АЛГЕБРА
ПЕРВЫЙ СЕМЕСТР

Алексей Львович Городенцев[1]

1996

[1]Независимый Московский Университет

Содержание

Лекция 1
Поля

▹Аксиомы поля ▹Расширения поля рациональных чисел ▹Поле комплексных чисел ▹Геометрические и алгебраические вычисления с комплексными числами ▹Правила раскрытия скобок и тригонометрические тождества ▹Гомоморфизмы полей

§1. Определение и примеры полей

1.1. Что такое поле. Интуитивно наиболее привычной алгебраической структурой является структура поля. Говоря наивно, поле — это такая «числовая область», в которой определены все четыре действия арифметики со всеми своими обычными свойствами. Модельный образец поля — это рациональные числа $\mathbb{Q}$. Строгое определение таково.

1.2. Определение. *Множество k называется полем, если на нём заданы две бинарные операции*[1]*, которые называют сложением: $(a,b) \longmapsto a+b$ и умножением: $(a,b) \longmapsto a \cdot b = ab$, и при этом выполнены следующие свойства:*

Аксиомы поля

1) Аксиомы сложения
   а) коммутативность (переместительный закон): $a+b=b+a \quad \forall a,b\in k$
   б) ассоциативность (сочетательный закон): $a+(b+c)=(a+b)+c \quad \forall a,b,c\in k$
   в) существование нейтрального элемента (нуля): $\exists 0\in k: \quad a=0=a \quad \forall a\in k$
   г) существование противоположного: $\forall a\in k \quad \exists(-a)\in k: \quad a+(-a)=0$
2) Аксиомы умножения
   а) коммутативность: $ab=ba \quad \forall a,b\in k$
   б) ассоциативность: $a(bc)=(ab)c \quad \forall a,b,c\in k$

[1] т. е. два правила, сопоставляющие каждой паре элементов $a,b\in k$ некие новые элементы из k, или, более научно, — два отображения из $k\times k$ в k

в) существование единицы: $\exists 1 \in k: \quad a \cdot 1 = a \quad \forall a \in k$

г) существование обратного: $\forall a \in k,\ a \neq 0 \quad \exists a^{-1} \in k: \quad a \cdot a^{-1} = 1$

3) Аксиома дистрибутивности (распределительный закон):

$$a(b+c) = ab + ac \quad \forall a, b \in k$$

4) Аксиома нетривиальности: $0 \neq 1$

1.2.1. Логические комментарии. Следуя современной моде, мы дали «максимально выжатый» список аксиом, из которого исключены все утверждения, являющиеся следствием остальных. Этот идущий от *логистиковков* (термин А.Пуанкаре) стиль подачи нового материала, бесспорно, не самый удобный для читателя: естественно было бы включить в наши аксиомы и такие (интуитивно ожидаемые из опыта работы с рациональными числами) дополнительные свойства операций:

Доп.1: В любом поле нуль единственен.

Доп.2: В любом поле единица единственна.

Доп.3: $\forall a \in k$ противоположный элемент $(-a)$ тоже единственен, в том смысле, что он однозначно определяется по a (отсюда и обозначение, зависящее лишь от а).

Доп.4: $\forall a \in k,\ a \neq 0$ обратный элемент a^{-1} также единственен.

Доп.5: $\forall a \in k \quad a \cdot 0 = 0$.

Доп.6: $(-1) \cdot a = (-a)$ (здесь в левой части стоит произведение элемента a на элемент, противоположный единице, а справа – элемент противоположный к a, и a priori неясно, с чего бы им совпадать)

1.2.2. Предложение. *Дополнительные свойства следуют из аксиом.*

Доказательство. *Доп.1*: Пусть 0_1 и 0_2 – любые два нуля. Тогда $0_2 = 0_2 + 0_1 = 0_1$ (первое равенство написано по аксиоме 1в для 0_1, а второе — по аксиоме 1в для 0_2). Таким образом два нуля равны.

Доп.2: аналогично.

Доп.3: Пусть $(-a)_1$ и $(-a)_2$ – любые два элемента, дающие 0 в сумме с a. Тогда $(-a)_1 = (-a)_1 + 0 = (-a)_1 + (a + (-a)_2) = ((-a)_1 + a) + (-a)_2 = 0 + (-a)_2 = (-a_2)$.

Доп.4: аналогично.

Доп.5: Пусть $a \cdot 0 = b$. Тогда $b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0+1) = a \cdot 1 = a$. Таким образом, $b+a$ и a – это две разных записи для одного и того же элемента. Прибавляя к этому элементу $(-a)$, мы получим новый элемент, который также допускает две разных записи: $b = b + a + (-a)$ и $0 = a + (-a)$. Тем самым $b = 0$.

Доп.6: Надо проверить, что $(-1) \cdot a + a = 0$. Имеем: $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = a \cdot ((-1) + 1) = a \cdot 0 = 0$ (по (Доп.5)). Предложение доказано.

1.2.3. Замечание. Рассуждение при доказательстве свойства (Доп.5) есть не что иное, как подробное объяснение привычной школьной процедуры *прибавления к обеим частям равенства одного и того же числа*. В дальнейшем такие подробности читателю предлагается восстанавливать самостоятельно.

Задача 1.1. Докажите, что аксиома нетривиальности ($0 \neq 1$) равносильна требованию, чтобы $k \neq \{0\}$.

Задача 1.2. Докажите, что требование $a \neq 0$ в аксиоме 2г существования обратного необходимо, ибо нуль не может иметь обратного в силу остальных аксиом.

1.3. Вычитание и деление. Определим еще две бинарных операции в поле k:

Вычитание: $(a, b) \longmapsto a - b \stackrel{\text{def}}{=} a + (-b)$ (определено для любых элементов поля)

Деление: $(a, b) \longmapsto a/b \stackrel{\text{def}}{=} ab^{-1}$ (определено $\forall a$ и $b \neq 0$).

Задача 1.3. Докажите, что $a - b$ можно было бы определить как единственный элемент из k, который в сумме с b дает a, и дайте аналогичное определение (с доказательством!) для a/b.

1.4. Примеры полей. Поле *рациональных чисел* $\mathbb{Q}$ (т.е. совокупность обыкновенных дробей с общеизвестными правилами действий над ними) является, как уже отмечалось, «основным первоисточником» для абстрактного определения поля.

Поле *вещественных чисел* $\mathbb{R}$ можно описывать двумя способами: либо как *пополнение* поля $\mathbb{Q}$ (*сечениями Дедекинда* или *последовательностями Коши*), либо независимо от $\mathbb{Q}$ как множество *бесконечных десятичных дробей*. В любом случае определение операций в $\mathbb{R}$ и проверка выполнения аксиом поля требуют определенной работы, которой посвящены первые главы стандартного курса анализа. Я буду предполагать, что эта работа была проделана вами в школе. Я буду считать также, что вы умеете изображать действительные числа *геометрически* — как точки *ориентированной числовой прямой*.

В каждом из трёх подходов к определению поля $\mathbb{R}$ имеется конструкция, отождествляющая поле $\mathbb{Q}$ с некоторым подмножеством в поле $\mathbb{R}$ причём это отождествление согласовано с операциями, так что всё равно – вычислять с рациональными числами как с обыкновенными дробями (т.е. по стандартным правилам поля $\mathbb{Q}$), или же как с действительными числами (по правилам действий в поле $\mathbb{R}$).

1.5. Подполя и расширения. Подмножество k в поле K называется *подполем*, если оно удовлетворяет аксиомам поля относительно тех операций сложения и умножения, которые имеются в K. Это равносильно тому, что все четыре арифметических операции над элементами из k не выводят за пределы k. *Расширением поля* k называется любое поле K, содержащее k в качестве *подполя*.

Например, $\mathbb{R}$ есть расширение поля $\mathbb{Q}$. В алгебре и теории чисел часто возникают другие расширения поля $\mathbb{Q}$.

1.5.1. Пример: $\mathbb{Q}[\sqrt{2}] \stackrel{\text{def}}{=} \{a+b\sqrt{2} \mid \quad a, b \in \mathbb{Q}\}$. На совокупности чисел вида $a+b\sqrt{2}$ можно определить сложение и умножение, просто раскрывая скобки (с учётом того, что $(\sqrt{2})^2 = 2$):

$$\begin{aligned}(a + b\sqrt{2}) \ + \ (c + \sqrt{2}) \quad &\stackrel{\text{def}}{=} \quad (a + c) + (b + d)\sqrt{2}. \\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \quad &\stackrel{\text{def}}{=} \quad (ac + 2bd) + (cb + ad)\sqrt{2}\end{aligned}$$

Задача 1.4. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ – это поле.

Подсказка: Для нахождение обратного элемента надо *домножить на сопряженное*:

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

1.5.2. Расширения поля $\mathbb{Q}$, , обобщающие предыдущую конструкция, можно строить следующим образом. Рассмотрим множество $\mathbb{Q}[\vartheta]$ выражений вида

$$\mathbb{Q}[\vartheta] \stackrel{\text{def}}{=} \{\xi = x_0\vartheta^{n-1} + x_1\vartheta^{n-1-1} + \cdots + x_{n-1-1}\vartheta + x_{n-1} \mid \text{ все } x_\nu \in \mathbb{Q}\}$$

где ϑ удовлетворяет алгебраическому уравнению

$$A(\vartheta) = a_0\vartheta^n + a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n = 0$$

При помощи этого уравнения степени ϑ^m с $m \geq n$ можно заменять на меньшие точно также, как и в предыдущем примере:

$$\vartheta^m = -a_n^{-1}\vartheta^{m-n}(a_0\vartheta^{n-1} + a_1\vartheta^{n-1-1} + \cdots + a_{n-1-1}\vartheta + a_{n-1})$$

А это, как и выше, позволяет определить на совокупности чисел вида $\xi = x_0\vartheta^{n-1} + x_1\vartheta^{n-1-1} + \cdots + x_{n-1-1}\vartheta + x_{n-1}$ сложение и умножение, которые следует делать по обычным правилам раскрытия скобок и приведения подобных слагаемых, но заменяя все возникающие по ходу дела степени ϑ с показателями, большими $(n-1)$, на степени, показатель которых лежит в требуемых пределах от 0 до $(n-1)$.

Задача 1.5. Проверьте, что в $\mathbb{Q}[\vartheta]$ выполняются все аксиомы поля, кроме аксиомы существования обратного элемента 2г.

Видимая трудность, возникающая при проверке аксиомы 2г, — подыскать замену трюку «умножения на сопряжённое». То, что реально требуется от этого трюка, — это возможность для каждого выражения $X(\vartheta) = x_0\vartheta^{n-1} + x_1\vartheta^{n-1-1} + \cdots + x_{n-1-1}\vartheta + x_{n-1}$ подобрать другое выражение $\bar{X}(\vartheta) = \bar{x}_0\vartheta^{n-1} + \bar{x}_1\vartheta^{n-1-1} + \cdots + \bar{x}_{n-1-1}\vartheta + \bar{x}_{n-1}$, так чтобы

$$X(\vartheta)\cdot\bar{X}(\vartheta) = q + Y(\vartheta)\cdot A(\vartheta),$$

где $q \in \mathbb{Q}$ – рациональное число, а из правого слагаемого выносится $A(\vartheta)$, так что согласно правилам действий в $\mathbb{Q}[\vartheta]$ это слагаемое обратится в нуль (ибо $A(\vartheta) = 0$). Поэтому будем иметь:

$$\frac{1}{X(\vartheta)} = \frac{\bar{X}(\vartheta)}{X(\vartheta)\bar{X}(\vartheta)} = \frac{1}{q}\bar{X}(\vartheta) \in \mathbb{Q}[\vartheta]$$

В случае $\vartheta^2 = 2$ из n° 1.5.1 возможность для такого манёвра у нас была: если $X(\vartheta) = x_0 + x_1\vartheta$, то полагая $\bar{X}(\vartheta) = x_0 - x_1\vartheta$, получаем $X(\vartheta)\bar{X}(\vartheta) = x_0^2 - \vartheta^2 x_1^2 - x_1^2(\vartheta^2 - 2)$. Разумеется, такая возможность есть не всегда.

Задача 1.6. Докажите, что $\mathbb{Q}[\vartheta]$ с $\vartheta^2 + \vartheta + 1 = 0$ является полем, а $\mathbb{Q}[\zeta]$ с $\zeta^3 + 1 = 0$ – не является.

Указание: число $1+\zeta \in \mathbb{Q}[\zeta]$ необратимо в $\mathbb{Q}[\zeta]$, а все числа $x_0+x_1\vartheta$ (составляющие $\mathbb{Q}[\vartheta]$) обратимы в $\mathbb{Q}[\vartheta]$.

Задача 1.7. Каким должно быть соотношение $a_0\vartheta^n + a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n = 0$ для того, чтобы совокупность чисел $\mathbb{Q}[\vartheta]$ составляла поле?

Утешение. Это трудная задача, и если не получается, – не волнуйтесь: её исчерпывающее решение будет дано в следующих двух лекциях.

1.6. Поле «мнимых» чисел. Заметим, что для конструкции расширения $\mathbb{Q}[\vartheta]$ поля $\mathbb{Q}$ совершенно безразлично *наличие настоящего числа* $\vartheta \in \mathbb{R}$, удовлетворяющего уравнению $a_0\vartheta^n + a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n = 0$. Иными словами, мы можем воспринимать ϑ не как действительное число, а как формальную букву, а элементы $\mathbb{Q}[\vartheta]$ — как формальные слова, над которыми производятся формальные преобразования по некоторым правилам.

За примером далеко ходить не надо. Положим $\mathbb{M} = \mathbb{R}[i]$, где $i^2+1=0$. Иначе говоря, $\mathbb{M}$ есть множество записей вида $a+bi$ с *вещественными* a и b, которые складываются и перемножаются по обычным правилам с учетом равенства $i^2=-1$:

$$\begin{aligned}(a+bi)+(c+di) &\overset{\text{def}}{=} (a+c)+(b+d)i\\ (a+bi)(c+di) &\overset{\text{def}}{=} (ac-bd)+(ad+bc)i\end{aligned}$$

1.6.1. Предложение. $\mathbb{M}$ – *поле.*

Доказательство. Коммутативность, ассоциативность и дистрибутивность сложения и умножения почти очевидны (однако проверьте их обязательно!). Нуль есть число $0+0i$, единица есть $1+0i$ (проверьте!). Противоположным к $a+bi$ будет $-a-bi$, обратным —

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Ясно, что $0 \neq 1$. Предложение доказано.

1.6.2. Замечание. Поля $\mathbb{Q}[\vartheta]$, где ϑ – «настоящие» числа типа $\sqrt{2}$, возникали еще в античных рассуждениях, которые происходили на геометрическом языке и не приводили к методологическим спорам, поскольку имели ясный геометрический смысл. Например, $\sqrt{5}$ – это гипотенуза прямоугольного треугольника со сторонами 1 и 2, а $\mathbb{Q}[\sqrt{5}]$ – это все отрезки, которые можно отложить, используя стороны этого треугольника и теорему Фалеса. Вычисления в поле $\mathbb{M} = \mathbb{R}[i]$ начали появляться в средние века при решении уравнений и имели несколько мистическую окраску, ибо необходимость прибегать к i с $i^2=-1$ для того, чтобы найти вещественный корень кубического уравнения с рациональными коэффициентами напоминает «сделку с дьяволом». Подсознательный протест против описанной выше конструкции поля $\mathbb{M}$ возник, я думаю, и у многих из вас. Причина в том, что математические построения лишь тогда входят в сознание с абсолютной ясностью и вызывают внутреннее удовлетворение, когда за ними стоят геометрические образы. Поэтому наряду с формально-алгебраической конструкцией поля $\mathbb{M}$, которое мы временно назовём *полем мнимых чисел*, мы дадим сейчас наглядно-геометрическое построение поля *комплексных чисел* $\mathbb{C}$, восходящее к Гауссу, Риману и Клейну (XIX век). Впоследствии эти два поля будут отждествлены, и название и обозначение для первого из них (не являющиеся общеупотребительными) мы после n° 2.8.2 применять никогда не будем.

§2. Комплексные числа

2.1. Что такое комплексные числа. Фиксируем на плоскости ориентированную прямую OX с отмеченной *начальной точкой* O и будем интерпритировать её как *числовую прямую*, изображающую поле $\mathbb{R}$ действительных чисел. Каждой точке z плоскости сопоставим её *радиус-вектор* $\vec{Oz}$ (в частности, начальной точке сопоставим нулевой вектор $\vec{O}$). Далее мы не будем различать точки и их радиус-векторы, ибо из контекста всегда будет ясно, что имеется в виду под z: сама точка z или вектор $\vec{Oz}$. Оснащённая таким образом плоскость называется *комплексной плоскостью*, а точки этой плоскости (и их радиус-векторы) называются *комплексными числами*.

У каждого комплексного числа z (радиус-вектора $\vec{Oz}$) имеются две важные геометрические характеристики:

модуль $|z|$ — это длина вектора $\vec{Oz}$;

аргумент $\mathrm{Arg}(z)$ — это *ориентированный угол* луча $[Oz)$ с лучом $[OX)$.

Про ориентированный угол надо сказать особо. По определению, он равен ориентированной длине той дуги[2] единичной окружности с центром в O, по которой надо поворачивать луч $[OX)$, чтобы совместить его с лучём $[Oz)$ (длина берется со знаком «+» при движении против часовой стрелки, и с «−» – в противном случае). Видно, что такая дуга определена *не однозначно*, а с точностью до *любого целого числа оборотов*. Таким образом, Arg(z) не есть конкретное число, но целое счётное множество действительных чисел, составляющих арифметическую пргрессию с разностью 2π. Это записывают в виде

$$\mathrm{Arg}(z) = \varphi + 2\pi n,\ n \in \mathbb{Z}\ ,$$

где φ – одно из значений угла. В старину сказали бы, что $\mathrm{Arg}(z)$ есть *многозначная функция* от комплексного числа z.

2.2. Определение операций. Сложение и умножение радиусов-векторов определим правилами:

сложение: обычное сложение векторов на плоскости;

умножение: премножение модулей и одновременное сложение аргументов, так что

$$\begin{aligned} |z_1 \cdot z_2| &= |z_1||z_2| \\ \mathrm{Arg}(z_1 \cdot z_2) &= \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2)\ , \end{aligned}$$

Важно осознать, что для векторов, лежащих на действительной числовой прямой OX, эти правила определяют обычные действия с действительными числами (минус на минус дает

[2] напомню, что длина дуги — это *действительным число*

плюс и т.п.). То, что такая геометрическая формулировка действий была придумана лишь в XIX веке ясно показывает, насколько трудно увидеть из одномерного мира, что этот мир есть срез двумерной геометрии.

2.3. Теорема. *Комплексные числа составляют поле.*

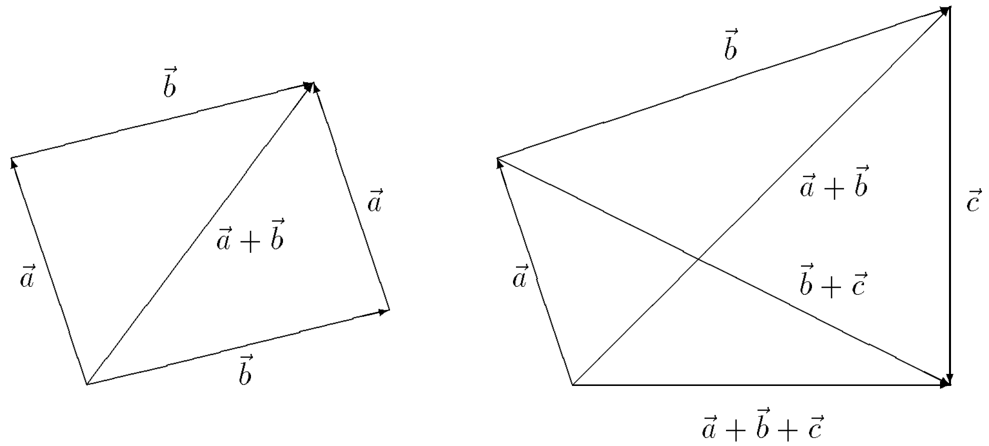


Рис. 1. Правило параллелограмма и правило треугольника

Доказательство. Аксиомы сложения хорошо известны из школьного курса геометрии как *правила сложения векторов*. Например, коммутативность есть не что иное, как *правило параллелограмма*, а ассоциативность следуют из *правила треугольника* (см. рис.рис.1). Коммутативность и ассоциативность умножения очевидны из определения. Единицей служит единичный вектор $\overrightarrow{01}$, лежащий на действительной оси (ибо его модуль равен 1, а угол – 0). Очевидно, что $0 \neq 1$.

Обратным к числу z будет число z^{-1}, модуль которого равен $|z|^{-1}$, а аргумент равен $\mathrm{Arg}(z^{-1}) = -\mathrm{Arg}(z)$ (луч на котором лежит z^{-1} симметричен лучу на котором лежит z относительно действительной оси).

Для проверки дистрибутивности заметим, что преобразование плоскости, состоящее в умножении всех точек на фиксированное комплексное число a: $z \mapsto az$ суть композиция поворота на угол $\mathrm{Arg}(a)$ вокруг 0 и гомотетии с коэффициентом $|a|$ относительно 0 (всё равно в каком порядке). Такое преобразование называется *поворотной гомотетией*. Аксиома дистрибутивности утверждает, что всё равно: применить поворотную гомотетию к сумме векторов $\vec b+\vec c$, либо применить её отдельно к $\vec b$ и отдельно к $\vec c$, а затем сложить полученные векторы. Но это очевидно, ибо и при повороте и при гомотетии параллелограмм для вычисления суммы $\vec b+\vec c$ перейдет в точности в параллелограмм для вычисления суммы их образов. Теорема доказана.

□

Задача 1.8. Убедитесь, что преобразование плоскости $z \mapsto z^{-1}$ является композицией осевой симметрии относительно действительной прямой OX и инверсии относительно единичной окружности $|z| = 1$.

2.3.1. Раскрытие скобок. Неформальное следствие состоит в том, что с геометрическими комплексными числами можно вычислять по всем правилам школьной алгебры. В частности, справедливы «формулы сокращенного умножения», из которых нам будут особенно полезны следующие две.

Задача 1.9. Докажите, что в любом поле имеют место равенства:

$$\begin{aligned} &\text{а)}\quad (a^m - b^m) : (a-b) &&= a^{m-1} + a^{m-2}b + a^{m-3}b^2 + \cdots + ab^{m-2} + b^{m-1} \\ &\text{б)}\quad (a_1 + a_2 + \cdots + a_k)^n &&= \sum_{\nu_1+\ldots+\nu_k=n} \frac{n!}{\nu_1!\nu_2!\cdots\nu_k!} a_1^{\nu_1} a_2^{\nu_2} \cdots a_k^{\nu_k} \end{aligned}$$

(суммирование производится по всем различным упорядоченным наборам неотрицательных целых чисел $(\nu_1, \nu_2, \ldots, \nu_k)$, сумма которых равна n).

Замечания к пункту (б):

1. Применительно к «любому полю» условие требует уточнения, поскольку коэффициент в правой части (б) – *натуральное число*. В произвольном поле этот коэффициент обозначает (по определению) сумму соответствующего количества *единиц этого поля*. В следующей лекции мы увидим, что это может отличаться от интуитивного представления о натуральном числе. Однако в поле комплексных чисел мы получим *настоящее натуральное число*, которое можно воспринимать как натуальную точку действительной прямой.

2. Определение коэффициента при $a_1^{\nu_1} a_2^{\nu_2} \cdots a_k^{\nu_k}$ тесно связано с комбинаторной задачей подсчета количества всевозможных слов , которые можно составить из n букв, из которых ν_1 штук букв a_1, ν_2 штук букв a_2, … , ν_k штук букв a_k. Прежде, чем выводить общую формулу, потренируйтесь, подсчитав, сколько слов (не обязательно осмысленных) можно получить, переставляя буквы в словах: рок, урок, шнурок, курок, колобок (хорошая идея — выписывать слова подряд по алфавиту).

2.4. Алгебраическая запись формул. Для алгебраической записи векторов на комплексной плоскости удобно ввести прямоугольные координаты OXY, ось OX которых совпадает с действительной прямой. Базисные векторы осей OX и OY обозначаются $\vec{1}$ и $\vec{\imath}$ (напомню, что $\vec{1}$ есть единица поля $\mathbb{C}$ (см.рис.рис.2)).

Произвольный вектор z имеет координаты: (x, y) – проекции точки z на оси. Таким образом вектор $\overrightarrow{Oz}$ может быть выражен через базисные векторы $\vec{1}$ и $\vec{\imath}$ в виде

$$\overrightarrow{0z} = x \cdot \vec{1} + y \cdot \vec{\imath}.$$

Поскольку умножение вектора на плоскости на вещественное число совпадает (как легко видеть) с умножением этого вектора как комплексного числа на то же вешественное число, но уже рассматриваемое как комплексное, предыдущая формула представляет собой *соотношение в поле* $\mathbb{C}$. Обычно его записывают не столь помпезно как выше, а в виде:

$$z = x + yi,$$

опуская стрелку над i и $\vec{1}$ (т.к. умножение на единицу поля вообще принято опускать).

Эта запись называется *алгебраическим представлением* комплексного числа z и чрезвычайно удобна, поскольку по теореме Теор.2.3 и следствию зад.1.9 мы вольны в вычислениях с такими записями пользоваться всем арсеналом школьных тождеств. Важно отметить, что действительные числа x и y в представлении $z = x+yi$ *однозначно* определяются по z (как координаты). Они обозначаются $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ и называются *действительной и мнимой частью* числа z. Если $\mathrm{Arg}(z) = \varphi$, то имеют место очевидные формулы:

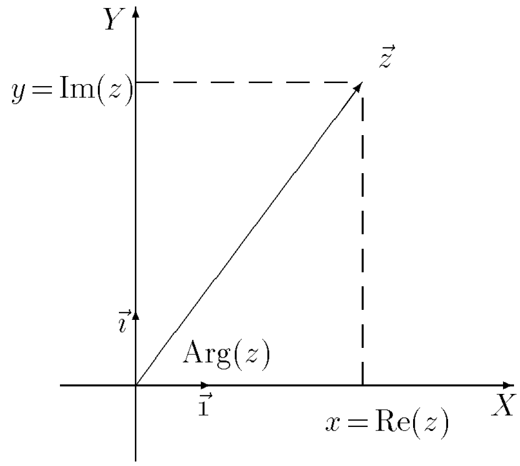


Рис. 2. Координаты на $\mathbb{C}$

$$x = |z|\cos(\varphi) \quad y = |z|\sin(\varphi)$$

$$|z| = \sqrt{x^2+y^2} \quad \mathrm{Arg}(z) = \arccos\left(x/\sqrt{x^2+y^2}\right) + 2\pi n = \arcsin\left(y/\sqrt{x^2+y^2}\right) + 2\pi n$$

Итак, всякий $z \in \mathbb{C}$ представляется в виде

$$z = x + iy = |z|(\cos\varphi + i\sin\varphi),$$

и эти выражения суть алгебраические равенства в поле $\mathbb{C}$, с которым мы можем вычислять пользуясь правилами раскрытия скобок, тождествами сокращённого умножения и т.п.

2.5. Примеры вычислений с комплексными числами. Комплексные числа являются удивительно гибким и могучим инструментом практически во всех областях естествознания. Причина в том, что при вычислениях с комплексными числами одинаково хорошо работают оба математических языка – и алгебраический язык формул, и геометрический язык картинок.

2.5.1. Корни из -1. Прямо из определения умножения получаем: $i^2 = i \cdot i = -1$ (т.к. $\mathrm{Arg}(i^2) = 2 \cdot \pi/2 = \pi$ и $|i^2| = 1$. Поэтому имеем разложение $z^2 + 1 = (z+i)(z-i)$, из которого следует, что уравнение $z^2 + 1 = 0$ имеет в поле $\mathbb{C}$ два корня: i и $-i$.

Задача 1.10. Докажите, что в произвольном поле уравнение

$$(x-a_1)(x-a_2)\cdots(x-a_k) = 0$$

имеет ровно k корней $\qquad x = a_1,\ \ldots,a_k.$

2.5.2. Основные тригонометрическин тождества. Пусть z_1 и z_2 – два числа, лежащие на единичной окружности: $|z_1| = |z_2| = 1$. Тогда $z_1 = \cos\varphi_1 + i\sin\varphi_1$ и $z_2 = \cos\varphi_2 + i\sin\varphi_2$. По определению умножения, $|z_1z_2| = 1$ и $\mathrm{Arg}(z_1z_2) = \varphi_1 + \varphi_2$, то есть

$$z_1z_2 = \cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)$$

С другой стороны, из дистрибутивности получаем

$$\begin{aligned} z_1z_2 &= (\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) = \\ &= \Big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2\Big) + i\Big(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2\Big) \end{aligned}$$

(мы воспользовались тем, что $i^2 = -1$). Сравнивая действительные и мнимые части, немедленно получаем основные тригонометрические тождества:

$$\begin{aligned} \cos(\varphi_1 + \varphi_2) &= \cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 \\ \sin(\varphi_1 + \varphi_2) &= \cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2 \end{aligned}$$

Это рассуждение наводит на мысль, что всё казуистическое изобилие формул школьной тригонометрии есть лишь бесформенная тень от стройного сооружения, построенного по простым правилам — аксиомам поля, выполненным в поле комплексных чисел $\mathbb{C}$.

2.5.3. Кратные углы. Пусть $|z| = 1$ и $z = \cos\varphi + i\sin\varphi$. Тогда по определению: $z^n = \cos(n\varphi) + i\sin(n\varphi)$. С другой стороны, по формуле бинома (которая получается из п.(б) зад.1.9 при $k = 2$, когда коэффициенты при $a_1^{\nu_1}a_2^{\nu_2} = a_1^{\nu}a_2^{n-\nu}$ принимают вид $\frac{n!}{\nu!(n-\nu)!}$ и обозначаются $\binom{n}{\nu}$ или C_n^k; они называются *биномиальными коэффициентами*) имеем:

$$\begin{aligned} &z^n = (\cos\varphi + i\sin\varphi)^n = \\ &= \cos^n\varphi + i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi - i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \cdots = \\ &= \left[\binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots\right] + \\ &\qquad + i\cdot\left[\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots\right] \end{aligned}$$

Отсюда получаем формулы для кратных углов:

$$\begin{aligned} \cos(n\varphi) &= \binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots \\ \sin(n\varphi) &= \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots \end{aligned}$$

Задача 1.11. Докажите, что при нечётном n функция $\sin(n\varphi)/\sin\varphi$ является многочленом от $\sin^2\varphi$ и найдите его степень, корни и старший коэффициент. Выпишите этот многочлен явно для $n = 3$ и $n = 5$.

Задача 1.12. Докажите для нечётных n тождество:

$$\frac{\sin(n\varphi)}{\sin\varphi} = (-4)^{\frac{n-1}{2}}\prod_{\nu=1}^{\frac{n-1}{2}}\left(\sin^2\varphi - \sin^2\frac{2\pi\nu}{n}\right)$$

Задача 1.13. В единичную окружность с ценром в начале координат вписан правильный m-угольник (m – нечётно) так, что одна из вершин находится в точке (1,0). Многоугольник поворачивают на угол φ вокруг начала координат против часовой стрелки. Вычислите произведение ординат вершин повернутого многоугольника.

2.6. Уравнение деления круга. Решим в поле $\mathbb{C}$ так называемое *уравнеие деления круга на n частей*: $z^n = 1$. Оно раносильно двум геометрическим соотношениям на вектор z: $|z|^n = 1$ и $n\mathrm{Arg}(z) = 0 + 2\pi k$ (где $k \in \mathbb{Z}$ — любое). Отсюда получаем ровно n различных корней, располагающихся на единичной окружности в вершинах правильного n-угольника (см.рис. рис.3 для $n = 5$):

$$|z_\nu| = 1, \quad \mathrm{Arg}(z_\nu) = 2\pi\nu/n, \text{ где } \nu = 0, 1, \ldots, (n-1)$$

Задача 1.14. Выразите $\cos 36°$ и $\sin 36°$ в радикалах.
Указание: после деления обеих частей на $z - 1$, уравнение $z^5 - 1 = 0$ становится *возвратным* и сводится к квадратному подстановкой $t = z + 1/z$.

2.7. Гомоморфизмы. Предыдущие вычисления показывают, что геометрическое поле комплексных чисел $\mathbb{C}$ «ничем не отличается» от формального поля мнимых чисел $\mathbb{M}$, веденного в n° 1.6. Для придания точного смысла фразе «ничем не отличается» придумано понятие гомоморфизма. Для сравнения множеств обычно используют их отображения друг в друга. Если множества имеют какую-либо алгебраическую структуру, то рассматривают не любые отображения, а только отображения, сохраняющие эту структуру. Такие отображения называют *гомоморфизмами*. В случае полей точное определение звучит так:

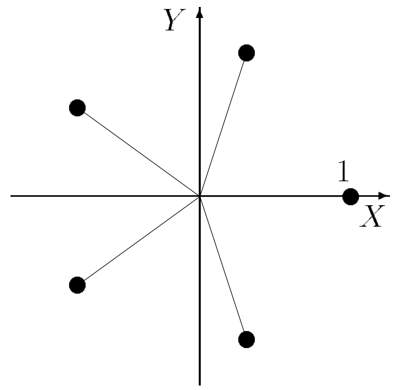


Рис. 3. Корни уравнения $z^5 = 1$

2.8. Определение. *Отображение полей $\sigma\colon K \longrightarrow L$ называется **гомоморфизмом**, если $\forall a, b \in K$ в поле L выполняются соотношения*

$$\begin{aligned} \sigma(a+b) &= \sigma(a) + \sigma(b) \\ \sigma(ab) &= \sigma(a)\sigma(b) \end{aligned}$$

Оказывается, требование совместимости с алгебраической структурой накладывает на отображение очень жёсткие ограничения.

2.8.1. Предложение. *Для любого гомоморфизма полей $\sigma\colon K \longrightarrow L$ обязательно выполнены следующие свойства:*

$$\begin{array}{lrcll} \text{а)} & \sigma(0) & = & 0 & \\ \text{б)} & \sigma(1) & = & 1, & \textit{если только } \sigma(K) \neq \{0\} \\ \text{в)} & \sigma(a-b) & = & \sigma(a) - \sigma(b) & \forall a, b \in K \\ \text{г)} & \sigma(a/b) & = & \sigma(a)/\sigma(b), & \textit{если только } b \neq 0 \textit{ и } \sigma(K) \neq \{0\} \end{array}$$

Более того: либо $\sigma(K) = \{0\}$, либо σ — вложение (то есть переводит разные элементы из K в разные элементы из L)

Терминологическое замечаеие. Гомоморфизм, переводщий всё поле K в нуль поля L, называется *тривиальным*, или *нулнвым*. Гомоморфизм, являющийся одновременно вложением, называется *инъективным* или *мономорфизмом*. Гомоморфизм, являющийся взаимнооднозначным, называется *изоморфизмом*.
Доказательство. (а): $\forall a \in K$ имеем

$$\sigma(a) = \sigma(a+0) = \sigma(a) + \sigma(0) \; .$$

Вычитая из левой и правой частей этого равенства $\sigma(a)$, получим $\sigma(0) = 0$.
(б): аналогично, только надо выбрать a так, чтобы $\sigma(a) \neq 0$ (т.е. был обратим).
(в): вычтем из левой и правой частей равенства $\sigma(a-b) + \sigma(b) = \sigma(a-b+b) = \sigma(a)$ число $\sigma(b)$.
(г): аналогично в).

Наконец, для доказательства последнего утверждения допустим, что σ не является вложением. Тогда найдутся $b, c \in K$ такие, что $b \neq c$ и $\sigma(b) = \sigma(c)$. Т.к. $d = b - c \neq 0$, оно обратимо в K. Но $\sigma(d) = \sigma(b) - \sigma(c) = 0$, и поэтому $\forall a \in K$ имеем $\sigma(a) = \sigma(add^{-1}) = \sigma(a)\sigma(d)\sigma(d^{-1}) = 0$. Таким образом, $\sigma(K) = \{0\}$ и σ тривиален. Предложение доказано.

2.8.2. Пример. Поле комплексных чисел $\mathbb{C}$ изоморфно полю мнимых чисел $\mathbb{M}$. Изоморфизм задаётся сопоставлением числу $\alpha + i\beta \in \mathbb{R}[i] = \mathbb{M}$ вектора с координатами (α, β) на комплексной плоскости $\mathbb{C}$. Мы отождествим $\mathbb{C}$ с $\mathbb{M}$ посредством этого изоморфизма и далее не будем их различать (и пользоваться обозначением $\mathbb{M}$).

2.8.3. Пример. Имеется ровно один нетождественный изоморфизм поля $\mathbb{C}$ на себя, сохраняющий неподвижным вещественное подполе $\mathbb{R} \subset \mathbb{C}$. Он переводит $z = x + iy$ в $\bar{z} = x - iy$ и называется *комплексным сопряжением*. Действительно, если $\mathbb{R}$ неподвижно, то $\sigma(x+iy) = x + y\sigma(i)$, и σ однозначно определяется заданием $\sigma(i)$. Поскольку $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, значение $\sigma(i)$ есть корень уравнения $t^2 = -1$. У этого уравнения в поле $\mathbb{C}$ имеется ровно два корня: i и $-i$. Тем самым, если нетривиальный гомомрфизм существует, то он совпадает с комплексным сопряжением. Остаётся проверить, что отображение $z \mapsto \bar{z}$ и в самом деле гомомрфизм.

