какого-то одного набора однородных координат точки $p \in \mathbb{P}^2(\mathbb{R})$, то оно выполнено для *всех* однородных координат этой точки. В самом деле, другой набор однородных координат имеет вид $\lambda(x, y, z) = (\lambda x, \lambda y, \lambda z)$; поэтому $A \cdot \lambda x + B \cdot \lambda y + C \cdot \lambda z = \lambda(Ax + By + Cz) = 0$. Далее мы увидим, что аналогичные соображения позволяют определить многообразия в проективном пространстве.

Для установления связи между двумя определениями проективной плоскости рассмотрим отображение

$$\mathbb{R}^2 \to \mathbb{P}^2(\mathbb{R}), \tag{1}$$

переводящее точку $(x, y) \in \mathbb{R}^2$ в точку $p \in \mathbb{P}^2(\mathbb{R}^2)$ с однородными координатами $(x, y, 1)$. Это отображение обладает следующими свойствами.

Предложение 4. *Отображение* (1) *инъективно, и дополнением до его образа является проективная прямая* H_∞ *с уравнением* $z = 0$.

Доказательство. Предположим, что образы в $\mathbb{P}^2(\mathbb{R})$ двух точек (x, y) и (x', y') совпадают. Тогда $(x, y, 1)$ и $(x', y', 1)$ являются однородными координатами одной и той же точки p; поэтому $(x, y, 1) = \lambda(x', y', 1)$ для некоторого λ. Но из этого равенства следует, что $\lambda = 1$, а значит, $(x, y) = (x', y')$.

Пусть точка $p \in \mathbb{P}^2(\mathbb{R})$ имеет однородные координаты (x, y, z). Если $z = 0$, то $p \in H_\infty$. С другой стороны, если $z \neq 0$, то тройка $(x/z, y/z, 1)$ также является однородными координатами точки p. Значит, p принадлежит образу отображения (1). Доказательство того, что образ не пересекается с H_∞, мы оставляем читателю. □

Мы будем называть H_∞ *бесконечно удаленной прямой*. Хотя это и не совсем аккуратно, $\mathbb{R}^2$ можно отождествить с его образом в $\mathbb{P}^2(\mathbb{R})$; поэтому

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup H_\infty.$$

Теперь вторая конструкция $\mathbb{P}^2(\mathbb{R})$ начинает напоминать первую. Осталось показать, что H_∞ состоит из точек на ∞ (в смысле определения 1). Для этого надо рассмотреть связь между прямыми в $\mathbb{R}^2$ (которые мы будем называть *аффинными прямыми*) и проективными прямыми. Эта связь описывается следующей таблицей:

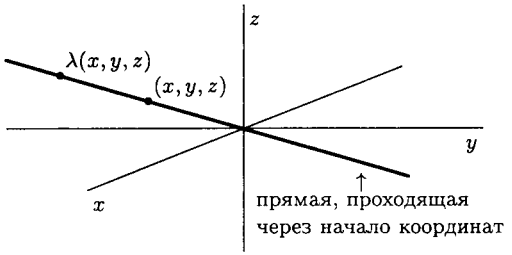
аффинная прямая		проективная прямая		точка на ∞
$L : y = mx + b$	$\to$	$\bar{L} : y = mx + bz$	$\to$	$(1, m, 0)$
$L : x = c$	$\to$	$\bar{L} : x = cz$	$\to$	$(0, 1, 0)$

Чтобы убедиться в этом, рассмотрим сначала невертикальную аффинную прямую L с уравнением $y = mx + b$. Отображение (1) переводит точку $(x, y) \in L$ в точку $(x, y, 1)$, которая принадлежит проективной прямой $\bar{L}$ с уравнением $y = mx + bz$, т. е. L можно рассматривать как подмножество в $\bar{L}$. По предложению 4 оставшиеся точки из $\bar{L}$ принадлежат проективной прямой $z = 0$. Но если $z = 0$, то мы получаем $y = mx$; поэтому оставшиеся точки имеют координаты $(x, mx, 0)$. Обратите внимание, что $x \neq 0$, иначе все три координаты были бы равны нулю, чего быть не может; поэтому оставшаяся точка единственна и имеет координаты $(1, m, 0)$. Она принадлежит пересечению двух прямых $\bar{L} \cap H_\infty$. Случай вертикальной прямой мы оставляем читателю в качестве упражнения.

Таблица показывает, что две прямые в $\mathbb{R}^2$ имеют общую точку на ∞ только в том случае, когда они параллельны. Для невертикальных прямых точка на ∞ соответствует наклону прямой, а все вертикальные прямые имеют одну (но отличную от невертикальных) общую точку на ∞. Постарайтесь разобраться во всем этом. В упражнениях мы проверим, что точки, перечисленные в таблице,

исчерпывают всю прямую H_∞. Следовательно, H_∞ состоит из точек на ∞, соответствующих всем классам параллельных прямых, по одной на класс. Таким образом, представление $\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup H_\infty$ доказывает эквивалентность определений 1 и 2.

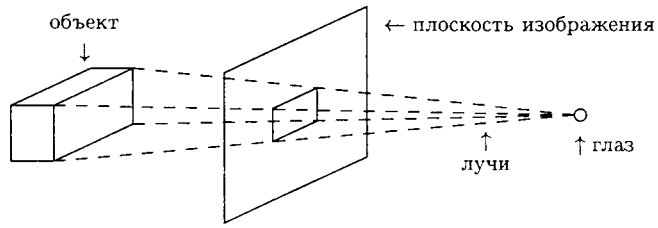
Теперь мы дадим геометрическую интерпретацию точек проективной плоскости. Пусть (x, y, z) — однородные координаты точки $p \in \mathbb{P}^2(\mathbb{R})$. Другие координаты той же точки имеют вид $\lambda(x, y, z)$, $\lambda \in \mathbb{R} - \{0\}$. Ключевым фактом является то, что точки с такими координатами лежат на одной прямой в $\mathbb{R}^3$, проходящей через начало координат:



Требование определения 2, что $(x, y, z) \neq (0, 0, 0)$, гарантирует, что получается прямая в $\mathbb{R}^3$. С другой стороны, если L — *произвольная* прямая в $\mathbb{R}^3$, проходящая через начало координат, то точки $(x, y, z) \in L - \{0\}$ задают однородные координаты однозначно определенной точки в $\mathbb{P}^2(\mathbb{R})$ (координаты ненулевых точек на L пропорциональны друг другу). Таким образом, мы имеем взаимно однозначное соответствие

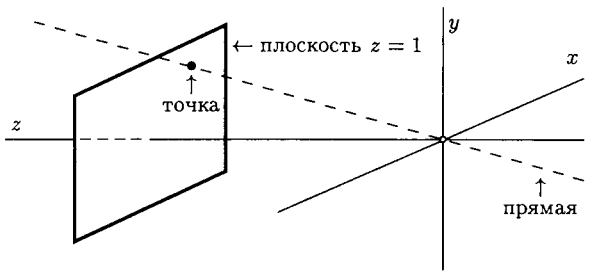
$$\mathbb{P}^2(\mathbb{R}) \cong \{\text{прямые в } \mathbb{R}^3, \text{ проходящие через начало координат}\}. \quad (2)$$

Хотя может показаться, что трудно думать о точках из $\mathbb{P}^2(\mathbb{R})$ как о прямых в $\mathbb{R}^3$, но есть и интуитивные основания для такой идентификации. Попытаемся изобразить, например, трехмерный объект на плоскости. Рассмотрим множество лучей, соединяющих наш глаз с точками объекта. Изображением является пересечение этого множества лучей с плоскостью:



Учение о перспективе в эпоху Возрождения оперировало с понятием «пирамиды лучей», соединяющей глаз художника с изображаемым объектом. Для нас основным является тот факт, что каждый луч пересекает плоскость изображения ровно в одной точке, что и задает взаимно однозначное соответствие между лучами и точками плоскости.

Для того чтобы формализовать это рассуждение, поместим «глаз» в начало координат, а плоскость зададим уравнением $z = 1$.



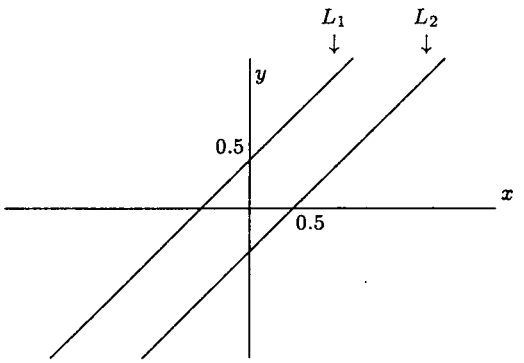
Вместо того чтобы работать с лучами (полупрямыми), мы будем работать с прямыми, проходящими через начало координат. Как показывает рисунок, каждой точке на плоскости $z = 1$ соответствует ровно одна такая прямая. Это позволяет говорить о *точке* на плоскости как о *прямой, проходящей через начало координат* в $\mathbb{R}^3$ (т. е. по (2) как о точке в $\mathbb{P}^2(\mathbb{R})$). Следует сделать два важных замечания:

- Точке (x, y) на аффинной плоскости соответствует точка $(x, y, 1)$ на плоскости $z = 1$. Соответствующая прямая задает точку $p \in \mathbb{P}^2(\mathbb{R})$ с однородными координатами $(x, y, 1)$. Это *в точности* то отображение $\mathbb{R}^2 \to \mathbb{P}^2(\mathbb{R})$, которое было определено в предложении 4.
- Это отображение не сюръективно, так как прямые, параллельные плоскости (x, y), не могут быть получены таким образом. Можно ли эти прямые рассматривать как точки на ∞?

Во многих ситуациях полезно одновременно воспринимать $\mathbb{P}^2(\mathbb{R})$ алгебраически (в терминах однородных координат) и геометрически (в терминах прямых, проходящих через начало координат).

Наконец, с помощью однородных координат мы рассмотрим бесконечно удаленную прямую. Начнем с того, что хотя декартовы координаты (x, y) и являются основой наших построений, но в системе однородных координат координата z ничем не отличается от координат x и y. В частности, мы можем рассматривать x и z как исходные координаты, а y как дополнительную.

Рассмотрим, например, параллельные прямые $L_1 : y = x + 1/2$ и $L_2 : y = x - 1/2$ на плоскости (x, y):

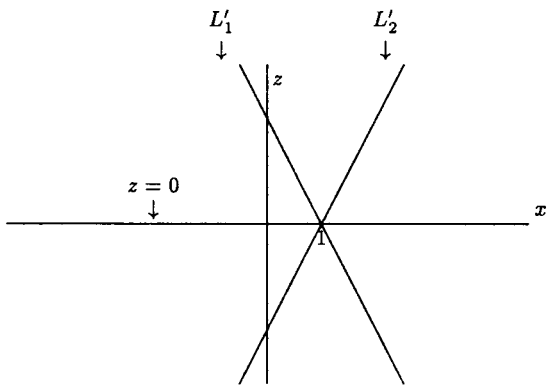


Плоскость (x, y)

Так как эти прямые параллельны, то они пересекаются на ∞. Но рисунок не показывает их точки пересечения. Чтобы увидеть ее, рассмотрим соответствующие проективные прямые

$$\bar{L}_1 : y = x + (1/2)z,$$
$$\bar{L}_2 : y = x - (1/2)z.$$

Будем считать x и z исходными переменными. Тогда мы отображаем плоскость (x, z) в проективную плоскость $\mathbb{P}^2(\mathbb{R})$: $(x, z) \mapsto (x, 1, z)$. Это отображение инъективно (по предложению 4), и образ этой плоскости в $\mathbb{P}^2(\mathbb{R})$ задается уравнением $y = 1$. Тогда проективные прямые $\bar{L}_1$ и $\bar{L}_2$ определяют прямые $L_1' : z = -2x + 2$ и $L_2' : z = 2x - 2$ на плоскости xz:



Плоскость (x, z)

На этом рисунке ось x задана уравнением $z = 0$, т. е. она является бесконечно удаленной прямой (в смысле исходного построения и предложения 4). Заметим, что L_1' и L_2' пересекаются на оси x, где $z = 0$, что соответствует тому факту, что прямые L_1 и L_2 пересекаются на ∞. Этот рисунок показывает, что происходит при приближении к бесконечно удаленной прямой. В упражнениях мы увидим, как некоторые стандартные кривые ведут себя на бесконечности.

Интересно сравнить этот рисунок с перспективным изображением двух дорог. Не случайно, что горизонт в перспективном изображении представляет собой бесконечно удаленную прямую. В упражнениях мы подробнее обсудим эту аналогию.

Следует также отметить, что евклидово понятие расстояния не играет большой роли в проективной геометрии. Например, прямые L_1 и L_2 находятся на постоянном расстоянии друг от друга на плоскости xy, но прямые L_1' и L_2' приближаются друг к другу на плоскости xz. Это также объясняет различие между евклидовой и проективной геометриями.

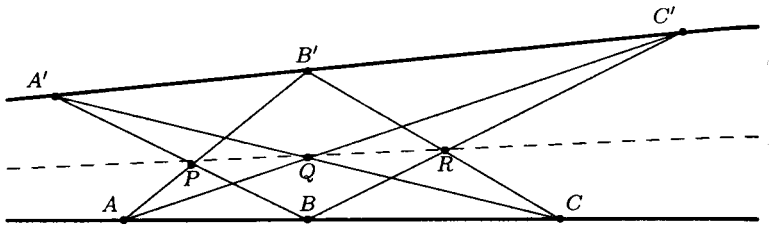
Упражнения к § 1

1. В этом упражнении мы будем работать в рамках определения 1, т. е. проективными прямыми в $\mathbb{P}^2(\mathbb{R})$ являются $\bar{L} = L \cup [L]_\infty$ и бесконечно удаленная прямая.
   (a) Докажите, что *любые* две различные точки на $\mathbb{P}^2(\mathbb{R})$ определяют единственную проективную прямую. Указание: нужно рассмотреть три случая в зависимости от того, сколько из этих точек лежит на ∞.
   (b) Докажите, что *любые* две различные проективные прямые пересекаются в единственной точке. Указание: здесь надо рассмотреть два случая.

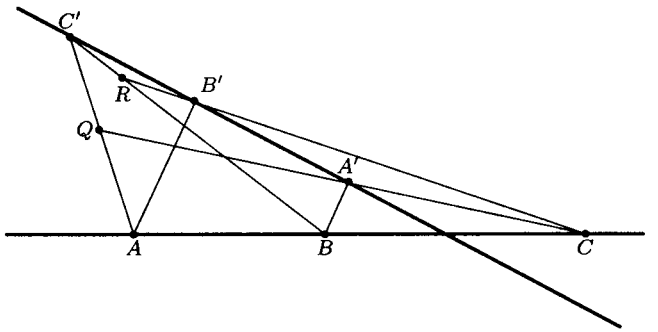
2. Большое количество теорем об объектах на евклидовой плоскости на самом деле являются (замаскированными) теоремами на проективной плоскости. Классическим примером является теорема Паппа, которая формулируется так. Пусть даны две тройки коллинеарных точек A, B, C и A', B', C'. Пусть

$$P = \overline{AB'} \cap \overline{A'B},$$
$$Q = \overline{AC'} \cap \overline{A'C},$$
$$R = \overline{BC'} \cap \overline{B'C}.$$

Теорема Паппа утверждает, что точки P, Q, R коллинеарны. В упр. 8 § 4 гл. 6 мы рисовали для иллюстрации этой теоремы такой рисунок:



(a) Однако если расположить точки на одной из прямых в обратном порядке, то может возникнуть такая конфигурация:



Обратите внимание, что точка P теперь лежит на ∞. Является ли теорема Паппа справедливой (в $\mathbb{P}^2(\mathbb{R})$) в этом случае?

(b) Перемещая точку C на втором рисунке, можно добиться того, что точка Q будет лежать на ∞. Останется ли теорема Паппа справедливой? На какой прямой будут лежать P, Q, R? Проиллюстрируйте это рисунком.

Если бы вы формулировали чисто аффинный вариант теоремы Паппа, учитывающий случаи (a) и (b), то утверждение получилось бы довольно громоздким. Работая в $\mathbb{P}^2(\mathbb{R})$, мы автоматически учитываем все возможные случаи.

3. Продолжим рассмотрение параметризации $(x, y) = ((1 + t^2)/(1 - t^2), 2t/(1 - t^2))$ гиперболы $x^2 - y^2 = 1$, начатое в тексте.

(a) Пусть t фиксировано. Докажите, что точка (x, y) на гиперболе, отвечающая значению t, является точкой пересечения гиперболы с прямой, проходящей через $(-1, 0)$ и имеющей коэффициент наклона t. Сделайте рисунок. Указание: используя параметризацию, покажите, что $t = y/(x + 1)$.

(b) Используя п. (a), объясните, почему значения $t = \pm 1$ соответствуют асимптотам. Сделайте рисунок.

(c) Используя однородные координаты, покажите, что рассматриваемая параметризация может быть записана в виде

$$((1 + t^2)/(1 - t^2), 2t/(1 - t^2), 1) = (1 + t^2, 2t, 1 - t^2).$$

Используя эту формулу, объясните, что происходит при $t = \pm 1$. Получите ли вы тот же ответ, что и в п. (b)?

(d) Ту же технику мы можем использовать, чтобы понять, что происходит при $t \to \infty$. А именно, в параметризации $(x, y, z) = (1 + t^2, 2t, 1 - t^2)$ мы положим $t = 1/u$, потом избавимся от знаменателей (это разрешенное преобразование для однородных координат) и перейдем к пределу при $u \to 0$. Какую точку гиперболы вы получите?

4. В этом упражнении мы изучим поведение гиперболы $x^2 - y^2 = 1$ на бесконечности.

(a) Объясните, почему уравнение $x^2 - y^2 = z^2$ корректно определяет кривую в $\mathbb{P}^2(\mathbb{R})$. Указание: см. обсуждение аналогичного вопроса после определения 3.

(b) Какие точки кривой C лежат на ∞? Как ваш ответ связать с результатами упр. 3?

(c) Перейдите в систему координат (x, z) (положив $y = 1$) и покажите, что C остается гиперболой.

(d) Перейдите в систему координат (y, z) (положив $x = 1$) и покажите, что C становится окружностью.

(e) Используя параметризацию из упр. 3, найдите параметризацию окружности из п. (d).

5. Рассмотрим параболу $y = x^2$.

(a) Какое преобразование уравнения превращает параболу в кривую в $\mathbb{P}^2(\mathbb{R})$?

(b) Сколько точек на бесконечности имеет парабола?

(c) Используя подходящие координаты (как в упр. 4), покажите, что парабола касается бесконечно удаленной прямой.

(d) Докажите, что парабола становится гиперболой в (y, z)-координатах.

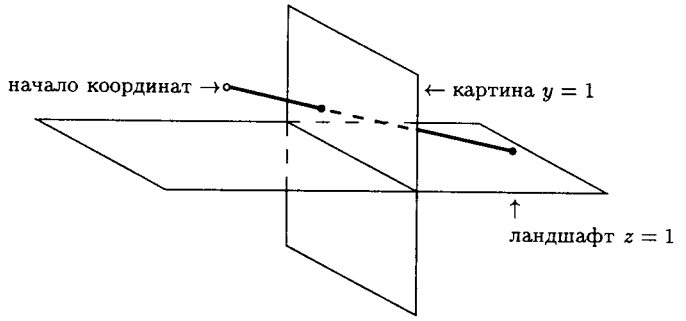
6. Использование системы координат (x, y) в $\mathbb{P}^2(\mathbb{R})$ позволяет увидеть только часть проективной плоскости. В частности, мы теряем бесконечно удаленную прямую. Чтобы ее увидеть, мы, как в тексте параграфа, можем использовать (x, z)-координаты. Докажите, что есть только одна точка в $\mathbb{P}^2(\mathbb{R})$, которая невидима в системах координат (x, y) и (x, z). Как увидеть, что происходит в этой точке?

7. Докажите, что образ плоскости при отображении (2) из предложения 4 не пересекается с H_∞.

8. Пусть прямая H_∞ задана уравнением $z = 0$. Таким образом, точки на H_∞ имеют однородные координаты $(a, b, 0)$, где $(a, b) \neq (0, 0)$.
   (a) Вертикальная аффинная прямая $x = c$ соответствует проективной прямой $x = cz$. Докажите, что эта проективная прямая пересекает H_∞ в точке $(0, 1, 0)$.
   (b) Докажите, что точка на H_∞, отличная от $(0, 1, 0)$, может быть однозначно записана в виде $(1, m, 0)$, где m — некоторое вещественное число.

9. В тексте параграфа мы рассматривали части плоскости $\mathbb{P}^2(\mathbb{R})$, описываемые системами (x, y)- и (x, z)-координат. В (x, z)-картине естественно спрашивать, что происходит с y. Для ответа на этот вопрос мы посмотрим, что происходит с (x, y)-координатами, когда мы рассматриваем их на (x, z)-плоскости.
   (a) Покажите, что точка (a, b) на (x, y)-плоскости дает точку $(a/b, 1/b)$ на (x, z)-плоскости.
   (b) Используя эту формулу, рассмотрите, как выглядят параболы $(x, y) = (t, t^2)$ и $(x, y) = (t^2, t)$ на (x, z)-плоскости. Сделайте рисунки в (x, y)- и (x, z)-плоскостях.

10. В этом упражнении мы обсудим математические основы теории перспективы. Предположим, что мы хотим изобразить ландшафт, представляющий собой горизонтальную плоскость. Изображение будет располагаться в вертикальной плоскости. Глаз расположен в некоторой точке выше плоскости ландшафта. Для изображения какой-либо точки ландшафта мы соединяем ее прямой с глазом. Точка пересечения этой прямой с плоскостью «картины» и будет изображением:



Поместим глаз в начало координат. Пусть плоскость $y = 1$ — плоскость изображения, а плоскость $z = 1$ — плоскость ландшафта (т. е. положительное направление оси z указывает вниз).
   (a) Найдите изображение точки $(a, b, 1)$.
   (b) Объясните связь между п. (a) и упр. 9. Кратко опишите связь между перспективным изображением и проективной плоскостью.

11. Пусть проективная прямая в $\mathbb{P}^2(\mathbb{R})$ задана уравнением $Ax + By + Cz = 0$, где $(A, B, C) \neq (0, 0, 0)$ (как в определении 3).
   (a) Почему мы требуем, чтобы $(A, B, C) \neq (0, 0, 0)$?
   (b) Докажите, что тройки (A, B, C) и (A', B', C') задают одну и ту же проективную прямую в том и только том случае, когда $(A, B, C) = \lambda(A', B', C')$ для некоторого ненулевого вещественного λ. Указание: в одну сторону это утверждение тривиально. Для доказательства обратного утверждения возьмем две различные точки (a, b, c) и (a', b', c') на прямой $Ax + By + Cz = 0$. Докажите, что (a, b, c) и (a', b', c') линейно независимы, а следовательно, система $Xa + Yb + Zc = Xa' + Yb' + Zc' = 0$ имеет одномерное пространство решений в переменных X, Y, Z.
   (c) Докажите, что множество проективных прямых в $\mathbb{P}^2(\mathbb{R})$ может быть отождествлено с множеством $\{(A, B, C) \in \mathbb{R}^3 : (A, B, C) \neq (0, 0, 0)\}/\sim$. Это множество называется *двойственной проективной плоскостью* и обозначается $\mathbb{P}^2(\mathbb{R})^\vee$.
   (d) Опишите подмножество в $\mathbb{P}^2(\mathbb{R})^\vee$, соответствующее аффинным прямым.
   (e) Пусть $p \in \mathbb{P}^2(\mathbb{R})$. Обозначим через $\tilde{p}$ множество всех проективных прямых, содержащих p. Мы можем рассматривать множество $\tilde{p}$ как подмножество в $\mathbb{P}^2(\mathbb{R})^\vee$. Докажите, что $\tilde{p}$ является проективной прямой в $\mathbb{P}^2(\mathbb{R})^\vee$. Множество $\tilde{p}$ называется *пучком прямых* в точке p.
   (f) В декартовом произведении $\mathbb{P}^2(\mathbb{R}) \times \mathbb{P}^2(\mathbb{R})^\vee$ есть естественное подмножество
   $$I = \{(p, L) \in \mathbb{P}^2(\mathbb{R}) \times \mathbb{P}^2(\mathbb{R})^\vee : p \in L\}.$$
   Докажите, что I задается уравнением $Ax + By + Cz = 0$, где (x, y, z) — однородные координаты на $\mathbb{P}^2(\mathbb{R})$, а (A, B, C) — однородные координаты на двойственной плоскости. Многообразия этого типа мы будем рассматривать в § 5.

Пункты (d), (e) и (f) этого упражнения показывают, что множества естественно определенных геометрических объектов могут иметь алгебраическую структуру.

§ 2. Проективное пространство и проективные многообразия

Конструкция вещественной проективной плоскости (определение 2 из § 1) может быть обобщена на любое количество измерений и на случай любого поля. Рассмотрим отношение эквивалентности $\sim$ на множестве ненулевых точек аффинного пространства k^{n+1}, полагая

$$(x_0', \ldots, x_n') \sim (x_0, \ldots, x_n),$$

если существует ненулевой элемент $\lambda \in k$, такой, что $(x_0', \ldots, x_n') = \lambda(x_0, \ldots, x_n)$. Обозначим через 0 нулевой вектор $(0, \ldots, 0) \in k^{n+1}$.

Определение 1. *n-мерным проективным пространством $\mathbb{P}^n(k)$ над полем k* называется множество классов эквивалентности в $k^{n+1} - \{0\}$ по отношению $\sim$, т. е.

$$\mathbb{P}^n(k) = (k^{n+1} - \{0\})/\sim .$$

Каждый ненулевой $(n+1)$-мерный вектор $(x_0, \ldots, x_n) \in k^{n+1}$ определяет точку $p \in \mathbb{P}^n(k)$, причем $(x_0, \ldots, x_n)$ называются *однородными координатами точки p.*

Как и в случае проективной плоскости, однородные координаты точки $p \in \mathbb{P}^n(k)$ не определены однозначно. Например, в $\mathbb{P}^3(\mathbb{C})$ однородные координаты $(0, \sqrt{2}, 0, i)$ и $(0, 2i, 0, -\sqrt{2})$ определяют одну точку: $(0, 2i, 0, -\sqrt{2}) = \sqrt{2}i(0, \sqrt{2}, 0, i)$. Мы будем писать $p = (x_0, \ldots, x_n)$ для указания того, что $(x_0, \ldots, x_n)$ являются однородными координатами точки $p \in \mathbb{P}^n(k)$ [1)].

Как и в § 1, $\mathbb{P}^n(k)$ можно представлять геометрически как множество прямых в k^{n+1}, проходящих через начало координат. Точнее (см. упр. 1), существует взаимно однозначное соответствие

$$\mathbb{P}^n(k) \cong \{\text{прямые в } k^{n+1}, \text{ проходящие через начало координат}\}. \tag{1}$$

Подобно тому, как проективная плоскость содержит аффинную в качестве подмножества, пространство $\mathbb{P}^n(k)$ содержит аффинное пространство k^n.

Предложение 2. *Пусть*

$$U_0 = \{(x_0, \ldots, x_n) \in \mathbb{P}^n(k) : x_0 \neq 0\}.$$

Тогда отображение ϕ, переводящее точку $(a_1, \ldots, a_n) \in k^n$ в точку $(1, a_1, \ldots, a_n) \in \mathbb{P}^n(k)$, устанавливает взаимно однозначное соответствие между k^n и $U_0 \subset \mathbb{P}^n(k)$.

Доказательство. Так как первая компонента точки $\phi(a_1, \ldots, a_n) = (1, a_1, \ldots, a_n)$ не равна нулю, то образ отображения ϕ принадлежит U_0. Определим обратное отображение $\psi : U_0 \to k^n$ следующим образом. Пусть $p = (x_0, \ldots, x_n) \in U_0$. Тогда $x_0 \neq 0$ и, следовательно, $p = (1, x_1/x_0, \ldots, x_n/x_0)$. Положим $\psi(p) = (x_1/x_0, \ldots, x_n/x_0) \in k^n$.

[1)] В литературе часто используется обозначение $p = (x_0 : \ldots : x_n)$. — *Прим. ред.*

Доказательство корректности определения отображения ψ и доказательство взаимной обратности отображений ϕ и ψ мы оставляем читателю в качестве упражнения. □

По определению множества U_0 имеем $\mathbb{P}^n(k) = U_0 \cup H$, где

$$H = \{p \in \mathbb{P}^n(k) : p = (0, x_1, \ldots, x_n)\}. \tag{2}$$

Отождествляя U_0 с k^n, мы можем считать H *бесконечно удаленной гиперплоскостью.* Из (2) следует, что ее точки определяются n-наборами $(x_1, \ldots, x_n)$, причем два набора определяют одну и ту же точку из H в том и только том случае, когда каждый из них является скалярным кратным другого (просто нужно игнорировать первую, нулевую координату точек из H). Другими словами, H является «копией» проективного пространства $\mathbb{P}^{n-1}(k)$ на единицу меньшей размерности. Отождествляя U_0 с k^n и H с $\mathbb{P}^{n-1}(k)$, мы можем записать

$$\mathbb{P}^n(k) = k^n \cup \mathbb{P}^{n-1}(k). \tag{3}$$

Что же означает равенство $H = \mathbb{P}^{n-1}(k)$ геометрически? По (1) точка $p \in \mathbb{P}^{n-1}(k)$ определяет прямую $L \subset k^n$, проходящую через начало координат. Следовательно, в (3) мы можем интерпретировать $p \in H$ как направление *всех* прямых в k^n, параллельных L. Это позволяет нам рассматривать p как точку на ∞ в смысле § 1 и дает возможность связать определение проективного пространства с интуитивным определением проективной плоскости. В упражнениях эта интерпретация будет рассмотрена на более алгебраическом уровне.

Следует особо отметить случай проективной прямой $\mathbb{P}^1(k)$. Так как $\mathbb{P}^0(k)$ состоит из одной точки (это следует из определения 1), то из (3) получаем

$$\mathbb{P}^1(k) = k^1 \cup \mathbb{P}^0(k) = k \cup \{\infty\},$$

где ∞ обозначает единственную точку пространства $\mathbb{P}^0(k)$. Если в соответствии с определением 1 мы будем воспринимать точки из $\mathbb{P}^1(k)$ как прямые в k^2, проходящие через начало координат, то выписанная формула отражает тот факт, что каждая прямая характеризуется своим наклоном, кроме вертикальной прямой, наклон которой бесконечен. Если $k = \mathbb{C}$, то

$$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$$

называют *сферой Римана.* Причину этого наименования мы рассмотрим в упражнениях.

Следует отметить, что $\mathbb{P}^n(k)$ содержит и другие копии k^n помимо U_0.

Следствие 3. *Для каждого $i = 0, \ldots, n$ определим подмножество*

$$U_i = \{(x_0, \ldots, x_n) \in \mathbb{P}^n(k) : x_i \neq 0\}.$$

(i) *Точки каждого множества U_i находятся во взаимно однозначном соответствии с точками пространства k^n.*
(ii) *Дополнение $\mathbb{P}^n(k) - U_i$ может быть отождествлено с $\mathbb{P}^{n-1}(k)$.*
(iii) $\mathbb{P}^n(k) = \bigcup_{i=0}^n U_i$.

Доказательство. См. упр. 5.

Наша следующая задача — дать определение проективного многообразия по аналогии с определением аффинного многообразия. Как, например, можно определить многообразие $\mathbf{V}(f)$, где $f \in k[x_0, \ldots, x_n]$? Следующий простой пример показывает, что здесь необходима осторожность. Рассмотрим $\mathbf{V}(x_1 - x_2^2)$ в $\mathbb{P}^2(\mathbb{R})$. Точка $p = (1, 4, 2)$ на первый взгляд принадлежит многообразию, потому что $4 - 2^2 = 0$. Но p также имеет координаты $2(1, 4, 2) = (2, 8, 4)$, для которых $8 - 4^2 = -8 \neq 0$. Таким образом, принадлежность точки многообразию зависит от конкретного выбора однородных координат.

Чтобы избежать этой неприятности, мы будем работать только с *однородными* полиномами. Напомним (см. определение 6 из § 1 гл. 7), что полином f называется *однородным* полной степени d, если каждый его член имеет полную степень d. Полином $f = x_1 - x_2^2$ не однороден. Именно это и является причиной того, что равенство $f = 0$ зависит от конкретного выбора однородных координат некоторой точки. С однородными полиномами этого не происходит.

Предложение 4. *Пусть $f \in k[x_0, \ldots, x_n]$ — однородный полином. Тогда если f обращается в нуль в точке p для какого-то конкретного набора ее однородных координат, то f обращается в нуль при любом выборе ее координат. В частности, $\mathbf{V}(f) = \{p \in \mathbb{P}^n(k) : f(p) = 0\}$ — это корректно определенное подмножество в $\mathbb{P}^n(k)$.*

Доказательство. Пусть $(a_0, \ldots, a_n)$ и $(\lambda a_0, \ldots, \lambda a_n)$ — два набора однородных координат точки $p \in \mathbb{P}^n(k)$. Предположим, что $f(a_0, \ldots, a_n) = 0$ и что f — однородный полином полной степени d. Тогда каждый член в f имеет вид

$$c x_0^{\alpha_0} \ldots x_n^{\alpha_n},$$

где $\alpha_0 + \ldots + \alpha_n = d$. Подставляя λa_i вместо x_i, получаем

$$c(\lambda a_0)^{\alpha_0} \ldots (\lambda a_n)^{\alpha_n} = \lambda^d c a_0^{\alpha_0} \ldots a_n^{\alpha_n}.$$

Суммируя по всем членам полинома f, мы можем вынести общий множитель λ^d:

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n) = 0.$$

Предложение доказано. □

Обратите внимание, что, даже если f однороден, уравнение $f = a$ не имеет смысла в $\mathbb{P}^n(k)$, если $0 \neq a \in k$. Уравнение $f = 0$ является здесь особым, поскольку оно корректно определяет подмножество в $\mathbb{P}^n(k)$. Мы будем изучать подмножества пространства $\mathbb{P}^n(k)$, определяемые *системами* однородных полиномов (возможно, различных полных степеней).

Определение 5. Пусть $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ — однородные полиномы. Положим

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_0, \ldots, a_n) \in \mathbb{P}^n(k) : f_i(a_0, \ldots, a_n) = 0, 1 \leq i \leq s\}.$$

$\mathbf{V}(f_1, \ldots, f_s)$ называется *проективным многообразием*, определенным полиномами $f_1, \ldots, f_s$.

Например, любой однородный полином степени 1

$$l(x_0, \ldots, x_n) = c_0 x_0 + \ldots + c_n x_n$$

определяет в $\mathbb{P}^n(k)$ проективное многообразие $\mathbf{V}(l)$, называемое *гиперплоскостью*. Один пример гиперплоскости нам известен — это бесконечно удаленная гиперплоскость $H = \mathbf{V}(x_0)$. Если $n = 2$, то гиперплоскости называются *проективными прямыми* или просто *прямыми* в $\mathbb{P}^2(k)$. Аналогично, при $n = 3$ гиперплоскости называются *плоскостями* в $\mathbb{P}^3(k)$. Многообразия, определенные одним или несколькими линейными полиномами (т. е. однородными полиномами степени 1), называются *линейными многообразиями* в $\mathbb{P}^n(k)$. Например, $\mathbf{V}(x_1, x_2) \subset \mathbb{P}^3(k)$ является линейным многообразием — проективной прямой в $\mathbb{P}^3(k)$.

Многообразие $\mathbf{V}(f)$, определенное одним однородным полиномом, называется *гиперповерхностью*. Гиперповерхности классифицируются в соответствии с полной степенью определяющего полинома f. Если f имеет полную степень 2, то $\mathbf{V}(f)$ называется *квадратичной гиперповерхностью* или *квадрикой*. Например, $\mathbf{V}(-x_0^2 + x_1^2 + x_2^2) \subset \mathbb{P}^2(\mathbb{R})$ — квадрика. Аналогично гиперповерхности, определяемые полиномами степеней 3, 4 и 5 называются соответственно *кубиками*, *квартиками* и *квинтиками*.

Для того чтобы лучше разбираться в проективных многообразиях, нам необходимо определить соответствующие алгебраические объекты. Этими объектами являются *однородные идеалы*, которые будут изучаться в § 3. Мы увидим, что алгебро-геометрическое соответствие из гл. 4 полностью переносится на проективный случай.

Теперь мы рассмотрим соотношение между аффинными и проективными многообразиями. Как мы видели в следствии 3, подмножества $U_i \subset \mathbb{P}^n(k)$ являются копиями пространства k^n, так что мы можем поинтересоваться, как аффинные многообразия в $U_i \cong k^n$ соотносятся с проективными многообразиями в $\mathbb{P}^n(k)$. Возьмем, например, некоторое проективное многообразие V и рассмотрим его пересечение с одним из U_i. Является ли это пересечение аффинным многообразием? Ответ на этот вопрос *положительный*, причем определяющие уравнения многообразия $V \cap U_i$ могут быть получены с помощью процедуры, называемой *дегомогенизацией* [1]. Рассмотрим, например, пересечение $V \cap U_0$. Мы знаем, что если точка p лежит в U_0, то ее однородные координаты имеют вид $(1, x_1, \ldots, x_n)$. Пусть $f \in k[x_0, \ldots, x_n]$ — один из полиномов, определяющих V. Тогда полином $g(x_1, \ldots, x_n) = f(1, x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ обращается в нуль в каждой точке множества $V \cap U_0$. Замена $x_0 = 1$ в f преобразует f в «дегомогенизированный» полином g, который, как правило, не является однородным. Мы утверждаем, что $V \cap U_0$ является аффинным многообразием, которое задано с помощью процедуры дегомогенизации полиномов, определяющих V.

Предложение 6. *Рассмотрим проективное многообразие* $V = \mathbf{V}(f_1, \ldots, f_s)$. *Тогда* $W = V \cap U_0$ *может быть отождествлено с аффинным многообразием* $\mathbf{V}(g_1, \ldots, g_s) \subset k^n$, *где* $g_i(y_1, \ldots, y_n) = f_i(1, y_1, \ldots, y_n), 1 \le i \le s$.

Доказательство. Очевидно, что при отображении $\psi : U_0 \to k^n$ (см. предложение 2) $\psi(W) \subset \mathbf{V}(g_1, \ldots, g_s)$. С другой стороны, если $(a_1, \ldots, a_n) \in \mathbf{V}(g_1, \ldots, g_s)$, то точка с однородными координатами $(1, a_1, \ldots, a_n)$ лежит в U_0 и имеет место равенство

$$f_i(1, a_1, \ldots, a_n) = g_i(a_1, \ldots, a_n) = 0.$$

Поэтому $\phi(\mathbf{V}(g_1, \ldots, g_s)) \subset W$. Так как отображения ϕ и ψ взаимно обратны, то точки из W находятся во взаимно однозначном соответствии с точками из $\mathbf{V}(g_1, \ldots, g_s)$. □

Рассмотрим, например, проективное многообразие

$$V = \mathbf{V}(x_1^2 - x_0x_2, x_1^3 - x_0^2x_3) \subset \mathbb{P}^3(\mathbb{R}). \tag{4}$$

[1] От английского «homogeneous» — однородный.— *Прим. ред.*

Чтобы найти пересечение $V \cap U_0$, нам нужно дегомогенизировать определяющие уравнения. В результате мы получим аффинное многообразие

$$\mathbf{V}(x_1^2 - x_2, x_1^3 - x_3) \subset \mathbb{R}^3,$$

которое является уже известной нам скрученной кубикой.

Процедуру дегомогенизации мы можем проводить относительно любой переменной. Например, если дано проективное многообразие $V \subset \mathbb{P}^3(\mathbb{R})$, то $V \cap U_1$ может быть отождествлено с аффинным многообразием в $\mathbb{R}^3$, определенным уравнениями $g_i(x_0, x_2, x_3) = f_i(x_0, 1, x_2, x_3)$. В случае многообразия (4) $V \cap U_1$ — это аффинное многообразие $\mathbf{V}(1 - x_0x_2, 1 - x_0^2x_3)$. В упр. 9 рассматривается общая формулировка этой задачи.

С другой стороны, мы можем задать следующий вопрос: верно ли, что любое аффинное многообразие в U_i является пересечением $V \cap U_i$ для некоторого проективного многообразия V? Ответ *положительный*, но оказывается, что такое V определено неоднозначно, и результаты могут быть неожиданными.

Естественно попытаться, обратив предыдущую операцию дегомогенизации, «гомогенизировать» уравнения, определяющие аффинное многообразие W, т. е. сделать их однородными. Пусть, например, $W = \mathbf{V}(x_2 - x_1^3 + x_1^2) \subset U_0 = \mathbb{R}^2$. Определяющее уравнение неоднородно; поэтому оно не определяет проективное многообразие в $\mathbb{P}^2(\mathbb{R})$. Но мы легко можем превратить его в однородное, добавив переменную x_0. Так как полная степень полинома $f = x_2 - x_1^3 + x_1^2$ равна трем, то мы преобразуем f так, чтобы каждый член имел полную степень 3, в результате получается однородный полином полной степени 3

$$f^h = x_0^2x_2 - x_1^3 + x_0x_1^2.$$

Отметим, что процедура дегомогенизации полинома f^h даст нам снова f.

Опишем общую схему.

Предложение 7. *Пусть* $g \in k[x_1, \ldots, x_n]$ — *полином полной степени* d.

(i) *Запишем* g *в виде* $g = \sum_{i=0}^{d} g_i$, *где* g_i — *однородный полином полной степени* i. *Тогда*

$$\begin{aligned} g^h(x_0, \ldots, x_n) &= \sum_{i=0}^{d} g_i(x_1, \ldots, x_n)x_0^{d-i} \\ &= g_d(x_1, \ldots, x_n) + g_{d-1}(x_1, \ldots, x_n)x_0 \\ &\quad + \ldots + g_0(x_1, \ldots, x_n)x_0^d \end{aligned}$$

является однородным полиномом в $k[x_0, \ldots, x_n]$ *полной степени* d, *который называется* гомогенизацией *полинома* g.

(ii) *Имеет место формула*

$$g^h = x_0^d \cdot g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

(iii) *Дегомогенизация полинома* g^h *дает снова* g, *т. е.* $g^h(1, x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$.

(iv) *Пусть* $F(x_0, \ldots, x_n)$ — *однородный полином, и пусть* x_0^e — *наивысшая степень переменной* x_0, *которая делит* F. *Пусть* $f = F(1, x_1, \ldots, x_n)$ — *дегомогенизация полинома* F; *тогда* $F = x_0^e \cdot f^h$.

Доказательство. Доказательство рассмотрено в упр. 10. □

По предложению 7, если нам дано аффинное многообразие $W = \mathbf{V}(g_1, \ldots, g_s) \subset k^n$, то гомогенизация уравнений, определяющих W, дает нам проективное многообразие $V = \mathbf{V}(g_1^h, \ldots, g_s^h) \subset \mathbb{P}^n(k)$. Согласно п. (iii) и предложению 6, $V \cap U_0 = W$. Таким образом, исходное аффинное многообразие W является *аффинной частью* проективного многообразия V.

Как мы уже упоминали, здесь есть некоторые неожиданные возможности.

Пример 8. В этом примере однородными координатами точек в $\mathbb{P}^2(k)$ будут переменные x, y, z (отвечающие номерам 0, 1, 2 соответственно). Тогда U_2 — это множество точек с однородными координатами вида $(x, y, 1)$, и x, y являются координатами на $U_2 \cong k^2$. Рассмотрим аффинное многообразие $W = \mathbf{V}(g) = \mathbf{V}(y - x^3 + x) \subset U_2$. Оно является аффинной частью $V \cap U_2$ проективного многообразия $V = \mathbf{V}(g^h) = \mathbf{V}(yz^2 - x^3 + xz^2)$.

Многообразие V состоит из W и точек на бесконечности $V \cap \mathbf{V}(z)$. Его аффинная часть W представляет собой график кубического полинома — неособую плоскую кривую. Точки на бесконечности, т. е. дополнение к W в V, являются решениями системы

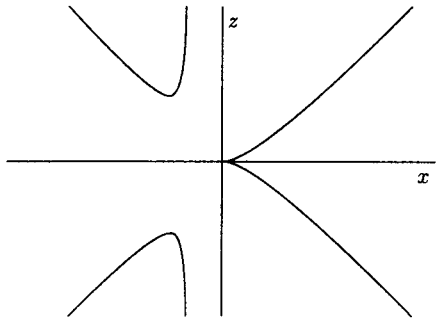
$$\begin{aligned} 0 &= yz^2 - x^3 + xz^2, \\ 0 &= z. \end{aligned}$$

Легко видеть, что эти решения даются формулой $z = x = 0$, а так как мы работаем в $\mathbb{P}^2(k)$, то решением является единственная точка $p = (0, 1, 0)$. Таким образом, $V = W \cup \{p\}$. Неожиданным здесь является природа этой точки p.

Чтобы увидеть, как V выглядит в окрестности p, дегомогенизируем определяющее уравнение многообразия V по отношению к y, т. е. рассмотрим пересечение $V \cap U_1$. Получаем

$$W' = V \cap U_1 = \mathbf{V}(g^h(x, 1, z)) = \mathbf{V}(z^2 - x^3 + xz^2).$$

Легко видеть (см. § 4 гл. 3), что точка p, которая имеет координаты $(0, 0)$ в U_1, является особой точкой в W':



Другими словами, если нам дано неособое (т. е. без особых точек) аффинное многообразие, то гомогенизация его уравнений может привести к более сложному геометрическому объекту. Это означает, что исходная аффинная часть многообразия «не дает полной картины». Для того чтобы ее увидеть, мы должны рассмотреть все аффинные части $V \cap U_i$ проективного многообразия $V \subset \mathbb{P}^n(k)$ (поскольку $\mathbb{P}^n(k) = \bigcup_{i=0}^n U_i$).

Наш следующий пример показывает, что простая гомогенизация определяющих уравнений может привести к «неправильному» проективному многообразию.

Пример 9. Рассмотрим скрученную кубику $W = \mathbf{V}(x_2 - x_1^2, x_3 - x_1^3) \subset \mathbb{R}^3$. По предложению 7 $W = V \cap U_0$, где V — проективное многообразие $\mathbf{V}(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3) \subset \mathbb{P}^3(\mathbb{R})$. Как и в примере 8, мы хотим узнать, какие точки из V отсутствуют в его аффинной части W. Дополнением к W в V является пересечение $V \cap H$, где $H = \mathbf{V}(x_0)$ — бесконечно удаленная плоскость. Таким образом, $V \cap H = \mathbf{V}(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3, x_0)$. Легко видеть, что эта система сводится к равенствам $x_0 = x_1^2 = x_1^3$, т. е. $x_0 = x_1 = 0$. Координаты x_2 и x_3 здесь произвольные. Поэтому $V \cap H$ — проективная прямая $\mathbf{V}(x_0, x_1) \subset \mathbb{P}^3(\mathbb{R})$. Значит, $V = W \cup \mathbf{V}(x_0, x_1)$.

Так как скрученная кубика — это кривая в $\mathbb{R}^3$, то наша интуиция подсказывает, что она должна иметь лишь конечное число

точек на бесконечности (в упражнениях мы увидим, что это так и есть). Это означает, что V слишком велико и есть меньшее проективное многообразие V', содержащее W. Чтобы найти такое V', можно попробовать гомогенизировать другие полиномы, обращающиеся в нуль на W. Параметризация (t, t^2, t^3) многообразия W подсказывает, что $x_1x_3 - x_2^2 \in \mathbf{I}(W)$. Так как полином $x_1x_3 - x_2^2$ уже однороден, то мы можем добавить его к определяющим уравнениям для V и получить

$$V' = \mathbf{V}(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3, x_1x_3 - x_2^2) \subset V.$$

Тогда $V' \cap U_0 = W$, а в упражнениях будет доказано, что $V' \cap H$ состоит из единственной точки $p = (0, 0, 0, 1)$. Таким образом, $V' = W \cup \{p\}$ является меньшим (по сравнению с V) проективным многообразием, содержащим W как аффинную часть. Различие между V и V' состоит в том, что V имеет лишнюю компоненту на бесконечности. В § 4 будет доказано, что V' — это наименьшее проективное многообразие, содержащее W.

В примере 9 мы строили проективное многообразие V прямой гомогенизацией уравнений, определяющих W, и получили слишком большой объект. Это означает, что какие-то тонкие вещи мы не учли. Полный ответ будет дан в § 4, где будет дан алгоритм описания наименьшего проективного многообразия, содержащего аффинное многообразие $W \subset k^n \cong U_i$.

Упражнения к § 2

1. В этом упражнении мы рассмотрим более геометрический подход к построению $\mathbb{P}^n(k)$. Через $\mathcal{L}$ мы обозначим множество прямых в k^{n+1}, проходящих через начало координат.
   (a) Докажите, что каждый элемент из $\mathcal{L}$ может быть представлен как множество векторов, кратных некоторому ненулевому вектору в k^{n+1}.
   (b) Докажите, что два ненулевых вектора $v, v' \in k^{n+1}$ определяют один и тот же элемент в $\mathcal{L}$ в том и только том случае, когда $v' \sim v$ в смысле определения 1.
   (c) Докажите, что существует взаимно однозначное соответствие между $\mathbb{P}^n(k)$ и $\mathcal{L}$.

2. Завершите доказательство предложения 2, показав, что отображения ϕ и ψ взаимно обратны.

3. В этом упражнении мы рассмотрим связь между прямыми в $\mathbb{R}^n$ и точками на бесконечности в $\mathbb{P}^n(\mathbb{R})$. Мы будем использовать формулу (3): $\mathbb{P}^n(\mathbb{R}) = \mathbb{R}^n \cup \mathbb{P}^{n-1}(\mathbb{R})$. Рассмотрим прямую L в $\mathbb{R}^n$ и ее параметризацию $a + bt$, где $a \in L$, а b — ненулевой вектор, параллельный L. В координатной записи эта параметризация имеет вид $(a_1 + b_1t, \ldots, a_n + b_nt)$.
   (a) Переходя к однородным координатам
   $$(1, a_1 + b_1t, \ldots, a_n + b_nt),$$
   мы будем считать, что $L \subset \mathbb{P}^n(\mathbb{R})$. Нас интересует, что происходит при $t \to \pm\infty$. Для этого поделим координаты точек из L на t,
   $$\left(\frac{1}{t}, \frac{a_1}{t} + b_1, \ldots, \frac{a_n}{t} + b_n\right).$$
   Какую точку из $H = \mathbb{P}^{n-1}(\mathbb{R})$ мы получим при $t \to \pm\infty$?
   (b) Прямая L может быть параметризована многими способами. Докажите, что точка из $\mathbb{P}^{n-1}(\mathbb{R})$, найденная в п. (a), одна и та же для всех параметризаций прямой L. Указание: два ненулевых вектора параллельны в том и только том случае, если они пропорциональны.
   (c) Пункты (a) и (b) показывают, что прямая $L \subset \mathbb{R}^n$ однозначно определяет точку в $H = \mathbb{P}^{n-1}(\mathbb{R})$. Докажите, что две прямые в $\mathbb{R}^n$ параллельны в том и только том случае, когда они имеют одну и ту же точку на бесконечности.

4. Если $k = \mathbb{R}$ или $\mathbb{C}$, то проективную прямую $\mathbb{P}^1(k)$ легко изобразить.
   (a) В тексте параграфа мы назвали $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ римановой сферой. Чтобы понять смысл этого названия, используйте параметризацию из упр. 6 к § 3 гл. 1 и докажите, что эта плоскость соответствует сфере без северного полюса. Это и объясняет, почему мы можем считать $\mathbb{C} \cup \{\infty\}$ сферой.
   (b) Какой хорошо знакомый геометрический объект соответствует $\mathbb{P}^1(\mathbb{R})$? Сделайте рисунок.

5. Докажите следствие 3.

6. В этом упражнении мы рассмотрим подмножества $U_i \subset \mathbb{P}^n(k)$.
   (a) Рассмотрим пространство $\mathbb{P}^4(k)$. Объясните, какие точки принадлежат подмножествам $U_2, U_2 \cap U_3$ и $U_1 \cap U_3 \cap U_4$.
   (b) Опишите $\mathbb{P}^4(k) - U_2, \mathbb{P}^4(k) - (U_2 \cup U_3)$ и $\mathbb{P}^4(k) - (U_1 \cup U_3 \cup U_4)$ как «копии» другого проективного пространства.
   (c) Что представляет собой множество $\bigcap_{i=0}^4 U_i$ в $\mathbb{P}^4(k)$?
   (d) Опишите подмножество $U_{i_1} \cap \ldots \cap U_{i_s} \subset \mathbb{P}^n(k)$, где $1 \le i_1 < i_2 < \ldots < i_s \le n$.

7. В этом упражнении мы выясним, когда можно корректно определить множество нулей неоднородных полиномов в $\mathbb{P}^n(k)$. Пусть поле k бесконечно. Мы хотим доказать, что если $f \in k[x_0, \ldots, x_n]$ *неоднороден*, но обращается в нуль на всех наборах однородных координат некоторой точки $p \in \mathbb{P}^n(k)$, то каждая его однородная компонента f_i обращается в нуль в p (см. определение 6 из § 1 гл. 7).

(a) Рассмотрим представление f в виде суммы однородных компонент, $f = \sum_i f_i$. Пусть $p = (a_0, \ldots, a_n)$. Докажите, что

$$f(\lambda a_0, \ldots, \lambda a_n) = \sum_i f_i(\lambda a_0, \ldots, \lambda a_n) = \sum_i \lambda^i f_i(a_0, \ldots, a_n).$$

(b) Докажите, что если f обращается в нуль при всех $\lambda \neq 0 \in k$, то $f_i(a_0, \ldots, a_n) = 0$ при всех i.

8. Используя дегомогенизацию определяющих уравнений проективного многообразия V, найдите уравнения указанных аффинных многообразий.
   (a) Пусть однородными координатами в $\mathbb{P}^2(k)$ являются (x, y, z). Рассмотрим многообразие $V = \mathbf{V}(x^2 + y^2 - z^2) \subset \mathbb{P}^2(\mathbb{R})$. Найдите уравнения многообразий $V \cap U_0$ и $V \cap U_2$. (Здесь $x \neq 0$ на U_0 и $z \neq 0$ на U_2.) Нарисуйте полученные кривые и объясните, что они говорят о проективном многообразии V.
   (b) Пусть $V = \mathbf{V}(x_0x_2 - x_3x_4, x_0^2x_3 - x_1x_2^2) \subset \mathbb{P}^4(k)$. Найдите уравнения аффинных многообразий $V \cap U_0 \subset k^4$ и $V \cap U_3 \subset k^4$.

9. Рассмотрим проективное многообразие $V = \mathbf{V}(f_1, \ldots, f_s)$, определенное однородными полиномами $f_i \in k[x_0, \ldots, x_n]$. Докажите, что подмножество $W = V \cap U_i$ может быть отождествлено с аффинным многообразием $\mathbf{V}(g_1, \ldots, g_s) \subset k^n$, определенным дегомогенизированными полиномами

$$g_j(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = f_j(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n),$$

где 1 заменяет x_i в f_j. Указание: используйте следствие 3 и следуйте доказательству предложения 6.

10. Докажите предложение 7.

11. Используя п. (iv) предложения 7, докажите, что если $f \in k[x_1, \ldots, x_n]$ и $F \in k[x_0, \ldots, x_n]$ — произвольный однородный полином, удовлетворяющий условию $F(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, то $F = x_0^e f^h$ для некоторого $e \geq 0$.

12. Каков будет результат гомогенизации (предложение 7) однородного полинома?

13. В примере 8 мы рассматривали многообразие $W' = \mathbf{V}(z^2 - x^3 + xz^2) \subset k^2$. Дайте строгое доказательство того, что точка $(x, z) = (0, 0)$ является особой точкой в W'. Указание: см. определение 3 из § 4 гл. 3.

14. Для каждого из следующих аффинных многообразий W с помощью процесса гомогенизации (предложение 7) постройте проективное многообразие V, такое, что $W = V \cap U_0$. В каждом случае дайте описание множества $V - W = V \cap H$, где H — бесконечно удаленная гиперплоскость.

   (a) $W = \mathbf{V}(y^2 - x^3 - ax - b) \subset \mathbb{R}^2, a, b \in \mathbb{R}$. Является ли точка $V \cap H$ особой? Указание: в качестве однородных координат на $\mathbb{P}^2(\mathbb{R})$ возьмите (z, x, y), так что U_0 задается условием $z \neq 0$.
   (b) $W = \mathbf{V}(x_1x_3 - x_2^2, x_1^2 - x_2) \subset \mathbb{R}^3$. Имеет ли V в этом случае дополнительную компоненту на бесконечности?
   (c) $W = \mathbf{V}(x_3^2 - x_1^2 - x_2^2) \subset \mathbb{R}^3$.

15. Рассмотрим скрученную кубику $W = \mathbf{V}(x_2 - x_1^2, x_3 - x_1^3) \subset \mathbb{R}^3$ из примера 9.
   (a) Рассмотрим параметризацию (t, t^2, t^3) кубики W в $\mathbb{R}^3$. Докажите, что при $t \to \pm\infty$ точка $(1, t, t^2, t^3)$ в $\mathbb{P}^3(\mathbb{R})$ стремится к точке $(0, 0, 0, 1)$ в $\mathbb{P}^3(\mathbb{R})$. Другими словами, мы ожидаем, что W имеет одну точку на бесконечности.
   (b) Теперь рассмотрим проективное многообразие

$$V' = \mathbf{V}(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3, x_1x_3 - x_2^2) \subset \mathbb{P}^3(\mathbb{R}).$$

   Докажите, что $V' \cap U_0 = W$ и что $V' \cap H = \{(0, 0, 0, 1)\}$.
   (c) Пусть $V = \mathbf{V}(x_0x_2 - x_1^2, x_0^3x_3 - x_1^3)$ — проективное многообразие из примера 9. Докажите, что $V = V' \cup \mathbf{V}(x_0, x_1)$. Это показывает, что V является объединением двух собственных проективных многообразий.

16. Однородный полином $f \in k[x_0, \ldots, x_n]$ определяет *аффинное* многообразие $C = \mathbf{V}_a(f) \subset k^{n+1}$, где нижний индекс указывает на то, что мы работаем в аффинном пространстве. Это многообразие называется *аффинным конусом* над проективным многообразием $V = \mathbf{V}(f) \subset \mathbb{P}^n(k)$. Рассмотрим его свойства.
   (a) Пусть C содержит точку $P \neq (0, \ldots, 0)$. Докажите, что тогда C содержит прямую, проходящую через начало координат и P.
   (b) Пусть $p \in \mathbb{P}^n(k)$ — такая точка, что ее однородные координаты совпадают с аффинными координатами точки P. Докажите, что $p \in V$ в том и только том случае, когда аффинная прямая, проходящая через P и начало координат, содержится в C. Указание: примените определение (1) и упр. 1.
   (c) Докажите, что C является объединением множества прямых, проходящих через начало координат и соответствующих точкам из V. Это объясняет смысл названия «конус», так как обычный конус также является объединением некоторого множества прямых, проходящих через начало координат. Подобный конус мы рассматривали в упр. 14, п. (c).

17. Для однородных полиномов справедливо важное соотношение, называемое *формулой Эйлера*. Пусть $f \in k[x_0, \ldots, x_n]$ — однородный полином полной степени d. Тогда формула Эйлера утверждает, что

$$\sum_{i=0}^{n} x_i \cdot \frac{\partial f}{\partial x_i} = d \cdot f.$$

(a) Проверьте справедливость формулы Эйлера для однородного полинома $f = x_0^3 - x_1x_2^2 + 2x_1x_3^2$.

(b) Докажите формулу Эйлера (для случая $k = \mathbb{R}$), рассматривая $f(\lambda x_0, \ldots, \lambda x_n)$ как функцию от λ и дифференцируя ее по λ.

18. В этом упражнении мы подробно изучим множество гиперплоскостей в $\mathbb{P}^n(k)$.

(a) Докажите, что два однородных линейных полинома

$$0 = a_0x_0 + \ldots + a_nx_n,$$
$$0 = b_0x_0 + \ldots + b_nx_n$$

определяют одну и ту же гиперплоскость в $\mathbb{P}^n(k)$ в том и только том случае, когда $b_i = \lambda a_i, i = 0, \ldots, n$, для некоторого $0 \neq \lambda \in k$. Указание: воспользуйтесь рассуждениями из упр. 11 к § 1.

(b) Докажите, что отображение, которое сопоставляет гиперплоскости с уравнением $a_0x_0 + \ldots + a_nx_n = 0$ вектор $(a_0, \ldots, a_n)$, индуцирует взаимно однозначное соответствие

$$\phi : \{\text{гиперплоскости в } \mathbb{P}^n(k)\} \to (k^{n+1} - \{0\})/\sim,$$

где $\sim$ — отношение эквивалентности из определения 1. Множество в левой части этой формулы называется *двойственным проективным пространством* и обозначается $\mathbb{P}^n(k)^\vee$. Точки в $\mathbb{P}^n(k)^\vee$ — это гиперплоскости в $\mathbb{P}^n(k)$.

(c) Опишите подмножество в $\mathbb{P}^n(k)$, соответствующее множеству гиперплоскостей, содержащих точку $p = (1, 0, \ldots, 0)$.

19. Пусть k — алгебраически замкнутое поле (например, $\mathbb{C}$). Докажите, что любой однородный полином $f(x_0, x_1) \in k[x_0, x_1]$ может быть разложен в произведение линейных однородных полиномов из $k[x_0, x_1]$:

$$f(x_0, x_1) = \prod_{i=1}^{d} (a_ix_0 + b_ix_1),$$

где d — полная степень полинома f. Указание: дегомогенизируйте f.

20. В § 4 гл. 5 мы ввели *пучок* гиперповерхностей, определенный двумя гиперповерхностями $V = \mathbf{V}(f)$ и $W = \mathbf{V}(g)$. Элементами этого пучка были гиперповерхности $\mathbf{V}(f + cg), c \in k$. Положив $c = 0$, мы получаем, что V является элементом пучка. Однако W, как правило, элементом этого пучка (в том виде, как он был определен) не является. Чтобы сделать W элементом пучка, мы поступим следующим образом.

(a) Пусть (a, b) — однородные координаты в $\mathbb{P}^1(k)$. Докажите, что $\mathbf{V}(af + bg)$ — корректно определенная гиперповерхность в том смысле, что если (a, b) и (c, d) — однородные координаты одной и той же точки в $\mathbb{P}^1(k)$, то многообразия $\mathbf{V}(af + bg)$ и $\mathbf{V}(cf + dg)$ совпадают. Таким образом, мы получили семейство многообразий, параметризованное точками из $\mathbb{P}^1(k)$, которое также называется *пучком* многообразий, определенным многообразиями V и W.

(b) Докажите, что и V, и W содержатся в пучке $\mathbf{V}(af + bg)$.

(c) Пусть $k = \mathbb{C}$. Докажите, что каждая аффинная кривая $\mathbf{V}(f) \subset \mathbb{C}^2$, где f — полином полной степени d, содержится в пучке кривых $\mathbf{V}(aF + bG)$, параметризованном многообразием $\mathbb{P}^1(\mathbb{C})$, где $\mathbf{V}(F)$ является объединением прямых, а степень полинома G строго меньше d. Указание: рассмотрите однородные компоненты полинома f и примените упр. 19.

21. Рассмотрим параметризованную кривую с параметром $t \in k$. Нас интересует ее поведение при $t \to \infty$. Так как $\mathbb{P}^1(k) = k \cup \{\infty\}$, то областью изменений параметра, видимо, должно быть $\mathbb{P}^1(k)$. Вот два примера.

(a) Рассмотрим параметризацию $(x, y) = ((1+t^2)/(1-t^2), 2t/(1-t^2))$ гиперболы $x^2 - y^2 = 1$ в $\mathbb{R}^2$. Чтобы превратить параметризацию в проективную, сначала перейдем к однородным координатам в $\mathbb{P}^2(\mathbb{R})$ и получим

$$((1 + t^2)/(1 - t^2), 2t/(1 - t^2), 1) = (1 + t^2, 2t, 1 - t^2)$$

(см. упр. 3 к § 1). Теперь сделаем t проективным. Если $(a, b) \in \mathbb{P}^1(\mathbb{R})$, то $(1, t) = (1, b/a)$ — координаты той же точки (если $a \neq 0$). Подставим $t = b/a$ в правую часть предыдущего равенства и освободимся от знаменателей. Объясните, почему полученная формула описывает корректно определенное отображение $\mathbb{P}^1(\mathbb{R}) \to \mathbb{P}^2(\mathbb{R})$.

(b) Скрученная кубика в $\mathbb{R}^3$ параметризована с помощью (t, t^2, t^3). Примените метод п. (a) и найдите проективную параметризацию $\mathbb{P}^1(\mathbb{R}) \to \mathbb{P}^3(\mathbb{R})$. Докажите, что образ этого отображения совпадает с многообразием V' из примера 9.

§ 3. Проективный алгебро-геометрический словарь

В этом параграфе мы рассмотрим, что представляет собой проективный алгебро-геометрический словарь. Мы обобщим теоремы из гл. 4 о связях между $\mathbf{V}$ и $\mathbf{I}$ на проективный случай и, в частности, докажем проективный вариант теоремы о нулях.

Отметим сначала различие между аффинным и проективным случаями в алгебраической части словаря. А именно, мы определили проективное многообразие (определение 5 из § 2) как множество общих нулей некоторого набора *однородных* полиномов. Но свойство быть однородным *не* сохраняется при сложении полиномов. Например, если мы сложим два однородных полинома с различными полными степенями, то их сумма *не* будет однородной. Таким образом, идеал $I = \langle f_1, \ldots, f_s \rangle \subset k[x_0, \ldots, x_n]$, порожденный однородными полиномами, будет содержать и *неоднородные* полиномы, которые не годятся для определения проективных многообразий.

Тем не менее каждый элемент из I обращается в нуль на **всех** наборах однородных координат всех точек из $V = \mathbf{V}(f_1, \dots, f_s)$. Это следует из того, что элемент $g \in I$ может быть представлен в виде

$$g = \sum_{j=1}^{s} A_j f_j, \tag{1}$$

где $A_j \in k[x_0, \dots, x_n]$. Подстановка однородных координат какой-либо точки из V в это равенство даст нуль, так как все f_j равны нулю в этой точке.

Более важное замечание связано с однородными компонентами полинома g. Представим каждый полином A_j в виде суммы однородных компонент:

$$A_j = \sum_{i=1}^{d_j} A_{ji}.$$

Если мы подставим эти выражения в (1) и соберем вместе члены одинаковой полной степени, то окажется, что однородные компоненты полинома g также принадлежат I (см. упр. 2).

Таким образом, хотя I и содержит неоднородные полиномы, но он содержит также их однородные компоненты. Это наблюдение приводит к рассмотрению специального класса идеалов в $k[x_0, \dots, x_n]$.

Определение 1. Идеал $I \subset k[x_0, \dots, x_n]$ называется *однородным*, если для любого $f \in I$ его однородные компоненты также принадлежат I.

Большинство идеалов *не* являются однородными. Пусть, например $I = \langle y - x^2 \rangle \subset k[x, y]$. Тогда однородные компоненты полинома f — это $f_1 = y$ и $f_2 = -x^2$. Ни одна из них не принадлежит I, так как элементами идеала I являются полиномы, делящиеся на $y - x^2$, т. е. I неоднороден. Имеются следующие полезные характеристики однородности.

Теорема 2. *Пусть $I \subset k[x_0, \dots, x_n]$ — идеал. Следующие условия эквивалентны:*

(i) *I однороден;*
(ii) *$I = \langle f_1, \dots, f_s \rangle$, где полиномы $f_1, \dots, f_s$ однородны;*
(iii) *редуцированный базис Грёбнера идеала I (по отношению к любому мономиальному упорядочению) состоит из однородных полиномов.*

Доказательство. Доказательство импликации (ii)⇒(i) намечено выше (см. также упр. 2). Докажем (i)⇒(ii). Пусть I однороден.

По теореме Гильберта о базисе $I = \langle F_1, \dots, F_t \rangle$ для некоторых полиномов $F_j \in k[x_0, \dots, x_n]$ (не обязательно однородных). Представим каждый полином F_j в виде суммы однородных компонент, $F_j = \sum_i F_{ji}$. Тогда каждый из F_{ji} лежит в I, так как I однороден. Рассмотрим идеал I', порожденный всеми однородными полиномами F_{ji}. Тогда $I \subset I'$, так как каждый F_j является суммой образующих идеала I'. С другой стороны $I' \subset I$, так как все F_{ji} лежат в I. Это доказывает равенство $I = I'$ и одновременно тот факт, что I имеет базис из однородных полиномов. Наконец, эквивалентность (ii)⇔(iii) будет доказана в упр. 3. □

Теорема 2 позволяет нам по однородному идеалу $I \subset k[x_0, \dots, x_n]$ определить (как и в аффинном случае) множество

$$\mathbf{V}(I) = \{p \in \mathbb{P}^n(k) : f(p) = 0 \text{ для всех } f \in I\},$$

которое является проективным многообразием, как показывает

Предложение 3. *Пусть $I \subset k[x_0, \dots, x_n]$ — однородный идеал, и пусть $I = \langle f_1, \dots, f_s \rangle$, где $f_1, \dots, f_s$ — однородные полиномы. Тогда*

$$\mathbf{V}(I) = \mathbf{V}(f_1, \dots, f_s),$$

так что $\mathbf{V}(I)$ — проективное многообразие.

Доказательство. (Легкое) доказательство этого утверждения мы оставляем читателю в качестве упражнения. □

По проективному многообразию мы можем построить однородный идеал, взяв в качестве базиса определяющие полиномы многообразия. Но есть и другой способ построить однородный идеал по проективному многообразию.

Предложение 4. *Пусть $V \subset \mathbb{P}^n(k)$ — проективное многообразие. Пусть*

$$\mathbf{I}(V) = \{f \in k[x_0, \dots, x_n] : f(a_0, \dots, a_n) = 0 \text{ для всех } (a_0, \dots, a_n) \in V\}.$$

(Это означает, что f обращается в нуль на всех наборах однородных координат всех точек из V.) Тогда, если k бесконечно, то $\mathbf{I}(V)$ является однородным идеалом в $k[x_0, \dots, x_n]$.

Доказательство. Множество $\mathbf{I}(V)$ замкнуто относительно сложения и относительно умножения на элементы из кольца $k[x_0, \dots, x_n]$ (это доказывается точно так же, как и в аффинном случае). Поэтому $\mathbf{I}(V)$ является идеалом. Пусть теперь $f \in \mathbf{I}(V)$. Зафиксируем точку $p \in V$. По условию f обращается в нуль на *всех* наборах $(a_0, \dots, a_n)$ однородных координат точки p. Так как k бесконечно,

то из этого вытекает (см. упр. 7 к § 2), что все однородные компоненты f_i полинома f равны нулю в $(a_0, \ldots, a_n)$. Следовательно, $f_i \in \mathbf{I}(V)$, т. е. идеал $\mathbf{I}(V)$ однороден. □

Теперь у нас есть базовые элементы словаря, описывающего соответствие между проективными многообразиями в $\mathbb{P}^n(k)$ и однородными идеалами в $k[x_0, \ldots, x_n]$. Следующая теорема является проективным обобщением п. (i) теоремы 7 из § 2 гл. 4 (аффинное соответствие идеал—многообразие).

Теорема 5. *Пусть поле k бесконечно. Тогда отображения*

$$\textit{проективные многообразия} \xrightarrow{\mathbf{I}} \textit{однородные идеалы}$$

и

$$\textit{однородные идеалы} \xrightarrow{\mathbf{V}} \textit{проективные многообразия}$$

обращают включения. Кроме того, для любого проективного многообразия

$$\mathbf{V}(\mathbf{I}(V)) = V,$$

так что отображение $\mathbf{I}$ инъективно.

Доказательство. Доказательство этой теоремы аналогично доказательству соответствующей аффинной теоремы. □

В качестве примера использования этой теоремы мы сейчас докажем, что каждое проективное многообразие может быть разложено в объединение неприводимых компонент. Как и в аффинном случае, многообразие $V \subset \mathbb{P}^n(k)$ называется *неприводимым*, если оно не может быть представлено в виде объединения двух строго меньших проективных многообразий.

Теорема 6. *Пусть k — произвольное поле.*

(i) *Рассмотрим убывающую цепь проективных многообразий в $\mathbb{P}^n(k)$*

$$V_1 \supset V_2 \supset V_3 \supset \ldots.$$

Тогда существует целое N, такое, что $V_N = V_{N+1} = \ldots$.

(ii) *Каждое проективное многообразие $V \subset \mathbb{P}^n(k)$ может быть единственным образом* [1] *представлено в виде объединения неприводимых проективных многообразий,*

$$V = V_1 \cup \ldots \cup V_m,$$

где $V_i \not\subset V_j$ при $i \neq j$.

[1] С точностью до перенумерации. — *Прим. ред.*

Доказательство. Так как отображение $\mathbf{I}$ обращает включение, то мы получаем возрастающую цепь однородных идеалов

$$\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \mathbf{I}(V_3) \subset \ldots$$

в $k[x_0, \ldots, x_n]$. Тогда по условию обрыва возрастающих цепей (теорема 7 из § 5 гл. 2) $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \ldots$, начиная с некоторого N. Так как отображение $\mathbf{I}$ имеет левое обратное, то п. (i) доказана.

Как и в аффинном случае, п. (ii) является прямым следствием п. (i) (см. теоремы 2 и 4 из § 6 гл. 4). □

Связи между суммами, произведениями и пересечениями однородных идеалов и соответствующими операциями на множестве проективных многообразий те же, что и в аффинном случае. Мы рассмотрим эти вопросы в упражнениях.

Радикал однородного идеала определяется обычным образом:

$$\sqrt{I} = \{f \in k[x_0, \ldots, x_n] : f^m \in I \text{ для некоторого } m \geq 1\}.$$

Радикал однородного идеала также однороден (как и следовало ожидать).

Предложение 7. *Пусть $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Тогда радикал $\sqrt{I}$ также является однородным идеалом.*

Доказательство. Пусть $f \in \sqrt{I}$. Тогда $f^m \in I$ для некоторого $m \geq 1$. Представим f в виде суммы однородных компонент,

$$f = \sum_i f_i = f_{\max} + \sum_{i<\max} f_i,$$

где $f_{\max}$ — это ненулевая однородная компонента полинома f максимальной полной степени. Легко видеть, что

$$(f^m)_{\max} = (f_{\max})^m.$$

Так как I однороден, то $(f^m)_{\max} \in I$. Следовательно, $(f_{\max})^m \in I$, а значит, $f_{\max} \in \sqrt{I}$.