Задача 1.15. Сделайте это.

2.8.4. Замечание. Интуитивно, последнее утверждение в предложении из Пр.2.8.1 означает, что два поля K и L либо вообще «несравнимы» (то есть между ними нет нетривиальных гомоморфизмов), либо одно из них можно отождествить с подполем в другом. Важно отметить, что отождествить поле K с подполем в L можно, как правило, многими разными способами.

2.8.5. Пример. Имеется ровно два вложения поля $\mathbb{Q}[\sqrt{2}]$ в поле $\mathbb{C}$. Образ обоих содержится в вещественном подполе $\mathbb{R} \subset \mathbb{C}$. Первое — тождественно, а второе переводит $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ в $a - b\sqrt{2} \in \mathbb{R} \subset \mathbb{C}$. Действительно, пусть $\sigma\colon \mathbb{Q}[\sqrt{2}] \hookrightarrow \mathbb{C}$ — вложение. Тогда $\sigma(a + b\sqrt{2}) = a + b\sigma(\sqrt{2})$ (ибо при $k \in \mathbb{N}$, $k = \underbrace{1 + 1 + \ldots + 1}_{k \text{ раз}}$ имеем $\sigma(k) = k\sigma(1) = k$, а значит и для любого рационального $a = p/q$ получим $\sigma(a) = \sigma(p)/\sigma(q) = p/q = a$). Тем самым, σ однозначно определяется значением $\sigma(\sqrt{2})$. Но $\sigma(\sqrt{2}) \in \mathbb{C}$ обязан быть корнем уравнения $z^2 = 2$ (почему?), а у такого уравнения в поле $\mathbb{C}$ ровно два корня: $\sqrt{2}$ и $-\sqrt{2}$. Поэтому имеется ровно две возможности: $\sigma(\sqrt{2}) = \sqrt{2}$ и $\sigma(\sqrt{2}) = -\sqrt{2}$.

Задача 1.16. Докажите, что поле $\mathbb{Q}[\vartheta]$ (где $\vartheta^2 + \vartheta + 1 = 0$) допускает ровно два вложения в поле $\mathbb{C}$. При одном из них ϑ переходит в $(-1 + i\sqrt{3})/2$, при другом — в $(-1 - i\sqrt{3})/2$.

Задача 1.17. Докажите, что поле $\mathbb{Q}[\vartheta]$ (где $\vartheta^3 + \vartheta + 1 = 0$) допускает три вложения в $\mathbb{C}$. Образ одного из них содержится в $\mathbb{R}$, а образы двух других — комплексно сопряжены.

Лекция 2
Коммутативные кольца

▷Определение и примеры коммутативных колец ▷Факторизация ▷Идеалы ▷НОД, взаимная простота и идеалы в кольце $\mathbb{Z}$ ▷Поле $\mathbb{Z}/p\mathbb{Z}$ ▷Определение и примеры гомоморфизмов колец ▷Простое подполе и характеристика ▷Гомоморфизм Фробениуса и малая теорема Ферма ▷Теорема о структуре гомоморфизма ▷Прямые суммы колец ▷Китайская теорема об остатках

§1. Определение и примеры коммутативных колец

1.1. Коммутативное кольцо с единицей — это множество A, на котором заданы две бинарные операции (сложение и умножение), которые удовлетворяют всем аксиомам поля (см. Опр.1.2 лекции 1) кроме аксиомы нетривиальности (4) и аксиомы существования обратного элемента (2г).

Выкидывая аксиому (4), мы допускаем в качестве колец *тривиальные кольца*, состоящие из одного нуля. Это делается исключительно ради формального удобства некоторых предстоящих в дальнейшем построений. Напротив, отсутствие обратных элементов является важным существенным отличием колец от полей: *деление* в кольце возможно не всегда, и поэтому между элементами кольца возникает новое нетривиальное отношение — они могут делиться или не делиться друг на друга.

Как и в прошлой лекции, к определению автоматически прилагается целый ряд дополнительных свойств операций:

Задача 2.1. Докажите, что в любом кольце выполнены следующие свойства сложения и умножения (ср. с Пр.1.2.2):

а) ноль единственен;
б) противоположный элемент единственен;
в) $0 \cdot a = 0 \quad \forall a \in A$;
г) $(-1) \cdot a = (-a)$;
д) единица единственна.

1.1.1. Несколько новых понятий. Нетривиальность деления принуждает к введению новых названий для тех явлений, которые не были заметны в рамках полей.

Элемент a кольца A называется *обратимым*, если существует элемент $a^{-1} \in A: \ a \cdot a^{-1} = 1$ (в поле все ненулевые элементы были обратимы). Множество обратимых элементов кольца A обозначается A_* и называется *мультипликативной группой* кольца A или *группой обратимых элементов*.

Ненулевой элемент a кольца A называется *делителем нуля*, если существует ненулевой элемент $b \in A$, такой что $ab = 0$ (в поле такого не бывает, поскольку умножив обе части последнего равенства на b^{-1}, получим $a = 0$). Кольцо без делителей нуля называется *целостным*.

Ненулевой элемент a называется *нильпотентным*, если $a^n = 0$ для некоторого натурального n. Разумеется, все нильпотенты автоматически являются делителями нуля (и в поле отсутсутствуют).

> Задача 2.2. Докажите, что обратимый элемент не может быть делителем нуля, и что если обратный элемент существует, то единственен.

> Задача 2.3. Докажите, что делители нуля не могут быть обратимы.

Рассмотрим некоторые примеры колец,

1.2. Кольцо $\mathbb{Z}$ целых чисел — простейший нетривиальный пример кольца. Это кольцо замечательно тем, что “не содержит ничего лишнего”: нуль 0, единица 1, противоположный к единице элемент -1 и всевозможные их суммы (чуть позже мы увидим, что $\mathbb{Z}$ — не единственное кольцо с такими свойствами). Обратимыми элементами в $\mathbb{Z}$ являются только 1 и -1. Кольцо $\mathbb{Z}$ является целостным.

1.3. Расширения $\mathbb{Q}[\vartheta]$ поля $\mathbb{Q}$, рассматривавшиеся в n° 1.5.2 лекции 1, все являются коммутативными кольцами вне зависимости от соотношения, которому удовлетворяет ϑ. Более того, аксиомы кольца останутся выполненными, если заменить $\mathbb{Q}$ на произвольное коммутативное кольцо. Один пример (восходящий к Гауссу) здесь заслуживает особого внимания.

1.4. Гауссовы целые числа $\mathbb{Z}[i] = \{x + iy \in \mathbb{C} | \ x, y \in \mathbb{Z}\}$ составляют целостное (как и всякое подкольцо в поле) подкольцо в $\mathbb{C}$. Обратимых элементов в $\mathbb{Z}[i]$ роно четыре: 1, -1, i, $-i$ (почему?). Геометрически $\mathbb{Z}[i]$ изображается целочисленной решёткой на комплексной плоскости.

Кольцо $\mathbb{Z}[i]$ имеет много приложений в арифметике. Например, оно играет важную роль в задаче об описании целых чисел, представимых в виде суммы двух квадратов. Дело в том, что квадратичная форма x^2+y^2 над $\mathbb{Z}[i]$ разлагается в произведение двух линейных множителей: $x^2+y^2 = (x+iy)(x-iy)$, и задача представления натурального числа в виде суммы квадратов двух целых чисел оказывается равносильной задаче о разложимости натурального числа как элемента $\mathbb{Z}[i]$ в произведение двух комплексно-сопряженных множителей, также лежащих в $\mathbb{Z}[i]$.

При таком подходе задача сильно проясняется. Скажем, если число m разложено в произведение $m = m_1 m_2$, и оба сомножителя m_1, m_2 представимы в виде суммы квадратов двух целых чисел, то и m представимо: равенства

$$m_1 = a_1^2 + b_1^2 \qquad \text{и} \qquad m_2 = a_2^2 + b_2^2$$

означают, что $m_1 = z_1\bar{z}_1$, $m_2 = z_2\bar{z}_2$ (где $z_\nu = a_\nu + b_\nu \in \mathbb{Z}[i]$), а значит

$$m = (z_1 z_2)\overline{(z_1 z_2)} = |z_1 z_2|^2 = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$$

Если доказать для кольца $\mathbb{Z}[i]$ аналог *основной теоремы арифметики* (что будет сделано на следующей лекции), то это вычисление полностью сводит исходную задачу к исследованию того, какие *простые* натуральные числа остаются простыми и в $\mathbb{Z}[i]$.

К сожалению, недостаток времени вынуждает меня здесь прервать дальнейшее обсуждение этой проблемы, но настойчивый заинтересовавшийся читатель сможет разобраться в ней до конца, решив следующие две (не являющиеся обязательными для понимания дальнейшего и довольно трудные) задачи[1]:

Задача 2.4. Докажите, что для представимости числа $n \in \mathbb{N}$ в виде суммы двух квадратов целых чисел (ноль тоже разрешается в качестве одного из двух квадратов!) необходимо и достаточно, чтобы это число имело вид

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_s \cdot k^2 ,$$

где $k \in \mathbb{Z}$ — любое, а $p_1, \dots, p_s$ — натуральные простые числа, представимые в виде суммы двух квадратов.

Задача 2.5. Докажите, что простое $p \in \mathbb{N}$ тогда и только тогда представимо в виде суммы двух квадратов, когда имеет вид $p = 4d + 1$ (т. е. имеет остаток 1 от деления на 4).

1.5. Кольцо $k[x]$ многочленов над полем k. Это кольцо состоит из *формальных выражений* вида

$$P(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n,$$

где $a_\nu \in k$, k — поле, $n \in \mathbb{N}$, а x — *формальный символ*, называемый *переменной*. Подчеркну, что с точки зрения кольцевой структуры мы рассматриваем многочлены лишь как слова, и содержательную информацию для нас будет нести лишь последовательность символов[2] $(a_0, a_1, a_2, \dots, a_n)$.

1.5.1. Определение сложения и умножения. При описании операций, удобно считать, что многочлен есть *бесконечное* вправо выражение $a_0 + a_1 x + a_2 x^2 + \cdots$, в котором, однако, лишь конечное число коэффициентов a_ν *отлично от нуля*. Тогда сумму и произведение многочленов

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \text{и} \qquad B(x) = b_0 + b_1 x + b_2 x^2 + \cdots$$

можно определить при помощи алгоритмов для вычисления последовательности коэффициентов суммы и произведения по коэффициеньам A и B. А именно, назовём *суммой* $S(x) =$

[1]Эти, а также рад других задач о Гауссовых числах, предполагается подробно обсудить на упражнениях. При их решении очень помогает владение техникой вычетов и разложения на простые множители (см. конец этой и следующей лекций, а также книгу Роузена и Айэрленда "Классическое введение в современную теорию чисел").

[2]Если вы откроете толстую книжку вроде Ленга, то увидите, что многочлены там "строго определяются" именно как последовательности коэффициентов $(a_0, a_1, a_2, \dots, a_n)$, а x и $+$ вообще в определении не упоминаются!

$A(x) + B(x) = s_0 + s_1x + s_2x^2 + \cdots$ многочлен, коэффициенты s_ν которого вычисляются по правилу

$$s_\nu = a_\nu + b_\nu,$$

а *произведением* $P(x) = A(x)B(x) = p_0 + p_1x + p_2x^2 + \cdots$ — многочлен с коэффициентами

$$p_\nu = \sum_{\alpha+\beta=\nu} a_\alpha b_\beta = a_0b_\nu + a_1b_{\nu-1} + \cdots + a_0b_\nu$$

Задача 2.6. Убедитесь, что эти формулы в точности соответствуют известным вам правилам раскрытия скобок и приведения подобных слагаемых.

Очень важное наблюдение состоит в том, что при перемножении *бесконечных сумм* $A(x)$ и $B(x)$ на значение коэффициента при x^k у произведения *влияет лишь конечное число* коэффициентов каждого из сомножителей, а потому он вычисляется за конечное число шагов.

1.5.2. Степень. Номер самого правого ненулевого коэффициента называется *степенью* многочлена $a_0 + a_1x + a_2x^2 + \cdots$. Легко заметить (внимательно продумайте это!), что *степень произведения* двух многочленов равна *сумме степеней* сомножителей, а *старший и младший коэффициенты* произведения равны, соответственно, *произведению старших и младших коэффициентов* сомножителей. Из этого немедленно следует, что в кольце $k[x]$ многочленов над полем k нет делителей нуля, а обратимые элементы в $k[x]$ — это в точности многочлены степени нуль , не равные нулю тождественно (т. е. ненулевые константы и только они).

Задача 2.7. Докажите, что $k[x]$ действительно является кольцом (т. е. проверьте, что определённые выше сложение и умножение удовлетворяют аксиомам коммутативного кольца с единицей).

1.6. Кольцо формальных степенных рядов $k[[t]]$ над полем k состоит из бесконечных формальных выражений вида $a_0 + a_1t + a_2t^2 + \cdots$, где в отличие от кольца многочленов *допускается бесконечно много ненулевых коэффициентов*. Операции определяются также, как и в кольце многочленов. Для бесконечных рядов теряет смысл понятие степени, но по-прежнему полезно бывает следить за *младшим* (т. е. самым левым ненулевым) членом и *свободным* членом a_0. Так, ввиду того, что младший коэффициент произведения рядов равен произведению младших коэффициентов сомножителей, кольцо $k[[t]]$ является целостным.

1.6.1. Предложение. *Множество обратимых элементов в $k[[t]]$ состоит из всех рядов с ненулевым свободным членом:*

$$k[[t]]_* = \{A(t) = a_0 + a_1t + a_2t^2 + \cdots \mid a_0 \neq 0\}.$$

Доказательство. Ряд с нулевым свободным членом $a_0 = 0$, очевидно, необратим: из его произведения с любым рядом выносится t. Пусть теперь $a_0 \neq 0$. Методом *неопределенных коэффициентов* подберём такой ряд

$$B(t) = b_0 + b_1t + b_2t^2 + \cdots,$$

чтобы $A(t)B(t) = 1$. Приравнивая в левой и правой частях коэффициенты при одинаковых степенях t, получаем систему уравнений:

$$\begin{array}{rcl} a_0b_0 &=& 1 \\ a_0b_1 + a_1b_0 &=& 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &=& 0 \\ \cdots && \\ a_0b_\nu + a_1b_{\nu-1} + \cdots + a_\nu b_0 &=& 0 \\ \cdots && \end{array},$$

из которой b_ν последовательно определяются по рекуррентным формулам:

$$\begin{array}{rcl} b_0 &=& a_0^{-1} \\ b_k &=& -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0). \end{array}$$

Предложение доказано.

1.6.2. Пример. Если $A(t) = 1 - t$, то предыдущее вычисление даёт:

$$(1-t)^{-1} = 1 + t + t^2 + t^3 + \cdots$$

(формула суммирования геометрической прогрессии).

Задача 2.8. Вычислите $(1 + t + t^2)^{-1}$.

1.7. Кольца $A[x]$ **и** $A[[x]]$ многочленов и формальных степенных рядов *над кольцом* A определяются дословно также как и над полем, только коэффициенты берутся уже не из поля k, а из кольца A. Поскольку в этом случае коэффициенты могут быть необратимы, все полученные выше результаты об отсутствии делителей нуля и обратимых элементах в $k[x]$ и $k[[x]]$ над произвольным кольцом A перестают быть верными, и свойства колец $A[x]$ и $A[[t]]$ во многом зависят от соответствующих свойств кольца A.

Задача 2.9. Опишите обратимые элементы в кольце $\mathbb{Z}[x]$.

Задача 2.10. Докажите, что ряд обратим в кольце $A[[t]]$ тогда и только тогда, когда его свободный член обратим в кольце A.

1.8. Многие переменные. Кольцо многочленов от многих переменных $A[x_1, \ldots, x_n]$ определяется по индукции:

$$A[x_1, \ldots, x_n] \overset{\text{def}}{=} B[x_n], \quad \text{где } B = A[x_1, \ldots, x_{n-1}].$$

При вычислениях в таком кольце следует иметь в виду все оговорки из предыдущего пункта. Легко видеть, что это индуктивное определение равносильно явному, согласно которому кольцо $A[x_1, \ldots, x_n]$ есть множество формальных сумм вида:

$$F(x) = a_0 + \sum_{\nu_1,\ldots,\nu_n \in \mathbb{N}} a_{\nu_1\ldots\nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n},$$

в которых лишь конечное число коэффициентов отлично от нуля.

Аналогично определяются кольца $A[[t_1, \dots, t_n]]$.

1.9. Кольца функций. Пусть X — произвольное множество, а A — любое кольцо. Множество всех функций на X со значениями в A обозначается[3] A^X и наделяется структурой кольца при помощи операций *поточечного сложения* и *поточечного умножения* значений функций: если $f: x \mapsto f(x)$ и $g: x \mapsto g(x)$ — две функции, то

$$f + g: x \mapsto f(x) + g(x) \qquad f \cdot g: x \mapsto f(x)g(x).$$

Нулем и единицей в A^X будут функции $0(x) \equiv 0$ и $1(x) \equiv 1$.

Если $Y \subset X$ — любое подмножество, то ему соответствует *индикаторная фунркция*:

$$I_Y(x) \stackrel{\text{def}}{=} \begin{cases} 1, \text{ если } x \in Y \\ 0, \text{ если } x \notin Y \end{cases}$$

Если $Y \neq \emptyset$, то $I_Y(x) \neq 0(x)$. Если $Y_1 \cap Y_2 = \emptyset$, то $I_{Y_1} \cdot I_{Y_2} = 0(x)$. Поэтому в A^X много делителей нуля. Обратимыми, очевидно, будут те и только те функции, значения которых во всех точках X являются обратимыми элементами в A.

В анализе часто рассматриваются различные подкольца в A^X, например: непрерывных, гладких, интегрируемых и т.п. функций.

1.10. Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$. По определению, элементом этого кольца является *подмножество в $\mathbb{Z}$, состояшее из всех чисел, имеющих один и тот же остаток от деления на n*. Такое подмножество называется *классом вычетов по модулю n*. Множество всех классов вычетов обозначается $\mathbb{Z}/n\mathbb{Z}$ и состоит из n элементов (ибо всего имеется n различных остатков от деления на n: $0, 1, 2, \dots, (n-1)$). Класс вычетов, в котором лежит целое число $a \in \mathbb{Z}$, мы будем обозначать $[a]_n$ или просто $[a]$, когда понятно, что за n имеется в виду. Принадлежность двух чисел a и b одному классу обозначается записью:

$$a \equiv b \pmod{n}.$$

В этом случае говорят, что *a сравнимо с b по модулю n*. Сами записи такого вида называют *сравнениями*. Они во многом аналогичны равенствам. А именно, они *рефлексивны* (т. е. $a \equiv a$, *симметричны* (т. е. $a \equiv b$ тогда и только тогда, когда $b \equiv a$) и *транзитивны* (т. е. если $a \equiv b$ и $b \equiv c$, то $a \equiv c$).

Задача 2.11. Докажите, что обе части сравнения можно умножить на одно и то же число или сложить с одним и тем же числом, а так же вычесть из обеих частей одно и то же число.

Предупреждение. Сокращать обе части сравнения на одно и то же число часто бывает нельзя, например: $3 \cdot 6 \equiv 3 \pmod{15}$, но $6 \not\equiv 1 \pmod{15}$.

[3] Обозначение связано с тем, что на m-элементном множестве M имеется ровно k^m различных функций со значениями в k-элементном множестве K (это — мудрёная перефразировка известной комбинаторной задачи о числе автомобильных номеров)

1.10.1. Сложение и умножение классов вычетов индуцируется сложением и умножением в кольце $\mathbb{Z}$:

$$[a]+[b] \overset{\text{def}}{=} [a+b] \qquad\qquad [a]\cdot[b] \overset{\text{def}}{=} [ab].$$

Это типичный пример *некорректного описания.* Действительно, вычеты — *подмножества* в $\mathbb{Z}$, и мы должны определить для двух таких подмножеств $[a]$ и $[b]$ новое подмножество, которое будет их суммой (или произведением). Написанная формула означает, что для этого мы *выбираем в* $[a]$ *конкретного представителя*, а именно, число a, и в $[b]$ — конкретного представителя, число b, и объявляем суммой $[a]+[b]$ класс, в котором лежит число $a+b$. A priori могло бы так случиться, что взяв других представителей $a_1 \in [a]$ и $b_1 \in [b]$ (при этом $[a_1]=[a]$ и $[b_1]=[b]$!), мы получим *другой* класс $[a_1+b_1] \neq [a+b]$. Тогда такое "определение" в действительности ничего бы не определило! К счастью, в нашем случае корректность можно *доказать*.

1.10.2. Предложение. (Проверка корректности.) *Классы* $[a+b]$ *и* $[ab]$ *не зависят от выбора представителей* a *в классе* $[a]$ *и* b *в классе* $[b]$.

Доказательство. Пусть $a_1 \in [a]$, $b_1 \in [b]$. Это значит, что $a_1 = a+kn$, $b_1 = b+mn$, где $m,k\in\mathbb{Z}$. Но тогда:

$$\begin{aligned} a_1+b_1 &= a+b+(k+m)n \\ a_1b_1 &= ab+(bk+am+kmn)n. \end{aligned}$$

Поэтому, $a_1+b_1 \equiv a+b \pmod n$ и $a_1b_1 \equiv ab \pmod n$.

Задача 2.12. Докажите, что $\mathbb{Z}/n\mathbb{Z}$ — коммутативное кольцо (проверьте выполнение аксиом).

В кольцах $\mathbb{Z}/n\mathbb{Z}$ можно увидеть весь спектр явлений, перечисленных в начале лекции. Так классы $[2]_{10}$ и $[5]_{10}$ в кольце $\mathbb{Z}/10\mathbb{Z}$ имеют нулевое произведение, хотя каждый из них сам нулю не равен. Класс $[3]_{27}\in\mathbb{Z}/27\mathbb{Z}$ нильпотентен: $[3]_{27}^3=[3^3]_{27}=[0]_{27}$, а класс $[4]_{27}\in\mathbb{Z}/27\mathbb{Z}$ — обратим: $[4]_{27}\cdot[7]_{27}=[28]_{27}=[1]_{27}$.

Задача 2.13. Составьте таблицы сложения и умножения в $\mathbb{Z}/n\mathbb{Z}$ для $n = 3$, 4, 5, 6, 7, 8. Найдите в этих кольцах все обратимые элементы, все делители нуля и все нильпотенты. Какие из колец являются полями?

§2. Факторизация

2.1. Разбиения и факторы Переход от кольца $\mathbb{Z}$ к кольцу $\mathbb{Z}/n\mathbb{Z}$ является примером важной общематематической конструкции — *факторизации* или (*склейки*). Состоит она в следующем. Пусть M — произвольное множество. Разбиением M называется представдение M в виде объединения попарно непересекающихся подмножеств, называемых *классами разбиения.*

Задача 2.14. Пусть на множестве M задано *бинарное отношение* (т. е. некоторые пары элементов объявлены "соотносящимися", или более научно, выделено подмножество в $M\times M$). Поместим в один класс все элементы, находящиеся в заданном отношении друг с другом. Докажите, что при этом тогда и только тогда получится разбиение множества M на непересекающиеся классы, когда рассматриваемое отношение *рефлексивно*, *симметрично* и *транзитивно* (такие бинарные отношения называются *отношениями эквивалентности*.

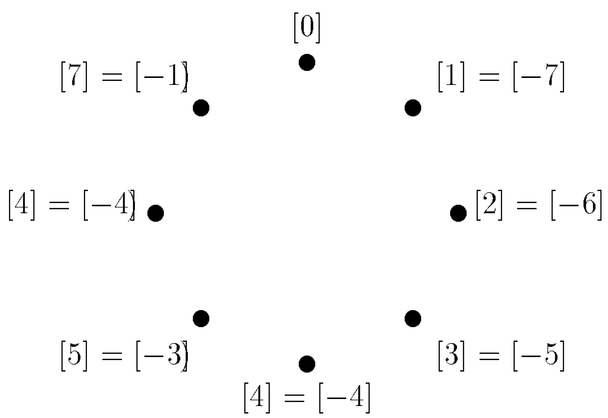


Рис. 1. Циферблат $\mathbb{Z}/8\mathbb{Z}$

Фактор-множеством данного множества M по данному разбиению называется новое множество $\bar{M}$, элементами которого являются классы рассматриваемого разбиения. Иными словами, $\bar{M}$ получается из M склеиванием всех элементов, лежащих в одном классе, в одну точку. Например, относя к одному классу все вещественные числа, отличающиеся друг от друга на целое кратное 2π, мы получим разбиение множества $\mathbb{R}$, фактор по которому геометрически изображается единичной окружностью. Переход от $\mathbb{Z}$ к $\mathbb{Z}/n\mathbb{Z}$ также удобно представлять себе аналогичной геометрической картиной и изображать элементы $\mathbb{Z}/n\mathbb{Z}$ в виде "циферблата", — это бывает полезно при вычислениях (см. рис.рис.1 для n=8).

2.2. Спуск кольцевой структуры на фактор. Если множество $M = A$ — кольцо, то фактор-множество $\bar{A}$ по какому-либо разбиению можно пытаться наделить структурой кольца, *индуцированной с* A, то есть как и выше положить

$$[a] + [b] \stackrel{\text{def}}{=} [a+b] \qquad \text{и} \qquad [a][b] \stackrel{\text{def}}{=} [ab]\,,$$

где через $[a]$ обозначается класс разбиения, содержащий элемент a. Эти операции тавтологически удовлетворяют аксиомам кольца (ибо они наследуются из *кольца* A – продумайте это!), если только они *корректно определены*. Выясним, при каких условиях на разбиение это имеет место.

2.2.1. Свойства класса [0]. Заметим прежде всего, что класс $[0]$ с необходимостью будет нулевым элементом в факторе, ибо $[a]+[0] = [a+0] = [a]$ $\forall a \in A$. Поэтому подмножество, составляющее класс $[0]$, далеко не любое: если операции корректны, то $\forall\, a, b \in [0]$ имеем

$$[0] = [0] - [0] = [a] - [b] = [a-b]\,,$$

т. е. $a - b \in [0]$ и класс $[0]$ замкнут относительно вычитания, а стало быть, и относительно перехода к противоположному элементу, а тем самым, и относительно сложения.

Задача 2.15. Докажите, что для подмножества $M \subset A$ условие замкнутости относительно разности равносильно тому, что M замкнуто относительно сложения, имеющегося в A, и для этого сложения на M выполняются все четыре аксиомы сложенеия.

Далее, $\forall\, b \in A$ и $\forall\, a \in [\,0]$ имеем $[0] = [0b] = [0][b] = [a][b] = [ab]$, откуда, $ab \in [0]$. Это означает, что элементы класса $[0]$ не выходят из этого класса при умножении *на любые* элементы кольца (в частности класс $[0]$ сам является замкнутым относительно умножения).

2.3. Определение. *Подмножество кольца называется* подкольцом*, если оно замкнуто относительно сложения и умножения, и удовлетворяет относительно этих операций всем аксиомам кольца.*

2.4. Определение. *Подкольцо $\mathfrak{I} \subset A$ называется* идеалом*, если оно выдерживает умножение на произвольные (не обязательно ему принадлежащие) элементы объемлющего кольца: $\forall\, a \in A$ и $\forall\, x \in \mathfrak{I}$ всегда $ax \in \mathfrak{I}$.*

Итак, Для того, чтобы операции на факторе были корректны, необходимо, чтобы класс $[0]$ был идеалом в A.

2.4.1. Свойства остальных классов. Если операции над классами корректны, то вычисление $[a] - [a] = [a - a] = [0]$ может быть проделано при помощи любого другого представителя $\tilde{a} \in [a]$, что даёт

$$[[0] = [\tilde{a}] - [a] = [\tilde{a}] - [a] = [\tilde{a} - a] \ ,$$

т. е. $\forall\, \tilde{a} \in [a]$ выполнено условие $\tilde{a} - a \in [0]$. Верно и обратное: если $\tilde{a} - a \in [0]$, то

$$[a] = [a] + [0] = [a] + [\tilde{a} - a] = [a + \tilde{a} - a] = [\tilde{a}] \ ,$$

т. е. $\tilde{a} \in [a]$.

Таким образом, каждый класс $[a]$ состоит из тех и только тех элементов $\tilde{a}$, для которых $\tilde{a} - a \in [0]$. Инче говоря, $[a]$ имеет вид $[a] = a + [0]$, т. е. получается “параллельным сдвигом” класса $[0]$ на элемент a. В частности, все классы находятся во взаимно-однозначном соответствии с классом $[0]$, и всё разбиение полностью определяются заданием идеала $[0] \subset A$.

2.5. Факторизация по идеалу. Итог предыдущего анализа можно сформулировать так: для того чтобы индуцированные с A операции на факторе кольца A по некоторому разбиению были корректны, необходимо, чтобы класс $[0]$ был идеалом в A, а все остальные классы $[a]$ имели вид:

$$[a] = a + [0] = \{\tilde{a} \in A \mid \tilde{a} - a \in [0]\} \ .$$

Для данного идеала $\mathfrak{I} \subset A$ два элемента $a, b \in A$, для которых $a - \tilde{a} \in \mathfrak{I}$, называются *сравнимыми по модулю идеала* $\mathfrak{I}$. Объединение всех попарно-сравнимых друг с другом элементов кольца назывется *классом вычетов по модулю идеала.*

2.5.1. Предложение. *Фактор-множество $\bar{A}$ кольца A тогда и только тогда является кольцом относительно операций, индуцированных с A, когда A является множеством классов вычетов по модулю некоторого идеала $\mathfrak{I} \subset A$.*

Название и обозначение. При выполнении условий теоремы фактор обозначается через $A/\mathfrak{I}$ и называется *фактором кольца A по идеалу* $\mathfrak{I}$.

Доказательство. С учётом вышесказанного, нам остается только проверить корректность операций на множестве классов вычетов по модулю идеала. Пусть $[a] = [\tilde{a}]$ и $[b] = [\tilde{b}]$, то есть $\tilde{a} = a + r$, $\tilde{b} = b + s$, где $s, r \in \mathfrak{I}$. Тогда

$$a + b = (\tilde{a} + \tilde{b}) + (r + s) \quad \text{и} \quad (r + s) \in \mathfrak{I},$$

$$ab = \tilde{a}\tilde{b} + (rb + sa + rs) \quad \text{и} \quad (rb + sa + sr) \in \mathfrak{I}.$$

Теорема доказана.

§3. Примеры идеалов

3.1. Тривиальные идеалы. Идеалы $\{0\}$ и A, имеющиеся в любом кольце, называются *тривиальными*. При этом $A/\{0\} = A$ и $A/A = \{0\}$.

Задача 2.16. Докажите, что для того чтобы идеал совпадал со всем кольцом необходимо и достаточно, чтобы он содержал какой-нибудь обратимый элемент кольца.

Задача 2.17. Докажите, что кольцо тогда и только тогда является полем, когда в нем нет нетривиальных идеалов.

3.2. Нильрадикал. *Нильрадикалом* кольца A называется множество всех нильпотентных элементов кольца A в объединении с нулем:

$$\mathfrak{n} = \{a \in A \mid a^n = 0 \ \text{ для некоторого } n \in \mathbb{N}\}.$$

Нильрадикал является идеалом в A. Действительно, если $a^n = 0$, то $\forall b \in A$ $(ab)^n = a^n b^n = 0$ и $\forall b\colon b^m = 0$ из формулы бинома заключаем, что $(a-b)^{n+m-1} = 0$.

3.3. Главные идеалы. *Главным идеалом, порожденным* $d \in A$ называется множество всех элементов кольца, кратных d: $\{ad \mid a \in A\}$ (проверьте, что это действительно идеал). Он обозначается символом (d) или dA. Фактор-кольцо $A/(a)$ называется *кольцом вычетов по модулю* a. В частности, $\mathbb{Z}/n\mathbb{Z}$ есть $\mathbb{Z}/(n)$, где $(n) \subset \mathbb{Z}$ — главный идеал, порожденный n. Тривиальные идеалы также главные: $\{0\} = (0)$, $\quad A = (1)$. Кольцо, в котором все идеалы исчерпываются главными, называется *кольцом главных идеалов.*

Следующий факт является важнейшим в арифметике целых чисел:

3.4. Теорема. *$\mathbb{Z}$ является кольцом главных идеалов.*

Доказательство. Пусть $\mathfrak{I} \subset \mathbb{Z}$ — нетривиальный идеал. Тогда он содержит какие-либо *натуральные* числа. Пусть d — наименьшее натуральное число в $\mathfrak{I}$. Я утверждаю, что $\mathfrak{I} = (d)$.

Действительно, $(d) \subset \mathfrak{I}$, ибо $d \in \mathfrak{I} \Rightarrow kd \in \mathfrak{I} \ \ \forall k \in \mathbb{Z}$.

Докажем противоположное включение. Пусть $a \in \mathfrak{I}$ — любое. Деля a на d с остатком, мы можем представить a в виде $a = kd + r$, где $0 \le r \le d-1$ — остаток, а $k \in \mathbb{Z}$. Так как $r = a - kd$ и $a, d \in \mathfrak{I}$, то $r \in \mathfrak{I}$. Следовательно, $r = 0$, ибо d вбыиралось наименьшим натуральнм числом в $\mathfrak{I}$. Значит, $a = kd \in (d)$ и $\mathfrak{I} \subset (d)$.

Теорема доказана.

3.5. Конечно-порождённые идеалы. Пусть A — кольцо. Для любого набора элементов $\{a_1, a_2, \dots, a_n\}$ обозначим через $(a_1, a_2, \dots, a_n)$ или $a_1A + a_2A + \dots + a_nA$ множество всех элементов в A, представимых в виде

$$a = a_1x_1 + a_2x_2 + \cdots a_nx_n \qquad \text{с} \quad x_1, \dots, x_n \in A.$$

Оно является идеалом в A, и называется *идеалом, порожденным* $(a_1, a_2, \dots, a_n)$. Сами элементы a_i в этом случае называются *образующими* идеала.

Задача 2.18. Докажите, что идеал (x, y), порожденный x и y в кольце $k[x, y]$ многочленов от двух переменных, не является главным.

3.6. НОД и взаимная простота в кольце $\mathbb{Z}$. Пусть $m_1, \ldots, m_k \in \mathbb{Z}$ — какие-то целые числа. Идеал $(m_1, m_2, \ldots, m_k) \subset \mathbb{Z}$ состоит из всех целых чисел m, представимых в виде $m = m_1x_1 + \cdots + m_kx_k$ с целыми $x_1, \ldots, x_k$ (геометрически — это множество всех векторов числовой прямой, которые можно отложить, имея k векторов $m_1, \cdots, m_k$). По теореме Теор.3.4 он является главным, т. е. $(m_1, m_2, \ldots, m_k) = (d)$ для некоторого $d \in \mathbb{N}$. Число d представимо в виде

$$d = m_1x_1 + \cdots + m_kx_k,$$

делит каждое из чисел m_ν и делится на любое другое число D, являющееся общим делителем для всех m_ν. Таким образом, $d = \text{НОД}(m_1, m_2, \ldots, m_k)$ — *наибольший общий делитель*. Замечу, что по школьному определению НОД есть наибольшее натуральное число, делящее каждое из m_ν, и a priori неясно, что оно должно делиться нацело на любой другой делитель и представляться в виде $m_1x_1 + \cdots + m_kx_k$.

Числа $m_1, \ldots, m_k$ называются *взаимно простыми в совокупности*, если

$$\text{НОД}(m_1, m_2, \ldots, m_k) = 1,$$

и *попарно взаимно простыми*, если

$$\text{НОД}(m_i, m_j) = 1 \ \forall i \neq j.$$

Совокупная взаимная простота равносильна (по предыдущему) возможности представить единицу в виде $1 = m_1x_1 + \cdots + m_kx_k$ с целыми x_ν. В частности, два числа a и b взаимно просты тогда и только тогда, когда существуют целые x и y такие, что $ax + by = 1$.

3.6.1. Предложение.

а) *Если a делит bc $(a, b, c \in \mathbb{Z})$ и a и b взаимно просты, то a делит c.*

б) *Если a и b взаимно просты и делят c, то их произведение ab также делит c.*

Доказательство. Умножая на c равенство $ax+by = 1$, получаем $c = acx+bcy$. Правая часть этого равенства делится на a при bc делящемся на a, и делится на ab при c делящемся и на a и на b (т. е. при $c = ar = bs$).

3.6.2. Предложение. *$\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда является полем, когда p — простое число.*

Доказательство. Если $n = n_1n_2 \in \mathbb{N}$ — не простое (т. е. $n_1 \neq n$ и $n_2 \neq n$), то в $\mathbb{Z}/n\mathbb{Z}$ имеем $[n_1][n_2] = [n] = [0]$, т. е. $[n_1]$ и $[n_2]$ — делители нуля, что невозможно в поле.

Наоборот, если $n = p \in \mathbb{N}$ — простое, то $\forall [m] \neq [0]$ число m будет взаимно просто с p, а стало быть $mx + py = 1$ для некоторых целых x и y. Но тогда $[m][x] = [mx] = [1 - py] = [1]$ и $[m]$ обратим. Предложение доказано.

3.7. Простые и максимальные идеалы. Для того, чтобы в случае произвольного кольца A уметь выяснять, является ли фактор $A/\mathfrak{p}$ по данному идеалу $\mathfrak{p}$ полем, можно попытаться сформулировать условие “p — простое число” в терминах свойств идеала (p). Поскольку число p просто тогда и только тогда, когда оно взаимно просто с любым числом не лежащем в (p), идею для нужной нам переформулировки можно взять из Пр.3.6.1.