Положим $g = f - f_{\max} \in \sqrt{I}$. Аналогичные рассуждения показывают, что $g_{\max} \in \sqrt{I}$. Но $g_{\max}$ — это одна из компонент полинома f. Повторяя это рассуждение, мы в конце концов докажем, что все однородные компоненты полинома f принадлежат $\sqrt{I}$. Следовательно, радикал является однородным идеалом. □

Последний раздел алгебро-геометрического словаря описывает соответствие идеал—многообразие для алгебраически замкнутого поля. В этом случае мы ожидаем, что связь между идеалами и многообразиями будет особенно тесной. В аффинном случае основой

такой связи являются две теоремы о нулях, слабая и сильная (гл. 4). Напомним их формулировки. Рассмотрим идеал $I \subset k[x_1, \ldots, x_n]$. Тогда

- (Слабая теорема о нулях) $\mathbf{V}_a(I) = \varnothing$ в $k^n \iff I = k[x_1, \ldots, x_n]$.
- (Сильная теорема о нулях) $\sqrt{I} = \mathbf{I}_a(\mathbf{V}_a(I))$ в $k[x_1, \ldots, x_n]$.

(Чтобы избежать путаницы, мы используем обозначения $\mathbf{I}_a$ и $\mathbf{V}_a$ для указания аффинного случая.)

Естественно спросить, можно ли перенести эти результаты на проективный случай?

Ответ, как ни странно, *отрицательный*. В частности, слабая теорема о нулях не имеет места для некоторых однородных идеалов. Рассмотрим, например, идеал $I = \langle x_0, \ldots, x_n\rangle \subset \mathbb{C}[x_0, \ldots, x_n]$. Тогда многообразие $\mathbf{V}(I) \subset \mathbb{P}^n(\mathbb{C})$ задано уравнениями $x_0 = \ldots = x_n = 0$. Единственным решением этой системы является $(0, \ldots, 0)$, но точки с такими координатами нет в $\mathbb{P}^n(\mathbb{C})$. Следовательно, $\mathbf{V}(I) = \varnothing$, хотя $I \neq \mathbb{C}[x_0, \ldots, x_n]$ (так как $1 \notin I$).

К счастью, $\langle x_0, \ldots, x_n\rangle$ — один из немногих идеалов, для которых $\mathbf{V}(I) = \varnothing$. Следующая версия слабой теоремы о нулях описывает *все* однородные идеалы, для которых соответствующее проективное многообразие пусто.

Теорема 8 (проективная слабая теорема о нулях). *Пусть поле k алгебраически замкнуто и $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Следующие условия эквивалентны:*

(i) *многообразие $\mathbf{V}(I) \subset \mathbb{P}^n(k)$ пусто;*

(ii) *если G — редуцированный базис Грёбнера идеала I (по отношению к некоторому мономиальному упорядочению), то для любого i, $0 \leq i \leq n$, существует $g \in G$, такой, что $\mathrm{LT}(g)$ является неотрицательной степенью переменной x_i;*

(iii) *для любого i, $0 \leq i \leq n$, существует целое $m_i \geq 0$, такое, что $x_i^{m_i} \in I$;*

(iv) *Существует $r \geq 1$, такое, что $\langle x_0, \ldots, x_n\rangle^r \subset I$.*

Доказательство. По идеалу I мы строим проективное многообразие $V = \mathbf{V}(I) \subset \mathbb{P}^n(k)$, а также строим аффинное многообразие $C_V = \mathbf{V}_a(I) \subset k^{n+1}$. Обратите внимание, что для построения C_V используется тот же идеал I, но решения ищутся в аффинном пространстве k^{n+1}. Мы назовем C_V *аффинным конусом* над V. Если мы отождествим точки пространства $\mathbb{P}^n(k)$ с прямыми в k^{n+1}, проходящими через начало координат, то C_V — это объединение прямых, соответствующих точкам из V (см. упр. 16 к § 2). В частности, C_V содержит все наборы однородных координат точек из V.

Докажем, что (ii)⇒(i). Для каждого i базис Грёбнера G идеала I содержит элемент g, такой, что $\mathrm{LT}(g) = x_i^{m_i}$ для некоторого $m_i \geq 0$. Тогда по теореме 6 из § 3 гл. 5 множество C_V конечно. Но если $p \in V$, то *все* однородные координаты точки p принадлежат C_V, т. е. если $p = (a_0, \ldots, a_n)$, то $\lambda(a_0, \ldots, a_n) \in C_V$ при $0 \neq \lambda \in k$. Но k алгебраически замкнуто, а следовательно, бесконечно. Противоречие показывает, что $V = \mathbf{V}(I) = \varnothing$.

Докажем, что (iii)⇒(ii). Пусть G — редуцированный базис Грёбнера идеала I. Если $x_i^{m_i} \in I$, то найдется элемент $g \in G$, такой, что его старший член делит $x_i^{m_i}$, т. е. $\mathrm{LT}(g)$ является степенью переменной x_i.

Импликация (iv)⇒(iii) очевидна, так как из $\langle x_0, \ldots, x_n\rangle^r \subset I$ следует, что $x_i^r \in I$ для всех i.

Осталось доказать, что (i)⇒(iv). Отметим, что из условия $V = \varnothing$ вытекает, что

$$C_V \subset \{(0, \ldots, 0)\} \subset k^{n+1}.$$

(В самом деле, если C_V содержит ненулевую точку $(a_0, \ldots, a_n)$, то точка $p \in \mathbb{P}^n(k)$ с однородными координатами $(a_0, \ldots, a_n)$ принадлежит V.) Тогда

$$\mathbf{I}_a(\{(0, \ldots, 0)\}) \subset \mathbf{I}_a(C_V).$$

Мы знаем, что $\mathbf{I}_a(\{(0, \ldots, 0)\}) = \langle x_0, \ldots, x_n\rangle$ (см. упр. 7 к § 5 гл. 4). Тогда по аффинной сильной теореме о нулях $\mathbf{I}_a(C_V) = \mathbf{I}_a(\mathbf{V}_a(I)) = \sqrt{I}$ (так как k алгебраически замкнуто). Следовательно,

$$\langle x_0, \ldots, x_n\rangle \subset \sqrt{I}.$$

Но в упр. 12 к § 3 гл. 4 было доказано, что если некоторый идеал содержится в $\sqrt{I}$, то некоторая степень этого идеала содержится в I. Это и завершает доказательство теоремы. □

Пункт (ii) позволяет построить алгоритм решения задачи о непустоте проективного многообразия (заданного однородным идеалом) над алгебраически замкнутым полем. В упр. 10 мы рассмотрим другие условия пустоты многообразия $\mathbf{V}(I)$ в $\mathbb{P}^n(k)$.

Исключая идеалы, описанные в теореме 8, из рассмотрения, мы получаем проективную версию теоремы о нулях.

Теорема 9 (проективная сильная теорема о нулях). *Пусть поле k алгебраически замкнуто, а I — однородный идеал в $k[x_0, \ldots, x_n]$. Если многообразие $V = \mathbf{V}(I)$ непусто, то*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Доказательство. Как и в доказательстве теоремы 8, мы будем одновременно рассматривать два многообразия: проективное многообразие $V = \mathbf{V}(I) \subset \mathbb{P}^n(k)$ и его аффинный конус $C_V = \mathbf{V}_a(I) \subset k^{n+1}$. Мы утверждаем, что

$$\mathbf{I}_a(C_V) = \mathbf{I}(V), \tag{2}$$

если $V \neq \varnothing$. В самом деле, пусть $f \in \mathbf{I}_a(C_V)$. Если $p \in V$, то все наборы однородных координат точки p принадлежат C_V. Поэтому f обращается в нуль на всех наборах однородных координат точки p. Значит, $f \in \mathbf{I}(V)$ по определению. Пусть теперь $f \in \mathbf{I}(V)$. Так как координаты любой ненулевой точки из C_V являются однородными координатами некоторой точки многообразия V, то f равен нулю на $C_V - \{0\}$. Осталось показать, что f равен нулю в нуле. Так как $\mathbf{I}(V)$ — однородный идеал, то f_i — однородные компоненты полинома f — принадлежат $\mathbf{I}(V)$ и, следовательно, равны нулю на V. В частности, это справедливо и для постоянного члена f_0 — однородной компоненты полной степени 0. Так как $V \neq \varnothing$, то $f_0 = 0$; следовательно, f равен нулю в начале координат и $f \in \mathbf{I}_a(C_V)$. Утверждение (2) доказано.

По аффинной сильной теореме о нулях $\sqrt{I} = \mathbf{I}_a(\mathbf{V}_a(I))$. Тогда из (2) следует, что

$$\sqrt{I} = \mathbf{I}_a(\mathbf{V}_a(I)) = \mathbf{I}_a(C_V) = \mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)).$$

Доказательство теоремы закончено. □

Теорема о нулях позволяет завершить описание соответствия идеал—многообразие, начатое в теореме 5. Радикальный однородный идеал в $k[x_0, \ldots, x_n]$ — это однородный идеал, удовлетворяющий условию $\sqrt{I} = I$. Как и в аффинном случае, существует взаимно однозначное соответствие между проективными многообразиями и радикальными однородными идеалами при условии, что идеалы вида $\sqrt{I} = \langle x_0, \ldots, x_n \rangle$ и $\sqrt{I} = \langle 1 \rangle$ не рассматриваются.

Теорема 10. *Пусть поле k алгебраически замкнуто. Мы будем рассматривать непустые проективные многообразия и однородные радикальные идеалы, строго содержащиеся в $\langle x_0, \ldots, x_n \rangle$. В этих условиях отображения*

$$\left\{\begin{array}{c}\textit{непустые проективные}\\ \textit{многообразия}\end{array}\right\} \xrightarrow{\ \mathbf{I}\ } \left\{\begin{array}{c}\textit{радикальные}\\ \textit{однородные идеалы,}\\ \textit{строго содержащиеся в}\\ \langle x_0, \ldots, x_n \rangle\end{array}\right\}$$

и

$$\left\{\begin{array}{c}\textit{радикальные}\\ \textit{однородные идеалы,}\\ \textit{строго содержащиеся в}\\ \langle x_0, \ldots, x_n \rangle\end{array}\right\} \xrightarrow{\ \mathbf{V}\ } \left\{\begin{array}{c}\textit{непустые проективные}\\ \textit{многообразия}\end{array}\right\}$$

взаимно обратны и являются биекциями, обращающими включение.

Доказательство. Из теоремы 8 следует, что если I — радикальный однородный идеал и $\mathbf{V}(I) = \varnothing$, то $I = \langle x_0, \ldots, x_n \rangle$ или $I = k[x_0, \ldots, x_n]$ (см. упр. 10). Кроме того, если I — радикальный однородный идеал и $I \neq k[x_0, \ldots, x_n]$, то $I \subset \langle x_0, \ldots, x_n \rangle$ (см. упр. 9).

Эти замечания показывают, что если I — радикальный однородный идеал и $\mathbf{V}(I) \neq \varnothing$, то $I \subsetneq \langle x_0, \ldots, x_n \rangle$. Теперь теорема следует из теоремы 9. □

Соответствие между *неприводимыми* проективными многообразиями и однородными *простыми* идеалами будет рассмотрено в упражнениях.

Упражнения к § 3

1. В этом упражнении мы элементарными методами решим задачу об условиях однородности главного идеала $I = \langle f \rangle$.
   (a) Не используя теорему 2, докажите, что идеал $I = \langle x^2y - x^3 \rangle$ однороден в $k[x, y]$. Указание: каждый элемент из I имеет вид $g = A \cdot (x^2y - x^3)$; представьте A в виде суммы однородных компонент и используйте это представление для нахождения однородных компонент полинома g.
   (b) Не используя теорему 2, докажите, что идеал $\langle f \rangle \subset k[x_0, \ldots, x_n]$ однороден в том и только том случае, когда f — однородный полином.

2. В этом упражнении мы рассмотрим некоторые полезные свойства однородных компонент полинома.
   (a) Пусть $f = \sum_i f_i$ и $g = \sum_i g_i$ — представления полиномов f и g в виде сумм однородных компонент. Докажите, что $f = g$ в том и только том случае, когда $f_i = g_i$ для всех i.
   (b) В условиях п. (a) докажите, что однородными компонентами полинома $h = fg$ являются $h_m = \sum_{i+j=m} f_i g_j$.
   (c) Используя пп. (a) и (b), дайте строгое доказательство (намеченное в тексте параграфа) импликации (ii)⇒(i) из теоремы 2.

3. В этом упражнении мы рассмотрим работу алгоритма деления в случае однородных полиномов.

(a) Предположим, что мы делим однородный полином f на однородные полиномы $f_1, \ldots, f_s$. В результате деления мы получаем выражение вида $f = a_1 f_1 + \ldots + a_s f_s + r$. Докажите, что $a_1, \ldots, a_s, r$ — однородные полиномы (или нули). Чему равна полная степень полинома r?

(b) Докажите, что если f, g однородны, то S-полином $S(f, g)$ тоже однороден.

(c) Анализируя работу алгоритма Бухбергера, докажите, что однородный идеал имеет однородный базис Грёбнера.

(d) Докажите эквивалентность (ii)⇔(iii) в теореме 2.

4. Предположим, что базис Грёбнера G идеала $I \subset k[x_0, \ldots, x_n]$ состоит из однородных полиномов.

(a) Докажите, что G является базисом Грёбнера по отношению к lex-упорядочению в том и только том случае, когда он является базисом Грёбнера по отношению к grlex-упорядочению (при условии, что порядок переменных один и тот же).

(b) Докажите, что редуцированные базисы Грёбнера однородного идеала по отношению к lex- и grlex-упорядочениям совпадают.

5. Докажите предложение 3.

6. В этом упражнении мы рассмотрим алгебраические операции на множестве идеалов (см. гл. 4) в однородном случае. Пусть $I_1, \ldots, I_m$ — однородные идеалы в $k[x_0, \ldots, x_n]$.

(a) Докажите, что сумма идеалов $I_1 + \ldots + I_m$ однородна. Указание: примените теорему 2.

(b) Докажите, что пересечение идеалов $I_1 \cap \ldots \cap I_m$ однородно.

(c) Докажите, что произведение идеалов $I_1 \ldots I_m$ однородно.

7. Связь между алгебраическими операциями на множестве однородных идеалов и соответствующими операциями на проективных многообразиях такая же, как и в аффинном случае. Пусть $I_1, \ldots, I_m$ — однородные идеалы в $k[x_0, \ldots, x_n]$, а $V_i = \mathbf{V}(I_i)$ — соответствующие проективные многообразия в $\mathbb{P}^n(k)$.

(a) Докажите, что $\mathbf{V}(I_1 + \ldots + I_m) = \bigcap_{i=1}^m V_i$.

(b) Докажите, что $\mathbf{V}(I_1 \cap \ldots \cap I_m) = \mathbf{V}(I_1 \ldots I_m) = \bigcup_{i=1}^m V_i$.

8. Пусть $f_1, \ldots, f_s$ — однородные полиномы полных степеней $d_1 < d_2 \leq \ldots \leq d_s$, и пусть $I = \langle f_1, \ldots, f_s \rangle \subset k[x_0, \ldots, x_n]$.

(a) Предположим, что однородный полином g полной степени d_1 принадлежит I; тогда g равен f_1 с точностью до постоянного множителя. Указание: примените пп. (a) и (b) упр. 2.

(b) Пусть g — однородный полином полной степени d и $g \in I$; тогда $g \in I_d = \langle f_i : \deg(f_i) \leq d \rangle \subset I$.

9. В этом упражнении мы изучим некоторые свойства идеала $I_0 = \langle x_0, \ldots, x_n \rangle \subset k[x_0, \ldots, x_n]$.

(a) Докажите, что каждый собственный однородный идеал из $k[x_0, \ldots, x_n]$ содержится в I_0.

(b) Докажите, что r-я степень I_0^r порождена множеством всех мономов из $k[x_0, \ldots, x_n]$ полной степени r. Докажите, что каждый однородный полином полной степени $\geq r$ содержится в I_0^r.

(c) Пусть $V = \mathbf{V}(I_0) \subset \mathbb{P}^n(k)$ и $C_V = \mathbf{V}_a(I_0) \subset k^{n+1}$. Докажите, что $\mathbf{I}_a(C_V) \neq \mathbf{I}(V)$, и объясните, почему этот факт не противоречит равенству (2).

10. Пусть поле k алгебраически замкнуто, а $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Докажите, что равенство $\mathbf{V}(I) = \varnothing$ в $\mathbb{P}^n(k)$ равносильно любому из двух следующих условий:

(i) существует число $r \geq 1$, такое, что каждый однородный полином полной степени $\geq r$ содержится в I;

(ii) радикал идеала I равен или $\langle x_0, \ldots, x_n \rangle$, или $k[x_0, \ldots, x_n]$.

Указание: в случае (i) примените упр. 9, а в случае (ii) примените теорему 8 и докажите, что $\langle x_0, \ldots, x_n \rangle \subset \sqrt{I}$.

11. Однородный идеал называется *простым*, если он прост как идеал в $k[x_0, \ldots, x_n]$.

(a) Докажите, что однородный идеал $I \subset k[x_0, \ldots, x_n]$ прост в том и только том случае, когда из того, что произведение $F \cdot G$ двух *однородных* полиномов F, G принадлежит I, следует, что $F \in I$ или $G \in I$.

(b) Пусть I — однородный идеал. Докажите, что проективное многообразие $\mathbf{V}(I)$ неприводимо в том и только том случае, когда I прост. Докажите, что в случае, когда I радикален, имеет место и обратное утверждение, т. е. I прост, если многообразие $\mathbf{V}(I)$ неприводимо. Указание: проанализируйте доказательство аналогичного утверждения в аффинном случае (предложение 3 из § 5 гл. 4).

(c) Пусть поле k алгебраически замкнуто. Докажите, что отображения $\mathbf{V}$ и $\mathbf{I}$ индуцируют взаимно однозначное соответствие между множеством однородных простых идеалов в $k[x_0, \ldots, x_n]$, которые строго содержатся в $\langle x_0, \ldots, x_n \rangle$, и множеством непустых неприводимых проективных многообразий в $\mathbb{P}^n(k)$.

12. Докажите, что однородный простой идеал в $k[x_0, \ldots, x_n]$ радикален.

§ 4. Проективное замыкание аффинного многообразия

В § 2 мы показали, что любое аффинное многообразие может рассматриваться как аффинная часть некоторого проективного многообразия. Так как такое проективное многообразие может быть построено несколькими способами (см. упр. 9 к § 2), то было бы желательно найти *наименьшее* проективное многообразие, содержащее данное аффинное. Как мы увидим, существует алгоритм построения такого многообразия.

Пусть $x_0, \ldots, x_n$ — однородные координаты на $\mathbb{P}^n(k)$, и рассмотрим подмножество $U_0 \subset \mathbb{P}^n(k)$, определенное условием $x_0 \neq 0$. Мы отождествим U_0 с k^n (см. предложение 2 из § 2) и будем считать $x_1, \ldots, x_n$ координатами на k^n. Как и в § 3, мы будем использовать обозначения $\mathbf{I}_a$ и $\mathbf{V}_a$ для аффинных вариантов отображений $\mathbf{I}$ и $\mathbf{V}$.

Сначала рассмотрим, как гомогенизировать идеал $I \subset k[x_1, \ldots, x_n]$ и получить однородный идеал $I^h \subset k[x_0, \ldots, x_n]$.

Определение 1. Пусть I — некоторый идеал в $k[x_1, \ldots, x_n]$. *Гомогенизацией* идеала I называется идеал

$$I^h = \langle f^h : f \in I \rangle \subset k[x_0, \ldots, x_n],$$

где f^h — гомогенизация полинома f (см. предложение 7 из § 2).

Справедливо следующее естественное утверждение.

Предложение 2. *Гомогенизация I^h произвольного идеала $I \subset k[x_1, \ldots, x_n]$ является однородным идеалом в $k[x_0, \ldots, x_n]$.*

Доказательство. См. упр. 1.

Определение 1 не вполне удовлетворительно, так как оно не дает нам *конечного* множества образующих идеала I^h. Однако получить его не так-то просто. Пусть $I = \langle f_1, \ldots, f_s \rangle$. Естественно ожидать, что $I^h = \langle f_1^h, \ldots, f_s^h \rangle$, но это не так! Идеал I^h может быть *строго больше* идеала $\langle f_1^h, \ldots, f_s^h \rangle$.

Пример 3. Рассмотрим идеал $I = \langle f_1, f_2 \rangle = \langle x_2 - x_1^2, x_3 - x_1^3 \rangle$ скрученной кубики в $\mathbb{R}^3$. Гомогенизируя f_1, f_2, мы получаем идеал $J = \langle x_0 x_2 - x_1^2, x_0^2 x_3 - x_1^3 \rangle \subset \mathbb{R}[x_0, x_1, x_2, x_3]$. Мы утверждаем, что $J \neq I^h$. Чтобы доказать это, рассмотрим полином

$$f_3 = f_2 - x_1 f_1 = x_3 - x_1^3 - x_1(x_2 - x_1^2) = x_3 - x_1 x_2 \in I.$$

Тогда $f_3^h = x_0 x_3 - x_1 x_2$ является однородным полиномом степени 2 в I^h. Так как образующие идеала J однородны степеней 2 и 3, то, если $f_3^h = A_1 f_1^h + A_2 f_2^h$, разлагая A_1, A_2 на однородные компоненты, мы получим, что f_3^h равен f_1^h с точностью до постоянного множителя (см. упр. 8 к § 3). Но это, очевидно, не так; поэтому $f_3^h \notin J$ и $J \neq I^h$.

Как же тогда найти конечное множество образующих для I^h? Ответ дает следующая теорема. Напомним, что мономиальное упорядочение кольца $k[x_1, \ldots, x_n]$ называется *градуированным*, если сначала сравниваются полные степени мономов, т. е.

$$x^\alpha > x^\beta, \text{ если } |\alpha| > |\beta|.$$

Отметим, что grlex и grevlex — это градуированные упорядочения, в то время как lex — нет.

Теорема 4. *Рассмотрим идеал $I \subset k[x_1, \ldots, x_n]$, и пусть $G = \{g_1, \ldots, g_s\}$ является его базисом Грёбнера по отношению к градуированному мономиальному упорядочению в $k[x_1, \ldots, x_n]$. Тогда $G^h = \{g_1^h, \ldots, g_s^h\}$ является базисом идеала $I^h \subset k[x_0, \ldots, x_n]$.*

Доказательство. Мы докажем более сильное утверждение, что G^h является даже базисом Грёбнера идеала I^h по отношению к некоторому мономиальному упорядочению на $k[x_0, \ldots, x_n]$, которое мы сейчас определим.

Каждый моном в $k[x_0, \ldots, x_n]$ может быть записан в виде

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} x_0^d = x^\alpha x_0^d,$$

где x^α не делится на x_0. Мы продолжим градуированное мономиальное упорядочение $>$ на $k[x_1, \ldots, x_n]$ до мономиального упорядочения $>_h$ на $k[x_0, \ldots, x_n]$ следующим образом:

$$x^\alpha x_0^d >_h x^\beta x_0^e \iff x^\alpha > x^\beta \text{ или } x^\alpha = x^\beta \text{ и } d > e.$$

В упр. 2 будет доказано, что это правило действительно задает мономиальное упорядочение на $k[x_0, \ldots, x_n]$. Обратите внимание, что $x_i >_h x_0$ при любом $i > 0$.

Важное для нас свойство упорядочения $>_h$ доказывается в следующей лемме.

Лемма 5. *Пусть $f \in k[x_1, \ldots, x_n]$ и $>$ — градуированное упорядочение на $k[x_1, \ldots, x_n]$. Тогда*

$$\mathrm{LM}_{>_h}(f^h) = \mathrm{LM}_>(f).$$

Доказательство. Так как $>$ — градуированное упорядочение, то $\mathrm{LM}_>(f)$ — один из мономов x^α, содержащихся в однородной компоненте полинома f *максимальной* полной степени. При гомогенизации этот член не меняется. Если $x^\beta x_0^e$ — один из мономов в f^h, то $\alpha > \beta$. По определению $>_h$ из этого следует, что $x^\alpha >_h x^\beta x_0^e$. Значит, $x^\alpha = \mathrm{LM}_{>_h}(f^h)$. Лемма доказана. □

Теперь мы докажем, что G^h является базисом Грёбнера идеала I^h по отношению к мономиальному упорядочению $>_h$. Каждый полином g_i^h принадлежит I^h по определению. Значит, достаточно доказать, что $\mathrm{LT}_{>_h}(G^h)$ порождает идеал старших членов $\langle \mathrm{LT}_{>_h}(I^h) \rangle$. Пусть $F \in I^h$. Так как I^h однороден, то каждая однородная компонента полинома F принадлежит I^h; следовательно, мы можем

считать полином F однородным. Тогда

$$F = \sum_j A_j f_j^h, \tag{1}$$

где $A_j \in k[x_0, \ldots, x_n]$, а $f_j \in I$. Обозначим через $f = F(1, x_1, \ldots, x_n)$ дегомогенизацию полинома F. Полагая $x_0 = 1$ в (1), получаем

$$\begin{aligned} f = F(1, x_1, \ldots, x_n) &= \sum_j A_j(1, x_1, \ldots, x_n) f_j^h(1, x_1, \ldots, x_n) \\ &= \sum_j A_j(1, x_1, \ldots, x_n) f_j, \end{aligned}$$

так как $f_j^h(1, x_1, \ldots, x_n) = f_j(x_1, \ldots, x_n)$ (п. (iii) предложения 7 из § 2). Таким образом, $f \in I \subset k[x_1, \ldots, x_n]$. По п. (iv) предложения 7 из § 2

$$F = x_0^e \cdot f^h$$

для некоторого $e \geq 0$. Поэтому

$$\mathrm{LM}_{>_h}(F) = x_0^e \cdot \mathrm{LM}_{>_h}(f^h) = x_0^e \cdot \mathrm{LM}_{>}(f), \tag{2}$$

где последнее равенство следует из леммы 5. Так как G является базисом Грёбнера идеала I, то $\mathrm{LM}_{>}(f)$ делится на некоторый старший моном $\mathrm{LM}_{>}(g_i) = \mathrm{LM}_{>_h}(g_i^h)$. Теперь из (2) следует, что $\mathrm{LM}_{>_h}(F)$ делится на $\mathrm{LM}_{>_h}(g_i^h)$, что и требовалось доказать. □

В упр. 5 будет показано, что в случае grevlex-упорядочения теорема 4 имеет более элегантную формулировку.

Рассмотрим пример. Пусть $I = \langle x_2 - x_1^2, x_3 - x_1^3 \rangle$ — идеал аффинной скрученной кубики $W \subset \mathbb{R}^3$. Базис Грёбнера для I по отношению к grevlex-упорядочению имеет вид

$$G = \{x_1^2 - x_2, x_1 x_2 - x_3, x_1 x_3 - x_2^2\}.$$

По теореме 4 гомогенизация этих полиномов порождает I^h. Тогда

$$I^h = \langle x_1^2 - x_0 x_2, x_1 x_2 - x_0 x_3, x_1 x_3 - x_2^2 \rangle. \tag{3}$$

Отметим, что этот идеал задает проективное многообразие $V' = \mathbf{V}(I^h) \subset \mathbb{P}^3(\mathbb{R})$, которое мы нашли в примере 9 из § 2.

Остаток этого параграфа мы посвятим обсуждению геометрического смысла процедуры гомогенизации идеала. Сначала мы изучим, что происходит при гомогенизации идеала $\mathbf{I}_a(W)$ всех полиномов, обращающихся в нуль на аффинном многообразии W.

Определение 6. Рассмотрим аффинное многообразие $W \subset k^n$[1]. Его *проективным замыканием* называется проективное многообразие $\overline{W} = \mathbf{V}(\mathbf{I}_a(W)^h) \subset \mathbb{P}^n(k)$, где $\mathbf{I}_a(W)^h \subset k[x_0, \ldots, x_n]$ — гомогенизация идеала $\mathbf{I}_a(W) \subset k[x_1, \ldots, x_n]$ (см. определение 1).

Важные свойства проективного замыкания доказываются в следующей теореме.

Теорема 7. *Пусть $W \subset k^n$ — аффинное многообразие, а $\overline{W} \subset \mathbb{P}^n(k)$ — его проективное замыкание. Тогда*

(i) $\overline{W} \cap U_0 = \overline{W} \cap k^n = W$;

(ii) *$\overline{W}$ является наименьшим проективным многообразием в $\mathbb{P}^n(k)$, содержащим W;*

(iii) *если W неприводимо, то $\overline{W}$ также неприводимо;*

(iv) *$\overline{W}$ не имеет неприводимых компонент, принадлежащих бесконечно удаленной гиперплоскости $\mathbf{V}(x_0) \subset \mathbb{P}^n(k)$.*

Доказательство. (i) Пусть G является базисом Грёбнера идеала $\mathbf{I}_a(W)$ по отношению к градуированному упорядочению на $k[x_1, \ldots, x_n]$. Тогда (теорема 4) $\mathbf{I}_a(W)^h = \langle g^h : g \in G \rangle$. Мы знаем, что, положив $x_0 = 1$, мы отождествляем k^n с подмножеством $U_0 \subset \mathbb{P}^n(k)$. Таким образом,

$$\overline{W} \cap U_0 = \mathbf{V}(g^h : g \in G) \cap U_0 = \mathbf{V}_a(g^h(1, x_1, \ldots, x_n) : g \in G).$$

Так как $g^h(1, x_1, \ldots, x_n) = g$ (п. (iii) предложения 7 из § 2), то $\overline{W} \cap U_0 = W$.

(ii) Пусть V — некоторое проективное многообразие, содержащее W. Мы должны доказать, что $\overline{W} \subset V$. Пусть $V = \mathbf{V}(F_1, \ldots, F_s)$. Полином F_i равен нулю на V; следовательно, его дегомогенизация $f_i = F_i(1, x_1, \ldots, x_n)$ обращается в нуль на W, т. е. $f_i \in \mathbf{I}_a(W)$ и, значит, $f_i^h \in \mathbf{I}_a(W)^h$. Таким образом, f_i^h обращается в нуль на $\overline{W}$, но тогда в силу п. (iv) предложения 7 из § 2 $F_i = x_0^{e_i} f_i^h$ для некоторого e_i и F_i обращается в нуль на $\overline{W}$. Таким образом, $\overline{W} \subset V$.

Доказательство п. (iii) мы оставляем читателю в качестве упражнения. Докажем (iv). Пусть $\overline{W} = V_1 \cup \ldots \cup V_m$ — разложение многообразия $\overline{W}$ в объединение неприводимых компонент, и пусть, например, компонента V_1 содержится в бесконечно удаленной ги-

[1] Здесь k^n отождествляется с подмножеством U_0 проективного пространства $\mathbb{P}^n(k)$. — *Прим. ред.*

перплоскости $\mathbf{V}(x_0)$. Тогда

$$\begin{aligned} W = \overline{W} \cap U_0 &= (V_1 \cup \ldots \cup V_m) \cap U_0 \\ &= (V_1 \cap U_0) \cup ((V_2 \cup \ldots \cup V_m) \cap U_0) \\ &= (V_2 \cup \ldots \cup V_m) \cap U_0. \end{aligned}$$

Поэтому $V_2 \cup \ldots \cup V_m$ является проективным многообразием, содержащим W. Тогда из минимальности многообразия $\overline{W}$ следует, что $\overline{W} = V_2 \cup \ldots \cup V_m$ и что $V_1 \subset V_2 \cup \ldots \cup V_m$. Но это невозможно, так как V_1 — неприводимая компонента многообразия $\overline{W}$ (объясните это). Утверждение (iv) доказано. □

В качестве примера применения проективного замыкания рассмотрим скрученную кубику $W \subset \mathbb{R}^3$. В § 4 гл. 1 было доказано, что

$$\mathbf{I}_a(W) = \langle x_2 - x_1^2, x_3 - x_1^3 \rangle.$$

По (3)

$$\mathbf{I}_a(W)^h = \langle x_1^2 - x_0x_2, x_1x_2 - x_0x_3, x_1x_3 - x_2^2 \rangle.$$

Значит, многообразие $V' = \mathbf{V}(x_1^2 - x_0x_2, x_1x_2 - x_0x_3, x_1x_3 - x_2^2)$ из примера 9 § 2 является проективным замыканием скрученной кубики.

Основным недостатком определения проективного замыкания является то, что мы должны работать с идеалом $\mathbf{I}_a(W)$. Было бы гораздо удобнее искать проективное замыкание, исходя из *любого* идеала, определяющего W. Если поле k алгебраически замкнуто, то это можно сделать.

Теорема 8. *Пусть поле k алгебраически замкнуто, а $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Тогда $\mathbf{V}(I^h) \subset \mathbb{P}^n(k)$ является проективным замыканием многообразия $\mathbf{V}_a(I) \subset k^n$.*

Доказательство. Пусть $W = \mathbf{V}_a(I) \subset k^n$, а $Z = \mathbf{V}(I^h) \subset \mathbb{P}^n(k)$. Тогда из теоремы 4 и п. (i) предложения 7 следует, что Z содержит W.

Докажем, что Z является наименьшим проективным многообразием, содержащим W. Мы будем рассуждать, как при доказательстве п. (ii) предложения 7. Пусть $V = \mathbf{V}(F_1, \ldots, F_s)$ — какое-либо проективное многообразие, содержащее W. Тогда дегомогенизация $f_i = F_i(1, x_1, \ldots, x_n)$ принадлежит $\mathbf{I}_a(W)$. Так как k алгебраически замкнуто, то по теореме о нулях $\mathbf{I}_a(W) = \sqrt{I}$; поэтому $f_i^m \in I$ для некоторого m. Значит,

$$(f_i^m)^h \in I^h$$

и, следовательно, $(f_i^m)^h$ обращается в нуль на Z. В упражнениях будет доказано, что

$$(f_i^m)^h = (f_i^h)^m,$$

а значит, f_i^h обращается в нуль на Z. Но $F_i = x_0^{e_i} f_i^h$; поэтому F_i равен нулю на Z. Как и в предложении 7, заключаем, что $Z \subset V$.

Мы доказали, что Z является наименьшим проективным многообразием, содержащим W, а так как и многообразие $\overline{W}$ обладает этим свойством, то $Z = \overline{W}$. □

Теоремы 4 и 8 позволяют построить *алгоритм вычисления проективного замыкания аффинного многообразия* над алгебраически замкнутым полем k: если $W \subset k^n$ задано как множество нулей полиномов $f_1 = \ldots = f_s = 0$, то нужно вычислить базис Грёбнера G идеала $\langle f_1, \ldots, f_s \rangle$ по отношению к какому-либо градуированному упорядочению, и тогда проективное замыкание многообразия W в $\mathbb{P}^n(k)$ есть множество нулей однородных полиномов g^h для $g \in G$.

К сожалению, теорема 8 перестает быть справедливой над полями, которые не являются алгебраически замкнутыми. Рассмотрим пример.

Пример 9. Пусть $I = \langle x_1^2 + x_2^4 \rangle \subset \mathbb{R}[x_1, x_2]$. Тогда $W = \mathbf{V}_a(I) = \{(0,0)\} \subset \mathbb{R}^2$. Следовательно, его проективное замыкание состоит из одной точки, $\overline{W} = \{(1,0,0)\} \subset \mathbb{P}^2(\mathbb{R})$ (так как очевидно, что $\{(1,0,0)\}$ является наименьшим проективным многообразием, содержащим W). С другой стороны, $I^h = \langle x_0^2x_1^2 + x_2^2 \rangle$, и легко проверить, что

$$\mathbf{V}(I^h) = \{(1,0,0), (0,1,0)\} \subset \mathbb{P}^2(\mathbb{R}).$$

Таким образом, многообразие $\mathbf{V}(I^h)$ строго больше проективного замыкания многообразия $W = \mathbf{V}_a(I)$.

Упражнения к § 4

1. Докажите предложение 2.
2. Докажите, что упорядочение $>_h$, определенное в доказательстве теоремы 4, является мономиальным упорядочением на $k[x_0, \ldots, x_n]$. Указание: это может быть сделано непосредственно или с помощью теории смешанных упорядочений из упр. 10 к § 4 гл. 2.
3. Приведите пример, показывающий, что теорема 4 *не верна*, если используется произвольное мономиальное упорядочение в $k[x_1, \ldots, x_n]$. Указание: рассмотрите идеал аффинной скрученной кубики и найдите его базис Грёбнера по отношению к неградуированному упорядочению.
4. Пусть $>$ — градуированное мономиальное упорядочение на $k[x_1, \ldots, x_n]$, а $>_h$ — упорядочение, определенное в теореме 4. Мы доказали, что если G является базисом Грёбнера идеала $I \subset k[x_1, \ldots, x_n]$ по отношению к $>$, то G^h является базисом Грёбнера идеала I^h по отноше-

нию к $>_h$. В этом упражнении мы рассмотрим другие мономиальные упорядочения на $k[x_0,\dots,x_n]$, обладающие этим свойством.

(a) Определим градуированный вариант упорядочения $>_h$, полагая

$$x^\alpha x_0^d >_{gh} x^\beta x_0^e \Longleftrightarrow |\alpha|+d > |\beta|+e$$
$$\text{или } |\alpha|+d = |\beta|+e \text{ и } x^\alpha x_0^d >_h x^\beta x_0^e.$$

Докажите, что G^h является базисом Грёбнера по отношению к $>_{gh}$.

(b) Пусть теперь $>'$ — мономиальное упорядочение на $k[x_0,\dots,x_n]$, которое совпадает с $>$ на $k[x_1,\dots,x_n]$ и обладает следующим свойством: для мономов одинаковой степени моном, содержащий x_0, больше любого монома, содержащего только $x_1,\dots,x_n$. Докажите, что G^h является базисом Грёбнера по отношению к $>'$.

5. Обозначим через $>$ grevlex-упорядочение в кольце $S = k[x_1,\dots,x_n, x_{n+1}]$. Пусть $R = k[x_1,\dots,x_n] \subset S$. Если $f \in R$, то через f^h мы обозначим гомогенизацию полинома f по отношению к переменной x_{n+1}.

(a) Пусть $f \in R$. Докажите, что $\mathrm{LT}_>(f) = \mathrm{LT}_>(f^h)$.

(b) Используя п. (a), докажите, что если G является базисом Грёбнера идеала $I \subset R$ по отношению к $>$, то G^h является базисом Грёбнера идеала $I^h \subset S$ по отношению к $>$.

6. Пусть $f, g \in k[x_1,\dots,x_n]$. Докажите, что

$$(fg)^h = f^h g^h,$$
$$(f^m)^h = (f^h)^m \text{ для любого целого } m \geq 0.$$

Указание: используйте формулу из п. (ii) предложения 7 из § 2.

7. Докажите, что идеал $I \subset k[x_1,\dots,x_n]$ прост в том и только том случае, когда идеал I^h прост в $k[x_0,\dots,x_n]$. Указание: для доказательства импликации $\Rightarrow$ примените п. (a) упр. 10 к § 3, а для доказательства $\Leftarrow$ примените упр. 6.

8. Используя доказательство п. (ii) предложения 7, докажите, что $\mathbf{I}(\overline{W}) = \mathbf{I}_a(W)^h$ для любого аффинного многообразия W.

9. Докажите, что аффинное многообразие W неприводимо в том и только том случае, когда его проективное замыкание $\overline{W}$ неприводимо.

10. Пусть $W = V_1 \cup \dots \cup V_m$ — разложение проективного многообразия в объединение неприводимых компонент, причем V_i не является подмногообразием в V_j при $i \neq j$. Докажите, что V_1 не принадлежит $V_2 \cup \dots \cup V_m$.

В упр. 11–14 мы рассмотрим несколько интересных многообразий в проективном пространстве. Для краткости мы будем писать $\mathbb{P}^n$ вместо $\mathbb{P}^n(k)$. Поле k мы будем считать алгебраически замкнутым, так что теорема 8 применима.

11. Скрученная кубика, которая часто фигурировала в примерах и упражнениях, является членом бесконечного семейства *рациональных нормальных кривых*. Рациональная нормальная кривая в k^n — это образ полиномиальной параметризованной кривой $\phi : k \to k^n$,

$$\phi(t) = (t, t^2, t^3, \dots, t^n).$$

Мы знаем (см. гл. 3), что рациональные нормальные кривые являются аффинными многообразиями. Их проективные замыкания в $\mathbb{P}^n$ также называются рациональными нормальными кривыми.

(a) Найдите аффинные уравнения для рациональных нормальных кривых в k^4 и k^5.

(b) Гомогенизируйте уравнения кривых из п. (a) и рассмотрите проективные многообразия, определенные полученными однородными полиномами. Определяют ли полученные уравнения проективные замыкания соответствующих аффинных кривых? Содержат ли соответствующие проективные многообразия дополнительные компоненты на бесконечности?

(c) Используя теоремы 4 и 8, найдите однородные уравнения, определяющие проективные замыкания этих рациональных нормальных кривых в $\mathbb{P}^4$ и в $\mathbb{P}^5$. Увидели ли вы здесь какую-либо закономерность?

(d) Докажите, что рациональная нормальная кривая в $\mathbb{P}^n$ — это многообразие, определенное множеством однородных квадратичных уравнений, которые строятся как 2×2-поддетерминанты $2 \times n$-матрицы

$$\begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{n-1} \\ x_1 & x_2 & x_3 & \dots & x_n \end{pmatrix}.$$

12. Аффинная поверхность Веронезе $S \subset k^5$ была определена в упр. 6 к § 1 гл. 5. Она является образом параметризации $\phi : k^2 \to k^5$, заданной формулой

$$\phi(x_1, x_2) = (x_1, x_2, x_1^2, x_1x_2, x_2^2).$$

Проективное замыкание поверхности S — это проективное многообразие, называемое *проективной поверхностью Веронезе*.

(a) Найдите однородные уравнения, определяющие проективную поверхность Веронезе в $\mathbb{P}^5$.

(b) Докажите, что параметризация аффинной поверхности Веронезе может быть продолжена до отображения $\tilde{\phi} : \mathbb{P}^2 \to \mathbb{P}^5$, образ которого совпадает с проективной поверхностью Веронезе. Указание: нужно доказать, что отображение $\tilde{\phi}$ корректно определено, т. е. что $\tilde{\phi}$ принимает одно и то же значение на всех однородных координатах произвольной точки в $\mathbb{P}^2$.

13. Декартово произведение двух аффинных пространств — это аффинное пространство: $k^n \times k^m = k^{n+m}$. Рассматривая стандартные включения $k^n \subset \mathbb{P}^n$, $k^m \subset \mathbb{P}^m$ и $k^{n+m} \subset \mathbb{P}^{n+m}$ (предложение 2 из § 2), объясните, чем отличается $\mathbb{P}^{n+m}$ от $\mathbb{P}^n \times \mathbb{P}^m$ (как множество).

14. В этом упражнении мы увидим, что $\mathbb{P}^n \times \mathbb{P}^m$ может быть отождествлено с некоторым проективным многообразием в $\mathbb{P}^{n+m+nm}$, которое называется *многообразием Сегре*. Конструкция здесь такова. Пусть $p = (x_0, \ldots, x_n)$ — однородные координаты точки $p \in \mathbb{P}^n$, а $q = (y_0, \ldots, y_m)$ — однородные координаты точки $q \in \mathbb{P}^m$. Отображение Сегре $\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{n+m+nm}$ сопоставляет паре точек $(p, q) \in \mathbb{P}^n \times \mathbb{P}^m$ точку из $\mathbb{P}^{n+m+nm}$ с однородными координатами

$$(x_0y_0, x_0y_1, \ldots, x_0y_m, x_1y_0, \ldots, x_1y_m, \ldots, x_ny_0, \ldots, x_ny_m).$$

Компонентами являются всевозможные произведения $x_iy_j, 0 \le i \le n$, $0 \le j \le m$. Образом этого отображения является проективное многообразие, называемое многообразием Сегре.

(a) Докажите, что отображение σ корректно определено, т. е. докажите, что при различных выборах однородных координат точек p и q мы получаем одну и ту же точку в $\mathbb{P}^{n+m+nm}$.

(b) Докажите инъективность отображения σ и докажите, что образ «аффинной части» $k^n \times k^m$ является аффинным многообразием в $k^{n+m+nm} = U_0 \subset \mathbb{P}^{n+m+nm}$, *изоморфным* k^{n+m} (См. § 4 из гл. 5).

(c) Пусть $n = m = 1$. Дайте явное описание отображения $\sigma : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ и найдите однородные уравнения, определяющие многообразие Сегре. Указание: нужно получить одно квадратичное уравнение, т. е. в этом случае многообразие Сегре является квадратичной поверхностью в $\mathbb{P}^3$.

(d) Рассмотрите случай $n = 2, m = 1$ и найдите однородные уравнения, определяющие многообразие Сегре в $\mathbb{P}^5$.

(e) Что является пересечением многообразия Сегре в $\mathbb{P}^5$ и поверхности Веронезе в $\mathbb{P}^5$? (См. упр. 12.)

§ 5. Проективная теория исключения

В гл. 3 мы часто сталкивались с примерами «недостающих» точек при изучении геометрических аспектов теории исключения. Так как одна из причин рассмотрения проективного пространства — учесть в наших рассмотрениях «недостающие» точки, то имеет смысл снова обратиться к теории исключения, но уже проективной. Мы рекомендуем читателю освежить в памяти первые два параграфа гл. 3, прежде чем разбирать новый материал.

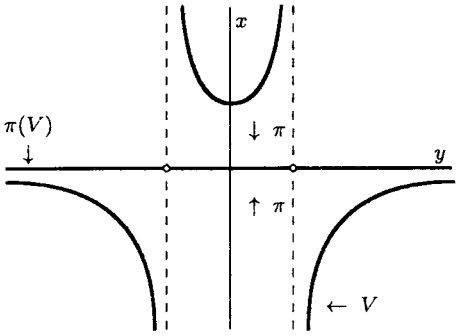
Начнем с рассмотрения следующего примера.

Пример 1. Рассмотрим многообразие $V \subset \mathbb{C}^2$, определенное уравнением

$$xy^2 = x - 1.$$

Для исключения переменной x мы используем исключающий идеал $I_1 = \langle xy^2 - x + 1 \rangle \cap \mathbb{C}[y]$. Легко показать, что $I_1 = \{0\} \subset \mathbb{C}[y]$. В

гл. 3 мы показали, что исключение переменной x геометрически соответствует переходу к проекции $\pi(V)$ на комплексную плоскость $\mathbb{C}$, где $\pi : \mathbb{C}^2 \to \mathbb{C}$ задано формулой $\pi(x, y) = y$. Мы знаем, что $\pi(V) \subset \mathbf{V}(I_1) = \mathbb{C}$, но рисунок показывает, что $\pi(V)$ является собственным подмножеством в $\mathbf{V}(I_1)$:



За недостающими точками мы можем проследить, используя геометрическую теорему о продолжении (теорема 2 из § 2 гл. 3). Напомним, как она работает. Запишем уравнение, определяющее V, в виде $(y^2 - 1)x - 1 = 0$. Тогда теорема о продолжении гарантирует, что мы можем разрешить это уравнение относительно x, если старший коэффициент при x не обращается в нуль. Таким образом, $y = \pm 1$ — это и есть недостающие точки.

Прежде, чем пытаться интерпретировать геометрическую теорему о продолжении в проективных терминах, отметим, что стандартная проективная плоскость $\mathbb{P}^2(\mathbb{C})$ — это не совсем то, что нам нужно. Нас интересуют направления проектирования (т. е. направления, параллельные оси x), так как недостающие точки лежат именно вдоль этих направлений. Поэтому вся плоскость $\mathbb{P}^2(\mathbb{C})$ нам не нужна. Другая проблема состоит в том, что в $\mathbb{P}^2(\mathbb{C})$ прямым, параллельным оси x, соответствует *одна* точка на бесконечности, в то время, как у нас недостает *двух*.

Чтобы избежать этих затруднений, мы будем использовать нечто отличное от $\mathbb{P}^2(\mathbb{C})$. Так как π — это отображение проекции $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$, то имеет смысл сделать проективным первый сомножитель, а не все проектируемое пространство. То есть мы будем рассматривать отображение проекции $\pi : \mathbb{P}^1(\mathbb{C}) \times \mathbb{C} \to \mathbb{C}$ на второй сомножитель.

Пусть (t, x, y) — координаты на $\mathbb{P}^1(\mathbb{C}) \times \mathbb{C}$, где (t, x) — однородные координаты на $\mathbb{P}^1(\mathbb{C})$, а y — обычная координата на $\mathbb{C}$. Тогда (по аналогии с предложением 2 из § 2) точка $(1, x, y) \in \mathbb{P}^1(\mathbb{C}) \times \mathbb{C}$ со-

ответствует точке $(x, y) \in \mathbb{C}\times\mathbb{C}$. Мы будем рассматривать $\mathbb{C}\times\mathbb{C}$ как подмножество в $\mathbb{P}^1(\mathbb{C}) \times \mathbb{C}$, но следует проверить, что дополнение состоит из «точек на бесконечности» с координатами $(0, 1, y)$.

Мы можем расширить многообразие $V \subset \mathbb{C}\times\mathbb{C}$ до многообразия $\tilde{V} \subset \mathbb{P}^1(\mathbb{C}) \times \mathbb{C}$, сделав уравнение многообразия V однородным по t и x. Таким образом, $\tilde{V}$ определено уравнением

$$xy^2 = x - t.$$

В упр. 1 будет доказано, что это уравнение корректно определяет подмножество в $\mathbb{P}^1(\mathbb{C}) \times \mathbb{C}$. Чтобы найти его решения, мы сначала положим $t = 1$ и найдем аффинные решения, а потом положим $t = 0$ и найдем точки на бесконечности. Имеем

$$\tilde{V} = V \cup \{(0, 1, \pm 1)\}$$

(t и x не могут одновременно обращаться в нуль, так как они являются однородными координатами). При отображении проекции $\pi : \mathbb{P}^1(\mathbb{C}) \times \mathbb{C} \to \mathbb{C}$ образ $\pi(\tilde{V})$ равен $\mathbb{C} = \mathbf{V}(I_1)$, потому что две точки на бесконечности отображаются в две «недостающие точки» $y = \pm 1$. Как мы вскоре увидим, равенство $\pi(\tilde{V}) = \mathbf{V}(I_1)$ является частным случаем проективного варианта геометрической теоремы о продолжении.

Рассмотрим общую постановку задачи. Пусть дана система уравнений

$$\begin{aligned} f_1(x_1, \dots, x_n, y_1, \dots, y_m) &= 0, \\ &\vdots \\ f_s(x_1, \dots, x_n, y_1, \dots, y_m) &= 0, \end{aligned}$$

где $f_1, \dots, f_s \in k[x_1, \dots, x_n, y_1, \dots, y_m]$. С алгебраической точки зрения исключение переменных $x_1, \dots, x_n$ состоит в вычислении идеала $I_n = \langle f_1, \dots, f_s \rangle \cap k[y_1, \dots, y_m]$ (теорема исключения из § 1 гл. 3 объясняет, как это надо делать). С геометрической точки зрения уравнения, приведенные выше, определяют многообразие $V \subset k^n \times k^m$ и исключению переменных $x_1, \dots, x_n$ соответствует рассмотрение образа $\pi(V)$, где $\pi : k^n \times k^m \to k^m$ — отображение проекции на последние m координат. Наша цель — описание связи между $\pi(V)$ и $\mathbf{V}(I_n)$.

Основная идея состоит в том, чтобы сделать первый сомножитель проективным. Чтобы упростить обозначения, мы будем писать $\mathbb{P}^n$ вместо $\mathbb{P}^n(k)$, если ясно о каком поле идет речь. Точка из $\mathbb{P}^n \times k^m$ имеет координаты $(x_0, \dots, x_n, y_1, \dots, y_m)$, где $(x_0, \dots, x_n)$ — однородные координаты в $\mathbb{P}^n$, а $(y_1, \dots, y_m)$ — обычные координаты в k^m. Таким образом $(1, 1, 1, 1)$ и $(2, 2, 1, 1)$ — это координаты одной

и той же точки в $\mathbb{P}^1 \times k^2$, но $(2, 2, 2, 2)$ — это координаты другой точки. Как и в предложении 2 из § 2, мы будем использовать отображение

$$(x_1, \dots, x_n, y_1, \dots, y_m) \mapsto (1, x_1, \dots, x_n, y_1, \dots, y_m),$$

чтобы отождествить $k^n \times k^m$ с тем подмножеством в $\mathbb{P}^n \times k^m$, где $x_0 \neq 0$.

Мы определим многообразия в $\mathbb{P}^n \times k^m$ с помощью «частично» однородных полиномов.

Определение 2. Пусть k — произвольное поле.

(i) Полином $F \in k[x_0, \dots, x_n, y_1, \dots, y_m]$ называется $(x_0, \dots, x_n)$-*однородным*, если существует такое целое число $l \geq 0$, что

$$F = \sum_{|\alpha|=l} h_\alpha(y_1, \dots, y_m) x^\alpha,$$

где x^α — это моном от $x_0, \dots, x_n$ мультистепени α, а $h_\alpha \in k[y_1, \dots, y_m]$.

(ii) *Многообразием* $\mathbf{V}(F_1, \dots, F_s) \subset \mathbb{P}^n \times k^m$, определенным $(x_0, \dots, x_n)$-однородными полиномами $F_1, \dots, F_s \in k[x_0, \dots, x_n, y_1, \dots, y_m]$, называется множество

$$\{(a_0, \dots, a_n, b_1, \dots, b_m) \in \mathbb{P}^n \times k^m : F_i(a_0, \dots, a_n, b_1, \dots, b_m) = 0 \text{ для всех } 1 \leq i \leq s\}.$$

В упражнениях будет доказано, что если $(x_0, \dots, x_n)$-однородный полином обращается в нуль на одном наборе координат некоторой точки из $\mathbb{P}^n \times k^m$, то он обращается в нуль на *всех* координатах этой точки. Это доказывает, что многообразие $\mathbf{V}(F_1, \dots, F_s)$ — корректно определенное подмножество в $\mathbb{P}^n \times k^m$, если полиномы $F_1, \dots, F_s$ являются $(x_0, \dots, x_n)$-однородными.

Теперь мы можем снова вернуться к теории исключения. Пусть даны $(x_0, \dots, x_n)$-однородные уравнения

$$\begin{aligned} F_1(x_0, \dots, x_n, y_1, \dots, y_m) &= 0, \\ &\vdots \\ F_s(x_0, \dots, x_n, y_1, \dots, y_m) &= 0. \end{aligned} \tag{1}$$

Эти уравнения определяют многообразие $V = \mathbf{V}(F_1, \dots, F_s) \subset \mathbb{P}^n \times k^m$. Рассмотрим отображение проекции

$$\pi : \mathbb{P}^n \times k^m \longrightarrow k^m$$

на последние m координат. Множество $\pi(V) \subset k^m$ — это множество таких m-наборов $(y_1, \dots, y_m)$, для которых система (1) имеет *не-*

тривиальное решение в переменных $x_0, \dots, x_n$ (это значит, что не все x_i равны нулю).

Рассмотрим пример.

Пример 3. Пусть (u, v, y) являются координатами на $\mathbb{P}^1 \times k$. Рассмотрим систему уравнений

$$\begin{aligned} F_1 &= u + vy = 0, \\ F_2 &= u + uy = 0. \end{aligned} \tag{2}$$

Так как (u, v) — однородные координаты на $\mathbb{P}^1$, то легко показать, что

$$V = \mathbf{V}(F_1, F_2) = \{(0,1,0), (1,1,-1)\}.$$

Тогда, если $\pi : \mathbb{P}^1 \times k \longrightarrow k$, то $\pi(V) = \{0, -1\}$; поэтому при заданном y система (2) имеет нетривиальное решение в том и только том случае, когда $y = 0, -1$, т. е. из (2) следует, что $y(1+y) = 0$.

Казалось бы, должен существовать чисто алгебраический способ «исключения» u и v из системы (2), чтобы получить $y(1+y) = 0$. К сожалению, тот метод исключения, которым мы пользовались в гл. 3, здесь не работает. Чтобы объяснить это, рассмотрим идеал $I = \langle F_1, F_2 \rangle \subset k[u, v, y]$. Так как каждый член в F_1 и F_2 содержит u или v, то

$$I \cap k[y] = \{0\}.$$

С аффинной точки зрения этот ответ правилен, так как *аффинное* многообразие

$$\mathbf{V}_a(F_1, F_2) \subset k^2 \times k$$

содержит точки вида $(0, 0, y)$ для *всех* $y \in k$. Аффинные методы гл. 3 могут помочь нам только в том случае, если мы найдем алгебраический метод исключать решения $u = v = 0$.

Некоторую ясность вносит вычисление базиса Грёбнера идеала $I = \langle F_1, F_2 \rangle$ по отношению к различным lex-упорядочениям:

$$\begin{aligned} &\text{для } u > v > y : I = \langle u + vy, v + vy \rangle, \\ &\text{для } v > u > y : I = \langle vu - u^2, vy + u, uy + uy^2 \rangle. \end{aligned}$$

Последние элементы в каждом базисе показывают, что наш полином $y(1+y)$ *почти* принадлежит I в том смысле, что

$$u \cdot y(1+y), v \cdot y(1+y) \in I. \tag{3}$$

На языке частных идеалов (см. § 4 из гл. 4) это означает, что

$$y(1+y) \in I : \langle u, v \rangle.$$

Напомним (см. гл. 4), что частному идеалов соответствует, грубо говоря, разность многообразий (см. теорему 7 из § 4 гл. 4, где дана точная формулировка). Таким образом, идеал $I : \langle u, v \rangle$ связан

с разностью

$$\mathbf{V}_a(F_1, F_2) - \mathbf{V}_a(u, v) \subset k^2 \times k.$$

Это множество состоит *в точности* из нетривиальных решений системы (2). Таким образом, частные идеалов естественно возникают в этой задаче.

Теперь задача проективного исключения u и v из (2) приводит к полиному

$$y(1+y) \in \widetilde{I} = (I : \langle u, v \rangle) \cap k[y].$$

Методами гл. 4 можно показать, что в данном случае $\widetilde{I} = \langle y(1+y) \rangle$.

При рассмотрении этого примера мы подошли очень близко к понятию проективного исключения. В общем случае в условиях типа (3) могут понадобиться более высокие степени переменных (см., например, упр. 7). А теперь мы можем дать строгое определение проективного исключающего идеала.

Определение 4. Рассмотрим идеал $I \subset k[x_0, \dots, x_n, y_1, \dots, y_m]$, порожденный $(x_0, \dots, x_n)$-однородными полиномами. *Проективным исключающим идеалом* идеала I называется множество

$$\hat{I} = \{f \in k[y_1, \dots, y_m] : \text{ для любого } 0 \le i \le n, \text{ существует } e_i \ge 0, \text{ такое, что } x_i^{e_i} f \in I\}.$$

Легко проверить, что $\hat{I}$ является идеалом в $k[y_1, \dots, y_m]$. Роль идеала $\hat{I}$ показывает следующий результат.

Предложение 5. *Пусть $V = \mathbf{V}(F_1, \dots, F_s) \subset \mathbb{P}^n \times k^m$ — многообразие, определенное $(x_0, \dots, x_n)$-однородными полиномами. Рассмотрим отображение проекции $\pi : \mathbb{P}^n \times k^m \to k^m$. Тогда*

$$\pi(V) \subset \mathbf{V}(\hat{I}),$$

где $\hat{I}$ — проективный исключающий идеал идеала $I = \langle F_1, \dots, F_s \rangle$.

Доказательство. Пусть $(a_0, \dots, a_n, b_1, \dots, b_m) \in V$ и $f \in \hat{I}$. Тогда $x_i^{e_i} f(y_1, \dots, y_m) \in I$; следовательно, этот полином обращается в нуль на V, т. е.

$$a_i^{e_i} f(b_1, \dots, b_m) = 0$$

для всех i. Так как $(a_0, \dots, a_n)$ — это набор однородных координат, то хотя бы одна компонента a_i отлична от 0; значит, $f(b_1, \dots, b_m) = 0$. Таким образом, f обращается в нуль на $\pi(V)$, и предложение доказано. □

Если поле алгебраически замкнуто, то имеет место следующая проективная версия теоремы о продолжении.

Теорема 6 (проективная теорема о продолжении). *Пусть поле k алгебраически замкнуто и многообразие $V = \mathbf{V}(F_1, \ldots, F_s) \subset \mathbb{P}^n \times k^m$ определено $(x_0, \ldots, x_n)$-однородными полиномами из $k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. Пусть $I = \langle F_1, \ldots, F_s \rangle$, а $\hat{I} \subset k[y_1, \ldots, y_m]$ — его проективный исключающий идеал. Если*

$$\pi : \mathbb{P}^n \times k^m \to k^m$$

— отображение проекции на последние m координат, то

$$\pi(V) = \mathbf{V}(\hat{I}).$$

Доказательство. Включение $\pi(V) \subset \mathbf{V}(\hat{I})$ доказано в предложении 5. Докажем обратное включение. Пусть $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbf{V}(\hat{I})$, и положим $F_i(x_0, \ldots, x_n, \mathbf{c}) = F_i(x_0, \ldots, x_n, c_1, \ldots, c_m)$. Это однородный полином от переменных $x_0, \ldots, x_n$ полной степени d_i (его полная степень равна полной степени полинома $F_i(x_0, \ldots, x_n, y_1, \ldots, y_m)$ по переменным $x_0, \ldots, x_n$).

Если $\mathbf{c} \notin \pi(V)$, то уравнения

$$F_1(x_0, \ldots, x_n, \mathbf{c}) = \ldots = F_s(x_0, \ldots, x_n, \mathbf{c}) = 0$$

определяют пустое многообразие в $\mathbb{P}^n$. Так как поле k алгебраически замкнуто, то из проективной слабой теоремы о нулях (теорема 8 из § 3) следует, что

$$\langle x_0, \ldots, x_n \rangle^r \subset \langle F_1(x_0, \ldots, x_n, \mathbf{c}), \ldots, F_s(x_0, \ldots, x_n, \mathbf{c}) \rangle$$

для некоторого $r \geq 1$. Это означает, что мономы $x^\alpha, |\alpha| = r$, являются полиномиальными линейными комбинациями полиномов $F_i(x_0, \ldots, x_n, \mathbf{c})$, т. е.

$$x^\alpha = \sum_{i=1}^{s} H_i(x_0, \ldots, x_n) F_i(x_0, \ldots, x_n, \mathbf{c}).$$

Рассматривая однородные компоненты, мы можем считать полиномы H_i однородными полной степени $r - d_i$. Записывая каждый H_i как линейную комбинацию мономов $x^{\beta_i}, |\beta_i| = r - d_i$, мы получаем, что линейная оболочка полиномов

$$x^{\beta_i} F_i(x_0, \ldots, x_n, \mathbf{c}), \quad i = 1, \ldots, s, \quad |\beta_i| = r - d_i,$$

совпадает с линейным пространством *всех* однородных полиномов от переменных $x_0, \ldots, x_n$ полной степени r. Пусть размерность этого пространства равна N_r. В силу стандартных результатов линейной алгебры мы можем найти N_r таких полиномов

$$G_j(x_0, \ldots, x_n, \mathbf{c}), \quad j = 1, \ldots, N_r,$$

которые образуют базис этого пространства. Наша цель — привести это рассуждение к противоречию. Для этого, используя свойства определителей, мы построим важный для нас элемент исключающего идеала $\hat{I}$. Полином $G_j(x_0, \ldots, x_n, \mathbf{c})$ возникает из полинома $G_j = G_j(x_0, \ldots, x_n, y_1, \ldots, y_m) \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. Каждый G_j имеет вид $x^{\beta_i} F_i$ для некоторого i и β_i и однороден полной степени r по $x_0, \ldots, x_n$. Таким образом,

$$G_j = \sum_{|\alpha|=r} a_{j\alpha}(y_1, \ldots, y_m) x^\alpha. \tag{4}$$

Так как $x^\alpha, |\alpha| = r$, образуют базис пространства всех однородных полиномов полной степени r, то их количество равно N_r. Следовательно, можно составить квадратную матрицу из полиномов $a_{j\alpha}(y_1, \ldots, y_m)$. Пусть

$$D(y_1, \ldots, y_m) = \det(a_{j\alpha}(y_1, \ldots, y_m) : 1 \leq j \leq N_r, |\alpha| = r)$$

— определитель этой матрицы. Если мы подставим $\mathbf{c}$ в (4), то получим, что

$$G_j(x_0, \ldots, x_n, \mathbf{c}) = \sum_{|\alpha|=r} a_{j\alpha}(\mathbf{c}) x^\alpha.$$

А так как полиномы $G_j(x_0, \ldots, x_n, \mathbf{c})$ и x^α образуют базисы одного и того же векторного пространства, то

$$D(\mathbf{c}) \neq 0.$$

В частности, $D(y_1, \ldots, y_m) \neq 0$ в $k[y_1, \ldots, y_m]$.

Работая над полем функций $k(y_1, \ldots, y_m)$ (см. § 5 из гл. 5), мы можем рассматривать (4) как систему линейных уравнений относительно переменных x^α. Тогда по правилу Крамера (предложение 3 из § 3 приложения А)

$$x^\alpha = \frac{\det(M_\alpha)}{D(y_1, \ldots, y_m)},$$

где M_α — это матрица, полученная из матрицы $(a_{j\alpha})$ при замене столбца, соответствующего α, столбцом $G_1, \ldots, G_{N_r}$. Умножая это равенство на $D(y_1, \ldots, y_m)$ и разлагая $\det(M_\alpha)$ по этому столбцу, мы получаем равенство

$$x^\alpha D(y_1, \ldots, y_m) = \sum_{j=1}^{N_r} H_{j\alpha}(y_1, \ldots, y_m) G_j(x_0, \ldots, x_n, y_1, \ldots, y_m).$$

Однако каждый полином G_j имеет вид $x^{\beta_i} F_i$, и если мы выразим сумму через F_i, то получим, что

$$x^\alpha D(y_1, \ldots, y_m) \in \langle F_1, \ldots, F_s \rangle = I.$$

Это показывает, что $D \in \hat{I}$, а так как $\mathbf{c} \in \mathbf{V}(\hat{I})$, то $D(\mathbf{c}) = 0$, что противоречит установленному выше соотношению $D(\mathbf{c}) \neq 0$. Значит, $\mathbf{c} \in \pi(V)$, что и требовалось доказать. □

Теорема 6 утверждает, что проекция многообразия $V \subset \mathbb{P}^n \times k^m$ на второй сомножитель является многообразием. Это утверждение может быть интерпретировано следующим образом: если переменные $y_1, \ldots, y_m$ рассматриваются как параметры в системе уравнений

$$F_1(x_0, \ldots, x_n, y_1, \ldots, y_m) = \ldots = F_s(x_0, \ldots, x_n, y_1, \ldots, y_m) = 0,$$

то уравнения, определяющие $\pi(V) = \mathbf{V}(\hat{I})$ в k^m, содержат информацию, каким условиям должны удовлетворять параметры, чтобы система имела нетривиальное решение (т. е. решение, где хотя бы одна из переменных x_i была отлична от нуля).

Применение теоремы 6 зависит от возможности вычислить исключающий идеал $\hat{I}$. Мы рассмотрим эту задачу в двух следующих предложениях. Сначала мы покажем, как представить $\hat{I}$ в виде частного идеалов.

Предложение 7. *Рассмотрим идеал $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. Тогда для достаточно большого целого e имеем*

$$\hat{I} = (I : \langle x_0^e, \ldots, x_n^e \rangle) \cap k[y_1, \ldots, y_m].$$

Доказательство. По определению частного идеалов имеем

$$f \in I : \langle x_0^e, \ldots, x_n^e \rangle \Longrightarrow x_i^e f \in I \text{ для всех } 0 \leq i \leq n.$$

Отсюда $(I : \langle x_0^e, \ldots, x_n^e \rangle) \cap k[y_1, \ldots, y_m] \subset \hat{I}$ при всех $e \geq 0$.

Нам нужно доказать, что имеет место противоположное включение при достаточно большом e. Рассмотрим возрастающую цепь идеалов

$$I : \langle x_0, \ldots, x_n \rangle \subset I : \langle x_0^2, \ldots, x_n^2 \rangle \subset \ldots.$$

По условию обрыва возрастающих цепей (теорема 7 из § 5 гл. 2)

$$I : \langle x_0^e, \ldots, x_n^e \rangle = I : \langle x_0^{e+1}, \ldots, x_n^{e+1} \rangle = \ldots$$

для некоторого e. Зафиксируем это e. Тогда

$$I : \langle x_0^d, \ldots, x_n^d \rangle \subset I : \langle x_0^e, \ldots, x_n^e \rangle \tag{5}$$

для *всех* целых $d \geq 0$.

Пусть теперь $f \in \hat{I}$. Это означает, что $x_i^{e_i} f \in I$ для всех $0 \leq i \leq n$ и некоторых $e_i \geq 0$. Пусть $d = \max(e_0, \ldots, e_n)$. Тогда $x_i^d f \in I$ для всех i, т. е. $f \in I : \langle x_0^d, \ldots, x_n^d \rangle$. Теперь из (5) следует, что $f \in (I : \langle x_0^e, \ldots, x_n^e \rangle) \cap k[y_1, \ldots, y_m]$. □

Теперь мы свяжем идеал $\hat{I}$ с процессом исключения, рассмотренным в гл. 3. Для этого мы превратим задачу в аффинную с помощью дегомогенизации. Зафиксируем i, $0 \leq i \leq n$, и положим $x_i = 1$ в $F \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. Тогда мы получим полином

$$F^{(i)}(x_0, \ldots, 1, \ldots, x_n, y_1, \ldots, y_m) \in k[x_0, \ldots, \hat{x}_i, \ldots, x_n, y_1, \ldots, y_m],$$

где $\hat{x}_i$ означает, что x_i исключена из списка переменных. Если задан идеал $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$, то его *дегомогенизацией* называется множество

$$I^{(i)} = \{F^{(i)} : F \in I\} \subset k[x_0, \ldots, \hat{x}_i, \ldots, x_n, y_1, \ldots, y_m].$$

Легко показать, что $I^{(i)}$ является идеалом в $k[x_0, \ldots, \hat{x}_i, \ldots, x_n, y_1, \ldots, y_m]$ и что

$$I^{(i)} = \langle F_1^{(i)}, \ldots, F_s^{(i)} \rangle, \tag{6}$$

если $I = \langle F_1, \ldots, F_s \rangle$ (докажите это самостоятельно).

Рассмотрим многообразие $V \subset \mathbb{P}^n \times k^m$, определенное идеалом I. Тогда идеал $I^{(i)}$ определяет аффинную часть $V \cap (U_i \times k^m)$, где $U_i \cong k^n$ — подмножество в $\mathbb{P}^n$, определенную условием $x_i \neq 0$. Так как мы сделали задачу чисто аффинной, то теперь можем использовать методы исключения, развитые в гл. 3. В частности, мы должны рассмотреть n-й исключающий идеал

$$I_n^{(i)} = I^{(i)} \cap k[y_1, \ldots, y_n],$$

где индекс n указывает, что исключаются n переменных $x_0, \ldots, \hat{x}_i, \ldots, x_n$. Мы вычислим $\hat{I}$ в терминах его дегомогенизаций $I^{(i)}$.

Предложение 8. *Пусть идеал $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$ порожден $(x_0, \ldots, x_n)$-однородными полиномами. Тогда*

$$\hat{I} = I_n^{(0)} \cap I_n^{(1)} \cap \ldots \cap I_n^{(n)}.$$

Доказательство. Достаточно доказать, что

$$\hat{I} = I^{(0)} \cap \ldots \cap I^{(n)} \cap k[y_1, \ldots, y_m].$$

Предположим, что $f \in \hat{I}$. Тогда $x_i^{e_i} f(y_1, \ldots, y_m) \in I$; поэтому если мы положим $x_i = 1$, то получим, что $f(y_1, \ldots, y_m) \in I^{(i)}$. Отсюда следует, что $f \in I^{(0)} \cap \ldots \cap I^{(n)} \cap k[y_1, \ldots, y_m]$.

Теперь докажем обратное включение. Сначала изучим связь между идеалами I и $I^{(i)}$. Элемент $f \in I^{(i)}$ получается из некоторого элемента $F \in I$ с помощью подстановки $x_i = 1$. Мы утверждаем, что F может быть выбран $(x_0, \ldots, x_n)$-однородным. В

самом деле, $F = \sum_{j=0}^{d} F_j$, где F_j суть $(x_0, \ldots, x_n)$-однородные полиномы полной степени j по переменным $x_0, \ldots, x_n$. Так как I порожден $(x_0, \ldots, x_n)$-однородными полиномами, то нетрудно показать (см. доказательство теоремы 2 из § 3 и упр. 4), что $F_j \in I$ для всех j. Следовательно,

$$\sum_{j=0}^{d} x_i^{d-j} F_j$$

является $(x_0, \ldots, x_n)$-однородным полиномом в I и его дегомогенизация при $x_i = 1$ равна f. Таким образом, мы можем считать, что $F \in I$ $(x_0, \ldots, x_n)$-однороден.

Тогда процедура гомогенизации, примененная к полиному

$$f \in k[x_0, \ldots, \hat{x}_i, \ldots, x_n, y_1, \ldots, y_m]$$

и использующая x_i в качестве дополнительной переменной, дает нам $(x_0, \ldots, x_n)$-однородный полином $f^h \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. Пусть f является дегомогенизацией $(x_0, \ldots, x_n)$-однородного полинома F. Доказательство того, что

$$F = x_i^e f^h \tag{7}$$

для некоторого $e \geq 0$, мы оставляем читателю.

Пусть теперь $f \in I^{(i)} \cap k[y_1, \ldots, y_m]$. Тогда, как показано выше, f получен дегомогенизацией $(x_0, \ldots, x_n)$-однородного полинома $F \in I$. Так как f не зависит от переменных $x_0, \ldots, x_n$, то $f^h = f$ и по (7) $x_i^e f \in I$. Отсюда следует, что $I^{(0)} \cap \ldots \cap I^{(n)} \cap k[y_1, \ldots, y_m] \subset \hat{I}$. Предложение доказано. □

Предложение 8 можно интерпретировать следующим образом. Идеал $I_n^{(i)}$ исключает переменные $x_0, \ldots, \hat{x}_i, \ldots, x_n$ на аффинной части пространства $\mathbb{P}^n \times k^m$ (там, где $x_i \neq 0$). Тогда пересечение этих аффинных исключающих идеалов (которое, грубо говоря, соответствует исключению на объединении аффинных частей) и является проективным исключающим идеалом.

Предложение 8 дает нам алгоритм вычисления идеала $\hat{I}$. А именно, пусть $I = \langle F_1, \ldots, F_s \rangle$. Равенство (6) указывает базис идеала $I^{(i)}$. Идеал $I_n^{(i)}$ вычисляется с помощью теоремы исключения из § 1 гл. 3. Теперь алгоритм, вычисляющий пересечения идеалов (§ 3 гл. 4), позволяет найти $\hat{I} = I_n^{(0)} \cap \ldots \cap I_n^{(n)}$. Второй алгоритм для вычисления идеала $\hat{I}$, использующий предложение 7, будет рассмотрен в упражнениях.

В качестве примера рассмотрим уравнения

$$F_1 = u + vy = 0,$$
$$F_2 = u + uy = 0$$

из примера 3. Положим $I = \langle u + vy, u + uy \rangle \subset k[u, v, y]$. Тогда

$$\text{если } u = 1, \text{ то } I_1^{(u)} = \langle 1 + vy, 1 + y \rangle \cap k[y] = \langle 1 + y \rangle,$$

$$\text{если } v = 1, \text{ то } I_1^{(v)} = \langle u + y, u + uy \rangle \cap k[y] = \langle y(1 + y) \rangle.$$

Отсюда следует, что $\hat{I} = I_1^{(u)} \cap I_1^{(v)} = \langle y(1 + y) \rangle$. Можете ли вы объяснить, почему идеалы $I_1^{(u)}$ и $I_1^{(v)}$ различны?

Теперь мы снова вернемся к вопросу о недостающих точках в аффинном случае. Идеал $I \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ определяет многообразие $V = \mathbf{V}_a(I) \subset k^n \times k^m$, и мы знаем, что $\pi(V) \subset \mathbf{V}(I_n)$, где $\pi : k^n \times k^m \to k^m$ — отображение проекции, а I_n — n-й исключающий идеал идеала I. Мы хотим показать, что точки из $\mathbf{V}(I_n) - \pi(V)$ возникают из бесконечно удаленных точек в $\mathbb{P}^n \times k^m$.

Проведем гомогенизацию по новой переменной x_0. Из доказательства предложения 8 следует, что полином $f \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ дает нам $(x_0, \ldots, x_n)$-однородный полином $f^h \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. В упр. 12 мы подробно изучим процесс гомогенизации. Идеал

$$I^h = \langle f^h : f \in I \rangle \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m].$$

называется $(x_0, \ldots, x_n)$-*гомогенизацией* идеала I. По теореме Гильберта о базисе I^h порожден конечным числом $(x_0, \ldots, x_n)$-однородных полиномов.

В следующем предложении перечислены основные свойства идеала I^h.

Предложение 9. *Рассмотрим идеал $I \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, и пусть I^h — его $(x_0, \ldots, x_n)$-гомогенизация. Тогда*

(i) *проективный исключающий идеал идеала I^h равен n-му исключающему идеалу идеала I, т. е. $\hat{I}^h = I_n \subset k[y_1, \ldots, y_m]$;*

(ii) *если поле k алгебраически замкнуто, то многообразие $\bar{V} = \mathbf{V}(I^h)$ является наименьшим многообразием в $\mathbb{P}^n \times k^m$, содержащим аффинное многообразие $V = \mathbf{V}_a(I) \subset k^n \times k^m$; многообразие $\bar{V}$ называется* проективным замыканием *многообразия V в $\mathbb{P}^n \times k^m$.*

Доказательство. (i) Легко доказать, что дегомогенизация идеала I^h по переменной x_0 дает $(I^h)^{(0)} = I$. Тогда из доказательства предложения 8 следует, что $\hat{I}^h \subset I_n$. С другой стороны, пусть $f \in I_n$.

Так как $f \in k[y_1, \ldots, y_m]$, то f является $(x_0, \ldots, x_n)$-однородным. Поэтому $f = f^h \in I^h$. Следовательно, $x_i^0 f \in I^h$ для всех i. Значит, $f \in \hat{I}^h$, и п. (i) доказан.

Доказательство п. (ii) аналогично доказательству теоремы 8 из § 4, и мы оставляем его читателю в качестве упражнения. □

Теорема 6 и предложение 9 дают нам следующий замечательный результат.

Следствие 10. *Пусть поле k алгебраически замкнуто, а $V = \mathbf{V}_a(I) \subset k^n \times k^m$, где $I \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ — некоторый идеал. Тогда*

$$\mathbf{V}(I_n) = \pi(\overline{V}),$$

где $\overline{V} \subset \mathbb{P}^n \times k^m$ — проективное замыкание многообразия V, а $\pi : \mathbb{P}^n \times k^m \to k^m$ — отображение проекции.

Доказательство. Согласно предложению 9, $\overline{V} = \mathbf{V}(I^h)$ и $\hat{I}^h = I_n$. Теперь утверждение непосредственно следует из теоремы 6. □

В гл. 3 точки из $\mathbf{V}(I_n)$ назывались частичными решениями. Частичные решения, которые не продолжаются до полных решений из V, и образуют множество $\mathbf{V}(I_n) - \pi(V)$. Следствие 10 показывает, что эти точки получаются из бесконечно удаленных точек проективного замыкания $\overline{V}$ многообразия V.

Применение следствия 10 требует умения вычислять I^h. Как и в § 4, трудность состоит в том, что если $I = \langle f_1, \ldots, f_s \rangle$, то это еще не значит, что $I^h = \langle f_1^h, \ldots, f_s^h \rangle$. Но если мы будем использовать подходящий базис Грёбнера, то эту трудность можно преодолеть.

Предложение 11. *Пусть $>$ — мономиальное упорядочение на кольце $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, такое, что для всех мономов $x^\alpha y^\gamma, x^\beta y^\delta$ мы имеем*

$$|\alpha| > |\beta| \Longrightarrow x^\alpha y^\gamma > x^\beta y^\delta.$$

Пусть $G = \{g_1, \ldots, g_s\}$ — базис Грёбнера некоторого идеала I по отношению к $>$. Тогда $G^h = \{g_1^h, \ldots, g_s^h\}$ является базисом идеала $I^h \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$.

Доказательство. Доказательство этого утверждения аналогично доказательству теоремы 4 из § 4, и мы оставляем его читателю в качестве упражнения. □

В примере 1 мы рассматривали идеал $I = \langle xy^2 - x + 1 \rangle \subset \mathbb{C}[x, y]$. Это главный идеал, и, следовательно, полином $xy^2 - x + 1$ образует

базис Грёбнера по отношению к любому мономиальному упорядочению (см. упр. 10 к § 5 гл. 2). Если мы проведем гомогенизацию по отношению к новой переменной t, то по предложению 11 идеал I^h порожден (t, x)-однородным полиномом $xy^2 - x + t$. Пусть $\overline{V} = \mathbf{V}(I^h) \subset \mathbb{P}^1 \times \mathbb{C}$. Тогда, согласно следствию 10, $\pi(\overline{V}) = \mathbf{V}(I_1) = \mathbb{C}$, что согласуются с результатами примера 1.

Следствие 10 и предложение 11 указывают на недостатки геометрической теоремы о продолжении из гл. 3. Эта теорема утверждает, что если $I = \langle f_1, \ldots, f_s \rangle$, то

$$\mathbf{V}(I_1) = \pi(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)), \tag{8}$$

где $V = \mathbf{V}_a(I)$, а $g_1, \ldots, g_s$ — старшие коэффициенты полиномов f_i по отношению к x_1. С проективной точки зрения $\{(0,1)\} \times \mathbf{V}(g_1, \ldots, g_s)$ — это точки на бесконечности многообразия $Z = \mathbf{V}(f_1^h, \ldots, f_s^h)$ (см. доказательство теоремы 6). Так как $f_1, \ldots, f_s$ — *произвольный* базис идеала I, то Z *не* обязательно является проективным замыканием многообразия V, и, следовательно, многообразие $\mathbf{V}(g_1, \ldots, g_s)$ может быть слишком большим. Чтобы получить проективное замыкание в (8), мы должны использовать базис Грёбнера идеала I по отношению к мономиальному упорядочению того типа, который рассматривался в предложении 11.

Конец параграфа мы посвятим изучению отображений проективных пространств в проективные пространства. Пусть $f_0, \ldots, f_m \in k[x_0, \ldots, x_n]$ — однородные полиномы полной степени d, причем $\mathbf{V}(f_0, \ldots, f_m) = \varnothing$ в $\mathbb{P}^n$. Тогда мы можем определить отображение $F : \mathbb{P}^n \to \mathbb{P}^m$ формулой

$$F(x_0, \ldots, x_n) = (f_0(x_0, \ldots, x_n), \ldots, f_m(x_0, \ldots, x_n)).$$

Так как $f_0, \ldots, f_m$ не обращаются одновременно в нуль на $\mathbb{P}^n$, то $F(x_0, \ldots, x_n)$ всегда определяет точку в $\mathbb{P}^m$. Далее, так как f_i имеют одинаковую полную степень d, то

$$F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n)$$

для всех $\lambda \in k - \{0\}$. Таким образом, F — корректно определенное отображение из $\mathbb{P}^n$ в $\mathbb{P}^m$.

С отображениями проективных пространств мы уже встречались. Так, например, в упр. 21 к § 2 мы изучали отображение $F : \mathbb{P}^1 \to \mathbb{P}^2$, определенное формулой

$$F(a, b) = (a^2 + b^2, 2ab, a^2 - b^2).$$

Это проективная параметризация многообразия $\mathbf{V}(x^2 - y^2 - z^2)$. Кроме того, в упр. 12 к § 4 мы рассматривали отображение Веро-

незе, определенное формулой

$$\phi(x_0, x_1, x_2) = (x_0^2, x_0x_1, x_0x_2, x_1^2, x_1x_2, x_2^2).$$

Образ этого отображения называется поверхностью Веронезе в $\mathbb{P}^5$.

Над алгебраически замкнутыми полями мы можем описать образ отображения $F : \mathbb{P}^n \to \mathbb{P}^m$, используя теорию исключения.

Теорема 12. *Пусть поле k алгебраически замкнуто и отображение $F : \mathbb{P}^n \to \mathbb{P}^m$ задано однородными полиномами $f_0, \dots, f_m \in k[x_0, \dots, x_n]$ одинаковой полной степени, не имеющими общих нулей в $\mathbb{P}^n$. Пусть $I = \langle y_0 - f_0, \dots, y_m - f_m \rangle \subset k[x_0, \dots, x_n, y_0, \dots, y_m]$ и $I_{n+1} = I \cap k[y_0, \dots, y_m]$. Тогда I_{n+1} является однородным идеалом в $k[y_0, \dots, y_m]$ и*

$$F(\mathbb{P}^n) = \mathbf{V}(I_{n+1}).$$

Доказательство. Докажем сначала, что I_{n+1} является однородным идеалом. Пусть все f_i имеют полную степень d. Так как образующие $y_i - f_i$ идеала I неоднородны (за исключением случая $d = 1$), то мы припишем переменным $x_0, \dots, x_n, y_0, \dots, y_m$ веса следующим образом: все x_i имеют вес 1, а все y_j имеют вес d. Тогда моном $x^\alpha y^\beta$ имеет вес $|\alpha| + d|\beta|$. Полином $f \in k[x_0, \dots, x_n, y_0, \dots, y_m]$ называется *взвешенно однородным*, если все его мономы имеют один и тот же вес.

Все образующие $y_i - f_i$ имеют вес d, т. е. I является взвешенно однородным идеалом. Если мы вычислим базис Грёбнера G идеала I по отношению к любому мономиальному упорядочению, то рассуждения, подобные тем, которые использовались в доказательстве теоремы 2 из § 3, показывают, что G состоит из взвешенно однородных полиномов. Для подходящего lex-упорядочения теорема исключения из гл. 3 утверждает, что $G \cap k[y_0, \dots, y_m]$ является базисом идеала $I_{n+1} = I \cap k[y_0, \dots, y_m]$. Таким образом, I_{n+1} имеет взвешенно однородный базис. Но так как все y_j имеют один и тот же вес, то полином в $k[y_0, \dots, y_m]$ является взвешенно однородным в том и только том случае, когда он однороден. Это доказывает однородность идеала I_{n+1}.

Для изучения образа отображения F нам понадобится рассматривать многообразия в произведении $\mathbb{P}^n \times \mathbb{P}^m$. Полином $h \in k[x_0, \dots, x_n, y_0, \dots, y_m]$ называется *биоднородным*, если он может быть представлен в виде

$$h = \sum_{|\alpha|=q, |\beta|=l} a_{\alpha\beta} x^\alpha y^\beta.$$

Если полиномы $h_1, \dots, h_s$ биоднородны, то они корректно определяют множество

$$\mathbf{V}(h_1, \dots, h_s) \subset \mathbb{P}^n \times \mathbb{P}^m,$$

многообразие, определенное полиномами $h_1, \dots, h_s$. Аналогично, если идеал $J \subset k[x_0, \dots, x_n, y_0, \dots, y_m]$ порожден биоднородными полиномами, то J определяет многообразие $\mathbf{V}(J) \subset \mathbb{P}^n \times \mathbb{P}^m$ (см. упр. 16).

Теория исключения прекрасно работает в такой ситуации. Проективный исключающий идеал $\hat{J} \subset k[y_0, \dots, y_m]$ однороден (упр. 16). Если $\pi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$ — отображение проекции, то из теоремы 6 следует, что

$$\pi(\mathbf{V}(J)) = \mathbf{V}(\hat{J}) \tag{9}$$

в $\mathbb{P}^m$ (см. упр. 16). Это равенство справедливо в случае алгебраически замкнутого поля k.

Теория исключения не может быть применена к идеалу I, так как он не является биоднородным. Поэтому мы будем работать с биоднородным идеалом $J = \langle y_i f_j - y_j f_i \rangle$. Докажем, что $\mathbf{V}(J) \subset \mathbb{P}^n \times \mathbb{P}^m$ — график отображения $F : \mathbb{P}^n \to \mathbb{P}^m$. Если $p \in \mathbb{P}^n$, то $(p, F(p)) \in \mathbf{V}(J)$, так как $y_i = f_i(p)$ для всех i. С другой стороны, пусть $(p, q) \in \mathbf{V}(J)$. Тогда $q_i f_j(p) = q_j f_i(p)$ для всех i, j, где q_i — это i-я координата точки q. Найдется j, такое, что $q_j \neq 0$, и по условию найдется i, такое, что $f_i(p) \neq 0$. Тогда соотношение $q_i f_j(p) = q_j f_i(p) \neq 0$ показывает, что $q_i \neq 0$. Пусть $\lambda = q_i / f_i(p) \neq 0$. Теперь определяющие уравнения многообразия $\mathbf{V}(J)$ показывают, что $q = \lambda F(p)$, т. е. точка (p, q) принадлежит графику отображения F в $\mathbb{P}^n \times \mathbb{P}^m$.

Как мы видели в § 3 гл. 3, проекция графика является образом отображения. Таким образом, $\pi(\mathbf{V}(J)) = F(\mathbb{P}^n)$ или, согласно (9), $F(\mathbb{P}^n) = \mathbf{V}(\hat{J})$ (так как k алгебраически замкнуто). Это доказывает, что образ отображения F является многообразием в $\mathbb{P}^m$.

Алгоритм вычисления идеала $\hat{J}$ нам известен, и на этом мы могли бы остановиться. Но, к сожалению, вычислить $\hat{J}$ не так-то просто. Гораздо проще работать с идеалом $I_{n+1} = I \cap k[y_0, \dots, y_m]$, для чего нужны только методы гл. 3. Поэтому окончательный шаг доказательства состоит в том, чтобы доказать равенство $\mathbf{V}(\hat{J}) = \mathbf{V}(I_{n+1})$ в $\mathbb{P}^m$.

Для этого достаточно показать, что $\mathbf{V}_a(\hat{J}) = \mathbf{V}_a(I_{n+1})$ в k^{m+1}. Заметим, что многообразие $\mathbf{V}_a(I) \subset k^{n+1} \times k^{m+1}$ является графиком отображения $k^{n+1} \to k^{m+1}$, заданного набором $(f_0, \dots, f_m)$. Пусть π — отображение проекции $\pi : k^{n+1} \times k^{m+1} \to k^{m+1}$. Мы утверж-

даем, что $\pi(\mathbf{V}_a(I)) = \mathbf{V}_a(\hat{J})$. Известно, что $\mathbf{V}(\hat{J})$ является образом отображения F в $\mathbb{P}^m$. Если мы исключим начало координат, то $q \in \mathbf{V}_a(\hat{J})$ в том и только том случае, когда существует точка $p \in k^{n+1}$, такая, что $q = F(p)$ в $\mathbb{P}^m$. Следовательно, $q = \lambda F(p)$ в k^{m+1} для некоторого $\lambda \neq 0$. Положим $\lambda' = \sqrt[d]{\lambda}$. Тогда $q = F(\lambda' p)$, т. е. $q \in \pi(\mathbf{V}_a(I))$. Утверждение доказано.

По теореме о замыкании (теорема 3 из § 2 гл. 3) $\mathbf{V}_a(I_{n+1})$ является наименьшим многообразием, содержащим $\pi(\mathbf{V}_a(I))$. Так как эта проекция равна многообразию $\mathbf{V}_a(\hat{J})$, то $\mathbf{V}_a(I_{n+1}) = \mathbf{V}_a(\hat{J})$, что и завершает доказательство теоремы. □

Упражнения к § 5

1. Объясните, почему уравнение $xy^2 - x + t = 0$ корректно определяет (см. пример 1) подмножество в $\mathbb{P}^1 \times \mathbb{C}$, где (t, x) — однородные координаты на $\mathbb{P}^1$, а y — координата на $\mathbb{C}$. Указание: см. упр. 2.
2. Пусть полином $F \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$ является $(x_0, \ldots, x_n)$-однородным. Докажите, что если F обращается в нуль на некотором наборе координат точки из $\mathbb{P}^n \times k^m$, то он обращается в нуль на *всех* координатах этой точки.
3. В примере 3 покажите, что $\mathbf{V}(F_1, F_2) = \{(0, 1, 0), (1, 1, -1)\}$.
4. В этом упражнении будут изучаться идеалы, порожденные $(x_0, \ldots, x_n)$-однородными полиномами.
   (a) Докажите, что каждый полином $F \in k[x_0, \ldots, x_n, y_1, \ldots, y_m]$ имеет единственное представление в виде суммы $(x_0, \ldots, x_n)$-однородных полиномов. Мы будем называть их $(x_0, \ldots, x_n)$-*однородными компонентами* полинома F.
   (b) Докажите, что идеал $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$ порожден $(x_0, \ldots, x_n)$-однородными полиномами в том и только том случае, когда он содержит все $(x_0, \ldots, x_n)$-однородные компоненты каждого своего элемента.
5. Рассмотрим идеал $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$, порожденный $(x_0, \ldots, x_n)$-однородными полиномами. Как найти идеал $(I : x_i) \cap k[y_1, \ldots, y_m]$? Для простоты мы рассмотрим случай $i = 0$. Пусть $>$ — это lex-упорядочение с $x_1 > \ldots > x_n > x_0 > y_1 > \ldots > y_m$, а G — редуцированный базис Грёбнера идеала I по отношению к этому упорядочению.
   (a) Пусть $g \in G$ и $\mathrm{LT}(g) = x_0 y^\alpha$. Докажите, что $g = x_0 h_1(y_1, \ldots, y_m) + h_0(y_1, \ldots, y_m)$.
   (b) В условиях п. (a) докажите, что $g = x_0 h_1(y_1, \ldots, y_m)$. Указание: используйте п. (b) упр. 4 и тот факт, что $G \cap k[y_1, \ldots, y_m]$ является базисом Грёбнера идеала $I \cap k[y_1, \ldots, y_m]$. Не забывайте, что G редуцирован.

   (c) Рассмотрим множество $G' = \{g \in k[y_1, \ldots, y_m] : \text{или } g, \text{ или } x_0 g \in G\}$. Докажите, что $G' \subset (I : x_0) \cap k[y_1, \ldots, y_m]$ и что старший член любого полинома из $(I : x_0) \cap k[y_1, \ldots, y_m]$ делится на старший член некоторого полинома из G'. Это доказывает, что G' является базисом Грёбнера.
   (d) Объясните, как вычислить $(I : x_0^e) \cap k[y_1, \ldots, y_m]$.
6. В примере 3 мы утверждали, что $(I : \langle u, v \rangle) \cap k[y] = \langle y(y+1) \rangle$, где $I = \langle u + vy, u + uy \rangle \subset k[u, v, y]$. Докажите это, используя метод упр. 5. Указание: $I : \langle u, v \rangle = (I : u) \cap (I : v)$. Необходимый базис Грёбнера вычислен в примере 3.
7. Пусть (u, v, y) — координаты на $\mathbb{P}^1 \times k$. Пусть $F_1 = u - vy$ и $F_2 = u^2 - v^2 y \in k[u, v, y]$.
   (a) Найдите $\mathbf{V}(F_1, F_2)$ и объясните геометрически, почему исключение переменных u и v приводит к уравнению $y(1-y) = 0$.
   (b) Вычислив подходящий базис Грёбнера, докажите, что $u^2 y(1-y)$, $v^2 y^2 (1-y) \in I = \langle F_1, F_2 \rangle$ и что $uy(1-y), vy(1-y) \notin I$.
   (c) Докажите, что $(I : \langle u, v \rangle) \cap k[y] = \{0\}$ и что $I : \langle u^2, v^2 \rangle) \cap k[y] = \langle y(1-y) \rangle$. Указание: используйте упр. 5.
8. Докажите, что множество $\hat{I}$ из определения 4 является идеалом в $k[y_1, \ldots, y_m]$. Замечание: хотя этот факт следует из предложения 7, желательно дать прямое доказательство.
9. Рассмотрим идеал $I \subset k[x_0, \ldots, x_n, y_1, \ldots, y_m]$. Используя рассуждения из доказательства предложения 7, покажите, что
$$\hat{I} = (I : \langle x_0, \ldots, x_n \rangle^e) \cap k[y_1, \ldots, y_m]$$
для всех достаточно больших e. Указание: идеал $\langle x_0, \ldots, x_n \rangle^e$ порожден всеми мономами x^α полной степени e (см. упр. 8 к § 3).
10. В этом упражнении мы используем предложение 7 для построения алгоритма, вычисляющего проективный исключающий идеал $\hat{I}$.
    (a) Пусть $I : \langle x_0^e, \ldots, x_n^e \rangle = I : \langle x_0^{e+1}, \ldots, x_n^{e+1} \rangle, e \geq 0$. Докажите, что $I : \langle x_0^e, \ldots, x_n^e \rangle = I : \langle x_0^d, \ldots, x_n^d \rangle$ при $d \geq e$.
    (b) Используя п. (a), найдите алгоритм, вычисляющий целое e, такое, что $\hat{I} = (I : \langle x_0^e, \ldots, x_n^e \rangle) \cap k[y_1, \ldots, y_m]$.
    (c) Как только мы нашли e, алгоритмы из гл. 3 и 4 помогут вычислить идеал $\hat{I}$ (с помощью предложения 7).
11. В этом упражнении мы рассмотрим процедуру дегомогенизации $F \mapsto F^{(i)}$, определенную перед предложением 8.
    (a) Докажите, что $I^{(i)} = \{F^{(i)} : F \in I\}$ является идеалом в $k[x_0, \ldots, \hat{x}_i, \ldots, x_n, y_1, \ldots, y_m]$.
    (b) Пусть $I = \langle F_1, \ldots, F_s \rangle$. Докажите, что $I^{(i)} = \langle F_1^{(i)}, \ldots, F_s^{(i)} \rangle$.
12. В доказательстве предложения 8 использовался оператор, превращающий полином $f \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ в $(x_0, \ldots, x_n)$-однородный полином f^h за счет введения новой переменной x_0.

(a) Дайте точное определение f^h.
(b) Дегомогенизируем f^h, положив $x_0 = 1$. Докажите, что $(f^h)^{(0)} = f$.
(c) Пусть $f = F^{(0)}$ является дегомогенизацией $(x_0, \ldots, x_n)$-однородного полинома F. Докажите, что $F = x_0^e f^h$ для некоторого $e \geq 0$.

13. Докажите п. (ii) предложения 9.

14. Докажите предложение 11. Приведите пример мономиального упорядочения, которое удовлетворяет условиям предложения 11. Указание: рассмотрите подходящее взвешенное упорядочение из упр. 12 к § 4 гл. 2.

15. В доказательстве теоремы 12 мы использовали взвешенно однородные полиномы. Общее определение таково. Пусть переменные $x_0, \ldots, x_n$ имеют веса $q_0, \ldots, q_n$, которые являются целыми положительными числами. *Весом* монома x^α является число $\sum_{i=0}^n q_i\alpha_i$, где $\alpha = (\alpha_0, \ldots, \alpha_n)$. Полином называется *взвешенно однородным*, если все его мономы имеют одинаковый вес.
(a) Докажите, что каждый полином $f \in k[x_0, \ldots, x_n]$ имеет единственное представление в виде суммы взвешенно однородных полиномов. Они называются *взвешенно однородными компонентами* полинома f.
(b) Что значит, что идеал $I \subset k[x_0, \ldots, x_n]$ является *взвешенно однородным*? Сформулируйте и докажите аналог теоремы 2 из § 3 для взвешенно однородных идеалов.

16. В этом упражнении мы рассмотрим теорию исключения в $\mathbb{P}^n \times \mathbb{P}^m$. Мы будем работать с полиномиальным кольцом $k[x_0, \ldots, x_n, y_0, \ldots, y_m]$, где $(x_0, \ldots, x_n)$ — однородные координаты на $\mathbb{P}^n$, а $(y_0, \ldots, y_m)$ — однородные координаты на $\mathbb{P}^m$.
(a) Полином $h \in k[x_0, \ldots, x_n, y_0, \ldots, y_m]$ называется *биоднородным*, если он имеет вид

$$h = \sum_{|\alpha|=q, |\beta|=l} a_{\alpha\beta} x^\alpha y^\beta.$$

В этом случае мы говорим, что h имеет *бистепень* (q, l). Докажите, что если полиномы $h_1, \ldots, h_s$ биоднородны, то они корректно определяют многообразие

$$\mathbf{V}(h_1, \ldots, h_s) \subset \mathbb{P}^n \times \mathbb{P}^m.$$

Пусть идеал $J \subset k[x_0, \ldots, x_n, y_0, \ldots, y_m]$ порожден биоднородными полиномами. Объясните, как определить множество $\mathbf{V}(J) \subset \mathbb{P}^n \times \mathbb{P}^m$, и докажите, что оно является многообразием.
(b) Пусть идеал J порожден биоднородными полиномами, и пусть $V = \mathbf{V}(J) \subset \mathbb{P}^n \times \mathbb{P}^m$. Так как J также $(x_0, \ldots, x_n)$-однороден, то мы можем построить его проективный исключающий идеал $\hat{J} \subset k[y_0, \ldots, y_m]$. Докажите, что $\hat{J}$ однороден.

(c) Пусть поле k алгебраически замкнуто, и пусть $\pi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$ — отображение проекции. Докажите, что

$$\pi(V) = \mathbf{V}(\hat{J})$$

в $\mathbb{P}^m$. Это главный результат теории исключения в $\mathbb{P}^n \times \mathbb{P}^m$. Указание: идеал J также определяет многообразие в $\mathbb{P}^n \times k^{m+1}$; поэтому можно применить теорему 6 к отображению проекции $\mathbb{P}^n \times k^{m+1} \to k^{m+1}$.

17. В тексте параграфа перед теоремой 12 были рассмотрены два отображения проективных пространств. Найдите определяющие уравнения образов этих отображений.

18. В упр. 11 к § 1 мы рассматривали проективную плоскость $\mathbb{P}^2$ с координатами (x, y, z) и двойственную проективную плоскость $\mathbb{P}^{2\vee}$, где точка с координатами $(A, B, C) \in \mathbb{P}^{2\vee}$ соответствует проективной прямой, заданной уравнением $Ax + By + Cz = 0$ в $\mathbb{P}^2$. Докажите, что подмножество

$$\{(p, L) \in \mathbb{P}^2 \times \mathbb{P}^{2\vee} : p \in L\} \subset \mathbb{P}^2 \times \mathbb{P}^{2\vee}$$

является многообразием, заданным биоднородным полиномом в $k[x, y, z, A, B, C]$ бистепени $(1, 1)$. Указание: см. п. (f) упр. 11 к § 1.

§ 6. Геометрия квадрик

В этом параграфе мы рассмотрим квадратичные гиперповерхности в $\mathbb{P}^n(k)$. Эти многообразия являются обобщениями конических сечений на плоскости, и их геометрия весьма интересна. Чтобы упростить обозначения, мы будем писать $\mathbb{P}^n$ вместо $\mathbb{P}^n(k)$. Однородные координаты мы обозначаем через $x_0, \ldots, x_n$. На протяжении этого параграфа мы будем считать, что характеристика поля k не равна 2. Это означает, что $2 = 1 + 1 \neq 0$ в k, в частности, мы можем делить на 2.

Прежде чем определять квадратичные гиперповерхности, нам необходимо ввести понятие *проективной эквивалентности*. Пусть $\mathrm{GL}(n+1, k)$ — множество обратимых $(n+1) \times (n+1)$-матриц с элементами из k. Матрица $A \in \mathrm{GL}(n+1, k)$ задает преобразование пространства $\mathbb{P}^n$ следующим образом. Умножение на A вектор-столбца длины $n+1$ определяет линейное отображение аффинных пространств $k^{n+1} \to k^{n+1}$, которое является изоморфизмом, так как A обратима. Это отображение переводит подпространства пространства k^{n+1} в подпространства той же размерности, в частности прямые, проходящие через начало координат, в такие же прямые. Таким образом, A задает отображение $A : \mathbb{P}^n \to \mathbb{P}^n$ (см. (1) из § 2). Мы назовем такое отображение *проективным линейным преобразованием*.

определителем. Этот определитель и дает ненулевую плюккерову координату.

Теперь посмотрим, как плюккеровы координаты зависят от выбора точек $p, q \in L$. Пусть мы выбрали другую пару точек $p', q' \in L$. По (10)

$$L = \{up - vq : (u, v) \in \mathbb{P}^1\}.$$

Следовательно,

$$p' = up - vq,$$
$$q' = sp - tq,$$

где (u, v) и (s, t) — две различные точки в $\mathbb{P}^1$. Доказательство того, что

$$\omega(p', q') = \omega(up - vq, sp - tq) = (vs - ut)\omega(p, q)$$

в k^6, мы оставляем читателю. Очевидно, что $vs - ut \neq 0$, так как $(u, v) \neq (s, t)$ в $\mathbb{P}^1$. Это показывает, что $\omega(p, q)$ определяет точку в $\mathbb{P}^5$, которая зависит *только* от L, т. е. прямая L однозначно определяет точку $\omega(L) \in \mathbb{P}^5$.

Если L пробегает все прямые в $\mathbb{P}^3$, то точки $\omega(L)$ образуют некоторое подмножество в $\mathbb{P}^5$. Исключая a_i и b_i из уравнений (11), мы получим, что $w_{01}w_{23} - w_{02}w_{13} + w_{03}w_{12} = 0$ для всех наборов плюккеровых координат. Обозначим через $z_{ij}, 0 \leq i < j \leq 3$, однородные координаты на $\mathbb{P}^5$. Тогда точки $\omega(L)$ лежат на неособой квадрике $\mathbf{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12}) \subset \mathbb{P}^5$. Докажем, что эта квадрика *совпадает* с множеством всех прямых в $\mathbb{P}^3$.

Теорема 11. *Отображение*

$$\{\textit{прямые в } \mathbb{P}^3\} \longrightarrow \mathbf{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12}),$$

которое прямой $L \subset \mathbb{P}^3$ ставит в соответствие набор ее плюккеровых координат $\omega(L) \in \mathbf{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12})$, является биекцией.

Доказательство. Стратегия доказательства состоит в том, чтобы реконструировать прямую $L \subset \mathbb{P}^3$ по ее плюккеровым координатам. Пусть точки $p = (a_0, a_1, a_2, a_3)$ и $q = (b_0, b_1, b_2, b_3)$ лежат на L. Тогда мы можем определить четыре вектора в k^4:

$$\begin{aligned} b_0p - a_0q &= (0, -w_{01}, -w_{02}, -w_{03}), \\ b_1p - a_1q &= (w_{01}, 0, -w_{12}, -w_{13}), \\ b_2p - a_2q &= (w_{02}, w_{12}, 0, -w_{23}), \\ b_3p - a_3q &= (w_{03}, w_{13}, w_{23}, 0). \end{aligned} \tag{12}$$

Некоторые из этих векторов могут быть нулевыми, но те из них, которые не равны нулю, отвечают точкам на L (см. (10)).

Докажем инъективность отображения ω. Предположим, что прямые L и L' таковы, что $\omega(L) = \lambda\omega(L')$ для некоторого $\lambda \neq 0$. В терминах плюккеровых координат это означает, что $w_{ij} = \lambda w'_{ij}$ для всех $0 \leq i < j \leq 3$. Мы знаем, что среди плюккеровых координат L есть ненулевые. Без ограничения общности мы можем считать, что $w_{01} \neq 0$. Тогда из (12) следует, что точки

$$\begin{aligned} P &= (0, -w'_{01}, -w'_{02}, -w'_{03}) = (0, -\lambda w_{01}, -\lambda w_{02}, -\lambda w_{03}) \\ &= (0, -w_{01}, -w_{02}, -w_{03}), \\ Q &= (w'_{01}, 0, -w'_{12}, -w'_{13}) = (\lambda w_{01}, 0, -\lambda w_{12}, -\lambda w_{13}) \\ &= (w_{01}, 0, -w_{12}, -w_{13}) \end{aligned}$$

лежат и на L, и на L'. Так как в $\mathbb{P}^3$ через две точки можно провести только одну прямую (см. упр. 14), то $L = L'$. Это доказывает инъективность.

Докажем сюръективность отображения ω. Пусть

$$(w_{01}, w_{02}, w_{03}, w_{12}, w_{13}, w_{23}) \in \mathbf{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12}).$$

Мы можем считать, что $w_{01} \neq 0$ (произведя замену координат). Тогда первые два вектора в (12) ненулевые, и, следовательно, соответствующие точки определяют прямую $L \subset \mathbb{P}^3$. Используя определение отображения ω и равенство $w_{01}w_{23} - w_{02}w_{13} + w_{03}w_{12} = 0$, легко показать, что w_{ij} являются плюккеровыми координатами прямой L (см. упр. 16). Теорема доказана. □

Замечательным следствием теоремы 11 является то, что множество прямых в $\mathbb{P}^3$ имеет структуру проективного многообразия. Как мы отмечали в конце гл. 7, идея, что любое множество интересных геометрических объектов образует многообразие, — одна из главных в алгебраической геометрии.

Теорема 11 допускает всевозможные обобщения. Можно рассматривать прямые в $\mathbb{P}^n$ и даже определить плюккеровы координаты линейных многообразий в $\mathbb{P}^n$ произвольной размерности. Все это приводит к изучению объектов, называемых *грассманианами*. Плюккеровы координаты позволяют задать на грассманиане структуру проективного многообразия, несмотря на то, что грассманиан имеет, как правило, несколько определяющих уравнений. См. упр. 17, в котором рассматривается случай прямых в $\mathbb{P}^4$.

Мы также можем рассматривать теорему 11 с аффинной точки зрения. Мы знаем о существовании естественной биекции

$$\{\text{прямые, проходящие через начало координат в } k^4\} \cong \{\text{точки в } \mathbb{P}^3\}.$$

В упражнениях будет описана другая биекция:

$$\{\text{плоскости, проходящие через начало координат в } k^4\} \cong \{\text{прямые в } \mathbb{P}^3\}.$$

Таким образом, теорема 11 показывает, что множество плоскостей, проходящих через начало координат в k^4, имеет структуру квадрики в $\mathbb{P}^5$. В упражнениях мы увидим, что этот факт имеет удивительную связь с матрицами главного ступенчатого вида. Более общим образом грассманианы, упомянутые в предыдущем абзаце, могут быть описаны в терминах подпространств некоторой размерности в k^{n+1}.

На этом мы заканчиваем наше обсуждение квадратичных гиперповерхностей, но мы лишь коснулись этой теории. Классические книги ROTH, SEMPLE (1949) и HODGE, PEDOE (1968) содержат обширный материал, посвященный квадрикам (а также многим другим интересным проективным многообразиям).

Упражнения к § 6

1. Множество $\mathrm{GL}(n+1,k)$ замкнуто относительно умножения матриц и взятия обратной матрицы и является группой в смысле приложения A. Мы знаем, что матрица $A \in \mathrm{GL}(n+1,k)$ задает проективное линейное преобразование $\mathbb{P}^n \to \mathbb{P}^n$. Для того чтобы описать множество всех таких преобразований, зададим на $\mathrm{GL}(n+1,k)$ следующее отношение:

$$A' \sim A \iff A' = \lambda A \text{ для некоторого } \lambda \neq 0.$$

   (a) Докажите, что $\sim$ является отношением эквивалентности. Соответствующее множество классов эквивалентности обозначается $\mathrm{PGL}(n+1,k)$.

   (b) Докажите, что если $A \sim A'$ и $B \sim B'$, то $AB \sim A'B'$. Следовательно, умножение матриц корректно определено на классах эквивалентности и $\mathrm{PGL}(n+1,k)$ является группой, которая называется *проективной линейной группой*.

   (c) Докажите, что две матрицы $A, A' \in \mathrm{GL}(n+1,k)$ задают одно и то же отображение $\mathbb{P}^n \to \mathbb{P}^n$ в том и только том случае, когда $A \sim A'$. Следовательно, мы можем рассматривать $\mathrm{PGL}(n+1,k)$ как множество обратимых линейных преобразований на $\mathbb{P}^n$.

2. Докажите равенство (2).
3. Докажите, что проективная эквивалентность является отношением эквивалентности на множестве проективных многообразий в $\mathbb{P}^n$.
4. Докажите, что гиперплоскости $\mathbf{V}(x_i)$ и $\mathbf{V}(x_0)$ проективно эквивалентны. Указание: см. (5).
5. В этом упражнении рассматривается доказательство теоремы 4.
   (a) Пусть $f = \sum_{i,j=0}^n a_{ij}x_ix_j$, $a_{01} \neq 0$ и $a_{ii} = 0$ для всех i. Докажите, что замена координат (6) преобразует f к виду $\sum_{i,j=0}^n c_{ij}X_iX_j$, где $c_{00} = a_{01}$.
   (b) Пусть $f = \sum_{i,j=0}^n a_{ij}x_ix_j$, $a_{00} \neq 0$. Докажите, что замена координат (7) преобразует f к виду $a_{00}X_0^2 + \sum_{i,j=1}^n d_{ij}X_iX_j$.
6. Пусть $f = \sum_{i,j=0}^n a_{ij}x_ix_j$, а Q — матрица (a_{ij}) размера $(n+1)\times(n+1)$.
   (a) Докажите, что $f(\mathbf{x}) = \mathbf{x}^tQ\mathbf{x}$.
   (b) Пусть поле k имеет характеристику 2 (например, $k = \mathbb{F}_2$) и $f = x_0x_1$. Докажите, что *не* существует симметрической 2×2-матрицы Q с элементами из k, такой, что $f(\mathbf{x}) = \mathbf{x}^tQ\mathbf{x}$.
7. Используя теорему 4 и предложение 7, представьте следующие выражения в виде суммы квадратов ($k = \mathbb{C}$):
   (a) $x_0x_1 + x_0x_2 + x_2^2$;
   (b) $x_0^2 + 4x_1x_3 + 2x_2x_3 + x_4^2$;
   (c) $x_0x_1 + x_2x_3 - x_4x_5$.
8. Пусть $f = \sum_{i,j=0}^n a_{ij}x_ix_j$ — ненулевой полином с вещественными коэффициентами. Докажите, что существуют целые числа $r \geq -1$ и $s \geq 0$, $0 \leq r+s \leq n$, такие, что f может быть преобразован к виду

$$x_0^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2$$

   с помощью подходящей замены координат (с вещественными коэффициентами). Можно также доказать, что числа r и s однозначно определяются по f.
9. Пусть $f = \sum_{i,j=0}^n a_{ij}x_ix_j \in k[x_0,\ldots,x_n]$ — ненулевой полином. Мы отмечали, что $\mathbf{V}(f)$ является неособой квадрикой в том и только том случае, когда $\det(a_{ij}) \neq 0$. В этом упражнении мы будем изучать *особые* квадрики (т. е. те, которые не являются неособыми).
   (a) Докажите, что $\mathbf{V}(f)$ особа в том и только том случае, когда существует точка $a \in \mathbb{P}^n$ с однородными координатами $(a_0,\ldots,a_n)$, такая, что

$$\frac{\partial f}{\partial x_0}(a) = \ldots = \frac{\partial f}{\partial x_n}(a) = 0.$$

   (b) Пусть точка $a \in \mathbb{P}^n$ такая же, как в п. (a). Докажите, что $a \in \mathbf{V}(f)$. Обобщая, можно дать следующее определение: точка a на гиперповерхности $\mathbf{V}(f)$ (квадратичной или нет) называется *особой*, если все частные производные полинома f обращаются в нуль в a. Указание: используйте упр. 17 к § 2.

10. Рассмотрим квадрику $\mathbf{V}(f) \subset \mathbb{P}^n$ ранга $p+1$, где $p < n$. Докажите, что существует биекция $\mathbf{V}(f) \cong \mathbf{V}(g) \times \mathbb{P}^{n-p}$, где $\mathbf{V}(g)$ — неособая квадрика. Указание: можно считать, что $f = c_0x_0^2 + \ldots + c_px_p^2$, где $c_0, \ldots, c_p$ не равны нулю.

11. Рассмотрим отображение $F : \mathbb{P}^1 \to \mathbb{P}^2, F(u,v) = (u^2, uv, v^2)$.
    (a) Используя теорию исключения, докажите, что образ отображения F принадлежит квадрике $\mathbf{V}(x_0x_2 - x_1^2)$.
    (b) Докажите, что $F : \mathbb{P}^1 \to \mathbf{V}(x_0x_2 - x_1^2)$ является биекцией. Указание: рассуждайте, как в доказательстве предложения 10.

12. В этом упражнении мы будем изучать отображение Сегре $\sigma : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$.
    (a) Используя теорию исключения, докажите, что образ отображения σ принадлежит квадрике $\mathbf{V}(z_0z_3 - z_1z_2)$.
    (b) Используя указания, данные в тексте параграфа, докажите инъективность σ.

13. В этом и в следующем упражнениях мы будем работать с прямыми в $\mathbb{P}^n$. Пусть $p, q \in \mathbb{P}^n$ — две различные точки, которые мы также будем рассматривать как линейно независимые векторы в k^{n+1}.
    (a) Определим отображение $F : \mathbb{P}^1 \to \mathbb{P}^n$ формулой $F(u,v) = up - vq$. Докажите, что это отображение определено на всем $\mathbb{P}^1$ и инъективно.
    (b) Пусть $l = a_0x_0 + \ldots + a_nx_n$. Докажите, что l обращается в нуль на образе отображения F в том и только том случае, когда $p, q \in \mathbf{V}(l)$.
    (c) Мы хотим доказать, что образом отображения F является многообразие, определенное линейными уравнениями. Пусть Ω есть $2 \times (n+1)$-матрица, строками которой являются координаты точек p и q. Обратите внимание, что Ω имеет ранг 2. Она задает линейное отображение $\Omega : k^{n+1} \to k^2$. Ядро этого отображения имеет размерность $n-1$. Пусть векторы $v_1, \ldots, v_{n-1}$ образуют базис ядра, а l_i — линейные полиномы, коэффициенты которых равны координатам векторов v_i. Докажите, что образ отображения F совпадает с многообразием $\mathbf{V}(l_1, \ldots, l_{n-1})$. Указание: рассмотрите подпространство в k^{n+1}, заданное уравнениями $l_1 = \ldots = l_{n-1} = 0$.

14. В этом упражнении мы обсудим некоторые элементарные свойства прямых в $\mathbb{P}^n$.
    (a) Рассмотрим точки $p \neq q$ в $\mathbb{P}^n$. Докажите, что существует только одна прямая, проходящая через p и q.
    (b) Пусть L — прямая в $\mathbb{P}^n$, а $U_i \cong k^n$ — аффинная часть пространства $\mathbb{P}^n$, где $x_i \neq 0$. Докажите, что $L \cap U_i$ является прямой в k^n в обычном смысле этого слова.
    (c) Докажите, что все прямые в $\mathbb{P}^n$ проективно эквивалентны. Указание: в п. (c) упр. 13 было доказано, что прямая имеет вид $L = \mathbf{V}(l_1, \ldots, l_{n-1})$. Докажите, что можно выбрать полиномы l_n и l_{n+1} так, что $X_0 = l_1, \ldots, X_n = l_{n+1}$ — замена координат. Как выглядит уравнение прямой L в новой системе координат?

15. Пусть $\sigma : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ — отображение Сегре.
    (a) Докажите, что $L'_a = \sigma(\{a\} \times \mathbb{P}^1)$ является прямой в $\mathbb{P}^3$.
    (b) Докажите, что каждая точка квадрики $\mathbf{V}(z_0z_3 - z_1z_2)$ лежит на единственной прямой L'_a. Это доказывает, что семейство прямых $\{L'_a : a \in \mathbb{P}^1\}$ «заметает» всю квадрику.

16. В этом упражнении мы рассмотрим доказательство теоремы 11.
    (a) Докажите, что $\omega(up - vq, sp - tq) = (vs - ut)\omega(p,q)$. Указание: обозначим 2×4-матрицу, строками которой являются координаты точек p и q, через $\begin{pmatrix} p \\ q \end{pmatrix}$. Тогда
    $$\begin{pmatrix} up - vq \\ sp - tq \end{pmatrix} = \begin{pmatrix} u & -v \\ s & -t \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix}.$$
    (b) Применяя теорию исключения к равенствам (11), докажите, что плюккеровы координаты удовлетворяют соотношению $w_{01}w_{23} - w_{02}w_{13} + w_{03}w_{12} = 0$.
    (c) Завершите доказательство теоремы 11, показав, что отображение ω сюръективно.

17. В этом упражнении мы рассмотрим плюккеровы координаты для прямых в $\mathbb{P}^4$.
    (a) Рассмотрим прямую $L \subset \mathbb{P}^4$. Используя однородные координаты точек $p, q \in L$, определите плюккеровы координаты и докажите, что точка $\omega(L) \in \mathbb{P}^9$ не зависит от выбора точек p и q на L.
    (b) Найдите соотношения между плюккеровыми координатами и определите с их помощью многообразие $V \subset \mathbb{P}^9$, такое, что $\omega(L) \in V$ для всех L.
    (c) Докажите, что ω задает биективное отображение множества прямых в $\mathbb{P}^4$ на V.

18. Докажите, что существует взаимно однозначное соответствие между множеством прямых в $\mathbb{P}^3$ и множеством плоскостей в k^4, проходящих через начало координат. Это объясняет, чем прямая в $\mathbb{P}^3$ отличается от прямой в k^3 или k^4.

19. Существует интересная связь между прямыми в $\mathbb{P}^3$ и главными ступенчатыми 2×4-матрицами ранга 2. Пусть $V = \mathbf{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12})$ — квадрика из теоремы 11.
    (a) Докажите, что существует взаимно однозначное соответствие между главными ступенчатыми матрицами вида
    $$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}$$
    и точками множества $V \cap U_{01}$, где U_{01} — аффинная часть пространства $\mathbb{P}^5$, определенная условием $z_{01} \neq 0$. Указание: строки

этой матрицы определяют прямую в $\mathbb{P}^5$. Что из себя представляют плюккеровы координаты этой прямой?

(b) Матрицы из п. (a) не исчерпывают все множество матриц главного ступенчатого вида ранга 3. Например, матрицы

$$\begin{pmatrix} 1 & a & 0 & b \\ 0 & 0 & 1 & c \end{pmatrix}$$

— также главные ступенчатые матрицы ранга 2. Докажите, что существует взаимно однозначное соответствие между такими матрицами и точками множества $V \cap U_{01} \cap U_{02}$.

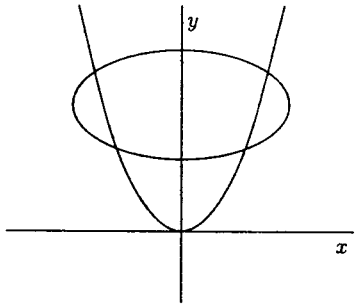
(c) Докажите, что существует еще четыре типа главных ступенчатых 2×4-матриц ранга 2 и докажите, что матрицы каждого типа находятся во взаимно однозначном соответствии с некоторыми подмножествами многообразия V. Указание: столбцы, содержащие главные единицы, соответствуют плюккеровым координатам, равным 1.

(d) Приведите прямое доказательство (не использующее плюккеровых координат) того, что главные ступенчатые 2×4-матрицы ранга 2 находятся во взаимно однозначном соответствии с прямыми в $\mathbb{P}^3$. Указание: см. упр. 18.

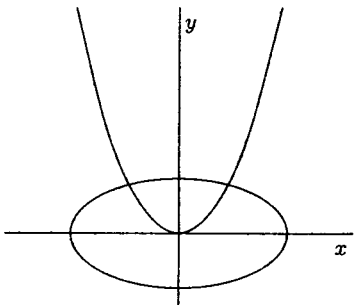
§ 7. Теорема Безу

В этом параграфе мы рассмотрим задачу о пересечении двух кривых на плоскости. Нас будет интересовать *число* точек пересечения. Следующие примеры показывают, почему ответ выглядит особенно хорошо, если мы работаем с кривыми в $\mathbb{P}^2(\mathbb{C})$. Нам понадобится также определить *кратность* точки пересечения. К счастью, техника гл. 3 позволяет относительно легко сделать это.

Пример 1. Рассмотрим пересечение параболы $y = x^2$ и эллипса $x^2 + 4(y - \lambda)^2 = 4$, где λ — параметр.



$\lambda = 2$



$\lambda = 0$

Над $\mathbb{R}$ число точек пересечения различно для разных λ и, более того, существуют такие значения λ, при которых эти кривые *не* пересекаются (см. упр. 1). Но над $\mathbb{C}$ эти кривые имеют четыре точки пересечения в *обоих* случаях ($\lambda = 0, 2$). Пусть, например, $\lambda = 0$. Тогда, исключая x из $y = x^2$ и $x^2 + 4y^2 = 4$, получаем, что $y + 4y^2 = 4$, т. е.

$$y = \frac{-1 \pm \sqrt{65}}{8}.$$

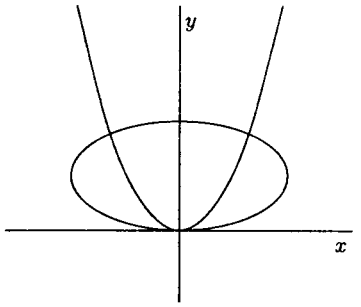
Следовательно,

$$x = \pm\sqrt{\frac{-1 \pm \sqrt{65}}{8}}.$$

Это дает нам 4 точки пересечения, две вещественные и две комплексные (так как $-1 - \sqrt{65} < 0$). Легко проверить, что при $\lambda = 2$ рассмотрение комплексных чисел не увеличивает количества пересечений по сравнению с четырьмя пересечениями, изображенными на рисунке (см. упр. 1).

Отсюда следует, что число точек пересечения легче предсказать, когда мы работаем над $\mathbb{C}$. Можно также проверить, что в тех случаях, когда вещественных пересечений нет совсем, мы по-прежнему имеем четыре точки пересечения над $\mathbb{C}$ (см. упр. 1).

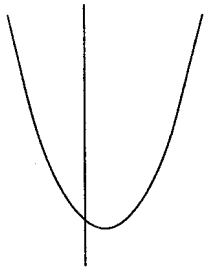
Но и над $\mathbb{C}$ возможны неожиданности. Рассмотрим, например, пересечение эллипса и параболы при $\lambda = 1$:



$\lambda = 1$

Мы видим только три точки пересечения, и то же самое справедливо над $\mathbb{C}$. Но начало координат, очевидно, является «особым» типом пересечения, так как две кривые касаются в этой точке. Как мы увидим ниже, эта точка пересечения имеет *кратность два*, в то время как другие точки пересечения имеют *кратность один*. Если мы будем учитывать и кратность точки пересечения, то получим в сумме четыре.

Пример 2. Рассмотрим пересечение параболы $y = x^2$ с прямой L. Легко видеть, что в большинстве случаев имеется две точки пересечения над $\mathbb{C}$ с учетом кратностей (см. упр. 2). Но если речь идет о пересечении с *вертикальной* прямой,



то имеется только одна точка пересечения кратности 1. Но мы хотим, чтобы их было две, так как во всех других случаях число точек пересечения именно таково. Где же прячется еще одна точка пересечения?

Чтобы ее найти нужно проективизировать задачу. Тогда ответ ясен: это точка «на бесконечности». Чтобы убедиться в этом, гомогенизируем уравнения параболы $y = x^2$ и прямой $x = c$ и получим уравнения $yz = x^2$ и $x = cz$. Тогда $yz = c^2z^2$ и точками пересечения будут $(c, c^2, 1)$ и $(0, 1, 0)$ (напомним, что это однородные координаты). Первая точка принадлежит аффинной части пространства $\mathbb{P}(\mathbb{C})$, где $z \neq 0$, и именно ее мы видим на рисунке, а вторая — прямой на бесконечности (где $z = 0$).

Пример 3. Рассмотрим две кривые в $\mathbb{P}^2(\mathbb{C})$: $C = \mathbf{V}(x^2 - z^2)$ и $D = \mathbf{V}(x^2y - xz^2 - xyz + z^3)$. Легко проверить, что точка $(1, b, 1)$ лежит в $C \cap D$ для любого $b \in \mathbb{C}$, так что пересечение $C \cap D$ бесконечно! Чтобы понять, почему это могло произойти, разложим определяющие полиномы на множители:

$$x^2 - z^2 = (x - z)(x + z), \quad x^2y - xz^2 - xyz + z^3 = (x - z)(xy - z^2).$$

Таким образом, C является объединением двух проективных прямых, а D есть объединение прямой и коники. На самом деле эти прямые и коника являются неприводимыми компонентами кривых C и D в смысле § 3 (см. предложение 4 ниже). Теперь мы видим причину: C и D имеют общую неприводимую компоненту $\mathbf{V}(x - z)$ и именно поэтому их пересечение бесконечно.

Эти примеры объясняют, почему мы предпочитаем комплексный случай. До конца параграфа мы будем работать над $\mathbb{C}$ и писать $\mathbb{P}^2$ вместо $\mathbb{P}^2(\mathbb{C})$. Под *кривой* мы будем понимать проективное

многообразие $\mathbf{V}(f)$, заданное ненулевым однородным полиномом $f \in \mathbb{C}[x, y, z]$. Рассмотренные примеры указывают, что мы должны учитывать кратности пересечения и неприводимые компоненты кривых. Мы начнем с изучения неприводимых компонент.

Предложение 4. *Пусть $f \in \mathbb{C}[x, y, z]$ — ненулевой однородный полином. Тогда его неприводимые сомножители также однородны, и если мы разложим f в произведение неприводимых сомножителей,*

$$f = f_1^{a_1} \dots f_s^{a_s},$$

где f_i попарно различны, причем ни один из f_i не является скалярным кратным другого, то

$$\mathbf{V}(f) = \mathbf{V}(f_1) \cup \dots \cup \mathbf{V}(f_s)$$

является минимальным разложением многообразия $\mathbf{V}(f)$ на неприводимые компоненты. Более того,

$$\mathbf{I}(\mathbf{V}(f)) = \sqrt{\langle f \rangle} = \langle f_1 \dots f_s \rangle.$$

Доказательство. Пусть $f = gh$, где $g, h \in \mathbb{C}[x, y, z]$. Мы утверждаем, что g и h однородны. Пусть $g = g_m + \dots + g_0$ — представление полинома g в виде суммы однородных компонент, где g_i имеет полную степень i и $g_m \neq 0$. Аналогично, пусть $h = h_n + \dots + h_0$. Тогда

$$\begin{aligned} f = gh &= (g_m + \dots + g_0)(h_n + \dots + h_0) \\ &= g_m h_n + \text{члены меньшей полной степени.} \end{aligned}$$

Так как f однороден, то $f = g_m h_n$ и $g = g_m, h = h_n$ (см. упр. 3), т. е. g и h однородны. Отсюда легко следует, что каждый неприводимый сомножитель полинома f однороден.

Тот факт, что $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \dots \cup \mathbf{V}(f_s)$ является минимальным разложением на неприводимые компоненты, следует из проективной версии упр. 9 к § 6 гл. 4. Так как многообразие $\mathbf{V}(f)$ непусто (см. упр. 6), то утверждение о $\mathbf{I}(\mathbf{V}(f))$ следует из проективной теоремы о нулях и предложения 9 из § 2 гл. 4.

Из предложения 4 следует, что каждая кривая $C \subset \mathbb{P}^2$ имеет «наилучшее» уравнение. Если $C = \mathbf{V}(f)$, где f — некоторый однородный полином, то $\mathbf{I}(C) = \langle f_1 \dots f_s \rangle$, где $f_1, \dots, f_s$ — различные неприводимые делители полинома f. Таким образом, любой полином, определяющий C, делится на $f_1 \dots f_s$; следовательно, $f_1 \dots f_s = 0$ является определяющим уравнением наименьшей степени. В терминах § 2 гл. 4 полином $f_1 \dots f_s$ является редуцированным (или свободным от квадратов). Поэтому $f_1 \dots f_s = 0$ называется *редуцированным* уравнением кривой C. Это уравнение единственно с точностью до постоянного множителя.

Рассматривая пересечение двух кривых C и D в $\mathbb{P}^2$, мы будем считать, что C и D не имеют общих неприводимых компонент. Это означает, что определяющие их полиномы не имеют общих сомножителей. Наша цель — связать число точек в $C \cap D$ со степенями редуцированных уравнений. Следующее свойство результантов играет важную роль в этой задаче.

Лемма 5. *Пусть $f, g \in \mathbb{C}[x, y, z]$ — однородные полиномы степеней m и n соответственно. Если $f(0,0,1) \neq 0$ и $g(0,0,1) \neq 0$, то* $\operatorname{Res}(f, g, z)$ *является однородным полиномом от x и y полной степени mn.*

Доказательство. Запишем f и g как полиномы от z:

$$f = a_0 z^m + \ldots + a_m,$$
$$g = b_0 z^n + \ldots + b_n.$$

Так как f — однородный полином полной степени m, то $a_i \in \mathbb{C}[x, y]$ — однородные полиномы полной степени i для всех i. Так как $f(0,0,1) \neq 0$, то a_0 — ненулевая константа. Аналогично b_i однородны полной степени i и $b_0 \neq 0$.

Результант — это определитель порядка $m+n$ (см. § 5 гл. 3)

$$\operatorname{Res}(f, g, z) = \det \begin{pmatrix} a_0 & & & b_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_m & & a_0 & b_n & & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_m & & & b_n \end{pmatrix},$$

где n столбцов отведено полиномам a_i, m столбцов отведено полиномам b_i, а на пустых местах стоят нули. Докажем, что $\operatorname{Res}(f, g, z)$ — однородный полином полной степени mn. Для этого обозначим через c_{ij} ij-й элемент матрицы. Если $c_{ij} \neq 0$, то

$$c_{ij} = \begin{cases} a_{i-j}, & \text{если } j \leq n, \\ b_{n+i-j}, & \text{если } j > n. \end{cases}$$

Таким образом, ненулевой элемент c_{ij} однороден полной степени $i - j$ (если $j \leq n$) или $n + i - j$ (если $j > n$).

Этот определитель является суммой произведений вида (см. § 3 из приложения А)

$$\pm \prod_{i=1}^{m+n} c_{i\sigma(i)},$$

где σ — перестановка набора $\{1, \ldots, m+n\}$. Предположим, что каждый элемент $c_{i\sigma(i)}$ в этом произведении не равен нулю. Запишем

это произведение в виде

$$\pm \prod_{\sigma(i) \leq n} c_{i\sigma(i)} \prod_{\sigma(i) > n} c_{i\sigma(i)}.$$

Это произведение является однородным полиномом степени

$$\sum_{\sigma(i) \leq n} (i - \sigma(i)) + \sum_{\sigma(i) > n} (n + i - \sigma(i)).$$

Так как σ — перестановка набора $\{1, \ldots, m+n\}$, то в первой сумме содержится n членов, а во второй содержится m членов, причем каждое $i, 1 \leq i \leq m+n$, появляется в этой сумме ровно один раз. Следовательно, мы можем преобразовать сумму к виду

$$mn + \sum_{i=1}^{m+n} i - \sum_{i=1}^{m+n} \sigma(i) = mn,$$

т. е. $\operatorname{Res}(f, g, z)$ является суммой однородных полиномов степени mn. □

Мы доказали, что результант $\operatorname{Res}(f, g, z)$ однороден по переменным x и y. Однородный полином от двух переменных имеет особенно простую структуру.

Лемма 6. *Рассмотрим ненулевой однородный полином $h \in \mathbb{C}[x, y]$. Он может быть записан в виде*

$$h = c(s_1 x - r_1 y)^{m_1} \ldots (s_t x - r_t y)^{m_t},$$

где $c \neq 0$ в $\mathbb{C}$, а $(r_1, s_1), \ldots, (r_t, s_t)$ — различные точки из $\mathbb{P}^1$. Более того,

$$\mathbf{V}(h) = \{(r_1, s_1), \ldots, (r_t, s_t)\} \subset \mathbb{P}^1.$$

Доказательство. Утверждение леммы является следствием того, что полином $h(x, 1) \in \mathbb{C}[x]$ разлагается в произведение линейных множителей (так как $\mathbb{C}$ алгебраически замкнуто). Детали доказательства мы оставляем в качестве упражнения. □

Теперь мы, используя эти леммы, найдем оценку числа точек пересечения двух проективных кривых.

Теорема 7. *Пусть C и D — проективные кривые в $\mathbb{P}^2$, не имеющие общих неприводимых компонент. Пусть степень редуцированного уравнения кривой C равна m, а степень редуцированного уравнения кривой D равна n. Тогда $C \cap D$ конечно и число точек в нем не превосходит mn.*

Доказательство. Пусть множество $C \cap D$ содержит более чем mn точек. Выберем $mn+1$ из них и обозначим их через $p_1, \ldots, p_{mn+1}$. Пусть $L_{ij}, 1 \le i < j \le mn+1$, обозначает прямую, проходящую через точки p_i и p_j. Выберем точку $q \in \mathbb{P}^2$, такую, что

$$q \notin C \cup D \cup \bigcup_{i<j} L_{ij} \tag{1}$$

(в упр. 6 будет дано подробное доказательство того, что такая точка существует).

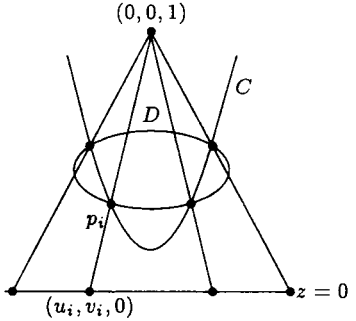
Найдем такую матрицу $A \in \mathrm{GL}(3, \mathbb{C})$ (напомним, что A задает линейное отображение $\mathbb{P}^2 \to \mathbb{P}^2$), что $A(q) = (0,0,1)$ (см. упр. 6). Будем считать, что A определяет новые координаты на $\mathbb{P}^2$ (см. формулу (3) в § 6). Тогда в новой системе координат точка q имеет координаты $(0,0,1)$.

Пусть $C = \mathbf{V}(f)$ и $D = \mathbf{V}(g)$, где f и g — редуцированные полиномы степеней m и n соответственно. Тогда из (1) следует, что $f(0,0,1) \neq 0$, так как $q \notin C$, и $g(0,0,1) \neq 0$, так как $q \notin D$. Тогда по лемме 5 результант $\mathrm{Res}(f,g,z)$ является однородным полиномом степени mn по x, y. Так как степени полиномов f и g по z положительны и эти полиномы не имеют общих делителей в $\mathbb{C}[x,y,z]$, то $\mathrm{Res}(f,g,z) \neq 0$ (предложение 1 из § 6 гл. 3).

Пусть $p_i = (u_i, v_i, w_i)$. Так как результант принадлежит идеалу, порожденному полиномами f и g (предложение 1 из § 6 гл. 3), то

$$\mathrm{Res}(f,g,z)(u_i, v_i) = 0. \tag{2}$$

Обратите внимание, что прямая, соединяющая точку $q = (0,0,1)$ с точкой $p_i = (u_i, v_i, w_i)$, пересекает прямую $z = 0$ в точке $(u_i, v_i, 0)$ (см. упр. 6). Вот рисунок:



Отображение, переводящее точку $(u,v,w) \in \mathbb{P}^2 - \{(0,0,1)\}$ в точку $(u,v,0)$, является *отображением проекции из точки на прямую*. Из (2) следует, что $\mathrm{Res}(f,g,z)$ обращается в нуль в проекциях точек $p_i \in C \cap D$.

По условию (1) прямые, соединяющие точки p_i и p_j, не проходят через точку $(0,0,1)$; следовательно, точки $(u_i, v_i, 0), i = 1, \ldots, mn+1$, — это различные точки на прямой $z = 0$. Будем рассматривать прямую $z = 0$ как проективное пространство $\mathbb{P}^1$ с однородными координатами x, y. Тогда ненулевой полином $\mathrm{Res}(f,g,z)$ обращается в нуль в $mn+1$ точках $(u_i, v_i) \in \mathbb{P}^1$. Но степень полинома $\mathrm{Res}(f,g,z)$ равна mn — противоречие. Теорема доказана. □

Мы получили критерий конечности пересечения $C \cap D$. Теперь нам нужно определить *кратность пересечения* в каждой точке $p \in C \cap D$. Это можно сделать многими способами, но проще всего — с помощью результанта.

Рассмотрим кривые C и D на $\mathbb{P}^2$, не имеющие общих компонент и заданные редуцированными уравнениями $f = 0$ и $g = 0$. Для каждой пары точек $p, q \in C \cap D, p \neq q$, обозначим через L_{pq} проективную прямую, соединяющую p и q. Найдем матрицу $A \in \mathrm{GL}(3, \mathbb{C})$, такую, что в новой системе координат, заданной этой матрицей,

$$(0,0,1) \notin C \cup D \cup \bigcup_{p,q \in C \cap D, p \neq q} L_{pq}. \tag{3}$$

(В примере 9 ниже показано, как найти такую систему координат.) Как и в доказательстве теоремы 7, если $p = (u,v,w) \in C \cap D$, то $\mathrm{Res}(f,g,z)(u,v) = 0$. Поэтому по лемме 6 полином $\mathrm{Res}(f,g,z)$ делится на $vx - uy$.

Определение 8. Рассмотрим кривые C и D на плоскости $\mathbb{P}^2$, не имеющие общих компонент и заданные редуцированными уравнениями $f = 0$ и $g = 0$. Выберем такую систему координат на $\mathbb{P}^2$, чтобы условие (3) было выполнено. Пусть $p = (u,v,w) \in C \cap D$. Тогда *кратностью пересечения* $I_p(C,D)$ кривых C и D в точке p называется степень множителя $vx - uy$ в разложении на множители полинома $\mathrm{Res}(f,g,z)$.

Чтобы убедиться в корректности этого определения, нам нужно доказать, что мы получим одну и ту же кратность во всех системах координат, удовлетворяющих условию (3). Примем пока этот факт на веру и рассмотрим несколько примеров.

Пример 9. Рассмотрим в $\mathbb{C}[x,y,z]$ два полинома

$$f = x^3 + y^3 - 2xyz,$$
$$g = 2x^3 - 4x^2y + 3xy^2 + y^3 - 2y^2z.$$

Эти полиномы (пример взят из книги WALKER (1950)) определяют кубические кривые $C = \mathbf{V}(f)$ и $D = \mathbf{V}(g)$ в $\mathbb{P}^2$. Найдем их результант

относительно z:

$$\operatorname{Res}(f,g,z) = -2y(x-y)^3(2x+y).$$

Так как результант принадлежит исключающему идеалу, то для точек из $C \cap D$ либо $y=0$, либо $x-y=0$, либо $2x+y=0$. Легко убедиться, что $C \cap D$ состоит из трех точек

$$p=(0,0,1), \quad q=(1,1,1), \quad r=(4/7,-8/7,1)$$

(см. упр. 7). В частности, это показывает, что C и D не имеют общих компонент.

Но найденный нами результант *не* дает правильных кратностей, так как точка $(0,0,1)$ лежит в C (она даже является точкой пересечения). Следовательно, нужно произвести замену координат. Начнем с точки

$$(0,1,0) \notin C \cup D \cup L_{pq} \cup L_{pr} \cup L_{qr}$$

и найдем замену координат, такую, что $A(0,1,0)=(0,0,1)$. Например, $A(x,y,z)=(z,x,y)$. Тогда

$$(0,0,1) \notin A(C) \cup A(D) \cup L_{A(p)A(q)} \cup L_{A(p)A(r)} \cup L_{A(q)A(r)}.$$

Для того чтобы найти определяющее уравнение кривой $A(C)$, отметим, что

$$(u,v,w) \in A(C) \iff A^{-1}(u,v,w) \in C \iff f(A^{-1}(u,v,w))=0.$$

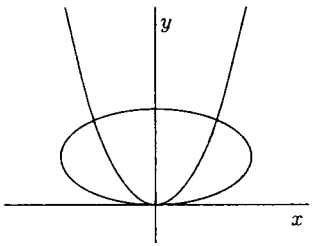
Таким образом, $A(C)$ определена уравнением $f \circ A^{-1}(x,y,z) = f(y,z,x)=0$. Аналогично $A(D)$ определена уравнением $g(y,z,x)=0$. Тогда по определению 8 результант $\operatorname{Res}(f(y,z,x),g(y,z,x),z)$ позволит найти кратности пересечения в точках $A(p)=(1,0,0)$, $A(q)=(1,1,1)$ и $A(r)=(1,4/7,-8/7)$. Имеем

$$\operatorname{Res}(f(y,z,x),g(y,z,x),z) = 8y^5(x-y)^3(4x-7y).$$

Значит,

$$I_p(C,D)=5, \quad I_q(C,D)=3, \quad I_r(C,D)=1.$$

Пример 1 (продолжение). В примере 1 положим $\lambda=1$. Тогда рассматриваемые кривые выглядят так:



Точка $(0,0,1)$ на этом рисунке находится в начале координат; поэтому опять необходимо сделать замену координат. В упражнениях такая замена будет найдена и будет показано, что кратность пересечения в начале координат равна двум.

Считая определение кратности корректным, мы можем теперь доказать теорему Безу.

Теорема 10 (теорема Безу). *Пусть C и D — кривые на проективной плоскости $\mathbb{P}^2$, не имеющие общих компонент, и пусть m и g — степени их редуцированных уравнений. Тогда*

$$\sum_{p \in C \cap D} I_p(C,D) = mn,$$

где $I_p(C,D)$ — кратность пересечения кривых C и D в точке p (см. определение 8).

Доказательство. Пусть $f=0$ и $g=0$ — редуцированные уравнения кривых C и D. Предположим, что система координат выбрана так, что условие (3) выполнено. Координаты точки $p \in C \cap D$ будем обозначать через (u_p,v_p,w_p). Мы утверждаем, что

$$\operatorname{Res}(f,g,z) = c \prod_{p \in C \cap D} (v_p x - u_p y)^{I_p(C,D)},$$

где c — ненулевая константа. Очевидно, что для каждого p по определению кратности $(v_p x - u_p y)^{I_p(C,D)}$ — это в точности степень полинома $v_p x - u_p y$, делящая результант. Надо доказать, что результант *не имеет* других корней. Пусть $(u,v) \in \mathbb{P}^1$ и $\operatorname{Res}(f,g,z)(u,v)=0$. Тогда из предложения 3 из § 6 гл. 3 следует, что существует $w \in \mathbb{C}$, такое, что $f(u,v,w)=g(u,v,w)=0$ (потому что в представлении полиномов f и g из леммы 5 a_0 и b_0 являются ненулевыми константами). Таким образом, $(u,v,w) \in C \cap D$, и утверждение доказано.

По лемме 5 $\operatorname{Res}(f,g,z)$ является ненулевым полиномом степени mn. Таким образом, теорема Безу сводится к сравнению степеней в правой и левой частях рассматриваемого равенства. □

Пример 9 (продолжение). В примере 9 две кубические кривые пересекаются в точках $(0,0,1),(1,1,1)$ и $(4/7,-8/7,1)$ с кратностями $5,3$ и 1 соответственно. Сумма кратностей равна $9=3\cdot 3$, как и ожидалось. Возвращаясь к нашим вычислениям в примере 9, мы видим, почему нам понадобилась замена координат для вычисления кратностей. В исходных координатах $\operatorname{Res}(f,g,z) = -2y(x-y)^3(2x+y)$, что дает кратности $1,3$ и 1. Этот результат не может быть правильным, так как их сумма не равна 9.

Наконец, нам нужно доказать, что кратности определены корректно.

Лемма 11. *В определении* 8 *все замены координат, удовлетворяющие условию* (3), *дают одну и ту же кратность пересечения* $I_p(C,D)$ *в точке* $p \in C \cap D$.

Доказательство. Хотя этот результат справедлив над любым алгебраически замкнутым полем, наше доказательство использует соображения непрерывности и потому корректно только над $\mathbb{C}$. Сначала точно определим, какие именно замены координат мы будем использовать. Как и в примере 9, выберем точку

$$r \notin C \cup D \cup \bigcup_{p,q \in C \cap D, p \neq q} L_{pq}$$

и матрицу $A \in \mathrm{GL}(3,\mathbb{C})$, такие, что $A(r) = (0,0,1)$. Это означает, что $A^{-1}(0,0,1) = r$. Поэтому матрица A должна удовлетворять условию

$$A^{-1}(0,0,1) \notin C \cup D \cup \bigcup_{p,q \in C \cap D, p \neq q} L_{pq}.$$

Обозначим через l_{pq} уравнение прямой L_{pq} и положим

$$h = f \cdot g \cdot \prod_{p,q \in C \cap D, p \neq q} l_{pq}.$$

Таким образом, матрица A должна удовлетворять условию $A^{-1}(0,0,1) \notin \mathbf{V}(h)$, т. е. $h(A^{-1}(0,0,1)) \neq 0$.

Переформулируем нашу задачу так, чтобы в ее формулировке не возникали обратные матрицы. Рассмотрим пространство $M_{3\times 3}(\mathbb{C})$ всех 3×3-матриц с комплексными элементами и определим функцию $H : M_{3\times 3}(\mathbb{C}) \to \mathbb{C}$ следующим образом:

$$H(B) = \det(B) \cdot h(B(0,0,1)),$$

где $B \in M_{3\times 3}(\mathbb{C})$. Если $B = (b_{ij})$, то $H(B)$ является полиномом от b_{ij}. Так как матрица обратима в том и только том случае, когда ее определитель не равен нулю, то

$$H(B) \neq 0 \Longleftrightarrow B \text{ обратима и } h(B(0,0,1)) \neq 0.$$

Тогда требуемая замена координат задается матрицей $A = B^{-1}$, $B \in M_{3\times 3}(\mathbb{C}) - \mathbf{V}(H)$.

Пусть $C \cap D = \{p_1, \ldots, p_s\}$ и для каждой матрицы $B \in M_{3\times 3}(\mathbb{C}) - \mathbf{V}(H)$ пусть $B^{-1}(p_i) = (u_{i.B}, v_{i.B}, w_{i.B})$. Рассуждая, как в теореме 10, имеем

$$\mathrm{Res}(f \circ B, g \circ B, z) = c_B (v_{1.B}x - u_{1.B}y)^{m_{1.B}} \ldots (v_{s.B}x - u_{s.B}y)^{m_{s.B}}, \tag{4}$$

где $c_B \neq 0$. Это означает, что $I_{p_i} = m_{i.B}$ при замене координат, заданной матрицей $A = B^{-1}$. Таким образом, мы должны доказать, что числа $m_{i.B}$ одни и те же для *всех* $B \in M_{3\times 3}(\mathbb{C}) - \mathbf{V}(H)$.