А именно, идеал $\mathfrak{p} \in A$ в произвольном коммутативном кольце A называется *простым*, если $\forall a, b \in A$ из $ab \in \mathfrak{p}$ и $a \notin \mathfrak{p}$ следует, что $b \in \mathfrak{p}$.

Задача 2.19. Докажите, что $(p) \subset \mathbb{Z}$ прост тогда и только тогда, когда p — простое число.

3.7.1. Предложение. *Фактор кольцо $A/\mathfrak{p}$ тогда и только тогда является целостным, когда $\mathfrak{p}$ — простой идеал.*

Доказательство. Отсутствие делителей нуля в $A/\mathfrak{p}$ равносильно тому, что $\forall a, b \in A$ равенство $[a][b] = [ab] = [0] = \mathfrak{p}$ при условии $[a] \neq [0]$ влечет за собой $[b] = [0] = \mathfrak{p}$. Но это и означает, что из $ab \in \mathfrak{p}$ и $a \notin \mathfrak{p}$ следует $b \in \mathfrak{p}$. Предложение доказано.

Однако, не всякое целостное кольцо — поле, и в частности, фактор по простому идеалу может и не быть полем.

Задача 2.20. Проверьте, что главный идеал $(x^2 - y) \subset \mathbb{C}[x, y]$ прост, и найдите в факторе по нему необратимые элементы.

Идеал $\mathfrak{m}$ называется *максимальным*, если он не содержится ни в каком другом нетривиальном идеале. Это условие равносильно тому, что в факторе $A/\mathfrak{m}$ нетривиальных идеалов нет вообще. Действительно, если $\mathfrak{I} \subset A/\mathfrak{m}$ — такой нетривиальный идеал, то подмножество $\tilde{\mathfrak{I}} = \{a \in A \mid [a]_{\mathfrak{m}} \in \mathfrak{I}\} \subset A$ составит нетривиальный идеал в A, строго содержащий $\mathfrak{m}$.

Задача 2.21. Проверьте последнее утверждение.

Задача 2.22. Докажите, что всякий максимальный идеал прост.

Задача 2.23. Докажите, что $A/\mathfrak{m}$ — поле тогда и только тогда, когда $\mathfrak{m}$ — максимальный идеал.

§4. Примеры гомоморфизмов

Гомоморфизм колец $f: A \longrightarrow B$ определяется дословно также, как и гомоморфизм полей: это такое отображение, при котором $\forall a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$f(a_1 + a_2) = f(a_1) + f(a_2)$$

$$f(a_1 a_2) = f(a_1) f(a_2)$$

Задача 2.24. Докажите, что если $f: A \longrightarrow B$ — гомоморфизм, то $f(0) = 0$ и $f(-a) = -f(a)$.

Рассмотрим несколько примеров.

4.1. Гомоморфизм обратного образа, Большая часть гомоморфизмов между кольцами, встречающимися в анализе, геометрии и топологии, строится по следующей схеме. Пусть X и Y — два множества, A — кольцо, и A^X, A^Y — кольца функций на X и Y со значениями в A. Тогда для любого отображения множеств

$$\varphi: X \longrightarrow Y$$

возникает гомоморфизм колец

$$\varphi^*: A^Y \longrightarrow A^X$$

называемый *гомоморфизмом обратного образа* или *поднятия* (обратите внимание, что он действует в направлении, противоположном φ).

По определению, для каждой функции F на Y функцмя $\varphi^*(F)$ на X действует на элементы $x \in X$ по правилу: $\varphi^*(F)(x) = F\big(\varphi(x)\big)$, т. е. является композицией исходной функции F и отображения φ.

Задача 2.25. Убедитесь, что φ^* действительно гомоморфизм.

Оказывается, что алгебраические свойства гомоморфизма φ^* на *структурное подкольцо* в A^Y (в ТФКП таковым служит кольцо голоморфных функций, в дифференциальной геометрии и топологии — кольцо гладких или непрерывных функций, в алгебраической геометрии — кольцо полиномиальных функций) очень хорошо отражают геометрические свойства как самого отображения φб так и пространств X и Y.

4.2. Гомоморфизмы вычисления. Рассмотрим предыдущую конструкцию в случае, когда $X = \{p\}$ состоит из одной точки и $\varphi: \{p\} \hookrightarrow Y$ отождествляет эту точку с некоторой точкой $y \in Y$. Здесь $A^X = A$ и гомоморфизм поднятия будет действовать из A^Y в A, сопоставляя функции $F \in A^Y$ её значение $F(y)$ в точке y. В такой ситуации он называется *гомоморфизмом вычисления значения* функций на Y в точке $y \in Y$ и обозначается

$$\mathrm{ev}_y: A^Y \longrightarrow A.$$

Другие гомоморфизмы вычисления встречаются в анализе. Например, для некоторых формальных рядов из $\mathbb{C}[[t]]$ (называемых *сходящимися*) можно определить их значение в точке $z \in \mathbb{C}$. Эта конструкция не алгебраическая, ибо результат подстановки числа в формальный ряд определяется не как результат конечного числа алгебраических действий, а при помощи перехода к пределу. В этом случае свойство ev_y быть гомоморфизмом перестаёт быть тривиальным и превращается в содержательную теорему из анализа. Алгебраическое значение этой теоремы состоит в том, что все формальные тождества между рядами в кольце $\mathbb{C}[[t]]$ при применении к сходящимся рядам влекут за собой соответствующие тождества между числами в $\mathbb{C}$ или между функциями в $\mathbb{C}^{\mathbb{C}}$.

4.3. Гомоморфизм факторизации. Отображение $\pi_n: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, при котором $m \mapsto [m]_n$ является (по определению операций в $\mathbb{Z}/n\mathbb{Z}$) гомоморфизмом. Он называется *редукцией по модулю n*. Этот гомоморфизм *сюрьективен*, т. е. у любого $x \in \mathbb{Z}/n\mathbb{Z}$ имеется прообраз[4].

Аналогично, для любого идеала $\mathfrak{J}$ в произвольном кольце A имеется эпиморфизм $\pi_{\mathfrak{J}}$: $A \longrightarrow A/\mathfrak{J}$ редукции по модулю этого идеала.

4.4. Простое подполе и характеристика. Пусть k — любое поле, $1 \in k$ — единица в этом поле. Определим отображение $f: \mathbb{Z} \longrightarrow k$, полагая:

$$f(0) \;=\; 0$$

[4]Сюрьективные гомоморфизмы называют также *эпиморфизмами*.

$$\begin{aligned} f(n) &= \underbrace{1+1+\cdots+1}_{n} \\ f(-n) &= \underbrace{-1-1-\cdots-1}_{n}, \end{aligned}$$

где n — любое натуралюное число. Очевидно, что f — это гомоморфизм кольца $\mathbb{Z}$ в поле k.

Если f является вложением, говорят, что поле k имееит *характеристику нуль*, и пишут: $\mathrm{char}(k) = 0$. В этом случае f однозначно продолжается по формуле $f(m/n) = f(m)/f(n)$ до вложения полей $\mathbb{Q} \longrightarrow k$, так что k содержит канонически определенное подполе, изоморфное $\mathbb{Q}$.

Если f не является вложением, скажем $f(m) = f(s)$ для некоторых $m, s \in \mathbb{Z}$, и, скажем, $m > s$, то $f(m-s) = f(m) - f(s) = 0$. Значит, имеется натуральное n, такое что

$$f(n) = \underbrace{1+1+\cdots+1}_{n} = 0.$$

Наименьшее такое n называется *характеристикой* поля k и обозначается $\mathrm{char}(k)$. При этом говорят, что поле *имеет положительную характеристику* (в отличие от случая нулевой характеристики).

Задача 2.26. Убедитесь, что $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$ (где $p \in \mathbb{N}$ — простое).

Ясно, что и в общем случае $\mathrm{char}(k)$ — простое число. Действительно, если $\mathrm{char}(k) = n = sr$, где $s < n$ и $r < n$ (так что $f(s)$ и $f(r)$ ненулевые в k), то

$$0 = \underbrace{1+1+\cdots+1}_{n} = \underbrace{(1+1+\cdots+1)}_{r}\underbrace{(1+1+\cdots+1)}_{s} = f(r)f(s),$$

что невозможно, ибо в поле нет делителей нуля.

При $\mathrm{char}(k) = p > 0$ *образ* гомоморфизма f (т. е. $f(\mathbb{Z}) \subset k$) составляет подполе в k, изоморфное полю $\mathbb{Z}/p\mathbb{Z}$. Действительно, этот образ будет подкольцом в k, которое можно рассматривать как фактор кольца $\mathbb{Z}$ по разбиению, объединяющему в один класс все числа, имеющие одинаковый образ в k. Но мы видели, что такое кольцо должно быть фактором $\mathbb{Z}$ по идеалу, состоящему из всех чисел n, для которых $f(n) = 0$. Наименьшее такое число —p, и значит идеал этот совпадает с (p), а $f(\mathbb{Z})$ есть $\mathbb{Z}/p\mathbb{Z}$.

Итак, в любом поле k можно *канонически* выделить наименьшее подполе, содержащее 0 и 1. Это подполе называется *простым подполем*. Оно изоморфно $\mathbb{Q}$ при $\mathrm{char}(k) = 0$ и изоморфно $\mathbb{Z}/p\mathbb{Z}$ при $\mathrm{char}(k) = p > 0$. Смысл эпитета "канонически" призвана прояснить следующая

Задача 2.27. Докажите, что все элементы простого подполя остаются на месте при любом ненулевом гомоморфизме из k в k.

4.5. Гомоморфизм Фробениуса. Если $\mathrm{char}(k) = p$, то отображение $F\colon x \mapsto x^p$ является *гомоморфизмом* из поля k в себя (он называется *гомоморфизмом Фробениуса*).

Действительно, $(xy)^p = x^p y^p$. Раскрывая скобки в $(x+y)^p$ по обычным правилам, мы получим сумму, состоящую из слагаемых вида $x^k y^{p-k}$. Как объяснялось на стр.14, всего членов, равных фиксированному $x^\nu y^{p-\nu}$, будет $\binom{p}{\nu}$, т. е. коэффициент при $x^\nu y^{p-\nu}$ будет равен

$$\underbrace{1+1+\cdots+1}_{\binom{p}{\nu}} = f\left(\frac{p!}{\nu!(p-\nu)!}\right)$$

(где f — гомоморфизм из предыдущего пункта). Но $\frac{p!}{\nu!(p-\nu)!} = 1$ при $\nu = 0$ и $\nu = p$, а во всех остальных случаях делится на p, ибо числитель дроби делится на p, а знаменатель взаимно прост с p при простом p. Поэтому все слагаемые в разложении $(x+y)^p$, кроме x^p и y^p сократятся, и $(x+y)^p = x^p + y^p$.

4.5.1. Предложение. (Малая теорема Ферма.) *Если p — простое число, то $\forall a \in \mathbb{Z}$ выполнено сравнение $a^p \equiv a \pmod p$. Если же a не делится на p, то $a^{p-1} \equiv 1 \pmod p$.*

Доказательство. Гомоморфизм Фробениуса тождественно действует на $\mathbb{Z}/p\mathbb{Z}$ (оно есть простое подполе самого себя), и значит, $[a^p] = [a]^p = [a]\ \forall a \in \mathbb{Z}$, то есть $a \equiv a \pmod p$.

Если же a не делится на p, то $[a]$ обратим в $\mathbb{Z}/p\mathbb{Z}$, и умножая на $[a]^{-1}$ равенство $[a^p] = [a]$, получим $[a^{p-1}] = [1]$, т. е. $a^{p-1} \equiv 1 \pmod p$.

4.6. Строение гомоморфизмов. Предыдущие примеры показывают, что гомоморфизмы колец (в отличие от гомоморфизмов полей) могут не быть вложениями. Тем не менее, их строение может быть детально описано.

4.7. Определение. *Пусть $f\colon A \longrightarrow B$ — гомоморфизм колец. Подмножество*

$$\ker(f) = \{a \in A \mid f(a) = 0\} \subset A$$

называется ядром гомоморфизма f, а подмножество

$$\operatorname{im}(f) = \{b \in B \mid \exists a \in A\colon f(a) = b\} \subset B$$

называется образом гомоморфизма f.

4.7.1. Предложение. *Образ гомоморфизма $f\colon A \longrightarrow B$ является подкольцом в B, а ядро — идеалом в A. При этом существует канонический изоморфизм*

$$\tilde{f}\colon\ A/\ker(f) \xrightarrow{\sim} \operatorname{im}(f),$$

при котором классу $[a]$ по модулю $\ker(f)$ соответствует $f(a) \in \operatorname{im}(f)$.

Доказательство. Если $a, \tilde{a} \in \ker(f)$, то $f(a-\tilde{a}) = f(a) - f(\tilde{a}) = 0 - 0 = 0$, так что $a - \tilde{a} \in \ker(f)$. Аналогично, если $a \in ker(F)$, и $b \in A$ — любой, то $f(ab) = f(a)f(b) = 0 \cdot f(b) = 0$, так что $ab \in \ker(f)$. Следовательно, $\ker(f)$ — идеал.

Пусть $\tilde{A} = A/\ker(f)$ — соответствующий фактор. Отображение $\tilde{f}\colon [a] \mapsto f(a)$ действует из $\tilde{A}$ в $\operatorname{im}(f)$. Оно определено корректно, поскольку $\forall \tilde{a} : [\tilde{a}] = [a]$ имеем $\tilde{a} = a + r$ (где $r \in ker(f)$), и $f(\tilde{a}) = f(a) + f(r) = f(a)$. Это отображение является гомоморфизмом (ибо f — гомоморфизм) и взаимно-однозначно, поскольку у каждого $b = f(a) \in \operatorname{im}(f)$ есть прообраз $[a] \in \tilde{A}$, причем ровно один, т.к. $b = f(a) = f(\tilde{a})$ означает, что $f(a-\tilde{a}) = f(a) - f(\tilde{a}) = 0$, откуда $a - \tilde{a} \in \ker(f)$ и $[a] = [\tilde{a}]$.

Таким образом, $\tilde{f}$ и в самом деле отождествляет $\tilde{A}$ с $\mathrm{im}(f)$ с сохранением операций, в частности, $\mathrm{im}(f)$ — подкольцо в B.

□

4.7.2. Следствие. *Произвольный гомоморфизм $f\colon A \longrightarrow B$ может быть разложен в композицию эпиморфизма редукции A по модулю идеала $\ker(f)$, изоморфизма*

$$\tilde{f}\colon A/ker(f) \xrightarrow{\sim} \mathrm{im}(f)$$

и вложения подкольца $\mathrm{im}(f)$ в B.

□

Схематически это изображается *коммутативной диаграммой*:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_{\ker(f)}"'] & B \\ A/\ker(f) \arrow[r, "\tilde{f}"] & \mathrm{im}(f) \arrow[u] \end{tikzcd}$$

Эпитет "коммутативный" означает, что результат переноса любого элемента $a \in A$ в B по стрелкам не зависит от выбора пути (в данном случае таких путей 2).

4.8. Прямые суммы колец. В заключение лекции приведем еще одну часто встречающуюся конструкцию с кольцами. Пусть A_1, A_2, ..., A_n — n колец.

4.9. Определение. *Прямой суммой*

$$\bigoplus_{\nu=1}^{n} A_\nu = A_1 \oplus A_2 \oplus \cdots \oplus A_n$$

называется кольцо, элементами которого служат наборы:

$$a = (a_1, a_2, \ldots, a_n), \qquad \text{где } a_\nu \in A_\nu,$$

а операции определяются покомпонентно: если $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n)$, то

$$a + b = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

$$ab = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

Нулем относительно этих операций будет набор $(0, 0, \ldots, 0)$, а единицей — набор $(1, 1, \ldots, 1)$.

Задача 2.28. Докажите, что $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ — кольцо (проверьте аксиомы).

Прямая сумма по своим свойствам дальше отстоит от поля, чем слагаемые. Например, в ней всегда есть делители нуля: $(0,1)(1,0) = (0,0)$. В частности, прямая сумма полей есть кольцо, но не поле.

Задача 2.29. Убедитесь, что в кольце

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

всего имеется ровно $n_1 n_2 \cdots n_k$ элементов.

В качестве примера, иллюстрирующего все конструкции этой лекции, укажем “научное” доказательство одной известной теоремы арифметики. Тем, кто знает ее “элементарное” доказательство, поучительно будет сравнить его с нашим и отметить для себя те алгебраические пружины, которые им движут.

4.9.1. Предложение. (Китайская теорема об остатках.) *Пусть* $(n_1, n_2, \ldots, n_k)$ — *набор попарно взаимно простых чисел. Тогда для любого набора* $(r_1, r_2, \ldots, r_k)$ *остатков от деления на* n_1, n_2, $\ldots$, n_k *соответственно можно подобрать такое целое число* a, *которое довало бы остаток* r_1 *от деления на* n_1, *остаток* r_2 *от деления на* n_2, *и так далее.*

Более того, если $\tilde{a}$ — *другое такое число, то разность* $a - \tilde{a}$ *делится на произведение* $n_1 n_2 \cdots n_k$.

Доказательство. Пусть $N = n_1 n_2 \cdots n_k$. Кольца

$$A = \mathbb{Z}/N\mathbb{Z} \qquad \text{и} \qquad B = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

состоят из одинакового числа элементов. Отображение $f\colon A \longrightarrow B$, переводящее класс $[a]_N$ в набор классов $([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_2})$ корректно определено, т. е. не зависит от выбора представителя $a \in [a]_N$, и является гомоморфизмом.

Его ядро состоит из таких классов $[a]_N$, что a делится на каждое из чисел n_ν. Но так как числа n_ν попарно взаимно просты, то каждое такое a будет делиться и на их произведение N (почему?), а сало быть $[a]_N = [0]_N$ и $\ker(f) = \{0\}$.

Образ $\mathrm{im}(f)$ изоморфен $A/ker(f) = A$. В частности, он состоит из того же количества элементов, что и A, а поэтому совпадает с B.

Итак, f — изоморфизм. Но это в точности и составляет утверждение теоремы.

Лекция 3
Делимость и многочлены

▷Деление в кольце $k[x]$ ▷Евклидовы кольца ▷Ассоциированные, простые и неприводимые элементы кольца ▷НОД и китайская теорема об остатках в кольце главных идеалов ▷Многочлены как функции ▷Корни ▷Производный многочлен ▷Сепарабельность ▷Алгебраические расширения полей ▷Лемма Гаусса и критерий Эйзенштейна ▷Разложение на множители многочленов с целыми коэффициентами ▷Факториальные кольца

§1. Кольца главных идеалов.

Целостное (т. е. без делителей нуля) коммутативное кольцо с единицей, в котором все идеалы являются главными, называется *областью главных идеалов*. С точки зрения делимости все такие кольца устроены подобно кольцу $\mathbb{Z}$, и на них можно распространить все результаты, доказанные про $\mathbb{Z}$ в прошлой лекции. Мы начнём с примеров колец главных идеалов, не совпадающих с $\mathbb{Z}$.

1.1. Деление с остатком в $k[x]$. Я буду считать, что читатель умеет делить многочлены с остатком (например, "уголком"). Точное утверждение, которое в дальнейшем понадобится, можно сформулировать так:

ЗАДАЧА 3.1. Пусть k – произвольное поле. Для любых двух многочленов $f(x), g(x) \in k[x]$ существуют многочлены $q(x) \in k[x]$ (*неполное частное*) и $r(x) \in k[x]$ (*остаток*), такие, что:

$$\begin{aligned} &(1) \quad f(x) = q(x) \cdot g(x) + r(x) \\ &(2) \quad 0 \le \deg r \le \deg(g) - 1\ , \quad \text{(где deg — это степень.)} \end{aligned}$$

Этими условиями $q(x)$ и $r(x)$ определяются по f и g однозначно.

ПОДСКАЗКА: существование обеспечивается процедурой "деления уголком". Единственность доказывается от противного: если $q_1(x)$ и $r_1(x)$ тоже удовлетворяют условиям (1) и (2), то $r_1(x) - r(x) = g(x) \cdot (q_1(x) - q(x))$. Степень левой части $\le \deg(g) - 1$, что возможно лишь при $q_1(x) - q(x) \equiv 0$. Но тогда и $r_1 \equiv r$.

1.1.1. ПРЕДЛОЖЕНИЕ. *$k[x]$ — область главных идеалов.*

Доказательство. Рассуждение дословно повторяет доказательство аналогичной теоремы про кольцо $\mathbb{Z}$. Пусть $\mathfrak{I} \subset k[x]$ — нетривиальный идеал. Выберем в $\mathfrak{I}$ произвольный многочлен $d(x) \neq 0$, степень которого имеет наименьшее возможное значение среди степеней ненулувых многочленов из $\mathfrak{I}$. Тогда $\mathfrak{I} = (d)$.

Действительно, $(d) \subset \mathfrak{I}$ по построению. Чтобы доказать, что $\mathfrak{I} \subset (d)$, поделим произвольный многочлен $f \in \mathfrak{I}$ на d с остатком:

$$f = q \cdot d + r, \quad \text{где} \quad \deg r \leq \deg d - 1.$$

Так как $r = f - q \cdot d \in \mathfrak{I}$, то $r \equiv 0$, ибо d имел наименьшую степень среди ненулевых многочлеов из $\mathfrak{I}$. Поэтому $f = q \cdot d \in (d)$ и $(d) = \mathfrak{I}$.
□

1.2. Евклидовы кольца. В приведённом выше доказательстве, также как и в прошлой лекции, ключевым местом является возможность деления с остатком. Можно аксиоматизировать класс колец, для которых такая возможность имеется.

1.3. Определение. *Целостное коммутативное кольцо A называется евклидовым, если существует функция λ (называемая высотой) из множества ненулевых элементов A в множество целых неотрицательных чисел, обладающая свойством $\lambda(ab) \geq \max(\lambda(a), \lambda(b))$ и такая, что $\forall\, a, b \in A,\ b \neq 0$ найдутся q и r из A такие, что $a = bq + r$ и либо $r = 0$, либо $\lambda(r) < \lambda(b)$.*

Задача 3.2. Докажите, что всякое евклидово кольцо является областью главных идеалов.

1.3.1. Примеры. Кольцо $\mathbb{Z}$ евклидово относительно высоты, равной абсолютной величине целого числа. Кольцо $k[x]$ евклидово с высотой равной степени многочлена.

Кольцо Гауссовых чисел $\mathbb{Z}[i]$ евклидово относительно высоты $\lambda(z) \stackrel{\text{def}}{=} |z|^2$. Действительно, возможность для данных $a, b \in \mathbb{Z}[i]$ подобрать такие $q, r \in \mathbb{Z}[i]$, что $a = bq + r$ и $|r|^2 < |b|^2$, равносильна тому, что в круге радиуса < 1 с центром в комплексной точке $\dfrac{a}{b} \in \mathbb{C}$ найдётся целая точка $q \in \mathbb{Z}[i]$. Но это очевидно.

Задача 3.3. Докажите, что кольцо $\mathbb{Z}[\vartheta]$, где ϑ – комплексный корень уравнения $\vartheta^2 + \vartheta + 1 = 0$, евклидово относительно той же высоты $\lambda(z) = |z|^2$.

Отметим, однако, что существуют кольца главных идеалов, не являющиеся евклидовыми.

1.4. Ассоциированные элементы. Пусть A — произвольное целостное кольцо. Элементы a и b из A называются *ассоциированными*, если порождённые ими главные идеалы совпадают: $(a) = (b)$. Это равносильно тому, что $a = bs$ для некоторого *обратимого* элемента $s \in A$.

Действительно, из равенств $a = bs$ и $b = as^{-1}$ следуют включения $(a) \subset (b)$ и $(b) \subset (a)$, т.е. равенство $(a) = (b)$. Наоборот, если $a \in (b)$, скажем: $a = rb$, и $b \in (a)$, скажем: $b = sa$, то $a = rb = rsa$, откуда $0 = a - rsa = a(1 - rs)$, что в виду целостности A влечёт $rs = 1$, т.е. обратимость r и s.

1.4.1. Пример: приведённые многочлены. Поскольку обратимые элементы в $k[x]$ — это константы и только они, предыдущее рассуждение показывает, что два многочлена f и g порождают один и тот же главный идеал в $k[x]$ тогда и только тогда, когда они пропорциональны, т.е. $f(x) = c \cdot g(x)$, где $c = \text{const}$.

Будем называть многочлен *приведённым*, если его старший коэффициент равен единице. Из предыдущего вытекает, что для каждого идеала $\mathfrak{I} \subset k[x]$, существует и единственен такой приведённый многочлен f, что $(f) = \mathfrak{I}$.

1.5. НОД. Пусть A — кольцо главных идеалов, и $\{a_1, a_2, \dots, a_n\} \subset A$ — произвольный набор элементов. Элемент $d \in A$, порождающий идеал

$$(a_1, a_2, \dots, a_n) = \{\, x_1a_1 + x_2a_2 + \dots + x_na_n \mid x_\nu \in A \text{ – любые} \,\} \subset A\,,$$

называется *наибольшим общим делителем* элементов $a_1, a_2, \dots, a_n$ и обозначается

$$\text{НОД}\,(a_1, a_2, \dots, a_n)\,.$$

Он определяется элементами a_ν однозначно с точностью до умножения на обратимые элементы кольца, по построению, делит каждый из a_ν, представим в виде $d = x_1a_1 + x_2a_2 + \dots + x_na_n$, и тем самым, делится нацело на любой другой общий делитель всех a_ν.

Если $\text{НОД}\,(a_1, a_2, \dots, a_n)$ обратим, то элементы a_ν называются *взаимно-простыми в совокупности* . Это равносильно наличию таких $x_1, x_2, \dots, x_n \in A$, что

$$x_1a_1 + x_2a_2 + \dots + x_na_n = 1$$

1.5.1. Пример: НОД в $k[x]$. В случае $A = k[x]$ (где k – поле) неоднозначность в определении НОД можно устранить, назвав наибольшим общим делителем многочленов $f_1, f_2, \dots, f_n$ *приведенный* многочлен $d(x)$, порождающий идеал $(f_1, f_2, \dots, f_n) \subset k[x]$.

Для практического нахождения $\text{НОД}\,(f, g)$ для пары $f, g \in k[x]$ имеется эффективная ппроцедура, называемая *алгоритмом Евклида*. Она заключается в построении последовательности многочленов $E_0(x)$, $E_1(x)$, $E_2(x)$, ... , определяемых рекуррентно по правилу:

$$\begin{aligned} E_0(x) &= f(x) \quad (\text{мы предполагаем, что } \deg f \geq \deg g) \\ E_1(x) &= g(x) \\ E_k(x) &= \text{остатку от деления } E_{k-1}(x) \text{ на } E_{k-2}(x). \end{aligned}$$

Нетрудно видеть, что степень многочленов E_ν строго убываеет до тех пор, пока очередной $E_{k+1}(x)$ не окажется нулевым, т.е. пока $E_{k-1}(x)$ не разделится на $E_k(x)$ нацело.

Задача 3.4. Докажите, что последний ненулевой многочлен $E_k(x)$ в последовательности $E_\nu(x)$ пропорционален $\text{НОД}\,(f, g)$.

Указание. Воспользуйтесь убывающей индукцией по ν, чтобы проверить, что E_0 и E_1 делятся на последний ненулувой E_k, и соответственно, возрастающей индукцией по ν — для проверки того, что этот последний E_k делится на любой общий делитель E_0 и E_1.

Задача 3.5. Найдите многочлены $g_1(x)$ и $g_2(x)$, для которых $f_1(x)g_1(x) + f_2(x)g_2(x) \equiv 1$, если

$$\begin{aligned} f_1(x) &= x^5 - 8x^4 + 15x^3 - x^2 + 8x - 15 \\ f_2(x) &= 21x^5 + 10x^4 - 41x^3 - 41x^2 - 12x - 1. \end{aligned}$$

Задача 3.6. Распространите алгоритм Евклида на произвольное евклидоао кольцо.

1.6. Китайская теорема об остатках. Для того, чтобы распространить китайскую теорему об остатках на произвольные кольца главных идеалов, нам понадобится

1.6.1. Лемма. *Пусть $q = q_1 q_2$ – произведение двух взаимно простых элементов в кольце главных идеалов A. Тогда правило $a \bmod q \longmapsto (a \bmod q_1, a \bmod q_2)$ устанавливает изоморфизм колец*

$$A/(q) \xrightarrow{\sim} \big(A/(q_1)\big) \oplus \big(A/(q_2)\big)\ .$$

Доказательство. Рассуждение будет почти таким же как в лекции 2. Корректность очевидна. Инъективность вытекает из того, что всякий $a \in A$, делящийся и на q_1 и на q_2, делится и на $q_1 q_2 = q$ (действительно, если $1 = xq_1 + yq_2$ и $a = mq_1 = nq_2$, то $a = (xn + ym)q_1 q_2$). Эпиморфность проверяется непосредственно: пара классов $(a \bmod q_1, b \bmod q_2)$ является образом элемента $c = ayq_2 + bxq_1$, где, как и выше, x и y подбираются из условия $1 = xq_1 + yq_2$.
□

1.6.2. Следствие. (Китайская теорема об остатках.) *Пусть $q = q_1 \cdot q_2 \cdot \dots \cdot q_s$ – разложение на попарно неассоциированные простые множители. Тогда имеется изоморфизм колец:*

$$\frac{A}{(q)} = \frac{A}{(q_1)} \oplus \frac{A}{(q_2)} \oplus \dots \oplus \frac{A}{(q_s)}\ ,$$

заданный правилом $a \bmod q \longmapsto (a \bmod q_1, a \bmod q_2, \dots, a \bmod q_s)$.

Доказательство. Индукция по числу s взаимно-простых сомножителей.

Задача 3.7. Проверьте, что если элемент q_1 взаимно прост с каждым из элементов $q_2, q_3, \dots, q_s$, то он взаимно прост и с их произведением $\tilde q_2 = q_2 \cdot \dots \cdot q_s$.

Пользуясь задачей, сначала применим предыдущую лемму к паре взаимно простых элементов q_1, $\tilde q_2 = q_2 \cdot \dots \cdot q_s$, а эатем применим индуктивное предположение к меньшему набору $q_2, q_3, \dots, q_s$. Получим композицию изоморфизмов

$$\frac{A}{(q)} \xrightarrow{\sim} \frac{A}{(q_1)} \oplus \frac{A}{(\tilde q_2)} \xrightarrow{\sim} \frac{A}{(q_1)} \oplus \frac{A}{(q_2)} \oplus \dots \oplus \frac{A}{(q_s)}\ .$$

□

Задача 3.8. В случае $A = k[x]$ переформулируйте эту теорему в терминах “настоящих” остатков от деления, аналогично тому, как это было сделано в конце прошлой лекции для $A = \mathbb{Z}$.

1.7. Простота и неприводимость. Пусть A — произвольное целостное кольцо. Имеются два подхода к тому, какие элементы в A считать аналогами простых чисел. Они приводят к разным результатам, и потому для соответствующих элементов кольца используются различные названия.

Первый подход опирается на данное в n° 3.7 лекции 2 определение простого идеала. Необратимый элемент $a \in A$ называется *простым*, если идеал $(a) \subset A$ — простой, т. е. если фактор-кольцо $A/(a)$ целостное. Это означает, что из условий $bc \in (a)$ и $b \notin (a)$ следует, что

$c \in (a)$. Иначе говоря, элемент $a \in A$ прост тогда и только тогда, когда произвольное произведение делится на a лишь при условии, что хотя бы один из сомножителей делится на a (ср. с Пр.3.6.1 из лекции 2).

Второй подход состоит в том, чтобы, не мудрствуя лукаво, переписать обычное школьное определение простого числа: необратимый элемент $a \in A$ называется *неприводимым* , если из разложения $a = bc$ следует, что один из сомножителей *обратим*. Например, неприводимые элементы в кольце многочленов — это в точности такие многочлены, которые нельзя разложить в произведение двух многочленов строго меньшей степени. Твакие многочлены называют *неприводимыми многочленами.*

Задача 3.9. Убедитесь, что в кольце $\mathbb{Z}$ оба понятия: простота и неприводимость совпадают и описывают в точности множество простых чисел.

В произвольном целостном кольце *из простоты следует неприводимость*. Действительно, если $a = bc$ и a прост, то либо b, либо c делится на a, скажем: $b = as$. Но тогда $a = asc$, откуда $sc = 1$ и c — обратим (мы воспользовались равенством $a(1 - sc) = 0$ и целостностью A).

Однако, бывают кольца, в которых имеются неприводимые, но не простые элементы, так что простота — это более сильное условие, чем неприводимость.

Задача 3.10. В кольце $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ найдите неприводимый, но не простой элемент.
Подсказка:$(1 + \sqrt{5})(-1 + \sqrt{5}) = 2 \cdot 2$.

1.7.1. Предложение. *Пусть A – область главных идеалов. Фактор-кольцо $A/(a)$ является полем тогда и только тогда, когда a неприводим.*

Доказательство. Проверим, что если a — неприводим, то всякий класс $[b] \neq [0]$ в $A/(a)$ обратим. Это аналогично Пр.3.6.2 из лекции 2: если $[b] \neq [0]$, то b не делится на a, а значит *НОД* (b, a) обратим (ибо все делители a либо обратимы, либо ассоциированы с a), и значит, $xa + yb = 1$ для некоторых $x, y \in A$, что означает, что $[b]$ обратим в $A/(a)$ и $[b]^{-1} = [y]$.
□

1.7.2. Следствие. *В кольце главных идеалов простота и неприводимость равносильны друг другу.*

§2. Многочлены и их корни

В этом параграфе мы применим предыдущие результаты к исследованию алгебраических свойств многочленов.

2.1. Вычисление значения многочлена в точке. Любой многочлен из $k[x]$ определяет функцию на поле k, а также на любом кольце A, содержащем поле k в качестве подкольца. Если $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ и $\lambda \in A$, то

$$f(\lambda) = \mathrm{ev}_\lambda(f) \stackrel{\mathrm{def}}{=} a_0\lambda^n + a_1\lambda^{n-1} + \cdots + a_{n-1}\lambda + a_n \in A$$

(где правая часть уже не формальный символ, но конкретный элемент кольца A) называется *значением многочлена f в точке $\lambda \in A$. Гомоморфизм вычисления*:

$$\mathrm{ev}_\lambda\colon\ k[x] \longrightarrow A$$

индуцирует гомоморфизм

$$\varphi:\ k[x] \longrightarrow A^A:\ f(x) \mapsto f(\lambda)$$

из кольца многочленов в кольцо A-значных функций на A. Вообще говоря, $\ker\varphi \neq 0$, т.е. разные элементы кольца многочленов могут давать одинаковые функции.

Задача 3.11. Найдите два разных многочлена над полем $\mathbb{Z}/p\mathbb{Z}$, задающиее, тем не менее, одинаковые функции на этом поле.

Гомоморфизм вычисления замечательным образом связан с делимостью. А именно, пусть $f(x) \in k[x] \subset A[x]$ —многочлен с коэффициентами из k, который можно также рассматривать и как многочлен из $A[x]$. Мы собираемся вычислять его значение в точке $a \in A$. Для этого заметим, что процедура “деления уголком” на линейный двучлен $x-a$ благополучно работает над любым коммутативным кольцом A, и позволяет представить любой многочлен $f(x) \in A[x]$ в виде

$$f(x) = (x-a)\cdot q(x) + r\ ,$$

где $q(x) \in A[x]$, а $r \in A$ – некоторая константа (называемая *остатком* по аналогии с евклидовым случаем). Вычисляя значения обеих частей в точке a, получаем:

$$f(a) = q(a)\cdot(a-a) + r = r\ .$$

2.1.1. Лемма. *Остаток от деления многочлена $f(x) \in A[x]$ на линейный двучлен $x-a$ в кольце $A[x]$ равен значению многочлена f в точке $a \in A$.*

□

2.2. Корни. Пусть A — произвольное коммутативное кольцо. Элемент $a \in A$ называется *корнем* многочлена $f(x) \in A[x]$, если $f(a) = 0$, т.е. если $f \in \ker(\mathrm{ev}_a)$. Прямо из предыдущего наблюдения мы получаем

2.2.1. Следствие. *Число $a \in A$ тогда и только тогда, является корнем многочлена $f(x) \in A[x]$, когда $f(x)$ делится нацело в кольце $A[x]$ на многочлен $(x-a)$.*

2.2.2. Следствие. *Пусть в кольце A нет делителей нуля. Если многочлен $f \in A[x]$ имеет несколько попарно-разных корней $a_1, a_2, \ldots, a_n \in A$, то он представим в виде $f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)g(x)$, где $g(x) \in A[x]$.*

Доказательство. Индукция по числу корней n. Случай $n = 1$ рассмотрен в предыдущем следствии. Применяя индуктивное предположение к первым $(n-1)$ корням $a_1, a_2, \ldots, a_{n-1}$, имеем

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_{n-1})h(x)\ .$$

с $h(x) \in A[x]$. Подставляя $x = a_n$ получим

$$0 = (a_n-a_1)(a_n-a_2)\cdots(a_n-a_{n-1})h(a_n)\ .,$$

что из-за целостности кольца A возможно лишь при $h(a_n) = 0$, т. е. при $h(x) = (x - a_n)g(x)$ с $g \in A[x]$.