Сначала рассмотрим, что происходит при разложении на множители

$$F(x,y) = (vx - uy)^m G(x,y),$$

где полиномы F и G однородны, а $(u,v) \neq (0,0)$. Нетрудно доказать, что

$$\frac{\partial^{i+j} F}{\partial x^i \partial y^j}(u,v) = \begin{cases} 0, & \text{если } 0 \leq i+j < m, \\ m! v^i (-u)^j G(u,v), & \text{если } i+j = m \end{cases} \tag{5}$$

(см. упр. 9). В частности, если $G(u,v) \neq 0$ (и $(u,v) \neq (0,0)$), то это означает, что хотя бы одна из m-х частных производных полинома F отлична от нуля в точке (u,v).

Определим расстояние между двумя матрицами $B, C \in M_{3\times 3}(\mathbb{C})$ как обычное евклидово расстояние, т. е. если $B = (b_{ij})$ и $C = (c_{ij})$, то

$$d(B,C) = \sqrt{\sum_{i,j=1}^{3} |b_{ij} - c_{ij}|^2}.$$

Решающим фактом является то, что функция $H : M_{3\times 3}(\mathbb{C}) \to \mathbb{C}$ непрерывна. Это означает, что ее значения для близких (в смысле расстояния) матриц близки. В частности, если $H(B_0) \neq 0$, то $H(B) \neq 0$, если B достаточно близка к B_0.

Рассмотрим теперь показатель степени $m = m_{i.B_0}$ для фиксированных i и B_0. Мы утверждаем, что $m_{i.B} \leq m$, если B достаточно близка к B_0. Отметим сначала, что из (4) и (5) следует, что некоторая m-я частная производная функции $\mathrm{Res}(f \circ B_0, g \circ B_0, z)$ не равна нулю в точке $(u_{i.B_0}, v_{i.B_0})$. Легко видеть, что значения частных производных функции $\mathrm{Res}(f \circ B, g \circ B, z)$ в точке $(u_{i.B}, v_{i.B})$ полиномиально зависят от элементов матрицы B. По соображениям непрерывности некоторая m-я частная производная функции $\mathrm{Res}(f \circ B, g \circ B, z)$ в точке $(u_{i.B}, v_{i.B})$ не равна нулю, если B достаточно близка к B_0. Отсюда следует, что $m_{i.B} \leq m$ (так как неравенство $m_{i.B} > m$ означает, что *все* m-е частные производные равны нулю в $(u_{i.B}, v_{i.B})$).

Но тогда, суммируя неравенства $m_{i.B} \leq m_{i.B_0}, i = 1, \ldots, s$, получаем

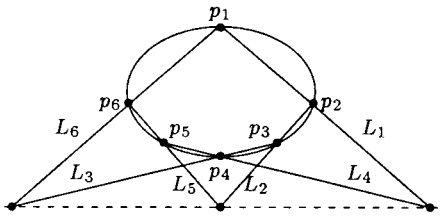
$$mn = \sum_{i=1}^{s} m_{i.B} \leq \sum_{i=1}^{s} m_{i.B_0} = mn.$$

Отсюда следует, что $m_{i.B} = m_{i.B_0}$, если матрица B достаточно близка к матрице B_0.

Это доказывает, что функция, сопоставляющая матрице B величину $m_{i.B}$, является *локально постоянной*, т. е. ее значения в близких точках совпадают. Чтобы доказать, что эта функция является константой на $M_{3\times3}(\mathbb{C}) - \mathbf{V}(H)$, нужно доказать, что множество $M_{3\times3}(\mathbb{C}) - \mathbf{V}(H)$ *линейно связно*. Это будет доказано в упр. 10, где также будет сформулировано точное определение линейной связности. Из теоремы о промежуточном значении непрерывной функции следует, что локально постоянная функция на линейно связном пространстве постоянна (см. упр. 10). Поэтому величина $m_{i.B}$ одна и та же для всех матриц $B \in M_{3\times3}(\mathbb{C}) - \mathbf{V}(H)$. Таким образом, корректность определения кратности пересечения доказана. □

Кратности пересечения $I_p(C, D)$ имеют ряд полезных свойств, которые облегчают их вычисление. Например, можно доказать, что $I_p(C, D) = 1$ в том и только том случае, когда p является неособой точкой как кривой C, так и кривой D, и касательные прямые к C и D в p различны. Обсуждение свойств кратностей читатель может найти в гл. 3 книги KIRWAN (1992). Следует указать, что использование результантов для определения и вычисления кратностей неудобно в следующем смысле. Кратность пересечения $I_p(C, D)$, очевидно, является *локальной* характеристикой — она зависит только от поведения кривых вблизи p, в то время как результант является *глобальной* характеристикой — для его вычисления используются уравнения кривых C и D. Существуют локальные методы вычисления кратностей пересечения, но они требуют более сложной математической техники. Локальная точка зрения рассматривается в гл. 3 книги FULTON (1969) и в гл. 4 книги WALKER (1950).

Применим результаты этого параграфа для доказательства следующей теоремы, принадлежащей Паскалю. Пусть даны 6 точек $p_1, \ldots, p_6$, лежащих на неприводимой конике в $\mathbb{P}^2$. По теореме Безу прямая пересекает конику не более чем в двух точках (см. упр. 11). Значит, существует 6 различных прямых, соединяющих p_1 и p_2, p_2 и p_3, ... и p_6 и p_1. Обозначим эти прямые через $L_1, \ldots, L_6$ (см. рисунок).



Прямые L_1 и L_4, L_2 и L_5, L_3 и L_6 мы назовем *противоположными*. Отрезки этих прямых, лежащие внутри коники, образуют шестиугольник, а противоположные прямые образуют противоположные стороны шестиугольника.

Если судить по этому рисунку, то точки пересечения противоположных прямых должны быть коллинеарны. Следующая теорема утверждает, что так оно и есть.

Теорема 12 (таинственный шестиугольник Паскаля). *Пусть даны шесть различных точек на неприводимой конике. Соединим их прямыми, как это было сделано выше. Тогда точки пересечения противоположных прямых коллинеарны.*

Доказательство. Обозначим конику через C. У нас есть 6 точек $p_1, \ldots, p_6$ и 3 пары противоположных прямых $\{L_1, L_4\}, \{L_2, L_5\}$ и $\{L_3, L_6\}$. Рассмотрим кривые $C_1 = L_1 \cup L_2 \cup L_3$ и $C_2 = L_4 \cup L_5 \cup L_6$. Эти кривые описываются кубическими уравнениями. Значит, по теореме Безу пересечение $C_1 \cap C_2$ состоит из 9 точек (с учетом кратностей). Но $C_1 \cap C_2$ содержит 6 исходных точек и 3 точки пересечений противоположных прямых (надо аккуратно это проверить). Таким образом, эти точки и составляют все множество $C_1 \cap C_2$, и кратность пересечения в каждой из них равна 1.

Пусть $C = \mathbf{V}(f), C_1 = \mathbf{V}(g_1)$ и $C_2 = \mathbf{V}(g_2)$, где f имеет степень 2, а g_1 и g_2 имеют степень 3. Возьмем на C точку p, отличную от $p_1, \ldots, p_6$. Тогда $g_1(p) \neq 0$ и $g_2(p) \neq 0$ (почему?); поэтому $g = g_2(p)g_1 - g_1(p)g_2$ является кубическим полиномом, который обращается в нуль в точках $p, p_1, \ldots, p_6$. Кроме того, $g \neq 0$; в противном случае полином g_1 был бы скалярным кратным полинома g_2 (и наоборот). Таким образом, кубика $\mathbf{V}(g)$ пересекает C по крайней мере в семи точках. Следовательно, условия теоремы Безу не выполнены. Значит, или полином g не является редуцированным, или C и $\mathbf{V}(g)$ имеют общую неприводимую компоненту. Первый случай не может иметь места, так как иначе кривая $\mathbf{V}(g)$ определялась бы полиномом степени не выше 2 и тогда пересечение $C \cap \mathbf{V}(g)$ состояло бы, самое большее, из четырех точек. Следовательно, C и $\mathbf{V}(g)$ имеют общую неприводимую компоненту. Но C неприводима; значит, $C = \mathbf{V}(f)$ является компонентой кривой $\mathbf{V}(g)$. Тогда по предложению 4 g делится на f.

Таким образом, $g = f \cdot l$, где полином l имеет степень 1. Так как g обращается в нуль в точках пересечения противоположных прямых, а f в этих точках нулю не равен, то l обращается в нуль в этих точках. Но $\mathbf{V}(l)$ является проективной прямой. Теорема доказана. □

Теорема Безу служит хорошим введением в теорию кривых на проективной плоскости. Эта часть алгебраической геометрии традиционно называется теорией *алгебраических кривых*. Она содер-

жит много важных разделов, которые мы не рассматривали (точки перегиба, двойственные кривые, эллиптические кривые и т. д.). Алгебраическим кривым посвящено много замечательных книг. Кроме уже упомянутых книг FULTON (1969), KIRWAN (1992) и WALKER (1950), следует рекомендовать книги CLEMENS (1980) и BRIESKORN, KNÖRRER (1986). Для читателей, знакомых с комплексным анализом и топологией, мы можем рекомендовать книгу GRIFFITHS (1989).

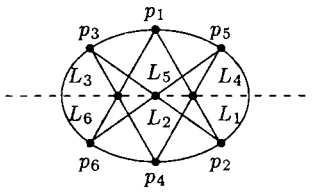
Упражнения к § 7

1. В этом упражнении мы будем изучать пересечение параболы $y = x^2$ и эллипса $x^2 + 4(y - \lambda)^2 = 1$ из примера 1.
   (a) Докажите, что пересечение этих кривых пусто над $\mathbb{R}$ при $\lambda < -1$. Нарисуйте взаимное расположение двух кривых при $\lambda < -1$ и при $\lambda = -1$.
   (b) Найдите наименьшее вещественное λ_0, такое, что соответствующее пересечение пусто над $\mathbb{R}$ при $\lambda > \lambda_0$. Нарисуйте взаимное расположение двух кривых при $\lambda > \lambda_0$ и при $\lambda = \lambda_0$.
   (c) Опишите возможные типы пересечений над $\mathbb{R}$ при $-1 < \lambda < \lambda_0$ и проиллюстрируйте их рисунками.
   (d) Для случаев (a), (b) и (c), используя интуитивное понимание кратности пересечения, объясните, на каких рисунках показано пересечение кратности > 1.
   (e) Не используя теорему Безу, объясните, почему над $\mathbb{C}$ число точек пересечения (с учетом кратностей) равно четырем (при вещественном λ). Указание: используйте формулы для x и y из примера 1.
2. В примере 2 мы изучали пересечение параболы $y = x^2$ с прямой L в аффинном пространстве. Пусть L не вертикальна.
   (a) Покажите, что над $\mathbb{R}$ число точек пересечения может быть равно 0, 1 и 2. Докажите, что пересечение состоит из одной точки, если L касательна к $y = x^2$ (в смысле § 4 гл. 3).
   (b) Докажите (не используя теорему Безу), что над $\mathbb{C}$ число точек пересечения (с учетом кратностей) равно двум.
3. В доказательстве предложения 4 было показано, что если $f = gh$, f однороден и $g = g_m + \ldots + g_0$ — представление полинома g в виде суммы однородных компонент, где $g_m \neq 0$, а степень компоненты g_i равна i, и если $h = h_n + \ldots + h_0$ — аналогичное представление для h, то $f = g_m h_n$. Завершите доказательство, показав, что $g = g_m$ и $h = h_n$. Указание: пусть m_0 — наименьший индекс, такой, что $g_{m_0} \neq 0$, и пусть n_0 аналогично определен для h. Рассмотрите произведение $g_{m_0} h_{n_0}$.
4. В этом упражнении мы наметим другое доказательство леммы 5. Пусть f и g такие же, как в условии леммы 5, а $R(x, y) = \operatorname{Res}(f, g, z)$. Достаточно доказать, что $R(tx, ty) = t^{mn} R(x, y)$.

   (a) Докажите, что $a_i(tx, ty) = t^i a_i(x, y)$, $b_i(tx, ty) = t^i b_i(x, y)$, затем покажите, что $R(tx, ty)$ — это определитель, элементы которого равны или 0, или $t^i a_i(x, y)$, или $t^i b_i(x, y)$.
   (b) В определителе из п. (a) умножьте второй столбец на t, третий — на t^2, ... , n-й — на t^{n-1}, $(n+2)$-й — на t, $(n+3)$-й — на t^2, ..., $(n+m)$-й — на t^{m-1}. Докажите, что $t^q R(tx, ty)$, где $q = n(n-1)/2 + m(m-1)/2$, равен определителю, у которого в каждой строке параметр t стоит в *одной и той же* степени.
   (c) Одинаковые степени параметра t из строк вынесем за знак определителя. Тогда $t^q R(tx, ty) = t^r R(x, y)$, где $r = (m+n)(m+n-1)/2$.
   (d) Используя п. (c), докажите, что $R(tx, ty) = t^{mn} R(x, y)$.
5. Завершите доказательство леммы 6, используя указания, данные в тексте. Указание: используйте предложение 7 и упр. 11 из § 2.
6. В этом упражнении мы рассмотрим доказательство теоремы 7.
   (a) Пусть $f \in \mathbb{C}[x_1, \ldots, x_n]$ — ненулевой полином. Докажите, что множества $\mathbf{V}(f)$ и $\mathbb{C}^n - \mathbf{V}(f)$ непусты. Указание: примените теорему о нулях и предложение 5 из § 1 гл. 1.
   (b) Используя п. (a), докажите, что существует $q \notin C \cup D \cup \bigcup_{i<j} L_{ij}$ (этот факт был сформулирован без доказательства).
   (c) Пусть $q \in \mathbb{P}^2(\mathbb{C})$; найдите матрицу $A \in \mathrm{GL}(3, \mathbb{C})$, такую, что $A(q) = (0, 0, 1)$. Указание: рассматривая q и $(0, 0, 1)$ как ненулевые векторы-столбцы в $\mathbb{C}^3$, найдите обратимую матрицу A, такую, что $A(q) = (0, 0, 1)$.
   (d) Докажите, что проективная прямая, соединяющая $(0, 0, 1)$ и (u, v, w), пересекает прямую $z = 0$ в точке $(u, v, 0)$. Указание: используйте уравнение (10) из § 6.
7. В примере 9 мы рассматривали кривые $C = \mathbf{V}(f)$ и $D = \mathbf{V}(g)$, где полиномы f и g определены в тексте параграфа.
   (a) Аккуратно проверьте, что только $p = (0, 0, 1), q = (1, 1, 1)$ и $r = (4/7, -8/7, 1)$ являются точками пересечения кривых C и D. Указание: если найден $\operatorname{Res}(f, g, z)$, остальное можно сделать вручную.
   (b) Докажите, что полиномы f и g редуцированы. Указание: используйте компьютер.
   (c) Докажите, что $(0, 1, 0) \notin C \cup D \cup L_{pq} \cup L_{pr} \cup L_{qr}$.
8. Для следующих пар кривых найдите точки их пересечения и кратности пересечения в этих точках.
   (a) $C = \mathbf{V}(yz - x^2), D = \mathbf{V}(x^2 + 4(y - z)^2 - 4z^2)$. Эта задача является проективной версией примера 1 при $\lambda = 1$. Указание: докажите, что замена координат $A(x, y, z) = (x, y + z, z)$ обладает требуемыми свойствами.
   (b) $C = \mathbf{V}(x^2y^3 - 2xy^2z^2 + yz^4 + z^5), D = \mathbf{V}(x^2y^2 - xz^3 - z^4)$. Указание: система имеет четыре решения, два вещественных и два ком-

плексных. Для нахождения комплексных решений используйте вычисление наибольшего общего делителя двух полиномов.

9. Докажите равенство (5). Указание: примените индукцию по m.
10. (Это упражнение требует знания анализа.) Открытое множество $U \subset \mathbb{C}^n$ называется *линейно связным*, если для любых двух точек $a, b \in U$ существует непрерывная функция $\gamma : [0,1] \to U$, такая, что $\gamma(0) = a$ и $\gamma(1) = b$.
    (a) Пусть функция $F : U \to \mathbb{Z}$ локально постоянна (т. е. ее значения в близких точках совпадают). Используйте теорему о промежуточном значении непрерывной функции и докажите, что F — постоянная функция, если U линейно связно. Указание: рассмотрим F как функцию $U \to \mathbb{R}$. Докажите, что F непрерывна. Затем обратите внимание, что функция $F \circ \gamma : [0,1] \to \mathbb{R}$ также непрерывна.
    (b) Пусть $f \in \mathbb{C}[x]$ — ненулевой полином. Докажите, что множество $\mathbb{C} - \mathbf{V}(f)$ линейно связно.
    (c) Пусть $f \in \mathbb{C}[x_1, \dots, x_n]$ — ненулевой полином. Докажите, что множество $\mathbb{C}^n - \mathbf{V}(f)$ линейно связно. Указание: пусть $a, b \in \mathbb{C}^n - \mathbf{V}(f)$. Рассмотрим комплексную прямую $\{ta + (1-t)b : t \in \mathbb{C}\}$. Объясните, почему $f(ta + (1-t)b)$ является ненулевым полиномом от t, и примените п. (b).
    (d) Приведите пример полинома $f \in \mathbb{R}[x, y]$, такого, что множество $\mathbb{R}^2 - \mathbf{V}(f)$ не является линейно связным. Найдите локально постоянную функцию $F : \mathbb{R}^2 - \mathbf{V}(f) \to \mathbb{Z}$, не являющуюся константой. Тот факт, что мы работаем над $\mathbb{C}$, имеет принципиальное значение.
11. Пусть C — неприводимая коника в $\mathbb{P}^2(\mathbb{C})$. Используя теорему Безу, объясните, почему прямая L пересекает C в двух точках. Что происходит, если C приводима? Что можно сказать о пересечении кривой C и прямой L, если C задана неприводимым полиномом степени n?
12. На рисунке в тексте параграфа шесть точек, образующие шестиугольник Паскаля, были расположены на конике в порядке обхода по часовой стрелке. Если мы изменим порядок точек, то по-прежнему можем образовать «шестиугольник», но при этом противоположные прямые могут пересекаться внутри коники. Например, это может выглядеть так:



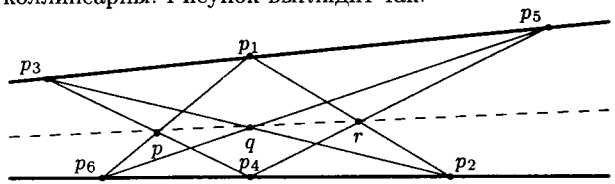
Объясните, почему теорема остается справедливой в этом случае.

13. Рассмотрим шестиугольник Паскаля, где коника является окружностью, а шесть точек — вершины правильного шестиугольника, вписанного в эту окружность. Где находятся точки пересечения противоположных прямых и на какой прямой они лежат?

14. Теорема Паппа (упр. 8 к § 4 гл. 6) утверждает, что если точки p_3, p_1, p_5 коллинеарны и точки p_6, p_4, p_2 коллинеарны, то точки

$$p = \overline{p_3p_4} \cap \overline{p_6p_1},$$
$$q = \overline{p_2p_3} \cap \overline{p_5p_6},$$
$$r = \overline{p_4p_5} \cap \overline{p_1p_2}$$

также коллинеарны. Рисунок выглядит так:



Объединение прямых $\overline{p_3p_1}$ и $\overline{p_6p_4}$ является приводимой коникой C'. Объясните, почему теорема Паппа может рассматриваться как «вырожденный» случай теоремы о шестиугольнике Паскаля. Указание: см. упр. 12. Обратите внимание, что в отличие от неприводимого случая, мы не можем выбрать любые 6 точек на C': мы не можем выбирать особую точку коники C' и каждая компонента коники C' должна содержать три точки.

15. Рассуждения, использованные при доказательстве теоремы 12, могут быть применены и в более общей ситуации. Пусть кривые C и D определены редуцированными уравнениями степени n, так что пересечение $C \cap D$ состоит ровно из n^2 точек. Предположим, что неприводимая кривая E, заданная редуцированным уравнением степени $m < n$, содержит mn из этих n^2 точек. Тогда, используя рассуждения из доказательства теоремы 12, докажите, что существует кривая F, заданная редуцированным уравнением степени $n - m$, которая содержит оставшиеся $n(n-m)$ точек из $C \cap D$.
16. Пусть C и D — кривые в $\mathbb{P}^2(\mathbb{C})$.
    (a) Докажите, что пересечение $C \cap D$ непусто.
    (b) Пусть C неособа в смысле п. (a) упр. 9 к § 6 (если $C = \mathbf{V}(f)$, то частные производные $\partial f/\partial x, \partial f/\partial y$ и $\partial f/\partial z$ не обращаются одновременно в нуль на $\mathbb{P}^2(\mathbb{C})$). Докажите, что C неприводима. Указание: если $C = C_1 \cup C_2$, то $F = f_1 f_2$; выясните, как ведут себя производные полинома f в точках из $C_1 \cap C_2$?
17. В этом упражнении мы рассмотрим неформальное доказательство теоремы Безу. Рассуждения будут нестрогими, но дают на интуитивном уровне объяснение, почему число точек пересечения равно mn.
    (a) Докажите, что в $\mathbb{P}^2(\mathbb{C})$ прямая L пересекает кривую C степени n в n точках (с учетом кратностей). Указание: выберите систему координат так, чтобы все точки пересечения лежали в аффинной

странства аф-
Многие из рас-
ют очевидным
е с интуитив-
ределение раз-
объясним, как
ние согласует-
соответствии
ект будет рас-

ла

ономиальных
ть многообра-
$I = \langle x^2y, x^3 \rangle \subset$
о уравнением
0. Имеем

(1)

H_x имеет раз-
ественно счи-
многообразие.

— плоскость,
я уравнением

$z = 0$. Обозначим через H_{xy} прямую, заданную уравнениями $x = y = 0$. Тогда

$$\begin{aligned}\mathbf{V}(I) &= \mathbf{V}(y^2z^3) \cap \mathbf{V}(x^5z^4) \cap \mathbf{V}(x^2yz^2)\\ &= (H_y \cup H_z) \cap (H_x \cup H_z) \cap (H_x \cup H_y \cup H_z)\\ &= H_z \cup H_{xy}\end{aligned}$$

(проведите вычисление самостоятельно). Таким образом, $\mathbf{V}(I)$ является объединением (x,y)-плоскости H_z и z-оси H_{xy}. Определим размерность объединения конечного числа векторных подпространств в k^n как максимум их размерностей. Тогда размерность многообразия $\mathbf{V}(I)$ равна 2.

Аналогичным образом может быть определена размерность многообразия произвольного мономиального идеала. Но сначала нам нужно описать, как выглядит такое многообразие. Для этого введем понятие *координатного подпространства*. Координатным подпространством в k^n называется векторное подпространство, заданное несколькими уравнениями вида $x_i = 0$, где $x_1, \ldots, x_n$ — координаты в k^n.

Предложение 1. *Многообразие мономиального идеала $I \subset k[x_1, \ldots, x_n]$ представляет собой конечное объединение координатных подпространств в k^n.*

Доказательство. Пусть $x_{i_1}^{\alpha_1} \ldots x_{i_r}^{\alpha_r}$ — моном в $k[x_1, \ldots, x_n]$, где $\alpha_j \geq 1$ при $1 \leq j \leq r$. Тогда

$$\mathbf{V}(x_{i_1}^{\alpha_1} \ldots x_{i_r}^{\alpha_r}) = H_{x_{i_1}} \cup \ldots \cup H_{x_{i_r}},$$

где $H_{x_l} = \mathbf{V}(x_l)$. Таким образом, многообразие, определенное мономом, является объединением координатных гиперплоскостей. Всего имеется n таких гиперплоскостей.

Так как мономиальный идеал порожден конечным набором мономов, то соответствующее многообразие является конечным пересечением конечных объединений координатных гиперплоскостей. В силу дистрибутивности пересечения относительно объединения его можно переписать в виде конечного объединения пересечений координатных гиперплоскостей (см. (1) в качестве примера). Но пересечение конечного числа координатных гиперплоскостей является координатным подпространством. □

В представлении многообразия мономиального идеала I в виде конечного объединения координатных подпространств мы исключим те подпространства, которые содержатся в других подпространствах этого объединения. Тогда

$$\mathbf{V}(I) = V_1 \cup \ldots \cup V_p,$$

где V_i не содержится в V_j при $i \neq j$. Такое разложение $\mathbf{V}(I)$ единственно (это будет доказано в упр. 8).

Дадим следующее важное определение.

Определение 2. Пусть многообразие V является объединением конечного числа линейных подпространств пространства k^n. Тогда его *размерностью*, обозначаемой $\dim V$, называется максимум размерностей этих подпространств[1)].

Таким образом, размерность объединения двух плоскостей и прямой равна 2, а размерность объединения трех прямых равна 1. Для того чтобы найти размерность многообразия мономиального идеала I, нужно просто найти максимум размерностей координатных подпространств, содержащихся в $\mathbf{V}(I)$.

Хотя это и просто сделать в каждом конкретном случае, имеет смысл упорядочить процесс вычисления. Пусть $I = \langle m_1, \ldots, m_t \rangle$ — собственный идеал, порожденный мономами m_j. При вычислении размерности $\dim \mathbf{V}(I)$ нам нужно найти компоненту многообразия

$$\mathbf{V}(I) = \bigcap_{j=1}^{t} \mathbf{V}(m_j)$$

наибольшей размерности. Если мы сможем найти набор переменных $x_{i_1}, \ldots, x_{i_r}$, таких, что каждая из них содержится по крайней мере в одном мономе, то координатное подпространство, заданное уравнениями $x_{i_1} = \ldots = x_{i_r} = 0$, содержится в $\mathbf{V}(I)$. Это означает, что нам нужно искать переменные, которые содержатся в как можно большем числе m_j. Точнее, пусть

$$M_j = \{l \in \{1, \ldots, n\} : x_l \text{ делит моном } m_j\}$$

— множество переменных, содержащихся в m_j. (Обратите внимание, что M_j непусто, так как I — собственный идеал.) Рассмотрим множество

$$\mathcal{M} = \{J \subset \{1, \ldots, n\} : J \cap M_j \neq \varnothing \text{ для всех } 1 \leq j \leq t\},$$

элементами которого являются подмножества из $\{1, \ldots, n\}$, имеющие непустые пересечения с *каждым* M_j. (Обратите внимание, что $\mathcal{M}$ непусто, так как $\{1, \ldots, n\} \in \mathcal{M}$.) Обозначим через $|J|$ число элементов конечного множества J. Тогда справедливо следующее утверждение.

Предложение 3. *В наших обозначениях*

$$\dim \mathbf{V}(I) = n - \min(|J| : J \in \mathcal{M}).$$

[1)] Размерность линейного подпространства понимается в смысле определения, даваемого в линейной алгебре.— *Прим. ред.*

Доказательство. Пусть $J = \{i_1, \ldots, i_r\}$ — такой элемент из $\mathcal{M}$, что $|J| = r$ минимально. Так как каждый моном m_j содержит некоторую степень какой-то переменной x_{i_l}, $1 \le l \le r$, то координатное подпространство $W = \mathbf{V}(x_{i_1}, \ldots, x_{i_r})$ содержится в $\mathbf{V}(I)$. Размерность подпространства W равна $n - r = n - |J|$; следовательно, по определению 2 размерность многообразия $\mathbf{V}(I)$ не меньше, чем $n - |J|$.

Если размерность многообразия $\mathbf{V}(I)$ превышает $n-r$, то существует координатное подпространство $W' = \mathbf{V}(x_{l_1}, \ldots, x_{l_s}) \subset \mathbf{V}(I)$, где $s < r$. Каждый моном m_j обращается в нуль на W', в частности, он обращается в нуль в точке, координаты $x_{l_1}, \ldots, x_{l_s}$ которой равны нулю, а остальные координаты отличны от нуля. Следовательно, хотя бы одна переменная x_{k_i} делит m_j. Отсюда $J' = \{l_1, \ldots, l_s\} \in \mathcal{M}$. Но так как $|J'| = s < r$, это противоречит минимальности r. Значит, размерность многообразия $\mathbf{V}(I)$ равна $n-r$.

Вернемся к рассмотрению второго примера. Обозначим переменные x, y, z через x_1, x_2, x_3. Тогда

$$I = \langle x_2^2 x_3^3, x_1^5 x_3^4, x_1^2 x_2 x_3^2 \rangle = \langle m_1, m_2, m_3 \rangle,$$

где

$$m_1 = x_2^2 x_3^3, \quad m_2 = x_1^5 x_3^4, \quad m_3 = x_1^2 x_2 x_3^2.$$

В наших обозначениях

$$M_1 = \{2,3\}, \quad M_2 = \{1,3\}, \quad M_3 = \{1,2,3\};$$

поэтому

$$\mathcal{M} = \{\{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{3\}\}.$$

Тогда $\min(|J| : J \in \mathcal{M}) = 1$, а следовательно,

$$\dim \mathbf{V}(I) = 3 - \min(|J| : J \in \mathcal{M}) = 3 - 1 = 2.$$

Обобщая этот пример, можно сказать, что если некоторая переменная x_i, например, входит в каждый моном из некоторого множества образующих собственного мономиального идеала I, то $\dim \mathbf{V}(I) = n - 1$, так как $J = \{i\} \in \mathcal{M}$. Обратное утверждение рассмотрено в упр. 4.

Интересно сравнить мономиальный идеал I с его радикалом $\sqrt{I}$. В упражнениях будет доказано, что если идеал I мономиален, то радикал $\sqrt{I}$ также мономиален. Мы знаем из гл. 4, что $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$ для любого идеала I. Поэтому $\mathbf{V}(I)$ и $\mathbf{V}(\sqrt{I})$ имеют одинаковую размерность. В упр. 10 будет показано, что это утверждение согласуется с формулой, приведенной в предложении 3.

Упражнения к § 1

1. Для каждого из следующих мономиальных идеалов I найдите представление многообразия $\mathbf{V}(I)$ в виде объединения координатных подпространств:
   (a) $I = \langle x^5, x^4yz, x^3z \rangle \subset k[x,y,z]$;
   (b) $I = \langle wx^2y, xyz^3, wz^5 \rangle \subset k[w,x,y,z]$;
   (c) $I = \langle x_1x_2, x_3 \ldots x_n \rangle \subset k[x_1, \ldots, x_n]$.
2. Найдите $\dim \mathbf{V}(I)$ для следующих мономиальных идеалов:
   (a) $I = \langle xy, yz, xz \rangle \subset k[x,y,z]$;
   (b) $I = \langle wx^2z, w^3y, wxyz, x^5z^6 \rangle \subset k[w,x,y,z]$;
   (c) $I = \langle u^2vwyz, wx^3y^3, uxy^7z, y^3z, uwx^3y^3z^2 \rangle \subset k[u,v,w,x,y,z]$.
3. Докажите, что множество $W \subset k^n$ является координатным подпространством в том и только том случае, когда W является линейной оболочкой некоторого подмножества базисных векторов $\{e_i : 1 \le i \le n\}$, где e_i — вектор, у которого на i-м месте стоит 1, а на остальных нули.
4. Предположим, что $I \subset k[x_1, \ldots, x_n]$ является мономиальным идеалом и $\dim \mathbf{V}(I) = n - 1$.
   (a) Докажите, что мономы из любого множества образующих идеала I имеют непостоянный общий делитель.
   (b) Пусть $\mathbf{V}(I) = V_1 \cup \ldots \cup V_p$, где V_i являются координатными подпространствами и V_i не содержится в V_j при $i \ne j$. Предположим далее, что в точности одно из пространств V_i имеет размерность $n-1$. Чему может равняться максимальное значение p? Приведите пример, когда это максимальное значение достигается.
5. Пусть I — мономиальный идеал в кольце $k[x_1, \ldots, x_n]$, такой, что $\dim \mathbf{V}(I) = 0$.
   (a) Что собой представляет многообразие $\mathbf{V}(I)$ в этом случае?
   (b) Докажите, что $\dim \mathbf{V}(I) = 0$ в том и только том случае, когда для каждого $1 \le i \le n$ имеет место включение $x_i^{l_i} \in I$ для некоторого $l_i \ge 1$. Указание: в каком случае в рамках предложения 3 множество $\mathcal{M}$ имеет единственный элемент $\{1, \ldots, n\}$?
6. Пусть $\langle m_1, \ldots, m_r \rangle \subset k[x_1, \ldots, x_n]$ — мономиальный идеал, порожденный r мономами, $r \le n$. Докажите, что $\dim \mathbf{V}(I) \ge n - r$.
7. Докажите, что координатное подпространство является неприводимым многообразием, если поле k бесконечно.
8. В этом упражнении мы найдем связь между разложением многообразия мономиального идеала I в объединение координатных подпространств и разложением многообразия $\mathbf{V}(I)$ в объединение неприводимых компонент. Поле k предполагается бесконечным.
   (a) Пусть $\mathbf{V}(I) = V_1 \cup \ldots \cup V_p$, где V_i — координатные подпространства, такие, что V_i не содержится в V_j при $i \ne j$. Докажите, что это объединение является также минимальным разложением многообразия $\mathbf{V}(I)$ в объединение неприводимых компонент (см. теорему 4 из § 6 гл. 4).

(b) Докажите единственность такого разложения с точностью до порядка слагаемых V_i.

9. Пусть $I = \langle m_1, \ldots, m_s \rangle \subset k[x_1, \ldots, x_n]$ — мономиальный идеал. Для каждого $j, 1 \le j \le s$, определим множество (как в тексте настоящего параграфа) $M_j = \{l : x_l \text{ делит } m_j\}$, и рассмотрим мономы

$$m_j' = \prod_{l \in M_j} x_l.$$

Таким образом, m_j' содержит те же переменные, что и m_j, но в первой степени.

(a) Докажите, что $m_j' \in \sqrt{I}$ для всех j, $1 \le j \le 3$.

(b) Докажите, что $\sqrt{I} = \langle m_1', \ldots, m_s' \rangle$. Указание: используйте леммы 2 и 3 из § 4 гл. 2.

10. Пусть I — мономиальный идеал. Используя упр. 9, докажите, что равенство $\dim \mathbf{V}(I) = \dim \mathbf{V}(\sqrt{I})$ следует из формулы для размерности, данной в предложении 3.

§ 2. Дополнение мономиального идеала

Одна из замечательных идей Гильберта, высказанная в его знаменитой статье Über die Theorie der algebraischen Formen (см. HILBERT (1890)), состоит в том, что размерность многообразия, определенного полиномиальным идеалом, может быть охарактеризована ростом числа мономов, не принадлежащих идеалу, при возрастании полной степени. Мы уже несколько раз касались этого явления в гл. 5 (особенно в упр. 12 к § 3).

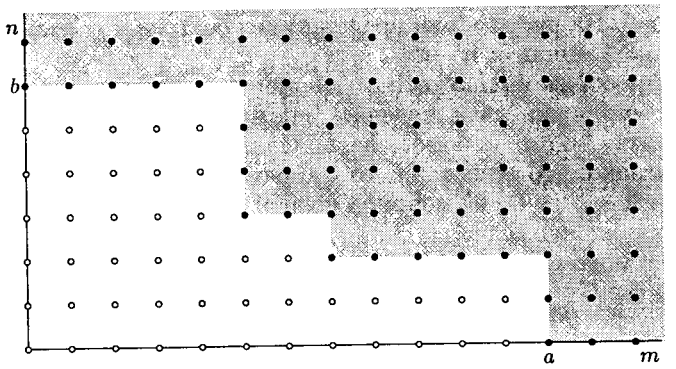
В этом параграфе мы подробно рассмотрим множество мономов, не содержащихся в мономиальном идеале $I \subset k[x_1, \ldots, x_n]$. Так как это множество может быть бесконечным, то наша цель — найти формулу для числа мономов $x^\alpha \notin I$, если значение $|\alpha|$ ограничено сверху некоторым заданным числом. Результаты этого параграфа играют решающую роль при определении размерности произвольного многообразия в § 3.

Пример 1. Рассмотрим собственный мономиальный идеал $I \subset k[x, y]$. Так как I является собственным (т. е. $I \neq k[x, y]$), то $\mathbf{V}(I)$ — это или

(a) начало координат $\{(0, 0)\}$, или
(b) ось x, или
(c) ось y, или
(d) объединение оси x и оси y.

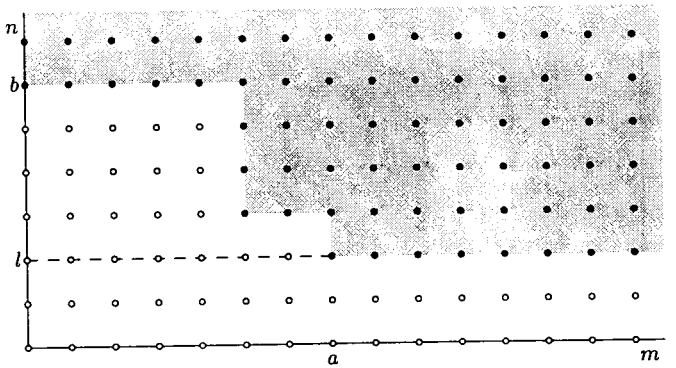
В случае (a) мы имеем $x^a \in I, y^b \in I$ для некоторых целых $a, b > 0$ (см. упр. 5 к § 1). В этом случае число мономов, не принадлежащих

I, конечно и равно $C_0 \le a \cdot b$. Пусть a, b — наименьшие положительные числа, удовлетворяющие условию $x^a, y^b \in I$. Тогда мы получим следующий рисунок, на котором показаны показатели степеней для мономов, принадлежащих I (черные кружки), и мономов, не принадлежащих I (белые кружки):



$(m, n) \leftrightarrow x^m y^n$

В случае (b) многообразия $\mathbf{V}(I)$ совпадает с осью x, и никакая степень x^k не принадлежит I. С другой стороны, так как ось y не принадлежит $\mathbf{V}(I)$, то существует $b > 0$, такое, что $y^b \in I$. Пусть b — наименьшее такое число. Здесь получается такая картина:



$(m, n) \leftrightarrow x^m y^n$

Обозначим через l максимальный показатель степени переменной y, такой, что *все* мономы из I делятся на y^l. Тогда $l \le b$, но также $l > 0$, так как никакая положительная степень переменной x не принадлежит I. Таким образом, мономы, принадлежащие дополнению

идеала I, — это мономы

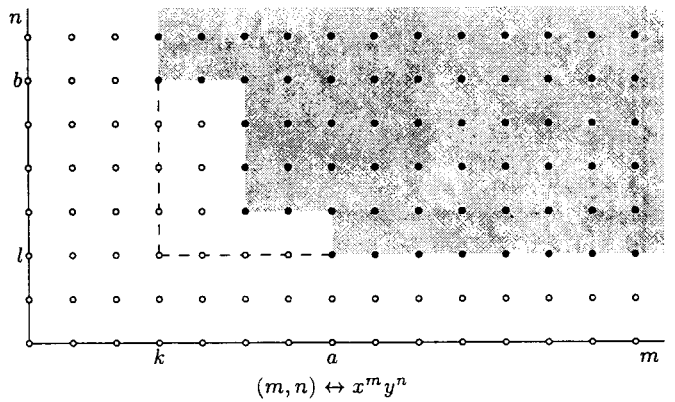
$$\{x^i y^j : i \in \mathbb{Z}_{\geq 0},\ 0 \leq j \leq l-1\},$$

показатели которых лежат на l экземплярах горизонтальной оси в $\mathbb{Z}^2_{\geq 0}$, и еще конечное число других мономов. Эти дополнительные мономы t обладают следующими свойствами: $x^r t \in I$ для некоторого $r > 0$. На рисунке они представлены белыми кружками выше пунктирной линии и на ней.

Таким образом, множество мономов в дополнении к I состоит из l «прямых» плюс конечное множество. Это позволяет нам «сосчитать» число мономов, не принадлежащих I. В упр. 1 будет доказано, что если $s > l$, то l «прямых» содержат в точности $ls - (1 + 2 + \ldots + l - 1)$ мономов полной степени $\leq s$. В частности, если s достаточно велико ($s > a+b$, где a указано на рисунке), то количество мономов полной степени $\leq s$, не принадлежащих I, равно $ls + C_0$, где C_0 — некоторая константа, зависящая только от I.

В случае (c) ситуация аналогична ситуации в случае (b), но «прямые» мономов параллельны вертикальной оси в плоскости $\mathbb{Z}^2_{\geq 0}$ показателей степеней. В частности, мы получаем аналогичную формулу для числа мономов полной степени $\leq s$, не принадлежащих I, для достаточно больших s.

В случае (d) пусть k — максимальный показатель степени, такой, что любой моном из I делится на x^k. Аналогично определяется показатель степени l для переменной y. Отметим, что $k > 0$ и $l > 0$, так как xy делит все мономы из I. Получаем следующий рисунок:



$(m, n) \leftrightarrow x^m y^n$

Мономы в дополнении к I образуют k «прямых»

$$\{x^i y^j : 0 \leq i \leq k-1,\ j \in \mathbb{Z}_{\geq 0}\},$$

параллельных вертикальной оси, l «прямых»

$$\{x^i y^j : i \in \mathbb{Z}_{\geq 0},\ 1 \leq j \leq l-1\},$$

параллельных горизонтальной оси, плюс конечное число мономов, обозначенных белыми кружками внутри и на границе области, ограниченной пунктирными прямыми.

Таким образом, мономы, не принадлежащие I, образуют $l + k$ «прямых» плюс конечное множество мономов. Если s достаточно велико ($s > a + b$, где a и b указаны на рисунке), то количество мономов полной степени $\leq s$, не принадлежащих I, равно $(l+k)s + C_0$, где C_0 — константа, зависящая только от I (см. упр. 1).

Описание структуры множества мономов, не принадлежащих I, полученное в примере 1 (а именно, тот факт, что множество мономов в дополнении к мономиальному идеалу $I \subset k[x, y]$ состоит из конечного числа бесконечных множеств, параллельных координатным подпространствам в $\mathbb{Z}^2_{\geq 0}$, плюс конечное множество), обобщается на случай произвольного мономиального идеала. В § 3 именно оно и будет основным ключевым моментом при определении и вычислении размерности произвольного многообразия.

Прежде чем рассматривать общую задачу, мы введем несколько новых обозначений. Для произвольного мономиального идеала I обозначим через

$$C(I) = \{\alpha \in \mathbb{Z}^n_{\geq 0} : x^\alpha \notin I\}$$

множество показателей степеней мономов, *не* принадлежащих I. Это множество и будет основным объектом изучения. Также положим

$$\begin{aligned} e_1 &= (1, 0, 0, \ldots, 0), \\ e_2 &= (0, 1, 0, \ldots, 0), \\ &\vdots \\ e_n &= (0, 0, \ldots, 0, 1). \end{aligned}$$

Координатным подпространством в $\mathbb{Z}^n_{\geq 0}$, определенным векторами $e_{i_1}, \ldots, e_{i_r}, i_1 < \ldots < i_r$, мы назовем множество

$$[e_{i_1}, \ldots, e_{i_r}] = \{a_1 e_{i_1} + \ldots + a_r e_{i_r} : a_j \in \mathbb{Z}_{\geq 0} \text{ для всех } 1 \leq j \leq r\}.$$

Мы будем называть $[e_{i_1}, \ldots, e_{i_r}]$ r-мерным координатным подпространством. Наконец, подмножество в $\mathbb{Z}^n_{\geq 0}$ называется *сдвигом* координатного подпространства $[e_{i_1}, \ldots, e_{i_r}]$, если оно имеет вид

$$\alpha + [e_{i_1}, \ldots, e_{i_r}] = \{\alpha + \beta : \beta \in [e_{i_1}, \ldots, e_{i_r}]\},$$

где $\alpha = \sum_{i \notin \{i_1, \ldots, i_r\}} a_i e_i$, $a_i \geq 0$. Это условие на α означает, что мы производим сдвиг на вектор, перпендикулярный $[e_{i_1}, \ldots, e_{i_r}]$. Так,

например, множество $\{(1,l) : l \in \mathbb{Z}_{\geq 0}\} = e_1 + [e_2]$ является сдвигом координатного подпространства $[e_2] \subset \mathbb{Z}^2_{\geq 0}$.

Теперь мы можем суммировать результаты, полученные при рассмотрении примера 1.

(a) Если $\mathbf{V}(I)$ состоит из одной точки — начала координат, то множество $C(I)$ конечно.
(b) Если $\mathbf{V}(I)$ является осью x, то $C(I)$ состоит из конечного числа сдвигов координатного подпространства $[e_1]$ и еще, может быть, конечного числа точек.
(c) Если $\mathbf{V}(I)$ является осью y, то $C(I)$ состоит из конечного числа сдвигов координатного подпространства $[e_2]$ и еще, может быть, конечного числа точек.
(d) Если $\mathbf{V}(I)$ является объединением оси x и оси y, то $C(I)$ состоит из конечного числа сдвигов координатного подпространства $[e_1]$, конечного числа сдвигов координатного подпространства $[e_2]$ и еще, может быть, конечного числа точек.

В упражнениях аналогичный анализ будет проведен для случая мономиальных идеалов в полиномиальном кольце от трех переменных.

Вернемся к общему случаю. Отметим сначала, что имеется прямое соответствие между координатными подпространствами, принадлежащими $\mathbf{V}(I)$, и координатными подпространствами в $\mathbb{Z}^n_{\geq 0}$, принадлежащими $C(I)$.

Предложение 2. *Рассмотрим собственный мономиальный идеал $I \subset k[x_1, \ldots, x_n]$.*

(i) *Координатное подпространство $\mathbf{V}(x_i : i \notin \{i_1, \ldots, i_r\})$ содержится в $\mathbf{V}(I)$ в том и только том случае, когда $[e_{i_1}, \ldots, e_{i_r}] \subset C(I)$.*
(ii) *Размерность многообразия $\mathbf{V}(I)$ равна размерности наибольшего координатного подпространства, содержащегося в $C(I)$.*

Доказательство. (i) $\Rightarrow$. Отметим сначала, что $W = \mathbf{V}(x_i : i \notin \{i_1, \ldots, i_r\})$ содержит точку p, i_j-я координата которой равна 1 при $1 \leq j \leq r$, а остальные координаты равны 0. Для любого $\alpha \in [e_{i_1}, \ldots, e_{i_r}]$ моном x^α имеет вид $x^\alpha = x_{i_1}^{\alpha_1} \ldots x_{i_r}^{\alpha_r}$. Тогда $x^\alpha = 1$ в точке p. Поэтому $x^\alpha \notin I$, так как $p \in W \subset \mathbf{V}(I)$ по условию. Следовательно, $\alpha \in C(I)$.

$\Leftarrow$. Пусть $[e_{i_1}, \ldots, e_{i_r}] \subset C(I)$. Так как I — собственный идеал, то каждый моном из I содержит хотя бы одну переменную, отличную от $x_{i_1}, \ldots, x_{i_r}$. Это означает, что каждый моном из I обращается в нуль в любой точке $(a_1, \ldots, a_n) \in k^n$, где $a_i = 0$ при $i \notin \{i_1, \ldots, i_r\}$.

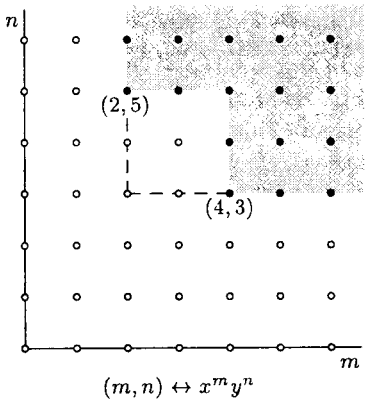
Поэтому каждый моном из I обращается в нуль на координатном подпространстве $\mathbf{V}(x_i : i \notin \{i_1, \ldots, i_r\})$. Следовательно, это подпространство содержится в $\mathbf{V}(I)$.

(ii) Координатное подпространство $\mathbf{V}(x_i : i \notin \{i_1, \ldots, i_r\})$ имеет размерность r. Из (i) следует, что размерности координатных подпространств пространства k^n, содержащихся в $\mathbf{V}(I)$, и координатных подпространств пространства $\mathbb{Z}^n_{\geq 0}$, содержащихся в $C(I)$, образуют одинаковые числовые множества. По определению 2 из § 1 $\dim \mathbf{V}(I)$ — это максимум размерностей координатных подпространств пространства k^n, содержащихся в $\mathbf{V}(I)$, откуда и следует утверждение (ii).

Теперь мы можем описать дополнение мономиального идеала.

Теорема 3. *Пусть $I \subset k[x_1, \ldots, x_n]$ — собственный мономиальный идеал. Тогда множество $C(I)$ является конечным объединением сдвигов (не обязательно непересекающихся) координатных подпространств пространства $\mathbb{Z}^n_{\geq 0}$.*

Прежде чем доказывать эту теорему, рассмотрим, например, идеал $I = \langle x^4y^3, x^2y^5 \rangle$.



$(m,n) \leftrightarrow x^m y^n$

Легко видеть, что $C(I)$ может быть представлено в виде

$$C(I) = [e_1] \cup (e_2 + [e_1]) \cup (2e_2 + [e_1]) \cup [e_2] \cup (e_1 + [e_2]) \cup \{(3,4)\} \cup \{(3,3)\} \cup \{(2,4)\} \cup \{(2,3)\}.$$

Последние четыре множества в этом объединении мы можем рассматривать как сдвиги 0-мерного координатного подпространства — начала координат в $\mathbb{Z}^n_{\geq 0}$.

Доказательство теоремы 3. Если $I = \{0\}$, то теорема, очевидно, верна. Поэтому мы будем рассматривать случай, когда идеал I ненулевой. Доказательство использует индукцию по числу переменных n. Если $n = 1$, то $I = \langle x^l \rangle$ для некоторого $l > 0$. Тогда $C(I) = \{0, 1, \ldots, l-1\} \subset \mathbb{Z}_{\geq 0}$. Таким образом, дополнение состоит из l точек, которые являются сдвигами начала координат.

Пусть утверждение теоремы справедливо для $n-1$ переменных. Рассмотрим мономиальный идеал $I \subset k[x_1, \ldots, x_n]$. Для каждого $j \geq 0$ обозначим через I_j идеал в $k[x_1, \ldots, x_{n-1}]$, порожденный такими мономами t, что $t \cdot x_n^j \in I$. Тогда $C(I_j)$ состоит из таких векторов $\alpha \in \mathbb{Z}_{\geq 0}^{n-1}$, что $x^\alpha x_n^j \notin I$. Геометрически это означает, что $C(I_j) \subset \mathbb{Z}_{\geq 0}^{n-1}$ является пересечением множества $C(I)$ и гиперплоскости $(0, \ldots, 0, j) + [e_1, \ldots, e_{n-1}]$ из $\mathbb{Z}_{\geq 0}^n$.

Так как I — идеал, то $I_j \subset I_{j'}$ при $j < j'$. По условию обрыва возрастающих цепей существует целое j_0, такое, что $I_j = I_{j_0}$ при $j \geq j_0$. Для любого целого j обозначим через $C(I_j) \times \{j\}$ множество $\{(\alpha, j) \in \mathbb{Z}_{\geq 0}^n : \alpha \in C(I_j) \subset \mathbb{Z}_{\geq 0}^{n-1}\}$. Мы утверждаем, что

$$C(I) = (C(I_{j_0}) \times \mathbb{Z}_{\geq 0}) \cup \bigcup_{j=1}^{j_0-1} (C(I_j) \times \{j\}). \qquad (1)$$

Отметим сначала, что $C(I_j) \times \{j\} \subset C(I)$ по определению $C(I_j)$. Докажем, что $C(I_{j_0}) \times \mathbb{Z}_{\geq 0} \subset C(I)$. В самом деле, $I_j = I_{j_0}$ при $j \geq j_0$, а значит, $C(I_{j_0}) \times \{j\} \subset C(I)$ при $j \geq j_0$. Если $j < j_0$, то $x^\alpha x_n^j \notin I$, когда $x^\alpha x_n^{j_0} \notin I$ (потому что I — идеал). Поэтому $C(I_{j_0}) \times \{j\} \subset C(I)$ при $j < j_0$. Таким образом, $C(I)$ содержит правую часть равенства (1).

Докажем противоположное включение. Пусть $\alpha = (\alpha_1, \ldots, \alpha_n) \in C(I)$. Тогда $\alpha \in C(I_{\alpha_n}) \times \{\alpha_n\}$. Если $\alpha_n < j_0$, то очевидно, что α принадлежит правой части формулы (1). Если же $\alpha_n \geq j_0$, то равенство $I_{\alpha_n} = I_{j_0}$ показывает, что $\alpha \in C(I_{j_0}) \times \mathbb{Z}_{\geq 0}$ и наше утверждение доказано.

По предположению индукции каждое множество $C(I_0), \ldots, C(I_{j_0})$ является конечным объединением сдвигов координатных подпространств пространства $\mathbb{Z}_{\geq 0}^{n-1}$. Подставляя эти конечные объединения в правую часть равенства (1), мы видим, что $C(I)$ является конечным объединением сдвигов координатных подпространств пространства $\mathbb{Z}_{\geq 0}^n$. □

Наша следующая цель — найти число мономов полной степени $\leq s$ в дополнении мономиального идеала $I \subset k[x_1, \ldots, x_n]$. Нам понадобится следующее важное утверждение.

Лемма 4. *Число мономов полной степени $\leq s$ в $k[x_1, \ldots, x_m]$ равно биномиальному коэффициенту $\binom{m+s}{s}$.*

Доказательство. См. упр. 11 к § 3 гл. 5. □

Далее число $|\alpha| = \alpha_1 + \ldots + \alpha_n$ мы будем называть *полной степенью* элемента $\alpha \in \mathbb{Z}_{\geq 0}^n$. Она равна полной степени монома x^α. В этих терминах лемма 4 означает, что число точек полной степени $\leq s$ в m-мерном координатном подпространстве пространства $\mathbb{Z}_{\geq 0}^n$ равно $\binom{m+s}{s}$ (см. упр. 5). Обратите внимание, что если m фиксировано, то выражение

$$\binom{m+s}{s} = \binom{m+s}{m} = \frac{1}{m!}(s+m)(s+m-1)\ldots(s+1)$$

является полиномом степени m от s, причем его старший коэффициент равен $1/m!$.

Что можно сказать о количестве мономов полной степени $\leq s$ в *сдвиге* m-мерного координатного подпространства в $\mathbb{Z}_{\geq 0}^n$? Рассмотрим, например, сдвиг $a_{m+1}e_{m+1} + \ldots + a_n e_n + [e_1, \ldots, e_m]$ координатного подпространства $[e_1, \ldots, e_m]$. Так как $a_{m+1}, \ldots, a_n$ фиксированы, то число точек полной степени $\leq s$ в сдвинутом подпространстве равно равно числу точек в $[e_1, \ldots, e_m]$ полной степени $\leq s - (a_{m+1} + \ldots + a_n)$ (при условии, конечно, что $s > a_{m+1} + \ldots + a_n$). Более общим образом, справедливо следующее утверждение.

Лемма 5. *Рассмотрим сдвиг $\alpha + [e_{i_1}, \ldots, e_{i_m}]$ координатного подпространства $[e_{i_1}, \ldots, e_{i_m}] \subset \mathbb{Z}_{\geq 0}^n$, где $\alpha = \sum_{i \notin \{i_1, \ldots, i_m\}} a_i e_i$.*

(i) *Число точек полной степени $\leq s$ в $\alpha + [e_{i_1}, \ldots, e_{i_m}]$ равно*

$$\binom{m+s-|\alpha|}{s-|\alpha|}$$

при условии, что $s > |\alpha|$.

(ii) *При $s > |\alpha|$ это число точек выражается полиномиальной функцией от s степени m со старшим коэффициентом $1/m!$.*

Доказательство. (i) Если $s > |\alpha|$, то каждая точка $\beta \in \alpha + [e_{i_1}, \ldots, e_{i_m}]$ полной степени $\leq s$ имеет вид $\beta = \alpha + \gamma$, где $\gamma \in [e_{i_1}, \ldots, e_{i_m}]$ и $|\gamma| \leq s - |\alpha|$. Теперь формула из п. (i) следует из леммы 4.

(ii) См. упр. 6.

Теперь мы готовы доказать существование связи между размерностью разнообразия $\mathbf{V}(I)$ для мономиального идеала I и степенью

полиномиальной функции, представляющей число точек степени $\leq s$ в $C(I)$.

Теорема 6. *Пусть $I \subset k[x_1, \ldots, x_n]$ — мономиальный идеал и $\dim \mathbf{V}(I) = d$. Тогда для достаточного большого s количество мономов полной степени $\leq s$, не принадлежащих I, выражается полиномиальной функцией от s степени d, причем коэффициент при s^d в этом полиноме положителен.*

Доказательство. Нам нужно найти число точек в $C(I)$ полной степени $\leq s$. По теореме 3

$$C(I) = T_1 \cup T_2 \cup \ldots \cup T_t,$$

где каждое T_i является сдвигом координатного подпространства из $\mathbb{Z}^n_{\geq 0}$. Мы можем считать, что $T_i \neq T_j$ при $i \neq j$.

Размерность сдвига T_i равна размерности соответствующего координатного подпространства. По условию размерность многообразия $\mathbf{V}(I)$ равна d; следовательно, по предложению 2 размерность каждого T_i не превосходит d и хотя бы одно T_i имеет размерность, равную d.

Мы лишь наметим дальнейшие шаги доказательства, оставляя детали читателю (в упражнениях). При подсчете точек степени $\leq s$ в $C(I)$ надо быть аккуратным, так как хотя $C(I)$ и является объединением сдвигов координатных подпространств, но эти сдвиги могут пересекаться (см., например, п. (d) примера 1). Мы будем использовать верхний индекс s для указания того, что рассматриваемое подмножество состоит из элементов степени $\leq s$. Имеем

$$C(I)^s = T_1^s \cup T_2^s \cup \ldots \cup T_t^s.$$

Число элементов множества $C(I)^s$ будет обозначаться через $|C(I)^s|$.

В упр. 7 будет рассмотрен метод (который называется методом включения-исключения), позволяющий найти число элементов в конечном объединении конечных множеств. Если множества имеют общие элементы, то мы не можем просто сложить мощности множеств, потому что тогда некоторые элементы будут подсчитаны несколько раз. Метод включения-исключения вводит «корректирующие слагаемые», которые позволяют учесть эти «кратные» элементы множеств. Эти корректирующие слагаемые суть числа элементов в двойных пересечениях, в тройных пересечениях и т. д.

Применение метода включения-исключения к $C(I)^s$ дает

$$|C(I)^s| = \sum_i |T_i^s| - \sum_{i<j} |T_i^s \cap T_j^s| + \sum_{i<j<k} |T_i^s \cap T_j^s \cap T_k^s| - \ldots. \quad (2)$$

Мы знаем, что при достаточно большом s число элементов в T_i^s выражается полиномиальной функцией степени $m_i = \dim(T_i) \leq d$ от s и коэффициент при s^{m_i} равен $1/m_i!$. Из этого следует, что $|C(I)^s|$ при достаточно большом s является полиномиальной функцией от s степени не больше d.

Первая сумма в (2) является полиномиальной функцией по s степени d при достаточно больших s, потому что хотя бы одно T_i имеет размерность d, а старшие коэффициенты соответствующих полиномов положительны и, значит, не сокращаются. Если мы докажем, что оставшиеся суммы в (2) выражаются полиномами степени меньшей d, то теорема будет доказана.

В упр. 8 будет доказано, что пересечение двух различных сдвигов координатных подпространств пространства $\mathbb{Z}^n_{\geq 0}$ размерностей m и r или пусто, или является сдвигом координатного подпространства размерности $<\max(m, r)$. Рассмотрим ненулевой член $|T_i \cap T_j|$ во второй сумме в (2). Так как $T_i \neq T_j$, то из упр. 8 вытекает, что $T = T_i \cap T_j$ является сдвигом координатного подпространства размерности $< d$. Поэтому в силу леммы 5 число точек в $T^s = T_i^s \cap T_j^s$ является полиномиальной функцией от s степени $< d$ (если s достаточно велико). Суммируя по всем $i < j$, получаем, что вторая сумма в (2) является полиномиальной функцией от s степени $< d$ для достаточно большого s. Остальные суммы в (2) рассматриваются аналогично. Таким образом, $|C(I)^s|$ является полиномиальной функцией от s (если s достаточно велико) степени d с положительным старшим коэффициентом. □

Рассмотрим еще раз идеал $I = \langle x^4y^3, x^2y^5 \rangle$. Мы уже видели, что $C(I) = C_0 \cup C_1$, где

$$\begin{aligned} C_1 &= [e_1] \cup (e_2 + [e_1]) \cup (2e_2 + [e_1]) \cup [e_2] \cup (e_1 + [e_2]), \\ C_0 &= \{(3,4), (3,3), (2,4), (2,3)\}. \end{aligned}$$

Чтобы найти число точек степени $\leq s$ в C_1, мы найдем число таких точек в каждом сдвиге, просуммируем эти числа и вычтем число тех точек, которые были сосчитаны более одного раза. (В этом примере тройные пересечения пусты. Почему?) Число точек степени $\leq s$ в $[e_2]$ равно $\binom{s+1}{s} = \binom{s+1}{1} = s + 1$, а число таких точек в $e_1 + [e_2]$ равно $\binom{1+s-1}{s-1} = s$. Аналогично, число таких точек в $[e_1], e_2 + [e_1]$ и в $2e_2 + [e_1]$ равно $s + 1, s$ и $s - 1$ соответственно. Среди возможных двойных пересечений шесть непусты и каждое состоит из одной точки. Вы можете проверить, что шесть точек $(1,2), (1,1), (1,0), (0,2), (0,1), (0,0)$ принадлежат более чем одному сдвигу. Поэтому при достаточно большом s число точек в C_1^s равно

$$|C_1^s| = (s+1) + s + (s+1) + s + (s-1) - 6 = 5s - 5.$$

Кроме того, имеется еще 4 точки в C_0; поэтому

$$|C(I)^s| = |C_1^s| + |C_0^s| = (5s-5) + 4 = 5s - 1,$$

если s достаточно велико. (В упр. 9 будет показано, что «достаточно велико» означает, что $s \geq 7$.)

Теорема 6 показывает, что размерность аффинного многообразия, определенного мономиальным идеалом, равна степени полинома от s, который выражает число точек степени $\leq s$ (при достаточно большом s) в $C(I)$. Это дает чисто алгебраическое определение размерности. В § 3 мы распространим эти идеи на произвольный идеал.

Полином из теоремы 6 обладает тем свойством, что его значения при достаточно больших целых s являются целыми числами. Нам понадобятся некоторые свойства таких полиномов. Отметим, во-первых, что такие полиномы *не обязательно* имеют целые коэффициенты. Например, полином $s(s-1)/2$ принимает целые значения при целых s, хотя его коэффициенты не являются целыми числами. Причина состоит в том, что либо s, либо $s-1$ является четным числом, а следовательно, делится на 2. Аналогично, полином $s(s-1)(s-2)/6$ принимает целые значения при целых s, так как из трех чисел $s, s-1, s-2$ одно делится на 3 и хотя бы одно делится на 2. Нетрудно доказать, что

$$\binom{s}{d} = \frac{s(s-1)\dots(s-(d-1))}{d!} = \frac{1}{d\cdot(d-1)\dots 2\cdot 1}s(s-1)\dots(s-(d-1))$$

принимает целые значения при целых s (см. упр. 10). В упр. 11 и 12 будет доказано, что любой полином степени d, принимающий целые значения при достаточно больших целых s, может быть однозначно представлен в виде целочисленной линейной комбинации полиномов

$$\binom{s}{0} = 1, \quad \binom{s}{1} = s, \quad \binom{s}{2} = \frac{s(s-1)}{2}, \quad \dots,$$
$$\binom{s}{d} = \frac{s(s-1)\dots(s-(d-1))}{d!}.$$

Используя это, мы можем дать следующее уточнение теоремы 6.

Предложение 7. *Пусть $I \subset k[x_1,\dots,x_n]$ — мономиальный идеал и $\dim \mathbf{V}(I) = d$. Тогда для достаточно больших s число точек степени $\leq s$ в $C(I)$ выражается полиномиальной функцией от s степени d, которая может быть представлена в виде*

$$\sum_{i=0}^{d} a_i \binom{s}{d-i},$$

где $a_i \in \mathbb{Z}$ при $0 \leq i \leq d$ и $a_0 > 0$.

В конце параграфа мы обсудим случай проективных многообразий, заданных мономиальным идеалом. Мономиальный идеал $I \subset k[x_1,\dots,x_n]$ однороден (см. упр. 13), а следовательно, он определяет проективное многообразие $\mathbf{V}_p(I) \subset \mathbb{P}^{n-1}(k)$, где нижний индекс p указывает, что мы находимся в проективном пространстве. В упр. 14 будет показано, что $\mathbf{V}_p(I)$ является конечным объединением проективных линейных подпространств с размерностями на единицу меньше, чем размерности соответствующих аффинных подпространств. Как и в аффинном случае, мы определяем *размерность* конечного объединения проективных линейных подпространств как максимум их размерностей. Тогда теорема 6 показывает, что размерность проективного многообразия $\mathbf{V}_p(I)$ мономиального идеала I на единицу меньше, чем степень полиномиальной функции от s, выражающей число мономов степени $\leq s$, не принадлежащих идеалу I.

В этом случае удобнее рассматривать полиномиальную функцию от s, выражающую число мономов степени, *равной* s. Причина объясняется в следующем предложении.

Предложение 8. *Пусть $I \subset k[x_1,\dots,x_n]$ — мономиальный идеал и $\mathbf{V}_p(I) \subset \mathbb{P}^{n-1}(k)$ — проективное многообразие, определенное идеалом I. Если $\dim \mathbf{V}_p(I) = d-1$, то для достаточно больших s число мономов полной степени s, не принадлежащих I, выражается полиномиальной функцией от s степени $d-1$ вида*

$$\sum_{i=0}^{d-1} b_i \binom{s}{d-1-i},$$

где $b_i \in \mathbb{Z}$ при $0 \leq i \leq d-1$ и $b_0 > 0$.

Доказательство. Аффинное многообразие $\mathbf{V}(I) \subset k^n$ имеет размерность d. Поэтому число мономов степени $\leq s$, не принадлежащих I, выражается полиномиальной функцией $p(s)$ степени d (при достаточно больших s). Коэффициент при s^d у этого полинома положителен. Значит, число мономов степени, *равной* s, для достаточно больших s выражается функцией

$$p(s) - p(s-1).$$

В упр. 15 будет доказано, что этот полином имеет степень $d-1$ и его старший коэффициент положителен. Так как он принимает целые значения при достаточно больших s, то $p(s)-p(s-1)$ имеет требуемый вид. □

В частности, из этого предложения следует, что если проективное многообразие задано мономиальным идеалом, то размерность этого многообразия и степень полинома, определенного в предложении 8, совпадают. В § 3 мы обобщим это утверждение на случай произвольного однородного идеала $I \subset k[x_1, \dots, x_n]$.

Упражнения к § 2

1. В этом упражнении мы докажем некоторые утверждения примера 1. Напомним, что $I \subset k[x,y]$ — собственный мономиальный идеал.
   (a) В случае (b) примера 1 докажите, что если $s > l$, то l «прямых» содержат $ls - (1+2+\dots+l-1)$ мономов полной степени $\le s$.
   (b) В случае (b) докажите, что количество мономов полной степени $\le s$, не принадлежащих I, равно $ls+C_0$, если s достаточно велико. Объясните, как найти C_0, и докажите, что $s > a+b$ «достаточно велико». Покажите на рисунке, что происходит, если s слишком мало.
   (c) В случае (d) примера 1 покажите, что константа C_0 в полиномиальной функции, выражающей число точек в $C(I)$ полной степени $\le s$, равна (конечному) числу мономов, не принадлежащих «прямым», минус lk мономов, принадлежащих обоим семействам «прямых», минус $1+2+\dots+(l-1)$, минус $1+2+\dots+(k-1)$.
2. Пусть $I \subset k[x_1, \dots, x_n]$ — мономиальный идеал. Предположим, что в $\mathbb{Z}^n_{\ge 0}$ сдвиг $\alpha + [e_{i_1}, \dots, e_{i_r}]$ содержится в $C(I)$. Пусть $\alpha = \sum_{i \notin \{i_1,\dots,i_r\}} a_i e_i$; докажите, что $C(I)$ содержит все сдвиги $\beta + [e_{i_1}, \dots, e_{i_r}]$ для всех $\beta = \sum_{i \notin \{i_1,\dots,i_r\}} b_i e_i$, где $0 \le b_i \le a_i$ для всех i. В частности, $[e_{i_1}, \dots, e_{i_r}] \subset C(I)$. Указание: I — это идеал.
3. В этом упражнении мы построим мономиальный идеал $I \subset k[x,y,z]$ по заданному $C(I) \subset \mathbb{Z}^3_{\ge 0}$.
   (a) Предположим, что $C(I)$ состоит из одного сдвига координатной плоскости $[e_1, e_2]$ и двух сдвигов координатной плоскости $[e_2, e_3]$. Используя упр. 2, докажите, что $C(I) = [e_1,e_2] \cup [e_2,e_3] \cup (e_1 + [e_2,e_3])$.
   (b) Найдите мономиальный идеал I по множеству $C(I)$, указанному в п. (a). Указание: выясните, какие из мономов малой степени принадлежат, а какие не принадлежат идеалу I?
   (c) Пусть $C(I)$ состоит из одного сдвига координатной плоскости $[e_1, e_2]$, двух сдвигов координатной плоскости $[e_2, e_3]$ и еще одного сдвига (не содержащегося в указанных сдвигах) прямой $[e_2]$. Используя упр. 2, дайте точное описание множества $C(I)$.

   (d) Найдите мономиальный идеал I по множеству $C(I)$ из п. (c).
4. Пусть $I \subset k[x,y,z]$ — мономиальный идеал. В этом упражнении мы изучим множество $C(I) \subset \mathbb{Z}^3_{\ge 0}$.
   (a) Докажите, что для $\mathbf{V}(I)$ имеются следующие возможности: начало координат; одна, две или три координатные прямые; одна, две или три координатные плоскости; объединение координатной плоскости и координатной прямой, перпендикулярной к ней.
   (b) Пусть многообразие $\mathbf{V}(I)$ является началом координат. Докажите, что множество $C(I)$ конечно.
   (c) Пусть многообразие $\mathbf{V}(I)$ является объединением одной, двух или трех координатных прямых. Докажите, что $C(I)$ является объединением конечного числа сдвигов координатных прямых $[e_1], [e_2]$ и/или $[e_3]$ плюс конечное множество точек, не принадлежащих этим сдвигам.
   (d) Пусть многообразие $\mathbf{V}(I)$ является объединением одной, двух или трех координатных плоскостей. Докажите, что $C(I)$ является объединением конечного числа сдвигов координатных плоскостей $[e_1,e_2], [e_1,e_3]$ и/или $[e_2,e_3]$ плюс, возможно, конечное число сдвигов координатных прямых $[e_1], [e_2]$ и/или $[e_3]$ (где сдвиг прямой $[e_i]$ может принадлежать $C(I)$ только в том случае, когда $[e_i,e_j] \subset C(I)$ для некоторого $i \ne j$) плюс, возможно, конечное множество точек, не принадлежащих этим сдвигам.
   (e) Пусть, наконец, многообразие $\mathbf{V}(I)$ является объединением координатной плоскости и координатной прямой, перпендикулярной к ней. Докажите, что $C(I)$ состоит из конечного числа сдвигов одной координатной плоскости $[e_i,e_j]$, плюс конечное ненулевое число сдвигов прямых $[e_k], k \ne i,j$, плюс конечное число сдвигов прямых $[e_i]$ и/или $[e_j]$ плюс конечное число точек, не принадлежащих этим сдвигам.
5. Докажите, что число точек полной степени $\le s$ в m-мерном координатном подпространстве пространства $\mathbb{Z}^n_{\ge 0}$ равно $\binom{m+s}{s}$.
6. Докажите п. (ii) леммы 5.
7. В этом упражнении мы рассмотрим метод вычисления, который называется методом включения-исключения. Этот метод предназначен для нахождения числа элементов конечного объединения конечных множеств. Через $|A|$ мы будем обозначать количество элементов конечного множества A.
   (a) Пусть A и B — конечные множества. Докажите, что
   $$|A \cup B| = |A| + |B| - |A \cap B|.$$
   (b) Пусть A, B, C — конечные множества. Докажите, что
   $$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

(c) Используя индукцию по числу множеств, докажите, что количество элементов конечного объединения конечных множеств $A_1 \cup \ldots \cup A_n$ равно сумме чисел $|A_i|$ минус сумма чисел $|A_i \cap A_j|, i < j$, по всем двойным пересечениям, плюс сумма чисел $|A_i \cap A_j \cap A_k|, i < j < k$, по всем тройным пересечениям, минус сумма по всем четверным пересечениям и т. д. Это может быть выражено следующей формулой:

$$|A_1 \cup \ldots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \left(\sum_{1 \le i_1 < \ldots < i_r \le n} |A_{i_1} \cap \ldots \cap A_{i_r}| \right).$$

8. В этом упражнении мы докажем, что пересечение двух сдвигов различных координатных подпространств в $\mathbb{Z}_{\ge 0}^n$ является сдвигом координатного подпространства меньшей размерности.
   (a) Пусть $A = \alpha + [e_{i_1}, \ldots, e_{i_m}]$, где $\alpha = \sum_{i \notin \{i_1, \ldots, i_m\}} a_i e_i$, и $B = \beta + [e_{j_1}, \ldots, e_{j_r}]$, где $\beta = \sum_{i \notin \{j_1, \ldots, j_r\}} b_i e_i$. Пусть $A \ne B$ и $A \cap B \ne \varnothing$. Докажите, что
   $$[e_{i_1}, \ldots, e_{i_m}] \ne [e_{j_1}, \ldots, e_{j_r}]$$
   и что $A \cap B$ является сдвигом пересечения
   $$[e_{i_1}, \ldots, e_{i_m}] \cap [e_{j_1}, \ldots, e_{j_r}].$$
   (b) Выведите отсюда, что $\dim A \cap B < \max(m, r)$.
9. Рассмотрим мономиальный идеал I из примера после теоремы 6. Докажите, что число точек полной степени $\le s$ в $C(I)$ для $s \ge 7$ описывается полиномом по $5s - 1$.
10. Докажите, что полином
    $$p(s) = \binom{s}{d} = \frac{s(s-1)\ldots(s-(d-1))}{d!}$$
    принимает целые значения для всех целых s. Обратите внимание, что $p(s)$ имеет степень d по s.
11. В этом упражнении мы докажем, что каждый полином $p(s)$ степени $\le d$, принимающий целые значения при $s \in \mathbb{Z}_{\ge 0}$, может быть единственным образом представлен в виде целочисленной линейной комбинации полиномов $\binom{s}{0}, \binom{s}{1}, \binom{s}{2}, \ldots, \binom{s}{d}$.
    (a) Докажите, что полиномы
    $$\binom{s}{0}, \binom{s}{1}, \binom{s}{2}, \ldots, \binom{s}{d}$$
    линейно независимы в том смысле, что из равенства
    $$a_0 \binom{s}{0} + a_1 \binom{s}{1} + \ldots + a_d \binom{s}{d} = 0$$
    следует, что $a_0 = a_1 = \ldots = a_d = 0$.

(b) Пусть полиномы $p(s)$ и $q(s)$ степени $\le d$ принимают одинаковые значения в $d+1$ точках $s = 0, 1, \ldots, d$. Докажите, что $p = q$. Указание: сколько корней имеет полином $p(s) - q(s)$?
(c) Предположим, что мы хотим построить полином $p(s)$, такой, что
$$\begin{aligned} p(0) &= c_0, \\ p(1) &= c_1, \\ &\vdots \\ p(d) &= c_d, \end{aligned} \tag{2}$$
где $c_i \in \mathbb{Z}$ — заданные числа. Пусть
$$\begin{aligned} \Delta_0 &= c_0, \\ \Delta_1 &= c_1 - c_0, \\ \Delta_2 &= c_2 - 2c_1 + c_0, \\ &\vdots \\ \Delta_d &= \sum_{n=0}^{d} (-1)^n \binom{d}{n} c_{d-n}. \end{aligned}$$
Тогда полином
$$p(s) = \Delta_0 \binom{s}{0} + \Delta_1 \binom{s}{1} + \ldots + \Delta_d \binom{s}{d} \tag{3}$$
удовлетворяет равенствам (2). Указание: примените индукцию по d. (Полином в (3) называется интерполяционным полиномом Ньютона–Грегори.)
(d) Объясните, почему полином (3) принимает целые значения при целых s. Указание: напомним, что числа c_i в (2) целые. См. также упр. 10.
(e) Используя п. (a)–(d), докажите, что любой полином степени d, принимающий целые значения при целых $s \ge 0$, может быть представлен единственным образом в виде целочисленной линейной комбинации полиномов $\binom{s}{0}, \ldots, \binom{s}{d}$.

12. Пусть полином $p(s)$ степени d принимает целые значения при всех достаточно больших положительных s, скажем, при $s \ge a$. Мы хотим доказать, что $p(s)$ является целочисленной линейной комбинацией полиномов $\binom{s}{0}, \ldots, \binom{s}{d}$, рассмотренных в упр. 10 и 11. Мы будем считать a положительным целым числом.
    (a) Докажите, что полином $p(s+a)$ может быть представлен в виде целочисленной линейной комбинации полиномов $\binom{s}{0}, \ldots, \binom{s}{d}$, и выведите отсюда, что $p(s)$ является целочисленной линейной комбинацией полиномов $\binom{s-a}{0}, \ldots, \binom{s-a}{d}$.
    (b) Используя упр. 10, докажите, что $p(s)$ принимает целые значения при *всех* целых s и является целочисленной линейной комбинацией полиномов $\binom{s}{0}, \ldots, \binom{s}{d}$.

13. Докажите, что каждый мономиальный идеал однороден.

14. Пусть $I \subset k[x_1, \ldots, x_n]$ — мономиальный идеал.
    (a) Пусть $\mathbf{V}(x_{i_1}, \ldots, x_{i_r}) \subset k^n$ — координатное подпространство размерности $n - r$, содержащееся в $\mathbf{V}(I)$. Докажите, что $\mathbf{V}_p(x_{i_1}, \ldots, x_{i_r}) \subset \mathbf{V}_p(I) \subset \mathbb{P}^{n-1}(k)$. Также докажите, что $\mathbf{V}_p(x_{i_1}, \ldots, x_{i_r})$ является копией проективного пространства $\mathbb{P}^{n-r-1}$ в $\mathbb{P}^{n-1}$. Таким образом, $\mathbf{V}_p(x_{i_1}, \ldots, x_{i_r})$ является проективным подпространством размерности $n - r - 1$.
    (b) Докажите, что $\mathbf{V}_p(I)$ является конечным объединением проективных линейных подпространств размерности на единицу меньшей, чем размерность соответствующих подпространств в аффинном случае.

15. Докажите утверждение из предложения 8 о том, что если $p(s)$ — полином степени d с положительным старшим коэффициентом, то $p(s) - p(s-1)$ является полиномом степени $d - 1$ с положительным старшим коэффициентом.

§ 3. Функция Гильберта и размерность многообразия

В этом параграфе мы определим функцию Гильберта идеала I и с ее помощью — размерность многообразия V. Определения будут даны и в аффинном, и в проективном случаях. Основная идея состоит в том, чтобы, опираясь на опыт, полученный в предыдущем параграфе, определить размерность в терминах числа мономов, не принадлежащих идеалу I. В аффинном случае мы будем использовать мономы степени $\leq s$, а в проективном случае — мономы степени, *равной* s.

Сразу отметим, что результаты § 2 не могут быть применены непосредственно, потому что когда идеал I не является мономиальным, различные мономы, не принадлежащие I, могут быть зависимыми. Пусть, например, $I = \langle x^2 - y^2 \rangle$. Тогда $x^2, y^2 \notin I$, но их разность принадлежит I. Поэтому x^2 и y^2 не могут рассматриваться как два разных монома из дополнения идеала I. Обобщая результаты § 2, мы должны рассматривать число мономов степени $\leq s$, «линейно независимых по модулю» I.

В гл. 5 было определено факторкольцо по идеалу. Аналогичная операция может быть определена на векторных пространствах. Она позволяет сделать предыдущие соображения точными. Рассмотрим векторное пространство V и его подпространство $W \subset V$. Легко видеть, что отношение $v \sim v' \Leftrightarrow v - v' \in W$ на V является отношением эквивалентности (см. упр. 1). Множество классов эквивалентности

по отношению $\sim$ обозначается через V/W, так что

$$V/W = \{[v] : v \in V\}.$$

В упражнениях будет доказано, что операции $[v] + [v'] = [v + v']$ и $a[v] = [av]$, где $a \in k$, $v, v' \in V$, определены корректно и V/W является векторным пространством над k, которое называется *факторпространством* пространства V по W.

Если V конечномерно, то размерность пространства V/W может быть вычислена следующим образом:

Предложение 1. *Пусть W является подпространством конечномерного векторного пространства V. Тогда W и V/W конечномерны и*

$$\dim V = \dim W + \dim V/W.$$

Доказательство. Конечномерность пространства W является стандартным результатом линейной алгебры. Пусть $v_1, \ldots, v_m$ — базис в W, так что $\dim W = m$. Векторы $v_1, \ldots, v_m$ линейно независимы в V и потому могут быть дополнены до базиса $v_1, \ldots, v_m, v_{m+1}, \ldots, v_{m+n}$ пространства V. Таким образом, $\dim V = m + n$. Мы утверждаем, что $[v_{m+1}], \ldots, [v_{m+n}]$ образуют базис в V/W.

Пусть $[v] \in V/W$ и $v = \sum_{i=1}^{m+n} a_i v_i$. Тогда $v \sim a_{m+1}v_{m+1} + \ldots + a_{m+n}v_{m+n}$, так как разность этих векторов — это $a_1v_1 + \ldots + a_mv_m \in W$. Таким образом,

$$\begin{aligned}[v] &= [a_{m+1}v_{m+1} + \ldots + a_{m+n}v_{m+n}] = \\ &= a_{m+1}[v_{m+1}] + \ldots + a_{m+n}[v_{m+n}].\end{aligned}$$

Доказательство линейной независимости элементов $[v_{m+1}], \ldots, [v_{m+n}]$ мы оставляем читателю в качестве упражнения (см. упр. 2). Предложение доказано. □

Размерность аффинного многообразия

Как векторное пространство над k кольцо $k[x_1, \ldots, x_n]$ имеет бесконечную размерность. То же самое справедливо для любого его ненулевого идеала (см. упр. 3). Чтобы перейти к конечномерному случаю, надо ограничиться рассмотрением полиномов полной степени $\leq s$. Обозначим через

$$k[x_1, \ldots, x_n]_{\leq s}$$

подмножество полиномов полной степени $\leq s$ в $k[x_1, \ldots, x_n]$. По лемме 4 из § 2 множество $k[x_1, \ldots, x_n]_{\leq s}$ является векторным пространством размерности $\binom{n+s}{s}$. Пусть I — идеал в $k[x_1, \ldots, x_n]$. Через

$$I_{\leq s} = I \cap k[x_1, \ldots, x_n]_{\leq s}$$

мы обозначим множество полиномов полной степени $\leq s$, принадлежащих идеалу I. Заметим, что $I_{\leq s}$ является подпространством векторного пространства $k[x_1, \ldots, x_n]_{\leq s}$. Теперь мы можем определить аффинную функцию Гильберта идеала I.

Определение 2. Пусть I является идеалом в $k[x_1, \ldots, x_n]$. *Аффинной функцией Гильберта* идеала I называется функция, определенная на множестве неотрицательных целых чисел следующим образом:

$$\begin{aligned} {}^aHF_I(s) &= \dim k[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} \\ &= \dim k[x_1, \ldots, x_n]_{\leq s} - \dim I_{\leq s} \end{aligned}$$

(второе равенство следует из предложения 1).

В рамках этого определения результаты § 2 могут быть переформулированы следующим образом.

Предложение 3. *Пусть I является собственным мономиальным идеалом в $k[x_1, \ldots, x_n]$.*

(i) *Для всех $s \geq 0$ значение ${}^aHF_I(s)$ равно числу мономов степени $\leq s$, не принадлежащих идеалу I.*

(ii) *Для достаточно больших s аффинная функция Гильберта идеала I является полиномиальной функцией вида*

$${}^aHF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

где $b_i \in \mathbb{Z}$ и $b_0 > 0$.

(iii) *Степень полинома в* (ii) *равна максимуму размерностей координатных подпространств, принадлежащих $\mathbf{V}(I)$.*

Доказательство. Докажем (i). Отметим, что $\{x^\alpha : |\alpha| \leq s\}$ является базисом для $k[x_1, \ldots, x_n]_{\leq s}$ как векторного пространства над k. Из леммы 3 из § 4 гл. 2 следует, что $\{x^\alpha : |\alpha| \leq s, x^\alpha \in I\}$ является базисом в $I_{\leq s}$. Следовательно, мономы из $\{x^\alpha : |\alpha| \leq s,\ x^\alpha \notin I\}$ дополняют базис подпространства $I_{\leq s}$ до базиса пространства $k[x_1, \ldots, x_n]_{\leq s}$. Из предложения 1 следует, что множество $\{[x^\alpha] : |\alpha| \leq s, x^\alpha \notin I\}$ является базисом факторпространства $k[x_1, \ldots, x_n]_{\leq s}/I_{\leq s}$.

(ii) и (iii) непосредственно следуют из п. (i) и предложения 7 из § 2. □

Теперь мы готовы установить связь между мономиальными идеалами и произвольными идеалами в $k[x_1, \ldots, x_n]$. Эта связь основана на следующем результате, принадлежащем Маколею. Как и

в § 4 гл. 8, мы будем называть мономиальное упорядочение $>$ на $k[x_1, \ldots, x_n]$ градуированным, если из $|\alpha| > |\beta|$ следует, что $x^\alpha > x^\beta$.

Предложение 4. *Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал, а $>$ — градуированное упорядочение на $k[x_1, \ldots, x_n]$. Тогда мономиальный идеал $\langle \mathrm{LT}(I) \rangle$ имеет ту же аффинную функцию Гильберта, что и идеал I.*

Доказательство. Зафиксируем s и рассмотрим старшие мономы $\mathrm{LM}(f)$ всех элементов $f \in I_{\leq s}$. Таких мономов только конечное число; поэтому

$$\{\mathrm{LM}(f) : f \in I_{\leq s}\} = \{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\} \tag{1}$$

для некоторых полиномов $f_1, \ldots, f_m \in I_{\leq s}$. Мы можем считать, что $\mathrm{LM}(f_1) > \mathrm{LM}(f_2) > \ldots > \mathrm{LM}(f_m)$. Мы утверждаем, что $f_1, \ldots, f_m$ образуют базис для $I_{\leq s}$ как векторного пространства над k.

Чтобы доказать это, рассмотрим нетривиальную линейную комбинацию $a_1 f_1 + \ldots + a_m f_m$ и найдем наименьшее i, такое, что $a_i \neq 0$. Тогда член $a_i \,\mathrm{LT}(f_i)$ не может ни с чем сократиться; следовательно, эта линейная комбинация не равна нулю. Поэтому элементы $f_1, \ldots, f_m$ линейно независимы. Пусть $W = [f_1, \ldots, f_m] \subset I_{\leq s}$ — линейная оболочка полиномов $f_1, \ldots, f_m$. Если $W \neq I_{\leq s}$, то выберем полином $f \in I_{\leq s} - W$ с минимальным старшим мономом $\mathrm{LM}(f)$. Согласно (1), $\mathrm{LM}(f) = \mathrm{LM}(f_i)$ для некоторого i; следовательно, $\mathrm{LT}(f) = \lambda \,\mathrm{LT}(f_i)$ для некоторого $\lambda \neq 0$. Тогда полином $f - \lambda f_i$ содержится в $I_{\leq s}$, и его старший моном меньше, чем $\mathrm{LM}(f)$. В силу минимальности $\mathrm{LM}(f)$ мы имеем $f - \lambda f_i \in W$. Но из этого следует, что $f \in W$. Противоречие. Следовательно, $W = [f_1, \ldots, f_m] = I_{\leq s}$ и $f_1, \ldots, f_m$ — базис в $I_{\leq s}$.

Мономиальный идеал $\langle \mathrm{LT}(I) \rangle$ порожден старшими членами (или старшими мономами) элементов из I. Поэтому $\mathrm{LM}(f_i) \in \langle \mathrm{LT}(I) \rangle_{\leq s}$. Мы утверждаем, что $\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)$ образуют базис векторного пространства $\langle \mathrm{LT}(I) \rangle_{\leq s}$. Рассуждая, как выше, легко показать, что эти мономы линейно независимы. Осталось доказать, что линейная оболочка $[\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)]$ совпадает с $\langle \mathrm{LT}(I) \rangle_{\leq s}$. Для этого достаточно доказать, что (см. лемму 3 из § 4 гл. 2)

$$\{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\} = \{\mathrm{LM}(f) : f \in I, \text{ степень } \mathrm{LM}(f) \leq s\}. \tag{2}$$

Так как $>$ является градуированным упорядочением, то *любой* ненулевой полином $f \in k[x_1, \ldots, x_n]$ имеет ту же полную степень, что и $\mathrm{LM}(f)$. В частности, если полная степень монома $\mathrm{LM}(f)$ не превышает s, то и полная степень полинома f не превышает s. Поэтому (2) прямо следует из (1).

Таким образом, пространства $I_{\le s}$ и $\langle \mathrm{LT}(I)\rangle_{\le s}$ имеют одинаковую размерность (так как оба они обладают базисом из m элементов). Теперь формула размерности из предложения 1 дает соотношение

$$\begin{aligned} {}^aHF_I(s) &= \dim k[x_1,\dots,x_n]_{\le s}/I_{\le s} \\ &= \dim k[x_1,\dots,x_n]_{\le s}/\langle \mathrm{LT}(I)\rangle_{\le s} = {}^aHF_{\langle \mathrm{LT}(I)\rangle}(s). \end{aligned}$$

Предложение доказано. □

Объединяя предложения 3 и 4, мы сразу получаем, что если I — *произвольный* идеал в $k[x_1,\dots,x_n]$, то для достаточно большого s его функция Гильберта может быть записана в виде

$${}^aHF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

где $b_i \in \mathbb{Z}$ и $b_0 > 0$. Дадим определение.

Определение 5. Полином, равный ${}^aHF_I(s)$ при достаточно больших s, называется *аффинным полиномом Гильберта* идеала I и обозначается ${}^aHP_I(s)$.

В качестве примера рассмотрим идеал $I = \langle x^3y^2+3x^2y^2+y^3+1\rangle \subset k[x,y,z]$. Используя grlex-упорядочение, получаем, что $\langle \mathrm{LT}(I)\rangle = \langle x^3y^2\rangle$. С помощью методов § 2 установлено, что число мономов степени $\le s$, не принадлежащих I, равно $5s-5$ при $s \ge 5$. Значит, в силу предложений 3 и 4

$${}^aHF_I(s) = {}^aHF_{\langle LT(I)\rangle}(s) = 5s-5$$

при $s \ge 5$. Следовательно,

$${}^aHP_I(s) = 5s-5.$$

По определению аффинная функция Гильберта идеала I совпадает с его аффинным полиномом Гильберта при достаточно больших s. Наименьшее целое s_0, такое, что ${}^aHF_I(s) = {}^aHP_I(s)$ при $s \ge s_0$, называется *индексом регулярности* идеала I. Задача вычисления индекса регулярности весьма интересна и важна при работе с идеалами, но мы не будем останавливаться на этом вопросе.

Сравним степени аффинных полиномов Гильберта идеалов I и $\sqrt{I}$.

Предложение 6. *Пусть $I \subset k[x_1,\dots,x_n]$ — некоторый идеал. Тогда аффинные полиномы Гильберта идеалов I и $\sqrt{I}$ имеют одинаковую степень.*

Доказательство. Если I — мономиальный идеал, то степень его аффинного полинома Гильберта равна наибольшей из размерностей координатных подпространств, принадлежащих $\mathbf{V}(I)$. Так как $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$, то ${}^aHP_I(s)$ и ${}^aHP_{\sqrt{I}}(s)$ имеют одинаковую степень.

Пусть теперь I — произвольный идеал. Выберем градуированное упорядочение $>$ на $k[x_1,\dots,x_n]$. Мы утверждаем, что

$$\langle \mathrm{LT}(I)\rangle \subset \langle \mathrm{LT}(\sqrt{I})\rangle \subset \sqrt{\langle \mathrm{LT}(I)\rangle}. \tag{3}$$

Первое включение очевидно, так как $I \subset \sqrt{I}$. Докажем второе. Пусть $x^\alpha \in \langle \mathrm{LT}(\sqrt{I})\rangle$. Это означает, что существует полином $f \in \sqrt{I}$, такой, что $\mathrm{LM}(f) = x^\alpha$. Но $f^r \in I$ для некоторого $r \ge 1$; следовательно, $x^{r\alpha} = \mathrm{LM}(f^r) \in \langle \mathrm{LT}(I)\rangle$. Таким образом, $x^\alpha \in \sqrt{\langle LT(I)\rangle}$.

В упр. 8 мы докажем, что если $I_1 \subset I_2$ — идеалы в $k[x_1,\dots,x_n]$, то $\deg {}^aHP_{I_2} \le \deg {}^aHP_{I_1}$. Тогда из (3) получаем

$$\deg {}^aHP_{\sqrt{\langle \mathrm{LT}(I)\rangle}} \le \deg {}^aHP_{\langle \mathrm{LT}(\sqrt{I})\rangle} \le \deg {}^aHP_{\langle \mathrm{LT}(I)\rangle}.$$

Но два крайних числа равны; следовательно, полиномы ${}^aHP_{\langle LT(I)\rangle}$ и ${}^aHP_{\langle LT(\sqrt{I})\rangle}$ имеют одинаковую степень. По предложению 4 то же самое верно для полиномов ${}^aHP_I$ и ${}^aHP_{\sqrt{I}}$. Предложение доказано. □

Смысл этого предложения состоит в том совсем не очевидном факте, что степень аффинного полинома Гильберта имеет *геометрическое* значение, а не только *алгебраическое*, — она указывает насколько $I_{\le s}$ отличается от $k[x_1,\dots,x_n]_{\le s}$. Напомним, что $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$ для любого идеала I. Таким образом, степень аффинного полинома Гильберта одна и та же для большой совокупности идеалов, которые определяют одно и то же многообразие. Кроме того, мы знаем из § 2, что степень аффинного полинома Гильберта мономиального идеала равна (интуитивно понимаемой) размерности многообразия мономиального идеала. Поэтому неудивительно, что и в общем случае мы определяем размерность в терминах аффинной функции Гильберта.

Определение 7. *Размерностью* аффинного многообразия $V \subset k^n$, обозначаемой $\dim V$, называется степень аффинного полинома Гильберта идеала $I = \mathbf{I}(V) \subset k[x_1,\dots,x_n]$.

В качестве примера рассмотрим скрученную кубику $V = \mathbf{V}(y-x^2, z-x^3) \subset \mathbb{R}^3$. В гл. 1 было доказано, что $I = \mathbf{I}(V) = \langle y-x^2, z-x^3\rangle \subset \mathbb{R}[x,y,z]$. Базис Грёбнера идеала I по отношению к grlex-упорядочению есть $\{y^3-z^2, x^2-y, xy-z, xz-y^2\}$. Поэтому

$\langle \mathrm{LT}(I)\rangle = \langle y^3, x^2, xy, xz\rangle$. Тогда

$$\dim V = \deg {}^aHP_I = \deg {}^aHP_{\langle \mathrm{LT}(I)\rangle} = \text{максимальная размерность координатного подпространства в } \mathbf{V}(\langle \mathrm{LT}(I)\rangle)$$

в силу предложений 3 и 4. Так как

$$\mathbf{V}(\langle \mathrm{LT}(I)\rangle) = \mathbf{V}(y^3, x^2, xy, xz) = \mathbf{V}(x, y) \subset \mathbb{R}^3,$$

то $\dim V = 1$. Этот результат согласуется с нашим интуитивным представлением о том, что кривая в $\mathbb{R}^3$ должна быть одномерной.

В качестве другого примера найдем размерность многообразия мономиального идеала. В упр. 10 будет показано, что $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ при условии, что поле k бесконечно. Тогда по предложению 6

$$\dim \mathbf{V}(I) = \deg {}^aHP_{\mathbf{I}(\mathbf{V}(I))} = \deg {}^aHP_{\sqrt{I}} = \deg {}^aHP_I.$$

Теперь из п. (iii) предложения 3 следует, что $\dim \mathbf{V}(I)$ равна максимальной размерности координатного подпространства, принадлежащего $\mathbf{V}(I)$. Это согласуется с определением размерности, данным в § 2. В упр. 10 будет показано, что этот результат становится неверным в случае конечного поля k.

Интересным исключительным случаем является пустое многообразие. Отметим, что $1 \in \mathbf{I}(V)$ в том и только том случае, когда $k[x_1, \ldots, x_n]_{\le s} = I_{\le s}$ для всех s. Следовательно,

$$V = \varnothing \iff {}^aHP_{\mathbf{I}(V)} = 0.$$

Так как нулевой полином не имеет степени, то мы не можем приписать никакой размерности пустому многообразию.

Недостатком определения 7 является то, что для вычисления размерности многообразия мы должны знать идеал $\mathbf{I}(V)$, найти который совсем не просто. Было бы гораздо лучше, если бы $\dim V$ равнялась степени полинома ${}^aHP_I$ для любого идеала I, задающего V. Но, к сожалению, это совсем не так. Пусть, например, $I = \langle x^2 + y^2\rangle \subset \mathbb{R}[x, y]$. Легко проверить, что степень полинома ${}^aHP_I(s)$ равна 1. Однако $V = \mathbf{V}(I) = \{(0,0)\} \subset \mathbb{R}^2$, и, значит, V имеет размерность 0, т. е. в этом случае $\dim \mathbf{V}(I) \neq \deg {}^aHP_I$ (см. упр. 11).

Если поле k алгебраическим замкнуто, то эти трудности пропадают, и мы имеем следующее утверждение о связи размерности многообразия и степени полинома Гильберта определяющего идеала.

Теорема 8 (теорема о размерности). *Рассмотрим аффинное многообразие $V = \mathbf{V}(I)$, где $I \subset k[x_1, \ldots, x_n]$ — идеал. Если k алгебраически замкнуто, то*

$$\dim V = \deg {}^aHP_I.$$

Кроме того, если $>$ — градуированное упорядочение на $k[x_1, \ldots, x_n]$, то

$$\dim V = \deg {}^aHP_{\langle \mathrm{LT}(I)\rangle} = \textit{максимальная размерность координатного подпространства в } \mathbf{V}(\langle \mathrm{LT}(I)\rangle).$$

Это соотношение справедливо над любым полем, если $I = \mathbf{I}(V)$.

Доказательство. Так как k алгебраически замкнуто, то $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ (теорема о нулях). Тогда

$$\dim V = \deg {}^aHP_{\mathbf{I}(V)} = \deg {}^aHP_{\sqrt{I}} = \deg {}^aHP_I,$$

где последнее равенство вытекает из предложения 6. Вторая часть теоремы следует из предложений 3 и 4. □

Таким образом, если нам нужно найти размерность многообразия $V = \mathbf{V}(I)$ над алгебраически замкнутым полем, то нужно действовать следующим образом:

- Вычислить базис Грёбнера идеала I, используя градуированное упорядочение, такое, как grlex или grevlex.
- Найти максимальную размерность d координатного подпространства, содержащегося в $\mathbf{V}(\langle \mathrm{LT}(I)\rangle)$. Обратите внимание, что предложение 3 из § 1 дает алгоритм вычисления этой размерности.

Теперь по теореме 8 мы имеем $\dim V = d$.

Размерность проективного многообразия

Наше обсуждение размерности проективных многообразий будет проходить аналогично тому, как это делалось в случае аффинных многообразий: методы и характер рассуждений во многом совпадают. Мы начнем с определения функции Гильберта и полинома Гильберта произвольного однородного идеала $I \subset k[x_0, \ldots, x_n]$.

Как мы видели в § 2, в проективном случае удобнее использовать полиномы степени, равной s, чем не превосходящей s. Так как полиномы степени s не образуют векторного пространства (см. упр. 13), то мы будем работать с *однородными* полиномами полной степени s [1]. Обозначим через $k[x_0, \ldots, x_n]_s$ множество однородных полиномов полной степени s (нулевой полином мы будем считать принадлежащим этому множеству). В упр. 13 будет доказано, что $k[x_0, \ldots, x_n]_s$ является векторным пространством размерности $\binom{n+s}{s}$. Пусть $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Через

$$I_s = I \cap k[x_0, \ldots, x_n]_s$$

[1] См. п. (b) упр. 13 к этому параграфу. — *Прим. ред.*

мы обозначим множество однородных полиномов степени s в I (вместе с нулевым полиномом). Заметим, что I_s является подпространством в $k[x_0,\dots,x_n]_s$. *Функция Гильберта* идеала I определяется так:

$$HF_I(s) = \dim k[x_0,\dots,x_n]_s/I_s.$$

Строго говоря, мы должны были бы называть эту функцию проективной функцией Гильберта, но приведенный выше термин является общепринятым в алгебраической геометрии.

Если I — мономиальный идеал, то рассуждая, как в предложении 3, мы можем доказать, что $HF_I(s)$ равно числу мономов степени s, не принадлежащих I. Тогда по предложению 8 из § 2

$$HF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i} \tag{4}$$

при достаточно большом s, где $b_i \in \mathbb{Z}$ и $b_0 > 0$. Мы также знаем, что d равно максимальной размерности проективного координатного подпространства в $\mathbf{V}(I) \subset \mathbb{P}^n(k)$.

Как и в аффинном случае, мы используем мономиальное упорядочение, чтобы найти связь между функцией Гильберта однородного идеала и функцией Гильберта мономиального идеала.

Предложение 9. *Пусть $I \subset k[x_0,\dots,x_n]$ — однородный идеал и $>$ — мономиальное упорядочение на $k[x_0,\dots,x_n]$. Тогда мономиальный идеал $\langle \mathrm{LT}(I)\rangle$ имеет ту же функцию Гильберта, что и I.*

Доказательство. Доказательство проводится так же, как доказательство предложения 4. Мы однако, *не* требуем, чтобы $>$ было градуированным упорядочением. Поэтому потребуются некоторые изменения в рассуждениях.

Зафиксируем s. Мы можем найти $f_1,\dots,f_m \in I_s$, такие, что

$$\{\mathrm{LM}(f) : f \in I_s\} = \{\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_m)\}, \tag{5}$$

причем $\mathrm{LM}(f_1) > \mathrm{LM}(f_2) > \dots > \mathrm{LM}(f_m)$. Как и в доказательстве предложения 4, $f_1,\dots,f_m$ образуют базис идеала I_s над k.

Рассмотрим $\langle \mathrm{LT}(I)\rangle_s$. Мы знаем, что $\mathrm{LM}(f_i) \in \langle \mathrm{LT}(I)\rangle_s$ (так как $f_i \in I_s$). Нам нужно доказать, что $\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_m)$ является базисом векторного пространства $\langle \mathrm{LT}(I)\rangle_s$. Эти мономы различны и, следовательно, линейно независимы. По лемме 3 из § 4 гл. 2 теперь достаточно доказать, что

$$\{\mathrm{LM}(f_1),\dots,\mathrm{LM}(f_m)\} = \{\mathrm{LM}(f) : f \in I, \mathrm{LM}(f) \text{ имеет степень } s\}. \tag{6}$$

Пусть $\mathrm{LM}(f)$ имеет полную степень s, где $f \in I$. Представим f в виде суммы однородных полиномов, $f = \sum_i h_i$, где h_i имеет степень i. Тогда $\mathrm{LM}(f) = \mathrm{LM}(h_s)$. Так как I — однородный идеал, то $h_s \in I$. Таким образом, $\mathrm{LM}(f) = \mathrm{LM}(h_s)$, где $h_s \in I$, и (6) следует из (5). Далее рассуждения проводятся, как в предложении 4. □

Объединяя предложение 9 с описанием функции Гильберта мономиального идеала (см. (4)), получаем, что функция Гильберта однородного идеала $I \subset k[x_0,\dots,x_n]$ имеет вид

$$HF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i}$$

(где s достаточно велико). Этот полином называется *полиномом Гильберта* идеала I и обозначается через $HP_I(s)$.

Теперь мы можем дать определение размерности проективного многообразия в терминах полинома Гильберта.

Определение 10. *Размерностью* проективного многообразия $V \subset \mathbb{P}^n(k)$, обозначаемой через $\dim V$, называется степень полинома Гильберта однородного идеала $I = \mathbf{I}(V) \subset k[x_0,\dots,x_n]$.

Над алгебраически замкнутым полем размерность может быть найдена следующим образом.

Теорема 11 (теорема о размерности). *Пусть $V = \mathbf{V}(I) \subset \mathbb{P}^n(k)$ — проективное многообразие, где $I \subset k[x_0,\dots,x_n]$ — однородный идеал. Если V непусто, а k алгебраически замкнуто, то*

$$\dim V = \deg HP_I.$$

Более того, для любого мономиального упорядочения

$$\dim V = \deg HP_{\langle \mathrm{LT}(I)\rangle} = \text{максимальная размерность проективного координатного подпространства в } \mathbf{V}(\langle \mathrm{LT}(I)\rangle).$$

Это соотношение выполнено над любым полем, если $I = \mathbf{I}(V)$.

Доказательство. На первом шаге нужно доказать, что степени полиномов Гильберта идеалов I и $\sqrt{I}$ совпадают. Это доказывается так же, как аналогичное утверждение доказывается в предложении 6.

По проективной теореме о нулях $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Далее доказательство проводится, как в аффинном случае (см. теорему 8). □

Теперь мы сравним размерности аффинных и проективных многообразий.

Теорема 12.

(i) *Пусть $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Тогда при $s \geq 1$*

$$HF_I(s) = {}^aHF_I(s) - {}^aHF_I(s-1).$$

Аналогичное соотношение выполнено для полиномов Гильберта. Таким образом, если $V \subset \mathbb{P}^n(k)$ — проективное многообразие, а $C_V \subset k^{n+1}$ — его аффинный конус (см. § 3 гл. 8), то

$$\dim C_V = \dim V + 1.$$

(ii) *Пусть $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал, а $I^h \subset k[x_0, \ldots, x_n]$ — его гомогенизация по отношению к x_0 (см. § 4 гл. 8). Тогда при $s \geq 0$ имеем*

$${}^aHF_I(s) = HF_{I^h}(s).$$

Аналогичное соотношение выполнено для полиномов Гильберта. Таким образом, если $V \subset k^n$ — аффинное многообразие, а $\overline{V} \subset \mathbb{P}^n(k)$ — его проективное замыкание (см. § 4 гл. 8), то

$$\dim V = \dim \overline{V}.$$

Доказательство. Мы будем использовать индексы «a» и «p», чтобы указывать на аффинный или проективный случай. Первая часть п. (i) легко сводится к случаю мономиального идеала, а затем мы можем использовать результаты § 2. Детали мы оставляем читателю в качестве упражнения. Теперь заметим, что аффинный конус — это просто *аффинное* многообразие в k^{n+1}, определенное идеалом $\mathbf{I}_p(V)$. Легко видеть, что $\mathbf{I}_a(C_V) = \mathbf{I}_p(V)$ (см. упр. 19). Поэтому размерности многообразий V и C_V равны степеням полиномов $HP_{\mathbf{I}_p(V)}$ и ${}^aHP_{\mathbf{I}_p(V)}$ соответственно. Тогда равенство $\dim C_V = \dim V + 1$ следует из упр. 15 к § 2.

Докажем первую часть п. (ii). Рассмотрим отображения

$$\phi : k[x_1, \ldots, x_n]_{\leq s} \longrightarrow k[x_0, \ldots, x_n]_s,$$
$$\psi : k[x_0, \ldots, x_n]_s \longrightarrow k[x_1, \ldots, x_n]_{\leq s},$$

заданные формулами

$$\begin{aligned} \phi(f) &= x_0^s f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \quad \text{для } f \in k[x_1, \ldots, x_n]_{\leq s}, \\ \psi(F) &= F(1, x_1, \ldots, x_n) \qquad \text{для } F \in k[x_0, \ldots, x_n]_s. \end{aligned} \tag{7}$$

Доказательство того, что эти отображения являются линейными и взаимно обратными, мы оставляем читателю в качестве упражнения. Таким образом, $k[x_1, \ldots, x_n]_{\leq s}$ и $k[x_0, \ldots, x_n]_s$ являются изоморфными векторными пространствами. Следует также доказать, что если полином $f \in k[x_1, \ldots, x_n]_{\leq s}$ имеет полную степень $d \leq s$, то

$$\phi(f) = x_0^{s-d} f^h,$$

где f^h — гомогенизация полинома f, определенная в предложении 7 из § 2 гл. 8.

В упражнениях будет доказано, что

$$\begin{aligned} \phi(I_{\leq s}) &\subset I_s^h \\ \psi(I_s^h) &\subset I_{\leq s} \end{aligned} \tag{8}$$

и что эти включения являются равенствами. Поэтому $I_{\leq s}$ и I_s^h — тоже изоморфные векторные пространства.

Все это показывает, что размерности пространств $k[x_1, \ldots, x_n]_{\leq s}$ и $k[x_0, \ldots, x_n]_s$ совпадают и что размерности пространств $I_{\leq s}$ и I_s^h совпадают тоже. Тогда по предложению 1

$$\begin{aligned} {}^aHP_I(s) &= \dim k[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} \\ &= \dim k[x_0, \ldots, x_n]_s/I_s^h = HP_{I^h}(s), \end{aligned}$$

что и требовалось доказать. □

Теперь рассмотрим вторую часть п. (ii). Пусть $V \subset k^n$, $I = \mathbf{I}_a(V) \subset k[x_1, \ldots, x_n]$, а $I^h \subset k[x_0, \ldots, x_n]$ — гомогенизация идеала I по отношению к переменной x_0. Тогда $\overline{V} = \mathbf{V}_p(I^h) \subset \mathbb{P}^n(k)$. Кроме того, $I^h = \mathbf{I}_p(\overline{V})$ (см. упр. 8 к § 4 гл. 8). Теперь равенства

$$\dim V = \deg {}^aHP_I = \deg HP_{I^h} = \dim \overline{V}$$

следуют из первой части п. (ii). Теорема доказана. □

Некоторые системы компьютерной алгебры могут вычислять полиномы Гильберта. Так, REDUCE располагает командой для вычисления аффинного полинома Гильберта произвольного идеала, а Macaulay и CoCoA — проективного полинома Гильберта однородного идеала.

Упражнения к § 3

1. В этом упражнении будет доказано, что если V — векторное пространство, а W — его подпространство, то V/W является векторным пространством.
   (a) Докажите, что отношение $\sim$ на V, определенное условием $v \sim v' \Leftrightarrow v - v' \in W$, является отношением эквивалентности.
   (b) Докажите корректность определения сложения классов и умножения класса на скаляр (это определение дано в тексте параграфа): если $v, v', w, w' \in V$ и $[v] = [v'], [w] = [w']$, то $[v+w] = [v'+w']$, и $[av] = [av']$ для всех $a \in k$.

(c) Докажите, что V/W является векторным пространством относительно операций, корректность которых доказана в п. (b).

2. Пусть V — конечномерное векторное пространство, а W — его подпространство. Пусть $\{v_1, \dots, v_m, v_{m+1}, \dots, v_{m+n}\}$ — базис пространства V, такой, что векторы $\{v_1, \dots, v_m\}$ образуют базис в W. Докажите, что классы $\{[v_{m+1}], \dots, [v_{m+n}]\}$ линейно независимы в V/W.

3. Докажите, что ненулевой идеал $I \subset k[x_1, \dots, x_n]$ бесконечномерен как векторное пространство над k. Указание: выберите $f \neq 0$ в I и рассмотрите полиномы $x^\alpha f$.

4. В доказательствах предложений 4 и 9 мы использовали базисы векторных пространств $I_{\leq s}$ и I_s, элементы которых имеют различные старшие члены. Мы показали, что такие базисы существуют, но наше доказательство было неконструктивным. В этом упражнении мы обсудим метод построения таких базисов. Будет рассмотрен только однородный случай, но метод применим и в аффинном случае тоже.

   Мы начинаем построение с некоторого базиса в I_s и упорядочиваем элементы этого базиса в соответствии с порядком их старших членов. Если два базисных элемента имеют одинаковые старшие мономы, мы заменяем один из них такой k-линейной их комбинацией, чтобы старший моном комбинации был меньше старших мономов двух этих элементов. Продолжая этот процесс, мы и получим требуемый базис.

   Приведем пример. Пусть $I \subset k[x, y]$ — однородный идеал, и пусть $\{x^3 - xy^2, x^3 + x^2y - z^3, x^2y - y^3\}$ является базисом в I_3. Мы будем использовать grlex-упорядочение с $x > y$.
   (a) Докажите, что если мы заменим второй полином разностью второго и первого, то получим новый базис в I_3.
   (b) Второй и третий полиномы нового базиса имеют одинаковые старшие мономы. Покажите, что, заменив третий полином разностью второго и третьего, мы получим базис $\{x^3 - xy^2, x^2y + xy^2 - z^3, xy^2 + y^3 - z^3\}$ пространства I_3, все старшие мономы которого различны.

5. Пусть $I = \langle x^3 - xyz, y^4 - xyz^2, xy - z^2\rangle$. Используя grlex-упорядочение с $x > y > z$, найдите базисы в I_3 и I_4, элементы которых имеют различные старшие мономы. Указание: используйте метод упр. 4.

6. Используя методы § 2, найдите аффинный полином Гильберта каждого из следующих идеалов.
   (a) $I = \langle x^3y, xy^2\rangle \subset k[x, y]$.
   (b) $I = \langle x^3y^2 + 3x^2y^2 + y^3 + 1\rangle \subset k[x, y]$.
   (c) $I = \langle x^3yz^5, xy^3z^2\rangle \subset k[x, y, z]$.
   (d) $I = \langle x^3 - yz^2, y^4 - x^2yz\rangle \subset k[x, y, z]$.

7. Найдите индекс регулярности (т. е. наименьшее s_0, такое, что ${}^aHF_I(s) = {}^aHP_I(s)$ при $s \geq s_0$) каждого идеала из упр. 6.

8. В этом упражнении мы докажем, что если $I_1 \subset I_2$ — идеалы в $k[x_1, \dots, x_n]$, то
$$\deg {}^aHP_{I_2} \leq \deg {}^aHP_{I_1}.$$
   (a) Докажите, что $C(\langle \mathrm{LT}(I_2)\rangle) \subset C(\langle \mathrm{LT}(I_1)\rangle)$ в $\mathbb{Z}^n_{\geq 0}$.
   (b) Докажите, что при $s \geq 0$ для аффинных *функций* Гильберта выполнено неравенство
$${}^aHF_{I_2}(s) \leq {}^aHF_{I_1}(s).$$
   (c) Используя п. (b), докажите требуемое утверждение о степенях *полиномов* Гильберта. Указание: рассуждайте от противного и рассмотрите значения полиномов при $s \to \infty$.

9. Используя определение 7 докажите, что точка $p = (a_1, \dots, a_n) \in k^n$ является многообразием размерности 0. Указание: используя упр. 7 к § 5 гл. 4, найдите $\mathbf{I}(\{p\})$.

10. Пусть $I \subset k[x_1, \dots, x_n]$ — мономиальный идеал, а поле k бесконечно. В этом упражнении мы исследуем идеал $\mathbf{I}(\mathbf{V}(I))$.
   (a) Докажите, что $\mathbf{I}(\mathbf{V}(x_{i_1}, \dots, x_{i_r})) = \langle x_{i_1}, \dots, x_{i_r}\rangle$. Указание: используйте предложение 5 из § 1 гл. 1.
   (b) Докажите, что пересечение мономиальных идеалов является мономиальным идеалом. Указание: используйте лемму 3 из § 4 гл. 2.
   (c) Докажите, что $\mathbf{I}(\mathbf{V}(I))$ является мономиальным идеалом. Указание: используйте пп. (a) и (b) и теорему 15 из § 3 гл. 4.
   (d) Здесь мы докажем, что $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Мы знаем, что $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$ и что $\mathbf{I}(\mathbf{V}(I))$ является мономиальным идеалом. Поэтому нужно доказать, что если $x^\alpha \in \mathbf{I}(\mathbf{V}(I))$, то $x^{r\alpha} \in I$ при некотором $r > 0$. Указание: если $I = \langle m_1, \dots, m_t\rangle$ и $x^{r\alpha} \notin I$ при $r > 0$, то покажите, что для каждого j существует переменная x_{i_j}, такая, что x_{i_j} делит m_j, но не делит x^α; используя набор переменных $x_{i_1}, \dots, x_{i_t}$, получите противоречие.
   (e) Рассмотрим поле $\mathbb{F}_2$, состоящее из двух элементов. Пусть $I = \langle x\rangle \subset \mathbb{F}_2[x, y]$. Докажите, что $\mathbf{I}(\mathbf{V}(I)) = \langle x, y^2 - y\rangle$. Этот идеал строго содержит идеал $\sqrt{I}$ и не является мономиальным.

11. Пусть $I = \langle x^2 + y^2\rangle \subset \mathbb{R}[x, y]$.
   (a) Докажите, что $\deg {}^aHP_I = 1$.
   (b) Используя упр. 9, докажите, что $\dim \mathbf{V}(I) = 0$.

12. Найдите размерность аффинных многообразий, заданных следующими идеалами. Поле k можно считать алгебраически замкнутым.
   (a) $I = \langle xz, xy - 1\rangle \subset k[x, y, z]$.
   (b) $I = \langle zw - y^2, xy - z^3\rangle \subset k[x, y, z, w]$.

13. Рассмотрим полиномиальное кольцо $k[x_0, \dots, x_n]$.
   (a) Покажите на примере, что множество полиномов полной степени s не замкнуто относительно сложения и, следовательно, не является векторным пространством.

(b) Докажите, что множество однородных полиномов полной степени s (вместе с нулевым полиномом) является векторным пространством над k.
(c) Используя лемму 5 из § 2 докажите, что размерность этого векторного пространства равна $\binom{n+s}{s}$. Указание: найдите число полиномов степени $\leq s$ и число полиномов степени $\leq s-1$.
(d) Дайте второе доказательство формулы размерности из п. (c), используя изоморфизм, определенный в упр. 20 ниже.

14. Пусть I — однородный идеал. Докажите, что степени полиномов Гильберта HP_I и $HP_{\sqrt{I}}$ совпадают. Указание: используйте теорему 12.

15. В этом упражнении мы выясним, когда полином Гильберта равен нулю.
(a) Пусть $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Докажите, что $\langle x_0, \ldots, x_n\rangle^r \subset I$ для некоторого $r > 0$, в том и только том случае, когда полином Гильберта идеала I равен нулю.
(b) Теперь докажите, что многообразие $V \subset \mathbb{P}^n(k)$ пусто в том и только том случае, когда его полином Гильберта равен нулю. Другими словами, пустое многообразие в $\mathbb{P}^n(k)$ не имеет размерности.

16. Найдите размерность проективных многообразий, заданных следующими идеалами. Поле k можно считать алгебраически замкнутым.
(a) $I = \langle x^2 - y^2, x^3 - x^2y + y^3\rangle \subset k[x, y, z]$.
(b) $I = \langle y^2 - xz, x^2y - z^2w, x^3 - yzw\rangle \subset k[x, y, z, w]$.

17. В этом упражнении будет показано, что в общем случае нет никакой связи между числом переменных n, числом r полиномов в базисе идеала I и размерностью многообразия V. Пусть $V \subset \mathbb{P}^3(k)$ — кривая, заданная проективной параметризацией $x = t^3u^2, y = t^4u, z = t^5, w = u^5$. Так как V — кривая в трехмерном пространстве, то наша геометрическая интуиция подсказывает, что она должна быть задана двумя уравнениями. Пусть поле k алгебраически замкнуто.
(a) Используя теорему 12 из § 5 гл. 8, найдите идеал $I \subset k[x, y, z, w]$, такой, что $V = \mathbf{V}(I)$ в $\mathbb{P}^3(k)$. Если вы будете использовать grevlex-упорядочение, то получите базис идеала I, состоящий из трех элементов.
(b) Докажите, что пространство I_2 одномерно, а пространство I_3 шестимерно.
(c) Докажите, что идеал I не может быть порожден двумя элементами. Указание: пусть $I = \langle A, B\rangle$, где полиномы A и B однородны; рассматривая I_2, покажите, что A или B скалярно кратен полиному $y^2 - xz$, а затем получите противоречие, рассматривая I_3.

Гораздо труднее доказать, что не существует двух однородных полиномов A, B, таких, что $V = \mathbf{V}(A, B)$.

18. В этом упражнении мы рассмотрим доказательство п. (i) теоремы 12.
(a) Используя методы § 2, докажите, что $HF_I(s) = {}^aHF_I(s) - {}^aHF_I(s-1)$, если I — мономиальный идеал.
(b) Докажите, что $HF_I(s) = {}^aHF_I(s) - {}^aHF_I(s-1)$, где I — произвольный однородный идеал.

19. Пусть $V \subset \mathbb{P}^n(k)$ — проективное многообразие, а $C_V \subset k^{n+1}$ — его аффинный конус. Докажите, что $\mathbf{I}_p(V) = \mathbf{I}_a(C_V)$ в $k[x_0, \ldots, x_n]$.

20. В этом упражнении мы рассмотрим доказательство п. (ii) теоремы 12.
(a) Докажите, что отображения ϕ и ψ, определенные в (7), являются линейными отображениями и обратны друг другу.
(b) Докажите (8) и выведите отсюда, что $\phi : I_{\leq s} \to I_s^h$ — изоморфизм, обратным к которому является отображение ψ.

§ 4. Элементарные свойства размерности

В этом параграфе мы установим основные свойства размерности. Вот первое из них.

Предложение 1. *Пусть V_1 и V_2 — аффинные или проективные многообразия над произвольным полем и $V_1 \subset V_2$. Тогда* $\dim V_1 \leq \dim V_2$.

Доказательство. Мы оставляем доказательство читателю (см. упр. 1). □

Далее мы рассмотрим связь между размерностью многообразия и числом определяющих его уравнений. Пусть сначала V задано одним уравнением.

Предложение 2. *Пусть поле k алгебраически замкнуто, а $f \in k[x_0, \ldots, x_n]$ — непостоянный однородный полином. Тогда размерность проективного многообразия, заданного полиномом f, определяется формулой*

$$\dim \mathbf{V}(f) = n - 1.$$

Доказательство. Зафиксируем мономиальное упорядочение $>$ на $k[x_0, \ldots, x_n]$. Так как k алгебраически замкнуто, то по теореме 11 из § 3 размерность многообразия $\mathbf{V}(f)$ равна максимальной размерности проективного координатного подпространства, содержащегося в $\mathbf{V}(\langle \mathrm{LT}(I)\rangle)$, где $I = \langle f\rangle$. Но $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(f)\rangle$;

следовательно, так как $\mathrm{LT}(f)$ — непостоянный моном, проективное многообразие $\mathbf{V}(\mathrm{LT}(f))$ является объединением координатных подпространств пространства $\mathbb{P}^n(k)$ размерности $n-1$. Значит, $\dim \mathbf{V}(I) = n-1$. □

Таким образом, если k алгебраически замкнуто, то гиперповерхность $\mathbf{V}(f) \subset \mathbb{P}^n(k)$ всегда имеет размерность $n-1$. Доказательство аналогичного утверждения в аффинном случае мы оставляем читателю в качестве упражнения.

Следует отметить, что это утверждение *не верно*, если поле k не является алгебраически замкнутым. Пусть, например, $I = \langle x^2 + y^2 \rangle \subset \mathbb{R}[x, y]$. В § 3 было доказано, что многообразие $\mathbf{V}(x^2 + y^2) = \{(0,0)\} \subset \mathbb{R}^2$ имеет размерность 0, хотя по предложению 2 его размерность была бы равной 1. На самом деле над полем, которое не является алгебраически замкнутым, многообразие в k^n или в $\mathbb{P}^n(k)$, определенное одним полиномом, может иметь любую размерность от 0 до $n-1$.

Следующее утверждение является аналогом предложения 2, когда пространство $\mathbb{P}^n(k)$ заменено произвольным многообразием V. Напомним, что если I — идеал, а f — полином, то $\mathbf{V}(I + \langle f \rangle) = \mathbf{V}(I) \cap \mathbf{V}(f)$.

Теорема 3. *Пусть поле k алгебраически замкнуто, а I — однородный идеал в $k[x_0, \ldots, x_n]$. Если f — непостоянный однородный полином, то*

$$\dim \mathbf{V}(I) \geq \dim \mathbf{V}(I + \langle f \rangle) \geq \dim \mathbf{V}(I) - 1.$$

Доказательство. Для вычисления размерности многообразия $\mathbf{V}(I + \langle f \rangle)$ нам нужно сравнить полиномы Гильберта HP_I и $HP_{I+\langle f \rangle}$. Так как $I \subset I + \langle f \rangle$, то (см. упр. 8 к § 3)

$$\deg HP_I \geq \deg HP_{I+\langle f \rangle};$$

следовательно, $\dim \mathbf{V}(I) \geq \dim \mathbf{V}(I + \langle f \rangle)$ по теореме 12 из § 3.

Докажем второе неравенство. Пусть полная степень полинома f равна $r > 0$. Зафиксируем $s \geq r$ и рассмотрим отображение

$$\pi : k[x_0, \ldots, x_n]_s / I_s \longrightarrow k[x_0, \ldots, x_n]_s / (I + \langle f \rangle)_s,$$

которое переводит класс $[g] \in k[x_0, \ldots, x_n]_s / I_s$ в $\pi([g]) = [g] \in k[x_0, \ldots, x_n]_s / (I + \langle f \rangle)_s$. В упр. 4 будет доказано, что отображение π определено корректно и является линейным. Легко видеть, что π отображает на все пространство. Найдем его ядро. Для этого рассмотрим отображение

$$\alpha_f : k[x_0, \ldots, x_n]_{s-r} / I_{s-r} \longrightarrow k[x_0, \ldots, x_n]_s / I_s,$$

которое переводит $[h] \in k[x_0, \ldots, x_n]_{s-r} / I_{s-r}$ в $\alpha_f([h]) = [fh] \in k[x_0, \ldots, x_n]_s / I_s$. В упр. 5 будет доказано, что отображение α_f определено корректно и также является линейным.

Мы утверждаем, что ядро отображения π совпадает с образом отображения α_f, т. е.

$$\alpha_f(k[x_0, \ldots, x_n]_{s-r} / I_{s-r}) = \{[g] : \pi([g]) = [0] \text{ в } k[x_0, \ldots, x_n]_s / (I + \langle f \rangle)_s\}. \quad (1)$$

Отметим, что если $h \in k[x_0, \ldots, x_n]_{s-r}$, то $fh \in (I + \langle f \rangle)_s$; следовательно, $\pi([fh]) = [0]$ в $k[x_0, \ldots, x_n]_s / (I + \langle f \rangle)_s$. Обратно, если $g \in k[x_0, \ldots, x_n]_s$ и $\pi([g]) = [0]$, то $g \in (I + \langle f \rangle)_s$. Это означает, что $g = g' + fh$, где $g' \in I$. Запишем g' и h в виде суммы однородных полиномов: $g' = \sum_i g'_i, h = \sum_i h_i$, где полная степень полиномов g'_i и h_i равна i. Тогда $g = g'_s + fh_{s-r}$, поскольку f и g однородны. Так как I — однородный идеал, то $g'_s \in I_s$; следовательно, $[g] = [fh_{s-r}] = \alpha_f([h_{s-r}])$ в $k[x_0, \ldots, x_n]_s / I_s$. Таким образом, $[g]$ принадлежит образу отображения α_f, и (1) доказано.

Так как π сюръективно и его ядро нам известно, то

$$\dim k[x_0, \ldots, x_n]_s / I_s = \dim \alpha_f(k[x_0, \ldots, x_n]_{s-r} / I_{s-r}) + \dim k[x_0, \ldots, x_n]_s / (I + \langle f \rangle)_s.$$

Но

$$\dim \alpha_f(k[x_0, \ldots, x_n]_{s-r} / I_{s-r}) \leq \dim k[x_0, \ldots, x_n]_{s-r} / I_{s-r}, \quad (2)$$

причем равенство достигается в том и только том случае, когда α_f инъективно. Следовательно,

$$\dim k[x_0, \ldots, x_n]_s / (I + \langle f \rangle)_s \geq \dim k[x_0, \ldots, x_n]_s / I_s - \dim k[x_0, \ldots, x_n]_{s-r} / I_{s-r}.$$

В терминах функций Гильберта это неравенство может быть переписано так:

$$HF_{I+\langle f \rangle}(s) \geq HF_I(s) - HF_I(s-r).$$

(если $s \geq r$). Таким образом, для достаточно больших s имеет место неравенство

$$HP_{I+\langle f \rangle}(s) \geq HP_I(s) - HP_I(s-r). \quad (3)$$

Предположим, что степень полинома HP_I равна d. Легко видеть, что полином, стоящий в правой части неравенства (3), имеет степень $d-1$ (рассуждения проводятся, как в упр. 16 к § 2). Тогда $\deg HP_{I+\langle f \rangle} \geq d-1$ в силу формулы (3) (см., например, п. (c) упр. 8 к § 3). Так как k алгебраически замкнуто, то из теоремы 8 § 3 следует, что $\dim \mathbf{V}(I + \langle f \rangle) \geq \dim \mathbf{V}(I) - 1$. □

Анализ доказательства теоремы 3 позволяет найти условие, гарантирующее выполнение равенства $\dim \mathbf{V}(I + \langle f \rangle) = \dim \mathbf{V}(I) - 1$.

Следствие 4. *Пусть поле k алгебраически замкнуто, а $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. Если f — непостоянный однородный полином, класс которого в факторкольце $k[x_0, \ldots, x_n]/I$ не является делителем нуля, то*

$$\dim \mathbf{V}(I + \langle f \rangle) = \dim \mathbf{V}(I) - 1.$$

Доказательство. Как мы отмечали выше, неравенство (2) является равенством в том и только том случае, когда отображение α_f инъективно. Мы утверждаем, что это так, если $[f] \in k[x_0, \ldots, x_n]/I$ не является делителем нуля. Пусть $[h] \in k[x_0, \ldots, x_n]_s/I_s$ — ненулевой класс, т. е. $h \notin I_s$ и, следовательно, $h \notin I$, так как $I_s = I \cap k[x_0, \ldots, x_n]_s$. Тогда $[h] \in k[x_0, \ldots, x_n]/I$ — ненулевой класс и, следовательно, $[f][h] = [fh] \neq [0]$ в $k[x_0, \ldots, x_n]/I$, так как $[f]$ не является делителем нуля. Значит, $fh \notin I$ и $\alpha_f([h]) = [fh]$ не равен нулю в $k[x_0, \ldots, x_n]_s/I_s$. Это и доказывает инъективность отображения α_f.

Так как (2) превращается в равенство, то

$$\begin{aligned}\dim k[x_0, \ldots, x_n]_s/(I + \langle f \rangle)_s = &\dim k[x_0, \ldots, x_n]_s/I_s \\ &- \dim k[x_0, \ldots, x_n]_{s-r}/I_{s-r}\end{aligned}$$

при $s \geq r$. В терминах полиномов Гильберта это означает, что $HP_{I+\langle f \rangle}(s) = HP_I(s) - HP_I(s - r)$, откуда следует, что $\dim \mathbf{V}(I + \langle f \rangle) = \dim \mathbf{V}(I) - 1$. □

Следует отметить, что теорема 3 может не выполняться для аффинных многообразий, даже если k алгебраически замкнуто. Рассмотрим, например, идеал $I = \langle xz, yz \rangle \subset \mathbb{C}[x, y, z]$. Легко видеть, что $\mathbf{V}(I) = \mathbf{V}(z) \cup \mathbf{V}(x, y) \subset \mathbb{C}^3$, т. е. $\mathbf{V}(I)$ является объединением плоскости (x, y) и оси z. В частности, $\mathbf{V}(I)$ имеет размерность **2** (почему?). Пусть теперь $f = z - 1 \in \mathbb{C}[x, y, z]$. Тогда $\mathbf{V}(f)$ является плоскостью $z = 1$ и, следовательно, $\mathbf{V}(I + \langle f \rangle) = \mathbf{V}(I) \cap \mathbf{V}(f)$ состоит из одной точки $(0, 0, 1)$ (см. упр. 7). В силу упр. 9 из § 3 мы знаем, что размерность точки равна 0, хотя по теореме 3 размерность этого многообразия должна быть не меньше 1.

Эта «неприятность» произошла по той причине, что плоскости $z = 0$ и $z = 1$ параллельны друг другу и, следовательно, не пересекаются в аффинном пространстве. Компонента размерности **1** на бесконечности пропала. Этот пример показывает, почему теория размерности выглядит более удовлетворительной в случае однородных идеалов и проективных многообразий. Существует, однако, аффинный аналог теоремы 3, но мы не будем здесь обсуждать этот вопрос.

Теорема 3 легко обобщается на случай нескольких полиномов.

Предложение 5. *Пусть поле k алгебраически замкнуто, а I — однородный идеал в $k[x_0, \ldots, x_n]$. Если $f_1, \ldots, f_r$ — однородные полиномы в $k[x_0, \ldots, x_n]$, то*

$$\dim \mathbf{V}(I + \langle f_1, \ldots, f_r \rangle) \geq \dim \mathbf{V}(I) - r.$$

Доказательство проводится индукцией по r с помощью теоремы 3. □

В упражнениях будет выведено условие на $f_1, \ldots, f_r$, которое гарантирует выполнение равенства

$$\dim \mathbf{V}(I + \langle f_1, \ldots, f_r \rangle) = \dim \mathbf{V}(I) - r.$$

Теперь мы рассмотрим нульмерные многообразия.

Предложение 6. *Пусть V — непустое аффинное или проективное многообразие. Тогда V является конечным множеством точек в том и только том случае, когда $\dim V = 0$.*

Доказательство. Мы дадим доказательство в аффинном случае. Пусть $>$ — градуированное упорядочение на $k[x_1, \ldots, x_n]$. Если V конечно и $a_j, j = 1, \ldots, m_i$, — множество различных i-х координат точек из V, то

$$f = \prod_{j=1}^{m_i} (x_i - a_i) \in \mathbf{I}(V).$$

Следовательно, $\operatorname{LT}(f) = x_i^{m_i} \in \langle \operatorname{LT}(\mathbf{I}(V)) \rangle$. Из этого вытекает, что $\mathbf{V}(\langle \operatorname{LT}\mathbf{V}(I) \rangle) = \{0\}$ и, значит, $\dim V = 0$ по теореме 8 из § 3.

Пусть теперь $\dim V = 0$. Тогда аффинный полином Гильберта идеала $\mathbf{I}(V)$ является константой C, т. е.

$$\dim k[x_0, \ldots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s} = C$$

для достаточно больших s. Если $s \geq C$, то классы $[1], [x_i], [x_i^2], \ldots, [x_i^s] \in k[x_1, \ldots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s}$ образуют $s + 1$ векторов в векторном пространстве размерности $C \leq s$. Значит, эти векторы линейно зависимы, т. е. существует нетривиальное линейное соотношение

$$[0] = \sum_{j=0}^{s} a_j \left[x_i^j\right] = \left[\sum_{j=0}^{s} a_j x_i^j\right].$$

Это означает, что ненулевой полином $\sum_{j=0}^{s} a_j x_i^j$ лежит в $\mathbf{I}(V)_{\leq s}$. Этот полином обращается в нуль на V; следовательно, множество i-х координат точек из V конечно. Так как это справедливо для всех $i, 1 \leq i \leq n$, то V конечно. □

Если поле k алгебраически замкнуто, то шесть условий теоремы 6 из § 3 гл. 5 эквивалентны условию $\dim V = 0$. В частности, если известен определяющий идеал многообразия V, то мы располагаем простым критерием нульмерности этого многообразия.

Теперь рассмотрим некоторые интересные свойства многообразий положительной размерности.

Предложение 7. *Пусть поле k алгебраически замкнуто.*

(i) *Пусть $V \subset \mathbb{P}^n(k)$ — проективное многообразие размерности > 0. Тогда $V \cap \mathbf{V}(f) \neq \varnothing$ для любого непостоянного однородного полинома $f \in k[x_0, \ldots, x_n]$. Таким образом, многообразие положительной размерности имеет непустое пересечение с любой гиперповерхностью в $\mathbb{P}^n(k)$.*

(ii) *Пусть $W \subset k^n$ — аффинное многообразие размерности > 0. Если $\overline{W}$ — проективное замыкание многообразия W в $\mathbb{P}^n$, то $W \neq \overline{W}$. Таким образом, аффинное многообразие положительной размерности всегда имеет точки на бесконечности.*

Доказательство. (i) Пусть $V = \mathbf{V}(I)$. Так как $\dim V > 0$, то из следствия 4 вытекает, что $\dim V \cup \mathbf{V}(f) \geq \dim V - 1 \geq 0$. Проверим, что тогда $V \cap \mathbf{V}(f) \neq \varnothing$.

Если $V \cap \mathbf{V}(f) = \varnothing$, то из проективной теоремы о нулях следует, что $\langle x_0, \ldots, x_n \rangle^r \subset I + \langle f \rangle$ для некоторого $r \geq 0$. Значит, $HP_{I+\langle f \rangle}$ — нулевой полином (см. упр. 15 к § 3). Но доказательство теоремы 3 показывает, что этот полином не может быть нулевым, если $\dim V > 0$. Детали мы оставляем читателю в качестве упражнения.

(ii) Точки на бесконечности многообразия W — это точки из $\overline{W} \cap \mathbf{V}(x_0)$, где $V(x_0)$ — гиперплоскость на бесконечности. Согласно теореме 12 из § 3, $\dim \overline{W} = \dim W > 0$. Теперь п. (ii) следует из п. (i).

Рассмотрим, далее, размерность объединения двух многообразий.

Предложение 8. *Пусть V и W — многообразия в k^n или в $\mathbb{P}^n(k)$. Тогда*

$$\dim(V \cup W) = \max(\dim V, \dim W).$$

Доказательство. Доказательства в аффинном и в проективном случаях почти одинаковы, поэтому ограничимся аффинным случаем. Если поле k конечно, то V, W и $V \cup W$ конечны и имеют размерность 0 по предложению 6, так что мы будем считать поле k бесконечным.

Пусть $I = \mathbf{I}(V)$ и $J = \mathbf{I}(W)$. Тогда $\dim V = \deg {}^aHP_I$ и $\dim W = \deg {}^aHP_J$. В силу теоремы 15 из § 3 гл. 4 имеет место соотношение $\mathbf{I}(V \cup W) = \mathbf{I}(V) \cap \mathbf{I}(W) = I \cap J$. Удобнее работать с произведением идеалов IJ, и мы отметим, что

$$IJ \subset I \cap J \subset \sqrt{IJ}$$

(см. упр. 15). Имеем

$$\deg {}^aHP_{\sqrt{IJ}} \leq \deg {}^aHP_{I \cap J} \leq \deg {}^aHP_{IJ}$$

(см. упр. 8 к § 3). По предложению 6 из § 3 все неравенства здесь на самом деле являются равенствами. Поэтому $\dim(V \cup W) = \deg {}^aHP_{IJ}$.

Зафиксируем градуированное упорядочение $>$ на $k[x_1, \ldots, x_n]$. По предложениям 3 и 4 из § 3 размерности $\dim V$, $\dim W$ и $\dim(V \cup W)$ равны максимальным размерностям координатных подпространств, содержащихся в $\mathbf{V}(\langle \mathrm{LT}(I) \rangle)$, $\mathbf{V}(\langle \mathrm{LT}(J) \rangle)$ и $\mathbf{V}(\langle \mathrm{LT}(IJ) \rangle)$ соответственно. В упр. 16 будет доказано, что

$$\langle \mathrm{LT}(IJ) \rangle = \langle \mathrm{LT}(I) \rangle \cdot \langle \mathrm{LT}(J) \rangle.$$

Тогда

$$\mathbf{V}(\langle \mathrm{LT}(IJ) \rangle) = \mathbf{V}(\langle \mathrm{LT}(I) \rangle) \cup \mathbf{V}(\langle \mathrm{LT}(J) \rangle).$$

Так как k бесконечно, то каждое координатное подпространство неприводимо (см. упр. 7 к § 1); следовательно, координатное подпространство содержится в $\mathbf{V}(\langle \mathrm{LT}(IJ) \rangle)$ в том и только том случае, когда оно содержится или в $\mathbf{V}(\langle \mathrm{LT}(I) \rangle)$, или в $\mathbf{V}(\langle \mathrm{LT}(J) \rangle)$. Отсюда сразу же следует, что $\dim(V \cup W)$ равна максимуму из $\dim V$ и $\dim W$. □

Приведем полезное следствие этого предложения.

Следствие 9. *Размерность многообразия равна максимуму размерностей его неприводимых компонент.*

Доказательство. Пусть $V = V_1 \cup \ldots \cup V_r$ — разложение многообразия в объединение неприводимых компонент. Тогда индукция по r и предложение 8 дают равенство

$$\dim V = \max(\dim V_1, \ldots, \dim V_r).$$ □

Следствие 9 позволяет нам при вычислении размерности ограничиться случаем неприводимых многообразий. Следующий результат показывает, что в неприводимом случае размерность имеет ряд дополнительных хороших свойств.

Предложение 10. *Пусть поле k алгебраически замкнуто, а $V \subset \mathbb{P}^n(k)$ — неприводимое многообразие.*

(i) *Если $f \in k[x_0, \dots, x_n]$ — однородный полином, не равный нулю на V, то* $\dim(V \cap \mathbf{V}(f)) = \dim V - 1$.

(ii) *Если $W \subset V$ — многообразие и $W \neq V$, то* $\dim W < \dim V$.

Доказательство. (i) Мы знаем, что $\mathbf{I}(V)$ — простой идеал, а $k[V] \cong k[x_0, \dots, x_n]/\mathbf{I}(V)$ — область целостности (предложение 4 из § 1 гл. 5). Так как $f \notin \mathbf{I}(V)$, то класс полинома f в $k[x_0, \dots, x_n]/\mathbf{I}(V)$ не равен нулю. Следовательно, он не является делителем нуля. Осталось применить следствие 4.

(ii) Пусть W — собственное подмногообразие многообразия V. Тогда существует функция $f \in \mathbf{I}(W) - \mathbf{I}(V)$. Таким образом, $W \subset V \cap \mathbf{V}(f)$; следовательно,

$$\dim(W) \leq \dim(V \cap \mathbf{V}(f)) = \dim V - 1 < \dim V$$

в силу п. (i) и предложения 1. □

Пункт (i) предложения 10 утверждает, что если многообразие V неприводимо и f не обращается в нуль на V, то некоторая компонента многообразий $V \cap \mathbf{V}(f)$ имеет размерность $\dim V - 1$. Затратив несколько больше усилий, можно показать, что каждая компонента пересечения $V \cap \mathbf{V}(f)$ имеет размерность $\dim V - 1$. См., например, теорему 3.8 из гл. IV книги KENDIG (1977) или теорему 5 из § 6 гл. 1 книги SHAFAREVICH (1974).

В следующем параграфе мы увидим, как определить размерность *неприводимого* многообразия V в терминах координатного кольца $k[V]$ и поля рациональных функций $k(V)$ (см. гл. 5).

Упражнения к § 4

1. Докажите предложение 1. Указание: используйте упр. 8 к § 3.
2. Пусть поле k алгебраически замкнуто и $f \in k[x_1, \dots, x_n]$ — непостоянный полином. Докажите, что размерность аффинной гиперповерхности $\mathbf{V}(f) \subset k^n$ равна $n - 1$.
3. Приведите примеры аффинных многообразий в $\mathbb{R}^4$, заданных одним уравнением и имеющих размерности 0, 1, 2, 3.
4. В этом упражнении мы рассмотрим отображение
$$\pi : k[x_0, \dots, x_n]_s/I_s \longrightarrow k[x_0, \dots, x_n]_s/(I + \langle f \rangle)_s,$$
определенное формулой $\pi([g]) = [g]$ для всех $g \in k[x_0, \dots, x_n]_s$.
   (a) Докажите, что π определено корректно, т. е. покажите, что образ класса $[g]$ не зависит от выбора представителя g. Мы назовем π отображением *естественной проекции* из $k[x_0, \dots, x_n]_s/I_s$ в $k[x_0, \dots, x_n]_s/(I + \langle f \rangle)_s$.

   (b) Докажите, что π является линейным отображением.
   (c) Докажите, что π сюръективно.
5. Пусть I — однородный идеал, а f — однородный полином степени r. Докажите, что отображение
$$\alpha_f : k[x_0, \dots, x_n]_{s-r}/I_{s-r} \longrightarrow k[x_0, \dots, x_n]_s/I_s,$$
$\alpha_f([h]) = [f \cdot h]$, определено корректно, т. е. докажите, что образ $\alpha_f([h])$ класса $[h]$ не зависит от выбора представителя h. Докажите также, что α_f является линейным отображением.
6. Пусть $f \in k[x_0, \dots, x_n]$ — однородный полином полной степени $r > 0$.
   (a) Найдите формулу для полинома Гильберта идеала $\langle f \rangle$. Эта формула должна содержать только n, r и, конечно, s (в качестве переменных). В частности, все однородные полиномы одинаковой степени в $k[x_0, \dots, x - n]$ определяют один и тот же полином Гильберта. Указание: проанализируйте доказательства теоремы 3 и следствия 4 в случае $I = \{0\}$.
   (b) Пусть теперь $V = \mathbf{V}(I)$ и класс f не является делителем нуля в $k[x_0, \dots, x_n]/I$. Докажите, что полином Гильберта идеала $I + \langle f \rangle$ зависит только от V и от r.

   Меняя f, мы можем рассматривать многообразия $\mathbf{V}(f) \subset \mathbb{P}^n(k)$ как алгебраическое семейство гиперповерхностей. Аналогично, меняя f, мы получаем семейство многообразий $V \cap \mathbf{V}(f)$. Из пп. (a) и (b) следует, что полиномы Гильберта не меняются при изменении f. В общем случае при выполнении технического условия, называемого «плоскостью», полином Гильберта постоянен на любом алгебраическом семействе многообразий.
7. Пусть $I = \langle xz, yz \rangle$. Докажите, что $\mathbf{V}(I + \langle z - 1 \rangle) = \{(0, 0, 1)\}$.
8. Пусть $R = k[x_0, \dots, x_n]$. Конечная последовательность $f_1, \dots, f_r$ однородных полиномов называется *R-последовательностью*, если класс $[f_{j+1}]$ не является делителем нуля в $R/\langle f_1, \dots, f_j \rangle$ ни для какого j, $1 \leq j < r$.
   (a) Докажите, что $x_0, \dots, x_r$, где $r \leq n$, является R-последовательностью.
   (b) Пусть поле k алгебраически замкнуто и $f_1, \dots, f_r$ есть R-последовательность. Докажите, что
$$\dim \mathbf{V}(f_1, \dots, f_r) = n - r.$$
   Указание: используйте следствие 4 и индукцию по r, работая с идеалами $I_j = \langle f_1, \dots, f_j \rangle$, $1 \leq j \leq r$.
9. Пусть $R = k[x_0, \dots, x_n]$. Однородный идеал I называется *полным пересечением*, если он порожден R-последовательностью. Проективное многообразие V называется *полным пересечением*, если $\mathbf{I}(V)$ является полным пересечением.
   (a) Докажите, что каждое неприводимое линейное подпространство в $\mathbb{P}^n(k)$ является полным пересечением.

(b) Докажите, что все проективные и аффинные гиперповерхности являются полными пересечениями.

(c) Докажите, что проективное замыкание объединения плоскостей (x, y) и (z, w) в k^4 не является полным пересечением.

(d) Пусть V — аффинная скрученная кубика $\mathbf{V}(y - x^2, z - x^3) \subset \boldsymbol{k^3}$. Является ли полным пересечением проективное замыкание кривой V?

Указание: пп. (c) и (d) требуют использования техники упр. 17 к § 3.

10. Рассмотрим идеал $I \subset k[x_1, \ldots, x_n]$. В этом упражнении мы докажем, что аффинный полином Гильберта является константой в том и только том случае, когда факторкольцо $k[x_1, \ldots, x_n]/I$ конечномерно как векторное пространство над k. Более того, в этом случае указанная константа равна размерности этого факторкольца как векторного пространства над k.

(a) Пусть $\alpha_s : k[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} \longrightarrow k[x_1, \ldots, x_n]/I$ — отображение, заданное формулой $\alpha_s([f]) = [f]$. Докажите, что α_s определено корректно и является инъективным.

(b) Пусть пространство $k[x_1, \ldots, x_n]/I$ конечномерно. Докажите, что α_s является изоморфизмом при достаточно большом s. Выведите отсюда, что полином Гильберта является константой, равной размерности указанного пространства. Указание: пусть $[f_1], \ldots, [f_m]$ — базис в $k[x_1, \ldots, x_n]/I$. Рассмотрите случай, когда s больше, чем полные степени полиномов $f_1, \ldots, f_m$.

(c) Пусть теперь полином Гильберта является константой. Докажите, что если $s \leq t$, то образ отображения α_s содержится в образе отображения α_t. Докажите, что если s и t достаточно велики, то образы отображений α_s и α_t совпадают. Докажите, далее, что α_s является изоморфизмом при достаточно большом s и что пространство $k[x_1, \ldots, x_n]/I$ конечномерно.