□

2.2.3. Следствие. *Ненулевой многочлен $f \in A[x]$ не может иметь более $\deg f$ корней ни в каком целостном кольце $B \supset A$.*

□

2.2.4. Следствие. *Если многочлены f и g совпадают как функции на некотором целостном кольце, содержащем более, чем $\max(\deg f, \deg g)$ элементов, то $f = g$ и как многочлены (т.е. гомоморфизм $\varphi\colon\ A[x] \longrightarrow A^A$ в этом случае инъективен).*

□

Доказательство. Многочлен $f - g$, обладая слишком большим количеством корней, должен быть нулевым.

□

2.2.5. Следствие. *Пусть k – поле. Если НОД $(f, g) = 1$, то f и g не могут иметь общих корней ни в каком кольце $A \supset k$.*

Доказательство. Если *НОД* $(f, g) = 1$, то $f(x) \cdot v(x) + g(x) \cdot w(x) = 1$ для подходящих $v, w \in k[x]$. Вычисляя обе части в точке $a \in A$, получаем $f(a) \cdot v(a) + g(a) \cdot w(a) = 1$, т.е. $f(a)$ и $g(a)$ не могут быть равны нулю одновременно.

□

Значение этого следствия в том, что равенство *НОД* $(f, g) = 1$ проверяется с помощью алгоритма Евклида вычислениями в поле k, тогда как вывод делается о любом расширении и о корнях, явного выражения для которых не требуется.

2.3. Кратные корни и производный многочлен. Число $a \in A$ называется *r-кратным корнем* многочлена $f \in A[x]$, если $f(x) = (x - a)^r \cdot g(x)$ в $A[x]$ и $g(a) \neq 0$. Корни с $r = 1$ называются *простыми*, а с $r \geq 2$ — *кратными*.

Замечательно, что о наличии кратных корней многочлена $f \in A[x]$ в произвольном кольце $B \supset A$ можно судить не находя самих корней, но проделав некоторые вычисления с коэффициентами многочлена в исходном кольце A. Причина состоит в том, что известная из анализа операция дифференцирования в применении к многочленам является *алгебраической*, т. е. может быть описана в терминах четырёх алгебраических операций без использования предельного перехода.

> Задача 3.12. Пусть A – любое кольцо. Убедитесь, что $\forall f \in A[x]$ многочлен $f(a) - f(b) \in A[a, b]$ делится нацело в $A[a, b]$ на двучлен $a - b$.
>
> Подсказка: см. тождество (a) из зад.1.9 лекции 1.

Пусть $f(x) \in A[x]$. Обозначим через $D_f(a, b) \in A[a, b]$ частное от деления $f(a) - f(b)$ на $a - b$ в кольце $A[a, b]$. Многочлен

$$f'(x) = D_f(x, x) \in A[x]$$

называется *производным* (или *производной*) от f. Другое обозначение[1]: $\frac{d}{dx}f$.

Задача 3.13. Убедитесь, что если $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, то

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + ba_nx^{n-1} = \sum_{\nu=1}^{n} \nu a_\nu x^{\nu-1} ,$$

где коэффициент ν перед a_ν есть элемент простого подкольца в A, т. е. он равен $\underbrace{1+1+\cdots+1}_{\nu \text{ раз}}$.

Задача 3.14. Убедитесь, что взятие производной удовлетворяет всем известным из анализа стандартным формальным правилам дифференцирования суммы, разности, произведения, частного и композиции.

Замечание: в дальнейшеем для нас особенно важным будет *правило Лейбница*:

$$(fg)' = f' \cdot g + f \cdot g' .$$

Оно следует из тождества $D_{fg}(a,b) = f(a) \cdot D_g(a,b) + \cdot D_f(a,b)g(b)$.

2.3.1. Предложение. *Пусть поле k имеет характеристику нуль. Корень a многочлена $f \in k[x]$ тогда и только тогда является r-кратным корнем, когда он будет корнем $(r-1)$-той производной $\left(\frac{d}{dx}\right)^r f$, но не будет корнем r-той производной $\left(\frac{d}{dx}\right)^{r-1} f$.*

Доказательство. Достаточно проверить, что максимальная степень $(x-a)$, которая делит $f'(x)$, ровно на единицу меньше максимальной степени $(x-a)$, делящей $f(x)$.

Пусть $f(x) = (x-a)^r g(x)$ и $g(x)$ не делится на $(x-a)$. По правилу Лейбница

$$f'(x) = r(x-a)^{r-1}g(x) + (x-a)^r g'(x) = (x-a)^{r-1}\Big(rg(x) + (x-a)g'(x)\Big) . \qquad (3\text{-}1)$$

Многочлен в скобках не делится на $(x-a)$, поскольку $rg(x) \neq 0$ и не делится на $(x-a)$.
□

Заметим, что в общем случае, из формулы (3-1) вытекают

2.3.2. Следствие. *Пусть A – любое коммутативное кольцо с единицей. Если $a \in A$ является r-кратным корнем многочлена $f \in A[x]$, то он является по меньшей мере $(r-1)$-кратным корнем его производной.*

□

2.3.3. Следствие. *Пусть A – любое коммутативное кольцо с единицей. Если $a \in A$ является простым корнем многочлена $f \in A[x]$, то $f'(a) \neq 0$.*

Доказательство. При $r = 1$ формула (3-1) имеет вид $f'(x) = g(x) - (x-a)g'(x)$, откуда $f'(a) = g(a) \neq 0$.
□

---

[1]символ $\frac{d}{dx}$ обычно используют для обозначения отображения из $A[x]$ в $A[x]$, сопоставляющего многочлену его производную

2.3.4. Сепарабельность. Пусть теперь k – поле. Многочлен $f \in k[x]$ называется *сепарабельным*, если он не имеет кратных корней ни в каком расширении $K \supset k$, и *несепарабельным* – в противном случае. Прямо из предыдущего следствия вытекает

2.3.5. Предложение. *Для несепарабельности $f \in k[x]$ необходимо и достаточно наличие общего корня у f и f' в некотором расширении поля k.*

2.3.6. Пример. Пусть $\mathrm{char}(k) = p > 0$ и $f(x) = x^p - 1 \in k[x]$. Так как $f'(x) = px^{p-1} = 0$ (ибо $p = \underbrace{1+1+\cdots+1}_{(p\text{ раз})} = 0$), то f — несепарабелен. Более того, если $K \supset k$ — какое-либо расширение, где у f есть корень ϑ : $\vartheta^p = 1$, то

$$x^p - 1 = x^p - \vartheta^p = (x - \vartheta)^p \;,$$

поскольку возведение в p-тую степень является в характеристике p гомоморфизмом. Таким образом, если в расширении K у f вообще есть корень, то он автоматически p-кратный (и единственный!).

2.3.7. Пример. Пусть $\mathrm{char}(k) = 0$. Тогда всякий неприводимый многочлен положительной степени $f(x) \in k[x]$ сепарабелен. В самом деле, $f'(x) \neq 0$ и *НОД* $(f, f') = 1$ из-за неприводимости f и неравенства $\deg f' < \deg f$. Следовательно, у f и f' нет общих корней ни в каком расширении.

2.4. Минимальный многочлен. Пусть $K \supset k$ — расширение полей. Элемент $\vartheta \in K$ называется *алгебраичным над* k, если $f(\vartheta) = 0$ для некоторого $f \in k[x]$. Приведенный многочлен f наименьшей степени, обладающий этим свойством, называется *минимальным многочленом* для ϑ над k, а его степень называется *степенью* ϑ над k.

Поскольку в поле нет делителей нуля, минимальный многочлен неприводим в $k[x]$, ибо подставляя ϑ в разложение $f(x) = g(x)h(x)$, мы должны будем иметь или $g(\vartheta) = 0$, или $h(\vartheta) = 0$, а значит, один из множителей имеет ту же степень что и f из-за минимальности f.

Опишем наименьшее подполе в K, содержащее k и ϑ. Для этого рассмотрим гомоморфизм вычисления значения в точке ϑ:

$$ev_\vartheta : \; k[x] \longrightarrow K : \; f \mapsto f(\vartheta).$$

Его ядро состоит из всех $g \in k[x]$, для которых ϑ будет корнем. Как и всякий идеал в $k[x]$, $\ker(ev_\vartheta)$ является главным идеалом, а его образующей будет приведённый многочлен наименьшей степени, зануляющийся на ϑ, т. е. в точности минимальный многочленом для ϑ. Мы получаем

2.4.1. Предложение. *Минимальный многочлен элемента ϑ над k делит в $k[x]$ любой другой многочлен $g \in k[x]$, для которого ϑ является корнем.*

□

Далее, по теореме о строении гомоморфизма образ $\mathrm{im}\,(ev_\vartheta) \subset K$ изоморфен фактор-кольцу $k[x]/(f)$. Последнее является полем, поскольку f неприводим. Это, очевидно, и есть наименьшее подполе в K, содержащее k и ϑ.

2.4.2. Предложение. *Множество значений всевозможных многочленов из $k[x]$ на элементе $\vartheta \in K$ составляет поле, являющееся наименьшим подполем в K, содержащим k и ϑ. Это поле изоморфно фактор-кольцу $k[x]/(f)$, где f – минимальный многочлен элемента ϑ.*

□

2.5. Присоединение корня. Предыдущая конструкция позволяет для любого поля k и любого неприводимого многочлена $f(x) \in k[x]$ построить такое расширение $K \supset k$, в котором у f появится корень. Действительно, в качестве K можно взять фактор-кольцо $k[x]/(f)$. Т. к. f неприводим, оно является полем. Поле k вложено в него посредством ограничения канонического гомоморфизма $k[x] \xrightarrow{res_f} k[x]/(f)$ редукции по модулю f на константы $k \subset k[x]$. Корнем многочлена f является элемент $\vartheta = res_f(x)$ — образ одночлена x.

Чтобы представить себе поле $K = k[x]/(f)$ более явно, зафиксируем в каждом классе вычетов по модулю f канонического представителя – остаток от деления элементов этого класса на f. Такой остаток может быть совершенно произвольным многочленом степени $\leq \deg(f) - 1$. Тем самым, если $\deg(f) = n$, то элементы $k[x]/(f)$ взаимно-однозначно записываются в виде

$$t_0 + t_1\vartheta + \cdots + t_{n-1}\vartheta^{n-1} ,$$

где $\vartheta = x(\bmod f)$ и $t_\nu \in k$ – любые, а операции над ними в $k[x]/(f)$ — это обычное сложение и умножение многочленов по модулю соотношения $f(\vartheta) = 0$, т. е. в точности те же операции, которые были описаны нами в лекции 1 при построении поля $k[\vartheta]$ с $f(\vartheta) = 0$.

Задача 3.15. Докажите, что $\mathbb{Q}[\vartheta]$ с $\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1 = 0$ — поле и найдите $(1+\vartheta^2)^{-1}$.

Задача 3.16. Пусть неприводимый многочлен $f \in k[x]$ имеет корень α в каком-то расширении $K \supset k$. Докажите, что поле $k[x]/(f)$ вкладывается в поле K гомоморфизмом, отображающим класс $x(\bmod f)$ в α.

Существование такого расширения, в котором данный многочлен имеет корень, позволяет обернуть доказанные выше результаты о наличии общих корней у пары многочленов и о кратных корнях.

2.5.1. Следствие. *Если $f, g \in k[x]$, где k – поле, и НОД $(f, g) \neq 1$, то f и g имеют в некотором расширении общий корень.*

Доказательство. Надо перейти к расширению, в котором будет иметь корень *НОД* (f, g).
□

2.5.2. Следствие. *Для сепарабельности многочлена f необходимо и достаточно, чтобы НОД $(f, f') = 1$.*

2.6. Алгебраические расширения полей. Расширение $K \supset k$ называется *алгебраическим*, если все элементы поля K алгебраичны над k.

2.6.1. Пример: конечные поля. Все элементы любого конечного поля $\mathbb{F}$ алгебраичны над простым подполем. Действительно, если $\vartheta \in \mathbb{F}$, то среди степеней ϑ^0, ϑ^1, ϑ^2, ... будут одинаковые, ибо $\mathbb{F}$ конечно. Если $\vartheta^k = \vartheta^m$, то ϑ — корень многочлена $x^{|m-k|} - 1 = 0$, определенного над простым подполем. Таким образом, если $\mathrm{char}\mathbb{F} = p$, то $\mathbb{F}$ получается из $\mathbb{Z}/p\mathbb{Z}$ при помощи конечного числа расширений, описанных в n° 2.5.

Задача 3.17. Докажите, что число элементов в конечном поле характеристики p равно p^n для некоторого $n \in \mathbb{N}$.

2.6.2. Пример: поле разложения многочлена. Для любого многочлена $f(x) \in k[x]$ существует расширение, в котором f полностью разлагается на линейные множители. Чтобы построить такое поле, надо присоединить к основному полю корень нелинейного неприводимого делителя f максимальной степени. В расширенном таким образом поле этот делитель станет приводимым, и тем самым, количество неприводимых делителей f максимальной степени уменьшится (либо уменьшится сама эта максимальная степень). Продолжая по индукции (т. е. присоединяя к уже построенному расширению корень неприводимого нелинейного делителя f уже над этим расширением), мы через конечное число шагов добьёмся того, что все неприводимые делители f станут линейными.

Посмтроенное таким образом расширение называется *полем разложения* многочлена f. Согласно зад.3.16, поле разложения вкладывается в любое другое поле, в котором f полностью разлагается на линейные множители. Поэтому поле разложения с точностью до автоморфизма, тождественного на исходном поле k, не зависит от произвола в своём построении, и может быть охарактеризовано[2] как *наименьшее* поле, в котором f распадается на линейные множители.

Задача 3.18. (необязательная) Пусть $K \supset k$ есть поле разложения неприводимого многочлена $f \in k[x]$. Докажите, что если какой-то неприводимый многочлен $g \in k[x]$ имеет корень в K, то он полностью разлагается в $K[x]$ на линейные множители.

Утешение: Это довольно трудная задача, и мы вернёмся к ней в последней лекции.

§3. Разложение на множители многочленов с целыми коэффициентами

3.1. Кольцо $\mathbb{Z}[x]$ Обратимыми элементами в $\mathbb{Z}[x]$, как и в $\mathbb{Z}$, являются только 1 и -1, так что коэффициенты многочленов, как правило, необратимы. Из-за этого многие факты о многочленах над полем перестают выполняться в $\mathbb{Z}[x]$.

Задача 3.19. Докажите, что идеал $(x, 2)$, порождённый в $\mathbb{Z}[x]$ многочленом x и постоянным многочленом 2, не является главным.

3.2. Лемма Гаусса. *Содержанием* $\mathrm{cont}(f)$ многочлена $f \in \mathbb{Z}[x]$ называется НОД его коэффициентов.

3.2.1. Предложение. (Лемма Гаусса) $\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$.

Доказательство. Из формулы, выражающей коэффициенты fg через коэффициенты f и g, следует, что всякий общий делитель коэффициентов f и всякий общий делитель коэффициентов g одновременно выносятся из коэффициентов fg. Поэтому $\mathrm{cont}(fg)$ делится на

[2] опять таки, однозначно с точностью до изоморфизма

$\mathrm{cont}(f)\cdot\mathrm{cont}(g)$. Сокращая на это произведение, мы без ущерба для общности можем предполагать, что $\mathrm{cont}(f) = 1$ и $\mathrm{cont}(g) = 1$, и должны будем показать, что в этом случае и $\mathrm{cont}(fg) = 1$.

Пусть это не так и $\mathrm{cont}(fg) = k \neq 1$, и p — какое-либо простое число, делящее k. Тогда p делит все коэффициенты fg, но не делит хотя бы один из коэффициентов f и хотя бы один из коэффициентов g. Рассмотрим гомоморфизм редукции по модулю p:

$$\pi_p\colon\ \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Он индуцирует гомоморфизм

$$\pi_p\colon\ \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x],$$

соответствующих колец многочленов, приводящий все коэффициенты многочлена $f(x)\in\mathbb{Z}[x]$ по модулю p:

$$\pi_p(a_0x^k + a_1x^{k-1} + \cdots + a_{k-1}x + a_k) = [a_0]_p + [a_1]_px + \cdots + [a_k]_px^k$$

(проверьте, что это гомоморфизм!). Но $\mathbb{Z}/p\mathbb{Z}[x]$, как и всякое кольцо многочленов над полем, не имеет делителей нуля, тогда как при наших предположениях $\pi_p(f) \neq 0$, $\pi_p(g) \neq 0$, но $\pi_p(f)\cdot\pi_p(g) = \pi_p(fg) = 0$.

Это противоречие показывает, что $\mathrm{cont}(fg) = 1$, что и требовалось.
□

3.2.2. Предложение. *Всякий многочлен $f(x) \in \mathbb{Q}[x]$ однозначно записывается в виде $f(x) = \dfrac{m}{n}\tilde{f}(x)$, где $\tilde{f}(x) \in \mathbb{Z}[x]$ – многочлен содержания 1, а $m/n \in \mathbb{Q}$ – несократимая дробь с положительным знаменателем.*

Доказательство. Существование разложения очевидно: надо привести все коэффициенты f к общему знаменателю, вынести его за скобку, затем вынести из оставшегося целочисленного многочлена *НОД* его коэффициентов и сократить возникашую в качестве множителя перед скобкой дробь.

Для доказательства единственности допустим, что $f(x) = \dfrac{m}{n}\tilde{f}(x) = \dfrac{r}{s}\widehat{f}(x)$ – два разложения с требуемыми свойствами. Умножая на ns и беря содержание обеих частей, получаем равенство $ms = nr$. Поскольку s взаимно прост с r, n будет делиться на s. Аналогично, r делится на m. Поэтому $n = s$ и $r = m$. Но тогда и $\tilde{f} = \widehat{f}$.
□

3.2.3. Следствие. *Если многочлен $f(x) \in \mathbb{Z}[x]$ раскладывается в $\mathbb{Q}[x]$ в произведение двух многочленов с рациональными коэффициентами, то он раскладывается и в $\mathbb{Z}[x]$ в произвеедение многочленов тех же степеней, но уже с целыми коэффициентами.*

Доказательство. Пусть в $\mathbb{Q}[x]$ имеется разложение $f(x) = g(x)h(x)$. В соответствии с предыдущим предложением, распишем

$$f(x) = m\tilde{f}(x) \quad , \qquad g(x) = \frac{p}{q}\tilde{g}(x) \quad , \qquad h(x) = \frac{r}{s}\tilde{h}(x)\ ,$$

где $\mathrm{cont}(\tilde{f}) = \mathrm{cont}(\tilde{g}) = \mathrm{cont}(\tilde{h}) = НОД\,(p,q) = НОД\,(p,q) = 1$. Умножая обе части равенства $f(x) = g(x)h(x)$ на qs и беря содержание, мы в следствие леммы Гаусса получим равенство $mqs = pr$, из которого, как и ранее, вытекает, что p делится на s, а r делится на q. Таким образом равенство

$$f(x) = \frac{r}{q}\tilde{g}(x)\frac{p}{s}\tilde{h}(x)$$

доставляет искомое разложение f в $\mathbb{Z}[x]$.
□

Непосредственно из доказательства получаем

3.2.4. Следствие. *Если $f(x) \in \mathbb{Z}[x]$, а $g(x) \in \mathbb{Z}[x]$ – многочлен содержания 1, делящий $f(x)$ в $\mathbb{Q}[x]$, то $g(x)$ делит $f(x)$ и в $\mathbb{Z}[x]$.*

3.2.5. Следствие. *Множество неприводимых элементов кольца $\mathbb{Z}[x]$ состоит из простых целых констант и неприводимых над полем $\mathbb{Q}$ целочисленных многочленов содержания 1.*

3.2.6. Следствие. *Неприводимые элементы $\mathbb{Z}[x]$ просты.*

Доказательство. Надо проверить, что если gh делится на неприводимый многочлен f, то либо g либо h делится на f.

Если $f \equiv p = \mathrm{const}$ — простое число, то либо $\mathrm{cont}(g)$, либо $\mathrm{cont}(h)$ делится на p (т.к. $\mathrm{cont}(g)\mathrm{cont}(h) = \mathrm{cont}(gh)$ делится на p).

Если f неприводим над $\mathbb{Q}$ и $\mathrm{cont}(f) = 1$, то либо g, либо h делится на f в $\mathbb{Q}[x]$, а значит и в $\mathbb{Z}[x]$ (по предыдущему следствию).
□

3.3. Разложение многочленов из $\mathbb{Z}[x]$ на множители над полем $\mathbb{Q}$. Все рациональные корни многочлена с целыми коэффициентами могут быть найдены при помощи конечного числа проб благодаря следующему факту:

3.3.1. Предложение. *Если несократимая дробь $a = p/q \in \mathbb{Q}$ является корнем многочлена $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x]$, то p делит a_0, а q делит a_n.*

Доказательство. Подставляя $x = p/q$ и приводя к общему знаменателю, получаем

$$a_0q^n + pq(\cdots) + a_np^n = 0.$$

Так как p и q взаимно просты, то p делит a_0 , а q делит a_n, что и требовалось доказать.
□

> Задача 3.20. Убедитесь, что $x^4 + 4$ раскладывается в $\mathbb{Z}[x]$ в произведением двух квадратных трёхчленов.

Эта задача показывает, что отсутствие рациональных корней вовсе не означает неприводимость многочлена с целыми коэффициентами. Вообще анализ неприводимости над полем $\mathbb{Q}$, хотя и является вполне алгоритмизуемой задачей, решаемой за конечное число шагов[3], часто оказывается очень тонким (или весьма трудоёмким) вопросом. Мы ограничимся здесь описанием двух прёмов, часто оказывающихся полезными

[3] см. например *Б. Л. ван дер Варден. Алгебра* (М. "Наука" (1976) гл. V §32 (с. 122)).

3.3.2. Предложение. (Критерий Эйзенштейна) *Пусть*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

приведённый многочлен с целыми коэффициентами. Если для некоторого простого $p \in \mathbb{Z}$ все коэффициенты a_ν делятся на p, но свободный член a_0 не делится при этом на p^2, то $f(x)$ неприводим над $\mathbb{Q}$.

Доказательство. Согласно лемме Гаусса достаточно доказать, что $f(x)$ не разлагается в $\mathbb{Z}[x]$ в произведение двух множителей меньшей степени. Допустим, что такое разложение $f(x) = g(x)h(x)$ существует. Как и в доказательстве теоремы Пр.3.2.1, применим к этому равенству гомоморфизм π_p приведения по модулю p. Получим равенство

$$\pi_p(f) = \pi_p(g)\pi_p(h) \qquad \text{в } \mathbb{Z}/p\mathbb{Z}[x].$$

По условию $\pi_p(f) = x^n$, т.е. состоит лишь из старшего члена. Из этого следует, что старшие коэффициенты многочленов g и h остаются ненулевыми при редукции по модулю p, а оба свободных члена зануляются (иначе произведение свободного члена на младший из ненулевых членов другого многочлена дало бы ненулевой младший член в $\pi_p(f)$ степени меньшей, чем n). Таким образом, свободные члены и у h и у g делятся на p. Но тогда свободный член у f делится на p^2, что запрещается условием.
□

3.3.3. Пример. Пусть p — простое число. Многочлен

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

называется *многочленом деления круга*, ибо его комплексные корни — это в точности все отличные от 1 корни уравнения деления единичного круга на p равных частей (см. лекцию 1). При помощи критерия Эйзенштейна докажем, что $f(x)$ неприводим в $\mathbb{Q}[x]$. Для этого заметим, что неприводимость $f(x)$ в $\mathbb{Q}[x]$ равносильна неприводимости многочлена $g(t) = f(t+1)$ в $\mathbb{Q}[t]$ (т.к. замена $x = t + 1$ обратима: $t = x - 1$). Но

$$g(t) = \frac{(t+1)^p - 1}{t} = t^{p-1} + \binom{p}{1}t^{p-2} + \binom{p}{2}t^{p-3} + \cdots + \binom{p}{p-2}t + \binom{p}{p-1}$$

удовлетворяет критерию Эйзенштейна: все его коэффициенты $\binom{p}{k}$ делятся на p, а свободный член (равный p), делясь на p, не делится на p^2. Стало быть, $g(t)$, а с ним и $f(x)$, неприводимы.

3.3.4. Приведение по простому модулю, которым мы уже много раз успешно пользовались в этой лекции, часто оказывается весьма эффективным средством при анализе разложимости целочисленного многочлена. Дело в том, что над полем $\mathbb{Z}/p\mathbb{Z}$ имеется лишь конечное число неприводимых многочленов данной степени, и при небольшой степени и малых p они могут быть легко перечислены.

Например, чтобы выяснить, разлагается ли $f(t) = t^5 + t^2 + 1$ на множители в $\mathbb{Z}[t]$, достаточно рассмотреть его над $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Если бы f был приводим над $\mathbb{Z}$, то над $\mathbb{F}_2$ он обязан был бы делится на неприводимый приведённый многочлен степени ≤ 2. Но таковых в $\mathbb{F}_2[t]$ всего три:

$$t \quad , \qquad t+1 \quad , \qquad t^2+t+1 \,,$$

и деля столбиком (над $\mathbb{F}_2$) непосредственно убеждаемся, что f имеет остаток 1 от деления на каждый из этих трёх многочленов.

Помимо информации негативного характера, редукция по модулю p позволяет делать и позитивные выводы — например, определить, какими могут быть степени неприводимых делителей, и каковы классы вычетов их коэффициентов по модулю p.

3.4. Разложение над $\mathbb{R}$ и $\mathbb{C}$ В любом курсе комплексного анализа доказывается.

3.4.1. Предложение. *Всякий многочлен из $\mathbb{C}[x]$ имеет корень в $\mathbb{C}$.*

□

Несмотря на то, что эту теорему часто называют *основной теоремой алгебры*, причина, по которой она справедлива, кроется не в *алгебраических* свойствах поля $\mathbb{C}$, а в его *аналитических* свойствах[4]. Мы не будем здесь доказывать эту теорему, но отметим её алгебраические следствия.

3.4.2. Следствие. *Неприводимыми в $\mathbb{C}[x]$ являются только константы и многочлены степени 1.*

3.4.3. Следствие. *Неприводимыми в $\mathbb{R}[x]$ являются константы, многочлены степени 1 и квадратичные многочлены с отрицательным дискриминантом.*

Доказательство. Если $z = a+ib$ — комплексный корень многочлена $f(x) = f_0x^n + f_1x^{n-1} + \dots + f_{n-1}x + f_n \in \mathbb{R}[x]$, то применяя к равенству $f(z) = 0$ гомоморфизм комплексного сопряжения (при котором вещественные числа неподвижны), получим

$$0 = \bar{0} = \overline{f(z)} = \overline{f_0z^n + f_1z^{n-1} + \dots + f_{n-1}z + f_n} = f_0\bar{z}^n + f_1\bar{z}^{n-1} + \dots + f_{n-1}\bar{z} + f_n = f(\bar{z}).$$

Поэтому $\bar{z} = a - ib$ таккее будет корнем для f. Но тогда f делится на

$$(x-z)(x-\bar{z}) = x^2 - (z+\bar{z})x + z\bar{z} = x^2 - 2\mathrm{Re}(z)x + |z|^2 = x^2 - 2ax + (a^2+b^2).$$

Следовательно, любой многочлен степени ≥ 3 приводим в $\mathbb{R}[x]$ и разлагается в произведение линейных и квадратичных. Квадратичные же многочлены приводимы тогда и только тогда, когда у них есть вещественные корни.

3.4.4. Следствие. *Комплексные невещественные корни многочленов из $\mathbb{R}[x]$ разбиваются на пары комплексно-сопряженных.*

[4]Видимо, самый прямой способ получить основную теорему алгебры — это применить *теорему Лиувилля* к аналитической (т.е. представимой в виде суммы *абсолютно сходящеегося ряда*) фунции $1/f(x)$, где $f \in \mathbb{C}[z]$ — многочлен, про который предполагается, что у него нет корней. Теорема Лиувилля утверждает, что ограниченная аналитическая функция, определенная на всем $\mathbb{C}$ — константа.

§4. Факториальность

4.1. Разложение на неприводимые множители и нётеровость. Пусть A — целостное кольцо. С точки зрения делимости неприводимые элементы A являются теми “атомами”, из которых составляются при помощи перемножения все прочие элементы A. Действительно, если $a \in A$ не является неприводимым, то $a = b_1 b_2$. Если b_1 и b_2 приводимы, скажем, $b_1 = c_1 c_2$, $b_2 = c_3 c_4$, то $a = c_1 c_2 c_3 c_4$ и т.д. Как правило, этот процесс не может продолжаться бесконечно. Например, в кольце $\mathbb{Z}$ с каждым шагом строго уменьшается модуль самого большого по модулю приводимого сомножителя, в кольце $k[x_1, \dots, x_n]$ — его степень, а в $\mathbb{Z}[x_1, \dots, x_n]$ — и то и то параллельно. Мы получаем

4.1.1. Предложение. *В кольцах $\mathbb{Z}$, $\mathbb{Z}[x_1, \dots, x_n]$, $k[x_1, \dots, x_n]$ (где k — поле) любой элемент является произведением конечного числа неприводимых.*

□

Если описанный выше процесс разложения на множители не заканчивается за конечное число шагов, то он позволяет построить *бесконечную* последовательность приводимых элементов c_ν, в которой $c_{\nu+1}$ является собственным делителем c_ν при каждом ν. На языке идеалов, это означает, что главные идеалы $\mathfrak{I}_\nu = (c_\nu)$ образуют бесконечную цепочку *строго* вложенных друг в друга идеалов:

$$\mathfrak{I}_1 \subset \mathfrak{I}_2 \subset \mathfrak{I}_3 \subset \cdots .$$

4.2. Определение. *Кольцо A называется нётеровым, если в нём не существует бесконечных возрастающих последовательностей строго вложенных идеалов.*

Без употребления отрицаний нётеровость можно охарактеризовать тем, что для любой последовательности идеалов $\mathfrak{I}_\nu$, в которой $\mathfrak{I}_\nu \subset \mathfrak{I}_{\nu+1}$, можно указать номер $N \in \mathbb{N}$, начиная с которого последовательность стабилизируется, т. е. $\mathfrak{I}_\nu = \mathfrak{I}\nu + 1 \ \forall \ \nu \geq N$.

Прямо из определений получаем

4.2.1. Предложение. *В целостном нётеровом кольце любой элемент является произведением конечного числа неприводимых.*

□

Один класс нётеровых колец нам хорошо известен.

4.2.2. Лемма. *Кольцо главных идеалов нётерово.*

Доказательство. Объединение $\mathfrak{I}_\infty \overset{\text{def}}{=} \bigcup\limits_\nu \mathfrak{I}_\nu$ всех идеалов любой цепочки вложенных идеалов является, очевидно, идеалом (проверьте!). Обозначим через d образующую этого идеала. Эта образующая лежит в одном из идеалов $\mathfrak{I}\nu$, скажем, пусть $d \in \mathfrak{I}_N$. Тогда $\mathfrak{I}_\infty = \mathfrak{I}_N$, что и означает нётеровость.

□

4.3. Однозначность разложения. Кольцо A называется *факториальным*, если оно целостное и каждый элемент $a \in A$ разлагается в произведение конечного числа неприводимых

$$a = p_1 p_2 p_3 \dots p_m \ ,$$

причем это разложение *единственно* с точностью до перестановки сомножителей и умножения их на обратимые элементы кольца. Иначе говоря, если $a = q_1q_2\dots q_k$ — другое разложение, то $m = k$ и, возможно, после подходящей перенумерации q_ν будет ассоциирован p_ν при всех ν.

В отличие от существования разложения, единственность разложения является весьма тонким фактом. Именно поэтому основную теорему арифметики иногда называют *теоремой об однозначности разложения на простые множители*, подчеркивая именно однозначность.

4.3.1. Лемма. *Если в целостном кольце A каждый элемент является произведением конечного числа неприводимых, то A факториально тогда и только тогда, когда каждый неприводимый элемент в A прост.*

Доказательство. Пусть A факториально, q — неприводим. Надо проверить, что если ab делится на q, то или a, или b делится на q.

Пусть $ab = qr$. Разложим в этом равенстве a, b и r на неприводимые:

$$\underbrace{(p_1\cdots p_m)}_{a}\cdot\underbrace{(p_{m+1}\cdots p_n)}_{b} = q\cdot\underbrace{(q_1\cdots q_k)}_{r}.$$

Из единственности один из множителей в левой части ассоциирован с q. Пусть $p_1 = sq$. Тогда $a = q(sp_1\cdots p_m)$ делится на q. Тем самым в факториальном кольце неприводимые элементы просты.

Пусть теперь дано, что в A все неприводимые элементы просты и имеется два разложения на неприводимые множители

$$p_1p_2\cdots p_k = q_1q_2\cdots q_m.$$

Так как p_1 прост, то произведение в правой части должно содержать множитель, делящийся на p. Пусть это q_1, т.е. $q_1 = sp_1$.

Задача 3.21. Убедитесь, что s — обратим.

Перенося правую часть влево и вынося общий множитель, получим, что

$$p_1(p_2\cdots p_k - sq_2\cdots q_m) = 0.$$

Так как A — целостное кольцо, получаем равенство двух разложений на неприводимые множители

$$p_2p_3\cdots p_k = (sq_2)q_3\cdots q_m,$$

состоящих из строго меньшего, чем ранее количества множителей. Продолжая так дальше, получим, что $m = n$, а соответственные сомножетели — ассоцированны. Лемма доказана. □

4.3.2. Следствие. *Кольца $\mathbb{Z}$, $k[x]$ и $\mathbb{Z}[x]$ факториальны.*

4.3.3. Следствие. *Любая область главных идеалов факториальна.*

4.3.4. Факториальность кольца многочленов. При помощи леммы Гаусса и рассуждений, аналогичных проделанным в §3, но с использованием более общих понятий, нетрудно доказать, что *кольцо многочленов* $A[x]$ *над любым факториальным кольцом* A *факториально*. В частности, факториальны кольца $\mathbb{Z}[x_1, \ldots, x_n]$ и $k[x_1, \ldots, x_n]$. Мы вернёмся к этому в лекции 8, но уже сейчас вы можете использовать эти факты при решении задач на упражнениях. Подробнее о факториальных кольцах см. в книге: Ленг С. Алгебра (стр.148-151 по изданию М."Мир".1968).

Лекция 4
Линейные уравнения и матрицы

▷Системы линейных уравнений, их матрицы и элементарные преобразования ▷Приведение матрицы над полем к строгому ступенчатому виду преобразованиями строк ▷Решение систем линейных уравнений над полем ▷Замены переменных и матрицы перехода ▷Сложение и умножение матриц ▷Аксиомы (некоммутативного) кольца с единицей ▷Элементарные матрицы ▷Отыскание обратной матрицы ▷Приведение матрицы над $\mathbb{Z}$ или $k[x]$ к диагональному виду преобразованиями строк и столбцов ▷Решение систем линейных уравнений над $\mathbb{Z}$ и $k[x]$

§1. Основные понятия

Система линейных уравнений — это одна из очень и очень немногих задач, допускающих полное и исчерпывающее решение, и принцип линеаризации, состоящий в том, что всякую вычислительную проблему, как правило, можно свести к линейным уравнениям, является излюбленным приёмом в алгебре, геометрии и анализе. Линейным уравнениям посвящены целая отрасль алгебры — *линейная алгебра*, и целая отрасль анализа — *линейный функциональный анализ.*

Как и всякую задачу, линейные уравнения можно решать на двух языках — геометрическом и алгебраическом. Первый сопоставляет задаче систему геометрических образов и исследует их взаимодействие, опираясь на интуицию картинок. Второй вводит удобную алгебраическую символику и аппелирует к интуиции формул. Геометрия линейных уравнений — это геометрия *векторных пространств*, или *модулей*. Алгебра линейных уравнений - это *алгебра матриц*. В этой лекции мы обсудим формально-алгебраическую сторону дела, а две следующие будут посвящены геометрическим аспектам.

1.1. Уравнения. Пусть требуется решить систему из m линейных уравнений с n неизвестными:

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \cdots & & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{cases} .$$

Это означает, что некотором коммутативном кольце R с единицей заданы mn чисел $\{a_{ij}\}$, называемых *коэффициентами* системы, и m чисел $\{b_i\}$, называемых *правыми частями* системы. Решить систему в некотором большем кольце $R_1 \supset R$, содержащем R в качестве подкольца, — это значит описать все возможные упорядоченные наборы $(c_1, c_2, \ldots, c_n) \in R_1 \times R_1 \times \cdots \times R_1$, которые при подстановке $x_i = c_i\,,\ (i = 1, 2, \cdots, n)$ превращают все уравнения системы в равенства, справедливые в кольце R_1. Каждый такой набор $(c_1, c_2, \ldots, c_n)$ называется *решением системы* в кольце $R_1 \supset R$.

Мы не будем в этих лекциях изучать системы уравнений в такой большой общности, а ограничимся случаями, когда $R = R_1$ будет (произвольным) полем k, кольцом целых чисел $\mathbb{Z}$ или кольцом многочленов $k[x]$.

1.2. Матрицы. Таблица коэффициентов из левых частей предыдущих уравнений

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

называется *матрицей системы*, а та же таблица, дополненная справа отдельной колонкой правых частей:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

называется *расширенной матрицей системы*. Она содержит всю необходимую для решения системы информацию, если раз и навсегда условиться писать все уравнения так, чтобы неизвестные шли в фиксированном порядке $x_1, x_2, \ldots, x_n$.

Всюду далее, решая системы, мы будем работать исключительно только с их матрицами. Вообще же под *$m \times n$-матрицей над кольцом R* мы всегда будем понимать прямоугольную таблицу из m строк длины n, заполненную числами из R. При этом m мы будем называть *высотой*, а n — *шириной* матрицы.

Матрицы мы будем обозначать большими латинскими буквами A, B, и т.д. Элемент матрицы A, стоящий в пересечении i-той строчки и j-того столбца, мы будем обозначать через a_{ij}. Иногда для обозначения матрицы мы будем писать (a_{ij}) вместо A.

§2. Метод Гаусса над полем

2.1. Элементарные преобразования уравнений. Следуя школьной традиции, будем называть две системы уравнений *равнолсильными*, если их множества решений совпадают. Один из способов решения систем состоит в том, чтобы последовательно заменять их на более простые равносильные системы. Особенно удобны три простейших замены подобного рода, называемых *элементарными преобразованиями* (эп):

(эп-1) Элементарное преобразования *первого типа*: перемена каких-либо двух уравнений местами.

(эп-2) Элементарные преобразования *второго типа*: вместо одного из уравнений системы написать его сумму с уравнением, полученным в результате умножения обеих частей любого другого уравнения системы на произвольное число. (Подчеркнём, что изменяется ровно одно уравнение — то, к которому прибавляют. Вспомогательное уравнение, кратность которого прибавляется к изменяемому уравнению, должно быть переписано в преобразованную систему без изменений.)

(эп-3) Элементарные преобразования *третьего типа*: умножить обе части какого-либо уравнения на число, не являющемся делителем нуля.

2.1.1. Предложение. *Элементарные преобразования меняют систему на равносильную.*

Доказательство. Рассмотрим, к примеру, случай (эп-2). Пусть система $\mathfrak{S}_2$ получается из системы $\mathfrak{S}_1$ заменой уравнеия $\mathfrak{a}\in\mathfrak{S}_1$ на уравнение $\mathfrak{c} = \mathfrak{a} + \lambda\mathfrak{b}$, где $\mathfrak{b}\in\mathfrak{S}_1$, $\mathfrak{b} \neq \mathfrak{a}$.

Ясно, что всякое решение $\mathfrak{S}_1$ останется и решением $\mathfrak{S}_2$, ибо оно обращает и $\mathfrak{a}$ и $\mathfrak{b}$ в верные равенства.

Заметим теперь, что система $\mathfrak{S}_1$ также может быть получена из системы $\mathfrak{S}_2$ при помощи (эп-2), а именно, к уравнению $\mathfrak{c}\in\mathfrak{S}_2$ надо прибавить уравнение $\mathfrak{b}\in\mathfrak{S}_2$, умноженное на $(-\lambda)$. Но тогда всякое решение $\mathfrak{S}_2$ является решением и для $\mathfrak{S}_1$.

Задача 4.1. Убедитесь, что (эп-1) и (эп-3) также является равносильным преобразованием.

Задача 4.2. Приведите пример уравнения над кольцом вычетов $\mathbb{Z}/n\mathbb{Z}$, множество решений которого меняется при умножении на ненулевой вычет.

2.2. Элементарные преобразования матриц. При рассмотренных выше элементарных преобразований систем их матрицы также подвергаются элементарным преобразованиям:

(1-й тип) перемена двух строк местами;

(2-й тип) замена строки на ее поэлементную сумму с какой-либо другой строкой, умноженной (поэлементно) на любое число (при этом сама эта вторая строка остается в матрице системы без изменения);

(3-й тип) поэлементное умножение какой-либо строки на число, не являющееся делителем нуля.

2.3. Теорема. *Над любым полем k любая $m\times n$-матрица элементарными преобразованиями строк может быть приведена к так называемому строгому ступенчатому виду, который характеризуется тем, что в каждой строке самый левый ненулевой элемент:*

(1) равен 1;

(2) располагается строго правее, чем в предыдущей строке;

(3) является единственным ненулевым элементом своего столбца.

Доказательство. Процесс приведения будет состоять из n последовательных шагов (по количеству столбцов).

Перед выполнением k-ого шага предполагается, что та часть матрицы, которая расположена слева от k-ого столбца уже имеет нужный вид (в частности, может быть пустой или тождественно нулевой). Пусть в ней имеется s ненулевых строк. Отметим, что $0 \leq s \leq k-1$.

Сам k-ый шаг состоит в следующем.

Прежде всего в k-ом столбце в позициях строго ниже s-той выбирается ненулевой элемент (если его нет, то часть матрицы, расположенная слева от $(k+1)$-го столбца имеет нужный вид и можно сразу переходить к $(k+1)$-му шагу).

После того, как этот элемент выбран, строка, в которой он стоит, меняется местами с $(s+1)$-ой строкой, а затем умножается на элемент, обратный выбранному. В результате левые $k-1$ столбцов матрицы не изменяются, а $(s+1)$-ая строка приобретает вид

$$\underbrace{0\,0\,\ldots\,0\,0}_{k-1}\,1\,\underbrace{*\,*\,\ldots\,*\,*}_{n-k}\,.$$

В заключение к каждой строке, имющей в k-том столбце отличный от нуля элемент (кроме, разумеется, самой $(s+1)$-ой строки) прибавляется подходящая кратность $(s+1)$-ой строки так, чтобы этот ненулевой элемент занулился. Это опять не портит левой части матрицы и зануляет весь k-ый столбец за исключением единицы в $(s+1)$-ой строке. В результате мы попадаем в исходное положение для $(k+1)$-ого шага.
□

2.4. Решение системы линейных уравнений над полем методом Гаусса. состоит в том, что исходная система описанным выше путем преобразуется в равносильную систему, расширенная матрица которой имеет строго ступенчатый вид. Перенумеровав, если надо, переменные (т.е. переставив столбцы матрицы), мы можем считать, что итоговая расширенная матрица имеет вид:

$$\left[\begin{array}{cccc|ccc|c}
1 & & & & * & \cdots & * & b_1 \\
 & 1 & & 0 & * & \cdots & * & b_2 \\
0 & & \ddots & & \vdots & \vdots & \vdots & \vdots \\
 & & & 1 & * & \cdots & * & b_r \\
\hline
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_{r+1} \\
\hline
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}\right]$$

Такая система легко решается. Назовём первые r неизвестных $x_1, x_2, \ldots, x_r$ *связанными*, а остальные неизвестные $x_{r+1}, \ldots, x_n$ будем назвать *свободными*. Имеются, очевидно, две качественно разных возможности для последнего столбца.

Первая: $b_{r+1} = 1$, $b_1 = b_2 = \cdots = b_r = 0$ (т.е. расширенная матрица имеет ровно на одну ненулевую строку больше, чем матрица коэффициентов). Это имеет место тогда и только тогда, когда система несовместна.

Вторая: $b_{r+1} = 0$, а остальные правые части $b_1, b_2, \ldots, b_r$ – произвольны. Здесь любой набор из $(n-r)$ значений свободных неизвестных однозначно дополняется до решения системы, в котором значения связанных неизвестных вычисляются по формулам

$$x_s = b_s - \sum_{\nu=r+1}^{n} m_{s\nu} x_\nu \ , \quad s = 1, 2, \ldots, r \ ,$$

где $m_{s\nu}$ – это элемент из s-той строки и ν-того столбца написанной выше матрицы. Таким образом, в этом случае все решения системы взаимно-однозначно линейно параметризуется $n - r$ “произвольными постоянными”. В частности, при $n = r$ решение существует и единственно.

Задача 4.3. Докажите, что две системы равносильны тогда и только тогда, когда их расширенные матрицы приводятся элементарными преобразованиями строк к одной и той же строго ступенчатой матрице.

Указание. Проверьте, что разные строго ступенчатые матрицы задают системы с разными множествами решений.

2.4.1. Пример: однородные системы. Система линейных уравнений называется *однородной*, если все её правые части равны нулю. Однородная система, очевидно, остаётся таковой и после элементарных преобразований, и поэтому относится ко второму из рассмотренных выше типов. В частности, однородная ситема всегда имеет тривиальное *нулевое* решение. Непосредственно из предыдущего анализа вытекают

2.4.2. Следствие. *Однородная система m линейных уравнений от $n > m$ неизвестных всегда имеет ненулевое решение.*

2.4.3. Следствие. (Альтернатива Фредгольма.) *Система, в которой число уравнений равно числу неизвестных, либо имеет единственное решение при любых правых частях, либо имеет ненулевое решение при нулевых правых частях.*

§3. Алгебра матриц

Алгебраический матричный формализм служит для того,чтобы записывать преобразования систем линейных уравнений короткими алгебраическими формулами. В основе его лежат две операции над матрицами - сложение и умножение.

3.1. Определение. *Сумма $A + B$ двух матриц A и B определена для любых двух матриц одинакового размера и представляет собой матрицу того же размера, элементы которой суть суммы соответствующих элементов у A и B.*

Иными словами, если $A = (a_{ij})$, $B = (b_{ij})$, то $C = A + B$ имеет $c_{ij} = a_{ij} + b_{ij}$.

Задача 4.4. Докажите, что сложение матриц (с элементами из некоторого фиксированного кольца) коммутативно, ассоциативно, обладает нулем, а также что у каждой матрицы имеется единственная противоположная.

3.2. Определение. *Произведение AB определено тогда и только тогда, когда горизонтальный размер матрицы A равен вертикальному размеру матрицы B. Результатом произведения матрицы $A = (a_{ij})$ размера $m \times n$ и матрицы $B = (b_{ij})$ размера $n \times k$ является матрица $C = AB = (c_{ij})$ размера $m \times k$, элементы c_{ij} которой находятся по правилу:*

$$c_{ij} = \sum_{\nu=1}^{n} a_{i\nu} b_{\nu j} \ .$$

Иными словами, матрица-произведение имеет столько же строк, сколько первый сомножитель и столько же столбцов, сколько второй сомножитель, а для вычисления элемента, стоящего на пересечении i-ой строки и j-ого столбца надо взять i-ую строку первого сомножителя и j-ый столбец второго и "скалярно перемножить" их (т.е. умножить первый элемент на первый, второй на второй, и т. д., а затем сложить полученные n произведений).

3.2.1. Замечание. Определение произведение *несимметрично*, и если AB определено, то BA может быть и не определено: AB и BA определены одновременно тогда и только тогда, когда при размере матрицы A равном $m \times n$ матрица B имеет "транспонированный" размер $n \times m$.

Более того, даже если A и B — это квадратные матрицы одинакового размера, произвендения AB и BA, как правило, не равны! Например:

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 12 & 15 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 23 \end{pmatrix}$$

3.2.2. Пример. Рассмотрим левую часть системы линейных уравнений как матрицу-столбец размера $m \times 1$:

$$\begin{pmatrix} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n \\ & & & \cdots & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n \end{pmatrix} .$$

Тогда мы можем записать её как произведение

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

матрицы системы (её размер $m \times n$) и матрицы-столбца высоты n, составленного из неизвестных. Таким образом, система линейных уравнений

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \cdots & & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{cases} .$$

может быть записана в виде *одного линейного уравнения на матрицы*

$$Ax = b\ ,$$

где $A = (a_{ij})$ и $b = (b_j)$ — заданные матрицы, а $x = (x_i)$ — неизвестная матрица, подлежащая определению. Возникает естественное желание: чтобы найти x надо "разделить" обе части этого уравнения на матрицу A. Ниже в этой лекции мы объясним, что это означает.

3.2.3. Пример: линейные замены переменных. Помимо рассмотренного выше способа упрощения систем путём преобразования уравнений, из школы хорошо известен и другой способ — *замена переменных*. Он заключается в переходе от переменных (x_i) к новым переменным (y_ν) (возможно, в другом количестве). при помощи подстановки

$$x_i = \varphi_i(y_1, y_2, \ldots, y_k)\ ,$$

где справа стоят какие-то явные выражения x_i через $(y_1, y_2, \ldots, y_k)$. Искусно подобрав эти выражения, можно надеяться получить на (y_ν) более простые уравнения, чем на (x_i), решить их, а затем вернуться к исходным переменным.

Простейшие замены переменных — линейные. Они заключаются в подстановке:

$$x_i = c_{i1}y_1 + c_{i1}y_2 + \cdots + c_{ik}y_k = \sum_{\nu=1}^{k} c_{i\nu}y_\nu\ ,$$

где $i = 1, 2, \ldots, n$. При помощи умножения матриц это коротко записывается в виде

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = C \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix}\ ,$$

где $C = (c_{ij})$ — матрица размера $n \times k$, называеиая *матрицей перехода* от x к y и обозначаемая (как правило) через C_{yx}.

Можно сказать,что данное выше определение произведения матриц в действительности *специально подгонялось* к тому, чтобы было выполнено свойство:

3.2.4. Предложение. *Пусть последовательно выполняются две линейных замены переменных:*

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = C_{yx} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} = C_{zy} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}\ ,$$

где C_{yx} и C_{zy} — матрицы размеров $m \times n$ и $k \times m$ соответственно. Тогда

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} = C_{zx} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}\ , \quad \text{где} \quad C_{zx} = C_{zy} \cdot C_{yz}\ .$$

Иными словами, матрица перехода для композиции двух линейных замен переменных равна произведению матриц перехода этих замен (в том же порядке).

Доказательство. Пусть $C_{zy} = A = (a_{ij})$ и $C_{zy} = B = (b_{ij})$. Тогда

$$z_i = \sum_{\nu=1}^{m} a_{i\nu} y_\nu = \sum_{\nu=1}^{m} a_{i\nu} \sum_{j=1}^{n} b_{\nu j} x_j \ .$$

Группируя вместе слагаемые с одинаковыми j и вынося x_j за скобку, получим:

$$z_i = \sum_{j=1}^{n} c_{ij} x_j \ , \quad \text{где} \quad c_{ij} = \sum_{\nu=1}^{m} a_{i\nu} b_{\nu j} \ ,$$

что и означает, что $C_{zx} = (c_{ij}) = A \cdot B = C_{zy} C_{yz}$.

3.3. Свойства действий над матрицами. Для того, чтобы введенные нами операции над матрицами превратились из удобных обозначений в эффективное вычислительное средство, необходимо выяснить, как они взаимодействуют между собой, т.е. описать "законы сложения и умножения".

3.3.1. Предложение. *Умножение матриц ассоциативно, т.е. всякий раз, как определена одна из матриц $(AB)C$ или $A(BC)$, вместе с ней определена и другая, причем $(AB)C = A(BC)$.*

Доказательство. Это немедленно следует из предыдущего предложения (ибо замена переменных, очевидно, ассоциативна). Для тех, кто не удовлетворён таким замечанием, приведём также и формальную выкладку.

Пусть $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ имеют размеры, соответственно, $m \times n$, $n \times k$, $k \times s$. Тогда (i, j)-тый элемент матрицы $F = (AB)C$ вычисляется по формуле

$$f_{ij} = \sum_{\nu=1}^{k} \Big(\sum_{\mu=1}^{n} a_{i\nu} b_{\nu\mu} \Big) c_{\mu j} = \sum_{\nu=1}^{k} \sum_{\mu=1}^{n} a_{i\nu} b_{\nu\mu} c_{\mu j} \quad .$$

Группируя вместе слагаемые с одинаковыми $a_{i\nu}$, получаем:

$$f_{ij} = \sum_{\nu=1}^{k} a_{i\nu} \Big(\sum_{\mu=1}^{n} b_{\nu\mu} c_{\mu j} \Big) = \sum_{\nu=1}^{k} a_{i\nu} g_{\nu j} \ .$$

Здесь $g_{\nu j} = \sum\limits_{\mu=1}^{n} b_{\nu\mu} c_{\mu j}$ является (ν, j)-м элементом матрицы BC, а значит, (f_{ij}) совпадает с (ij)-тым элементом матрицы $A(BC)$.
□

3.3.2. Предложение. *Сложение и умножение дистрибутивны друг относительно друга. Точнее, если определена одна из частей в равенствах:*

$$\begin{aligned} A(B + C) &= AB + AC \qquad \text{(левая дистрибутивность)} \\ (A + B)C &= AC + BC \qquad \text{(правая дистрибутивность)} \end{aligned}$$

то определена и другая, а сами равенства верны.

Доказательство. Чтобы $A(B+C)$ (или $AB+AC$) имело смысл, размеры A, B, C должны иметь вид: $m \times n$, $n \times k$, $n \times k$. Если $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$, то (i,j)-тый элемент матрицы $F = A(B+C)$ есть

$$f_{ij} = \sum_{\nu=1}^{k} a_{i\nu}(b_{\nu j} + c_{\nu j} = \sum_{\nu=1}^{k} a_{i\nu}b_{\nu j} + \sum_{\nu=1}^{k} a_{i\nu}c_{\nu j} \ .$$

Справа стоит сумма (i,j)-того элемента матрицы AB с (i,j)-тым элементом матрицы AC, то есть (i,j)-ый элемент матрицы $AC + AB$. Это доказывает левую дистрибутивность.

Задача 4.5. Докажите праую дистрибутивность.

3.4. Определение. *Множество R с двумя бинарными операциями: сложением и умножением называется (некоммутативным) кольцом с единицей, если выполняются следующие*

Аксиомы (некоммутативного) ассоциативного кольца

1) Сложение коммутативно, ассоциативно, обладает нулем, и у каждого элемента есть противоположный.

2) Умножение ассоциативно и обладает двусторонней единицей; последнее означает, что

$$\exists E \in R: \quad AE = EA = A \qquad \forall A \in R \, .$$

3) Имеется левая и правая дистрибутивность:

$$A(B+C) = AB + AC \qquad \text{и} \qquad (A+B)C = AC + BC \qquad \forall\, A, B, C \in R \, .$$

3.4.1. Замечание. Отличие от аксиом коммутативного кольца — отсутствие коммутативности умножения — означает, неформально, что *умножение на A слева* и *умножение на A справа*— это две *разные* операции, имеющие, вообще говоря, разные свойства. Поэтому в теории некоммутативных колец свойства левого и правого умножений постоянно приходится рассматривать по отдельности, начиная уже с формулировок аксиом.

Задача 4.6. Докажите, что из аксиом кольца вытекает, что:
а) нулевой элемент $O \in R$ единственен;
б) $(-E)A = (-A) = A(-E)$;
в) $OA = AO = O \qquad \forall A \in R$.

3.5. Теорема. *Квадратные матрицы размера $n \times n$, элементы которых принадлежат фиксированному (возиожно, некоммутативному) кольцу R сами составляют кольцо*[1].

Доказательство. Легко видеть, что проделанные выше вычисления, доказывающие ассоциативность и дистрибутивность умножения, сохраняют смысл над любым (некоммутативным) кольцом R.

[1] Оно обозначается $Mat_n(R)$

Единицей в $Mat_n(R)$ служит так называемая *единичная матрица*

$$E \stackrel{\text{def}}{=} \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix},$$

на диагонали которой стоят единичные элементы кольца R, а в остальных местах - нули.

Задача 4.7. Проверьте, что $AE = EA = A \qquad \forall\, A \in Mat_n(R)$.

Выполнение аксиом сложения немедленно следует из их выполнения в R (ср. с зад.4.4).

□

3.5.1. Терминология. Диагонали $\begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix}$ и $\begin{pmatrix} & & * \\ & * & \\ * & & \end{pmatrix}$ называются *главной* и *побочной*. Матрицы, под главной диагональю которых стоят нули, называются *верхнетреугольными*. Аналогично бывают и *нижнетреугольные* матрицы.

Задача 4.8. Докажите, что верхнетреугольные матрицы составляют подкольцо в $Mat_n(R)$.

Верхнетреугольная матрица с единицами на главной диагонали называется *верхней унитреугольной*.

Задача 4.9. Проверьте, что произведение любых двух верхних унитреугольных матриц снова будет верхней унитреугольной матрицей.

Задача 4.10. Докажите, что система линейных уравнений, матрица которой — квадратная верхняя унитреугольная, при любом столбце правых частей всегда имеет и притом единственное решение в любом (в том числе и некоммутативном) кольце.

3.6. Алгебраическая запись элементарных преобразований. Вернемся к элементарным преобразованиям строк. Мы собираемся реализовать их как умножения на подходящие *элементарные матрицы*. Чтобы найти эти матрицы мы применим элементарные преобразования к единичной матрице E. Полученные матрицы мы, как и выше, будем относить к трём типам:

(1 тип) получается переменой местами двух строк в матрице E;

(2 тип) получается прибавлением к одной из строк матрицы E какой-либо другой строки, умноженной на λ (или, что то же самое, заменой какого-то одного из нулей, стоящих вне главной диагонали на λ);

(3 тип) получается умножением одной из строк матрицы E на λ (т. е. заменой на λ одной из стоящих на главной диагонали единиц).

3.6.1. Предложение. *При умножении слева на элементарную матрицу произвольная матрица подвергается элементарному преобразованию строк соответствующего типа.*

Задача 4.11. Докажите предложение проделав все необходимые выкладки.

Совет: на самом деле можно считать преобразуемую матрицу состоящей из одного столбца.

3.7. Элементарные преобразования столбцов. Введённые выше три типа элементарных преобразований можно применять не только к строкам, но и к столбцам матрицы. С точки зрения матричного умножения это означает следующее.

3.7.1. Лемма. *Умножение произвольной матрицы $A \in Mat_n(R)$ справа на элементарную матрицу 1-го, 2-го или 3-го типа приводит к соответствующему элементарному преобразованию столбцов этой матрицы.*

Задача 4.12. Проверьте лемму.

3.7.2. Пример: элементарные замены переменного. Если мы осуществляем линейную замену переменных в системе $A(x) = (b)$ при помощи подстановки $(x) = C_{xy}(y)$, то матрица системы уравнений на y будет получаться из исходной матрицы A умножением справа на матрицу перехода. Это немедленно следует из ассоциативности матричного умножения:

$$A(x) = (b) \Longleftrightarrow A(C_{xy}(y)) = (AC_{xy})(y) = (b) .$$

Всякая элементарная матрица U порождает элементарную замену переменного $(x) = U(y)$. В каждом из случаев эти элементарные замены таковы:

$$(1) \qquad x_\nu = \begin{cases} y_j, & \text{при } \nu = i \\ y_i, & \text{при } \nu = j \\ y_\nu, & \text{при } \nu \neq i, j \end{cases} ,$$

$$(2) \qquad x_\nu = \begin{cases} y_i + \lambda y_j, & \text{при } \nu = i \\ y_\nu, & \text{при } \nu \neq i \end{cases} ,$$

$$(3) \qquad x_\nu = \begin{cases} \lambda y_i, & \text{при } \nu = i \\ y_\nu, & \text{при } \nu \neq i \end{cases} .$$

При подстановке $(x) = U(y)$ система уравнений $A(x) = (b)$ на (x) превращается в систему уравнений на (y) вида $B(y) = (b)$, где $B = AU$.

Таким образом при элементарных заменнах переменного матрица системы подвергается соответствующему элементарному преобразованию столбцов.

3.8. Обратная матрица. Теперь мы можем придать точный смысл фразе “разделим обе части равенства на матрицу A”. Заранее отметим, что из-за несимметричности левого и правого сомножителей в произведении нам, вообще говоря, придётся различать “деление слева” и “деление справа”.

3.8.1. Обратимость в некоммутативном кольце. Элемент A (некоммутативного) кольца R называется *обратимым справа*, если $\exists B \in R : \ AB = 1$. Аналогично, A называется *обратимым слева*, если $\exists C \in R : \ CA = 1$.

Если элемент A обратим и слева и справа, скажем $CA = AB = 1$, то левый и правый обратные к A элементы C и B совпадают, ибо

$$C = C \cdot 1 = CAB = 1 \cdot B = B$$

Такие элементы A называются просто *обратимыми*, а (двусторонне) обратный к A элемент обозначается A^{-1}.

ЗАДАЧА 4.13. Докажите, что двусторонне обратный элемент единственен (если существует).

3.8.2. Пример. Элементарные матрицы первого и второго типов обратимы в кольце $Mat_n(R)$ над любым кольцом R. Действительно, обратной (и слева и справа) к элементарной матрице первого типа будет она же сама, а обратной (и слева и справа) к элементарной матрице второго типа будет матрица, отличающаяся от исходной заменой знака у λ.

ЗАДАЧА 4.14. Обязательно убедитесь в этом!

3.8.3. Пример. Элементарная матрица третьего типа обратима в кольце матриц над полем. Обратная матрица получается из исходной заменой λ на λ^{-1}.

3.8.4. Решение системы в терминах матричной алгебры. Если квадратная матрица $A \in Mat_n(R)$ обратима, то система $A(x) = (b)$ (где (x) и (b) – столбцы высоты n, состоящие, соответственно, из неизвестных и правых частей) имеет и притом единственное решение при любом столбце правых частей.

Действительно, если $(x) = (c)$ — решение, то умножая обе части матричного равенства $A(c) = (b)$ слева на A^{-1}, получим $(c) = A^{-1}(b)$, т.е. (c) однозначно восстанавливается по (b).

Наоборот, полагая $(x) = A^{-1}(b)$, мы получим решение системы.

3.9. Отыскание обратной матрицы над полем. Пусть $R = k$ — произвольное поле. Как показывает метод Гаусса, в этом случае квадратная матрица A обратима тогда и только тогда, когда она приводится элементарными преобразованиями к строго ступенчатому виду

$$E = \begin{pmatrix} 1 & & 0 & \\ & 1 & & \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix} .$$

Пусть последовательность элементарных преобразований, превращающая A в E, состоит в умножению A слева на элементарные матрицы $U_1, U_2, \ldots, U_s$. Это записывается равенством

$$U_s \cdot U_{s-1} \cdot \cdots \cdot U_2 \cdot U_1 \cdot A = E \ .$$

Поскольку все U_ν обратимы в $Mat_n(k)$, мы можем умножить обе части этого равенства слева на

$$U_1^{-1} U_2^{-1} \cdots U_s^{-1} \ .$$

Получим, что $A = U_1^{-1} U_2^{-1} \cdots U_s^{-1} \cdot E$, откуда $A^{-1} = U_s U_{s-1} \cdots U_2 U_1$, что можно переписать в виде

$$A^{-1} = U_s U_{s-1} \cdots U_2 U_1 \cdot E$$

и воспринимать как результат воздействия на матрицу E ровно той же последовательности элементарных преобразований строк, которая превращает A в E. Мы получаем

3.9.1. Предложение. *Пусть $A \in \mathrm{Mat}_n(k)$ — произвольная квадратная матрица над полем. Если приписать к ней справа матрицу E и привести полученную $n \times 2n$-матрицу (AE) к строгому ступенчатому виду элементарными преобразованиями срок, то либо в результате получится матрица, содержащая по меньшей мере одну нулевую строку (что равносильно необратимости A), либо — матрица (EA^{-1}).*

§4. Метод Гаусса над евклидовым кольцом

До конца этого параграфа мы будем считать, что R – это *евклидово кольцо* (см. начало лекции 3). Основными примерами, которые читателю рекомендуется держать в голове, являются $R = \mathbb{Z}$ или $R = k[x]$, где k – произвольное поле.

4.1. Обратимые элементарные преробразования. Условимся называть элементарное преобразование *обратимым*, если оно задаётся умножением на обратимую элементарную матрицу. Отметим, что элементарные преобразования первых двух типов обратимы всегда (и над любым кольцом). Элементарное преобразование третьего типа обратимо тогда и только тогда, когда λ — обратимый элемент (т. е. ± 1 для $R = \mathbb{Z}$ и любая ненулевая константа для $R = k[x]$). Мы собираемся выяснить, до какой степени можно упростить прямоугольную матрицу над R при помощи обратимых элементарных преобразований строк и столбцов. Окончательный вид матрицы , к которому мы стремимся, мы будем называть *строгим диагональным*.

4.2. Строгий диагональный вид. Прямоугольную матрицу над R будем называть *диагональный* если она имеет вид

$$D = \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & 0 & \\ & & \ddots & & & \\ & & & d_s & & \\ & 0 & & & 0 & \\ & & & & & \ddots \end{pmatrix},$$

в котором все ненулевые элементы исчерпываются числами $d_1, d_2, \dots, d_s$, расположенными в верхней части главной диагонали[2].

Мы называем диагональную матрицу *строгой диагональной*, если её ненулевые элементы $d_1, d_2, \dots, d_s$ таковы, что каждое d_i делится в R на все предыдущие d_j с $j < i$.

4.3. Теорема. *Любая прямоугольная матрица A с коэффициентами из R обратимыми элементарными преобразованиями строк и столбцов приводится к строго диагональному виду.*

[2]Для прямоугольной неквадратной матрицы A мы понимаем под "главной диагональю" совокупность элементов вида a_{ii} (которая диагональю в строгом смысле и не является, ибо начавшись в левом верхнем углу, кончается где придётся).

Доказательство. Пусть $R \xrightarrow{\lambda} \mathbb{N} \cup 0$ – высота в евклидовом кольце R (т. е. модуль целого числа для $R = \mathbb{Z}$ и степень многочлена для $R = k[x]$). Будем преобразовывать строки и столбцы матрицы A с таким расчётом, чтобы высота элемента, стоящего в левом верхнем углу уменьшалась. Поскольку натуральные числа нельзя уменьшать безгранично, в какой-то момент дальнейшее уменьшение $\lambda(a_{11})$ станет невозможным. Я утверждаю, что в этот момент все элементы матрицы обязаны будут нацело делиться на a_{11}.

Действительно, пусть в первом столбце есть элемент a_{k1}, не делящийся нацело на a_{11}. Деление с остатком даёт $a_{k1} = qa_{11} + r$, где $\lambda(r) < \lambda(a_{11})$. Следовательно, если отнять из k-ой строки первую, умноженную на q, а затем поменять местами первую строку с k-ой, в верхнем левом углу возникнет элемент r, высота которого меньше, чем высота a_{11}.

Меняя в только что проделанном рассуждении строки и столбцы ролями, мы видим, что вся первая строка также делится на a_{11}.

Наконец, пусть элемент a_{ij}, не делящийся на a_{11}, найдется где-либо вне первых строки и столбца. Отнимая из всех строк и всех столбцов подходящие кратные первых строки и столбца, можно добиться того, чтобы первые строка и столбец обнулились вне a_{11}. К элементу a_{ij} при этом прибавится нечто кратное a_{11}, а значит он по прежнему не будет делится на a_{11}. Прибавив в полученной новой матрице к первому столбцу j-ый, я получу матрицу, содержащую a_{ij} в первом столбце, после чего a_{11} можно будет уменьшить так, как это уже было описано выше.

Итак, за конечное число обратимых элементарных преобразований я могу привести матрицу A к виду
$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix},$$
где через B обозначена $(m-1) \times (n-1)$-матрица, все элементы которой нацело делятся на d_1. Далее продолжаем по индукции.

Теорема доказана.

4.3.1. Следствие. *Пусть A - матрица размера $m \times n$ над R. Тогда существуют обратимые над R $m \times m$-матрица U и $n \times n$-матрица V, такие что $D = UAV$ имеет строгий диагональный вид.*

Задача 4.15. Докажите, что эти матрицы U и V можно явно отыскать так: припишем к матрице A справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ соответственно, так чтобы получилась Г-образная таблица вида $\begin{matrix} A & E \\ E & \end{matrix}$; затем элементарными преобразованиями строк и столбцов этой таблицы добьёмся того, чтобы угловой блок A приобрёл строгий диагональный вид D, и в этот момент вся таблица приобретёт вид $\begin{matrix} D & U \\ V & \end{matrix}$ с искомыми U и V.

4.3.2. Следствие. *Всякая система уравнений $A(x) = (b)$ с коэффициентами из R при помощи обратимой линейной замены переменного $(x) = V(y)$ может быть преобразована в* *систему, равносильную системе*

$$\begin{cases} d_1 y_1 & = & c_1 \\ d_2 y_2 & = & c_2 \\ & \dots & \\ d_k y_k & = & c_k \end{cases},$$

в которой каждое d_j делит все последующие d_i с $i > j$.

Эти следствия и задача дают вполне исчерпывающий алгоритм для решения систем линейных уравнений над евклидовыми кольцами.

4.3.3. Замечание. В действительности диагональные элементы $d_1, d_2, \dots, d_s$ с точностью до умножения на обратимые элементы кольца R не зависят от того способа, которым матрица A приводилась к строгому диагональному виду. Мы докажем это в лекции 7, а пока лишь отметим, что элементы d_ν называются *инвариантными множителями* матрицы A, а их количество – *рангом* матрицы A.

Лекция 5
Язык векторов

▷Векторное и аффинное координатные пространства k^n ▷Системы линейных уравнений и подпространства ▷Модули, абелевы группы, векторные пространства ▷Образующие, линейная зависимость, базисы и координаты ▷Свободные модули, гомоморфизмы и соотношенгия ▷Теоремы о базисах конечномерных векторных пространств ▷Замены базисов и матрицы перехода ▷Задание гомоморфизмов матрицами ▷Ранг матрицы

§1. Координатные пространства

1.1. Алгебраизация оснований геометрии. В этой лекции мы рассмотрим алгебраическую структуру, аксиоматизирующую геометрические представления о пространстве. Из школы Вам уже должны быть известны два пути для внедрения алгебры в геометрию: векторы и координаты. Оба дают возможность алгебраически вычислять с линейными геометрическими объектами: точками, прямыми, плоскостями и т. п. Векторы и координаты в школьном курсе обычно возникают на основе уже довольно далеко продвинутой геометрической техники, а их свойства в конечном итоге выводятся из Евклидовых аксиом планиметрии (или стереометрии). С алгебраической точки зрения намного удобнее обратить этот порядок, и с самого начала аксиоматизировать свойства векторов, взяв их за основу для дальнейшего построения геометрии.

В этих лекциях у нас не будет времени для подобного сравнения оснований геометрии по Евклиду и на основе аксиом векторнго пространства[1]. Тем не менее, мы настоятельно рекомендуем читателю следующие две вещи.

Во-первых, всюду далее при слове *вектор* черезвычайно полезно иметь в виду именно самый обычный школьный геометрический вектор, а *векторное пространство* представлять себе как множество "свободных векторов" (которые можно откладывать от любой точки), живущих в обычном школьном геометрическом пространстве.

Во-вторых, алгебраическое построение оснований геометрии позволяет геометризовать

[1]интересующиеся могут прочесть о нём в лекции 33 из книги: *М. М. Постников. Лекции по геометрии. 1-й семестр.* М., "Наука", 1986 (второе, "синее" издание).

многие, на первый взгляд, негеометричные задачи, ибо на языке векторов и координат объяснить, что такое "n-мерная геометрия" или что такое "конечная геометрия над полем из q элементов" ничуть не сложнее, чем объяснить, что такое 3-мерное пространство Евклида.

1.2. Векторное и аффинное координатные пространства. Мы начнём с основного модельного примера, непосредственно обобщающего школьные представления о координатах. Напомню, что если ввести в пространстве систему координат (скажем, декартовых) с центром в некоторой точке O, то каждой точке $P = (p_1, p_2, p_3)$ можно сопоставить радиус-вектор $\overrightarrow{OP}$, задав тем самым биекцию между точками пространства и векторами. При этом каждый вектор $p = \overrightarrow{OP}$ приобретет координаты — декартовы координаты своего конца (p_1, p_2, p_3). Хорошо известно, что действия над векторами легко описываются в терминах этих координат: при сложении векторов их соответственные координаты складываются, а при умножении на число — умножаются на это число. Обобщение этой конструкции напрашивается само собой.

1.3. Определение. *Множество всех матриц-столбцов высоты n с элементами из k вместе с операциями сложения векторов и умножением векторов на числа $\lambda \in k$:*

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \overset{\text{def}}{=} \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \qquad \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \overset{\text{def}}{=} \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

называется координатным векторным пространством над полем k и обозначается k^n. Координатные столбцы $v \in k^n$ называются n-мерными векторами.

1.4. Определение. *То же самое множество всех матриц-столбцов высоты n с элементами из k называется n-мерным аффинным*[2] *координатным пространством $\mathbb{A}_n = \mathbb{A}_n(k)$ (а его элементы — точками) над полем k, если оно рассматривается вместе с операцией откладывания векторов $v \in k^n$ от точек $P \in \mathbb{A}_n$:*

$$+ : \mathbb{A}_n \times k^n \longrightarrow \mathbb{A}_n \ : \quad (P, v) = \left(\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}, \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right) \longmapsto P + v \overset{\text{def}}{=} \begin{pmatrix} p_1 + v_1 \\ p_2 + v_2 \\ \vdots \\ p_n + v_n \end{pmatrix} \in \mathbb{A}_n \quad .$$

Отметим, что хотя точки и векторы обозначаются одинаково (таково уж неприятное свойство координат), разница между ними та же, что и в школьной геометрии: с векторами можно вычислять, а из точек — составлять геометрические фигуры. Если в аффинном пространстве $\mathbb{A}_n$ зафиксировать какую-либо точку O (так называемое *начало отсчёта*), то можно установить взаимно-однозначное соответствие между точками и векторами, сопоставляя каждой

[2] слово "аффинный", как показывает его орфография, не имеет ни малейшего отношения к Греции, а является всего лишь бесхитросной калькой с английского affine – "ассоциированный"

точке $P \in \mathbb{A}_n$ её *радиус-вектор*

$$\overrightarrow{OP} \stackrel{\text{def}}{=} v \in k^n \quad \text{такой что} \quad O + v = P \ .$$

Это соответствие позволяет переводить геометрические построения с языка точек на язык векторов и наоборот.