11. Пусть $V \subset k^n$ — конечное множество точек. В этом упражнении мы докажем, что пространство $k[x_1, \ldots, x_n]/\mathbf{I}(V)$ конечномерно и его размерность равна $|V|$, числу точек в V. Тогда из предыдущего упражнения следует, что аффинный полином Гильберта идеала $\mathbf{I}(V)$ является константой $|V|$. Пусть $V = \{p_1, \ldots, p_m\}$, где $m = |V|$.

(a) Определим отображение $\phi : k[x_1, \ldots, x_n]/\mathbf{I}(V) \to k^m$ формулой $\phi([f]) = (f(p_1), \ldots, f(p_m))$. Докажите, что ϕ является корректно определенным линейным инъективным отображением.

(b) Зафиксируем i, и пусть $W_i = \{p_j : j \neq i\}$. Докажите, что $\mathbf{I}(W_i) + \mathbf{I}(\{p_i\}) = 1$. Указание: докажите, что $\mathbf{I}(\{p_i\})$ — максимальный идеал.

(c) Из п. (b) следует, что существуют полиномы $f_i \in \mathbf{I}(W_i)$ и $g_i \in \mathbf{I}(\{p_i\})$, такие, что $f_i + g_i = 1$. Докажите, что $\phi([f_i])$ — это вектор e_i из k^m с 1 на i-м месте и нулем на остальных.

(d) Докажите, что ϕ является изоморфизмом и $\dim k[x_1, \ldots, x_n]/\mathbf{I}(V) = |V|$.

12. Пусть $I \subset k[x_0, \ldots, x_n]$ — однородный идеал. В этом упражнении мы рассмотрим геометрический смысл коэффициента b_0 полинома Гильберта

$$HP_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i}.$$

Коэффициент b_0 называется *степенью* идеала I. *Степень* проективного многообразия мы определим как степень идеала $\mathbf{I}(V)$. Мы увидим, что степень является в некотором смысле обобщением понятия полной степени полинома, задающего гиперповерхность. В этих терминах в упр. 10 и 11 вычисляется степень идеалов и многообразий с постоянным полиномом Гильберта.

(a) Докажите, что степень идеала $\langle f \rangle$ равна полной степени полинома f. Пусть k алгебраически замкнуто. Докажите, что степень гиперповерхности $\mathbf{V}(f)$ равна степени редуцированного полинома f_{red} (см. § 2 гл. 4). Указание: используйте упр. 6.

(b) Пусть I является полным пересечением (упр. 9), заданным R-последовательностью $f_1, \ldots, f_r$. Тогда степень идеала I равна

$$\deg f_1 \cdot \deg f_2 \ldots \deg f_r.$$

Указание: проанализируйте и используйте доказательство теоремы 3. Также используйте указание к упр. 8.

(c) Найдите степень проективного замыкания стандартной скрученной кубики.

13. Докажите утверждение из предложения 7 о том, что $HP_{I+\langle f \rangle}$ не может быть нулевым полиномом, если $\dim V > 0$. Указание: используйте неравенство (3).

14. В этом упражнении мы проанализируем условие предложения 7.

(a) Пусть $V = \mathbf{V}(x) \subset k^2$. Докажите, что $V \cap \mathbf{V}(x - 1) = \varnothing$, и объясните, почему этот результат не противоречит п. (i) предложения 7.

(b) Пусть $W = \mathbf{V}(x^2 + y^2 - 1) \subset \mathbb{R}^2$. Докажите, что $W = \overline{W}$ в $\mathbb{P}^2(\mathbb{R})$, и объясните, почему этот результат не противоречит п. (ii) предложения 7.

15. Рассмотрим идеалы $I, J \subset k[x_1, \ldots, x_n]$. Докажите, что $IJ \subset I \cap J \subset \sqrt{IJ}$.

16. Пусть I и J — произвольные идеалы и $>$ — некоторое мономиальное упорядочение. Тогда

$$\langle \text{LT}(I) \rangle \cdot \langle \text{LT}(J) \rangle = \langle \text{LT}(I \cdot J) \rangle.$$

17. Используя предложение 10, мы можем дать другое определение размерности неприводимого многообразия. Поле k мы будем считать алгебраически замкнутым. Пусть многообразие $V \subset \mathbb{P}^n(k)$ неприводимо.

(a) Пусть $\dim V > 0$. Докажите, что существует неприводимое многообразие $W \subset V$, такое, что $\dim W = \dim V - 1$. Указание: используйте предложение 10 и рассмотрите неприводимые компоненты для $V \cap \mathbf{V}(f)$.

(b) Пусть $\dim V = m$. Докажите, что существует цепь из $m+1$ неприводимых многообразий

$$V_0 \subset V_1 \subset \ldots \subset V_m = V,$$

причем $V_i \neq V_{i+1}$ при $0 \leq i < m$.

(c) Докажите, что не существует такой цепи длины $> m+1$. Выведите отсюда, что размерность неприводимого многообразия на единицу меньше максимальной длины строго возрастающей цепи неприводимых многообразий, содержащихся в нем.

18. Докажите аффинную версию п. (ii) предложения 10.

§ 5. Размерность и алгебраическая независимость

В § 3 мы определили размерность аффинного многообразия как степень аффинного полинома Гильберта. Это позволило исследовать в § 4 свойства размерности. Однако полиномы Гильберта не исчерпывают всех возможностей. В алгебраической геометрии есть и другие способы определить понятие размерности. В этом и в следующем параграфах мы изучим два наиболее интересных.

Рассмотрим аффинное многообразие $V \subset k^n$. Напомним, что *координатное кольцо* $k[V]$ (см. гл. 5) состоит из всех полиномиальных функций на V. Существует естественный изоморфизм $k[V] \cong k[x_1, \ldots, x_n]/\mathbf{I}(V)$, тождественный на k (теорема 7 из § 1 гл. 5). Изучим связь координатного кольца $k[V]$ с размерностью многообразия V. Отметим сначала, что при $s \geq 0$ корректно определено линейное инъективное отображение

$$k[x_1, \ldots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s} \longrightarrow k[x_1, \ldots, x_n]/\mathbf{I}(V) \cong k[V] \qquad (1)$$

(упр. 10 к § 4). Таким образом, мы можем рассматривать пространство $k[x_1, \ldots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s}$ как конечномерную «часть» в $k[V]$, аппроксимирующую $k[V]$ все точнее и точнее с ростом s. Так как степень полинома ${}^aHP_{\mathbf{I}(V)}$ измеряет скорость роста размерности этих конечномерных аппроксимаций, мы видим, что $\dim V$ является некоторой характеристикой «размера» $k[V]$.

Это рассуждение подсказывает, что можно определить размерность многообразия V непосредственно в терминах координатного кольца $k[V]$. Чтобы сделать это, дадим сначала определение алгебраически независимых элементов.

Определение 1. Элементы $\phi_1, \ldots, \phi_r \in k[V]$ называются *алгебраически независимыми над* k, если не существует ненулевого полинома p от r переменных с коэффициентами из k, такого, что $p(\phi_1, \ldots, \phi_r) = 0$ в $k[V]$.

Обратите внимание, что если $\phi_1, \ldots, \phi_r \in k[V]$ алгебраически независимы над k, то все эти функции отличны от нуля и среди них нет двух одинаковых. Также очевидно, что алгебраически независимо любое подмножество множества $\{\phi_1, \ldots, \phi_r\}$ (см. подробнее упр. 1).

Рассмотрим простой пример. Пусть $V = k^n$. Если поле k бесконечно, то $\mathbf{I}(V) = \{0\}$ и, следовательно, $k[V] = k[x_1, \ldots, x_n]$. Тогда элементы $x_1, \ldots, x_n$ алгебраически независимы над k, потому что равенство $p(x_1, \ldots, x_n) = 0$ означает, что p — нулевой полином.

В качестве другого примера рассмотрим скрученную кубику в $\mathbb{R}^3$. Здесь $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$. Докажем, что $[x] \in \mathbb{R}[V]$ алгебраически независим над $\mathbb{R}$. Пусть p — полином с вещественными коэффициентами, такой, что $p([x]) = [0]$ в $\mathbb{R}[V]$. Это означает, что $[p(x)] = [0]$. Поэтому $p(x) \in \mathbf{I}(V)$. Однако нетрудно показать, что $\mathbb{R}[x] \cap \langle y - x^2, z - x^3 \rangle = \{0\}$, т. е. p — нулевой полином. С другой стороны, легко видеть, что $[x], [y] \in \mathbb{R}[V]$ не являются алгебраически независимыми элементами, так как $[y] - [x]^2 = [0]$ в $\mathbb{R}[V]$.

Теперь мы свяжем размерность многообразия V с числом алгебраически независимых элементов в координатном кольце $k[V]$.

Теорема 2. *Пусть $V \subset k^n$ — аффинное многообразие. Тогда его размерность равна максимальному числу алгебраически независимых над k элементов координатного кольца $k[V]$.*

Доказательство. Докажем сначала, что если $d = \dim V$, то мы можем найти d алгебраически независимых над k элементов кольца $k[V]$. Пусть $I = \mathbf{I}(V)$. Рассмотрим идеал старших членов $\langle \mathrm{LT}(I) \rangle$ для некоторого градуированного упорядочения на $k[x_1, \ldots, x_n]$. Мы знаем (теорема 8 из § 3), что d равно максимальной размерности координатного подпространства, принадлежащего $\mathbf{V}(\langle \mathrm{LT}(I) \rangle)$. Координатное подпространство $W \subset \mathbf{V}(\langle \mathrm{LT}(I) \rangle)$ размерности d задается так: $W = \mathbf{V}(x_j : j \notin \{i_1, \ldots, i_d\})$ для некоторых $1 \leq i_1 < \ldots < i_d \leq n$, т. е. W — это множество точек, j-е координаты которых для $j \notin \{i_1, \ldots, i_d\}$ равны нулю. Докажем, что $[x_{i_1}], \ldots, [x_{i_d}] \in k[V]$ алгебраически независимы над k.

Пусть точка $p \in W \subset \mathbf{V}(\langle \mathrm{LT}(I) \rangle)$ такова, что ее i_j-е координаты равны 1 для $1 \leq j \leq d$, а остальные равны нулю. Тогда любой моном из $\langle \mathrm{LT}(I) \rangle$ равен нулю в p; следовательно, моном из $\langle \mathrm{LT}(I) \rangle$ должен содержать хотя бы одну переменную x_i, где $i \notin \{i_1, \ldots, i_d\}$

(см. доказательство предложения 2 из § 2). Так как $\langle \mathrm{LT}(I)\rangle$ — мономиальный идеал, то $\langle \mathrm{LT}(I)\rangle \cap k[x_{i_1},\dots,x_{i_d}] = \{0\}$. Таким образом,

$$I \cap k[x_{i_1},\dots,x_{i_d}] = \{0\}, \tag{2}$$

потому что ненулевой элемент $f \in I \cap k[x_{i_1},\dots,x_{i_d}]$ дает ненулевой элемент $\mathrm{LT}(f) \in \langle \mathrm{LT}(I)\rangle \cap k[x_{i_1},\dots,x_{i_d}]$.

Теперь мы можем доказать, что $[x_{i_1}],\dots,[x_{i_d}]$ алгебраически независимы над k. Пусть p — полином с коэффициентами из k, такой, что $p([x_{i_1}],\dots,[x_{i_d}]) = [0]$. Тогда $[p(x_{i_1},\dots,x_{i_d})] = [0]$ в $k[V]$, т. е. $p(x_{i_1},\dots,x_{i_d}) \in I$. Из (2) следует, что $p(x_{i_1},\dots,x_{i_d}) = 0$, а так как $x_{i_1},\dots,x_{i_d}$ — это переменные, то p — нулевой полином. Но $d = \dim V$; значит, мы нашли требуемое количество алгебраически независимых над k элементов координатного кольца $k[V]$.

Теперь нужно доказать, что если r элементов координатного кольца $k[V]$ алгебраически независимы, то $r \le \dim V$. Пусть $[f_1],\dots,[f_r] \in k[V]$ алгебраически независимы. Обозначим через N максимальную из полных степеней полиномов f_i и введем новые переменные $y_1,\dots,y_r$. Пусть $p \in k[y_1,\dots,y_r]$ — полином полной степени $\le s$. Тогда $p(f_1,\dots,f_r) \in k[x_1,\dots,x_n]$ — полином полной степени $\le sN$ (см. упр. 2). Рассмотрим отображение

$$\alpha : k[y_1,\dots,y_r]_{\le s} \longrightarrow k[x_1,\dots,x_n]_{\le sN}/I_{\le sN}, \tag{3}$$

которое переводит $p \in k[y_1,\dots,y_r]_{\le s}$ в класс $[p(f_1,\dots,f_r)] \in k[x_1,\dots,x_n]_{\le sN}/I_{\le sN}$. Мы оставляем в качестве упражнения доказательство того, что α определено корректно и является линейным отображением.

Мы утверждаем, что α инъективно. Пусть $p \in k[y_1,\dots,y_r]_{\le s}$ и $[p(f_1,\dots,f_r)] = [0]$ в $k[x_1,\dots,x_n]_{\le sN}/I_{\le sN}$. Тогда из (1) следует, что

$$[p(f_1,\dots,f_r)] = p([f_1],\dots,[f_r]) = [0] \text{ в } k[x_1,\dots,x_n]/I \cong k[V].$$

Так как $[f_1],\dots,[f_r]$ алгебраически независимы, то p — нулевой полином; следовательно, α инъективно.

Сравним размерности в правой и левой частях формулы (3). Имеем

$$^aHF_I(sN) = \dim k[x_1,\dots,x_n]_{\le sN}/I_{\le sN} \ge \dim k[y_1,\dots,y_r]_{\le s}. \tag{4}$$

Так как $y_1,\dots,y_r$ — переменные, то $\dim k[y_1,\dots,y_r]_{\le s}$ равна $\binom{r+s}{s}$ — это полином от s степени r. Следовательно,

$$^aHP_I(sN) \ge \binom{r+s}{s} = \text{ полином степени } r \text{ от } s$$

при достаточно большом s. Поэтому степень полинома $^aHP_I(sN)$, а следовательно, и полинома $^aHP_I(s)$ не меньше r. Таким образом, $r \le \dim V$. Теорема доказана. □

Следствием этой теоремы является тот факт, что размерности изоморфных многообразий совпадают.

Следствие 3. *Пусть V и V' — изоморфные аффинные многообразия (см. определение в § 4 гл. 5). Тогда* $\dim V = \dim V'$. □

Доказательство. Согласно теореме 9 из § 4 гл. 5, мы знаем, что V и V' изоморфны в том и только том случае, когда существует изоморфизм колец $\alpha : k[V] \to k[V']$, тождественный на константах. Следовательно, элементы $\phi_1,\dots,\phi_r \in k[V]$ алгебраически независимы в том и только том случае, когда алгебраически независимы элементы $\alpha(\phi_1),\dots,\alpha(\phi_r) \in k[V']$. Теперь утверждение следует из теоремы 2. □

В доказательстве теоремы 2 $d = \dim V$ алгебраически независимых элементов в $k[V]$ мы нашли в множестве координатных функций. Используя это, дадим другое определение размерности.

Следствие 4. *Пусть $V \subset k^n$ — аффинное многообразие. Его размерность равна наибольшему числу r, для которого существует r переменных $x_{i_1},\dots,x_{i_r}$, таких, что $\mathbf{I}(V) \cap k[x_{i_1},\dots,x_{i_r}] = \{0\}$ (т. е. полином от этих переменных может принадлежать $\mathbf{I}(V)$ только в том случае, когда он равен нулю).*

Доказательство. Из (2) следует, что мы можем найти $d = \dim V$ таких переменных. Предположим, что существует $d+1$ переменных $x_{j_1},\dots,x_{j_{d+1}}$, таких, что $\mathbf{I}(V) \cap k[x_{j_1},\dots,x_{j_{d+1}}] = \{0\}$. Тогда из доказательства теоремы 2 следует, что элементы $[x_{j_1}],\dots,[x_{j_{d+1}}] \in k[V]$ алгебраически независимы над k. Но по теореме 2 это невозможно. □

В упражнениях мы докажем, что для алгебраически замкнутого поля k следствие 4 остается справедливым, если мы заменим $\mathbf{I}(V)$ *любым* идеалом I, определяющим V. Так как мы умеем находить пересечение $I \cap k[x_{i_1},\dots,x_{i_r}]$, используя теорию исключения, то следствие 4 дает нам другой метод (хотя и не очень эффективный) вычисления размерности многообразия.

Следствие 4 можно интерпретировать в терминах проекций. Выберем r переменных $x_{i_1},\dots,x_{i_r}$. Тогда определено отображение проекции $\pi : k^n \to k^r$, $\pi(a_1,\dots,a_n) = (a_{i_1},\dots,a_{i_r})$. Пусть $\widetilde{I} = \mathbf{I}(V) \cap k[x_{i_1},\dots,x_{i_r}]$ — соответствующий исключающий идеал. Если k алгебраически замкнуто, то теорема о замыкании из § 2 гл. 3 гарантирует, что $\mathbf{V}(\widetilde{I})$ является наименьшим многообразием, содержащим $\pi(V)$. Следовательно,

$$\widetilde{I} = \{0\} \Longleftrightarrow \mathbf{V}(\widetilde{I}) = k^r$$

$$\Longleftrightarrow \text{ наименьшее многообразие, содержащее } \pi(V), \text{ есть } k^r.$$

Подмножество в k^r называется *плотным по Зарисскому*, если наименьшее многообразие, содержащее его, совпадает со всем k^r. Таким образом, следствие 4 утверждает, что размерность многообразия V равна максимальной размерности такого координатного подпространства, что проекция многообразия V плотна по Зарисскому в этом подпространстве.

Мы можем рассматривать отображение π как линейное отображение пространства k^n в себя, которое не меняет координаты i_j при $1 \le j \le r$, а остальные координаты заменяет нулями. Легко показать, что $\pi \circ \pi = \pi$ и что $k^r \subset k^n$ является образом отображения π (см. упр. 8). Есть общее определение: линейное отображение $\pi : k^n \to k^n$ называется *отображением проекции*, если $\pi \circ \pi = \pi$. Если его ранг равен r, то его образом является r-мерное подпространство $H \subset k^n$. В этом случае мы говорим, что π является *отображением проекции на* H.

Пусть теперь π — отображение проекции на $H \subset k^n$. По любому многообразию $V \subset k^n$ можно построить подмножество $\pi(V) \subset H$. Теперь мы можем интерпретировать размерность многообразия V в терминах проекций $\pi(V)$.

Предложение 5. *Пусть поле k алгебраически замкнуто, а $V \subset k^n$ — аффинное многообразие. Его размерность равна максимальной размерности подпространства $H \subset k^n$, такого, что проекция $\pi(V)$ многообразия V на H плотна по Зарисскому в H.*

Доказательство. Если V имеет размерность d, то по предыдущему мы можем найти проекцию π на d-мерное координатное подпространство, такую, что $\pi(V)$ плотно в этом пространстве по Зарисскому.

Пусть теперь $\pi : k^n \to k^n$ — отображение проекции на r-мерное подпространство $H \subset k^n$, причем $\pi(V)$ плотно по Зарисскому в H. Нам нужно доказать, что $r \le \dim V$. Найдем такой базис в k^n, что в новых координатах $\pi(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$ (см. например, разд. 3.4 книги FINKBEINER (1978)). Так как замена координат не меняет размерности многообразия (это следует из аффинной версии предложения 11 из § 4), то этот случай аналогичен случаю проекции на координатное подпространство. □

Пусть π — отображение проекции k^n на r-мерное подпространство H. По теореме замыкания из § 2 гл. 3, если $\pi(V)$ плотно по Зарисскому в H, то существует собственное многообразие $W \subset H$, такое, что $H - W \subset \pi(V)$. Значит, $\pi(V)$ «заполняет» большую часть r-мерного подпространства H, и, следовательно, разумно ожидать, что V по крайней мере r-мерно. Таким образом, предложение 5 дает нам геометрическую интерпретацию размерности многообразия.

До конца параграфа мы будем считать V *неприводимым* многообразием. Тогда (предложение 4 из § 1 гл. 5) идеал $\mathbf{I}(V)$ прост и $k[V]$ является областью целостности. Как и в § 5 гл. 5, мы построим поле частных $k(V)$ кольца $k[V]$, которое является *полем рациональных функций* на V. Алгебраическая независимость элементов из $k(V)$ определяется так же, как алгебраическая независимость элементов из $k[V]$ (см. определение 1). Найдем связь между размерностью многообразия V и полем $k(V)$.

Теорема 6. *Пусть $V \subset k^n$ — неприводимое аффинное многообразие. Его размерность равна максимальному числу алгебраически независимых над k элементов поля $k(V)$.*

Доказательство. Пусть $d = \dim V$. Так как $k[V] \subset k(V)$, то d алгебраически независимых элементов кольца $k[V]$ будут алгебраически независимы и как элементы поля $k(V)$, так что осталось показать, что если элементы $\phi_1, \ldots, \phi_r \in k(V)$ алгебраически независимы, то $r \le \dim V$. Каждый элемент ϕ_i является частным элементов из $k[V]$. Если f — наименьшее общее кратное всех знаменателей, то $\phi_i = [f_i]/[f]$, $1 \le i \le r$. Отметим, что $[f] \ne [0]$ в $k[V]$. Теперь мы модифицируем доказательство теоремы 2 с целью учесть знаменатель $[f]$.

Обозначим через N максимум полных степеней полиномов $f, f_1, \ldots, f_r$ и введем новые переменные $y_1, \ldots, y_r$. Пусть $p \in k[y_1, \ldots, y_r]$ — полином полной степени $\le s$. Несложно доказать (проделайте это самостоятельно), что

$$f^s p(f_1/f, \ldots, f_r/f)$$

является полиномом в $k[x_1, \ldots, x_n]$ полной степени $\le sN$ (см. упр. 10). Рассмотрим отображение

$$\beta : k[y_1, \ldots, y_r]_{\le s} \longrightarrow k[x_1, \ldots, x_n]_{\le sN}/I_{\le sN}, \tag{5}$$

переводящее полином $p \in k[y_1, \ldots, y_r]_{\le s}$ в класс $[f^s p(f_1/f, \ldots, f_r/f)] \in k[x_1, \ldots, x_n]_{\le sN}/I_{\le sN}$. Отображение β является корректно определенным линейным отображением (докажите это самостоятельно).

Докажем его инъективность. Пусть $p \in k[y_1, \ldots, y_r]_{\le s}$ — такой полином, что $[f^s p(f_1/f, \ldots, f_r/f)] = [0]$ в $k[x_1, \ldots, x_n]_{\le sN}/I_{\le sN}$. Используя (1), получаем, что

$$[f^s p(f_1/f, \ldots, f_r/f)] = [0] \text{ в } k[x_1, \ldots, x_n]/I \cong k[V].$$

Но мы работаем в $k(V)$. Поэтому перепишем это равенство в следующем виде:

$$[f]^s p([f_1]/[f], \ldots, [f_r]/[f]) = [f]^s p(\phi_1, \ldots, \phi_r) = [0] \text{ в } k(V).$$

Так как $k(V)$ — поле, а $[f] \neq [0]$, то $p(\phi_1, \ldots, \phi_r) = [0]$. Отсюда следует, что p — нулевой полином, потому что элементы $\phi_1, \ldots, \phi_r$ алгебраически независимы. Значит, β инъективно.

Теперь из неравенства (5) следует неравенство (4), а рассуждения, аналогичные рассуждениям в доказательстве теоремы 2, показывают, что $\dim V \geq r$. Теорема доказана. □

Следствием этой теоремы является тот факт, что бирационально эквивалентные многообразия имеют одинаковую размерность.

Следствие 7. *Пусть V и V' — бирационально эквивалентные (§ 5 гл. 5) неприводимые аффинные многообразия. Тогда* $\dim V = \dim V'$.

Доказательство. В теореме 10 из § 5 гл. 5 было доказано, что аффинные многообразия V и V' бирационально эквивалентны в том и только том случае, когда изоморфны их поля функций $k(V)$ и $k(V')$. Далее рассуждения проводятся, как в следствии 3. □

Понятие *степени трансцендентности* в теории полей тесно связано с понятием размерности. В общем случае мы рассматриваем поле K, которое содержит поле k.

Определение 8. Пусть поле K является расширением поля k. Мы говорим, что K имеет *степень трансцендентности d над k*, если K содержит d элементов, алгебраически независимых над k, и не содержит большего числа таких алгебраически независимых элементов.

Объединяя это определение с теоремой 6, мы получаем, что для любого неприводимого аффинного многообразия V

$$\dim V = \text{степень трансцендентности поля } k(V) \text{ над } k.$$

Во многих книгах по алгебраической геометрии именно так и определяется размерность неприводимого многообразия, а далее размерность произвольного многообразия определяется как максимум размерностей его неприводимых компонент.

В качестве примера рассмотрим многообразие $V = k^n$, где поле k предполагается бесконечным. Тогда $k(V) = k(x_1, \ldots, x_n)$. Так как $\dim V = n$, то поле $k(x_1, \ldots, x_n)$ имеет степень трансцендентности n над k. Здесь очевидно, что степень трансцендентности не меньше n, но то, что любые $n+1$ элементов из $k(x_1, \ldots, x_n)$ алгебраически зависимы, уже не столь очевидно. Таким образом, изучение размерности помогает понять структуру полей.

Чтобы лучше разобраться в понятии степени трансцендентности, нужны более глубокие познания в теории алгебраических и трансцендентных расширений полей (см. например гл. 7 и 10 книги LANG (1965)).

Упражнения к § 5

1. Пусть $\phi_1, \ldots, \phi_r \in k[V]$ алгебраически независимы над k.
   (a) Докажите, что ϕ_i различны и не равны нулю.
   (b) Докажите, что любое непустое подмножество множества $\{\phi_1, \ldots, \phi_r\}$ состоит из алгебраически независимых элементов.
   (c) Введем переменные $y_1, \ldots, y_r$ и рассмотрим отображение $\alpha : k[y_1, \ldots, y_r] \to k[V]$, определенное формулой $\alpha(p) = p(\phi_1, \ldots, \phi_r)$. Докажите, что α является инъективным гомоморфизмом колец.
2. В этом упражнении мы рассмотрим доказательство теоремы 2.
   (a) Пусть полные степени полиномов $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ не превосходят N и полная степень полинома $p \in k[y_1, \ldots, y_r]$ не превосходит s. Докажите, что полная степень полинома $p(f_1, \ldots, f_r)$ не превосходит sN.
   (b) Докажите, что отображение α из доказательства теоремы 2 определено корректно и является линейным.
3. Завершите доказательство следствия 3.
4. Пусть поле k алгебраически замкнуто, а $I \subset k[x_1, \ldots, x_n]$ — некоторый идеал. Докажите, что размерность многообразия $\mathbf{V}(I)$ равна наибольшему целому r, для которого существует r переменных $x_{i_1}, \ldots, x_{i_r}$, таких, что $I \cap k[x_{i_1}, \ldots, x_{i_r}] = \{0\}$. Указание: используйте I вместо $\mathbf{I}(V)$ в доказательстве теоремы 2; продумайте, почему $\dim V = \deg {}^aHP_I$.
5. Пусть $I = \langle xy - 1 \rangle \subset k[x, y]$. Что представляют собой проекции многообразия $\mathbf{V}(I)$ на ось x и на ось y? Обратите внимание, что обе проекции плотны, но не совпадают со всей осью.
6. Пусть поле k алгебраически замкнуто и $I = \langle xy, xz \rangle \subset k[x, y, z]$.
   (a) Докажите, что $I \cap k[x] = \{0\}$, но $I \cap k[x, y]$ и $I \cap k[x, z]$ не равны нулю.
   (b) Докажите, что $I \cap k[y, z] = \{0\}$, но $I \cap k[x, y, z] \neq \{0\}$.
   (c) Что можно сказать о размерности многообразия $\mathbf{V}(I)$?
7. Рассмотрим пример, аналогичный примеру из упр. 6, но более сложный. Поле k предполагается алгебраически замкнутым, а $I = \langle zx - x^2, zy - xy \rangle \subset k[x, y, z]$.
   (a) Докажите, что $I \cap k[z] = \{0\}$. Верно ли, что $I \cap k[x, z] = \{0\}$ или $I \cap k[y, z] = \{0\}$?
   (b) Докажите, что $I \cap k[x, y] = \{0\}$, но $I \cap k[x, y, z] \neq \{0\}$.
   (c) Чему равна размерность многообразия $\mathbf{V}(I)$?
8. Пусть $1 \leq i_1 < \ldots < i_r \leq n$. Рассмотрим линейное отображение $\pi : k^n \to k^n$, переводящее вектор $(a_1, \ldots, a_n)$ в вектор, i_j-е координаты которого равны a_{i_j} для $1 \leq j \leq r$, а остальные равны 0. Докажите, что $\pi \circ \pi = \pi$, и найдите образ π.
9. В этом упражнении мы покажем, что отображение проекции на данное подпространство $H \subset k^n$ определено неоднозначно.

(a) Докажите, что матрицы

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

определяют отображения проекции пространства $\mathbb{R}^2$ на ось x. Покажите на рисунке, как действуют эти отображения на точки из $\mathbb{R}^2$.

(b) Докажите, что существует взаимно однозначное соответствие между отображениями проекции пространства $\mathbb{R}^2$ на ось x и негоризонтальными прямыми, проходящими через начало координат.

(c) Зафиксируем r-мерное подпространство $H \subset k^n$. Докажите, что существует взаимно однозначное соответствие между отображениями проекции пространства k^n на H и $(n-r)$-мерными подпространствами $H' \subset k^n$, такими, что $H \cap H' = \{0\}$. Указание: рассмотрите ядро проекции.

10. В этом упражнении мы рассмотрим доказательство теоремы 6.

(a) Пусть полные степени полиномов $f, f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ не превышают N, а полная степень полинома $p \in k[y_1, \ldots, y_r]$ не превышает s. Докажите, что $f^s p(f_1/f, \ldots, f_r/f)$ является полиномом из $k[x_1, \ldots, x_n]$.

(b) Докажите, что степень этого полинома $\leq sN$.

(c) Докажите, что отображение β из доказательства теоремы 6 определено корректно и является линейным.

11. Завершите доказательство следствия 7.

12. Пусть $\phi : V \to W$ — полиномиальное отображение аффинного многообразия V в аффинное многообразие W (см. § 1 гл. 5). В § 4 гл. 5 было доказано, что ϕ индуцирует гомоморфизм колец $\phi^* : k[W] \to k[V]$, тождественный на константах. Рассмотрим образ $\phi(V) \subset W$. Отображение ϕ называется *доминирующим*, если наименьшее многообразие в W, содержащее $\phi(V)$, — это W. Другими словами, ϕ — доминирующее отображение, если его образ плотен по Зарисскому в W.

(a) Докажите, что ϕ доминирующее в том и только том случае, когда гомоморфизм $\phi^* : k[W] \to k[V]$ инъективен. Указание: докажите, что $W' \subset W$ является собственным подмногообразием в том и только том случае, когда существует ненулевой элемент $[f] \in k[W]$, такой, что $W' \subset W \cap \mathbf{V}(f)$.

(b) Пусть ϕ — доминирующее отображение. Тогда $\dim V \geq \dim W$. Указание: примените теорему 2 и п. (a).

13. В этом упражнении мы рассмотрим связь между параметризацией и размерностью. Поле k предполагается бесконечным.

(a) Пусть $F : k^m \to V$ — полиномиальная параметризация многообразия V (см. § 3 гл. 3). Таким образом, m — это число параметров, а V — наименьшее многообразие, содержащее $F(k^m)$. Докажите, что $\dim V \leq m$.

(b) Приведите пример полиномиальной параметризации, где $\dim V < m$.

(c) Пусть $F : k^m - W \to V$ — рациональная параметризация многообразия V (см. § 3 гл. 3). Тогда V неприводимо (предложение 6 из § 5 гл. 4). Докажите, что можно определить инъективный гомоморфизм полей $F^* : k(V) \to k(t_1, \ldots, t_m)$. Указание: см. доказательство теоремы 10 из § 5 гл. 5.

(d) Пусть $F : k^m - W \to V$ — рациональная параметризация. Докажите, что $\dim V \leq m$.

14. В этом упражнении мы покажем, как определить поле рациональных функций на неприводимом проективном многообразии $V \subset \mathbb{P}^n(k)$. Однородный полином $f \in k[x_0, \ldots, x_n]$ *не* задает функцию на V. В самом деле, пусть точка $p \in V$ имеет однородные координаты $(a_0, \ldots, a_n)$. Тогда $(\lambda a_0, \ldots, \lambda a_n)$ — также координаты точки p и

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n),$$

где d — полная степень полинома f.

(a) Объясните, почему нельзя рассматривать полином f как однозначную функцию на V.

(b) Пусть степень однородного полинома $g \in k[x_0, \ldots, x_n]$ также равна d и $g \notin \mathbf{I}(V)$. Докажите, что $\phi = f/g$ является корректно определенной функцией на непустом подмножестве $V - (V \cap \mathbf{V}(g)) \subset V$.

(c) Функции $\phi = f/g$ и $\phi' = f'/g'$ называются эквивалентными на V, $\phi \sim \phi'$, если существует собственное подмногообразие $W \subset V$, такое, что $\phi = \phi'$ на $V - W$. Докажите, что $\sim$ является отношением эквивалентности. Соответствующие классы эквивалентности называются *рациональными функциями* на V. Множество классов эквивалентности обозначается через $k(V)$. Указание: неприводимость многообразия V очень существенна.

(d) Докажите, что сложение и умножение классов эквивалентности определены корректно и задают на $k(V)$ структуру поля. Оно называется *полем рациональных функций* на проективном многообразии V.

(e) Пусть U_i — аффинная часть пространства $\mathbb{P}^n(k)$, где $x_i \neq 0$. Рассмотрим неприводимое аффинное многообразие $V \cap U_i \subset U_i \cong k^n$. Пусть $V \cap U_i \neq \varnothing$. Докажите, что $k(V)$ изоморфно полю $k(V \cap U_i)$ рациональных функций на аффинном многообразии $V \cap U_i$. Указание: можно считать, что $i = 0$; выясните, что получится, если мы положим $x_0 = 1$ в частном f/g из п. (b).

15. Рассмотрим неприводимое многообразие $V \subset \mathbb{P}^n(k)$. Пусть $k(V)$ — поле рациональных функций на V, определенное в предыдущем упражнении.

(a) Докажите, что размерность многообразия V равна степени трансцендентности поля $k(V)$ над k. Указание: сведите задачу к аффинному случаю.

(b) Два неприводимых проективных многообразия V и V' (принадлежащие, возможно, различным проективным пространствам) называются *бирационально эквивалентными*, если любые их аффинные части $V \cap U_i$ и $V' \cap U_j$ бирационально эквивалентны в смысле § 5 гл. 5. Докажите, что V и V' бирационально эквивалентны в том и только том случае, когда существует изоморфизм полей $k(V) \cong k(V')$, тождественный на k. Указание: используйте предыдущее упражнение и теорему 10 из § 5 гл. 5.

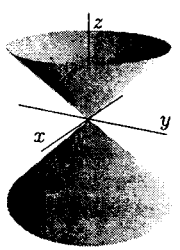
(c) Докажите, что размерности бирационально эквивалентных проективных многообразий совпадают.

§ 6. Размерность и неособость

В этом параграфе мы рассмотрим вопрос о том, как размерность связана с геометрическими свойствами многообразия V. Наше обсуждение будет сильно отличаться от методов § 5, где основную роль играли алгебраические свойства кольца $k[V]$ и поля $k(V)$. Мы введем некоторые довольно сложные понятия, и ряд теорем будет доказан только в частных случаях. Для простоты мы будем считать V аффинным многообразием.

Когда мы рассматриваем поверхность $V \subset \mathbb{R}^3$, то утверждение о ее двумерности на интуитивном уровне означает, что малая окрестность точки $p \in V$ выглядит, как маленький кусочек плоскости. Этот взгляд отражает то, как касательная плоскость аппроксимирует многообразие V в точке p:

Конечно, мы должны быть осторожны, так как поверхность может иметь точки, в которых нет касательной плоскости. Рассмотрим, например, конус $\mathbf{V}(x^2+y^2-z^2)$. Эта поверхность имеет касательную плоскость в каждой точке, кроме начала координат:



В этом параграфе мы введем понятие *неособой* точки p многообразия V и дадим аккуратное определение *касательного пространства* $T_p(V)$ к V в точке p. Наше рассмотрение является обобщением соответствующих рассмотрений для кривых (см. § 4 гл. 3). Касательное пространство описывает поведение многообразия V в окрестности точки p. Это то, что называется «локальным подходом». Хотя эта тема и не затрагивалась нами раньше, она играет важную роль в алгебраической геометрии. Вообще, характеристики многообразия, описывающие его поведение в окрестности данной точки, называются *локальными свойствами*.

Начнем рассмотрение с касательного пространства. Пусть кривая $V \subset \mathbb{R}^2$ задана уравнением $f(x,y) = 0$. Тогда (см. гл. 3) касательная прямая к V в точке $(a,b) \in V$ задана уравнением

$$\frac{\partial f}{\partial x}(a,b) \cdot (x-a) + \frac{\partial f}{\partial y}(a,b) \cdot (y-b) = 0$$

при условии, что обе частные производные не обращаются в нуль одновременно (см. упр. 4 к § 4 гл. 3). Обобщим это определение на случай произвольного многообразия.

Определение 1. Пусть $V \subset k^n$ — аффинное многообразие и $p = (p_1, \ldots, p_n)$ — его точка.

(i) Если $f \in k[x_1, \ldots, x_n]$ — некоторый полином, то его *линейной частью* в точке p называется полином

$$d_p(f) = \frac{\partial f}{\partial x_1}(p)(x_1 - p_1) + \ldots + \frac{\partial f}{\partial x_n}(p)(x_n - p_n).$$

Отметим, что его полная степень не превышает 1.

(ii) *Касательным пространством* к V в точке p называется многообразие

$$T_p(V) = \mathbf{V}(d_p(f) : f \in \mathbf{I}(V)).$$

Когда мы работаем над $\mathbb{R}$, частная производная $\frac{\partial f}{\partial x_i}$ определяется обычным образом. В случае произвольного поля мы используем *формальную частную производную*, определенную формулой

$$\frac{\partial}{\partial x_i}\left(\sum_{\alpha_1,\ldots,\alpha_n} c_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \ldots x_i^{\alpha_i} \ldots x_n^{\alpha_n}\right) = \sum_{\alpha_1,\ldots,\alpha_n} c_{\alpha_1,\ldots,\alpha_n} \alpha_i x_1^{\alpha_1} \ldots x_i^{\alpha_i - 1} \ldots x_n^{\alpha_n}.$$

В упр. 1 будет показано, что формальная частная производная обладает всеми свойствами обычной частной производной.

Сначала рассмотрим некоторые простые свойства касательного пространства $T_p(V)$.

Предложение 2. *Пусть* $p \in V \subset k^n$.

(i) *Если* $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$, *то* $T_p(V) = \mathbf{V}(d_p(f_1), \ldots, d_p(f_s))$.

(ii) $T_p(V)$ *является сдвигом линейного подпространства пространства* k^n.

Доказательство. (i) Легко видеть, что

$$d_p(hf) = h(p) \cdot d_p(f) + d_p(h) \cdot f(p)$$

(см. упр. 2). Из этого следует, что $d_p(hf) = h(p) \cdot d_p(f)$, если $f(p) = 0$. Таким образом, если $g = \sum_{i=1}^{s} h_i f_i \subset \mathbf{I}(V)$, то

$$d_p(g) = \sum_{i=1}^{s} d_p(h_i f_i) = \sum_{i=1}^{s} h_i(p) \cdot d_p(f_i) \in \langle d_p(f_1), \ldots, d_p(f_s) \rangle.$$

Это показывает, что $T_p(V)$ задано как множество общих нулей линейных полиномов $d_p(f_i)$.

(ii) Введем новую систему координат на k^n, полагая $X_i = x_i - p_i$, $1 \le i \le n$. Эта замена координат является просто сдвигом начала координат в точку p. Из (i) мы знаем, что многообразие $T_p(V)$ задано уравнениями $d_p(f_1) = \ldots = d_p(f_s) = 0$. Каждый полином $d_p(f_i)$ линеен по переменным X_i. Поэтому $T_p(V)$ является линейным подпространством в системе координат X_i, а это означает, что $T_p(V)$ является сдвигом подпространства пространства k^n. □

Интуитивное представление о касательном пространстве мы можем получить, рассматривая *формулу Тейлора* для полинома от нескольких переменных. Для полинома от одной переменной стандартная формула имеет вид

$$f(x) = f(a) + f'(a)(x - a) + \text{члены, содержащие старшие степени } x - a.$$

Если $f \in k[x_1, \ldots, x_n]$, то в точке $p = (p_1, \ldots, p_n)$ имеет место равенство (см. упр. 3)

$$f = f(p) + \frac{\partial f}{\partial x_1}(p)(x_1 - p_1) + \ldots + \frac{\partial f}{\partial x_n}(p)(x_n - p_n) + \text{члены полной степени } \ge 2 \text{ по переменным } x_1 - p_1, \ldots, x_n - p_n.$$

Это равенство представляет собой частный случай формулы Тейлора. Если $p \in V$, а $f \in \mathbf{I}(V)$, то $f(p) = 0$ и

$$f = d_p(f) + \text{члены полной степени } \ge 2 \text{ по переменным } x_1 - p_1, \ldots, x_n - p_n.$$

Другими словами, $d_p(f)$ представляет собой наилучшую линейную аппроксимацию полинома f в окрестности точки p. Пусть теперь $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$. Тогда многообразие V определяется обращением в нуль полиномов f_i, и его наилучшая линейная аппроксимация в окрестности точки p определена обращением в нуль линейных полиномов $d_p(f_i)$. Но это и задает касательное пространство к V.

Мы можем также описать $T_p(V)$ в терминах прямых, которые пересекают V в точке p с «высокой кратностью». В гл. 3 мы именно так и определяли касательную прямую к плоской кривой. Рассмотрим многомерный случай. Пусть $p \in V$, а прямая L пересекает V в p. Параметризуем L, положив $F(t) = p + tv$, где $v \in k^n$ — вектор, параллельный L. Если $f \in k[x_1, \ldots, x_n]$, то $f \circ F(t)$ является полиномом от t и $f \circ F(0) = f(p)$. Таким образом, 0 является корнем этого полинома, если $f \in \mathbf{I}(V)$. Тогда кратность корня 0 определяет, принадлежит L пространству $T_p(V)$ или нет.

Предложение 3. *Пусть* L *— прямая, проходящая через точку* p *и параметризованная формулой* $F(t) = p + vt$. *Тогда* $L \subset T_p(V)$ *в том и только том случае, когда* 0 *является корнем кратности* ≥ 2 *полинома* $f \circ F(t)$ *для всех* $f \in \mathbf{I}(V)$.

Доказательство. Запишем параметризацию прямой L в виде $x_i = p_i + tv_i$, $1 \le i \le n$, где $p = (p_1, \ldots, p_n)$, а $v = (v_1, \ldots, v_n)$. Тогда для любого $f \in \mathbf{V}(I)$

$$g(t) = f \circ F(t) = f(p_1 + tv_1, \ldots, p_n + tv_n).$$

Мы знаем, что $g(0) = 0$, так как $p \in V$. Поэтому 0 является корнем полинома $g(t)$. В упр. 4 к § 4 гл. 3 было показано, что $t = 0$ является корнем кратности ≥ 2 в том и только том случае, когда $g'(0) = 0$. Тогда

$$\frac{dg}{dt} = \frac{\partial f}{\partial x_1}\frac{dx_1}{dt} + \ldots + \frac{\partial f}{\partial x_n}\frac{dx_n}{dt} = \frac{\partial f}{\partial x_1}v_1 + \ldots + \frac{\partial f}{\partial x_n}v_n.$$

Следовательно, $g'(0) = 0$ в том и только том случае, когда

$$0 = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p)v_i = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p)((p_i + v_i) - p_i).$$

Выражение справа представляет собой значение полинома $d_p(f)$ в точке $p + v \in L$; следовательно, $p + v \in T_p(V)$ в том и только том случае, когда $g'(0) = 0$ для всех $f \in \mathbf{I}(V)$. Так как $p \in L$, то $L \subset T_p(V)$ в том и только том случае, когда $p + v \in T_p(V)$, что и доказывает предложение. □

Рассмотрим примеры.

Пример 4. Пусть $V \subset \mathbb{C}^n$ — гиперповерхность, заданная уравнением $f = 0$, где $f \in \mathbb{C}[x_1, \ldots, x_n]$ — непостоянный полином. По предложению 9 из § 2 гл. 4

$$\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(f)) = \sqrt{\langle f \rangle} = \langle f_{\text{red}} \rangle,$$

где $f_{\text{red}} = f_1 \ldots f_r$ — произведение различных неприводимых делителей полинома f. Мы будем считать, что $f = f_{\text{red}}$. Тогда

$$V = \mathbf{V}(f) = \mathbf{V}(f_1 \ldots f_s) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_r)$$

является разложением многообразия V в объединение неприводимых компонент (упр. 9 к § 6 гл. 4). В частности, каждая компонента многообразия V имеет размерность $n-1$ (по аффинной версии предложения 2 из § 4).

Так как $\mathbf{I}(V) = \langle f \rangle$, то для любой точки $p \in V$ пространство $T_p(V)$ является линейным пространством, заданным одним уравнением

$$\frac{\partial f}{\partial x_1}(p)(x_1 - p_1) + \ldots + \frac{\partial f}{\partial x_n}(p)(x_n - p_n) = 0.$$

Из этого следует, что

$$\dim T_p(V) = \begin{cases} n-1, & \dfrac{\partial f}{\partial x_i} \neq 0 \text{ хотя бы для одного } i, \\ n, & \dfrac{\partial f}{\partial x_i} = 0 \text{ для всех } i. \end{cases} \tag{1}$$

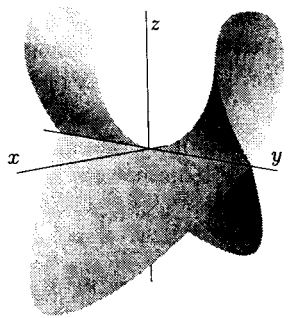
Проверьте, что это утверждение является обобщением предложения 2 из § 2 гл. 3.

Пусть $V = \mathbf{V}(x^2 - y^2z^2 + z^3)$. В упр. 4 будет доказано, что полином $f = x^2 - y^2z^2 + z^3 \in \mathbb{C}[x, y, z]$ неприводим и, значит, $\mathbf{I}(V) = \langle f \rangle$. Имеем

$$\frac{\partial f}{\partial x} = 2x, \quad \frac{\partial f}{\partial y} = -2yz^2, \quad \frac{\partial f}{\partial z} = -2y^2z + 3z^2.$$

Докажите самостоятельно, что частные производные обращаются в нуль одновременно только в точках оси y, которая принадлежит V. Таким образом, касательные пространства везде двумерны, кроме

точек оси y, где они совпадают с $\mathbb{C}^3$. Над $\mathbb{R}$ эта гиперповерхность выглядит так:



(Этот рисунок уже появлялся в § 2 гл. 1.) Позже мы увидим, что точки многообразия V, лежащие на оси y, являются особыми, а остальные его точки неособые.

Пример 5. Рассмотрим кривую $C \subset \mathbb{C}^3$, которая является пересечением поверхности V из примера 4 и плоскости $x+y+z=0$. Таким образом, $C = \mathbf{V}(x + y + z, x^2 - y^2z^2 + z^3)$. Используя методы § 3, покажите, что $\dim C = 1$.

В упражнениях будет доказано, что идеал $\langle f_1, f_2 \rangle = \langle x + y + z, x^2 - y^2z^2 + z^3 \rangle$ прост, а следовательно, кривая C неприводима. Так как простой идеал радикален, то из теоремы о нулях следует, что $\mathbf{I}(C) = \langle f_1, f_2 \rangle$. Пусть теперь $p = (a, b, c) \in C$. Тогда $T_p(C)$ задается линейными уравнениями

$$d_p(f_1) = 1 \cdot (x - a) + 1 \cdot (y - b) + 1 \cdot (z - c) = 0,$$
$$d_p(f_2) = 2a \cdot (x - a) + (-2bc^2) \cdot (y - b) + (-2b^2c + 3c^2) \cdot (z - c) = 0.$$

Это система линейных уравнений от переменных $x - a, y - b, z - c$ с матрицей

$$J_p(f_1, f_2) = \begin{pmatrix} 1 & 1 & 1 \\ 2a & -2bc^2 & -2b^2c + 3c^2 \end{pmatrix}.$$

Обозначим через $\operatorname{rank}(J_p(f_1, f_2))$ ранг этой матрицы. Так как $T_p(C)$ представляет собой сдвиг ядра матрицы $J_p(f_1, f_2)$, то

$$\dim T_p(C) = 3 - \operatorname{rank}(J_p(f_1, f_2)).$$

В упражнениях будет доказано, что $T_p(C)$ везде одномерно, кроме начала координат, где $T_0(C)$ является двумерной плоскостью $x + y + z = 0$.

В этих примерах мы должны были вычислять идеал $\mathbf{I}(V)$. Было бы гораздо удобнее, если бы мы могли работать с любыми уравнениями, определяющими многообразие V. К сожалению, это может привести к ошибкам: если $V = \mathbf{V}(f_1, \ldots, f_s)$, то касательное пространство $T_p(V)$ *не обязательно* определено равенствами $d_p(f_1) = \ldots = d_p(f_s) = 0$. Пусть, например, $V = \mathbf{V}(x^2)$. Тогда V представляет собой ось y в k^2, но, как легко проверить, $T_p(V) \neq \mathbf{V}(d_p(x^2))$ при $p \in V$. В теореме 9 будут сформулированы условия на определяющие полиномы $f_1, \ldots, f_s$, выполнение которых гарантирует, что $T_p(V) = \mathbf{V}(d_p(f_1), \ldots, d_p(f_s))$.

Примеры 4 и 5 показывают, что «хорошие» точки многообразия V — это те точки, где $T_p(V)$ имеет ту же размерность, что и V. Но этот принцип не работает, если V содержит неприводимые компоненты разных размерностей. Пусть, например, $V = \mathbf{V}(xz, yz) \subset \mathbb{R}^3$. Это многообразие является объединением плоскости (x, y) и оси z. Легко видеть, что

$$\dim T_p(V) = \begin{cases} 2, & p \text{ принадлежит плоскости } (x,y) \text{ минус начало координат,} \\ 1, & p \text{ принадлежит оси } z \text{ минус начало координат,} \\ 3, & p = (0,0,0). \end{cases}$$

За исключением начала координат, в точках оси z касательное пространство одномерно, что кажется правильным, так как эти точки принадлежат одномерной компоненте. Но в такой точке $\dim T_p(V) < \dim V$. Это, конечно, происходит по той причине, что у V есть компонента размерности 2.

Чтобы избежать подобных затруднений, мы определим размерность многообразия в точке.

Определение 6. Пусть V — аффинное многообразие и $p \in V$. *Размерностью многообразия V в p*, обозначаемой $\dim_p V$, называется максимум размерностей его неприводимых компонент, содержащих p.

По следствию 9 из § 4 размерность $\dim V$ равна максимуму $\dim_p V$ по всем $p \in V$. Если V является гиперповерхностью в $\mathbb{C}^n$, то $\dim_p V$ легко найти, так как в примере 4 мы показали, что каждая неприводимая компонента многообразия V имеет размерность $n-1$. Следовательно, $\dim_p V = n - 1$ для всех $p \in V$. Если же V — произвольное многообразие, то теория, развитая в §§ 3 и 4, позволяет найти $\dim V$, но если мы не знаем, как разложить V в объединение неприводимых компонент, то для вычисления $\dim_p V$ нужны более тонкие методы. Такие методы будут рассмотрены в § 7.

Дадим определение неособой точки.

Определение 7. Пусть V — аффинное многообразие и $p \in V$. Точка p называется *неособой* (или *гладкой*), если $\dim T_p(V) = \dim_p V$. В противном случае точка p называется *особой* точкой многообразия V.

Возвращаясь к примерам 4 и 5, легко понять, какие точки особые, а какие – нет. Кривая C из примера 5 неприводима, а потому $\dim_p C = 1$ для всех $p \in C$. Следовательно, особые точки — это такие точки p, в которых $\dim T_p(C) \neq 1$ (такая точка в этом случае только одна). Для гиперповерхностей $V = \mathbf{V}(f)$ из примера 4 имеем $\dim_p V = n - 1$ для всех $p \in V$. Поэтому из (1) следует, что p является особой точкой в том и только том случае, когда все частные производные полинома f обращаются в нуль в p. Это означает, что особые точки на V образуют многообразие

$$\Sigma = \mathbf{V}\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right). \tag{2}$$

В общем случае особые точки на многообразии V обладают следующими свойствами.

Теорема 8. *Пусть $V \subset k^n$ — аффинное многообразие и*

$$\Sigma = \{p \in V : p - \text{особая точка на } V\}.$$

Мы будем называть Σ особым множеством *многообразия V. Тогда*

(i) *Σ — аффинное многообразие, содержащееся в V;*
(ii) *если $p \in \Sigma$, то $\dim T_p(V) > \dim_p V$;*
(iii) *Σ не содержит неприводимых компонент многообразия V;*
(iv) *если V_i и V_j — различные неприводимые компоненты многообразия V, то $V_i \cap V_j \subset \Sigma$.*

Доказательство. Объем этой книги не позволяет привести здесь полное доказательство этой теоремы. Мы ограничимся частным случаем, когда V — гиперповерхность в $\mathbb{C}^n$, и укажем, где можно ознакомиться с полным доказательством.

Пусть $V = \mathbf{V}(f) \subset \mathbb{C}^n$ — гиперповерхность, такая, что $\mathbf{I}(V) = \langle f \rangle$. Мы знаем, что $\dim_p V = n - 1$ и что Σ состоит из тех точек многообразия V, в которых частные производные полинома f обращаются в нуль одновременно. Тогда из (2) следует, что Σ является аффинным многообразием, что доказывает (i) (в нашем случае). Доказательство в общем случае дано в § 2 гл. 2 книги SHAFAREVICH (1974) (следствие к теореме 6).

Пункт (ii) утверждает, что в особой точке многообразия V касательное пространство слишком велико. Если V — гиперповерхность

и $p \in V$ — особая точка, то из (1) нам известно, что $\dim T_p(V) \geq n > n-1 = \dim_p V$. Это доказывает п. (ii) в нашем случае. Полное доказательство содержится в § 1 гл. 2 книги SHAFAREVICH (1974) (теорема 3).

Пункт (iii) утверждает, что пересечение особого множества с каждой неприводимой компонентой многообразия V является собственным подмногообразием этой компоненты. Следовательно, большинство точек многообразия неособы. Докажем это для случая гиперповерхности. Пусть $V = \mathbf{V}(f) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_r)$ — разложение многообразия V в объединение неприводимых компонент (см. пример 4). Предположим, что одна из компонент, $\mathbf{V}(f_1)$ например, содержится в Σ. Тогда каждая частная производная $\frac{\partial f}{\partial x_i}$ обращается в нуль на $\mathbf{V}(f_1)$. Запишем f в виде $f = f_1 g$, где $g = f_2 \ldots f_r$. Имеем

$$\frac{\partial f}{\partial x_i} = f_1 \frac{\partial g}{\partial x_i} + \frac{\partial f_1}{\partial x_i} g.$$

Так как f_1 обращается в нуль на $\mathbf{V}(f_1)$, то $\frac{\partial f_1}{\partial x_i} g$ также обращается в нуль на $\mathbf{V}(f_1)$. Но f_1 — неприводимый полином по условию. Поэтому

$$\frac{\partial f_1}{\partial x_i} g \in \mathbf{I}(\mathbf{V}(f_1)) = \langle f_1 \rangle.$$

Таким образом, f_1 делит произведение $\frac{\partial f_1}{\partial x_i} g$, а значит, делит либо $\frac{\partial f_1}{\partial x_i}$, либо g. Но f_1 не может делить g, так как g — это произведение неприводимых полиномов, отличных от f_1. Таким образом, f_1 делит $\frac{\partial f_1}{\partial x_i}$ для всех i. Так как степень производной $\frac{\partial f_1}{\partial x_i}$ меньше, чем степень f_1, то $\frac{\partial f_1}{\partial x_i} = 0$ для всех i, откуда следует, что f_1 — константа (см. упр. 9). Это противоречие доказывает п. (iii) в нашем случае.

В общем случае доказательство п. (iii) можно найти в гл. 4 книги KENDIG (1977) (теоремы 4.1 и 4.3). Можно ознакомиться также с обсуждением, предшествующим определению особой точки, в § 1 гл. 2 книги SHAFAREVICH (1974). Если п. (iii) доказан в неприводимом случае, то общий случай следует из п. (iv) (см. упр. 11).

Наконец, п. (iv) утверждает, что неособая точка принадлежит ровно одной неприводимой компоненте. Если V — гиперповерхность, то $V = \mathbf{V}(f) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_r)$. Предположим, что $p \in \mathbf{V}(f_i) \cap \mathbf{V}(f_j), i \neq j$. Запишем f в виде $f = gh$, где f_i делит g, а f_j делит h. Тогда $g(p) = h(p) = 0$. Дифференцируя, получаем, что $\frac{\partial f}{\partial x_i} = 0$ для всех i. Это доказывает п. (iv) в нашем случае. Доказательство в общем случае можно найти в § 2 гл. 2 книги SHAFAREVICH (1974) (теорема 6). □

В некоторых случаях можно доказать неособость некоторой точки многообразия V, не вычисляя $\mathbf{I}(V)$. Прежде чем формулировать точное утверждение, введем обозначения. Пусть $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. Через $J(f_1, \ldots, f_r)$ обозначим $r \times n$-матрицу частных производных

$$J(f_1, \ldots, f_r) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial x_1} & \cdots & \frac{\partial f_r}{\partial x_n} \end{pmatrix}.$$

Если $p \in k^n$, то, вычисляя производные в этой точке, получаем числовую матрицу, которую мы будем обозначать $J_p(f_1, \ldots, f_r)$. Тогда имеет место следующий результат.

Теорема 9. *Пусть $V = \mathbf{V}(f_1, \ldots, f_r) \subset \mathbb{C}^n$ — некоторое многообразие, и пусть ранг матрицы $J_p(f_1, \ldots, f_r)$ в точке $p \in V$ равен r. Тогда p является неособой точкой многообразия V и принадлежит единственной компоненте размерности $n - r$.*

Доказательство. Как и в теореме 8, мы проведем доказательство только в случае гиперповерхности $V = \mathbf{V}(f) \subset \mathbb{C}^n$ (здесь $r = 1$). Обратите внимание, что f может быть *любым* полиномом, определяющим V, т. е. мы допускаем, что $\mathbf{I}(V) \neq \langle f \rangle$. Из определения касательного пространства следует, что

$$T_p(V) \subset \mathbf{V}(d_p(f)). \tag{3}$$

Так как $r = 1$, то $J_p(f)$ — вектор-строка с компонентами $\frac{\partial f}{\partial x_i}(p)$. Если ранг матрицы $J_p(f)$ равен 1, то это означает, что хотя бы одна частная производная не равна нулю в p. Тогда $d_p(f)$ является ненулевой линейной функцией от $x_i - p_i$, и из (3) следует, что $\dim T_p(V) \leq n-1$. Если сравнить это неравенство с формулой (1), получится, что p неособа, и в силу п. (iv) теоремы 8 точка p принадлежит ровно одной неприводимой компоненте многообразия V. Так как эта компонента имеет размерность $n - r = n - 1$, то в случае гиперповерхности утверждение доказано. В общем случае доказательство см. в книге MUMFORD (1976) (теорема (1.16)). □

Теорема 9 очень важна по нескольким причинам. Во-первых, она позволяет находить неособые точки и размерность многообразия. Например, мы можем провести вычисления в примерах 4 и 5, не определяя $\mathbf{I}(V)$ и $\mathbf{I}(C)$. Во-вторых, теорема 9 согласуется с нашим интуитивным представлением о том, что размерность должна

убывать на единицу при увеличении на один числа определяющих уравнений. Это примерно то, что и говорит теорема, но с одним важным уточнением, а именно: размерность убывает на единицу, если определяющие уравнения достаточно независимы (это означает, что ранг матрицы $J_p(f_1,\dots,f_r)$ равен r). В упр. 16 мы найдем более точную формулировку этого утверждения. Обратите внимание, однако, что все эти замечания относятся к неособой части V.

Имеется связь между теоремой 9 и некоторыми разделами анализа. В частности, в условии *теоремы о неявной функции* содержатся те же предположения о $J_p(f_1,\dots,f_r)$, что и в теореме 9. Если $V = \mathbf{V}(f_1,\dots,f_r)$ удовлетворяет этим условиям, то комплексная версия теоремы о неявной функции утверждает, что в окрестности точки p многообразие V выглядит как график регулярной функции, и поэтому понятно, почему V имеет размерность $n-r$ в p. Чтобы понять смысл теоремы 9 полностью, нужно ознакомиться с понятием *гладкого многообразия*. О гладких многообразиях, об их размерности и особых точках на них можно прочитать в книге KENDIG (1977).

Упражнения к § 6

1. В этом упражнении мы рассмотрим формальную производную.
   (a) Докажите, что формальная производная $\frac{\partial}{\partial x_i}$ является k-линейной и для нее выполнено обычное правило дифференцирования произведения.
   (b) Докажите, что $\frac{\partial}{\partial x_i}\left(\frac{\partial}{\partial x_j}f\right) = \frac{\partial}{\partial x_j}\left(\frac{\partial}{\partial x_i}f\right)$ для всех i,j.
   (c) Пусть $f_1,\dots,f_r \in k[x_1,\dots,x_n]$. Найдите $\frac{\partial}{\partial x_i}(f_1^{\alpha_1}\dots f_r^{\alpha_r})$.
   (d) Сформулируйте и докажите правило дифференцирования сложной функции вида $F(f_1,\dots,f_r)$. Указание: используйте п. (c).
2. Докажите, что $d_p(hf) = h(p)\cdot d_p(f) + d_p(h)\cdot f(p)$.
3. Пусть $p = (p_1,\dots,p_n) \in k^n$ и $f \in k[x_1,\dots,x_n]$.
   (a) Докажите, что f может быть представлен как полином от $x_i - p_i$. Указание: $x_i^m = ((x_i-p_i)+p_i)^m$.
   (b) Предположим, что в представлении f в виде полинома от $x_i - p_i$ каждый член имеет степень ≥ 2. Докажите, что $\frac{\partial f}{\partial x_i}(p) = 0$ для всех i.
   (c) Представим f в виде полинома от $x_i - p_i$. Докажите, что в этом представлении его свободный член равен $f(p)$, а линейная часть равна $d_p(f)$. Указание: используйте п. (b).
4. Как в примере 4, пусть $f = x^2 - y^2z^2 + z^3 \in \mathbb{C}[x,y,z]$, и пусть $V = \mathbf{V}(f) \subset \mathbb{C}^3$.
   (a) Докажите, что f неприводим в $\mathbb{C}[x,y,z]$.
   (b) Докажите, что V содержит ось y.

   (c) Пусть $p \in V$. Докажите, что все частные производные равны нулю в p в том и только том случае, когда p принадлежит оси y.
5. Рассмотрим $m \times n$-матрицу A, где $n \geq m$. Пусть $r \leq m$. Матрица B называется $r \times r$-*подматрицей* матрицы A, если она может быть получена из A путем выбора r ее строк и r столбцов.
   (a) Для произвольной числовой 3×4-матрицы выпишите все 3×3- и 2×2-подматрицы.
   (b) Докажите, что ранг матрицы A меньше r в том и только том случае, когда определители всех ее $t \times t$-подматриц, где $r \leq t \leq m$, равны 0. Указание: ранг матрицы равен максимальному числу ее линейно независимых столбцов, и если ранг матрицы A равен s, то можно найти $m \times s$-подматрицу ранга s; но ранг также равен максимальному числу линейно независимых строк. В каком случае $r \times r$-матрица имеет ранг $< r$?
6. Как и в примере 5, пусть $C = \mathbf{V}(x+y+z, x^2 - y^2z^2 + z^3) \subset \mathbb{C}^3$, и пусть $I = \langle x+y+z, x^2-y^2z^2+z^3\rangle \subset \mathbb{C}[x,y,z]$.
   (a) Докажите, что идеал I прост. Указание: введите новые координаты $X = x+y+z$, $Y = y$, $Z = z$ и докажите, что $I = \langle X, F(Y,Z)\rangle$ для некоторого полинома F от Y, Z; далее докажите, что $\mathbb{C}[X,Y,Z]/I \cong \mathbb{C}[Y,Z]/\langle F\rangle$ и что полином $F \in \mathbb{C}[Y,Z]$ неприводим.
   (b) Докажите, что многообразие C неприводимо и что $\mathbf{I}(C) = I$.
   (c) Найдите размерность многообразия C.
   (d) Найдите все точки $(a,b,c) \in C$, такие, что 2×3-матрица
   $$J_p(f_1,f_2) = \begin{pmatrix} 1 & 1 & 1 \\ 2a & -2bc^2 & -2b^2c+3c^2 \end{pmatrix}$$
   имеет ранг < 2. Указание: используйте упр. 5.
7. Пусть $f = x^2 \in k[x,y]$. Докажите, что $T_p(\mathbf{V}(f)) \neq \mathbf{V}(d_p(f))$ для всех $p \in \mathbf{V}(f)$.
8. Пусть $V = \mathbf{V}(xz, yz) \in k^3$, где поле k бесконечно.
   (a) Найдите $\mathbf{I}(V)$.
   (b) Проверьте справедливость формулы для $\dim T_p(V)$, приведенной в тексте параграфа.
9. Пусть $f \in k[x_1,\dots,x_n]$ — полином, такой, что $\frac{\partial}{\partial x_i}f = 0$ для всех i. Пусть характеристика поля k равна нулю (т. е. k содержит подполе, изоморфное $\mathbb{Q}$). Докажите, что f — нулевой полином.
10. Утверждение упр. 9 может не иметь места, если характеристика поля k не равна нулю.
    (a) Пусть $f = x^2+y^2 \in \mathbb{F}_2[x,y]$, где $\mathbb{F}_2$ — поле, содержащее только два элемента. Чему равны частные производные полинома f?
    (b) Чтобы изучить случай ненулевой характеристики, сначала нужно определить *характеристику* поля k. Покажите, что для любого поля k существует гомоморфизм колец $\phi : \mathbb{Z} \to k$, который

переводит число $n \in \mathbb{Z}$ в единицу поля k, сложенную саму с собой n раз. Пусть ϕ инъективен. Докажите, что k содержит подполе, изоморфное $\mathbb{Q}$, и, следовательно, его характеристика равна 0.

(c) Если характеристика поля k не равна нулю, то ϕ не инъективно. Докажите, что его ядром является идеал $\langle p \rangle \subset \mathbb{Z}$, где p — простое число. В этом случае мы говорим, что *характеристика поля* k равна p. Указание: используйте теорему об изоморфизме из упр. 16 к § 2 гл. 5 и тот факт, что k является областью целостности.

(d) Пусть характеристика поля k равна p. Докажите, что $(a+b)^p = a^p + b^p$ для всех $a, b \in k$.

(e) Пусть характеристика поля k равна p и $f \in k[x_1, \ldots, x_n]$. Докажите, что все частные производные полинома f тождественно равны нулю в том и только том случае, когда $f(x_1, \ldots, x_n) = g(x_1^p, \ldots, x_n^p)$ для некоторого полинома $g \in k[x_1, \ldots, x_n]$.

(f) Пусть поле k алгебраически замкнуто и имеет характеристику p. Предположим, что полином $f \in k[x_1, \ldots, x_n]$ неприводим. Докажите, что некоторая его частная производная не равна тождественно нулю. Это показывает, что теорема 8 справедлива в случае гиперповерхности над *любым* алгебраически замкнутым полем. Указание: используя пп. (d) и (e), докажите, что если все частные производные тождественно равны нулю, то f является p-й степенью некоторого полинома. Почему требование алгебраической замкнутости поля k является существенным?

11. Пусть $V = V_1 \cup \ldots \cup V_r$ — разложение многообразия в объединение неприводимых компонент.

(a) Предположим, что точка $p \in V$ принадлежит единственной неприводимой компоненте V_i. Докажите, что $T_p(V) = T_p(V_i)$. Этот факт иллюстрирует локальную природу касательного пространства. Указание: одно включение легко следует из того, что $V_i \subset V$; с другой стороны, если $f \in \mathbf{I}(W) - \mathbf{I}(V_i)$, где W — объединение остальных компонент, и $g \in \mathbf{I}(V_i)$, то $fg \in \mathbf{I}(V)$.

(b) Докажите, что точка p неособа в V в том и только том случае, когда она неособа в V_i.

(c) Пусть Σ — особое множество многообразия V, а Σ_i — особое множество многообразия V_i. Докажите, что

$$\Sigma = \bigcup_{i \neq j} (V_i \cap V_j) \cup \bigcup_i \Sigma_i.$$

Указание: используйте п. (b) и п. (iv) теоремы 8.

(d) Предположим, что каждое Σ_i является собственным подмножеством в V_i. Докажите, что Σ не содержит неприводимых компонент многообразия V. Это показывает, что п. (iii) теоремы 8 является следствием справедливости этой теоремы в неприводимом случае.

12. Найдите особые точки следующих кривых в k^2. Поле k считается алгебраически замкнутым.

(a) $y^2 = x^3 - 3$.
(b) $y^2 = x^3 - 6x^2 + 9x$.
(c) $x^2y^2 + x^2 + y^2 + 2xy(x + y + 1) = 0$.
(d) $x^2 = x^4 + y^4$.
(e) $xy = x^6 + y^6$.
(f) $x^2y + xy^2 = x^4 + y^4$.
(g) $x^3 = y^2 + x^4 + y^4$.

13. Найдите особые точки следующих поверхностей в k^3. Поле k считается алгебраически замкнутым.

(a) $xy^2 = z^2$.
(b) $x^2 + y^2 = z^2$.
(c) $x^2y + x^3 + y^3 = 0$.
(d) $x^3 - xyz + y^3 = 0$.

14. Докажите, что $\mathbf{V}(y - x^2 + y^2, 4x - y^2 + w^3) \subset \mathbb{C}^4$ является непустой гладкой поверхностью.

15. Рассмотрим гиперповерхность $V \subset k^n$, которая не является гиперплоскостью. Пусть $p \in V$ — неособая точка. Докажите, что p является особой точкой многообразия $V \cap T_p(V)$. Указание: используйте новые координаты, в которых $T_p(V)$ задается уравнением $x_1 = 0$, т. е. мы можем рассматривать $T_p(V)$ как пространство k^{n-1}, и тогда $V \cap T_p(V)$ — гиперповерхность в k^{n-1}.

16. Пусть $V \subset \mathbb{C}^n$ — неприводимое многообразие размерности d, а $p \in V$ — неособая точка.

(a) Докажите, что существуют полиномы $f_1, \ldots, f_{n-d} \in \mathbf{I}(V)$, такие, что $T_p(V) = \mathbf{V}(d_p(f_1), \ldots, d_p(f_{n-d}))$.

(b) Пусть $f_1, \ldots, f_{n-d}$ такие же, как в п. (a). Докажите, что $J_p(f_1, \ldots, f_{n-d})$ имеет ранг $n - d$ и что V является неприводимой компонентой многообразия $\mathbf{V}(f_1, \ldots, f_{n-d})$. Это показывает, что хотя само V может и не быть определено $n - d$ уравнениями, но оно является компонентой многообразия, определенного $n - d$ уравнениями. Указание: используйте теорему 9.

17. Пусть $V \subset \mathbb{C}^n$ — неприводимое многообразие размерности d, и пусть $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$.

(a) Докажите, что точка $p \in V$ неособа в том и только том случае, когда $J_p(f_1, \ldots, f_s)$ имеет ранг $n - d$. Указание: используйте предложение 2.

(b) Из теоремы 8 мы знаем, что у V есть неособые точки. Используя это и п. (a), докажите, что $d \geq n - s$. Какова связь этого утверждения с предложением 5 из § 4?

(c) Пусть $\mathcal{D}$ — множество определителей всех $(n - d) \times (n - d)$-подматриц матрицы $J(f_1, \ldots, f_s)$. Докажите, что особым множе-

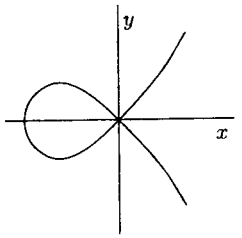
ством многообразия V является множество $\Sigma = V \cap \mathbf{V}(g : g \in \mathcal{D})$. Указание: используйте п. (а) и упр. 5. Что часть п. (ii) теоремы 8 говорит о ранге $J_p(f_1, \ldots, f_s)$?

§ 7. Касательный конус

В этом, последнем, параграфе книги мы рассмотрим *касательный конус* многообразия V в точке p. Если точка p неособа, то в ее окрестности многообразие V аппроксимируется касательным пространством $T_p(V)$. Но это не так, если p — особая точка, потому что, как мы видели в теореме 8 из § 6, касательное пространство в этом случае имеет неправильную размерность — оно слишком большое. Аппроксимация многообразия V в окрестности особой точки требует другого подхода.

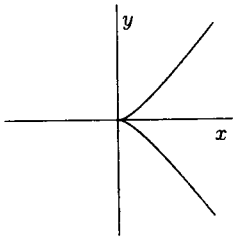
Начнем с примера.

Пример 1. Рассмотрим кривую $y^2 = x^2(x+1)$, график которой над $\mathbb{R}$ имеет следующий вид:



Начало координат является особой точкой. В окрестности начала координат кривая аппроксимируется прямыми $y = \pm x$. Эти прямые заданы уравнением $x^2 - y^2 = 0$. Записав определяющее уравнение в виде $f(x,y) = x^2 - y^2 + x^3$, мы видим, что $x^2 - y^2$ является ненулевой однородной компонентой полинома f наименьшей степени.

Рассмотрим теперь кривую $y^2 - x^3 = 0$:



Для этой кривой начало координат также является особой точкой, а ненулевой однородной компонентой полинома $y^2 - x^3$ наименьшей степени является y^2. Здесь $\mathbf{V}(y^2)$ — это ось x, и она наилучшим образом аппроксимирует кривую в окрестности особой точки.

В обоих случаях для аппроксимации кривой в окрестности особой точки мы использовали ненулевую однородную компоненту определяющего уравнения наименьшей степени. Изложим эти идеи в общем виде. Пусть $p = (p_1, \ldots, p_n) \in k^n$. Если $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$, то положим

$$(x-p)^\alpha = (x_1 - p_1)^{\alpha_1} \ldots (x_n - p_n)^{\alpha_n}.$$

Отметим, что полная степень полинома $(x-p)^\alpha$ равна $|\alpha| = \alpha_1 + \ldots + \alpha_n$. Пусть теперь дан полином $f \in k[x_1, \ldots, x_n]$ полной степени d. Представим его в виде полинома от $x_i - p_i$, т. е. в виде k-линейной комбинации полиномов $(x-p)^\alpha$ при $|\alpha| \leq d$. Тогда

$$f = f_{p,0} + f_{p,1} + \ldots + f_{p,d}, \tag{1}$$

где $f_{p,j}$ — это k-линейная комбинация полиномов $(x-p)^\alpha$ с $|\alpha| = j$. Отметим, что $f_{p,0} = f(p)$, а $f_{p,1} = d_p(f)$ (см. определение 1 из предыдущего параграфа). В упражнениях мы рассмотрим формулу Тейлора, которая позволяет определить $f_{p,j}$ в терминах частных производных полинома f в p. Часто бывает удобным перейти к новым координатам, в которых p является началом координат, и работать далее с обычными однородными компонентами.