1.5. Некоторые примеры из аффинной геометрии. Удобно представлять себе n-мерное аффинное пространство $\mathbb{A}_n$ вместе с системой координат с центром в нулевом столбце и координатными осями, каждая из которых напрвленна вдоль соответствующего базисного вектора e_i, у которого все координаты, кроме i-той, нулевые, а i-тая координата равна 1.

Задача 5.1. Сколько координатных "октантов" имеет описанная выше система координат?

Задача 5.2. Рассмотрим единичный стандартный 4-мерный куб в $\mathbb{A}_4(\mathbb{R})$ (натянутый на четыре базисных координатных вектора). Сколько у него:
а) i-мерных граней ($i = 0, 1, 2, 3$);
б) внутренних (т. е. не лежащих на гранях) диагоналей?

При помощи векторов нетрудно определить в $\mathbb{A}_n(k)$ линейные геометрические объекты: прямые, плоскости и т. п. Так *прямая*, проходящая через точку $P \in \mathbb{A}_n$ вдоль вектора $v \in k^n$ есть множество всех точек вида

$$Q(t) = P + tv \ ,$$

где p пробегает k (механическая аналогия: частица, движущаяся с постоянной скоростью v и в начальный момент времени $t = 0$ находящаяся в точке P, в произвольный момент времени t находится в точке $Q(t)$).

Задача 5.3. Докажите, что две прямые либо пересекаются по одной точке, либо совпадают, либо не пересекаются вообще.

Задача 5.4. Пусть $k = \mathbb{Z}/p\mathbb{Z}$ - конечное поле. Сколько всего имеется в $\mathbb{A}_n(k)$:
а) точек;
б) прямых, проходящих через фиксированную точку;
в) всего прямых?
(если общий случай вызывает затруднения, рассмотрите $n = 2.3.4$).

Аналогично, плоскость в $\pi \subset \mathbb{A}_n$ можно определить как множество точек вида

$$Q(s, t) = P + su + tv \ ,$$

где $P \in \pi$ — некоторая фиксированная начальная точка, $u, v \in k^n$ — фиксированная пара не пропорциональные друг другу векторов, параллельных плоскости, а s, t независимо пробегают k (их можно воспринимать как координаты на плоскости π).

Определения прямой и плоскости являются частными случаями более общего понятия *подпространства.*

1.6. Векторные подпространства и однородные линейные уравнения. Подмножество векторов $V \subset k^n$ называется *векторным подпространством*, если оно замкнуто относительно сложения векторов и умножения векторов на числа. Примером векторного подпространства является множество $W = W(v_1, v_2, \ldots, v_m)$, состоящее из всех векторов $w \in k^n$, представимых в виде $w = \sum t_i v_i$, где $(v_1, v_2, \dots, v_n)$ есть фиксированный набор векторов из k^m, а числовые параметры $(t_1, t_2, \dots, t_m)$ независимо пробегают k. Векторы $(v_1, v_2, \dots, v_m)$ в этом случае называются *порождающими* подпространство W. Другой пример приходит из прошлой лекции

1.6.1. Предложение. *Пусть над полем k задана система из s однородных линейных уравнений от n неизвестных:*

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0 \,,$$

где A — матрица размера $n \times s$ над полем k. Тогда множество её решений представляет собой векторное подпространство в k^n.

Доказательство. Действительно, если $a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ и $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ — решения, то

$$\begin{aligned} A \cdot (a+b) &= A \cdot a + A \cdot b = (0) + (0) = (0) \\ A \cdot (\lambda a) &= \lambda A \cdot a = \lambda(0) = (0) \,, \end{aligned}$$

где через (0) обозначен нулевой вектор-столбец. Тем самым $a+b$ и λa — также решения. □

Отметим, что описанный в прошлой лекции способ решения линейных систем над полем при помощи приведения их матрицы к ступенчатому виду доставляет алгоритм для отыскани порождающих векторов в подпространстве, заданном системой однородных линейных уравнений.

1.7. Аффинные подпространства и неоднородные линейные уравнения. Назовём *аффинным подпространством* в $\mathbb{A}_n$ всякое подмножество $\pi(P, W) \subset \mathbb{A}_n$, которое состоит из всех точек вида $P + v$, где $P \in \mathbb{A}_n$ —некоторая фиксированныя точка, а векторы v пробегают некоторое фиксированное векторное подпространство $W \subset k^n$. Говорят также, что $\pi(P, W)$ есть *аффинная (гипер)плоскость*, проходящая через точку P и параллельная подпространству W. Рассматривавшиеся выше прямые и плоскости доставляют примеры аффинных подпространств. Другие примеры вновь приходят из прошлой лекции.

1.7.1. Предложение. *Множество решений неоднородной системы $Ax = b$ из s линейных уравнений с n неизвестными либо пусто, либо является аффинной гиперплоскостью вида $\pi(a, W)$, где $a \in \mathbb{A}_n$ – какое-либо одно решение неоднородной системы, а $W \subset k^n$ есть векторное подпространство решений однородной системы $Ax = (0)$ с той же матрицей A.*

Доказательство. Пусть $a \in \mathbb{A}_n$ — решение системы $Ax = b$. Поскольку равенство $Aa' = b$ равносильно тому, что $a' = a + w$, где $w \in k^n$ удовлетворяет равенству $Aw = Aa' - Aa = b - b = 0$, откладывание векторов $w \in k^n$, являющихся решениями однородной системы $Ax = (0)$, от

точки a задает биекцию между множеством решений системы $Ax = b$ и множеством решений системы $Ax = 0$.
□

Отметим, что описанное в прошлой лекции решение неоднородных систем вновь может восприниматься как переход от неявного задания аффинной гиперплоскости к явному её заданию.

Задача 5.5. Выясните, как устроены сечения 4-мерного куба из зад.5.2 3-мерными плоскостями $x_1 + x_2 + x_3 + x_4 = d$, где $0 \le d \le 4$.

§2. Модули

2.1. Определение модуля. Пусть K – коммутативное кольцо с единицей. *K-модулем* называется всякое множество V (элементы которого называются *векторами*), наделенное бинарной операцией сложения векторов

$$+ : V \times V \longrightarrow V \quad : \qquad (v, w) \longmapsto v + w \in V$$

и операцией умножения векторов на числа из K:

$$\cdot : K \times V \longrightarrow V \quad : \qquad (\lambda, v) \longmapsto \lambda v \in V\ ,$$

так что выполнены аксиомы:

Аксиомы K-модуля

1) Аксиомы сложения векторов

   а) коммутативность: $a + b = b + a \quad \forall a, b \in V$

   б) ассоциативность: $a + (b + c) = (a + b) + c \quad \forall a, b, c \in V$

   в) существование нуля: $\exists 0 \in V :\ a + 0 = a \quad \forall\, a \in k$

   г) существование противоположного: $\forall a \in V \quad \exists (-a) \in V : \quad a + (-a) = 0$

2) Аксиомы умножения векторов на числа

   а) ассоциативность: $\lambda(\mu a) = (\lambda\mu)a \quad \forall\, a \in V\ ,\ \forall\, \lambda, \mu \in K$

   б) дистрибутивность по отношению к сложению чисел:

   $$(\lambda + \mu)a = \lambda a + \mu a \qquad \forall\, a \in V\ ,\ \forall\, \lambda, \mu \in K$$

   в) дистрибутивность по отношению к сложению векторов:

   $$\lambda(a + b) = \lambda a + \lambda b \qquad \forall\, \lambda \in K\ ,\ \forall\, a, b \in K$$

г) умножение на единицу $1 \in K$: $\quad 1 \cdot a = 1 \qquad \forall\, a \in V$.

2.1.1. Частный случай: векторные пространства. Если $K = k$ — поле, то k-модули называются *векторными пространствами* над k, и термин "k-модуль" в этой ситуации практически не употребляется.

Задача 5.6. Проверьте, что координатное пространство k^n удовлетворяет аксиомам векторного пространства.

2.1.2. Частный случай: абелевы группы. Если на множестве A задана бинарная операция сложения

$$+ : A \times A \longrightarrow A \quad : \qquad (a, b) \longmapsto a + b \in A\,,$$

которая удовлетворяет всем четырем аксиома сложения векторов, то A называют *абелевой группой*. Иначе говоря, абелева группа — это векторное пространство, в котором "исключили из рассмотрения" умножение на числа.

Тем не менее, абелевы группы являются частными случаями модулей, а именно, модулями над кольцом $K = \mathbb{Z}$, ибо умножение на *целые* числа есть внутреннее свойство абелевой группы: всегда можно считать по определению, что

$$n \cdot a \overset{\text{def}}{=} \begin{cases} \underbrace{a + a + \cdots + a}_{n}\,, & \text{при} \quad n \geq 0 \\ \underbrace{-a - a - \cdots - a}_{-n}, & \text{при} \quad n < 0 \end{cases} \qquad \forall\, n \in \mathbb{Z}\;,\;\; \forall\, a \in A\;\;.$$

Задача 5.7. Проверьте выполнение аксиом $\mathbb{Z}$-модуля.

Приведённый выше список аксиом, как обычно, можно дополнить несколькими интуитивно ожидаемыми свойствами векторов, формально вытекающими из аксиом:

Задача 5.8. Докажите, что в любой абелевой группе 0 единственен, а противоположный элемент $(-a)$ к элементу a однозначно определяется по a.

Задача 5.9. Докажите, что в любом K-модуле V справедливы равенства:

а) $0 \cdot v = 0 \in V \quad \forall\, v \in V$;

б) $\lambda \cdot 0 = 0 \quad \forall\, \lambda \in K$;

в) $(-1) \cdot v = (-v) \in V \quad \forall\, v \in V$.

2.2. Определение. *Отображение $\varphi : V_1 \longrightarrow V_2$ между двумя K-модулями V_1 и V_2 называется **гомоморфизмом** K-модулей (или K-**линейным отображением**), если оно перестанофочно со сложением векторов и умножением векторов на числа:*

$$\varphi(v + w) = \varphi(v) + \varphi(w) \quad \text{и} \quad \varphi(\lambda v) = \lambda\varphi(v) \quad , \qquad \forall\, \lambda \in K\;,\, \forall\, v, w \in V \quad .$$

*Гомоморфизм модулей $V \xrightarrow{\varphi} W$ называется **мзоморфизмом**, если он обратим, т. е. существует гомоморфизм модулей $W \xrightarrow{\psi} V$, такой, что $\psi\varphi$ и $\varphi\psi$ – тождественные отображения. Эпиморфизмы и мономорфизмы — это гомоморфизмы, которые на уровне множеств являются отображениями "на" и "в" соответственно.*

Задача 5.10. Докажите, что для любой гомоморфизма K-модулей $V \xrightarrow{\varphi} W$ обладает следующими свойствами:

а) $\varphi(0) = 0$ б) $\varphi(-w) = -\varphi(w)$ в) $\varphi(v - w) = \varphi(v) - \varphi(w)$.

Как и для гомоморфизма колец, подмножества

$$\ker(\varphi) = \{ v \in V \mid \varphi(v) = 0 \} \quad \text{и} \quad \mathrm{im}\,(\varphi) = \{ w \in W \mid \exists v \in V : \varphi(v) = w \}$$

называются, соответственно, *ядром* и *образом* гомоморфизма $V \xrightarrow{\varphi} W$. В этих терминах эпиморфность φ означает равенство $\mathrm{im}\,\varphi = W$, а критерием мономорфности является

2.2.1. Предложение. $\ker(\varphi) = \{0\}$ *тогда и только тогда, когда* $V \xrightarrow{\varphi} W$ *— мономорфизм.*

Доказательство. Равенство $\varphi(v_1) = f(v_2)$ равносильно тому, что $v_1 - v_2 \in \ker\varphi$, ибо $\varphi(v_1 - v_2) = \varphi(v_1) - f(v_2)$.
□

2.2.2. Предложение. *Если* $V \xrightarrow{\varphi} W$ *– гомоморфизм модулей, то* $\ker(\varphi)$ *является подмодулем в* V, *а* $\mathrm{im}\,(\varphi)$ *– подмодулем в* W.

Доказательство. Чтобы проверить, что подмножество M является подмодулем в модуле V, достаточно проверить, что $\forall\, \lambda, \mu \in K$ и $\forall\, u, v \in K$ комбинация $\lambda u + \mu v$ также лежит в M. Если $\varphi(u) = \varphi(v) = 0$, то $\varphi(\lambda u + \mu v) = \lambda\varphi(u) + \mu\varphi(v) = 0$. Если $w_1 = \varphi(v_1)$ и $w_2 = \varphi(v_2)$, то $\lambda w_1 + \mu w_2 = \lambda\varphi(v_1) + \mu\varphi(v_2) = \varphi(\lambda v_1 + \mu v_2)$.
□

2.3. Примеры векторных пространств и модулей. Как мы уже видели в зад.5.6, примером векторного пространства является координатное векторное пространство из предыдущего параграфа. Рассмотрим некоторые другие примеры.

2.3.1. Многочлены. Ясно, что $K[x]$ является K-модуль. Все многочлены, степень которых не превосходит некоторого фиксированного числа, также образуют K-модуль[3], который уже не является кольцом. Мы далее будем обозначать этот модуль через $P_n = P_n(K)$.

Задача 5.11. Постройте изоморфизм пространства многочленов степенеи не выше n с коэффициентами из поля k с координатным пространством $k^{(n+1)}$.

Отображение $k[x] \xrightarrow{d/dx} k[x]$ (k – поле), сопоставляющее каждому многочлену его производную, является K-линейным эндоморфизмом пространства многочленов[4]. Если $\mathit{char}\,(k) = 0$, то его образ совпадает со всем пространством (почему?), а ядро есть пространство многочленов степени нуль (почему?).

Задача 5.12. Опишите $\ker(d/dx)$ и $\mathrm{im}\,(d/dx)$, если $\mathit{char}\,(k) = p \neq 0$.

Пусть $f(x) \in k[x]$ — некий многочлен степени n. Отображение res_f, сопоставляющее каждому многочлену $g(x) \in k[x]$ его остаток от деления на f, является гомоморфизмом k-модулей, отображающим $k[x]$ на пространство P_{n-1} многочленов степени не выше, чем $(n-1)$. Этот гомоморфизм сюръективен, а его ядро совпадает с идеалом $(f) \in k[x]$.

[3]отметим, что множество всех многочленов строго фиксированной степени не является K-модулем

[4]аналогично, интегрирование, переход к пределу и т. д. также являются линейными отображениями в соответствующих пространствах функций

Задача 5.13. Убедитесь, что отображение $\varphi\colon\ k[x]/(f)\longrightarrow P_{n-1}$, переводящее класс $g(\bmod f)$ в $res_f(g)$ корректно определено и является изоморфизмом векторных пространств.

2.3.2. Расширения полей. Если $k\subset K$ — расширение полей, то поле K часто бывает удобно рассматривать как векторное пространство над k. Если $K=k[\vartheta]$ – алгебраическое расширение при помощи элемента ϑ, удовлетворяющего минимальному уравнению

$$Q(\vartheta)=\vartheta^n+q_1\vartheta^{n-1}+\cdots+q_{n-1}\vartheta+q_n=0$$

степени n с коэффициентами из k, то K как векторное пространство над k, изоморфно координатному пространству k^n. В самом деле, во лекции 3 мы видели, что элементы поля K однозначно записываются многочленами от ϑ степени $\leq(n-1)$, причём такое представление согласовано со сложением и умножением на числа из k. Сопоставляя многочлену столбец его коэффициентов, мы и получим изоморфизм между K и k^n. В частности, если поле k — конечное поле из q элементов, то поле K будет полем из q^n элементов.

Задача 5.14. Докажите, что число элементов в любом конечном поле является степенью простого числа.

Указание: представьте конечное поле как расширение простого подполя при помощи одного алгебраического элемента, или дождитесь Пр.3.7.1

Если K является конечным алгебратческим расширениям поля $\mathbb{Q}$, то его можно воспринимать как полноценное геометрическое пространство, в котором можно заниматься "настоящей" наглядной геометрией, что позволяет элегантно доказывать трудные арифметические теоремы и вылилось в настоящее время в целую науку, именуемую *геометрией чисел*.

2.3.3. Модули и идеалы. Если отвлечься от геометрии, то с алгебраической точки зрения модуль есть обобщение идеала. Действительно, сопоставление определений показывает, что подмножество $I\subset K$ тогда и только тогда является K-подмодулем, когда I — это идеал в K. В лекциях 2,3 мы задавали идеалы *образующими*, т. е. представляли их в виде

$$I=(a_1,a_2,\dots,a_m)=a_1K+a_2K+\cdots a_mK\ .$$

Модули тоже удобно задавать образующими (или *порождающими*) элементами (ср. с n° 1.6).

§3. Образующие, базисы и линейная зависимость.

3.1. Образующие. Про (возможно бесконечный) набор векторов $\{v_i\}$ K-модуля V говорят, что он *порождает* V, если каждый вектор $v\in V$ можно представить в виде *конечной линейной комбинации* векторов v_i с коэффициентами из K, т. е. записать в виде:

$$v=x_1e_1+x_2e_2+\cdots+x_ne_n\qquad\text{с}\quad x_i\in K\ . \tag{5-1}$$

Векторы v_i в этом случае называются *образующими* модуля V над K.

Модуль называется *конечно порожденным*, если он допускает конечное множество образующих.

3.2. Базисы и координаты. Набор векторов $\{e_i\} \subset V$ (возможно бесконечный) называется *базисом*, если он порождает V и для любого $v \in V$ существует *ровно одно* разложение (5-1): $v = \sum x_i e_i$, т. е. из равенства

$$\sum x_i e_i = \sum y_i e_i$$

вытекает, что $x_i = y_i \ \forall i$. При этом коэффициенты x_i разложения $v = \sum x_i e_i$ называются *координатами* вектора v в базисе e_i. Модули, обладающие базисом, называются *свободными*.

3.3. Линейная зависимость. Набор векторов $\{v_i\}$ в K-модуле V называется *линейно-независимым*, если из того, что конечная линейная комбинация $\sum \lambda_i v_i$ векторов из этого набора равна нулевому вектору, вытекает, что все коэффициенты λ_i — нулевые.

Напротив, если для некоторых x_i, среди которых есть ненулевые, выполнено равенство $\sum x_i v_i = 0$, то набор $\{v_i\}$ называется *линейно-зависимым*, а само это соотношение называется *линейной зависимостью*.

3.3.1. Предложение. *Порождающий набор векторов тогда и только тогда является базисом, когда он линейно независим.*

Доказательство. Если $\sum \lambda_i e_i = 0$ и не все λ_i нулевые, то всякий вектор $v = \sum x_i e_i$ можно *иначе* разложить в виде $v = \sum (x_i + \lambda_i) e_i$.

Наоборот, если $v = \sum x_i e_i = \sum y_i e_i$ — два различных представления одного вектора, то перенося праую часть в середину, получаем линейную зависимость $\sum (x_i - y_i) v_i = 0$.
□

3.4. Кручение. Разумеется, неверно, что любой модуль свободен. Простейшим[5] препятствием к свободе является кручение. Элемент v K-модуля V называется *элементом кручения*, если $v \neq 0$ и набор $\{v\}$, состоящий из одного этого вектора, линейно зависим, т. е. $\lambda v = 0$ для некоторого ненулевого $\lambda \in K$.

Если $I \subset K$ – идеал в K, то элементы кручения в K-модуле I — это в точности делители нуля в I. Но даже если K — это целостное кольцо, K-модули, не являющиеся идеалами, вполне могут иметь кручение.

Например, множество вычетов $\mathbb{Z}/n\mathbb{Z}$ с операцией сложения является абелевой группой, а стало быть, $\mathbb{Z}$-модулем. Более того, он может быть порождён над $\mathbb{Z}$ одним элементом.

> Задача 5.15. Докажите, что если m взаимно просто с n, то класс $v(\bmod n)$ порождает $\mathbb{Z}$-модуль $\mathbb{Z}/n\mathbb{Z}$.

Вместе с тем, все элементы в $\mathbb{Z}/n\mathbb{Z}$ являются элементами кручения, ибо $\forall\, a \in \mathbb{Z}\ /n\mathbb{Z}$, класс $na(\bmod n)$ равен нулю в $\mathbb{Z}/n\mathbb{Z}$, хотя $n \neq 0$ в $\mathbb{Z}$. Поэтому любой набор векторов из $\mathbb{Z}/n\mathbb{Z}$ линейно зависим, и значит, в этом модуле нет базиса.

> Задача 5.16. Докажите, что все элементы кручения вместе с нулевым вектором составляют подмодуль в любом K-модуле V над произвольным коммутативным кольцом K (он обозначается $Tors(V)$ и называется *подмодулем кручения*)

3.5. Конечно порождённые свободные модули. Координатный модуль K^n определяется для произвольного коммутативного кольца K дословно также, как и координатное пространство k^n. Отметим, что как множество он совпадает с n-кратной прямой суммой кольца

[5] но, конечно, не единственным

K самого с собой, но мы забываем часть мультипликативной структуры, принимая во внимание лишь умножение на диагональные элементы $(\lambda, \lambda, \ldots, \lambda) \subset K^{\oplus n}$.

Если V — конечно порождённый свободный K-модуль с базисом $(e_1, e_2, \ldots, e_n)$, то сопоставляя произвольному вектору $v \in V$ столбец из его координат в этом базисе, мы получим изоморфизм V с K^n.

Задача 5.17. Убедитесь в этом.

Наоборот, фиксация некоторого изоморфизма $\kappa\colon\ V \longrightarrow K^n$ равносильна выбору базиса в V — в качестве базисных можно взять прообразы стандартных базисных векторов из K^n.

Задача 5.18. Убедитесь, что эти прообразы действительно образуют базис.

Таким образом, изоморфизмы $V \xrightarrow{\sim} K^n$ биективно соответствуют базисам из n векторов в V. В следующей лекции мы докажем[6], что модули K^n и K^m неизоморфны при $n \neq m$. Поэтому число векторов во всех базисах произвольного свободного модуля V одно и то же. Оно называется *рангом* свободного модуля и обозначается $\operatorname{rk} V$.

Задача 5.19. Докажите, что многочлены степени $\le n$ с коэффициентами из произвольного коммутативного кольца K составляют свободный K-модуль ранга $(n+1)$.

3.6. Гомоморфизмы и соотношения. Пусть $\varphi\colon\ V \longrightarrow W$ — гомоморфизм модулей, и модуль V порождается (возможно бесконечным) набором образующих $\{e_i\}$. Тогда φ однозначно восстанавливается по их образам $\varphi(e_i) \in W$. Действительно, разложив произвольный вектор $v \in V$ по e_i: $v = \sum x_i e_i$, мы получаем

$$f(v) = \sum x_i \varphi(e_i)\ .$$

Наоборот, произвольным образом выбрав векторы $w_i \in W$, можно попытаться задать гоморфизм $V \xrightarrow{\varphi} W$, полагая $\varphi(e_i) = w_i$ и распространяя его на произвольные $v \in V$ при помощи предыдущей формулы (это называется *продолжением по линейности* теоретико-множественного отображения $e_i \longmapsto w_i$). Однако, такое задание гоморфизма может оказаться некорректным, поскольку вектор v может иметь несколько разных выражений через образующие.

Рассмотрим, например, $\mathbb{Z}$-модули $V = \mathbb{Z}/n\mathbb{Z}$ и $W = \mathbb{Z}$. Тогда V порождается одним элементом $[1] = 1(\bmod n)$, и поланая $f([1]) = k \in \mathbb{Z}$, мы получим гомоморфизм лишь в единственном случае: при $k = 0$. Действительно, в $\mathbb{Z}/n\mathbb{Z}$ выполнено соотношение $n[1] = [0]$, и если φ – гомоморфизм, то в $\mathbb{Z}$ должно выполняться соотношение:

$$n\varphi([1]) = \varphi(n[1]) = \varphi(0) = 0\ ,$$

откуда $f([1]) = 0$, ибо $\mathbb{Z}$ – целостное кольцо.

3.6.1. Предложение. *Для того чтобы отображение $e_i \longmapsto w_i$, $w_i \in W$, можно было продолжить по линейности до гомоморфизма модуля, порождённого векторами e_i, в модуль W, необходимо и достаточно, чтобы всякая конечная линейная зависимость*

$$\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n = 0$$

[6] для векторных пространств мы сделаем это уже в Сл.3.7.5

между векторами e_i в V влекла бы точно такую же зависимость

$$\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_n w_n = 0$$

между векторами w_i в W.

Доказательство. В одну сторону утверждение следует непосредственно из определения гомомрфизма: если φ – гомоморфизм, то

$$\sum \lambda_i w_i = \sum \lambda_i \varphi(e_i) = \varphi(\sum \lambda_i e_i) = \varphi(0) = 0 \ ,$$

как только $\sum \lambda_i e_i = 0$.

Наоборот, проверим, что продолжение по линейности корректно, если только все соотношения между e_i выполнены и между w_i. Пусть

$$v = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n = y_1 e_1 + y_2 e_2 + \cdots + y_n e_n$$

два разных разложения. Тогда $\sum (x_i - y_i) e_i = 0$, и по предположению, $\sum (x_i - y_i) w_i = 0$. Но тогда и

$$x_1 w_1 + x_2 w_2 + \cdots + x_n w_n = y_1 w_1 + y_2 w_2 + \cdots + y_n w_n$$

в W, и стало быть $\varphi(v)$ не зависит от того, каким из разложений пользоваться.
□

> Задача 5.20. Если модуль W не имеет кручения, то всякий гомоморфизм $V \xrightarrow{\varphi} W$ переводит все элементы кручения из V в нуль.

3.6.2. Следствие. *Модуль V тогда и только тогда является свободным с (возможно, бесконечным) базисом $E = \{e_i\}$, когда всякое теоретико-множественное отображение $E \longrightarrow W$ из множества базисных векторов в произвольный модуль W может быть единственным способом продолжено до гомомрфизма $V \longrightarrow W$.*

Доказательство. То, что любое теоретико-множественное отображение базиса свободного модуля в произвольный модуль можно единственным способом продолжить до гомомрфизма модулей, вытекает непосредственно из предыдущего предложения.

Наоборот, пусть некий набор векторов $\{e_1, e_2, \dots, e_n\}$ некого модуля V обладает указанным в следствии свойством. Возьмём в качестве W свободный модуль с n образующими $(w_1, w_2, \dots, w_n)$ и отобразим биективно e_i на w_i. Тогда это отображение продолжается до гомоморфизма модулей $V \xrightarrow{\varphi} W$. Этот гомоморфизм является изоморфизмом, ибо у него есть обратный — гомоморфизм $W \xrightarrow{\psi} V$, который продолжает по линейности отображение $w_i \longmapsto e_i$ (он существует по предыдущему абзацу). В самом деле, композиция $V \xrightarrow{\psi\varphi} V$ есть гомоморфизм, который продолжает тождественное отображение из e_i в себя, а стало быть, совпадает с тождественным отображением (вследствие единственности продолжения). Аналогично, композиция $W \xrightarrow{\varphi\psi} W$ будет тождественным отображением из W в W.
□

3.7. Конечномерные векторные пространства. Всюду в этом пункте мы будем считать, что k — произвольное поле. Конечно порождённые векторные пространства над k называются *конечномерными*. Теория конечномерных векторных пространств много проще, чем теория произвольных модулей, поскольку в ней не возникает никаких неприятностей, связанных с несвободой и неоднозначностью разложения в линейные комбинации.

Задача 5.21. Пусть k – поле. Докажите, что любой набор многочленов $f_i(x) \in k[x]$, $i = 0, 1, 2, \ldots, n$, таких что $\deg(f_i)$ равна в точности i, составляет базис в пространстве всех многочленов степени $\le n$ над k.

3.7.1. Предложение. *Всякое конечномерное векторное пространство обладает базисом, причём этот базис можно получить из любой наперёд заданной системы образующих удаляя из из неё (если надо) некоторые векторы*[7].

Доказательство. Пусть V – векторное пространство над полем k, порождённое конечным набором векторов $(e_1, e_2, \ldots, e_n)$. Из всех таких наборов мы выберем набор, состоящий из наименьшего возможного количества векторов. Покажем, что он линейно-независим. Действительно, пусть $\sum \lambda_i e_i = 0$, и скажем, $\lambda_n \ne 0$. Тогда

$$e_n = -\sum_{i=1}^{n-1} \frac{\lambda_i}{\lambda_n} e_i$$

линейно выражается через первые $(n-1)$ векторов, и подставляя это выражение в разложение произвольного вектора $v \in V$ через e_i, мы видим, что V в действительности порождается первыми $(n-1)$ векторами нашей системы вопреки предположению.

□

3.7.2. Следствие. *Всякое конечномерное векторное пространство над полем k изоморфно некоторому координатному векторному пространству k^n.*

□

3.7.3. Предложение. *Всякий пабор $(v_1, v_2, \ldots, v_m)$ из $m > n$ векторов в k^n линейно-зависим.*

Доказательство. Пусть A — это матрица, составленная из вектор-столбцов v_i. Подобрать ненулевой набор констант x_i, дающих линейную зависимость

$$x_1 v_1 + x_2 v_2 + \cdots + x_m v_m = 0$$

это то же самое, что найти ненулевое решение системы однородных линейных уравнений

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Как мы видели в прошлой лекции, в нашем случае, когда уравнений меньше, чем неизвестных, ненулевое решение всегда существует.

□

[7] машинерия “трансфинитной” теории множеств (теорема Цермело или лемма Цорна) позволяет распространить приводимое ниже доказательство и на случай пространств, порождённых бесконечными семействами образующих, так что предложение сохраняет силу для любых векторных пространств

3.7.4. Следствие. *Векторные пространства k^m и k^n изоморфны тогда и только тогда, когда $m = n$.*

□

3.7.5. Следствие. *Все базисы конечномерного векторного пространства V состоят из одного и того же числа векторов (это число называется **размерностью** V и обозначается $\dim V$).*

□

3.7.6. Следствие. *Всякий линейно независимый набор векторов может быть дополнен до базиса.*

Доказательство. Точно также, как и в доказательстве Пр.3.7.1, легко увидеть, что если вектор v не выражается через линейно-независимый набор векторов $(v_1, v_2, \dots, v_m)$, то набор $(v,\ v_1, v_2, \dots, v_m\ )$ также будет линейно-независим. Добавляя таким образом к набору новые векторы мы в конце концов получим базис, ибо число векторов в линейно-независимом наборе не может превысить $\dim V$.

□

3.7.7. Предложение. *Пусть $V \xrightarrow{\varphi} W$ — гомоморфизм конечномерных векторных пространств. Тогда в V и W можно так выбрать базисы $(v_1, v_2, \dots, v_n)$ и $(w_1, w_2, \dots, w_m)$, что*

$$f(e_i) = \begin{cases} w_i\ , & \text{при} \quad 1 \le i \le r \\ 0\ , & \text{при} \quad r < i \le m \end{cases} \quad ,$$

причём число $r = \dim(\operatorname{im}\varphi) = \dim(V) - \dim(\ker\varphi)$ не зависит от выбора базисов.

Доказательство. Выберем базис в $\ker\varphi \subset V$, обозначим его через $(v_{r+1}, \dots, v_n)$ (это определение числа r), и дополним его до базиса $(v_1, v_2, \dots, v_n)$ в V. Векторы

$$\varphi(v_1), \varphi(v_2), \dots, \varphi(v_r)$$

порождают $\operatorname{im}\varphi$ (ибо остальные базисные векторы V переходят в нуль) и линейно независимы, поскольку из равенства

$$0 = \sum_{i=1}^{r} \lambda_i \varphi(v_i) = \varphi\left(\sum_{i=1}^{r} \lambda_i v_i\right)$$

вытекает равенство $\sum\limits_{i=1}^{r} \lambda_i v_i \in \ker\varphi$, означающее, что эта сумма линейно выражается через векторы $v_{r+1}, \dots, v_n$, что из-за единственности разложения по базису возможно лишь при $\sum\limits_{i=1}^{r} \lambda_i v_i = 0$, т. е. только если все $\lambda_i - 0$. Тем самым, векторы $w_i \stackrel{\text{def}}{=} \varphi(v_i)$ с $1 \le i \le r$ составляют базис в $\operatorname{im}\varphi$. Дополняя этот базис до базиса$(w_1, w_2, \dots, w_m)$ в W получаем утверждение предложения.

□

§4. Матричный формализм

4.1. Векторы как матрицы. Условимся записывать наборы векторов матрицами-строками, элементами которых служат эти векторы, а наборы чисел[8] — матрицами-столбцами, составленными из этих чисел. Договоримся также, что векторы можно умножать на числа и справа и слева, полагая по определению $v \cdot \lambda \stackrel{\text{def}}{=} \lambda v$.

В этих соглашениях равенство $v = \sum\limits_{i=1}^{n} x_i v_i$ можно интерпретировать как матричное равенство

$$(v) = (v_1, v_2, \ldots, v_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} ,$$

где (v) есть 1×1-матрица с единственным элементом v.

4.2. Матрицы перехода. Пусть $(v_1, v_2, \ldots, v_s)$ — какой-либо набор векторов K-модуля V, порождённого векторами $(e_1, e_2, \ldots, e_n)$. Матрицу размера $n \times s$, по столбцам которой стоят коэффициенты разложений векторов v_i по образующим e_i, мы будем называть *матрицей перехода от v_i к e_i* и обозначать C_{ev}. Отметим, что это обозначение не вполне корректно, ибо если e_i линейно-зависимы, то можно написать много разных матриц перехода. Тем не менее, любая из них, по определению, удовлетворяет матричному равенству

$$(v_1, v_2, \ldots, v_s) = (e_1, e_2, \ldots, e_n) C_{ev} .$$

Если набор $(v_1, v_2, \ldots, v_s)$ также порождает V, то наряду с матрицей C_{ev} можно рассматривать матрицу перехода C_{ve} от e_i к v_i, по столбцам которой стоят коэффициенты разложений векторов e_i через образующие v_i. Возникает равенство

$$(e_1, e_2, \ldots, e_n) = (v_1, v_2, \ldots, v_s) C_{ve} = (e_1, e_2, \ldots, e_n) C_{ev} C_{ve} ,$$

которое означет, что произведение $C_{ev}C_{ve}$ является матрицей перехода C_{ee} набора e_i к самому же набору e_i, т. е. имеет в качестве столбцов коэффициенты разложения векторов e_i по самим себе.

Допустим теперь, что набор векторов e_i составляет *базис* в V. Тогда разложение каждого e_i по этому базису единственно: $e_i = e_i$, и матрица C_{ee} — это единичная матрица E размера $n \times n$. Таким образом, для любого базиса $(e_1, e_2, \ldots, e_n)$ и любого набора векторов $(v_1, v_2, \ldots, v_s)$, порождающего V, мы имеем соотношение

$$C_{ev} C_{ve} = E .$$

4.2.1. Предложение. *Пусть набор векторов $(e_1, e_2, \ldots, e_n)$ является базисом свободного модуля V над коммутативным кольцом K. Другой набор из n векторов $(v_1, v_2, \ldots, v_n)$ тогда*

[8] обычно это будут координаты или коэффициенты разложения по образующим

и только тогда является базисом V, когда матрица перехода C_{ev} обратима в $Mat_n(K)$. При этом противоположный переход будет задаваться обратной матрицей $C_{ve} = C_{ev}^{-1}$.

Доказательство. В одну сторону мы всё уже доказали: если $(v_1, v_2, \ldots, v_n)$ — базис в V, то как мы видели выше, матрицы перехода обязяны удовлетворять соотношениям $C_{ev}C_{ve} = C_{ve}C_{ev} = E$, где E — единичная матрица размера $n \times n$.

Докажем противоположную имликацию. Пусть C_{ev} обратима в $Mat_n(K)$. Тогда из равенства $(v_1, v_2, \ldots, v_n) = (e_1, e_2, \ldots, e_n)C_{ev}$ вытекает, что $(e_1, e_2, \ldots, e_n) = (v_1, v_2, \ldots, v_n)C_{ev}^{-1}$. Покажем, что v_i порождают V. Всякий вектор $v \in V$ имеет разложение вида

$$v = \sum x_i e_i = (e_1, e_2, \ldots, e_n)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (v_1, v_2, \ldots, v_n)C_{ev}^{-1}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} ,$$

которое показывает, что $v = \sum y_i v_i$, где $\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = C_{ev}^{-1}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Остаётся проверить, что набор $(v_1, v_2, \ldots, v_n)$ линейно-независим. Пусть

$$\sum \lambda_i v_i = (v_1, v_2, \ldots, v_n)\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = 0 .$$

Подставляя $(v_1, v_2, \ldots, v_n) = (e_1, e_2, \ldots, e_n)C_{ev}$, получим $\sum \mu_i e_i = 0$, где $\begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{pmatrix} = C_{ev}\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$.

Поскольку e_i линейно-независимы, левый столбец последнего равенства должен быть нулевым. Умножая обе части на C_{ev}^{-1} получаем, что и столбец из λ_i тоже нулевой. Итак, v_i – это тоже базис в V.

□

Отметим, что из доказательства леммы вытекает следующее правило для пересчёта координат:

4.2.2. Следствие. *Если $(e_1, e_2, \ldots, e_n)$ и $(v_1, v_2, \ldots, v_n)$ — два базиса в свободном модуле V и x_i^e и x_i^v — координаты одного и того же вектора $w \in V$ в этих базисах, то*

$$\begin{pmatrix} x_1^e \\ x_2^e \\ \vdots \\ x_n^e \end{pmatrix} = C_{ev}\begin{pmatrix} x_1^v \\ x_2^v \\ \vdots \\ x_n^v \end{pmatrix} .$$

□

4.3. Матрицы гомоморфизмов. Пусть $V = K^n$, $W = K^m$ — свободные модули, и A — некая матрица размера $m \times n$ с элементами из K. Гомоморфизм

$$\mu_A \colon K^n \longrightarrow K^m \quad : \qquad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \longmapsto A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^m$$

называется *гомоморфизмом умножения на матрицу A*

Задача 5.22. Проверьте, что μ_A есть гомоморфизмом K-модулей.

4.3.1. Предложение. *Всякий гомоморфизм модулей $K^n \xrightarrow{\varphi} K^m$ является гомоморфизмом умножения на матрицу, которая однозначно определяется по φ и называется матрицей гомоморфизма φ.*

Доказательство. Пусть $e_i \in K^n$ — стандартные базисные векторы. Обозначим через Φ матрицу размера $m \times n$, столбцы которой суть вектор-столбцы $\varphi(e_i) \in K^m$. Тогда φ и μ_Φ одинаково действут на базис e_i свободного модуля K^n, и согласно Сл.3.6.2, $\varphi = \mu_\Phi$.
□

Для произвольных свободных модулей V и W выбор в V базиса $(v_1, v_2, \ldots, v_n)$, а в W – базиса $(w_1, w_2, \ldots, w_m)$ позволяет записать любой гомоморфизм $V \xrightarrow{\varphi} W$ в виде умножения на $m \times n$-матрицу $\Phi = \Phi_{wv}$, по столбцам которой стоят координаты векторов $\varphi(e_i)$ в базисе w_i. Эта матрица называется *матрицей*[9] *φ в базисах v_i и w_i.*

4.3.2. Следствие. *Пусть V и W — свободные модули с базисами v_i и w_i, и $V \xrightarrow{\varphi} W$ — гомоморфизм модулей с матрицей Φ_{wv}. Тогда вектор с координатами переходит в вектор с координатами x_i^w, вычисляемыми по формуле*

$$\begin{pmatrix} x_1^w \\ x_2^w \\ \vdots \\ x_m^w \end{pmatrix} = \Phi_{wv} \begin{pmatrix} x_1^v \\ x_2^v \\ \vdots \\ x_n^v \end{pmatrix} .$$

□

В случае, когда $W = V$, т. е. $V \xrightarrow{\varphi} V$ – эндоморфизм свободного модуля V, достаточно выбрать один базис $(e_1, e_2, \ldots, e_n)$ в V и рассматривать его и как базис в образе и как базис в прообразе. Соответствующая матрица Φ_{ee} обозначается просто Φ_e и называется матрицей φ в базисе e.

Задача 5.23. Пусть k – поле, и $q(x) \in k[x]$ — произвольный многочлен. Убедитесь, что фактор-кольцо $k[x]/(q)$ имеет естественную структуру конечномерного векторного пространства над k размерности $\sum \deg q_i$, постройте какой-либо базис в нём и напишите матрицу оператора умножения на класс $x \bmod q$ в этом базисе.

[9]здесь и всюду далее мы будем обозначать гомоморфизмы модулей маленькими греческими буквами, а их матрицы – соответствующими большими буквами

Задача 5.24. Пусть в условиях предыдущей задачи $k = \mathbb{C}$ и $q(x) = (x - \lambda)^n$, где $\lambda \in \mathbb{C}$. Постройте в $k[x]/(q)$ базис, в котором матрица оператора умножения на класс $x \bmod q$ имеет вид $\begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}$.

4.3.3. Изменение матрицы гомоморфизма при замене базисов. Разумеется, матрица Φ_{wv} гомоморфизма $V \xrightarrow{\varphi} W$ зависит от выбора базисов. Если выбрать другие базисы

$$(v'_1, v'_2, \dots, v'_n) = (e_1, e_2, \dots, e_n)C_{ee'} \qquad \text{и} \qquad (w'_1, w'_2, \dots, w'_m) = (w_1, w_2, \dots, w_m)C_{ww'}\,,$$

то матрица $\Phi_{w'v'}$ гомоморфизма φ в этих новых базисах определяется соотношением

$$(f(v'_1), f(v'_2), \dots, f(v'_n)) = (w'_1, w'_2, \dots, w'_n)\Phi_{w'v'}\,.$$

С другой стороны, имеем:

$$\begin{aligned} (f(v'_1), f(v'_2), \dots, f(v'_n)) &= (f(v_1), f(v_2), \dots, f(v_n))C_{vv'} = \\ &= (w_1, w_2, \dots, w_m)\Phi_{wv}C_{vv'} = \\ &= (w'_1, w'_2, \dots, w'_m)C_{w'w}\Phi_{wv}C_{vv'}\,, \end{aligned}$$

откуда $\Phi_{w'v'} = C_{w'w}\Phi_{wv}C_{vv'} = C_{ww'}^{-1}\Phi_{wv}C_{vv'}$.

4.3.4. Пример: элементарные преобразования. Если $m \times n$ матрица A рассматривается как матрица $A = \Phi_{wv}$ гомоморфизма $V \xrightarrow{\varphi} W$ между свободными модулями, то элементарные преобразования матрицы A, скоторыми мы имели дело в прошлой лекции, можно интерпретировать как элементарные замены базисов в V и W.

Задача 5.25. Убедитесь, что элементарные преобразования строк 1-го, 2-го и 3-го типа индуцированы следующими заменами базиса $(w_1, w_2, \dots, w_m)$ модуля W: перестановкой пары векторов w_i, w_j, заменой w_j на $w_j - \lambda w_i$ и умножением w_i на обратимый элемент кольца K. Убедитесь также, что элементарным преобразованиям столбцов отвечают аналогичные замены базисных векторов в V.

В частности, Пр.3.7.7 можно получить как следствие теоремы о том, что всякую матрицу над полем можно одновременными элементарными преобразованиями строк и столбцов привести к диагональному виду

$$D = \underbrace{\begin{pmatrix} 1 & & & & & \\ & 1 & & 0 & & \\ & & \ddots & & & \\ & & & 1 & & \\ & 0 & & & 0 & \\ & & & & & \ddots \end{pmatrix}}_{n} \Bigg\} m\,.$$

Действительно, пусть в некоторых базисах v_i и w_i гомоморфизм φ имеет матрицу Φ. В прошлой лекции мы построили обратимые матрицы B и C (возникавшие как произведения элементарных матриц), такие что $B\Phi C = D$. Тогда в базисах

$$(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n)C \quad \text{и} \quad (w_1, w_2, \dots, w_m) = (e_1, e_2, \dots, e_m)B^{-1}$$

(где e_i — стандартные координатные базисные векторы) гомомрфизм φ будет задаваться матрицей D, что и требуется в Пр.3.7.7.

4.4. Ранг матрицы над полем. Размерность образа оператора $k^n \xrightarrow{\mu_A} k^m$ умножения на матрицу A называется *рангом* этой матрицы и обозначается $\operatorname{rk} A$.

4.5. Теорема. (Теорема о ранге матрицы.) *Пусть A — прямоугольная матрица размера из m строк и n столбцов с элементами из поля k. Тогда следующие числа совпадают:*

(i) $\operatorname{rk} A$;

(ii) размерность подпространства, порождённого в k^m столбцами A;

(iii) размерность подпространства, порождённого в k^n строками A;

(iv) число ненулевых строк после приведения матрицы A к строгому ступенчатому виду элементарными преобразованиями строк:

(v) число диагональных единиц после приведения матрицы A к диагональному виду элементарными преобразованиями строк и столбцов

(в частности, последние два числа не зависят от способа приведения).

Доказательство. Образ гомоморфизма умножения на матрицу A порождается её столбцами. Поэтому число в (ii) совпадает с $\dim(\operatorname{im} \mu_A)$.

Поскольку элементарные преобразования матрицы A суть матрицы того же самого гомоморфизма μ_A, но в других базисах, $\dim(\operatorname{im} \mu_A)$ не меняется при элементарных преобразованиях строк и столбцов. Когда матрица приобретает диагональный вид, эта размерность, очевидно, равна числу диагональных единиц.

Если рассмотреть транспонированную матрицу A^t, полученную из A симметрией относительно главной диагонали (т. е. $a^t_{ij} \stackrel{\text{def}}{=\!=} a_{ji}$), то строки и столбцы A и A^t поменяются ролями, тогда как число единиц в диагональном виде A^t будет тем же самым. Поэтому числа (iii) и (v) также совпадают.

Наконец ясно, что ненулевые строки матрицы, полученной в результате приведения матрицы A к строго ступенчатому виду элементарными преобразованиями строк, составляют базис в подпространстве, порождённом в k^n строками A (эти строки линейно-независимы, и их число не меньше числа единиц в диагональном виде).

$\square$

Задача 5.26. Проверьте, что транспонирование $A \longmapsto A^t$ является кольцевым *антигомоморфизмом* (т. е. $(A+B)^t = A^t + B^t$, но $(AB)^t = B^t A^t$), — сложение сохраняется, а в произведениях изменяется порядок сомножителей).

Лекция 6
Определители

▷Ориентированный объём n-мерного параллелепипеда ▷Полилинейность, знакопеременность, кососимметричность ▷Знак перестановки ▷Описание полилинейных косых форм на свободном модуле ▷Определитель матрицы ▷Правило Крамера ▷Миноры и формулы Лапласа ▷Присоединенная матрица ▷Явная формула для обратной матрицы ▷Тождество Гамильтона-Кэли

§1. Форма объёма

1.1. Алгебраическая мотивировка. Когда мы решаем однородную систему линейных уравнений $Ax = 0$ методом Гаусса, вопрос о том, имеет ли она ненулевые решения, как правило, остаётся открытым вплоть до самого последнего шага. В этой лекции мы построим некий универсальный многочлен от элементов квадратной матрицы, значение которого на конкретной матрице A показывает, обратима ли она, и если да, то позволяет написать явную формулу для решения неоднородной системы $Ax = b$.

Для того чтобы судить о том, что будет на выходе каго-либо процесса, глядя на то, что подаётся на вход, надо, как известно, придумать *инвариант* этого процесса — нечто не меняющееся в ходе процесса и различающее конечные состояния. Чтобы построить многочлен, инвариантный относительно тех или иных алгебраических преобразований, следует обратиться к геометрии, ибо неинвариантность алгебраических выражений связана, как правило, с тем, что они неуклюже кодируют некую геометрическую картину, привлекая для этого избыточные данные: систему координат, неоднозначую запись и т. п. Независимость выражения от произвола в выборе этих данных (в частности, его инвариантность относительно их допустимых преобразований) означает, что это выражение является *геометрической величиной*. Итак, нам предстоит связать с каждой матрицей геометрическую величину.

Столбцы квадратной $(n \times n)$-метрицы над полем k можно воспринимать как некоторый набор векторов $(v_1, v_2, \ldots, v_n)$ координатного пространства k^n. Фигура, связанная с набором из n векторов — это натянутый на них параллепипед (см. рис.1 для $n = 3$). Геометрическая величина, ассоциированная с параллелипипедом, — это его объём. Объём как нельзя более подходит для того, чтобы выяснить, является ли набор векторов $(v_1, v_2, \ldots, v_n)$ линейно зависимым[1], а это то же самое что проверить обратима ли соответствующая матрица.

Задача 6.1. Убедитесь, что следующие свойства набора из n векторов v_i в k^n равносильны друг другу:

а) $(v_1, v_2, \dots, v_n)$ — базис в k^n;

б) $(v_1, v_2, \dots, v_n)$ — линейно независим;

в) матрица перехода C_{ev} от v_i к стандартному базису e_i в k^n обратима.

Мы не будем в этий лекции детально объяснять, что такое "объём тела в n-мерном пространстве" (переложив эту почётную обязанность на могучие плечи математического анализа). Вместо этого мы сначала выясним (про себя) какие интуитвные свойства объёма n-мерного параллелипипеда нам хотелось бы иметь, затем сформулируем их в виде аксиом и проверим, что удовлетворяющая этим аксиомам *форма объёма* существует и единственна (мы найдём для неё явное алгебраическое выражение).

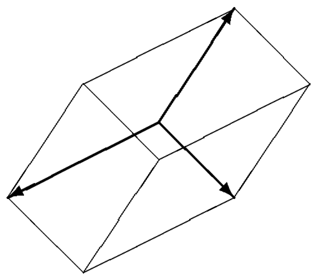


Рис. 1. Параллелепипед, натянутый на векторы

1.2. Геометрические свойства объёма. Обозначим искомую функцию объёма через

$$Vol\,(v_1, v_2, \dots, v_n)\,.$$

Во-первых, мы фиксируем единицу измерения: будем считать, что объём параллелипипеда, натянутого на стандартный базис $(e_1, e_2, \dots, e_n)$ в k^n равен единице:

$$Vol\,(e_1, e_2, \dots, e_n) = Vol\left(\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\ \vdots\\0\end{pmatrix}, \cdots \begin{pmatrix}0\\0\\ \vdots\\1\end{pmatrix}\right) \stackrel{\text{def}}{=} 1\,.$$

Во-вторых, ясно что $Vol\,(v_1, v_2, \dots, v_n)$ не изменяется, когда к одному из векторов v_i прибавляется кратность кокого-либо другого вектора v_j. Проекция того, что при этом происходит, на 2-мерную плоскость, порождённую векторами v_i и v_j показана на рис.2. Читателю предлагается представить себе всю n-мерную картинку и увидеть, что кусок, который при этом отрезается от параллелипипеда равен куску, который прикладывается к нему с другой стороны (ибо эти куски получаются друг из друга параллельным переносом).

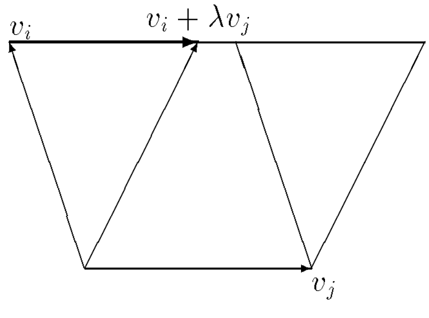


Рис. 2. Объём не меняется при перекосе

[1] линейная зависимость векторов $(v_1, v_2, \dots, v_n) \subset k^n$ равносильна тому, что они лежат в одной $(n-1)$-мерной гиперплоскости, а в этом случае натянутый на них параллепипед "уплощается" в фигуру нулевого объёма

Третье свойство является наиболее тонким. Интуитивно, над полем $k = \mathbb{R}$ при увеличении одной из сторон в λ раз ($\lambda > 0$) объём также должен увеличиваться в λ раз. Над произвольным полем k условие $\lambda > 0$ теряет смысл, и естественно потребовать, чтобы объём был просто однороден по каждому аргументу: $Vol(\dots\ \lambda v\,,\ \dots) = \lambda Vol(\dots\ v\,,\ \dots)\quad \forall\,\lambda \in k$ (здесь и во всех последующих подобных формулах многоточими обозначены аргументы, которые при переходе от левой части равенства к правой переписываются без изменений).

При $k = \mathbb{R}$ это приведёт к тому, что у некоторых параллелипипедов будет *отрицательный* объём: смена знака одного из векторов будет менять знак и у объёма. Так, при $n = 1$ стандартная длина вектора x – это *модуль* $|x|$, тогда как однородная длина — это линейная функция $Vol(x) = x$. Помимо того, что вторая намного удобнее первой в вычислениях, она дополнительно улавливает *ориентацию*, ибо векторы отрицательной длины — это в точности векторы, ориентированые противоположно стандартному базисному вектору. Многомерный однородный объём на $\mathbb{R}^n$ также учитывает *ориентауию набора векторов* и поэтому называется *ориентированным объёмом*.

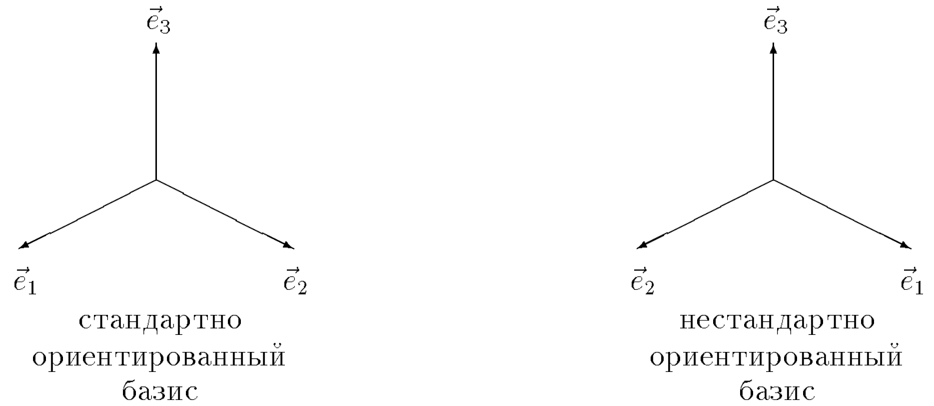


Рис. 3. Две возможных ориентации базиса в $\mathbb{R}^3$

Например, в $\mathbb{R}^3$ с точностью до непрерывной деформации имеется ровно два типа базисов[2] (см. рис.3), и тип базиса меняется на противоположный при смене знака одного из базисных векторов.

1.3. Определение. *Функция $\omega(v_1, v_2, \dots, v_n)$ от n аргументов $v_i \in k^n$ со значениями в поле k называется **ориентированным объёмом n-мерного параллелипипеда** (или просто **формой объёма**), если она обладает следующими свойствами:*

(i) $\omega(e_1, e_2, \dots, e_n) = 1$, *если* $\{e_1, e_2, \dots, e_n\}$ *— это стандартный базис в* k^n*;*

(ii) $\omega(\,\dots, v, \dots, w, \dots) = \omega(\,\dots, v + \lambda w, \dots, w, \dots)\ \ \forall\,\lambda \in k$ *и любых значений v, w любых двух различных аргументов (при фиксированных остальных аргументах);*

(iii) $\omega(\,\dots, \lambda v, \dots) = \lambda\omega(\,\dots, v, \dots)\ \ \forall\,\lambda \in k$ *и любого значения v любого из аргументов (при фиксированных остальных аргументах).*

[2] по определению, два базиса приннадлежат одному типу, если их можно включить в непрерывное семейство базисов $\{e_i(t)\}_{i=1,2,3}$, $t \in [0, 1]$

Из перечисленных свойств формально вытекает ещё несколько.

Задача 6.2. Выведите из однородности (iii), что форма объёма обращается в ноль, если хотя бы один из аргументов равен нулю.

Указание: $\vec{0} = 0 \cdot \vec{0}$, где $\vec{0} \in k^n$, а $0 \in k$.

1.3.1. Лемма. . *Форма объёма зануляется на всяком линейно зависимом наборе векторов.*

Доказательство. Если векторы $(v_1, v_2, \dots, v_n)$ линейно зависим, то один из них линейно выражается через остальные, скажем: $v_n = x_1v_1 + x_2v_2 + \dots + x_{n-1}v_{n-1}$. Многократно применяя свойство (ii), получаем:

$$\begin{aligned} \omega(v_1, v_2, \dots, v_n) &= \omega(\, v_1, v_2, \dots, v_{n-1}\,, \vec{0} + x_1v_1 + x_2v_2 + \dots + x_{n-1}v_{n-1}\,) = \\ &= \omega(\, v_1, v_2, \dots, v_{n-1}\,, \vec{0}\,) = 0 \end{aligned}$$

□

Следующее свойство геометриически уже не столь очевидно.

1.3.2. Лемма. *Фома объёма линейна по каждому аргументу, т. е. для каждого из аргументов (при фиксированных остальных) выполнено равенство:*

$$\omega(\,\dots,\, \lambda v + \mu w,\, \dots\,) = \lambda\omega(\,\dots,\, v,\, \dots\,) + \mu\omega(\,\dots,\, w,\, \dots\,)$$

при любых $v, w \in k^n$, $\lambda, \mu \in k$.

Доказательство. Принимая во внимание свойство (iii) формы объёма, достаточно доказать лишь равенство

$$\omega(\,\dots,\, v + w,\, \dots\,) = \omega(\,\dots,\, v,\, \dots\,) + \omega(\,\dots,\, w,\, \dots\,) \qquad \forall\, v, w \in k^n\,. \tag{6-1}$$

Предположим сначала, что один из наборов аргументов $(\,\dots,\, v,\, \dots\,)$ или $(\,\dots,\, w,\, \dots\,)$, — скажем, первый, — линейно независим, а значит, составляет базис в k^n. Тогда мы имеем разложения вида

$$\begin{aligned} w &= x \cdot v + (\text{линейная комбинация значений остальных аргументов}) \\ v + w &= (1 + x) \cdot v + (\text{линейная комбинация значений остальных аргументов}) \end{aligned}$$

(взятая в скобки линейная комбинация одинакова в обоих разложениях) с некоторым $x \in k$. Многократно примененяя свойство (ii) из определения формы объёма получаем:

$$\omega(\,\dots,\, w,\, \dots\,) = \omega(\,\dots,\, xv,\, \dots\,) = x \cdot \omega(\,\dots,\, v,\, \dots\,)$$

$$\omega(\,\dots,\, v + w,\, \dots\,) = \omega(\,\dots,\, (1 + x)v,\, \dots\,) = (1 + x) \cdot \omega(\,\dots,\, v,\, \dots\,)\,,$$

откуда сразу следует (6-1). Остаётся рассмотреть случай, когда оба набора $(\,\dots,\, v,\, \dots\,)$ и $(\,\dots,\, w,\, \dots\,)$ линейно зависимы. Но тогда и набор $(\,\dots,\, v+w,\, \dots\,)$ тоже будет линейно зависим (почему?), а значит, все три члена в формуле (6-1) обратятся в ноль.

□

В следующем параграфе мы представим оказательство существования и единственности формы объёма на k^n. Оно будет выведено из общих свойств полилинейных форм, справедливых над любыми коммутативными кольцами.

§2. Полилинейные косые формы

2.1. Полилинейность, знакопеременность и кососимметричность. Пусть V — произвольный модуль над любым коммутативным кольцом K. K-значная функция $f(v_1, v_2, \ldots, v_n)$ от n аргументов $v_i \in V$ называется

– *полилинейной формой*[3], если она удовлетворяет условию Лм.1.3.2, т. .е. K-линейна по каждому из аргументов (при фиксированных остальных).

– *знакопеременной*, если она меняет знак при перестановке любых двух аргументов, т. е. $f(\ldots, v, \ldots, w, \ldots) = -f(\ldots, w, \ldots, v, \ldots)$,

– *косой* (или *кососимметричной*), если она обращается в нуль при совпадении значений любой пары различных аргументов, т. е. $f(\ldots, v, \ldots, v, \ldots) = 0$.
Отметим, что форма объёма на k^n, буде она существует, является примером полилинейной кососимметричной формы, ибо имеет место

2.1.1. Предложение. *Если $2 = 1 + 1$ не нуль и не делитель нуля в K, то для любой полилинейной формы $f(v_1, v_2, \ldots, v_n)$ знакопеременность, кососимметричность и свойство (ii) из определения формы объёма попарно эквивалентны.*

Доказательство. Знакопеременность влечет кососимметричность, поскольку переставляя в $f(\ldots, v, \ldots, v, \ldots)$ равные аргументы v и v получим:

$$f(\ldots, v, \ldots, v, \ldots) = -f(\ldots, v, \ldots, v, \ldots)\,,$$

откуда $2f(\ldots, v, \ldots, v, \ldots) = 0$, что влечет $f(\ldots, v, \ldots, v, \ldots) = 0$, если $2 = 1 + 1$ не является делителем нуля (и не равна нулю).

Кососимметричность влечет свойство (ii) из Опр.1.3 над любым кольцом, поскольку

$$f(\ldots, v + \lambda w, \ldots, w, \ldots) = f(\ldots, v, \ldots, w, \ldots) + \lambda f(\ldots, w, \ldots, w, \ldots)\,,$$

и второе слагаемое зануляется.

Наконец, свойство (ii) влечет знакопеременность также над любым кольцом:

$$\begin{aligned} f(\ldots, v, \ldots, w, \ldots) &= f(\ldots, v + w, \ldots, w, \ldots) = \\ &= f(\ldots, v + w, \ldots, w - (v + w), \ldots) = \\ &= f(\ldots, v + w, \ldots, -v, \ldots) = \\ &= f(\ldots, v + w - v, \ldots, -v, \ldots) = \\ &= f(\ldots, w, \ldots, -v, \ldots) = \\ &= -f(\ldots, w, \ldots, v, \ldots)\,. \end{aligned}$$

□

[3] термин *форма* в алгебре и анализе является синонимом сочетания *однородная функция*; K-линейность — это однородность плюс аддитивность

2.1.2. Соглашение о характеристике. Всюду далее мы будем предполагать, что $2 = 1 + 1 \neq 0$ не является делителем нуля в кольце K (или что поле k имеет $\mathrm{char}\, k \neq 2$). Таким образом, знакопеременность и кососимметричность будут означать для нас одно и то же.

2.2. Перестановки. В предстоящих далее вычислениях нам потребуется следить за тем, как меняется знак кососимметричной формы не только при перестановке пары аргументов, но и при произвольных перестановках всей совокупности её аргументов. Аргументы представляют собой упорядоченное множество $(v_1, v_2, \dots, v_n)$ и говоря об их перестановках, удобно опускать бессодержательный символ v и следить только за номерами, а вернее за тем, на каких позициях стоят какие номера.

Формально, *перестановкой* конечного упорядоченного множества $\{1, 2, \dots, n\}$ из n попарно разных элементов (мы обозначили их числами $1, 2, \dots, n$) называется строчка

$$\{\sigma(1), \sigma(2), \dots, \sigma(n)\} ,$$

где σ — произвольное взаимно-однозначное отображение множества $\{1, 2, \dots, n\}$ на себя. Совокупность всех перестановок n-элементного упорядоченного множества обозначается $\mathfrak{S}_n$.

Задача 6.3. Сколько всего перестановок имеется в $\mathfrak{S}_n$?

Ответ: $n!$.

Символами $\sigma, \tau, \varrho, \eta, \dots$ мы далее будем обозначать как сами перестановки, так и соответствующие им взаимно-однозначные отображения $\{1, 2, \dots, n\}$ на себя. Тождественная перестановка обозначается через Id. *Композиция* $\tau\sigma \in \mathfrak{S}_n$ перестановок $\{\sigma(1), \sigma(2), \dots, \sigma(n)\}$ и $\{\tau(1), \tau(2), \dots, \tau(n)\}$ есть, по определению, перестановка $\{\tau(\sigma(1)), \tau(\sigma(2)), \dots, \tau(\sigma(n))\}$, отвечающая композиции соответствующих отображений σ, τ множества $\{1, 2, \dots, n\}$ на себя. Например, если $\sigma = (3, 2, 4, 5, 1), \tau = (5, 4, 2, 3, 1) \in \mathfrak{S}_5$, то $\tau\sigma = (2, 4, 3, 1, 5)$.

Задача 6.4. Убедитесь, что композиция перестановок ассоцитивна: $\sigma(\tau\eta) = (\sigma\tau)\eta$ $\forall\, \sigma, \tau, \eta \in \mathfrak{S}_n$, но не коммутативна.

Задача 6.5. Убедитесь, что всякая перестановка $\sigma \in \mathfrak{S}_n$ имеет единственную обратную $\sigma^{-1} \in \mathfrak{S}_n : \sigma^{-1}\sigma = \sigma\sigma^{-1} = Id$, и что отображение взятия композиции с фиксированной перестановкой $\sigma \in \mathfrak{S}_n : \quad \tau \longmapsto \sigma\tau$ является биекцией $\mathfrak{S}_n$ на себя.

Перестановка каких-то двух элементов между собой, не меняющая никаких других элементов, называется *транспозицией*. Всякая транспозиция τ, очевидно, обратна сама себе.

Задача 6.6. Убедитесь, что всякая перестановка есть композиция некоторого количества транспозиций. Единственно ли такое разложение?

Ответ: Очевидно нет !

2.2.1. Чётность и знак перестановки. Перестановка называется *чётной* или *нечётной* в соответствии с тем, произведением чётного или нечётного числа транспозиций она является. По определению, *знак* $sgn(\sigma)$ перестановки σ — это $+1$, если σ чётна, и -1, если σ нечётна. Корректность всего сказанного (т. е. невозможность представить одну и ту же перестановку в виде композиции как чётного, так и нечётного числа транспозиций) вытекает из следующего предложения, которое позволяет определить чётность перестановки не прибегая к её разложению.

2.2.2. Предложение. *Чётность перестановки $\{\sigma(1), \sigma(2), \dots, \sigma(n)\}$ совпадает с чётностью числа всех пар $(\sigma(i), \sigma(j))$ (где $1 \le i < j \le n$ – любые), у которых $\sigma(i) > \sigma(j)$, т. е. всех пар, порядок элементов в которых изменился под действием σ на противоположный (такие пары называются инверсиями или беспорядками).*

Доказательство. Достаточно показать, что количество беспорядков у композиции произвольной перестановки σ с любой транспозицией τ_{ij} (переставляющей между собой i и j) отличается от количества беспорядков в σ на нечётное число. Но $\sigma\tau_{ij}$ отличается от σ тем, что элементы $\sigma(i)$ и $\sigma(j)$ переставлены:

$$\begin{aligned} \sigma &= (*****\sigma(i)\ *****\ \sigma(j)\ *****) \\ \sigma\tau_{ij} &= (*****\sigma(j)\ *****\ \sigma(i)\ *****)\,, \end{aligned}$$

и от такой перестановки число беспорядков изменится на удвоенное число элементов, стоящих между $\sigma(i)$ и $\sigma(j)$ (ибо все пары $(\sigma(i), *)$ и $(*, \sigma(j))$, где $*$ стоит между $\sigma(i)$ и $\sigma(j)$, превратятся, соответственно, в пары $(\sigma(j), *)$ и $(*, \sigma(i))$ противоположной "инверсности") да ещё на единицу за счёт изменения "инверсности" в самой паре $(\sigma(i), \sigma(j))$, подвергнутой транспозиции.
□

2.2.3. Следствие. *Значение кососимметричной формы не изменяется при чётных перестановках аргументов и меняет знак при нечётных перестановках аргументов.*

Задача 6.7. Как чётность композиции $\sigma\tau$ зависит от чётности σ и τ ?

Задача 6.8. Докажите, что взятие композиции с произвольно зафиксированной нечётной перестановкой задаёт биекцию между множеством чётных перестановок и множеством нечётных перестановок.

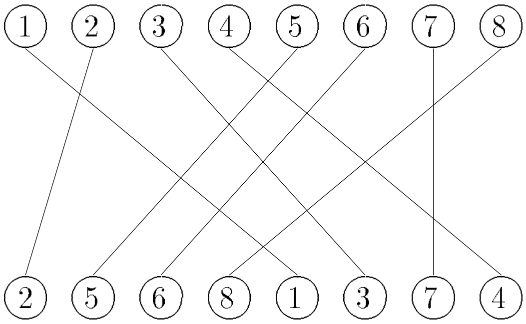


Рис. 4. Правило ниточек

Для практического определения чётности перестановки обычно используют *правило ниточек*, позволяющее легко подсчитать число беспорядков. Надо соединить ниточками пары одинаковых чисел в записанных друг под другом наборах $\{1, \dots, n\}$ и $\{\sigma(1), \dots, \sigma(n)\}$, следя за тем, чтобы эти ниточки пересекались не более, чем по две. Тогда каждая инверсная пара превносит ровно одно пересечение ниточек, и общее число инверсий есть суммарное число пересечений. Например, число инверсий в перестановке $(2, 5, 6, 8, 1, 3, 7, 4) \in \mathfrak{S}_8$ равно 12 (см. рис.4).

2.3. Ключевое вычисление. Пусть $f(v_1, v_2, \dots, v_n)$ — полилинейная кососсимметричная форма на K^n. Тогда значение $f(v_1, v_2, \dots, v_n) = 1$ на произвольном наборе векторов можно явно выразить через значение f на стандартном базисе $(e_1, e_2, \dots, e_n)$. В самом деле, пусть

$$v_j = \sum_i c_{ij} e_i\,, \qquad j = 1, 2, \dots, n\,,$$

где $(c_{\alpha\beta}) = C_{ev}$ — это матрица перехода, по столбцам которой стоят координаты векторов v_i в базисе e_i. Пользуясь полилинейностью, находим:

$$\begin{aligned} f(v_1, v_2, \dots, v_n) &= f\left(\sum_i c_{i1}e_i\,,\ \sum_i c_{i2}e_i\,,\ \dots\,,\ \sum_i c_{in}e_i\right) = \\ &= \sum_{i_1}\sum_{i_2}\cdots\sum_{i_n} f\Big(c_{i_11}e_{i_1}\,,\ c_{i_22}e_{i_2}\,,\ \dots\,,\ c_{i_nn}e_{i_n}\Big) = \\ &= \sum_{i_1,i_2,\dots,i_n} c_{i_11}c_{i_22}\cdots c_{i_nn} f(e_{i_1}, e_{i_2}, \dots, e_{i_n})\,. \end{aligned}$$

Из кососимметричности f вытекает, что $f(e_{i_1}, e_{i_2}, \dots, e_{i_n}) = 0$ если среди индексов i_ν есть совпадающие. Поэтому в последней сумме реально участвуют лишь слагаемые, у которых набор индексов $(i_1, i_2, \dots, i_n)$ является *перестановкой* набора $(1, 2, \dots, n)$. Таким образом, принимая во внимание Сл.2.2.3, мы можем переписать эту сумму в виде

$$f(v_1, v_2, \dots, v_n) = \sum_{\sigma\in\mathfrak{S}_n} sgn\,(\sigma) c_{\sigma(1)1}c_{\sigma(2)2}\cdots c_{\sigma(n)n}\cdot f(e_1, e_2, \dots, e_n)\,.$$

2.4. Определение. *Пусть $C = (c_{\alpha\beta})$ — квадратная матрица с элементами из некоторого коммутативного кольца K. Число*

$$\det C = \det(c_{\alpha\beta}) \overset{\text{def}}{=} \sum_{\sigma\in\mathfrak{S}_n} sgn\,(\sigma) c_{\sigma(1)1}c_{\sigma(2)2}\cdots c_{\sigma(n)n} \in K\,, \tag{6-2}$$

называется определителем квадратной матрицы $C = (c_{\alpha\beta})$.

Предыдущее вычисление доказывает

2.4.1. Предложение. *Пусть f — полилинейная кососсосимметричная форма от n аргументов на произвольном K-модуле, и $\{e_i\}$ и $\{v_i\}$ — два набора из n векторов, связанные при помощи матрицы перехода $C \in Mat_n(K)$:*

$$(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n)C\,.$$

Тогда $f(v_1, v_2, \dots, v_n) = \det(C)\cdot f(e_1, e_2, \dots, e_n)$.

□

В частности, мы получаем, что форма объёма на координатном векторном пространстве k^n единственна (если существует) и задаётся формулой

$$\omega(v_1, v_2, \dots, v_n) = \det C_v\,,$$

где C_v — матрица, составленная из вектор-столбцов $v_i \in k^n$, а для доказательства существования формы обёма остаётся лишь доказать

2.4.2. Предложение. *Определитель $\det(C)$ является полилинейной кососимметричной функцией от столбцов матрицы $C \in Mat_n(K)$ (где K – произвольное коммутативное кольцо), и $\det E = 1$, если E — единичная матрица.*

Доказательство. Полилинейность видна непосредственно из (6-2) — каждое из складываемых произведений содержит ровно по одному элементу из каждого столбца, а значит, линейно по каждому столбцу. Свойство $\det E = 1$ тоже очевидно, ибо если

$$(c_{\alpha\beta}) = \begin{cases} 1\ , & \text{при} \quad \alpha = \beta \\ 0\ , & \text{при} \quad a \neq \beta \end{cases} ,$$

то сумма в правой части (6-2) содержит лишь одно ненулевое слагаемое, соответствующее тождественной перестановке.