Теперь дадим определение касательного конуса.

Определение 2. Рассмотрим аффинное многообразие $V \subset k^n$, и пусть $p = (p_1, \ldots, p_n) \in V$.

(i) Если $f \in k[x_1, \ldots, x_n]$ — ненулевой полином, то через $f_{p,\min}$ мы будем обозначать компоненту $f_{p,j}$, где j — минимальное число, такое, что $f_{p,j} \neq 0$ в представлении (1).

(ii) *Касательным конусом* многообразия V в точке p, обозначаемым через $C_p(V)$, называется многообразие

$$C_p(V) = \mathbf{V}(f_{p,\min} : f \in \mathbf{I}(V)).$$

Название «касательный конус» объясняется следующим предложением.

Предложение 3. *Пусть $p \in V \subset k^n$. Тогда $C_p(V)$ является сдвигом аффинного конуса некоторого многообразия в $\mathbb{P}^{n-1}(k)$.*

Доказательство. Введем новые координаты на k^n, положив $X_i = x_i - p_i$. В этих координатах точка p находится в начале координат.

Тогда $f_{0,\min}$ — однородный полином от $X_1, \ldots, X_n$; следовательно, всевозможные $f_{0,\min}$ при $f \in \mathbf{I}(V)$ порождают однородный идеал $J \subset k[X_1, \ldots, X_n]$. Теперь $C_p(V) = \mathbf{V}_a(J) \subset k^n$ по определению. Так как J однороден, то он задает также проективное многообразие $W = \mathbf{V}_p(J) \subset \mathbb{P}^{n-1}(k)$. Но это и означает (см. гл. 8), что касательный конус $C_p(V)$ совпадает с аффинным конусом $C_W \subset k^n$. □

Касательный конус гиперповерхности $V \subset k^n$ легко найти. В упр. 2 будет показано, что если $\mathbf{I}(V) = \langle f \rangle$, то конус $C_p(V)$ задан уравнением $f_{p,\min} = 0$. Это именно то, что мы делали в примере 1. Однако если $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$, $s > 1$, то $C_p(V)$ может *не* совпадать с многообразием $\mathbf{V}((f_1)_{p,\min}, \ldots, (f_s)_{p,\min})$. Рассмотрим, например, многообразие V, заданное уравнениями $xy = xz + z(y^2 - z^2) = 0$. В упр. 3 будет доказано, что $\mathbf{I}(V) = \langle xy, xz + z(y^2 - z^2) \rangle$. Докажем, что $C_0(V) \neq \mathbf{V}(xy, xz)$. Для этого отметим, что $f = yz(y^2 - z^2) = y(xz + z(y^2 - z^2)) - z(xy) \in \mathbf{I}(V)$. Тогда $f_{0,\min} = yz(y^2 - z^2)$ равен нулю на $C_0(V)$, но он не равен нулю на $\mathbf{V}(xy, xz)$.

Мы преодолеем эту трудность с помощью выбора подходящего базиса Грёбнера. Результат особенно ясно формулируется, когда p — начало координат.

Предложение 4. *Пусть начало координат 0 содержится в $V \subset k^n$. Введем новую переменную x_0 и зададим на $k[x_0, \ldots, x_n]$ мономиальное упорядочение, такое, что из двух мономов одинаковой полной степени моном, содержащий x_0, больше монома, не содержащего x_0* (lex *и* grlex *с $x_0 > \ldots > x_n$ удовлетворяют этому требованию).*

(i) *Пусть $\mathbf{I}(V)^h \subset k[x_0, \ldots, x_n]$ — гомогенизация идеала $\mathbf{I}(V)$ и $G_1, \ldots, G_n$ — базис Грёбнера идеала $\mathbf{I}(V)^h$ по отношению к определенному выше мономиальному упорядочению. Тогда*

$$C_0(V) = \mathbf{V}((g_1)_{0,\min}, \ldots, (g_s)_{0,\min}),$$

где $g_i = G_i(1, x_1, \ldots, x_n)$ — дегомогенизации полиномов G_i.

(ii) *Пусть k алгебраически замкнуто, а I — любой идеал, такой, что $V = \mathbf{V}(I)$. Если $G_1, \ldots, G_s$ — базис Грёбнера идеала I^h, то*

$$C_0(V) = \mathbf{V}((g_1)_{0,\min}, \ldots, (g_s)_{0,\min}),$$

где $g_i = G_i(1, x_1, \ldots, x_n)$ — дегомогенизация полинома G_i.

Доказательство. Здесь мы будем писать f_j и $f_{\min}$ вместо $f_{0,j}$ и $f_{0,\min}$.

(i) Пусть $I = \mathbf{I}(V)$. Достаточно показать, что $f_{\min} \in \langle (g_1)_{\min}, \ldots, (g_s)_{\min} \rangle$ для всех $f \in I$. Если это утверждение неверно, то можно

найти $f \in I$, такой, что $f_{\min} \notin \langle (g_1)_{\min}, \ldots, (g_s)_{\min} \rangle$ и, кроме того, $\mathrm{LT}(f_{\min})$ минимален в множестве полиномов с такими свойствами (мы можем рассматривать $f_{\min}$ как полином из $k[x_0, \ldots, x_n]$, так что $\mathrm{LT}(f_{\min})$ корректно определен). Представим f в виде суммы однородных компонент,

$$f = f_{\min} + \ldots + f_d,$$

где d — полная степень полинома f. Тогда

$$f^h = x_0^a f_{\min} + \ldots + f_d \in I^h$$

для некоторого a. Мы задали мономиальное упорядочение на $k[x_0, \ldots, x_n]$ так, что $\mathrm{LT}(f^h) = \mathrm{LT}(f_{\min})x_0^a$. Так как $G_1, \ldots, G_s$ — базис Грёбнера, то некоторый $\mathrm{LT}(G_i)$ делит $\mathrm{LT}(f_{\min})x_0^a$.

Пусть g_i — дегомогенизация полинома G_i. Тогда $g_i \in I$. Докажите самостоятельно, что

$$\mathrm{LT}(G_i) = \mathrm{LT}((g_i)_{\min})x_0^b$$

для некоторого b. Тогда $\mathrm{LT}(f_{\min}) = cx^\alpha \,\mathrm{LT}((g_i)_{\min})$, где c — ненулевая константа из k, а x^α — моном от переменных $x_1, \ldots, x_n$. Теперь рассмотрим полином $\tilde{f} = f - cx^\alpha g_i \in I$. Так как $f_{\min} \notin \langle (g_1)_{\min}, \ldots, (g_s)_{\min} \rangle$, то $f_{\min} - cx^\alpha (g_i)_{\min} \neq 0$, откуда

$$\tilde{f}_{\min} = f_{\min} - cx^\alpha (g_i)_{\min}.$$

Но тогда $\mathrm{LT}(\tilde{f}_{\min}) < \mathrm{LT}(f_{\min})$, так как старшие члены полиномов $f_{\min}$ и $cx^\alpha (g_i)_{\min}$ совпадают. Однако это противоречит минимальности $\mathrm{LT}(f_{\min})$. Пункт (i) доказан. В упражнениях будет показано, что полиномы $g_1, \ldots, g_s$ образуют базис идеала I, но не обязательно базис Грёбнера.

(ii) Пусть $W = \mathbf{V}(f_{\min} : f \in I)$. Из п. (i) следует, что

$$W = \mathbf{V}((g_1)_{\min}, \ldots, (g_s)_{\min}).$$

Осталось доказать, что W является касательным конусом в начале координат. Так как $I \subset \mathbf{I}(V)$, то $C_0(V) \subset W$. С другой стороны, пусть $g \in \mathbf{I}(V)$. Нам нужно показать, что $g_{\min}$ обращается в нуль на W. По теореме о нулях $g^m \in I$ для некоторого m. Следовательно, $(g^m)_{\min} = 0$ на W. В упражнениях будет доказано, что $(g^m)_{\min} = (g_{\min})^m$. Значит, $g_{\min}$ равен нулю на W. Это завершает доказательство предложения 4. □

Это предложение удобно применять в случае алгебраически замкнутого поля, потому что п. (ii) объясняет, как найти касательный конус, используя *любой* набор определяющих уравнений.

Пусть, например, $V = \mathbf{V}(xy, xz + z(y^2 - z^2))$. Положим $I = \langle xy, xz + z(x^2 - y^2)\rangle$. На первом шаге мы строим однородный идеал $I^h \subset k[w, x, y, z]$, где w — дополнительная переменная. Базис Грёбнера идеала I по отношению к grlex-упорядочению есть $\{xy, xz + z(x^2 - y^2), x^2z - xz^3\}$. Тогда $\{xy, xzw + z(x^2 - y^2), x^2zw - xz^3\}$ — это базис идеала I^h (см. § 4 гл. 8). Этот базис является базисом Грёбнера относительно grlex-упорядочения с $x > y > z > w$ (см. упр. 5). Но такое мономиальное упорядочение не удовлетворяет условию предложения 4. Однако если мы используем grlex-упорядочение с $w > x > y > z$, то получим базис Грёбнера

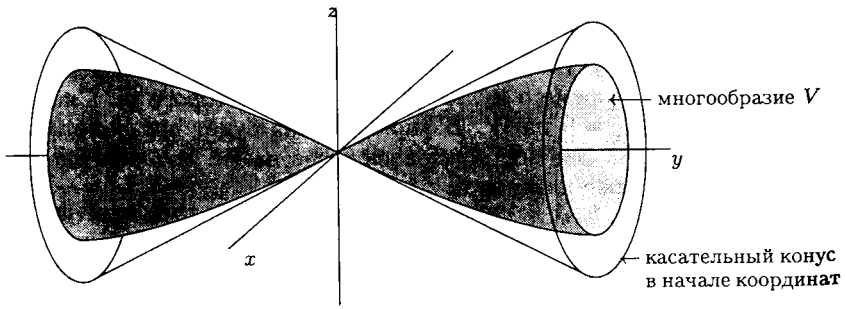
$$\{xy, xzw + z(x^2 - y^2), yz(y^2 - z^2)\}.$$

Тогда из предложения 4 следует, что для определения касательного конуса в нуле нам нужно дегомогенизировать элементы базиса и взять минимальные однородные компоненты. Имеем

$$C_0(V) = \mathbf{V}(xy, xz, yz(y^2 - z^2)).$$

В упражнениях будет показано, что это есть объединение пяти прямых, проходящих через начало координат в k^3.

Теперь мы рассмотрим, как касательный конус аппроксимирует многообразие в окрестности точки p. По предложению 3 конус $C_p(V)$ является сдвигом аффинного конуса, т. е. $C_p(V)$ является объединением прямых, проходящих через точку p. Поэтому нам нужно указать, какие именно прямые принадлежат $C_p(V)$. Мы сделаем это, используя секущие прямые. Дадим определение. Пусть прямая $L \subset k^n$ проходит через точку p. Тогда L называется *секущей прямой* многообразия V, если она содержит еще хотя бы одну точку этого многообразия, отличную от p. Вот главное соображение: когда секущие прямые определены точками из V, стремящимися к p, то «предел» этих секущих должен принадлежать касательному конусу. Приведем рисунок:

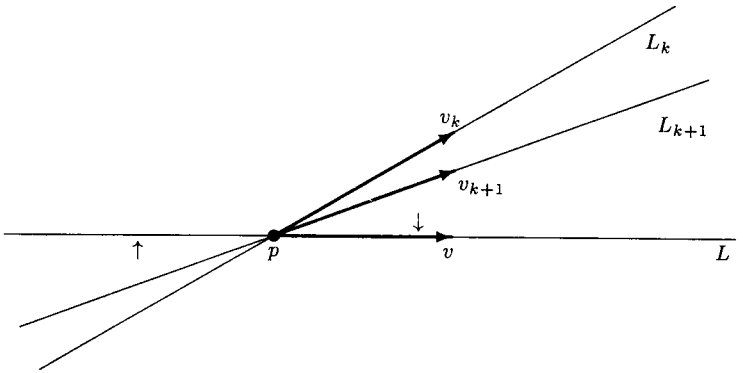


Чтобы добиться строгости, мы будем работать над полем комплексных чисел $\mathbb{C}$. В этом случае последовательность точек $q_k \in \mathbb{C}^n$ сходится к точке $q \in \mathbb{C}^n$, если координаты точек q_k сходятся к соответствующим координатам точки q. Мы предполагаем, что читатель имеет некоторый опыт работы с такими последовательностями.

Мы будем считать, что прямые заданы параметрическими уравнениями, т. е. прямая L задана в виде $p + tv$, где v — вектор, параллельный L, а $t \in \mathbb{C}$. Определим предел прямых.

Определение 5. Прямая $L \subset \mathbb{C}^n$, проходящая через точку p, называется *пределом прямых* $\{L_k\}_{k=1}^{\infty}$, проходящих через ту же точку p, если для заданной параметризации $p + vt$ прямой L существуют параметризации $p + tv_k$ прямых L_k, такие, что $\lim_{k\to\infty} v_k = v$.

Следующий рисунок поясняет это определение:



Теперь мы можем сформулировать точное утверждение об аппроксимации.

Теорема 6. *Пусть $V \subset \mathbb{C}^n$ — аффинное многообразие. Прямая L, проходящая через точку $p \in V$, принадлежит касательному конусу $C_p(V)$ в том и только том случае, когда существует последовательность точек $\{q_k\}_{k=1}^{\infty}$ в $V - \{p\}$, сходящаяся к p и такая, что L является пределом секущих L_k, где L_k — прямая, соединяющая p и q_k.*

Доказательство. Мы можем считать, что $p = 0$. Пусть последовательность $\{q_k\}$ точек из V сходится к нулю, а последовательность прямых L_k (L_k соединяет 0 и точку q_k) сходится (в смысле определения 5) к прямой L. Мы хотим доказать, что $L \subset C_0(V)$.

Существуют параметризации tv_k прямых L_k (напомним, что $p = 0$), такие, что $v_k \to v$ при $k \to \infty$, где tv — параметр прямой L. Так как $q_k \in L_k$, то $q_k = t_k v_k$. Здесь $t_k \neq 0$, так как в противном случае $q_k = p$. Мы утверждаем, что $t_k \to 0$. В самом деле, $v_k \to v \neq 0$, а $t_k v_k = q_k \to 0$ (подробнее это будет рассматриваться в упр. 8).

Пусть полином f обращается в нуль на V. Мы будем писать f_j и $f_{\min}$ вместо $f_{0,j}$ и $f_{0,\min}$. Если степень полинома f равна d, то $f = f_l + f_{l+1} + \ldots + f_d$, где $f_l = f_{\min}$. Так как $q_k = t_k v_k \in V$, то

$$0 = f(t_k v_k) = f_l(t_k v_k) + \ldots + f_d(t_k v_k). \tag{2}$$

Так как f_i однороден и имеет степень i, так что $f_i(t_k v_k) = t_k^i f(v_k)$, то

$$0 = t_k^l f_l(v_k) + \ldots + t_k^d f_d(v_k). \tag{3}$$

Поскольку $t_k \neq 0$,

$$0 = f_l(v_k) + t_k f_{l+1}(v_k) + \ldots + t_k^{d-l} f_d(v_k). \tag{4}$$

Рассматривая предел правой части формулы (4) при $k \to \infty$ (поскольку $v_k \to v$, а $t_k \to 0$), получаем, что $f_l(v) = 0$, а так как $f_l(tv) = t^l f_l(v) = 0$ для всех t, то $L \subset C_0(V)$. Это означает, что $C_0(V)$ содержит все пределы секущих, определенных последовательностями точек из V, сходящимися к нулю.

Докажем обратное включение. Для этого рассмотрим множество

$$\mathcal{V} = \{(v,t) \in \mathbb{C}^n \times \mathbb{C} : tv \in V, t \neq 0\} \subset \mathbb{C}^{n+1}. \tag{5}$$

Если $(v,t) \in \mathcal{V}$, то прямая L, проходящая через 0 и точку tv, является секущей. Мы хотим понять, что происходит с $\mathcal{V}$, когда $t \to 0$. Для этого мы рассмотрим замыкание Зарисского $\overline{\mathcal{V}}$ множества $\mathcal{V}$, которое является наименьшим многообразием в $\mathbb{C}^{n+1}$, содержащим $\mathcal{V}$. Мы утверждаем, что

$$\overline{\mathcal{V}} = \mathcal{V} \cup (C_0(V) \times \{0\}). \tag{6}$$

Мы знаем, что $\overline{\mathcal{V}} = \mathbf{V}(\mathbf{I}(\mathcal{V}))$ (см. § 4 гл. 4). То есть нам нужно описать функции, равные нулю на $\mathcal{V}$. Пусть $f \in \mathbf{I}(V)$, где $f = f_l + \ldots + f_d$. Положим

$$\tilde{f} = f_l + t f_{l+1} + \ldots + t^{d-l} f_d \in \mathbb{C}[t, x_1, \ldots, x_n].$$

Мы докажем, что

$$\mathbf{I}(\mathcal{V}) = \langle \tilde{f} : f \in \mathbf{I}(V) \rangle. \tag{7}$$

В одну сторону это просто: если $f \in \mathbf{I}(V)$ и $(v,t) \in \mathcal{V}$, то $f(tv) = 0$, и тогда из (2), (3) и (4) следует, что $\tilde{f}(v,t) = 0$. С другой стороны, пусть $g \in \mathbb{C}[t, x_1, \ldots, x_n]$ обращается в нуль на $\mathcal{V}$. Пусть $g = \sum_i g_i t^i$,

где $g_i \in \mathbb{C}[x_1, \ldots, x_n]$, и пусть $g_i = \sum_j g_{ij}$ — разложение полинома g_i в сумму однородных компонент. Если $(v,t) \in \mathcal{V}$, то $(\lambda v, \lambda^{-1} t) \in \mathcal{V}$ для любого $\lambda \in \mathbb{C} - \{0\}$, потому что $(\lambda^{-1} t) \cdot (\lambda v) \in V$. Таким образом,

$$0 = g(\lambda v, \lambda^{-1} t) = \sum_{i,j} g_{ij}(\lambda v)(\lambda^{-1} t)^i = \sum_{i,j} \lambda^j g_{ij}(v) \lambda^{-i} t^i = \sum_{i,j} \lambda^{j-i} g_{ij}(v) t^i$$

для всех $\lambda \neq 0$. Положим $m = j - i$ и перепишем сумму в виде

$$0 = \sum_m \left(\sum_i g_{i,m+i}(v) t^i \right) \lambda^m.$$

Так как это равенство выполнено для любого элемента $\lambda \neq 0$, то $\sum_i g_{i,m+i}(v) t^i = 0$ для всех m. Следовательно, $\sum_i g_{i,m+i}(v) t^i \in \mathbf{I}(\mathcal{V})$. Пусть $f_m = \sum_i g_{i,m+i} \in \mathbb{C}[x_1, \ldots, x_n]$. Так как $(v,1) \in \mathcal{V}$ для всех $v \in V$, то $f_m \in \mathbf{I}(V)$. Обозначим через i_0 наименьшее i, такое, что $g_{i,m+i} \neq 0$. Тогда

$$\tilde{f}_m = g_{i_0, m+i_0} + g_{i_0+1, m+i_0+1} t + \ldots;$$

следовательно, $\sum_i g_{i,m+i} t^i = t^{i_0} \tilde{f}_m$. Отсюда сразу вытекает, что $g \in \langle \tilde{f} : f \in \mathbf{I}(V) \rangle$. Таким образом, (7) доказано.

Из (7) следует, что $\overline{\mathcal{V}} = \mathbf{V}(\tilde{f} : f \in \mathbf{I}(V))$. Опишем это многообразие. Пусть $(v,t) \in \mathbb{C}^{n+1}$ и $t \neq 0$. Из (2), (3) и (4) следует, что $\tilde{f}(v,t) = 0$ в том и только том случае, когда $f(tv) = 0$. Значит,

$$\overline{\mathcal{V}} \cap \{(v,t) : t \neq 0\} = \mathcal{V}.$$

Пусть теперь $t = 0$. Если $f = f_l + \ldots + f_d$, где $f_l = f_{\min}$, то из определения полинома $\tilde{f}$ следует, что $\tilde{f}(v,0) = 0$ в том и только том случае, когда $f_l(v) = 0$. Следовательно,

$$\overline{\mathcal{V}} \cap \{(v,t) : t = 0\} = C_0(V) \times \{0\},$$

и (6) доказано.

Чтобы закончить доказательство теоремы 6, нам понадобится следующее свойство замыкания Зарисского.

Предложение 7. *Пусть $Z \subset W \subset \mathbb{C}^n$ — аффинные многообразия и W является замыканием Зарисского множества $W - Z$. Если $z \in Z$ — произвольная точка, то существует последовательность точек $\{w_k \in W - Z\}_{k=1}^{\infty}$, сходящаяся к z.*

Доказательство. Доказательство этого утверждения требует сложной техники и выходит за рамки этой книги. В книге MUMFORD (1976) это утверждение доказано для неприводимых многообразий в $\mathbb{P}^n(\mathbb{C})$ (теорема (2.33)). В упр. 9 будет показано, как вывести предложение 7 из теоремы Мамфорда. □

Чтобы применить предложение 7, положим $Z = C_0(V) \times \{0\} \subset W = \overline{\mathcal{V}}$. По (6) имеем $W - Z = \overline{\mathcal{V}} - (C_0(V) \times \{0\}) = \mathcal{V}$; следовательно, $W = \overline{\mathcal{V}}$ является замыканием Зарисского множества $W - Z$. Тогда из предложения 7 следует, что каждая точка $Z = C_0(V) \times \{0\}$ является пределом точек из $W - Z = \mathcal{V}$.

Теперь мы можем завершить доказательство теоремы 6. Пусть прямая L с параметризацией tv принадлежит $C_0(V)$. Тогда $v \in C_0(V)$ и, следовательно, $(v, 0) \in C_0(V) \times \{0\}$. Найдем последовательность точек $(v_k, t_k) \in \mathcal{V}$, сходящуюся к $(v, 0)$. Обозначим через L_k прямую с параметризацией tv_k. Тогда $L_k \to L$. Кроме того, так как $q_k = t_k v_k \in V$ и $t_k \neq 0$, то L_k — секущая, определенная точкой $q_k \in V$. Наконец, $q_k = t_k \cdot v_k \to 0 \cdot v = 0$ при $k \to \infty$. Это и означает, что L является пределом секущих, определенных точками $q_k \in V$, сходящимися к 0. Доказательство теоремы закончено. □

Если мы работаем над произвольным полем, то мы не можем определить сходимость секущих. Поэтому не очевидно, как обобщить теорему 6 на случай произвольного поля. Но если $p \in V$ является началом координат, то над любым полем мы можем определить многообразие $\mathcal{V}$, как в (5), и каждая секущая по-прежнему определяет точку $(v, t) \in \mathcal{V}$ с $t \neq 0$. Чисто алгебраический способ перехода к пределу при $t \to 0$ состоит в рассмотрении наименьшего многообразия, содержащего $\mathcal{V}$, и анализа того, что происходит при $t = 0$, т. е. рассмотрения множества $\overline{\mathcal{V}} \cap (k^n \times \{0\})$, которое по (6) равно $C_0(V) \times \{0\}$. Проверьте самостоятельно, что доказательство формулы (6) корректно над любым полем и потому разложение

$$\overline{\mathcal{V}} = \mathcal{V} \cup (C_0(V) \times \{0\})$$

может рассматриваться, как обобщение теоремы 6 на случай произвольного поля. В упр. 10 будут рассматриваться некоторые интересные свойства многообразия $\mathcal{V}$.

Касательный конус также аппроксимирует многообразие в терминах размерности. Напомним (см. § 6), что $\dim_p V$ — это максимум размерностей неприводимых компонент, содержащих p.

Теорема 8. *Пусть точка p принадлежит многообразию $V \subset k^n$. Тогда $\dim_p V = \dim C_p(V)$.*

Доказательство. Это стандартный результат из коммутативной алгебры (см., например, MATSUMURA (1986), Theorem 13.9). Как и в § 6, мы докажем это утверждение только в случае гиперповерхности в $\mathbb{C}^n$. Если $V = \mathbf{V}(f)$, то $C_p(V) = \mathbf{V}(f_{p,\min})$ (упр. 2). Таким образом, V и $C_p(V)$ — гиперповерхности, а следовательно, их размерность равна $n-1$ во всех точках. Значит, $\dim_p V = \dim C_p(V)$. □

Это полезный результат, так как он дает возможность найти $\dim_p V$, не разлагая V на неприводимые компоненты.

Обсудим, наконец, связь между касательным конусом и касательным пространством. В упражнениях будет доказано, что для любой точки $p \in V$ имеет место включение

$$C_p(V) \subset T_p(V).$$

В терминах размерностей это означает, что

$$\dim C_p(V) \leq \dim T_p(V).$$

Следующее утверждение дает критерий совпадения этих множеств.

Следствие 9. *Пусть поле k алгебраически замкнуто, а точка p принадлежит многообразию $V \subset k^n$. Следующие три условия эквивалентны:*

(i) *p — неособая точка многообразия V;*
(ii) $\dim C_p(V) = \dim T_p(V)$;
(iii) $C_p(V) = T_p(V)$.

Доказательство. Так как $\dim C_p(V) = \dim_p V$ по теореме 8, то эквивалентность условий (i) и (ii) сразу следует из определения неособой точки. Импликация (iii)⇒(ii) тривиальна; поэтому нужно доказать, что (ii)⇒(iii).

Так как k алгебраически замкнуто, то оно бесконечно; поэтому $T_p(V)$ является неприводимым многообразием в k^n. (Если $T_p(V)$ — координатное подпространство, то это следует из упр. 7 к § 1. Общий случай рассмотрен в упр. 12.) Таким образом, если размерности пространств $C_p(V)$ и $T_p(V)$ совпадают, то равенство $C_p(V) = T_p(V)$ непосредственно следует из аффинной версии предложения 10 из § 4 (см. упр. 18 к § 4).

Из теоремы 6 и следствия 9 получаем, что касательное пространство в неособой точке p многообразия $V \subset \mathbb{C}^n$ является объединением всех пределов секущих, определенных последовательностями точек из V, сходящимися к p. Это важное обобщение теоремы из элементарного анализа, утверждающей, что касательная к кривой является пределом секущих.

Упражнения к § 7

1. Пусть поле k имеет характеристику 0. Рассмотрим точку $p \in k^n$ и полином $f \in k[x_1, \dots, x_n]$. Тогда f может быть записан в виде $f = \sum_\alpha c_\alpha (x-p)^\alpha$, где $c_\alpha \in k$, а $(x-p)_\alpha$ определен в тексте параграфа. При заданном α положим

$$\frac{\partial^\alpha}{\partial^\alpha x} = \frac{\partial^{\alpha_1}}{\partial^{\alpha_1} x_1} \cdots \frac{\partial^{\alpha_n}}{\partial^{\alpha_n} x_n},$$

где $\frac{\partial^{\alpha_i}}{\partial^{\alpha_i} x_i}$ означает α_i-кратное дифференцирование по переменной x_i. Положим далее

$$\alpha! = \alpha_1! \cdot \alpha_2! \dots \alpha_n!.$$

(a) Докажите, что

$$\frac{\partial^\alpha (x-p)^\beta}{\partial^\alpha x}(p) = \begin{cases} \alpha!, & \text{если } \alpha = \beta, \\ 0, & \text{если } \alpha \neq \beta. \end{cases}$$

Указание: надо рассмотреть два случая: когда $\beta_i < \alpha_i$ для некоторого i и когда $\beta_i \geq \alpha_i$ для всех i.

(b) Пусть $f = \sum_\alpha c_\alpha (x-p)^\alpha$. Докажите, что

$$c_\alpha = \frac{1}{\alpha!} \frac{\partial^\alpha f}{\partial^\alpha x}(p)$$

и что

$$f = \sum_\alpha \frac{1}{\alpha!} \frac{\partial^\alpha f}{\partial^\alpha x}(p)(x-p)^\alpha.$$

Это равенство называется *формулой Тейлора* для f в точке p. Указание: объясните, почему характеристика поля k должна быть равна нулю.

(c) Выпишите формулу из п. (b) в явном виде для полинома $f \in k[x, y]$ полной степени 3.

(d) Как определить $f_{p,j}$ в терминах частных производных полинома f?

(e) Покажите на примере, что над полем положительной характеристики не всегда можно выразить полиномом f в терминах частных производных. Указание: см. упр. 10 к § 6.

2. Рассмотрим гиперповерхность $V \subset k^n$.

(a) Пусть $\mathbf{I}(V) = \langle f \rangle$. Докажите, что $C_p(V) = \mathbf{V}(f_{p,\min})$.

(b) Пусть k алгебраически замкнуто, а $V = \mathbf{V}(f)$. Докажите, что утверждение п. (a) остается справедливым. Указание: см. доказательство п. (ii) предложения 4.

3. В этом упражнении мы покажем, что идеал $I = \langle xy, xz + z(y^2 - z^2) \rangle \subset k[x, y, z]$ радикален (характеристика поля k равна 0).

(a) Докажите, что

$$\langle x, z(y^2 - z^2) \rangle = \langle x, z \rangle \cap \langle x, y - z \rangle \cap \langle x, y + z \rangle.$$

Докажите, что три идеала в правой части равенства просты. Указание: работайте в факторкольце $k[x, y, z]/\langle x \rangle \cong k[y, z]$ и используйте тот факт, что в кольце $k[y, z]$ разложение на множители однозначно. Объясните, почему этот результат неверен над полем $\mathbb{F}_2$ из двух элементов.

(b) Докажите, что

$$\langle y, xz - z^3 \rangle = \langle y, z \rangle \cap \langle y, x - z^2 \rangle.$$

Докажите, что оба идеала в правой части равенства просты.

(c) Докажите, что $I = \langle x, z(y^2 - z^2) \rangle \cap \langle y, xz - z^3 \rangle$. Указание: можно использовать алгоритм пересечения идеалов из § 3 гл. 4, но можно обойтись и без этого.

(d) Из (a), (b) и (c) следует, что I является пересечением пяти простых идеалов. Докажите, что I радикален. Используя его разложение, опишите $V = \mathbf{V}(I) \subset k^3$.

(e) Пусть k алгебраически замкнуто. Что представляет собой идеал $\mathbf{I}(V)$?

4. В этом упражнении мы рассмотрим доказательство предложения 4. Зафиксируем мономиальное упорядочение $>$ на $k[x_0, \dots, x_n]$, удовлетворяющее условиям предложения 4.

(a) Пусть $g \in k[x_1, \dots, x_n]$ является дегомогенизацией полинома $G \in k[x_0, \dots, x_n]$. Докажите, что $\mathrm{LT}(G) = \mathrm{LT}(g_{\min}) x_0^b$ для некоторого b.

(b) Пусть $G_1, \dots, G_s$ образуют базис идеала I^h. Докажите, что дегомогенизации $g_1, \dots, g_s$ этих полиномов образуют базис в I. В упр. 5 мы покажем, что если $G_1, \dots, G_s$ образуют базис Грёбнера идеала I^h по отношению к $>$, то $g_1, \dots, g_s$ могут не образовывать базис Грёбнера идеала I по отношению к индуцированному упорядочению на $k[x_1, \dots, x_n]$.

(c) Пусть $f, g \in k[x_1, \dots, x_n]$. Докажите, что $(f \cdot g)_{\min} = f_{\min} \cdot g_{\min}$. Выведите из этого, что $(f^m)_{\min} = (f_{\min})^m$.

5. Продолжим изучение многообразия $V = \mathbf{V}(xy, xz + z(y^2 - z^2))$, начатое в тексте параграфа.

(a) Используя grlex-упорядочение с $w > x > y > z$, докажите, что базисом Грёбнера идеала $I^h \subset k[w, x, y, z]$ является $\{xy, xzw + z(y^2 - z^2), yz(y^2 - z^2)\}$.

(b) Дегомогенизируя базис Грёбнера из п. (a), мы получим базис идеала I. Докажите, что этот базис *не* является базисом Грёбнера идеала I по отношению к grlex-упорядочению с $x > y > z$.

(c) Используя предложение 4, докажите, что касательный конус $C_0(V)$ является объединением пяти прямых, проходящих через начало координат в k^3. Сравните ваш ответ с ответом к п. (e) упр. 3.

6. Найдите размерность касательного конуса и размерность касательного пространства в нуле для многообразий, заданных следующими идеалами:
   (a) $\langle xz, xy\rangle \subset k[x,y,z]$;
   (b) $\langle x-y^2, x-z^3\rangle \subset k[x,y,z]$.

7. В § 3 гл. 3 с помощью теории исключения мы показали, что касательная поверхность S скрученной кубики $\mathbf{V}(y-x^2, z-x^3) \subset \mathbb{R}^3$ задана уравнением

$$x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2 = 0.$$

   (a) Докажите, что скрученная кубика является особым множеством касательной поверхности S. Указание: два разных идеала могут определять одно и то же многообразие. См. формулу (14) из § 4 гл. 3.
   (b) Найдите касательное пространство и касательный конус поверхности S в нуле.

8. Рассмотрим две последовательности векторов v_k и t_kv_k в $\mathbb{C}^n$, где $t_k \in \mathbb{C}$, $v_k \to v \neq 0$ и $t_kv_k \to 0$. Мы утверждаем, что $t_k \to 0$ в $\mathbb{C}$. Чтобы доказать это, определим модуль комплексного числа $t = x + iy$ формулой $|t| = \sqrt{x^2+y^2}$, а норму вектора $v = (z_1, \ldots, z_n) \in \mathbb{C}^n$ формулой $|v| = \sqrt{|z_1|^2 + \ldots + |z_n|^2}$. Напомним, что сходимость $v_k \to v$ означает, что для любого ϵ найдется N, такое, что $|v_k - v| < \epsilon$ для всех $k \geq N$.
   (a) Пусть $v = (z_1, \ldots, z_n)$, а $v_k = (z_{k1}, \ldots, z_{kn})$. Докажите, что из сходимости $v_k \to v$ следует, что $z_{kj} \to z_j$ для всех j. Указание: обратите внимание, что $|z_j| \leq |v|$.
   (b) Выберите ненулевую компоненту z_j вектора v. Докажите, что $z_{kj} \to z_j \neq 0$ и что $t_kz_{kj} \to 0$. Теперь разделите на z_j и покажите, что $t_k \to 0$.

9. Теорема (2.33) из книги MUMFORD (1976) утверждает, что если $W \subset \mathbb{P}^n(\mathbb{C})$ — неприводимое проективное многообразие, а $Z \subset W$ — проективное многообразие, не равное W, то каждая точка из Z является пределом точек из $W - Z$. С помощью этой теоремы мы хотим доказать предложение 7.
   (a) Пусть $Z \subset W \subset \mathbb{C}^n$ — аффинные многообразия и W является замыканием Зарисского множества $W - Z$. Докажите, что Z не содержит неприводимых компонент многообразия W.

   (b) Покажите, что достаточно доказать предложение 7 в случае, когда W неприводимо. Указание: если $p \in Z$, то p принадлежит некоторой компоненте W_1 многообразия W. Что п. (a) говорит о $W_1 \cap Z \subset W_1$?
   (c) Пусть $Z \subset W \subset \mathbb{C}^n$, где W неприводимо и $Z \neq W$. Пусть $\overline{Z}$ и $\overline{W}$ — проективные замыкания многообразий W и Z в $\mathbb{P}^n(\mathbb{C})$. Докажите, что неприводимый случай предложения 7 следует из упомянутой выше теоремы Мамфорда (2.33). Указание: рассмотрите $\overline{Z} \cup (\overline{W} - W) \subset \overline{W}$.
   (d) Докажите, что справедливо обратное утверждение. А именно, пусть $p \in \mathbb{C}^n$. Если $p \notin W - Z$ и p является пределом точек из $W - Z$, то $p \in Z$. Указание: докажите, что $p \in W$, и воспользуйтесь непрерывностью полиномов.

10. Пусть многообразие $V \subset k^n$ содержит начало координат. Рассмотрим многообразие $\mathcal{V} \subset k^{n+1}$, определенное в (5). Для $\lambda \in k$ определим «срез» $(k^n \times \lambda) \cap \mathcal{V}$.
   (a) Докажите, что этот срез равен множеству $V_\lambda \times \{\lambda\}$, где $V_\lambda = \{v \in k^n : \lambda v \in V\}$. Докажите, что V_λ — аффинное многообразие.
   (b) Докажите, что $V_1 = V$ и что V_λ изоморфно V при $\lambda \neq 0$. Указание: рассмотрите полиномиальное отображение, переводящее x в λx, где $x \in k^n$.
   (c) Пусть $k = \mathbb{R}$ или $\mathbb{C}$, и пусть $\lambda \neq 0$ — малое число. Объясните, почему V_λ представляет собой «увеличение» многообразия V в $1/\lambda$ раз. Покажите, что V_λ при $\lambda \to 0$ показывает, как ведет себя V в окрестности начала координат.
   (d) Используя (6), докажите, что $V_0 = C_0(V)$. Объясните это равенство в терминах «увеличения» из части (c).

11. Пусть $p \in V \subset k^n$. Докажите, что $C_p(V) \subset T_p(V)$.

12. Пусть k — бесконечное поле и $V \subset k^n$ — линейное подпространство. Докажите, что V неприводимо. Указание: в упр. 7 к § 1 было показано, что это так, если V — координатное подпространство; теперь выберите подходящий базис в k^n.

13. Пусть $W \subset \mathbb{P}^{n-1}(\mathbb{C})$ — проективное многообразие и $C_W \subset \mathbb{C}^n$ — его аффинный конус.
   (a) Докажите, что касательный конус многообразия C_W в начале координат равен C_W.
   (b) Докажите, что начало координат является гладкой точкой конуса C_W в том и только том случае, когда W является проективным линейным подпространством в $\mathbb{P}^{n-1}(\mathbb{C})$. Указание: используйте следствие 9.

В упр. 14–17 мы изучим «раздутие» многообразия V в точке $p \in V$. Процесс раздутия определяет отображение многообразий $\pi : \widetilde{V} \to V$, такое, что вне точки p многообразия V и $\widetilde{V}$ одинаковы, но в p многообразие $\widetilde{V}$ может быть значительно больше, чем V (в зависимости от вида касательного конуса $C_p(V)$).

14. Пусть k — произвольное поле. В § 5 гл. 8 мы изучали многообразия в $\mathbb{P}^{n-1} \times k^n$, где $\mathbb{P}^{n-1} = \mathbb{P}^{n-1}(k)$. Пусть $y_1, \ldots, y_n$ — однородные координаты на $\mathbb{P}^{n-1}$, а $x_1, \ldots, x_n$ — координаты на k^n. Тогда $(y_1, \ldots, y_n)$-однородные полиномы $x_i y_j - x_j y_i$ (см. § 5 гл. 8) определяют многообразие $\Gamma \subset \mathbb{P}^{n-1} \times k^n$. Это многообразие имеет ряд интересных свойств.
   (a) Пусть $(p, q) \in \mathbb{P}^{n-1} \times k^n$. Докажите (рассматривая p в однородных, а q в обычных координатах), что $(p, q) \in \Gamma$ в том и только том случае, когда $q = tp$ для некоторого $t \in k$ (t может быть нулем).
   (b) Пусть $q \neq 0$ в k^n. Докажите, что $(\mathbb{P}^{n-1} \times \{q\}) \cap \Gamma$ состоит из единственной точки (q, q), где первое q — это точка в $\mathbb{P}^{n-1}$ с однородными координатами, определенными точкой $q \in k^n - 0$. Пусть $q = 0$. Тогда докажите, что $(\mathbb{P}^{n-1} \times \{q\}) \cap \Gamma = \mathbb{P}^{n-1} \times \{0\}$.
   (c) Пусть $\pi : \Gamma \to k^n$ — отображение проекции. Докажите, что прообраз $\pi^{-1}(q)$ состоит из одной точки, если $q \neq 0$. Если же $q = 0$, то $\pi^{-1}(0)$ изоморфно $\mathbb{P}^{n-1}$. Таким образом, мы можем рассматривать Γ как многообразие, полученное удалением начала координат из k^n и вклеиванием вместо него $\mathbb{P}^{n-1}$.
   (d) Чтобы понять, что из себя представляет $\mathbb{P}^{n-1} \times \{0\} \subset \Gamma$, рассмотрим прямую L в k^n, проходящую через начало координат, с параметризацией tv. Докажите, что точки $(v, tv) \in \mathbb{P}^{n-1} \times k^n$ принадлежат Γ и, следовательно, описывают кривую $\widetilde{L} \subset \Gamma$. Рассмотрите, в какой точке $\widetilde{L}$ пересекает $\mathbb{P}^{n-1} \times \{0\}$, и выведите отсюда, что разные прямые, проходящие через начало координат в k^n, определяют разные точки в $\pi^{-1}(0)$. Таким образом, в отличие от k^n многообразие Γ отделяет друг от друга касательные направления в начале координат. Мы называем $\pi : \Gamma \to k^n$ *раздутием* пространства k^n в нуле.

15. Это упражнение является продолжением упр. 14. Пусть $V \subset k^n$ — многообразие, содержащее начало координат, и пусть начало координат не является неприводимой компонентой многообразия V. Мы хотим определить раздутие многообразия V в нуле. Пусть $\Gamma \subset \mathbb{P}^{n-1} \times k^n$ определено, как в предыдущем упражнении. Тогда $\widetilde{V} \subset \Gamma$ определено как наименьшее многообразие в $\mathbb{P}^{n-1} \times k^n$, содержащее $(\mathbb{P}^{n-1} \times (V - \{0\})) \cap \Gamma$. Пусть $\pi : \Gamma \to k^n$ — отображение проекции. Докажите, что $\pi(\widetilde{V}) = V$. Указание: докажите сначала, что $\widetilde{V} \subset \mathbb{P}^{n-1} \times V$.

Это упражнение показывает, что существует отображение $\pi : \widetilde{V} \to V$, которое называется *раздутием* многообразия V в нуле. В упр. 14 было доказано, что $\pi^{-1}(q)$ состоит из единственной точки, если $q \neq 0$. В упр. 16 мы опишем $\pi^{-1}(0)$ в терминах касательного конуса $C_0(V)$.

16. Пусть $V \subset k^n$ — многообразие, содержащее начало координат. Предположим, что начало координат не является неприводимой компонентой многообразия V. Мы знаем, что касательный конус $C_0(V)$ является аффинным конусом некоторого проективного многообразия $W \subset \mathbb{P}^{n-1}$. Назовем W *проективизированным касательным конусом* многообразия V в нуле. Мы хотим показать, что $\pi^{-1}(0) = W \times \{0\}$, где π определено в упр. 15.
   (a) Пусть 0 не является неприводимой компонентой многообразия V. Докажите, что поле k бесконечно и что V является замыканием Зарисского множества $V - \{0\}$.
   (b) Пусть $g \in k[y_1, \ldots, y_n, x_1, \ldots, x_n]$. Докажите, что $g \in \mathbf{I}(\widetilde{V})$ в том и только том случае, когда $g(tq, q) = 0$ для всех $q \in V - \{0\}$ и всех $t \in k - \{0\}$. Указание: примените п. (a) упр. 14.
   (c) Далее, докажите, что $g \in \mathbf{I}(\widetilde{V})$ в том и только том случае, когда $g(tq, q) = 0$ для всех $q \in V$ и всех $t \in k$. Указание: используйте пп. (a) и (b).
   (d) Объясните, почему идеал $\mathbf{I}(\widetilde{V})$ порожден $(y_1, \ldots, y_n)$-однородными полиномами.
   (e) Пусть $g = \sum_\alpha g_\alpha(y_1, \ldots, y_n) x^\alpha \in \mathbf{I}(\widetilde{V})$. Из п. (d) следует, что g_α мы можем считать однородными полиномами одной и той же полной степени d. Пусть
   $$f(x_1, \ldots, x_n) = \sum_\alpha g_\alpha(x_1, \ldots, x_n) x^\alpha.$$
   Докажите, что $f \in \mathbf{I}(V)$. Указание: сначала докажите, что $f(x_1, \ldots, x_n) t^d = g(tx_1, \ldots, tx_n, x_1, \ldots, x_n)$, а потом примените п. (c).
   (f) Докажите, что $W \times \{0\} \subset \widetilde{V} \cap (\mathbb{P}^{n-1} \times \{0\})$. Указание: достаточно доказать, что $g(v, 0) = 0$ для всех $g \in \mathbf{I}(\widetilde{V})$ и $v \in C_0(V)$. В обозначениях п. (e) имеем $g(v, 0) = g_0(v)$. Если $g_0 \neq 0$, то докажите, что $g_0 = f_{\min}$, где f — полином, определенный в п. (e).
   (g) Докажите, что $\widetilde{V} \cap (\mathbb{P}^{n-1} \times \{0\}) \subset W \times \{0\}$. Указание: докажите, что если $f = f_l + \ldots + f_d \in \mathbf{I}(V)$, где $f_l = f_{\min}$, и g является остатком от деления полинома $t^l f$ на $tx_1 - y_1, \ldots, tx_n - y_n$, то g не зависит от t и $g \in \mathbf{I}(\widetilde{V})$; затем найдите $g(v, 0)$, используя пп. (e) и (f).

Прямая, принадлежащая касательному конусу, может рассматриваться как направление приближения к началу координат по точкам из V. Поэтому проективизированный касательный конус описывает все такие пути. Равенство $\pi^{-1}(0) = W \times \{0\}$ означает, что каждое

такое направление определяет свою точку в раздутии. Обратите внимание, что этот факт является глубоким обобщением упр. 14.

17. Пусть k — алгебраически замкнутое поле, а многообразие $V = \mathbf{V}(f_1, \ldots, f_s) \subset k^n$ содержит начало координат.
   (a) Анализируя п. (g) предыдущего упражнения, объясните, как найти определяющие уравнения раздутия $\widetilde{V}$.
   (b) Найдите раздутие в начале координат многообразия $\mathbf{V}(y^2 - x^2 - x^3)$ и объясните, как ваш ответ согласуется с первым рисунком в примере 1.
   (c) Найдите раздутие в начале координат многообразия $\mathbf{V}(y^2 - x^3)$.

   Обратите внимание, что раздутия в пп. (b) и (c) — гладкие кривые. В общем случае раздутие является важным инструментом *десингуляризации* многообразий с особыми точками.

Приложение A
Некоторые понятия из алгебры

В этом приложении собраны строгие определения понятий и точные формулировки утверждений из алгебры, используемых в книге. Читателю, знакомому с абстрактной алгеброй, большая часть изложенного здесь материала хорошо известна. Если же читатель с этим сталкивается впервые, то он должен иметь в виду, что абстрактные понятия, определенные в этом приложении, используются в книге в весьма частных ситуациях.

§ 1. Поля и кольца

Сначала мы дадим строгое определение поля.

Определение 1. *Полем* называется множество k с двумя заданными на нем бинарными операциями $\cdot$ и $+$, которые удовлетворяют следующим условиям:

(i) $(a + b) + c = a + (b + c)$ и $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для всех $a, b, c \in k$ (ассоциативность);
(ii) $a + b = b + a$ и $a \cdot b = b \cdot a$ для всех $a, b \in k$ (коммутативность);
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ для всех $a, b, c \in k$ (дистрибутивность);
(iv) существуют элементы $0, 1 \in k$, называемые нулем и единицей соответственно, такие, что $a + 0 = a \cdot 1 = a$ для любого $a \in k$;
(v) для любого элемента $a \in k$ существует элемент $b \in k$, такой, что $a + b = 0$ (существование аддитивного обратного);
(vi) для любого элемента $a \in k, a \neq 0$, существует элемент $c \in k$ такой, что $a \cdot c = 1$ (существование мультипликативного обратного).

Мы, главным образом, работаем с полями $\mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$. Кроме того, в упражнениях к § 1 упоминается поле $\mathbb{F}_2$, состоящее из двух

элементов 0 и 1. В книге рассматриваются также и более сложные поля. Например, в § 3 гл. 1 мы определяем поле $k(t_1, \ldots, t_m)$ рациональных функций от переменных $t_1, \ldots, t_m$ с коэффициентами из k, а в § 5 гл. 5 — поле $k(V)$ рациональных функций на неприводимом многообразии V.

Если мы не требуем существования мультипликативного обратного, то получаем определение коммутативного кольца.

Определение 2. *Коммутативным кольцом* называется множество R с двумя бинарными операциями $\cdot$ и $+$, которые удовлетворяют следующим условиям:

(i) $(a+b)+c = a+(b+c)$ и $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для всех $a, b, c \in R$ (ассоциативность);
(ii) $a + b = b + a$ и $a \cdot b = b \cdot a$ для всех $a, b \in R$ (коммутативность);
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ для всех $a, b, c \in R$ (дистрибутивность);
(iv) существуют элементы $0, 1 \in R$, называемые нулем и единицей соответственно, такие, что $a + 0 = a \cdot 1 = a$ для любого $a \in R$;
(v) для любого элемента $a \in R$ существует элемент $b \in R$, такой, что $a + b = 0$ (существование аддитивного обратного).

Любое поле, разумеется, является коммутативным кольцом. Другими примерами коммутативных колец служат кольцо целых чисел $\mathbb{Z}$ и кольцо полиномов $k[x_1, \ldots, x_n]$. Последнее и есть основной предмет рассмотрения этой книги. В гл. 5 мы строим еще два коммутативных кольца: координатное кольцо $k[V]$ полиномиальных функций на аффинном многообразии V и факторкольцо $k[x_1, \ldots, x_n]/I$ по идеалу $I \subset k[x_1, \ldots, x_n]$.

Особым классом коммутативных колец являются *области целостности*.

Определение 3. Коммутативное кольцо R называется *областью целостности*, если из равенства $a \cdot b = 0$, где $a, b \in R$, следует, что или $a = 0$, или $b = 0$.

Любое поле является областью целостности. Кольцо полиномов $k[x_1, \ldots, x_n]$ также является областью целостности. В гл. 5 доказывается, что координатное кольцо $k[V]$ многообразия V является областью целостности в том и только том случае, когда V неприводимо.

Наконец, дадим определение идеала в случае произвольного кольца.

Определение 4. Пусть R — коммутативное кольцо. Подмножество $I \subset R$ называется *идеалом*, если выполнены следующие условия:

(i) $0 \in I$;
(ii) если $a, b \in I$, то $a + b \in I$;
(iii) если $a \in I$, а $b \in R$, то $b \cdot a \in I$.

Обратите внимание, что это определение является обобщением определения идеала, данного в § 4 гл. 1.

§ 2. Группы

Группа определяется следующим образом.

Определение 1. *Группой* называется множество G с заданной на нем бинарной операцией $\cdot$, которая удовлетворяет следующим условиям:

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для всех $a, b, c \in G$ (ассоциативность);
(ii) существует элемент $1 \in G$, называемый единицей, такой, что $1 \cdot a = a \cdot 1 = a$ для любого $a \in G$;
(iii) для любого элемента $a \in G$ существует элемент $b \in G$, такой, что $a \cdot b = b \cdot a = 1$ (существование обратного элемента).

Простой пример группы представляет собой множество целых чисел $\mathbb{Z}$ с операцией сложения. Обратите внимание, что $\mathbb{Z}$ не образует группу по умножению. Более интересный пример дает линейная алгебра. Пусть k — некоторое поле. Рассмотрим множество

$$\mathrm{GL}(n, k) = \{A : A \text{ — обратимая } n \times n\text{-матрица с элементами из } k\}.$$

Так как произведение двух обратимых матриц является обратимой матрицей, то матричное умножение — бинарная операция на $\mathrm{GL}(n, k)$. Легко проверить, что все аксиомы группы выполнены.

В качестве последнего примера группы рассмотрим множество

$$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} : \sigma \text{ — взаимно однозначное отображение «на»}\},$$

где n — положительное целое число. Операция композиции функций превращает S_n в группу. Так как элементы $\sigma \in S_n$ можно рассматривать как перестановки чисел от 1 до n, то S_n называется *группой перестановок*. Заметим, что S_n содержит $n!$ элементов.

Наконец, дадим определение подгруппы.

Определение 2. Пусть G — некоторая группа. Подмножество $H \subset G$ называется *подгруппой*, если выполнены следующие условия:

(i) $1 \in H$;
(ii) если $a, b \in H$, то $a \cdot b \in H$;
(iii) если $a \in H$, то $a^{-1} \in H$.

В гл. 7 мы рассматриваем конечные подгруппы группы $\mathrm{GL}(n, k)$.

§ 3. Определители

Теперь мы дадим формулу для вычисления определителя $n \times n$-матрицы. Начнем с определения *знака* перестановки (см. определение группы S_n).

Определение 1. Пусть $\sigma \in S_n$ и P_σ — матрица, полученная перестановкой столбцов единичной $n \times n$-матрицы в соответствии с перестановкой σ. Тогда *знаком* перестановки σ называется

$$\mathrm{sgn}(\sigma) = \det(P_\sigma).$$

Заметим, что мы можем преобразовать P_σ в единичную матрицу с помощью попарных перестановок столбцов. При перестановке двух столбцов определитель меняет знак. Следовательно, $\mathrm{sgn}(\sigma) = \pm 1$. Определитель может быть вычислен следующим образом.

Предложение 2. *Пусть $A = (a_{ij})$ — произвольная $n \times n$-матрица. Тогда*

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

Доказательство. Доказательство можно найти в любом учебнике по линейной алгебре.

Эта формула играет ключевую роль в нашем рассмотрении результантов (см. предложение 4 из § 5 гл. 3).

Нам нужна формула решения системы из n линейных уравнений с n неизвестными. В матричном виде такая система может быть записана следующим образом:

$$AX = B,$$

где $A = (a_{ij})$ есть $n \times n$-матрица коэффициентов системы, B — вектор-столбец, а X — вектор-столбец, элементами которого являются неизвестные $x_1, \dots, x_n$. Если A обратима, то система имеет единственное решение $X = A^{-1}B$. В этом случае можно вывести явную формулу для решения системы.

Предложение 3 (правило Крамера). *Пусть дана система линейных уравнений $AX = B$, где A — обратимая матрица. Тогда единственное решение системы дается следующей формулой:*

$$x_i = \frac{\det(M_i)}{\det(A)},$$

где M_i — матрица, полученная из матрицы A заменой ее i-го столбца столбцом B.

Доказательство. Доказательство этого утверждения можно найти в любом учебнике по линейной алгебре.

Это предложение мы используем для доказательства некоторых важных свойств результантов (см. предложение 5 из § 5 гл. 3).

Приложение B

Псевдокод

Псевдокоды используются в математике и информатике для описания алгоритмов. Здесь мы рассмотрим псевдокод, применяемый в этой книге. Если читатель знаком с языком Паскаль, то он заметит сходство Паскаля с нашим псевдокодом. Это не случайно, так как языки программирования и созданы для описания алгоритмов. В самом деле, названия языка ALGOL, одного из предшественников Паскаля, означает ALGOrithmic Language (алгоритмический язык). Синтаксис, или «правила грамматики» нашего псевдокода не столь жесткие, как в языках программирования, потому что речь не идет о компьютерной реализации наших алгоритмов. Тем не менее, псевдокод служит той же цели, что и языки программирования.

Как указано в тексте книги, алгоритм — это набор инструкций для выполнения определенных численных или символьных вычислений. Алгоритм имеет *вход* или *входные данные*, т. е. информацию, которую он обрабатывает, и *выход* — результат его вычислений. На каждом шаге очередная операция полностью определена текущим состоянием алгоритма. Наконец, алгоритм прекращает работу после конечного числа шагов.

В то время как простой алгоритм представляет собой последовательность инструкций, выполняемых по очереди, большинство алгоритмов содержит следующие специальные структурные компоненты:

- Структуры повторения, которые позволяют неоднократно повторять одну и ту же последовательность инструкций. Такие структуры называются *циклами*. Решение о том, повторять или нет определенную последовательность инструкций, может быть осуществлено различными способами, и наш псевдокод содержит различные типы структур повторения, предназначенных для использования в различных ситуациях.
- Структуры условного перехода, которые позволяют выполнять разные наборы инструкций в зависимости от обстоятельств.

Эти структуры, а также другие компоненты псевдокода будут описаны ниже.

§ 1. Вход, выход, переменные и константы

Вход и выход алгоритма указывается в двух строчках перед началом собственно алгоритма. Входу и выходу присвоены имена в соответствии с правилами математических обозначений. Иногда мы не указываем *тип* данных входа и выхода. В этом случае содержание входа и выхода должно быть ясным из контекста. Переменные (т. е. информация, используемая в процессе выполнения алгоритма) также имеют свои имена. Мы свободно вводим новые переменные в ходе алгоритма. Их типы определены самим процессом вычисления. Так, например, если переменная a появляется в некоторой инструкции алгоритма, а потом a полагается равной некоторому полиному, то, начиная с этого места, a рассматривается как полином. Для описания численных констант используются обычные правила математической записи. Два слова *true* и *false* используются для обозначения истинности или ложности утверждений. Эти слова ведут себя так же, как булевы константы true и false в Паскале.

§ 2. Операторы присваивания

Так как наши алгоритмы предназначены для описания математических операций, то, пожалуй, наиболее часто встречающимся типом инструкций является оператор *присваивания*. Правило записи этого оператора таково:

<переменная> := <выражение>.

Символ := тот же, что и для оператора присваивания в Паскале. Смысл этого оператора таков. Сначала мы *вычисляем* значение правой части оператора присваивания, используя хранимые в памяти значения переменных, содержащихся в выражении. Результат вычисления хранится в памяти под именем переменной из левой части оператора. Если под этим именем хранилось какое-то другое значение, то оно *стирается* и *заменяется* вычисленным новым. Пусть, например, переменная i имеет численное значение 3, и мы выполняем присваивание

$$i := i + 1.$$

Тогда вычисляется значение $3 + 1 = 4$ и сохраняется в памяти под именем i, т. е. после выполнения оператора i равно 4.

§ 3. Операторы цикла

В наших алгоритмах используется три типа структур повторения. Они аналогичны соответствующим структурам в Паскале. Наиболее общая и часто встречающаяся структура повторения в наших алгоритмах — это структура WHILE. Она записывается так:

WHILE <условие> DO <действие>.

Здесь под <действием> понимается последовательность инструкций. В структуре WHILE «действие» — это и есть последовательность инструкций, которая повторяется. Мы всегда записываем это действие с отступом. *Конец* действия обозначен возвращением на тот же уровень отступа, на котором находится слово WHILE.

<Условие> после слова WHILE — это утверждение о значениях переменных и т. п., которое может быть истинным или ложным на каждом шаге алгоритма. Например, условие

$i \leq s$ AND деление произошло = false

имеется в цикле WHILE в алгоритме деления из § 3 гл. 2.

Когда в процессе выполнения алгоритма мы доходим до цикла WHILE, то определяем истинность или ложность условия. Если условие *истинно*, то действие выполняется один раз, и мы снова возвращаемся к проверке условия. Если оно по-прежнему истинно, то действие выполняется еще раз. Таким образом, действие будет выполняться, пока условие остается истинным. Если условие становится ложным (в некоторый момент выполнения действия), то выполнение действия заканчивается, и только после этого происходит прекращение выполнения цикла. Другими словами, в цикле WHILE условие проверяется *перед* выполнением действия, и это условие должно быть *истинным*, чтобы действие повторялось.

Вторая структура повторения, которую мы используем в книге несколько раз, — это структура REPEAT, которая записывается следующим образом:

REPEAT <действие> UNTIL <условие>.

Смысл структуры ясен из ее описания. В отличие от структуры WHILE условие в REPEAT указывает, когда надо *остановиться*. Другими словами, действие повторяется пока условие *ложно*. Кроме того, действие в REPEAT выполняется по крайней мере один раз, так как проверка условия происходит *после* выполнения действия. Как и в записи цикла WHILE, инструкции действия в REPEAT записываются с отступом.

Последняя структура повторения аналогична циклу FOR Паскаля. Она записывается так:

FOR each s in S DO <действие>

и означает: «выполняй указанное действие для каждого элемента $s \in S$». Здесь S — конечное множество объектов, и характер действия обычно зависит от того, какие s мы рассматриваем. Порядок, в котором записаны элементы из S, не имеет значения. В отличие от предыдущих структур повторения структура FOR выполняет действие фиксированное количество раз (столько раз, сколько элементов содержит S). Цикл FOR в Паскале применяется в том случае, когда S — множество последовательных целых чисел, такое, как $S = \{1, \ldots, n\}$. Тогда действие выполняется для каждого s между 1 и n.

§ 4. Условный оператор

Мы используем только один тип условного оператора, который записывается так:

IF <условие> THEN <действие1> ELSE <действие2>.

Смысл этого оператора состоит в следующем. Если условие истинно в тот момент, когда выполняется IF, то выполняется действие1 (один раз). В противном случае (когда условие ложно), выполняется действие2 (также один раз). Инструкции в действии1 и действии2 пишутся с отступом, и слово ELSE отделяет эти две последовательности инструкций. Конец действия2 обозначен возвращением на тот уровень отступа, на котором записаны слова IF и ELSE.

В общем случае истинность или ложность условия определяет, какое действие будет выполнено. В некоторых случаях мы *опускаем* ELSE и действие2. Этот тип условного оператора имеет следующий смысл:

IF <условие> THEN <действие1> ELSE <ничего не делать>.

Приложение C

Системы компьютерной алгебры

В этом приложении мы рассмотрим несколько систем компьютерной алгебры, которые могут быть использованы для решения упражнений. Мы достаточно подробно обсудим системы AXIOM, Maple, Mathematica и REDUCE и упомянем некоторые другие системы. Все они представляют собой удивительно мощные пакеты программ, и наше краткое обсуждение, безусловно, не воздает им должного.

Важно отметить, что мы *не пытаемся* дать что-то вроде общего введения для пользователя обсуждаемых систем — это задача специальных курсов по таким системам. В частности, мы предполагаем, что читатель знаком с тем:

- Как входить в систему и выходить из нее, как вводить команды и полиномы. Некоторые системы требуют ставить точку с запятой в конце команды (Maple и REDUCE, например), а другие — нет. Работа некоторых систем (Mathematica, например) зависит от типа предлагаемой задачи, а работа других — нет. В некоторых системах умножение обозначается звездочкой (AXIOM), а в других — нет.
- Как обращаться к предыдущим командам и как сохранить результаты в файле. Последнее может оказаться важным, особенно если ответ занимает более чем один компьютерный экран. Читатель должен уметь сохранить ответ в файле и распечатать его для дальнейшего изучения.
- Как работать со списками. Например, при вычислении базиса Грёбнера мы вводим список полиномов, а система выдает список элементов базиса Грёбнера для идеала, порожденного полиномами первого списка. Читатель должен уметь найти длину списка и извлечь любой полином из него.
- Как присваивать имена объектам. Часто при работе со сложными данными бывает удобным использовать имена полиномов, списков полиномов, списков переменных и т. п.

Если эта книга используется в учебном курсе с практическими занятиями, то мы бы советовали преподавателю на первом же практическом занятии разъяснить указанные вопросы применительно к конкретной используемой системе компьютерной алгебры.

§ 1. AXIOM

Система AXIOM — это коммерческая версия системы SCRATCHPAD, которая разрабатывалась фирмой IBM на протяжении долгого времени. Здесь мы рассматриваем версию 2.0. Для нас наиболее важными командами AXIOM являются `normalForm` (команда, реализующая алгоритм деления) и `groebner` (команда, реализующая алгоритм вычисления базиса Грёбнера).

В AXIOM каждый объект имеет свой тип. В частности, это свойство системы влияет на работу с мономиальными упорядочениями: порядок является типом. Пусть, например мы используем lex-упорядочение на $\mathbb{Q}[x,y,z]$ с $x > y > z$. Для этого мы вводим команду `DMP([x,y,z],FRAC INT)` (напоминаем, что списки в AXIOM заключены в квадратные скобки `[...]`). Здесь `DMP` означает «распределенный полином от нескольких переменных» (Distributed Multivariate Polynomial), а `FRAC INT` означает «отношения целых чисел», т. е. рациональные числа (fractions of integer). Аналогично, grevlex-упорядочение на $\mathbb{Q}[x,y,z]$ с $x > y > z$ вводится командой `HDMP([x,y,z], FRAC INT)`, где `HDMP` означает «однородный распределенный полином от нескольких переменных» (Homogeneous Distributed Multivariate Polynomial). В конце параграфа мы объясним, как задать grlex-упорядочение.

В качестве примера рассмотрим процесс деления в AXIOM полинома $x^3 + 3y^2$ на $x^2 + y$ и $x + 2xy$ при использовании grevlex-упорядочения с $x > y$. Сначала введем полиномы и объявим их типы:

```
-> f:HDMP([x,y],FRAC INT):=x^3+3*y^2
-> g:HDMP([x,y],FRAC INT):=x^2+y
-> h:HDMP([x,y],FRAC INT):=x+2*x*y
```

Здесь `->` — это приглашение AXIOM, а двоеточие — объявление типа. Можно дать команде `HDMP([x,y],FRAC INT)` имя и в дальнейшем работать только с ним). Остаток вычисляется с помощью команды

```
-> normalForm(f,[g,h])
```

Выходом является остаток от деления `f` на `g,h`. В общем случае синтаксис этой команды таков:

```
-> normalForm(poly,polylist),
```

где `poly` — это полином, который мы делим на полиномы из списка `polylist` (при условии, что все типы корректно заданы).

То же самое деление с использованием lex-упорядочения с $x > y$ реализуется следующей последовательностью команд:

```
-> Lex:=DMP([x,y],FRAC INT)
```

(мы даем команде `DMP([x,y],FRAC INT)` имя `Lex`),

```
-> normalForm(f::Lex,[g::Lex,h::Lex])
```

Здесь команда `::` преобразует один тип в другой.

Синтаксис команды `groebner` таков:

```
-> groebner(polylist)
```

Она вычисляет базис Грёбнера идеала, порожденного полиномами из списка `polylist`. Он оказывается редуцированным базисом Грёбнера в смысле § 7 гл. 2. Так, например, команда

```
-> gb:=groebner([g,h])
```

где `g`, `h` определены выше, находит список (с именем `gb`) элементов базиса Грёбнера идеала $\langle x^2+y, x+2xy\rangle \subset \mathbb{Q}[x,y]$ по отношению к grevlex-упорядочению с $x > y$. Если вам необходима информация о промежуточных шагах вычисления, то нужно в команду `groebner` включить опции `"redcrit"` и `"info"`. Так, например, команда

```
-> groebner([g,h],"redcrit")
```

напечатает все остатки S-полиномов (в этом случае один остаток), порожденные в ходе вычисления. Опция `"info"` позволяет получить еще больше информации.

AXIOM способна работать не только над полем рациональных чисел. Для этого нужно вместо `FRAC INT` объявить другой тип. Например, при вычислении базисов Грёбнера над полем рациональных функций (от полиномов с целыми коэффициентами) мы объявляем тип `FRAC POLY INT`. Рассмотрим в качестве примера вычисление базиса Грёбнера идеала $\langle vx^2+y, uxy+y^2\rangle \subset \mathbb{Q}(u,v)[x,y]$ по отношению к lex-упорядочению с $x > y$. Это вычисление реализуется следующей последовательностью команд:

```
-> m:List DMP([x,y],FRAC POLY INT)
-> m:=[v*x^2+y,u*x*y+y^2]
-> groebner(m)
```

Обратите внимание, что здесь использован другой метод объявления типа полинома.

Вот еще примеры объявления полей: команда `FRAC COMPLEX INT` объявляет поле рациональных гауссовских чисел $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$ (обратите внимание, что AXIOM обозначает $i = \sqrt{-1}$ через `%i`); команда `PrimeField(p)` объявляет конечное поле с p элементами (p — простое число). Базис Грёбнера можно вычислять над любым конечным полем. Методы работы AXIOM с конечными полями объяснены в разд. 8.11 книги JENKS, SUTOR (1992). Возможность просто «вставить» объявление поля в команду, вычисляющую базис Грёбнера, является показателем силы AXIOM.

Кроме возможности работать со списком полиномов, AXIOM позволяет объявить список полиномов идеалом. Синтаксис этой команды таков:

```
-> ideal polylist
```

где `polylist` — список полиномов нужного типа. Это объявление весьма полезно, так как AXIOM содержит команды операций над идеалами, включая:

- `intersect` для вычисления пересечения списка идеалов;
- `zeroDim?` для выяснения, конечно или бесконечно число решений системы над алгебраически замкнутым полем (см. § 3 гл. 5);
- `dimension` для вычисления размерности многообразия, определенного идеалом;
- `prime?` для выяснения, прост ли заданный идеал;
- `radical` для вычисления радикала заданного идеала;
- `primaryDecomp` для вычисления примарного разложения заданного идеала.

Примеры использования этих и других команд системы AXIOM можно найти в разделе 8.12 книги JENKS, SUTOR (1992). Следует упомянуть команды `leadingMonomial` и `leadingCoefficient` для определения старшего члена и старшего коэффициента данного полинома.

Все эти команды требуют предварительного задания типа используемого полинома. Но если вам нужно только найти базис Грёбнера по отношению к lex или grevlex над $\mathbb{Q}$, то можно использовать команды `lexGroebner` и `totalGroebner`. Например, команда

```
-> lexGroebner([2*x^ 2+y,2*y^ 2+x],[x,y])
```

вычисляет редуцированный (с точностью до констант) базис Грёбнера идеала $\langle 2x^2+y, 2y^2+x\rangle \subset \mathbb{Q}[x,y]$ для lex-упорядочения с $x > y$. Обратите внимание, что мы не объявляли тип полиномов заранее — команда `lexGroebner` позаботилась об этом. То же самое можно сказать о `totalGroebner` — команде вычисления базиса Грёбнера для grevlex-упорядочения.

В заключение этого параграфа объясним, как в AXIOM работать с grlex-упорядочением. В AXIOM имеется все необходимое, но чтобы собрать все это воедино, нужно немного потрудиться. Пусть мы хотим объявить grlex-упорядочение на $\mathbb{Q}[x,y]$ с $x > y$. Для этого нужны команды

```
-> )set expose add constructor GDMP
-> )set expose add constructor ODP
-> Grlex:=GDMP([x,y],FRAC INT,ODP(2,NNI,totalLex$ORDFUNS
   (2,NNI)))
```

Основная идея состоит в том, что команда GDMP (General Distributed Multivariate Polynomial, т. е. обобщенный распределенный полином от нескольких переменных) позволяет задать тип *произвольного* мономиального упорядочения, а функция totalLex упорядочивает мономы в соответствии с grlex-упорядочением с $x > y$. Объявляя тип полинома как Grlex, мы теперь можем вычислить базис Грёбнера для grlex-упорядочения с $x > y$. Соблюдайте осторожность: преобразование типа не работает между Grlex и типами, объявленными командами DMP и HDMP, хотя можно написать программу преобразования типа. Используя методы AXIOM задания пакета, можно самому создать пакет прикладных программ для работы со всеми мономиальными упорядочениями, описанными в упражнениях к § 4 гл. 2, и преобразованиями их друг в друга.

§ 2. Maple

Здесь мы рассматриваем версию 3 системы Maple V. Самым важным для нас является пакет в Maple для работы с базисами Грёбнера. Этот пакет вызывается командой:

```
> with(grobner);
```

(> — это приглашение Maple, и каждый оператор в Maple заканчивается точкой с запятой). После загрузки пакета можно делить полиномы, вычислять базис Грёбнера и производить другие вычисления, описанные далее.

Мономиальное упорядочение в Maple называется «termorder». Из мономиальных упорядочений, рассмотренных в гл. 2, Maple умеет работать с lex и grevlex. Lex-упорядочение называется plex (т. е. чистое (pure) лексиграфическое упорядочение), а grevlex называется tdeg (от «total degree» — полная степень). Не путайте tdeg и grlex.

Так как мономиальное упорядочение зависит от порядка переменных, Maple должен знать termorder (plex или tdeg) *и* список переменных. Например, если вы хотите использовать lex с $x > y > z$, то вам необходимо ввести plex и список [x,y,z] (напомним, что списки в Maple заключаются в квадратные скобки [...]). Если termorder не введен, то по умолчанию используется tdeg. Список переменных должен быть введен обязательно (это нельзя сделать по умолчанию).

Наиболее часто используемые команды из пакета Грёбнер — это normalf (алгоритм деления) и gbasis (вычисление базиса Грёбнера). Имя normalf означает «нормальная форма». Эта команда имеет следующий синтаксис:

```
> normalf(f,polylist,varlist,termorder);
```

Результатом является остаток от деления полинома f на полиномы из списка polylist при использовании мономиального упорядочения, заданного termorder и varlist. Например, деление полинома $x^3 + 3y^2$ на $x^2 + y$ и $x + 2xy$ для grevlex-упорядочения с $x > y$ осуществляется следующей командой:

```
> normalf(x^3+3*y^2[x^2+y,x+2*x*y],[x,y]);
```

Мы опустили указание termorder, так как tdeg используется по умолчанию. Основным полем здесь является $\mathbb{Q}$. Обратите внимание, что normalf не выдает частных в алгоритме деления.

Команда gbasis означает, разумеется, «базис Грёбнера». Она имеет следующий синтаксис:

```
> gbasis(polylist,varlist,termorder);
```

и вычисляет базис Грёбнера идеала, порожденного полиномами из списка polylist по отношению к мономиальному упорядочению, заданному termorder и varlist. Результатом является редуцированный базис Грёбнера (в смысле § 7 гл. 2) с целыми коэффициентами. Например, в результате выполнения команды

```
> gb := gbasis([x^2+y,2*x*y+y^2],[x,y],plex);
```

выдается список (с именем gb) полиномов, которые образуют базис Грёбнера идеала $\langle x^2 + y, 2xy + y^2\rangle \subset \mathbb{Q}[x,y]$ для lex-упорядочения с $x > y$.

Если вы работаете с полиномами с целыми или рациональными коэффициентами и команды normalf и gbasis, то Maple будет считать основным полем поле $\mathbb{Q}$. Обратите внимание, что в Maple нет ограничений на размер коэффициентов. Эта система может также работать с коэффициентами из поля рациональных функций. Если вы хотите объявить некоторую переменную «параметром», то достаточно не упоминать ее в списке переменных. Так, команда

```
> gbasis([v*x^2+y,u*x*y+y^2],[x,y],plex);
```

вычислит базис Грёбнера идеала $\langle vx^2+y, uxy+y^2\rangle \subset \mathbb{Q}(u,v)[x,y]$ для lex-упорядочения с $x>y$. Результатом является редуцированный базис, старшие коэффициенты элементов которого являются полиномами от u, v.

При вычислении базиса Грёбнера над полем рациональных гауссовских чисел $\mathbb{Q}(i)=\{a+bi : a,b\in\mathbb{Q}\}$, где $i=\sqrt{-1}$, могут возникнуть затруднения. В этом случае следует ввести новую переменную j (вместо мнимой единицы) и еще один образующий полином j^2+1. Если исходными переменными являются $x_1,\ldots,x_n$, то теперь следует вычислять базис Грёбнера для такого мономиального упорядочения, когда каждая переменная x_i больше любой степени j. Докажите самостоятельно, что, заменив j на i в ответе, мы получим требуемый базис Грёбнера.

Пакет для вычисления базиса Грёбнера содержит и другие полезные команды:

- `leadmon` для вычисления $\mathrm{LC}(f)$ и $\mathrm{LM}(f)$ для полинома f;
- `spoly` для вычисления S-полинома $S(f,g)$;
- `solvable` для определения, с использованием алгоритма совместимости из § 1 гл. 4, существуют ли решения данной полиномиальной системы над алгебраически замкнутым полем;
- `finite` для определения, с использованием алгоритма конечности из § 3 гл. 5, конечно или бесконечно число решений данной полиномиальной системы над алгебраически замкнутым полем.

Имеется еще команда `solve`, предназначенная для решения (нахождения полного списка решений) систем уравнений. Maple содержит отличную диалоговую систему help, которая позволяет легко освоить команды. Можно ознакомиться также со справочным пособием CHAR ET AL. (1991).

Следует упомянуть, что библиотека содержит еще два полезных пакета. Это пакет «GB», который вычисляет остатки от деления и базисы Грёбнера по модулю простых чисел. Для загрузки этого пакета нужно ввести команды

```
> with(share);
> readshare('mod/GB');
```

Основными командами в этом пакете являются `Normalform` и `GB` для вычисления остатков и базисов Грёбнера над конечными полями с p элементами (p — простое число). Получить информацию об этих командах можно из системы help. Например, команда

```
> help(GB);
```

объяснит, как пользоваться командой `GB`. Интересной опцией этой команды является переменная `infolevel[GB]`. Задав ее значение, можно получать информацию о ходе вычисления базиса Грёбнера (о числе рассмотренных остатков, например, и т. д.).

Другим полезным пакетом является «charsets», упомянутый в § 5 гл. 6. Этот пакет реализует алгоритм Ву—Ритта. Если команда `with(share)` уже введена, то charsets загружается командой

```
> readshare(charsets,algebra);
```

Получить информацию об этой команде можно через help или с помощью файла charsets.tex в соответствующей директории. Этот файл является LaTeX-версией работы WANG (1994a).

Наконец, следует упомянуть о пакете в Maple, написанном Альбертом Лином (Lin) и Филиппом Лустану (Loustaunau) из университета Джорджа Мейсона, который является расширением пакета для базиса Грёбнера. Этот пакет позволяет находить частные (а не только остатки) при делении полиномов и матрицу, позволяющую описывать базис Грёбнера в терминах образующих идеала. Команды этого пакета выполняются довольно медленно (по сравнению с командой `gbasis`), но полезны при решении многих задач из этой книги. Этот пакет может быть получен по адресу David A. Cox, Department of Mathematics and Computer Science, Amherst College, Amherst MA 01002. Получить электронную копию пакета можно по адресу `dac@cs.amherst.edu`.

§ 3. Mathematica

Здесь мы рассматриваем версию 3 системы Mathematica, которая имеет существенно лучшие возможности вычисления базисов Грёбнера, чем предыдущие версии. Эта система не содержит специального пакета для вычисления базисов Грёбнера: основные команды являются частью ядра системы.

Mathematica знает все мономиальные упорядочения, упомянутые в гл. 2. В типичном для Mathematica стиле lex-упорядочение называется `Lexicographic`, grlex — `DegreeLexicographic`, grevlex — `DegreeReverseLexicographic`. Мономиальное упорядочение задается опцией `MonomialOrder`, которую мы опишем ниже. Упорядочение по умолчанию — это lex. Mathematica также может работать с взвешенными упорядочениями, упомянутыми в упражнениях к § 4 гл. 2.

Так как мономиальное упорядочение зависит от порядка переменных, то Mathematica должна знать список переменных. Если, например, вы хотите задать lex-упорядочение с $x>y>z$, то должны ввести список `{x,y,z}` (напоминаем, списки в Mathematica заключены в фигурные скобки).

Для нас наиболее важными командами являются команды `PolynomialReduce` и `GroebnerBasis`. Полезным свойством команды `PolynomialReduce` является то, что она выполняет алгоритм деления из гл. 2, одновременно вычисляя частные. Синтаксис команды таков:

```
In[1]:= PolynomialReduce[f,polylist,varlist,options]
```

(где `In[1]:=` — это приглашение системы). Эта команда вычисляет остаток и частные от деления полинома `f` на полиномы из списка `polylist`, используя мономиальное упорядочение, заданное списком `varlist` и опцией `MonomialOrder`. Например, деление $x^3 + 3y^2$ на $x^2 + y$ и $x + 2xy$ с использованием grlex-упорядочения с $x > y$ осуществляется следующей командой:

```
In[2]:= PolynomialReduce[x^2+3y^2,{x^2+y,x+2*x*y},
        {x,y},MonomialOrder -> DegreeLexicigraphic]
```

Результатом выполнения этой команды будет список из двух элементов, первый элемент — это список частных, а второй — остаток.

Разумеется, команда `GroebnerBasis` вычисляет базис Грёбнера. Ее синтаксис таков:

```
In[3]:= GroebnerBasis[polylist,varlist,options]
```

Эта команда вычисляет базис Грёбнера идеала, порожденного полиномами из списка `polylist`, по отношению к мономиальному упорядочению, заданному опцией `MonomialOrder`, с порядком переменных, определенным списком `varlist`. Результатом является редуцированный базис Грёбнера (в смысле § 7 гл. 2) с целыми коэффициентами. В качестве примера рассмотрим команду

```
In[4]:= gb = GroebnerBasis[{x^2+y,2*x*y+y^2},{x,y}]
```

Результатом будет список (с именем `gb`) полиномов, которые образуют базис Грёбнера идеала $\langle x^2 + y, 2xy + y^2\rangle \subset \mathbb{Q}[x, y]$ для lex-упорядочения с $x > y$. Мы опустили опцию `MonomialOrder`, так как lex-упорядочение принимается по умолчанию.

Если вы задаете полиномы с целыми или рациональными коэффициентами в командах `GroebnerBasis` или `PolynomialReduce`, то Mathematica будет считать, что основным полем является $\mathbb{Q}$. Ограничение на размер коэффициентов отсутствует. Другим возможным полем коэффициентов является поле рациональных гауссовских чисел $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, где $i = \sqrt{-1}$ (обратите внимание, что мнимая единица в Mathematica обозначается через `I`). Для вычисления базиса Грёбнера над конечным полем из p элементов (p — простое число) нужно включить опцию `Modulus -> p` в команду `GroebnerBasis`. (Эту опцию можно применять и в команде `PolynomialReduce`.)

Mathematica может работать с коэффициентами из поля рациональных функций. Для этого переменные, принадлежащие полю («параметры»), должны быть исключены из списка переменных, и опция `CoefficientDomain` должна быть выбрана в качестве `RationalFunctions`. Например, команда

```
In[5]:= GroebnerBasis[{v*x^2+y,u*x*y+y^2},{x,y},
        CoefficientDomain -> RationalFunctions]
```

вычисляет базис Грёбнера идеала $\langle vx^2 + y, uxy + y^2\rangle \subset \mathbb{Q}(u, v)[x, y]$ для lex-упорядочения с $x > y$. Знаменатели в ответе отсутствуют и потому коэффициенты — это полиномы от u, v. (Опцию `CoefficientDomain` можно использовать и в команде `PolynomialReduce`.)

Полезными командами являются также:

- `MonomialList`, которая генерирует список членов полинома в соответствии с заданным упорядочением;
- `Eliminate`, которая исключает переменные из системы полиномиальных уравнений, используя для этого теорему исключения из § 1 гл. 3;
- `Solve`, находящая все решения системы.

Информация о системе Mathematica и примеры ее применения содержатся в книге WOLFRAM (1996).

Наконец, следует упомянуть о пакете, написанном Сьюзен Голдстайн (Goldstine) из Амест-Колледжа, для решения задач, подобных рассмотренным в этой книге. Этот пакет вычисляет базисы Грёбнера, одновременно выдавая информацию о числе ненулевых остатков, решает задачу о принадлежности идеалу, о принадлежности радикалу, о конечности числа решений. Этот пакет работает медленней, чем команда `GroebnerBasis`, но вполне пригоден для решения задач из этой книги. Получить пакет можно по адресу David A. Cox, Department of Mathematics and Computer Science, Amherst College, Amherst MA 01002. Электронную копию пакета можно получить по адресу `dac@cs.amherst.edu`.

§ 4. REDUCE

Мы рассматриваем здесь версию 3.5 системы REDUCE. Для вычисления в REDUCE базиса Грёбнера нужно использовать либо пакет Groebner, либо пакет Cali.

Groebner

Мы опишем версию пакета Groebner, датированную 18 ноября 1994 г. Для загрузки пакета нужно набрать команду

```
1: load_package groebner;
```

(здесь 1: — это приглашение REDUCE, а команды в REDUCE заканчиваются точкой с запятой). После загрузки пакета мы можем осуществлять деление, находить базис Грёбнера и выполнять другие операции, описанные ниже.

В пакете Groebner мономиальное упорядочение называется «term order». REDUCE умеет работать с большинством мономиальных упорядочений, описанных в гл. 2, включая lex, grlex и grevlex. Lex-упорядочение в REDUCE называется `lex`, grlex — `gradlex` и grevlex — `revgradlex`. Пакет Groebner также умеет работать с произведениями упорядочений (см. упр. 10 к § 4 гл. 2), с взвешенными упорядочениями (см. упр. 12 к § 4 гл. 2 — обратите внимание, что в случае взвешенных упорядочений Groebner использует lex, если весовая функция не может определить порядок мономов), а также с более общими упорядочениями, заданными матрицами (см. замечания после упражнений к § 4 гл. 2). Эти упорядочения подробно описаны в разд. 4.10 справочника MELENK, MÖLLER, NEUN (1994).

Порядок членов в Groebner задается командой `torder`. Так как мономиальное упорядочение зависит от порядка переменных, Groebner должен знать *u* порядок членов, *u* список переменных. Другими словами, команда `torder` имеет два аргумента: список переменных и порядок членов. Если, например, вы хотите использовать `grevlex` с $x > y > z$, то надо ввести команду

```
2: torder({x,y,z},revgradlex);
```

(напоминаем, что в REDUCE список заключен в фигурные скобки). В качестве ответа REDUCE напечатает предыдущий порядок членов.

Наиболее часто используемые команды пакета Groebner — это `preduce` (деление полиномов) и `groebner` (вычисление базиса Грёбнера). Имя `preduce` означает «редукция полинома» (polynomial reduce). Эта команда имеет следующий синтаксис:

```
3: preduce(f,polylist);
```

Результатом является остаток от деления полинома `f` на полиномы из списка `polylist` при использовании мономиального упорядочения, определенного командой `torder`. Например, чтобы разделить

$x^3 + 3y^2$ на $x^2 + y$ и $x + 2xy$, используя grlex с $x > y$, нужно ввести следующие команды:

```
4: torder({x,y},gradlex);
5: preduce(x^3+3*y^2,{x^2+y,x+2*x*y},{x,y});
```

В этом примере основным полем является $\mathbb{Q}$. Обратите внимание, что `preduce` не выдает частных.

Команда `groebner`, естественно, вычисляет базис Грёбнера и имеет следующий синтаксис:

```
6: groebner(polylist);
```

Эта команда вычисляет базис Грёбнера идеала, порожденного полиномами из списка `polylist`, по отношению к мономиальному упорядочению, заданному командой `torder`. Результатом является редуцированный базис Грёбнера (в смысле § 7 гл. 2) с целыми коэффициентами. В качестве примера рассмотрим команду:

```
7: gb:=groebner({x^2+y,2*x*y+y^2});
```

Результатом является список полиномов (с именем `gb`), которые образуют базис Грёбнера идеала $\langle x^2 + y, 2xy + y^2\rangle \subset \mathbb{Q}[x, y]$ для порядка членов, заданного командой `torder`.

Если вы работаете с полиномами, коэффициенты которых — целые или рациональные числа, то пакет Groebner будет считать $\mathbb{Q}$ основным полем. Ограничений на размер коэффициентов нет. Можно работать также над полем рациональных гауссовских чисел $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, где $i = \sqrt{-1}$. Для этого надо ввести команду

```
8: on complex;
```

перед вычислением базиса Грёбнера (напоминаем, что REDUCE обозначает $\sqrt{-1}$, через `I`). Аналогично, для работы над конечным полем из p элементов (где p — простое число) надо сначала ввести команду:

```
9: on modular; setmod p;
```

Чтобы вернуться к основному полю $\mathbb{Q}$, нужно ввести команду: `off modular`.

Groebner может работать над полем рациональных функций. Чтобы указать, что некоторая переменная принадлежит основному полю (является «параметром»), достаточно просто исключить ее из списка переменных. Например, команда:

```
10: groebner({v*x^2+y,u*x*y+y^2});
```

вычислит базис Грёбнера идеала $\langle vx^2+y, uxy+y^2\rangle \subset \mathbb{Q}(u,v)[x,y]$ для упорядочения, заданного командой `torder`. Результатом является редуцированный базис Грёбнера, старшими коэффициентами элементов которого являются полиномы от u, v.

Пакет Groebner имеет два «переключателя», которые управляют вычислениями. (В REDUCE *переключатель* — это переменная, которая может принимать два значения `on` и `off`. Примерами переключателей являются `complex` и `modular`.) В процессе вычисления базиса Грёбнера алгоритм должен принимать решения о пути вычислений. И эти решения могут оказывать значительное влияние на объем и сложность вычислений. Мы рассмотрим два переключателя, `groebort` и `gsugar`, которые влияют на характер выполнения команды `groebner`.

В некоторых случаях можно повысить эффективность, изменив порядок переменных, но сохраняя тип упорядочения (т. е. используя, например, lex с $y > x$, вместо $x > y$). Такой алгоритм описан в работе Boege, Gebauer, Kredel (1986). Чтобы использовать этот алгоритм в системе REDUCE, надо ввести команду:

```
11: on groebopt;
```

После завершения работы алгоритма, можно узнать порядок переменных с помощью команды:

```
12: gvarslast;
```

которая выводит список переменных в том порядке, который был использован в вычислениях. В некоторых случаях (например, при исключении неизвестных) порядок переменных менять нельзя. Здесь можно использовать команду `depend`. Пусть, например, переменными являются s, t, x, y, z, и вы хотите исключить s, t. Тогда после ввода команды `groebopt` вы должны ввести команду

```
13: depend s,x,y,z; depend t,x,y,z;
```

После этого команда `groebopt` всегда будет ставить s, t перед x, y, z.

Алгоритм, используемый командой `groebner`, работает с понятием сахарной стратегии (sugar), упомянутым в § 9 гл. 2. Вы можете провести эксперимент и изучить ее влияние на характер вычислений. Здесь надо иметь в виду, что по умолчанию переключатель `gsugar` находится в положении on. Поэтому если вы хотите выключить `sugar`, то перед началом вычислений надо ввести команду `off gsugar`.

Переключатели `groebstat`, `trgroeb` и `trgroebs` для команды `groebner` определяют характер представления информации о ходе вычислений. Подробности можно узнать в разделе 4.2 справочного издания Melenk, Möller, Neun (1994).

Перечислим другие полезные команды пакета Groebner:

- `gsplit` для вычисления $\mathrm{LT}(f)$ и $f - \mathrm{LT}(f)$;
- `gsort`, которая печатает список членов полинома в соответствии с текущим упорядочением;
- `gspoly` для вычисления S-полинома $S(f, g)$;
- `greduce` для вычисления остатка от деления на базис Грёбнера идеала, порожденного вводимыми полиномами;
- `preducet` для вычисления частных делений;
- `gzerodim?` для проверки конечности числа решения (с помощью методов § 3 гл. 5) полиномиальной системы над алгебраически замкнутым полем;
- `glexconvert`, которая базис Грёбнера для произвольного мономиального упорядочения с конечным числом решений над $\mathbb{C}$ преобразует в базис Грёбнера для lex. Такой алгоритм обсуждается в теме 5 приложения D;
- `groesolve` для поиска всех решений полиномиальной системы;
- `idealquotient` для нахождения частного идеалов $I : f$ (здесь используется алгоритм более эффективный, чем тот, который рассматривался в § 4 гл. 4);
- `hilbertpolynomial`, которая вычисляет полином Гильберта данного идеала (как это описано в § 3 гл. 9).

Эти и многие другие команды подробно рассмотрены в справочном издании Melenk, Möller, Neun (1994). Эта работа распространяется вместе с самой системой REDUCE.

Cali

Мы будем рассматривать версию 2.2.1 пакета Cali. Этот пакет использует более сложную математику, чем пакет Groebner, и поэтому он труднее для начинающего. С другой стороны, Cali может производить вычисления (такие, как нахождение радикалов и примарных разложений), которые недоступны пакету Groebner. Загрузка Cali осуществляется командой

```
1: load_package cali;
```

Нельзя загружать Cali и Groebner одновременно — это может привести к конфликту.

В Cali сначала нужно объявить список переменных и задать упорядочение, а только потом вводить полиномы. Это делается командой `setring` с синтаксисом

```
2: setring(vars,weight,order);
```

Здесь `vars` — список переменных, `weight` — список весовых векторов (возможно, пустой), а `order` — это либо `lex`, либо `revlex`. Например

```
3: setring({x,y,z},{},lex);
```

задает lex-упорядочение на $\mathbb{Q}[x,y,z]$, в то время как

```
4: setring({x,y,z},{{1,1,1}},lex);
```

задает grlex-упорядочение на том же кольце. Упорядочение grevlex задается той же командой с заменой `lex` на `revlex`. Можно задать взвешенные, исключающие и матричные упорядочения (см. упр. 12 к § 4 гл. 2). В разд. 2.1 справочного издания GRÄBE (1995) подробно описана работа с мономиальными упорядочениями в рамках Cali.

После того как кольцо задано, можно задавать идеалы списками полиномов. Каждый идеал должен быть именован. Пусть, например, мы хотим обозначить через `j` идеал $\langle x^2+y, x+2xy\rangle$. В Cali это делается командой

```
5: setideal(i,{x^2+y,x+2*x*y});
```

Как только идеал задан, мы можем работать с ним. Например, деление x^3+3y^2 на x^2+y и $x+2xy$ выполняется командой

```
6: x^3+3*y^2 mod j;
```

Для вычисления базиса Грёбнера идеала `j` нужно ввести команду

```
7: gbasis j;
```

Результатом будет базис Грёбнера идеала $\langle x^2+y, x+2xy\rangle \subset \mathbb{Q}[x,y]$ для мономиального упорядочения, заданного командой `setring`. Ответ дается в редуцированной форме (см. § 7 гл. 2) с целыми коэффициентами.

Если вы вводите полиномы с целыми или рациональными коэффициентами, то Cali будет считать основным полем $\mathbb{Q}$. Вычисление базиса Грёбнера над конечным полем осуществляется теми же командами, что и в пакете Groebner. С другой стороны, при вычислении в поле $\mathbb{Q}(i)$ могут возникнуть трудности. Здесь можно прибегнуть к приему, который уже рассматривался применительно к системе Maple. Если же коэффициенты принадлежат полю рациональных функций, то, как и в пакете Groebner, достаточно исключить эти переменные из списка `vars` в команде `setring`. Если, например, команда `setring` введена, как в `4:`, то команды

```
8: setideal(m,{v*x^2+y,u*x*y+y^2});
9: gbasis m;
```


вычислят базис Грёбнера идеала $\langle vx^2+y, uxy+y^2\rangle \subset \mathbb{Q}(u,v)[x,y]$ для grlex-упорядочения с $x>y$. Ответом является редуцированный базис Грёбнера, старшие коэффициенты элементов которого — это полиномы от u,v.

Вот некоторые полезные команды Cali:

- `dimzerop` для проверки конечности числа решений (с помощью метода из § 3 гл. 5) полиномиальной системы над алгебраически замкнутым полем;
- `dim` для вычисления размерности многообразия, определенного идеалом;
- `idealquotient` для вычисления частного $I:f$;
- `isprime` для проверки идеала на простоту;
- `radical` для вычисления радикала данного идеала;
- `primarydecomposition` для вычисления примарного разложения данного идеала (см. § 7 гл. 4).

Кроме того, Cali может работать с такими сложными объектами, как модули, раздутия, свободные резольвенты и касательные конусы. Соответствующие команды подробно описаны в справочном издании GRÄBE (1995).

Получить копию Cali можно через справочную сеть REDUCE, которая поддерживается в США RAND Corporation. Электронный адрес:

```
gopher://is.rand.org/11/software/reduce
```

Информацию о Cali можно также получить, послав e-mail автору пакета (H.-G. Gräbe) по адресу `graebe@informatik.uni-leipzig.de`.

§ 5. Другие системы

Еще одной известной системой компьютерной алгебры является MACSYMA, которая обладает примерно теми же возможностями, что и AXIOM, Maple, Mathematica и REDUCE, включая работу с базисами Грёбнера. К сожалению, в процессе работы над этой книгой мы не имели доступа к этой системе и потому не может дать ее описания.

Кроме «общих» алгебраических систем, рассмотренных выше, имеются две специализированные — Macaulay и CoCoA [1], которые заслуживают упоминания. Хотя эти программы и ориентированы на специалистов в области алгебраической геометрии и коммутативной алгебры, но и обычный пользователь может с успехом с

[1] От Computation in Commutative Algebra.— *Прим. ред.*

ними работать. Весьма привлекательной их чертой является свободное (некоммерческое) распространение.

Начать сеанс работы с Macaulay или CoCoA непросто. Сначала нужно задать список переменных и основное поле. Переменные имеют вес (в нашем случае, как правило, все переменные имеют вес 1). Macaulay работает только с однородными полиномами и потому задать lex-упорядочение непросто. В результате работа с Macaulay трудна для новичка и вначале требует постоянной помощи специалиста.

Macaulay всегда работает над конечным полем, а CoCoA дает пользователю выбор между конечным полем и $\mathbb{Q}$. Над конечным полем вычисления проводятся быстрее. Пока размер коэффициентов не превышает характеристику поля (как это бывает в простых примерах), никаких проблем не возникает. Но при решении более сложных задач могут возникать трудности. При этом нужно помнить, что такие задачи трудно решать и с помощью других систем по причине большого объема требуемой памяти.

Для специалиста Macaulay и CoCoA предлагают удивительный набор сложных математических объектов. Исследователи часто прибегают к помощи этих программ для вычисления сизигий и свободных резольвент. Macaulay также дает возможность работать с раздутиями, когомологиями, кокасательными пучками, двойственными многообразиями, нормальными конусами, радикалами и другими объектами алгебраической геометрии. Обе эти программы доступны в рамках сети: как получить Macaulay, указано в разд. 15.12 книги EISENBUD (1995)[1)], а как получить CoCoA, сообщается в приложении A книги ADAMS, LOUSTAUNAU (1994)[2)].

Наконец, следует упомянуть систему MAS — алгебраическую систему, доступную в рамках сети. Кроме вычисления обычного базиса Грёбнера, она может находить исчерпывающий базис Грёбнера и базис Грёбнера над областями целостности (см. тему 16 в приложении D). Как получить MAS, сообщается на с. xiii книги BECKER, WEISPFENNING (1993).

Кроме перечисленных компьютерных систем, некоторые системы находятся в процессе разработки:

- Новая версия Macaulay, имеющая дружественный интерфейс и рассчитанная на более широкий круг пользователей (при этом система не потеряла в скорости и эффективности).

[1)] Она может быть получена по ftp: `math.harvard.edu`, `login ftp`, `password any`, `ed. Macaulay`. — *Прим. ред.*

[2)] Информацию можно получить по адресу: `cocoa@dima.unige.it`. — *Прим. ред.*

- Компьютерная алгебраическая система Magma [1)], разрабатываемая в Австралии, которая позволяет проводить вычисления в теории групп, теории чисел, комбинаторике и коммутативной алгебре. Информацию о Magma можно найти по адресу:

`http:/www.maths.usyd.edu.au:8000/comp/magma/Overview.html`

- Проект PoSSo — это большой европейский проект, нацеленный на создание мощных программ в области коммутативной алгебры. Кроме вычисления базисов Грёбнера PoSSo может исследовать особенности и другие интересные объекты алгебраический геометрии.
- SINGULAR — система компьютерной алгебры для вычисления базисов Грёбнера и исследования особенностей многообразий (и многих других вещей). Эта система описана в работе GREUEL (1996) и может быть получена по анонимному ftp: `helios.mathematik.uni-kl.de`.

Некоторые из этих систем, возможно, уже будут доступны в тот момент, когда вы читаете эту книгу. Так как компьютеры становятся все быстрее, а программное обеспечение — все более мощным и более простым в использовании, то можно ожидать, что область приложения базисов Грёбнера и алгебраической геометрии в целом будет расширяться.

[1)] Magma является коммерческой системой. — *Прим. ред.*

Приложение D

Темы для самостоятельных исследований

В отличие от основного текста книги, это приложение адресовано научному руководителю. Мы обсудим несколько тем для самостоятельных исследований, имеющих отношение к материалу, изложенному в книге.

§ 1. Общие замечания

Ценность самостоятельных исследований состоит в том, что

- они заставляют студента воспринимать активно (а не пассивно) идеи и методы книги;
- они помогают студентам подготовиться к изучению более сложного материала;
- они помогают студентам приобрести опыт работы с системами компьютерной алгебры.

Работа над предлагаемыми темами представляет отличную возможность научиться работать небольшими группами.

Некоторые из предлагаемых тем содержат значительную чисто компьютерную часть, в то время как другие скорее теоретически ориентированы. Список тем ни в коей мере не является обязательным или исчерпывающим, и мы будем рады, если читатели предложат нам другие темы и самостоятельные проекты.

Мы даем лишь краткие описания тем. Хотя библиографические ссылки и приведены, мы рекомендуем руководителю излагать темы студентам более подробно.

§ 2. Предлагаемые темы

(i) *Реализация алгоритма деления в* $k[x_1, \ldots, x_n]$. Большинство систем компьютерной алгебры (включая Maple и REDUCE) имеют команды типа «normal form» или «reduce», которые реализуют алгоритм деления из гл. 2. Однако эти команды выдают только остаток от деления. Кроме того, иногда система

позволяет задать лишь несколько мономиальных упорядочений. Задача состоит в том, чтобы реализовать общий алгоритм деления, где пользователь задает полином f, список делителей F, список переменных X и мономиальное упорядочение. Результатом должен быть остаток и список частных. Такой алгоритм, вероятно, может быть реализован в рамках системы компьютерной алгебры типа Maple или Mathematica.

(ii) *Реализация алгоритма Бухбергера.* Большинство систем компьютерной алгебры имеет команды для вычисления редуцированного базиса Грёбнера идеала $\langle f_1, \ldots, f_s \rangle$. Задача состоит в создании алгоритма, который выдавал бы больше информации о своей работе и (возможно) умел бы работать с большим числом мономиальных упорядочений. А именно, если пользователь задает список полиномов F, список переменных X и мономиальное упорядочение на $k[x_1, \ldots, x_n]$, то программа должна выдать редуцированный базис Грёбнера G идеала, порожденного F, и матрицу полиномов A, выражающую элементы базиса G через исходные полиномы, $G = AF$. Как и в первой теме, такой алгоритм может быть реализован в рамках системы компьютерной алгебры. Программа также должна выдавать дополнительную информацию (например, о числе остатков, вычисленных на каждом шаге алгоритма).

(iii) *Сложность задачи о принадлежности идеалу.* В § 9 гл. 2 мы кратко упомянули о некоторых плохих (в смысле сложности) случаях, встречающихся при вычислении базисов Грёбнера и решении задачи о принадлежности идеалу. Цель этой темы — дать студентам представление о примерах, придуманных Майром (Mayr) и Мейером (Meyer), и объяснить им, что такое *двойной экспоненциальный* рост верхней границы сложности в задаче о принадлежности идеалу. В работе Bayer, Stillman (1988) дано хорошее изложение этих результатов. С помощью руководителя сильные студенты младших курсов могут усвоить эту работу.

(iv) *Решение полиномиальных уравнений.* Эта прекрасная тема предназначена для студентов, интересующихся численными методами решения полиномиальных систем. Смысл темы состоит в реализации критерия конечности числа решений полиномиальной системы над $\mathbb{C}$, изложенного в теореме 6 из § 3 гл. 5. Если конечность числа решений установлена, то программа должна найти их с заданной точностью. Для этого нужно находить (численно) значения переменных по очереди, используя базис Грёбнера по отношению к lex-упорядочению. Следует также сравнить этот метод со стандартными методами ре-

шения систем, такими, как метод Ньютона в случае многих переменных. Следует отметить, что такие сравнения на теоретическом уровне практически не проводились.

(v) *Преобразования базисов Грёбнера для нульмерных идеалов.* Как и предыдущая тема, эта также имеет отношение к решению полиномиальных систем. Здесь лексикографический базис Грёбнера наиболее удобен для исключения переменных. Но такой базис находится труднее, чем базисы Грёбнера для других упорядочений. В случае нульмерных идеалов (т. е. таких идеалов $I \subset k[x_1, \ldots, x_n]$, что $\mathbf{V}(I)$ конечно) существуют методы *преобразования* базиса Грёбнера для некоторого упорядочения в лексикографический базис. Целью этой темы является изучение этих методов и (возможно) их реализация. Введение в эти методы содержится в книге HOFFMANN (1989). См. также работу FAUGÉRE, GIANNI, LAZARD, MORA (1993).

(vi) *Особенности кривых.* Особые точки на кривых — это целая область математики, и здесь можно сформулировать большое количество задач. Простейшей из них, возможно, является реализация алгоритма определения особых точек кривой $\mathbf{V}(f(x,y)) \subset \mathbb{R}^2$ (или $\mathbb{C}^2$). Студент должен освоить некоторые теоретические методы анализа особенностей на кривых: полиномы Ньютона, разложения Пюизо, разрешения особенностей с помощью квадратичных преобразований и др. Этот материал содержится в книге BRIESKORN, KNÖRRER (1986). Те же вещи обсуждаются в многих других книгах по теории алгебраических кривых. С практической точки зрения эти методы («трассировка кривой») рассмотрены в книге HOFFMANN (1989).

(vii) *Пересечения поверхностей.* Цель этой темы — создание алгоритмов для описания проекций пространственных кривых, являющихся пересечениями поверхностей $\mathbf{V}(f_1(x,y,z))$ и $\mathbf{V}(f_2(x,y,z))$ в $\mathbb{R}^3$. Эта очень важная задача в геометрическом моделировании. Один метод ее решения, основанный на нахождении «простой» поверхности в пучке, определенном полиномами f_1 и f_2, описан в книге HOFFMANN (1989). Этот метод использует изучение проективного замыкания двух данных поверхностей. См. также работу GARRITY, WARREN (1989).

(viii) *Сплайны Безье.* Кубики Безье, которые были определены в § 3 гл. 1, предназначены для описания областей с криволинейной границей. Это делается так: граница области разбивается на сегменты, которые далее аппроксимируются кубиками Безье. В результате мы получаем *кусочную* кривую Безье, или сплайн Безье. Целью этой темы является создание алгоритма, который по заданным контрольным точкам, описывающим кривую, строит и выводит соответствующий сплайн Безье. Другой интересной задачей является создание алгоритма для определения *точек пересечения* двух сплайнов Безье. Некоторые ссылки можно найти на с. xvi книги FARIN (1990). Также имеется недавняя теоретическая работа BILLERA, ROSE (1989), в которой базисы Грёбнера применяются для вычисления размерности векторного пространства сплайнов полиномов данной степени от нескольких переменных на данном полиэдральном разбиении области в $\mathbb{R}^n$.

(ix) *Общий метод Ву.* В нашем обсуждении метода Ву (гл. 6) мы не касались такой алгебраической техники, как характеристические множества и метод разложения Ритта, которые необходимы для реализации доказывателя теорем в общем случае. Цель темы состоит в изучении этих методов и (возможно) в их компьютерной реализации. См. CHOU (1988), MISHRA (1993), WANG (1994a) и (1994b), WU (1983).

(x) *Теорема Молина.* Вопросы, связанные с теоремой Молина в теории инвариантов (см. § 3 гл. 7), являются интересной темой самостоятельных исследований. Алгоритм из работы STURMFELS (1989) позволяет найти множество образующих в $k[x_1, \ldots, x_n]^G$. Этот алгоритм дает возможность найти инварианты таких сравнительно больших групп, как группа вращений куба в $\mathbb{R}^3$. Теорема Молина рассмотрена в гл. 7 книги BENSON, GROVE (1985).

(xi) *Базисы Грёбнера над общими полями.* Эта хорошая тема для студентов, знакомых с теорией полей. Ее цель — вычисление базисов Грёбнера над полями, отличными от поля $\mathbb{Q}$. В приложении C, когда мы рассматривали систему Maple, мы объяснили, как найти базис Грёбнера над $\mathbb{Q}(i)$ (для этого нужно ввести дополнительную переменную j и дополнительный полином $j^2 + 1$). Пусть α — алгебраическое число. Тогда аналогичный метод работает над полем $\mathbb{Q}(\alpha)$ при условии, что нам известен минимальный полином для α над $\mathbb{Q}$. Необходимый теоретический материал изложен в любом учебнике по высшей алгебре, где рассматривается теория полей. Более трудной задачей является вычисление базисов Грёбнера над конечными расширениями вида $\mathbb{Q}(u_1, \ldots, u_m)$. (Так можно задать любое конечное расширение поля $\mathbb{Q}$).

(xii) *Компьютерная графика.* В § 1 гл. 8 мы использовали проекции для изображения трехмерных объектов. Все эти идеи исключительно важны в компьютерной графике. Цель темы состоит в том, чтобы студент изучил проекции, используемые в компью-

терной графике, и понял их связь с проективным пространством. Если вы посмотрите на формулы, приведенные в гл. 6 книги FOLEY, VAN DAM, FEINER, HUGHES (1990), то вы увидите 4×4-матрицы. Эти матрицы появляются в формулах по той причине, что точка в $\mathbb{P}^3$ имеет 4 однородные координаты!

(xiii) *Построение неявного описания с помощью результантов.* Как указывалось в § 3 гл. 3, задачу построения неявного описания удобнее решать с помощью результантов, чем с помощью вычисления базиса Грёбнера. Хорошей темой является изучение работ ANDERSEN, GOLDMAN, SEDERBERG (1984a, 1984b) и MANOCHA (1994). Результанты, используемые в этих работах, отличаются от результантов двух полиномов, определенных в гл. 3. Для решения задачи построения неявного описания нужны результанты трех и более полиномов, которые называются *мультиполиномиальными результантами*. Эти результанты рассмотрены в работе BAJAJ, GARRITY, WARREN (1988) и в книге COX, LITTLE, O'SHEA (1998).

(xiv) *Оптимальный порядок переменных.* Известны случаи, когда изменение порядка переменных (при сохранении типа упорядочения) сильно влияет на процесс вычисления базиса Грёбнера. Например, в п. (a) упр. 13 к § 9 гл. 2 вычислялся достаточно сложный базис Грёбнера для lex-упорядочения с $x > y > z$. Но изменение порядка переменных на $z > y > x$ (при сохранении lex) дает значительно более простой базис. Эвристический алгоритм выбора оптимального порядка переменных описан в работе BOEGE, GEBAUER, KREDEL (1986). Хорошей темой была бы прямая реализация алгоритма Бухбергера плюс выбор оптимального порядка переменных. Такой алгоритм включен в состав пакета Groebner системы REDUCE (см. § 4 приложения C).

(xv) *Выбор стратегий в алгоритме Бухбергера.* В нашем обсуждении алгоритма Бухбергера (после теоремы 11 из § 9 гл. 2) мы упоминали стратегию выбора пары $(i, j) \in B$ в теореме 11, которая состоит в минимизации монома $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$. Этот подход называется *нормальной стратегией выбора*. Существуют, однако, и другие стратегии выбора, причем некоторые из них реализованы в действующих алгоритмах. Хорошей задачей является разобраться в этих стратегиях (и реализовать их). Вот две из них:

(a) Концепция сахарной стратегии (*sugar*), введенная в работе GIOVINI, MORA, NIESI, ROBBIANO, TRAVERSO (1991). В этой работе объясняется, почему нормальная стратегия выбора может приводить к трудностям при работе с неградуированными упорядочениями (такими, как lex), и определяется понятие сахарной стратегии, позволяющее устранить эти трудности. Эта стратегия реализована в большинстве систем, описанных в приложении C.

(b) В случае lex-упорядочения некоторые эвристики выбора пар обсуждаются в работе CZAPOR (1991). Основной идеей здесь является выбор пары (i, j), такой, чтобы мультистепень S-полинома $S(f_i, f_j)$ была бы как можно меньше.

(xvi) *Другие типы базисов Грёбнера.* В гл. 2 мы определили базис Грёбнера идеала в кольце полиномов для данного мономиального упорядочения и данного основного поля. Но есть и другие подходы к тому, что такое базис Грёбнера. Хорошей темой является изучение этих подходов. Вот некоторые интересные типы базисов Грёбнера:

(a) Мы знаем, что различные упорядочения дают различные базисы Грёбнера. Меняя упорядочения, мы обнаруживаем, что существует лишь конечное число базисов Грёбнера данного идеала. Объединим их и образуем *универсальный базис Грёбнера*, который является базисом Грёбнера для *всех возможных* упорядочений. См. с. 514–515 книги BECKER, WEISPFENNING (1993).

(b) Если основное поле содержит параметры, то возможен случай (см. § 3 гл. 6), когда базис Грёбнера некоторого идеала перестает быть им при специализации параметров. Можно, однако, построить базис Грёбнера, который остается им при *любой специализации* параметров. Такие базисы называются *исчерпывающими базисами Грёбнера*. Описание таких базисов и ссылки можно найти на с. 515–518 книги BECKER, WEISPFENNING (1993).

(c) Иногда базис Грёбнера можно определить для идеалов в кольцах полиномов $R[x_1, \ldots, x_n]$, где R — кольцо. Это проще всего сделать, когда R является кольцом главных идеалов (см. § 1 гл. 5). Основы теории таких базисов Грёбнера изложены в гл. 4 книги ADAMS, LOUSTAUNAU (1994) и в разд. 10.1 книги BECKER, WEISPFENNING (1993).

(d) Обобщением понятия идеала $I \subset k[x_1, \ldots, x_n]$ является понятие *модуля* $M \subset k[x_1, \ldots, x_n]^r$. Можно естественным образом определить упорядочения и базисы Грёбнера для модулей. Основные определения и интересные примеры можно найти в книгах ADAMS, LOUSTAUNAU (1994), BECKER, WEISPFENNING (1993), COX, LITTLE, O'SHEA (1998) и EISENBUD (1995).

Кроме тем, перечисленных выше, научный руководитель может почерпнуть интересные темы исследований для студентов в следующих книгах:

- Cox, Little, O'Shea (1998). В главах этой книги, посвященных локальным кольцам, алгебраической теории кодирования и целочисленному программированию, можно найти немало тем для самостоятельных исследований. В зависимости от интересов студентов можно найти такие темы и в других главах.
- Adams, Loustaunau (1994). Главы о минимальных полиномах расширений полей, о проблеме трех красок и целочисленном программировании могут дать материал для нескольких интересных исследований.
- Eisenbud (1995). В этой книге в разд. 15.12 дан список из семи тем. Это более трудные темы, и они требуют больших знаний в области коммутативной алгебры, чем темы из нашего списка. Но, с другой стороны, они дают хорошее введение в актуальные области исследования в алгебраической геометрии.

Если вы придумаете новые темы самостоятельных исследований, нам будет интересно узнать о них. Имеется *масса* удивительных вещей, которые можно делать с базисами Грёбнера и алгебраической геометрией. Темы, перечисленные выше, есть не более чем попытки, не идущие дальше поверхности.

Литература

Adams W., Loustaunau P. (1994), An Introduction to Gröbner Bases, Graduate Studies in Mathematics, **3**, Amer. Math. Soc., Providence.

Anderson D., Goldman R., Sederberg T. (1984a), Implicit representation of parametric curves and surfaces, Comput. Vision, Graphics, and Image Design, **28**, 72–84.

Anderson D., Goldman R., Sederberg T. (1984b), Vector elimination: a technique for the implicitization, inversion and intersection of planar parametric rational polynomial curves, Comput. Aided Geom. Design, **1**, 327–356.

Atiyah M. F., MacDonald I. G. (1969), Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass. [Имеется перевод: Атья М., Макдональд И. Введение в коммутативную алгебру. — М.: Мир, 1972.]

Baillieul J. et al. (1990), Robotics, Proceedings of Symposia in Applied Mathematics, **41**, Amer. Math. Soc., Providence, R.I.

Bajaj C., Garrity T., Warren J. (1988), On the applications of multi-equational resultants, Technical Report CSD-TR-826, Department of Computer Science, Purdue University.

Ball A. A. (1987), The parametric representation of curves and surfaces using rational polynomial functions, in: The Mathematics of Surfaces, II, ed. by Martin R. R., Clarendon Press, Oxford, 39–61.

Bayer D. (1982), The division algorithm and the Hilbert scheme, Ph.D. thesis, Harvard University.

Bayer D., Mumford D. (1993), What can be computed in algebraic geometry?, in: Computational Algebraic Geometry and Commutative Algebra, ed. by Eisenbud D., Robbiano L., Cambridge University Press, Cambridge, 1–48.

Bayer D., Stillman M. (1987a), A criterion for detecting m-regularity, Invent. Math., **87**, 1–11.

Bayer D., Stillman M. (1987b), A theorem on refining division orders by the reverse lexicographic order, Duke J. Math., **55**, 321–328.

Bayer D., Stillman M. (1988), On the complexity of computing syzygies, in: Computational Aspects of Commutative Algebra, ed. by Robbiano L., Academic Press, New York, 1–13.

Becker T., Weispfenning V. (1993), Gröbner Bases, Springer-Verlag, New York–Berlin–Heidelberg.

Benson D. (1993), Polynomial Invariants of Finite Groups, Cambridge University Press, Cambridge.

Benson C. T., Grove L. C. (1985), Finite Reflection Groups, 2nd ed., Springer-Verlag, New York–Berlin–Heidelberg.

Billera L., Rose L. (1989), Gröbner basis methods for multivariate splines, in: Mathematical Methods in Comput. Aided Geom. Design, ed. by Lyche T., Schumacher L., Academic Press, New York, 93–104.

Boege W., Gebauer R, Kredel H. (1986), Some examples for solving systems of algebraic equations by calculating Groebner bases, J. Symbolic Comput., **2**, 83–98.

Brieskorn E., Knörrer H. (1986), Plane Algebraic Curves, Birkhäuser, Basel–Boston–Stuttgart.

Bruce J. W., Giblin P. J. (1992), Curves and Singularities, 2nd ed., Cambridge University Press, Cambridge. [Имеется перевод I изд.: Брус Дж., Джиблин П. Кривые и особенности. — М.: Мир, 1988.]

Buchberger B. (1985), Groebner bases: an algorithmic method in polynomial ideal theory, in: Multidimensional Systems Theory, ed. by Bose N. K., D. Reidel Publishing Company, Dordrecht, 184–232.

Canny J., Manocha D. (1992), Algorithm for implicitizing rational parametric surfaces, Comput. Aided Geom. Design, **9**, 25–50.

Canny J., Manocha D. (1993), Multipolynomial resultant algorithms, J. Symbolic Comput., **15**, 99–122.

Char B., Geddes K., Gonnet G., Leong B., Monogan M., Watt S. (1991), Maple V Library Reference Manual, Springer-Verlag, New York–Berlin–Heidelberg.

Chou S.-C. (1988), Mechanical Geometry Theorem Proving, D. Reidel Publishing Company, Dordrecht.

Clemens H. (1980), A Scrapbook of Complex Curve Theory, Plenum Press, New York–London. [Имеется перевод: Клеменс Г. Мозаика теории комплексных кривых. — М.: Мир, 1972.]

Cox D., Little J., O'Shea D. (1998), Using Algebraic Geometry, Springer-Verlag, New York–Berlin–Heidelberg.

Coxeter H. S. M. (1973), Regular Polytopes, 3d ed., Dover, New York.

Czapor S. (1991), A heuristic selection strategy for lexicographic Cröbner bases?, in: ISSAC 1991, Proc. of the 1991 Intern. Symp. on Symbolic and Algebraic Comput., ed. by Watt S., ACM Press, New York, 39–48.

Davenport J. H., Siret Y., Tournier E. (1993), Computer Algebra, 2nd ed., Academic Press, New York. [Имеется перевод I изд.: Давенпорт Дж., Сире Й., Турнье Е. Компьютерная алгебра. — М.: Мир, 1991.]

Dubé T. W. (1990), The structure of polynomial ideals and Gröbner bases, SIAM J. Comput., **19**, 750–775.

Eisenbud D. (1995), Commutative Algebra with a View Toward Algebraic Geometry, Springer-Werlag, New York–Berlin–Heidelberg.

Eisenbud D., Huneke C., Vasconcelos W. (1992), Direct methods for primary decomposition, Invent. Math., **110**, 207–235.

Farin G. (1990), Curves and Surfaces for Computer Aided Geometric Design, 2nd ed., Academic Press, New York.

Faugère J., Gianni P., Lazard D., Mora T. (1993), Efficient change of ordering for Gröbner bases of zero-dimensional ideals, J. Symbolic Comput., **16**, 329–344.

Finkbeiner D. T. (1978), Introduction to Matrices and Linear Transformations, 3d ed., Freeman W. H. and Co., San Francisco.

Foley J., van Dam A., Feiner S., Hughes J. (1990), Computer Graphics: Principles and Practice, 2nd ed., Addison-Wesley, Reading, Mass.

Fulton W. (1969), Algebraic Curves, Benjamin W. A., New York.

Garrity T., Warren J. (1989), On computing the intersection of a pair of algebraic surfaces, Comput. Aided Geom. Design, **6**, 137–163.

Gauss C. F. (1876), Volume III, Königlichen Gesellschaft der Wissenschaften zu Göttingen, Göttingen. [См. также Гаусс К. Ф. Труды по теории чисел. — М.: Изд-во АН СССР, 1959.]

Gebauer R., Möller H. M. (1988), On an installation of Buchberger's algorithm, in: Computational Aspects of Commutative Algebra, ed. by Robbiano L., Academic Press, New York, 141–152.

Gelfand I., Kapranov M., Zelevinsky A. (1994), Discriminants, Resultants and Multidimensional Determinants, Birkhäuser, Basel–Boston–Berlin. [Готовится русск. перевод.]

Gianni P., Trager B., Zacharias G. (1988), Gröbner bases and primary decomposition of polynomial ideals, in: Computational Aspects of Commutative Algebra, ed. by Robbiano L., Academic Press, New York, 15–33.

Giovini A., Mora T., Niesi G., Robbiano L., Taverso C. (1991), «One sugar cube, please», or Selection strategies in the Buchberger algorithm, in: ISSAC 1991, Proc. of the 1991 Intern. Symp. on Symbolic and Algebraic Comput., ed. by Watt S., ACM Press, New York, 49–54.

Giusti M., Heintz J. (1993), La détermination des points isolés et de la dimension d'une variété algebrique peut se faire en temps polynomial, in: Computational Algebraic Geometry and Commutative Algebra, ed. by Eisenbud D., Robbiano L., Cambridge University Press, Cambridge, 216–256.

Gräbe H.-G. (1995), CALI: A REDUCE package for commutative algebra, Version 2.2.1, Universität Leipzig, Institut für Informatik.

Greuel G.-M., Description of SINGULAR: A computer algebra system for singularity theory, algebraic geometry and commutative algebra, Euromath Bulletin, **2**, 1996.

Griffiths P. (1989), Introduction to Algebraic Curves, Transl. of Math. Monographs, **76**, Amer. Math. Soc., Providence.

Gritzmann P., Sturmfels B. (1993), Minkowski addition of polytopes: computational complexity and applications to Gröbner bases, SIAM J. Discrete Math., **6**, 246–269.

Hermann G. (1926), Der Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann., **95**, 736–788.

Herstein I. N. (1975), Topics in Algebra, 2nd ed., John Wiley & Sons, New York.

Hilbert D. (1890), Über die Theorie der algebraischen Formen, Math. Ann., **36**, 473–534. Reprinted in Ges. Abh., Vol. II, Chelsea, New York, 1965. [Имеется перевод: Гильберт Д. Избранные труды. Т. I. — М.: Факториал, 1998, с. 16–66.]

Hilbert D. (1993), Theory of Algebraic Invariants, Cambridge University Press, Cambridge. [Перевод основополагающих статей Гильберта по теории инвариантов см. в указанном выше томе.]

Hodge W. V. D., Pedoe D. (1968), Methods of Algebraic Geometry, Volumes I and II, Cambridge University Press, Cambridge. [Имеется перевод I изд.:

Ходж В., Пидо Д. Методы алгебраической геометрии. Тт. I–III. — М.: ИЛ, 1954, 1955.]
Hoffmann C. (1989), Geometric and Solid Modeling: An Introduction, Morgan Kaufmann Publishers, San Mateo, California.
Jenks R., Sutor R. (1992), Axiom: the scientific computation system, Springer-Verlag, New York–Berlin–Heidelberg.
Jouanolou J. (1991), Le formalisme du résultant, Advances in Math., **90**, 117–263.
Kendig K. (1977), Elementary Algebraic Geometry, Springer-Verlag, New York–Berlin–Heidelberg.
Kirwan F. (1992), Complex Algebraic Curves, Lond. Math. Soc. Student Texts, **23**, Cambridge University Press, Cambridge.
Klein F. (1884), Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom Fünften Grade, Teubner, Leipzig. [Имеется перевод: Клейн Ф. Лекции об икосаэдре и решение уравнений пятой степени. — М.: Наука, 1990.] Degree, Trubner, London, 1888. Reprinted by Dover, New York, 1956.
Lang S. (1965), Algebra, Addison-Wesley, Reading, Mass. [Имеется перевод: Ленг С. Алгебра. — М.: Мир, 1968.]
Lazard D. (1983), Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, in: Computer Algebra: EUROCAL 83, ed. by van Hulzen J. A., Lect. Notes Comput. Sci., **162**, Springer-Verlag, New York–Berlin–Heidelberg, 146–156.
Lazard D. (1993), Systems of algebraic equations (algorithms and complexity), in: Computational Algebraic Geometry and Commutative Algebra, ed. by Eisenbud D., Robbiano L., Cambridge University Press, Cambridge, 84–105.
Lejeune-Jalabert M. (1985), Effectivité des calculs polynomiaux, Cours de DEA 1984–85, Institut Fourier, Université de Grenoble I.
Macaulay F. (1902), On some formula in elimination, Proc. Lond. Math. Soc., **3**, 3–27.
Manocha D. (1994), Solving systems of polynomial equations, IEEE Comput. Graph. Appl., **14**, March 1994, 46–55.
Matsumura H. (1986), Commutative Ring Theory, Cambridge University Press, Cambridge.
Mayr E., Meyer A. (1982), The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. Math., **46**, 305–329.
Melenk H., Möller H. M., Neun W. (1994), Groebner: A package for calculating Groebner bases, Konrad-Zuse-Zentrum für Informationstechnik, Berlin.
Mignotte M. (1992), Mathematics for Computer Algebra, Springer-Verlag, New York–Berlin–Heidelberg.
Mines R., Richman F., Ruitenburg W. (1988), A Course in Constructive Algebra, Springer-Verlag, New York–Berlin–Heidelberg.
Mishra B. (1993), Algorithmic Algebra, Texts and Monographs in Computer Science, Springer-Verlag, New York–Berlin–Heidelberg.
Möller H. M., Mora F. (1984), Upper and lower bounds for the degree of Groebner bases, in: EUROSAM 1984, ed. by Fitch J, Lect. Notes Comput. Sci., **174**, Springer-Verlag, New York–Berlin–Heidelberg, 172–183.

Mumford D. (1976), Algebraic Geometry I: Complex Projective Varieties, Springer-Verlag, New York–Berlin–Heidelberg. [Имеется перевод: Мамфорд Д. Алгебраическая геометрия. Комплексные алгебраические многообразия. — М.: Мир, 1979.]
Paul R. (1981), Robot Manipulators: Mathematics, Programming and Control, MIT Press, Cambridge, Mass.
Robbiano L. (1986), On the theory of graded structures, J. Symbolic Comp., **2**, 139–170.
Roth L., Semple J. G. (1949), Introduction to Algebraic Geometry, Clarendon Press, Oxford.
Seidenberg A. (1974), Constructions in algebra, Trans. Amer. Math. Soc., **197**, 273–313.
Seidenberg A. (1984), On the Lasker–Noether decomposition theorem, Amer. J. Math., **106**, 611–638.
Shafarevich I. R. (1974): Шафаревич И. Р. Основы алгебраической геометрии. — М.: Наука, 1972.
Smith L. (1995), Polynomial Invariants of Finite Groups, Peters A. K., Ltd., Wellesley, Mass.
Sturmfels B. (1989), Computing final polynomials and final syzygies using Buchberger's Gröbner bases method, Results Math., **15**, 351–360.
Sturmfels B. (1993), Algorithms in Invariant Theory, Texts and Monographs in Symbolic Computation, Springer-Verlag, New York–Vienna.
van der Waerden B. (1931), Moderne Algebra, Vol. II, Springer-Verlag, Berlin. [Имеется русский перевод I изд. 1931 г.: Ван дер Варден Б. Л. Современная алгебра. Т. 2. — М.: ГИТТЛ, 1937; II изд. 1940 г.: Гостехиздат, 1947, а также V изд. т. I и V изд. т. II: Ван дер Варден Б. Л. Алгебра. — М.: Наука, 1976.] Глава по теории исключения входила только в три первых оригинальных издания (и в соответствующие переводы).
Walker R. (1950), Algebraic Curves, Princeton University Press, Princeton. Reprinted by Dover, 1962. [Имеется перевод: Уокер Р. Алгебраические кривые. — М.: ИЛ, 1952.]
Wang D. (1994a), An implementation of the characteristic set method in Maple, in: Automated Practical Reasoning: Algebraic Approaches, ed. by Pfalzgraf J. and Wang D., Springer-Verlag, New York–Vienna, 187–201.
Wang D. (1994b), Characteristic sets and zero structure of polynomial sets (Revised version of May 1994), Lect. Notes, RISC-LINZ, Johannes Kepler University, Linz, Austria.
Winkler F. (1984), On the complexity of the Gröbner bases algorithm over $K[x, y, z]$, in: EUROSAM 1984, ed. by Fitch J, Lect. Notes Comput. Sci., **174**, Springer-Verlag, New York–Berlin–Heidelberg, 184–194.
Wolfram S. (1996), The Mathematica Book, 3d ed., Wolfram Media, Champaign, Illinois.
Wu W.-T. (1983), On the decision problem and the mechanization of theorem-proving in elementary geometry, in: Automated Theorem Proving: After 25 Years, ed. by Bledsoe S. and Loveland D., Contemp. Math., **29**, Amer. Math. Soc., Providence, R.I., 213–234.

Предметный указатель

автоморфизм многообразий 314
алгебраическая параметризация 160
алгебраически замкнутое поле 15
алгебраическое соотношение 434
алгоритм *Бухбергера* 121, 122
- - усовершенствованный 144
- вычисления проективного замыкания аффинного многообразия 491
- деления 57, 88
- для вычисления GCD 61
- - - базиса частного идеалов 254
- - - наибольшего общего делителя 246
- - - наименьшего общего кратного 246
- - - пересечения идеалов 244
- *Евклида* 61
- построения неявного представления для полиномиальной параметризации 170
- - - - - рациональной параметризации 174
- принадлежности радикальному идеалу 233
- проверки равенства идеалов 125
- - совместности 225
- псевдоделения 389
- решения задачи о принадлежности идеалу 128
аффинная плоскость 13
- прямая 13, 453
- функция *Гильберта* 572
- часть многообразия 468
аффинное многообразие 17
- преобразование 351
- пространство 13
аффинный конус 473, 480
- полином *Гильберта* 574

базис *Грёбнера* 105
- - исчерпывающий 358, 669
- - минимальный 123
- - редуцированный 123
- идеала 47
- минимальный 54
- - для мономиального идеала 100
- сизигий 140
- стандартный 105
бесконечно удаленная гиперплоскость 463
- - прямая 450, 453
- - точка 450
бесконечное поле 14
биоднородный полином 508, 512
бирациональная эквивалентность 325, 605
бистепень 512

великая теорема Ферма 26
вес монома 512
взвешенно однородный полином 508, 512
взвешенное упорядочение 101
возрастающая цепь идеалов 106
вполне упорядочение 77
вход 642
входные данные 56, 642
выпуклое подмножество 43
выход 642
выходные данные 56

гиперплоскость 465, 515
- бесконечно удаленная 463
гиперповерхность 465
- квадратичная 465, 516
главный идеал 60, 110
- ступенчатый вид 72
гладкая точка 613
гомогенизация идеала 486, 505
- полинома 228, 468
гомоморфизм кольцевой 228, 288
градиент полинома 181
градуированное упорядочение 80, 486
- лексикографическое упорядочение 80
- обратное лексикографическое упорядочение 81
график функции 314
группа 639
- *Клейна* четверная 417
- линейная проективная 526
- матричная конечная 412
- общая линейная 412
- перестановок 639
- циклическая 413

двойное отношение 383
двойственная кривая 447
- проективная плоскость 461
двойственное многообразие 447
- проективное пространство 474
дегомогенизация идеала 503
- полинома 466
декартов лист 178
делимое промкжуточное 87
дискриминант 408
дискриминант полинома 206
доминирующее отображение 604

задача кинематическая обратная 343
- - прямая 343
- неявного представления 70, 131, 167
- о принадлежности идеалу 65, 70, 128
- - - радикальному идеалу 233
- - решении полиномиальных уравнений 70, 128
- описания идеала 70, 102
- совместности 67, 224
заключение обобщенно следующее 379
- строго следующее 376
замыкание *Зарисского* 163, 250
- проективное 489, 505
знак перестановки 640
зонтик *Уитни* 176

идеал 45
- взвешенно однородный 512
- главный 60, 110
- детерминантный 148
- исключающий 152
- - проективный 499
- кольца 290, 639
- конечно порожденный 47
- максимальный 260
- многообразия 49
- мономиальный 95
- неприводимый 271
- однородный 476
- - простой 485
- - радикальный 482
- порожденный множеством полиномов 46
- примарный 270

- P-примарный 271
- простой 256
- - , принадлежащий идеалу 273
- радикальный 54, 229
- сизигий 434
- собственный 260
- соотношений 434
- старших членов 102
идеалы комаксимальные 248
изоморфизм кольцевой 288
- многообразий 309
инвариантный полином 415
индекс регулярности 574
исключающее упорядочение 102, 157
исключающий идеал 152
- - проективный 499
исчерпывающий базис *Грёбнера* 358, 669

касательная к многообразию 182
- поверхность скрученной кубики 34
касательное пространство 607
касательный конус 621
- - проективизированный 635
квадратичная гиперповерхность 465
квадрика 465, 516
- неособая 520
- особая 527
квартика 465
квинтика 465
кинематическая особенность 357, 360
кинематически избыточный робот 369
кисть робота 340
класс эквивалентности 285
кольца изоморфные 288
кольцевой гомоморфизм 228, 288
- изоморфизм 288
кольцо 416
- коммутативное 638
- координатное 306, 596
- полиномиальное 13
- полиномов 13, 75
комаксимальные идеалы 248
конечное поле 14
коника 516
коническое сечение 43
конструктивное множество **165**, 336
конус аффинный 473, 480
- касательный 621
- - проективизированный 635
конфигурационное пространство 342
координатная функция 306
координатное кольцо 306, 596
- подпространство 550, 557
координаты однородные **452**, 462
- плюккеровы 523
корректность операций 286
коэффициент монома 13
- полинома старший 83
коэффициенты мультиномиальные 431
кратность особой точки 191
- пересечения 180, 537
кривая в $\mathbb{P}^2(\mathbb{C})$ 532
- двойственная 447
- рациональная нормальная **493**
критерий *Бухбергера* S-пар **117**
кубика 465
- *Безье* 35
- скрученная 19

лексикографическое упорядочение 78
лемма *Диксона* 97
линейная часть полинома 607
линейно связное множество **542**, 546
линейное многообразие 21, **465**

- отображение 276
- упорядочение 77
линейчатая поверхность 522
локальные свойства многообразия 607

максимальный идеал 260
матрица максимального ранга 359
- неполного ранга 359
- перестановки 413
- *Сильвестра* 200
метод базисов *Грёбнера* 381
- *Ву* 388
- вырождения 548
минимальное разложение идеала 267
- - многообразия 266
минимальный базис *Грёбнера* 123
многообразие аффинное 17
- двойственное 447
- идеала 108, 477
- линейное 21, 465
- неприводимое 256, 478
- определенное идеалом 108
- приводимое 279
- проективное 465
- рациональное 325
- *Сегре* 494
- унирациональное 31
многообразия бирационально эквивалентные 325, 605
- изоморфные 309
- проективно эквивалентные 514
многоугольник управляющий 36
множество конструктивное 336
- линейно связное 542, 546
- особое 613
- уровня 283
моном 12
мономиальное упорядочение 77
- - взвешенное 101
- - градуированное 80, 486
- - - лексикографическое 80
- - - обратное лексикографическое 81
- - исключающего типа 159
- - исключающее 102, 159
- - лексикографическое 78
- - противоположное лексикографическое 84
мономиальный идеал 95
мультиномиальные коэффициенты 431
мультиполиномиальный результат 204
мультистепень полинома 83

наибольший общий делитель полиномов 61, 63, 235
наименьшее общее кратное мономов 113
- - - полиномов 295
насыщение идеала 255
неизбыточное объединение многообразий 266
- пересечение идеалов 267
- примарное разложение идеала 271
неособая квадрика 520
- точка 182, 613
неприводимое многообразие 256, 478
неприводимый идеал 271
- полином 194, 234
неявное представление 30
нильпотентный элемент 289
нормальная форма полинома 112

область главных идеалов (ОГИ) 60
- целостности 280, 638
обобщенный результант 212
образующие идеала 46
общая линейная группа 412

объединение многообразий неизбыточное 266
огибающая семейства 185
однородная компонента полинома 406, 510
однородные координаты 452, 462
однородный идеал 476
- - простой 485
- - радикальный 482
- полином 406, 464
оператор присваивания 643
- *Рейнольдса* 423
- условный 645
- цикла 644
определитель 639
орбита 440
ортоцентр 384
особая квадрика 527
- точка 134, 178, 182, 527, 613
особенность кинематическая 357, 360
особое множество 613
остаток 88
отображение доминирующее 604
- линейное 276
- обратного образа 311
- полиномиальное 277
- проекции 161, 600
- рациональное 321, 322
- регулярное 277
- *Сегре* 521

параметр 28
параметризация 28
- алгебраическая 160
- полиномиальная 30, 168
- рациональная 29
пересечение идеалов 242
- - неизбыточное 267
- полное 593
плоскость в $\mathbb{P}^3(k)$ 465
- аффинная 13
- двойственная проективная 461
- проективная 449, 452
плотное по *Зарисскому* подмножество 600
плюккеровы координаты 523
поверхность *Веронезе* 283
- - проективная 493
- *Энпепера* 176
- касательная скрученной кубики 34
- линейчатая 522
подгруппа 639
- изотропии 445
подкольцо 416
подматрица 617
подмногообразие 306
подмножество плотное по *Зарисскому* 600
подпространство координатное 550, 557
поле 11, 637
- алгебраически замкнутое 15
- бесконечное 14
- конечное 14
- положительной характеристики 238
- рациональных функций 318, 319, 605
- функций 319
- характеристики нуль 238, 412
- частных 318
полином 12, 75
- *Гильберта* 579
- - аффинный 574
- *Ньютона—Грегори* интерполяционный 569
- биоднородный 508, 512
- взвешенно однородный 508, 512
- инвариантный 415
- неприводимый 194, 234
- однородный 406, 464
- редуцированный 235
- редуцируемый к нулю 137

- свободный от квадратов 235
- симметрический 400
- целочисленный 200
- «частично» однородный 497
полиномиальная параметризация 30
полиномиальное отображение 277
полиномы, сравнимые по модулю идеала 285
полная степень монома 12
- - полинома 13
- - элемента из $\mathbb{Z}^n_{\geq n}$ 561
полное пересечение 593
порождающие группы 417
- подкольца 423
порождающие элементы идеала 46
порядок группы 412
правило *Крамера* 202, 639
предел прямых 625
представление неявное 30
- параметрическое рациональное 29
преобразование аффинное 351
- проективное линейное 513
приводимое многообразие 279
примарное разложение идеала 271
- - - неизбыточное 271
примарный идеал 270
принцип двойственности 450
- максимума 338
- минимума 338
проективная линейная группа 526
- плоскость 449, 452
- поверхность *Веронезе* 493
- прямая 449, 452, 465, 522
- эквивалентность 514
проективное замыкание 489, 505
- линейное преобразование 513
- многообразие 465
- пространство 462
проективный исключающий идеал 499
произведение идеалов 241
- упорядочений 101
производная формальная 68, 293, 607
промежуточное делимое 87
простой идеал 256, 485
- идеал, принадлежащий идеалу 273
пространство аффинное 13
- касательное 607
- конфигурационное 342
- операционное 342
- орбит 440
- проективное 462
- проективное двойственное 474
- сочленений 342
противоположное лексикографическое упорядочение 84
прямая аффинная 13, 453
- бесконечно удаленная 450, 453
- проективная 449, 452, 465, 522
- секущая 624
- *Эйлера* 384
псевдокод 642
псевдоостаток 389
псевдочастное 389
пучок многообразий 474
- поверхностей 309
- прямых 461

равенство рациональных отображений 323
радикал идеала 230
радикальный идеал 54, 229, 482
раздутие 634
разложение идеала примарное 271
- - - минимальное 271
- - - неизбыточное 271
- идеала минимальное 267

- многообразия минимальное 266
размерность 359, 551, 562, 565, 575, 579
- в точке 612
ранг квадрики 518
расширение идеала 249
рациональная нормальная кривая 493
- параметризация 29
- функция 605
рациональное многообразие 325
- отображение 321, 322
- параметрическое представление 29
рациональные отображение равные 323
регулярное отображение 277
редукция полинома 235
редуцированная часть полинома 68
редуцированное уравнение 533
редуцированный базис *Грёбнера* 123
- полином 235
- элемент 124
результант двух полиномов 200, 209
- мультиполиномиальный 204
- обобщенный 212
решение частичное 154, 161
робот 339
- кинематически избыточный 369
рука робота 340

свободная от квадратов часть полинома 68
свободный от квадратов полином 235
сдвиг координатного подпространства 557
семейство кривых 184
сжатие идеала 249
сизигия 434
- однородная 140
- старших членов 139
сильная теорема о нулях 231, 481
симметрическая функция элементарная 400
симметрический полином 400
система компьютерной алгебры
- - - AXIOM 647
- - - CoCoA 661
- - - Maple 650
- - - Mathematica 653
- - - REDUCE 655
- - - Macaulay 661
- - - MACSYMA 661
скрученная кубика 19
слабая теорема о нулях 222, 480
слой над точкой 337
смежный класс левый 446
собственный идеал 260
соединение «круг» 352
- винтовое 341
- призматическое 340
- спиральное 341
- шарнирное плоское 340
- - шаровое 341
специализация 355
стабилизатор 445
стандартные представители 295
стандартный базис 105
старший коэффициент полинома 83
- моном полинома 83
- член 57, 83
степень идеала 595
- полная монома 12
- - полинома 13
- - элемента из $\mathbb{Z}^n_{\geq n}$ 561
- проективного многообразия 595
- трансцендентности 602
стратегия двойная сахарная 146

- нормального выбора 146
- сахарная 146
строфоида 40
сумма идеалов 239
сфера *Римана* 463

теорема алгебры основная 13, 400
- *Аполлония* об окружности 374
- *Безу* 539
- геометрическая допустимая 373
- *Гильберта* о базисе 104
- - - нулях 225
- *Нётер* 425
- о замыкании 163, 330
- - нормальной форме квадратики 516
- - нулях в $k[V]$ 303
- - - сильная 231
- - - - проективная 481
- - - слабая 222
- - - - проективная 480
- - полиномиальном неявном представлении 169
- - принадлежности радикальному идеалу 233
- - продолжении 155, 211, 213
- - - проективная 500
- - разложении *Ласкера—Нётер* 272
- - размерности 576
- - - проективная 579
- - рациональном неявном представлении 174
- - симметрических полиномах 401
- об исключении 153
- - - обобщенная 174
- *Паппа* 384
- *Ферма* великая 26
тип 643
тождества *Ньютона* 407
- - несимметрические 411
точка *Штейнера* 387
- бесконечно удаленная 450
- гладкая 613
- неособая 182, 613
- особая 134, 179, 182, 527, 613
- перегиба 191
- схода 450
точки управляющие 36

убывающая цепь многообразий 110
унирациональное многообразие 31
упорядочение взвешенное 101
- градуированное лексикографическое 80
- - обратное лексикографическое 81
- исключающего типа 159
- исключающее 102, 159
- линейное 77
- лексикографическое 78
- мономиальное 77
- противоположное лексикографическое 84
управляющие точки 36
управляющий многоугольник 36
уравнение редуцированное 533
условие обрыва возрастающих цепей (УОВЦ) 107
условие обрыва убывающих цепей 263

фактор формы 44
факторкольцо 286
факторпространство 571
формальная производная 68, 293, 607
формула *Тейлора* 608, 630
- *Эйлера* 473
функции алгебраически независимые 379
функция *Гильберта* 577

- - аффинная 572
- координатная 306
- рациональная 605
- элементарная симметрическая 400

характеристика поля 238, 618

целочисленный полином 200
центроид 384
цикл 642
циклическая группа 413
циссоида 40

«частично» однородный полином 497
частичное решение 154, 161
частное идеалов 252
четверная группа Клейна 417
четырехлепестковая роза 25
член полинома 13

элемент нильпотентный 289
- редуцированный 124
элементарная симметрическая функция 400
элементы алгебраически независимые 597
эффектор 340

ядро гомоморфизма 294
- отображения 249

AXIOM 647
CoCoA 661
grevlex-упорядочение 81
grlex-упорядочения 80
invlex-упорядочение 84
lex-упорядочение 78
Macaulay 661
MACSYMA 661
Maple 650
Mathematica 653
REDUCE 655
R-последовательность 593
S-полином 113

Оглавление

Предисловие к русскому изданию 5

Предисловие к первому изданию 6

Предисловие ко второму изданию 9

1 Геометрия, алгебра и алгоритмы 11
§ 1. Полиномы и аффинное пространство 11
§ 2. Аффинные многообразия 17
§ 3. Параметризации аффинных многообразий 28
§ 4. Идеалы 45
§ 5. Полиномы от одной переменной 56

2 Базисы Грёбнера 70
§ 1. Введение 70
§ 2. Упорядочение мономов в $k[x_1, \ldots, x_n]$ 75
§ 3. Алгоритм деления в $k[x_1, \ldots, x_n]$ 85
§ 4. Мономиальные идеалы и лемма Диксона 95
§ 5. Теорема Гильберта о базисе и базисы Грёбнера 102
§ 6. Свойства базисов Грёбнера 111
§ 7. Алгоритм Бухбергера 119
§ 8. Первые применения базисов Грёбнера 128
§ 9. Дополнение. Усовершенствования алгоритма Бухбергера 136

3 Теория исключения 151
§ 1. Теоремы об исключении и продолжении 151
§ 2. Геометрия исключения 161
§ 3. Неявное представление 167
§ 4. Особые точки и огибающие 179
§ 5. Единственность разложения на множители и результанты 194
§ 6. Результанты и теорема о продолжении 209

4 Алгебро-геометрический «словарь» 221
§ 1. Теорема Гильберта о нулях . . . 221
§ 2. Радикальные идеалы и соответствие идеал—многообразие . . . 229
§ 3. Суммы, произведения и пересечения идеалов . . . 238
§ 4. Замыкание Зарисского и частные идеалов . . . 250
§ 5. Неприводимые многообразия и простые идеалы . . . 256
§ 6. Разложение многообразия в объединение неприводимых . . . 263
§ 7. Дополнение. Примарное разложение идеалов . . . 270
§ 8. Сводка результатов . . . 275

5 Полиномиальные и рациональные функции на многообразии 276
§ 1. Полиномиальные отображения . . . 276
§ 2. Факторкольца полиномиальных колец . . . 284
§ 3. Алгоритмические вычисления в $k[x_1,\dots,x_n]/I$ . . . 295
§ 4. Координатное кольцо аффинного многообразия . . . 306
§ 5. Рациональные функции на многообразии . . . 318
§ 6. Дополнение. Доказательство теоремы о замыкании . 330

6 Роботика и автоматическое доказательство геометрических теорем 339
§ 1. Геометрическое описание роботов . . . 339
§ 2. Прямая кинематическая задача . . . 345
§ 3. Обратная кинематическая задача и планирование движения . . . 353
§ 4. Автоматическое доказательство геометрических теорем 369
§ 5. Метод Ву . . . 388

7 Теория инвариантов конечных групп 399
§ 1. Симметрические полиномы . . . 399
§ 2. Конечные матричные группы и кольца инвариантов . 412
§ 3. Образующие кольца инвариантов . . . 422
§ 4. Соотношения между образующими и геометрия орбит 433

8 Проективная алгебраическая геометрия 448
§ 1. Проективная плоскость . . . 448
§ 2. Проективное пространство и проективные многообразия . . . 461
§ 3. Проективный алгебро-геометрический словарь . . . 475
§ 4. Проективное замыкание аффинного многообразия . . 485
§ 5. Проективная теория исключения . . . 494

§ 6. Геометрия квадрик . . . 5
§ 7. Теорема Безу . . . 5

9 Размерность многообразия 5
§ 1. Многообразие мономиального идеала . . . 5
§ 2. Дополнение мономиального идеала . . . 5
§ 3. Функция Гильберта и размерность многообразия . . . 5
§ 4. Элементарные свойства размерности . . . 5
§ 5. Размерность и алгебраическая независимость . . . 5
§ 6. Размерность и неособость . . . 6
§ 7. Касательный конус . . . 6

A Некоторые понятия из алгебры 6
§ 1. Поля и кольца . . . 6
§ 2. Группы . . . 6
§ 3. Определители . . . 6

B Псевдокод 6
§ 1. Вход, выход, переменные и константы . . . 6
§ 2. Операторы присваивания . . . 6
§ 3. Операторы цикла . . . 6
§ 4. Условный оператор . . . 6

C Системы компьютерной алгебры 6
§ 1. AXIOM . . . 6
§ 2. Maple . . . 6
§ 3. Mathematica . . . 6
§ 4. REDUCE . . . 6
§ 5. Другие системы . . . 6

D Темы для самостоятельных исследований 66
§ 1. Общие замечания . . . 66
§ 2. Предлагаемые темы . . . 66

Литература 67

Предметный указатель 67