Для проверки кососимметричности обозначим через C' матрицу, полученную из C перестановкой i-ого и j-того столбцов. Произведения, входящие в выражение для $\det(C')$ отличается от произведений в (6-2) толко i-тым и j-тым множителями: вместо

$$sgn\,(\sigma) \cdot *****c_{\sigma(i)i}\ *****\ c_{\sigma(j)j}\ *****$$

теперь будут складываться произведения

$$sgn\,(\sigma) \cdot *****c_{\sigma(i)j}\ *****\ c_{\sigma(j)i}\ *****\ ,$$

которые, если переставить в них i-тый и j-тый множители местами, можно записать в виде

$$sgn\,(\sigma) c_{\varrho(1)1} c_{\varrho(2)2} \cdots c_{\varrho(n)n}\ ,$$

где $\varrho = \sigma\tau_{ij}$ есть композиция перестановки σ и транспозиции τ_{ij} индексов i и j (ср. с доказательством Пр.2.2.2). Поскольку по зад.6.5 композиция $\varrho = \sigma\tau_{ij}$ также пробегает $\mathfrak{S}_n$ когда σ пробегает $\mathfrak{S}_n$, а $sgn\,(\varrho) = -sgn\,(\sigma)$, имеем:

$$\det C' = \sum_{\sigma\in\mathfrak{S}_n} sgn\,(\sigma) c_{\varrho(1)1} c_{\varrho(2)2} \cdots c_{\varrho(n)n} = -\sum_{\varrho\in\mathfrak{S}_n} sgn\,(\varrho) c_{\varrho(1)1} c_{\varrho(2)2} \cdots c_{\varrho(n)n} = -\det C\ .$$

□

2.4.3. Следствие. *Форма объёма на векторном пространстве k^n существует и единственна. Её значение на наборе вектор-столбцов равно определителю матрицы, составленной из этих столбцов.*

□

2.4.4. Следствие. *Определитель матрицы обращается в ноль, если столбцы матрицы линейно-зависимы (в частности, если есть нулевой столбец или два совпадающих столбца).*

□

2.4.5. Следствие. *Пусть V — свободный K-модуль ранга n. Совокупность всех полилинейных косых форм от n аргументов $v_i \in V$ представляет собой свободный K-модуль*[4] *ранга 1. Для любого базиса $\{e_1, e_2, \dots, e_n\} \subset V$ существует единственная форма $\omega_e \in \Lambda^n(K^n)$, для*

[4] он обозначается $\Lambda^n(K^n)$ и называется *n-той внешней степенью* модуля K^n

которой $\omega_e(e_1, e_2, \dots, e_n) = 1$. *Произвольная форма* $f \in \Lambda^n(K^n)$ *будет линейно выражаться через* ω_e *по формуле*

$$f(v_1, v_2, \dots, v_n) = f(e_1, e_2, \dots, e_n) \cdot \omega_e(v_1, v_2, \dots, v_n) \qquad \forall\ v_1, v_2, \dots, v_n\ \in V$$

(т. е. форма ω_e *является базисной образующей модуля всех полилинейных косых форм).*

Доказательство. Согласно Пр.2.4.1, значение полилинейной кососимметричной формы f на произвольном наборе векторов $(v_1, v_2, \dots, v_n)$ выражается через её значение на произвольном базисе $(e_1, e_2, \dots, e_n)$ по формуле

$$f(v_1, v_2, \dots, v_n) = \det C_{ev} f(e_1, e_2, \dots, e_n)\ , \tag{6-3}$$

где $(c_{\alpha\beta}) = C_{ev})$ — это матрица перехода, по столбцам которой стоят координаты векторов $(v_1, v_2, \dots, v_n)$ в базисе $\{e_i\}$. Полагая

$$\omega_e(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \det C_{ev}\ ,$$

из доказанных выше свойств определителя немедленно получаем, что ω_e – это полилинейная косая форма, принимающая значение 1 на базисе $(v_1, v_2, \dots, v_n)$. Равенство (6-3) показывает, что все остальные формы пропорциональны ω_e, откуда сразу следуют все утверждения следствия.
□

§3. Свойства определителей.

3.1. Комбинаторный анализ формулы. С комбинаторной точки зрения, формула для определителя $(n \times n)$-матрицы $C = (c_{\alpha,b})$

$$\det(C) = \sum_{\sigma \in \mathfrak{S}_n} sgn\,(\sigma) c_{\sigma(1)1} c_{\sigma(2)2} \cdots c_{\sigma(n)n}$$

представляет собой сумму всех возможных произведений из n матричных элементов, выбранных так, чтобы в каждой строке и в каждом столбце присутствовал ровно один из этих элементов. Позиции выбираемых элементов можно воспринимать как *график* взаимнооднозначного отображения $\{\text{номера столбцов}\} \xrightarrow{\sigma} \{\text{номера строк}\}$ (в i-том столбце выбирается $\sigma(i)$-тый элемент). Знак с которым входит в сумму соответствующее произведение есть знак σ как перестановки номеров $\{1, 2, \dots, n\}$. Например,

$$\det\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = c_{11}c_{22} - c_{21}c_{12}$$

$$\det\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = \big(c_{11}c_{22}c_{33} + c_{21}c_{32}c_{13} + c_{31}c_{12}c_{23}\big) - \big(c_{31}c_{22}c_{13} + c_{21}c_{12}c_{33} + c_{11}c_{32}c_{23}\big)\quad .$$

В частности, определитель не изменяется при замене матрицы $C = (c_{\alpha\beta})$ на транспонированную матрицу $C^t = (c^t_{\alpha\beta})$, где $c^t_{\alpha\beta} \stackrel{\text{def}}{=} c_{\beta\alpha}$. В самом деле, от транспонирования строки и столбцы меняются ролями, что в предыдущем комбинаторном описании проявляется только в том, что вместо σ для определения знака следует брать обратную перестановку σ^{-1}.

Задача 6.9. Докажите, что $sgn\,(\sigma^{-1}) = sgn\,(\sigma) \quad \forall\, \sigma \in \mathfrak{S}_n$.

Таким образом, мы доказали

3.1.1. Предложение. $\det(C) = \det(C^t) \qquad \forall\, A \in Mat_n(K)$.

□

3.1.2. Следствие. *Определитель является полилинейной кососимметричной формой от строк матрицы и не меняется при при почленном прибавлении к любой строке кратности какой-либо другой строки.*

□

В частности, формулу для вычисления определителя можно переписать в виде

$$\det C = \det(c_{\alpha\beta}) \stackrel{\text{def}}{=} \sum_{\sigma\in\mathfrak{S}_n} sgn\,(\sigma) c_{1\sigma(1)} c_{2\sigma(2)} \cdots c_{n\sigma(n)} \in K \ , \tag{6-4}$$

3.2. Мультипликативные свойства определителя обусловлены формулой Пр.2.4.1, показывающей как меняется значение полилинейной кососимметричной формы при линейной замене переменных.

3.2.1. Предложение. $\det(AB) = \det(A)\det(B) \qquad \forall\, A, B \in Mat_n(K)$.

Доказательство. Пусть $(e_1, e_2, \ldots, e_n)$ — стандартный базис в K^n, а наборы векторов $\{v_i\}$ и $\{w_i\}$ определены формулами

$$\begin{aligned} (v_1, v_2, \ldots, v_n) &= (e_1, e_2, \ldots, e_n)A\,, \\ (w_1, w_2, \ldots, w_n) &= (v_1, v_2, \ldots, v_n)B = (e_1, e_2, \ldots, e_n)AB\ . \end{aligned}$$

Если ω_e — полилинейная косая форма на K^n, такая что $\omega_e(e_1, e_2, \ldots, e_n) = 1$, то согласно Пр.2.4.1

$$\begin{aligned} \omega(v_1, v_2, \ldots, v_n) &= \det(A)\,, \\ \omega(w_1, w_2, \ldots, w_n) &= \det(AB)\ . \end{aligned}$$

С другой стороны, используя выражение векторов w_i через векторы v_i получаем

$$\omega(w_1, w_2, \ldots, w_n) = det(B) \cdot \omega(v_1, v_2, \ldots, v_n)\ ,$$

откуда $\det(AB) = \det(A)\det(B)$.

□

3.2.2. Следствие. $\det(AB) = \det(BA) \qquad \forall\, A, B \in Mat_n(K)$.

Доказательство. $\det(A)$ и $\det(B)$ коммутируют как и все элементы K.
□

3.2.3. Следствие. *Если матрица A обратима в $\mathrm{Mat}_n(K)$, то $\det(A)$ обратим в K.*

Доказательство. $\det(A)\det(A^{-1}) = \det(E) = 1$ означает, что $\det(A^{-1}) = \det(A)^{-1}$.
□

3.2.4. Следствие. *Квадратная матрица A над полем*[5] *обратима тогда и только тогда, когда $\det(A) \neq 0$ (такие матрицы называются невырожденными).*

Доказательство. Пусть векторы $(e_1, e_2, \ldots, e_n)$ составляют базис векторного пространства V над полем k.

Если векторы $(v_1, v_2, \ldots, v_n) = (e_1, e_2, \ldots, e_n)A$ линейно независимы, то они тоже составляют базис, и значит, матрица A будет обратимой (обратная матрица $A^{-1} = C_{ev}$ будет иметь по столбцам координаты векторов e_i в базисе v_i). По предыдущему следствию, $\det(A) \neq 0$.

Если векторы v_i (т. е. столбцы матрицы A) линейно зависимы, то $\det(A) = 0$.

Других возможностей нет.
□

3.3. Правило Крамера. Вернёмся теперь к задаче, которая была сформулирована в начале лекции, и покажем, как можно использовать определители при решении систем линейных уравнений. Условимся обозначать через $\det(a_1, a_2, \ldots, a_n)$, где $a_i \in K^n$, определитель матрицы $A = (a_1, a_2, \ldots, a_n)$, по столбцам которой стоят координаты векторов a_i в стандартном базисе K^n. Если числа $x_1, x_2, \ldots, x_n \in K$ удовлетворяют системе уравнений

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = b \ ,$$

т. е. доставляют разложение вектора $b \in K^n$ в виде

$$b = x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \ ,$$

то вследствие линейности определителя по i-тому аргументу и кососимметричности мы имеем

$$\det(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n) = \det(a_1, \ldots, a_{i-1}, \sum_{i-1}^{n} x_\nu a_\nu, a_{i+1}, \ldots, a_n) =$$

$$= \sum_{\nu=1}^{n} x_\nu \det(a_1, \ldots, a_{i-1}, a_\nu, a_{i+1}, \ldots, a_n) = x_i \cdot \det(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) = x_i \det(A) \ ,$$

что доказывает

3.3.1. Предложение. (Правило Крамера.) *При умножении определителя матрицы системы $Ax = b$ на i-тую координату решения получается определитель матрицы, которая*

[5] обобщение на произвольное коммутативное кольцо будет получено ниже в Сл.4.3.4

отличается от матрицы системы заменой i-того столбца на столбец правых частей (для каждого $i = 1, 2, \ldots, n$).

□

Когда мы имеем дело с системой $Ax = b$ из n линейных уравнений от n неизвестных над *полем* $K = k$, из правила Крамера следует, что если $\det(A) \neq 0$, то для любой правой части b решение существует, единственно и даётся формулой

$$x_i = \frac{\det(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n)}{\det(A)}\,, \quad i = 1, 2, \ldots, n\;.$$

Задача 6.10. Пусть $\det(A)$ обратим в K. Попытайтесь при помощи правила Крамера получить явную формулу для элементов обратной матрицы A^{-1} в терминах самой матрицы A.

3.4. Пример: результант и дискриминант. Пусть

$$A(t_1, t_2) = \sum_{\nu=1}^{n} a_\nu t_1^\nu t_2^{n-\nu} \qquad \text{и} \qquad B(t_1, t_2) = \sum_{\mu=1}^{m} b_\mu t_1^\mu t_2^{n-\mu}$$

два однородных многочлена степеней n и m с коэффициентами в некотором поле k. Как выяснить, имеют ли они нетривиальный общий множитель в $k[t_1, t_2]$? Если таковым множителем является t_1 (или t_2), то это заметно на глаз. Если же нет, то многочлены

$$\begin{aligned} \widehat{A}(t) &\stackrel{\text{def}}{=} A(1,t) = a_0 n^t + a_1 n^{t-1} + \cdots + a_{t-1} n + a_t \in k[t] \\ \widehat{B}(t) &\stackrel{\text{def}}{=} B(1,t) = b_0 m^t + b_1 m^{t-1} + \cdots + b_{t-1} m + b_t \in k[t] \end{aligned}$$

имеют степени в точности n и m (т. е. имеют ненулевые a_0 и b_0 соответственно), и наличие нетривиального общего делителя у A и B в $k[t_1, t_2]$ равносильно наличию нетривиального общего делителя у $\widehat{A}$ и $\widehat{B}$ в $k[t]$, а значит, может быть проверено при помощи алгоритма Евклида. Однако, как и метод Гаусса, алгоритм Евклида не позволяет сделать никаких качественных выводов *заранее*. Теперь мы в состоянии исправить это неудобство, ибо алгоритм Евклида также, как и метод Гаусса, в сущности, решает систему линейных уравнений.

В самом деле, если $A = DA'$, $B = DB'$, где $D, A', B' \in k[t_1, t_2]$ – некоторые однородные многочлены, то мы можем подобрать однородные многочлены X и Y степеней $\deg X = \deg B - \deg D$ и $\deg Y = \deg A - \deg D$, так чтобы в $k[t_1, t_2]$ выполнялось равенство

$$AX = DA'B' = BY\;.$$

Таким образом условие $\deg D \geq 1$ равносильно возможности подобрать многочлен $X \neq 0$ степени $\leq (m-1)$ и многочлен $Y \neq 0$ степени $\leq (n-1)$, удовлетворяющие равенству $AX = BY$, которое легко превратить в однородную систему из $n+m$ линейных уравнений на $m+n$ коэффициентов $x_0, x_1, \ldots, x_{m-1}$, $y_1, y_2, \ldots, y_{n-1}$ многочленов X, Y, сравнивая мономы одинаковой степени в AX и BY.

Задача 6.11. Напишите явно матрицу этой системы.

Пусть K – произвольное коммутативное кольцо, а $A, B \in K[t_1, t_2]$ и $\widehat{A}, \widehat{B} \in K[t]$ – многочлены с коэффициентами $a_0, a_1, \dots, a_n$ и $b_0, b_1, \dots, b_m$ как и выше. Определитель матрицы

$$\underbrace{\begin{pmatrix} a_0 & a_1 & \dots & a_n & & & \\ & a_0 & a_1 & \dots & a_n & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & & & \\ & b_0 & b_1 & \dots & b_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & \dots & b_m \end{pmatrix}}_{m+n} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \end{matrix} \tag{6-5}$$

называется *результантом* двух однородных форм A, B (или двух многочленов $\widehat{A}, \widehat{B} \in k[t]$) и обозначается $R(A, B)$ (или $R_{n,m}(A, B)$).

Задача 6.12. Убедитесь, что над полем k однородные многочлены A и B из $k[t_1, t_2]$ тогда и только тогда обладают нетривиальным общим делителем в $k[t_1, t_2]$, когда $R(A, B) = 0$.

Указание. это сразу следует из предыдущей задачи и свойств определетилей.

Задача 6.13. Пусть $f, g \in k[t]$ – многочлены степени $\le n$ и $\le m$ соответственно. Докажите, что равенство $R_{n.m}(f, g) = 0$ равносильно совокупности трёх условий: либо $\deg f < n$, либо $\deg g < m$, либо НОД$(f, g) \neq 1$.

Задача 6.14. Убедитесь, что результант многочлена и его производной делится на старший коэффициент этого многочлена (над любым кольцом).

Пусть $f = a_0 n^t + a_1 n^{t-1} + \dots + a_{t-1} n + a_t \in K[t]$ – многочлен с $a_0 \neq 0$, и f' – его производная. Число $D(f) \overset{\text{def}}{=} (-1)^{\frac{n(n-1)}{2}} \dfrac{R_{n,n-1}(f, f')}{a_0} \in K$ называется *дискриминантом* f.

Задача 6.15. Убедитесь, что обращение дискриминанта в нуль равносильно наличию кратных корней и вычислите дискриминант квадратного и кубического многочленов.

3.4.1. Предложение. *Пусть*

$$f = a_0 n^t + a_1 n^{t-1} + \dots + a_{t-1} n + a_t \qquad \text{и} \qquad g = b_0 m^t + b_1 m^{t-1} + \dots + b_{t-1} m + b_t$$

два многочлена с коэффициентами из произвольного коммутативного кольца K. Существуют такие многочлены $u, v \in K[t]$, что $uf + vg = R_{n,m}(f, g)$ как элементы $K[t]$.

Доказательство. Равенства

$$
\begin{array}{rcl}
t^{m-1}f &=& a_0t^{m+n-1} + a_1t^{n+m-2} + \cdots + a_nt^{m-1} \\
t^{m-1}f &=& a_0t^{m+n-2} + a_1t^{n+m-3} + \cdots + a_nt^{m-1} \\
\vdots && \ddots \\
f &=& a_0t^n + a_1t^{n-1} + \cdots + a_n \\
t^{n-1}g &=& b_0t^{m+n-1} + b_1t^{n+m-2} + \cdots + b_nt^{m-1} \\
t^{n-1}g &=& b_0t^{m+n-2} + b_1t^{n+m-3} + \cdots + b_nt^{m-1} \\
\vdots && \ddots \\
g &=& b_0t^m + b_1t^{m-1} + \cdots + b_m
\end{array}
$$

означают, что столбец $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{m+n} \end{pmatrix} = \begin{pmatrix} t^{m+n-1} \\ t^{m+n-2} \\ \vdots \\ 1 \end{pmatrix} \in K[t]^{m+n}$ является решением системы из $m+n$ линейных уравнений вида

$$
\begin{array}{rcl}
t^{m-1}f &=& a_0x_1 + a_1x_2 + \cdots + a_nx_{n+1} \\
t^{m-1}f &=& a_0x_2 + a_3x_2 + \cdots + a_nx_{n+1} \\
\vdots && \ddots \\
f &=& a_0x_{m-1} + a_1x_{m-2} + \cdots + a_nx_{m+n} \\
t^{n-1}g &=& b_0x_1 + b_1x_2 + \cdots + b_nx_{m+1} \\
t^{n-1}g &=& b_0x_2 + b_1x_3 + \cdots + b_nx_{m+1} \\
\vdots && \ddots \\
g &=& b_0x_{n-1} + b_1x_{n-2} + \cdots + b_mx_{m+n}
\end{array}
$$

над кольцом $K[t]$, матрица которой совпадает с (6-5). По правилу Крамера, применённому к последней координате решения, мы получаем, что $R(f,g)$ равен определителю матрицы, полученной из (6-5) заменой ненулевых элементов a_0 и b_0 в последнем столбце на f и g соответственно. Поскольку никаких других ненулевых элементов в последнем столбце нет, вычисляя этот определитель, получаем выражение вида $u(t)f(t)+v(t)g(t)$, где $f,g \in K[t]$.
□

Вот ещё несколько упражнений на вычисление определителей:

Задача 6.16. Пусть $A(t_1,t_2)$ – однородная форма степени n, и $f(t) = A(1,t)$. Докажите, что дискриминант f с точностью до умножения на ненулевую константу совпадает с результантом пары форм $\dfrac{\partial A}{\partial t_1}$ и $\dfrac{\partial A}{\partial t_1}$ и найдите точно, чему равна эта констаната.

Задача 6.17. Пусть $n \geq m$ и пусть d_k, $k = 0,1,2,\ldots$, — определитель матрицы, которая получается из матрицы

$$\underbrace{\begin{pmatrix}
a_0 & \dots & \dots & a_{n-1} & a_n & & & & \\
 & a_0 & \dots & \dots & a_{n-1} & a_n & & & \\
 & & \ddots & & & \ddots & \ddots & & \\
 & & & a_0 & \dots & \dots & a_{n-1} & a_n \\
 & & & & b_0 & \dots & b_{m-1} & b_m \\
 & & & \iddots & & \iddots & \iddots & & \\
 & & \iddots & & \iddots & \iddots & & & \\
 & b_0 & \dots & b_{m-1} & b_m & & & & \\
b_0 & \dots & b_{m-1} & b_m & & & & &
\end{pmatrix}}_{m+n}
\begin{matrix}\left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}m\\ \left.\vphantom{\begin{matrix}b\\b\\b\\b\\b\end{matrix}}\right\}n\end{matrix}$$

выкидыванием по k строк и k столбцов свеху, сницу, слева и справа (т. е. выкидыванием внешнего контура толщины k). Докажите, что индекс первого ненулевого члена последовательности $d_0, d_1, d_2, \dots$ равен степени наибольшего общего делителя пары однородных форм $A = \sum a_\nu t_1^\nu t_2^{n-\nu}$ и $B = \sum a_\mu t_1^\mu t_2^{m-\mu}$ в $k[t_1, t_2]$.

§4. Соотношения Лапласа.

Площадь параллелограмма можно выразить через длины сторон, а объём параллелепипеда — через длины рёбер и площади граней. Естественно ожидать, что должны быть универсальные формулы, выражающие ориентированный объём n-мерного параллалипипеда через k-мерные объёмы k-мерных граней ($k < n$). И хотя мы пока что не обладаем надлежащей геометрической техникой для того, чтобы эти формулы *увидеть*[6] у нас есть всё необходимое для их формально-алгебраического доказательства. На языке алгебры, эти формулы (называемые формулами *разложения определителя*) означают, что $\det(C)$ можно выразить через определители подматриц, содержащихся в C. Чтобы написать их явно, нам потребуются кое-какие обозначения.

4.1. Мультииндексы, подматрицы и миноры. Буквами $I, J, K, \dots$ мы далее будем обозначать упорядоченные поднаборы вида

$$I = (i_1, i_2, \dots, i_m)\ , \quad i_1 < i_2 < \dots < i_m\ ,$$

в наборе $(1, 2, \dots, n)$. Каждый такой поднабор I мы будем называть *мультииндексом*, а число m элементов набора I — *длиной мультииндекса* и обозначать $\#I$. Сумма $i_1 + i_2 + \dots + i_m$ называется *весом* мультииндекса $I = (i_1, i_2, \dots, i_m)$ и обозначается $|I|$. Мультииндекс, состоящий из всех элементов набора $(1, 2, \dots, n)$, не входящих в мультииндекс I, называется *дополнительным* к I и обозначается $\widehat{I}$. Ясно, что J совпадает с $\widehat{I}$ если и только если $\#I + \#J =$

[6] мы построим соответствующую геометрическую теорию в следующих двух семестрах

n и $I \cap J = \emptyset$. Отметим также, что всего имеется $\binom{n}{k}$ мультииндексов длины k, и что всегда

$$|I| + |\widehat{I}| = \frac{n(n+1)}{2} \, .$$

Например: если $n = 8$ и $I = (1, 3, 4, 6, 8)$, то $\#I = 5$, $|I| = 22$, $\widehat{I} = (2, 5, 7)$, $\#\widehat{I} = 3$, $|\widehat{I}| = 14$.

Мы будем использовать мультииндексы для задания подматриц в данной $(n \times n)$-матрице $C = (c_{\alpha\beta})$. А именно, через $C[IJ]$, где $I = (i_1, i_2, \dots, i_m)$, $J = (j_1, j_2, \dots, j_m)$, мы обозначаем квадратную $(m \times m)$-подматрицу, образованную элементами $c_{i_\alpha j_\beta}$, $1 \le \alpha, \beta \le m$. Определитель $\det(C[IJ])$ называется IJ-м *минором* (m-того порядка) матрицы C и обозначается C_{IJ} (по аналогии с матричными элементами, которые есть ни что иное как миноры 1-го порядка).

Например: если $C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}$, то $C_{(2,4),(2,3)} = \det \begin{pmatrix} c_{22} & c_{23} \\ c_{42} & c_{43} \end{pmatrix} = c_{22}c_{43} - c_{42}c_{23}$.

Если упорядочить мультииндексы длины m каким-то фиксированным способом[7], то из миноры m-того порядка также можно записать в виде квадратной матрицы $\big(C_{IJ}\big)$ размера $\binom{n}{m} \times \binom{n}{m}$. Эта матрица обозначается $\Lambda^m C$ и называется *m-той внешней степенью* матрицы C.

4.2. Теорема. (Теорема Лапласа.) *Для любой квадратной матрицы A над любым коммутативным кольцом выполнены следующие два набора тождеств:*

(А) *разложение определителя по строкам из I: для произвольным образом выбранного мультииндекса I длины $\#I = k$*

$$\det A = \sum_{J \,:\, \#J = k} (-1)^{|I|+|J|} A_{IJ} A_{\widehat{I}\widehat{J}}$$

(суммирование происходит по всем мультииндексам J длины $\#J = \#I = k$);

(Б) *теорема об умножении на чужие дополнения: для двух произвольным образом выбранных различных мультииндексов $I \neq J$, одинаковой длины $\#I = \#J = k$*

$$\sum_{K \,:\, \#K = k} (-1)^{|I|+|K|} A_{IK} A_{\widehat{J}\widehat{K}} = 0$$

(суммирование происходит по всем мультииндексам K длины $\#K = k$).

Доказательство. Поскольку в каждом из $n!$ произведений, входящих в сумму из (6-4):

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} sgn\,(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \, ,$$

[7] например, *лексикографически*, т. е. полагая, что $I < J$, если первый считая слева из несовпадающих элементов в I меньше, чем в J; самым маленьким при таком порядке будет мультииндекс $(1, 2, \dots, m)$, за ним будет следовать мультииндекс $(1, 2, \dots, m-1, m+1)$ и т. д.

присутствует ровно по одному элементу из каждой строки, можно переупорядочить множители так, чтобы сначала шли элементы из строк с номерами из набора $I = (i_1, i_2, \dots, i_k)$, а потом — из дополнительного набора $\widehat{I} = (\widehat{\imath}_1, \widehat{\imath}_2, \dots, \widehat{\imath}_{n-k})$ (напомню, что $i_1 < i_2 < \cdots < i_k$ и $\widehat{\imath}_1 < \widehat{\imath}_2 < \cdots \widehat{\imath}_{n-k}$. В результате получим:

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} sgn\,(\sigma) a_{i_1\sigma(i_1)} a_{i_2\sigma(i_2)} \cdots a_{i_k\sigma(i_k)} a_{\widehat{\imath}_1\sigma(\widehat{\imath}_1)} a_{\widehat{\imath}_2\sigma(\widehat{\imath}_2)} \cdots a_{\widehat{\imath}_{n-k}\sigma(\widehat{\imath}_{n-k})} .$$

Разобьём теперь множество всех перестановок $\mathfrak{S}_n$ в объединение непересекающихся подмножеств $\mathfrak{S}_{JI}$, каждое из которых состоит из всех перестановок, переводящих набор $I = (i_1, i_2, \dots, i_k)$ в какую-либо перестановку набора $J = (j_1, j_2, \dots, j_k)$ (напомню, что $j_1 < j_2 < \cdots < j_k$). Каждая перестановка $\sigma \in \mathfrak{S}_{JI}$ однозначно представимых в виде композиции $\sigma = \tau\eta\sigma_{JI}$, где $\sigma_{JI} \in \mathfrak{S}_n$ — фиксированная перестановка, отображающая I на J и $\widehat{I}$ на $\widehat{J}$ с сохранением порядка (т. е. $\sigma_{JI}(i_\alpha) = j_\alpha$ и $\sigma_{JI}(\widehat{\imath}_\alpha) = \widehat{\imath}_\alpha$), $\tau \in \mathfrak{S}_k$ — произвольная перестановка индексов $\{1, 2, \dots, k\}$ в наборе $(j_1, j_2, \dots, j_k)$, а η — произвольная перестановка индексов $\{1, 2, \dots, (n-k)\}$ в дополнительном наборе $(\widehat{\jmath}_1, \widehat{\jmath}_2, \dots, \widehat{\jmath}_{n-k})$.

Задача 6.18. Сколько всего перестановок в $\mathfrak{S}_{JI}$?

Задача 6.19. Убедитесь, что $sgn\,(\sigma_{JI}) = (-1)^{|I|+|J|}$.

Задача 6.20. Убедитесь, что знак $\tau\eta\sigma_{JI}$ как подстановки из $\mathfrak{S}_n$ есть произведение знака σ_{JI} как элемента $\mathfrak{S}_n$, знака η как элемента $\mathfrak{S}_{n-k}$ и знака τ как элемента $\mathfrak{S}_k$.

Таким образом, выражение для $\det(A)$ можно переписать в виде:

$$\sum_J \sum_{\sigma \in \mathfrak{S}_{JI}} sgn\,(\sigma) a_{i_1\sigma(i_1)} a_{i_2\sigma(i_2)} \cdots a_{i_k\sigma(i_k)} a_{\widehat{\imath}_1\sigma(\widehat{\imath}_1)} a_{\widehat{\imath}_2\sigma(\widehat{\imath}_2)} \cdots a_{\widehat{\imath}_k\sigma(\widehat{\imath}_k)} =$$

$$= \sum_J \sum_{\tau \in \mathfrak{S}_k} \sum_{\eta \in \mathfrak{S}_{n-k}} (-1)^{|I|+|J|} sgn\,(\tau) sgn\,(\eta) a_{i_1 j_{\tau(1)}} a_{i_2 j_{\tau(2)}} \cdots a_{i_k j_{\tau(k)}} a_{\widehat{\imath}_1 \widehat{\jmath}_{\eta(1)}} a_{\widehat{\imath}_2 \widehat{\jmath}_{\eta(2)}} \cdots a_{\widehat{\imath}_{n-k} \widehat{\jmath}_{\eta(n-k)}} =$$

$$= \sum_J (-1)^{|I|+|J|} \left(\sum_{\tau \in \mathfrak{S}_k} sgn\,(\tau) a_{i_1 j_{\tau(1)}} a_{i_2 j_{\tau(2)}} \cdots a_{i_k j_{\tau(k)}} \right) \left(\sum_{\eta \in \mathfrak{S}_{n-k}} sgn\,(\eta) a_{\widehat{\imath}_1 \widehat{\jmath}_{\eta(1)}} a_{\widehat{\imath}_2 \widehat{\jmath}_{\eta(2)}} \cdots a_{\widehat{\imath}_{n-k} \widehat{\jmath}_{\eta(n-k)}} \right)$$

Последнее, по определению, совпадает с $\sum_J (-1)^{|I|+|J|} A_{IJ} A_{\widehat{I}\widehat{J}}$, что доказывает тождество (А).

Тождество (Б) следует из формулы (А), применённой к матрице, имеющей одинаковые строки (и стало быть, нулевой определитель). Точнее, пусть I и J — два разных мультииндекса одинаковой длины k. Тогда $I \neq I \cap J$ и $J \neq I \cap J$, но $\#\Big(J \setminus (I \cap J)\Big) = \#\Big(I \setminus (I \cap J)\Big)$. Модифицируем матрицу A, заменив в ней строки из набора $J \setminus (I \cap J)$ на строки из набора $I \setminus (I \cap J)$ (с сохранением порядка). Полученная в результате матрица A' имеет дублирующиеся строки, а значит, $\det(A') = 0$. С другой стороны, при любом K минор A'_{JK} совпадает с минором A_{IK}, а минор $A'_{\widehat{J}\widehat{K}}$ — с минорами $A_{\widehat{J}\widehat{K}}$ (ибо совпадают соответствующие подматрицы). Поэтому

$$\sum_K (-1)^{|I|+|K|} A_{IK} A_{\widehat{J}\widehat{K}} = (-1)^{|I|-|J|} \sum_K (-1)^{|J|+|K|} A_{IK} A_{\widehat{J}\widehat{K}} =$$

$$= (-1)^{|I|-|J|} \sum_K (-1)^{|J|+|K|} A'_{JK} A_{\widehat{J}\widehat{K}} = (-1)^{|I|-|J|} \det(A') = 0 .$$

□

4.2.1. Терминологические замечания. Минор $A_{\widehat{I}\widehat{J}}$ называется *дополнительным* к соответствующему минору A_{IJ}, а число $(-1)^{|I|+|J|}A_{\widehat{I}\widehat{J}}$ называется *алгебраическим дополнением* к минору A_{IJ}.

Если лексикографически упорядочить все мультииндексы длины k и рассмотреть $(\binom{n}{k} \times \binom{n}{k})$-матрицы $\Lambda^k(A)$ и $\widehat{\Lambda^k(A)}$, у которых в (IJ)-той клетке расположены, соответственно, минор A_{IJ} и его алгебраическое дополнение $(-1)^{|I|+|J|}A_{\widehat{I}\widehat{J}}$, то все соотношения Лапласа можно записать одной формулой

4.2.2. Следствие. *В кольце квадратных матриц размера $\binom{n}{k} \times \binom{n}{k}$ над произвольным коммутативным кольцом K выполнено тождество*

$$\Lambda^k(A) \cdot \widehat{\Lambda^k(A)}^t = \begin{pmatrix} \det(A) & & & 0 \\ & \det(A) & & \\ & & \ddots & \\ 0 & & & \det(A) \end{pmatrix} = \det(A) \cdot E\ , \tag{6-6}$$

где $A \in Mat_n(K)$ — произвольная матрица, а в правой части стоит диагональная матрица с элементами $\det(A)$ на главной диагонали.

□

Задача 6.21. Пользуясь равенством $\det(A) = \det(A^t)$ напишите формулу для разложения определителя по столбцам с номерами $(i_1, i_2, \ldots, i_k)$ и соответствующее тождество для умножения на чужие алгебраические дополнения.

Задача 6.22. Докажите, что если квадратная матрица имеет блочный вид

$$A = \begin{pmatrix} B & D \\ 0 & C \end{pmatrix}\ ,$$

где B, C — квадратные подматрицы (а 0 – нулевая подматрица), то $\det(A) = \det(B)\det(C)$.

Задача 6.23. Докажите, что если $AB = E$ (то есть матрицы A и B обратны друг другу), то $A_{IJ} = (-1)^{|I|+|J|}B_{\widehat{J}\widehat{I}}$, т. е. каждый минор матрицы A равен своему алгебраическому дополнению в матрице, транспонированной к B.

4.3. Присоединенная матрица. Наиболее часто формулы Лапласа используются в ситуации, когда $I = (i)$ – один индекс. В этом случае $A_{IJ} = a_{ij}$, где $(j) = J$, т. е. матрица из миноров $\Lambda^1(A)$ совпадает с самой матрицей A. Алгебраическое дополнение $A_{\widehat{i}\widehat{j}}$ к минору $A_{IJ} = a_{ij}$ есть определитель матрицы, которая получается из A вычеркиванием i-той строки и j-того столбца, умноженный на $(-1)^{i+j}$.

4.3.1. Следствие. (Формула для разложения определителя по строке.)

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} A_{\widehat{\imath j}}$$

для любого фиксированного $1 \le i \le n$.

□

4.3.2. Следствие. (Теорема об умножении на чужие дополнения.)

$$\sum_{j=1}^{n} (-1)^{i+j} a_{kj} A_{\widehat{kj}}$$

для любых фиксированных $i \ne k$, $1 \le i, k \le n$.

□

Задача 6.24. Получите аналогичные формулы для разложения по столбцу.

Матрица алгебраических дополнений $\Lambda^{\widehat{n-1}}(A) = \widehat{A} = (\widehat{a}_{ij})$ имеет $\widehat{a}_{ij} = (-1)^{i+j} A_{\widehat{\imath j}}$ и называется *присоединённой матрицей* матрицы A. Как и соотношения Лапласа, два редыдущих следствия можно записать одной матричной формулой, являющейюся специализацией формулы (6-6).

4.3.3. Следствие. (Теорема о присоединенной матрице.) *Над любым коммутативным кольцом* K *в кольце* $Mat_n(K)$ *выполнено тождество*

$$A \cdot \widehat{A}^t = \begin{pmatrix} \det(A) & & & 0 \\ & \det(A) & & \\ & & \ddots & \\ 0 & & & \det(A) \end{pmatrix} = \det(A) \cdot E\ , \qquad \forall\, A \in Mat_n(K)\ .$$

□

4.3.4. Следствие. (Критерий обратимости матрицы.) *Квадратная матрица* $A \in Mat_n(K)$ *над произвольным коммутативным кольцом* K *обратима тогда и только тогда, когда* $\det(A)$ *обратим в* K, *причём в этом слечае* $A^{-1} = \dfrac{1}{\det(A)} \widehat{A}^t$ *(где умножение матрицы* $\widehat{A}$ *на число* $\det(A)^{-1}$ *означает умножение каждого элемента матрицы на это число).*

□

4.3.5. Следствие. *Набор векторов* $(v_1, v_2, \ldots, v_n)$ *тогда и только тогда составляет базис в свободном модуле* K^n *над произвольным коммутативным кольцом* K, *когда определитель матрицы, составленной из координат векторов* v_i, *обратим в* K.

□

4.3.6. Следствие. *Пусть* V *— произвольный* K*-модуль, порождённый набором векторов* $(v_1, v_2, \ldots, v_n)$, *и* $\varphi\colon\ V \longrightarrow V$ *— произвольный эндоморфизм. Если действие* φ *на образующие происходит по правилу* $\varphi(v_j) = \sum_i a_{ij} v_i$, *т. е.*

$$(\,\varphi(v_1),\, \varphi(v_2),\, \ldots,\, \varphi(v_n)\,) = (v_1, v_2, \ldots, v_n) A\ , \qquad \text{где} \qquad A = (a_{ij})\ ,$$

то подмодуль $\det(A)\cdot V \overset{\text{def}}{=} \{\, w = \det(A)v \mid v\in V \,\}$ *содержится в образе* $\operatorname{im}(\varphi)$.

Доказательство. В самом деле, если $w = \det(A)\cdot v$ для некоторого $v = \sum\limits_{i=1}^{n} x_i v_i$, то

$$
\begin{aligned}
w &= (v_1, v_2, \dots, v_n)\cdot \begin{pmatrix} \det(A) & & & 0 \\ & \det(A) & & \\ & & \ddots & \\ 0 & & & \det(A) \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \\
&= (v_1, v_2, \dots, v_n)\cdot A \cdot \widehat{A}^t \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (\, \varphi(v_1),\, \varphi(v_2),\, \dots,\, \varphi(v_n)\,)\cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in \operatorname{im}(\varphi)\ ,
\end{aligned}
$$

где $(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_n)\widehat{A}$.
□

4.4. Тождество Гамильтона - Кэли. Пусть $A \in Mat_n(K)$ — произвольная квадратная матрица над коммутативным кольцом K. Координатный K-модуль K^n можно наделить структурой модуля над кольцом многочленов $K[t]$, полагая по определению, что результатом умножения столбца $v \in K^n$ на многочлен $c(t) = c_0 + c_1 t + \dots + c_d t^d$ является столбец

$$c(t)v \overset{\text{def}}{=} c_0 v + c_1 A v + c_2 A^2 v + \dots + c_d A^d v$$

(правую часть можно воспринимать как результат умножения столбца v на матрицу $c(A)$, полученную подстановкой в многочлен $c(t)$ значения $t = A$ из K-алгебры[8] $Mat_n(K)$).

Задача 6.25. Проверьте выполнения аксиом $K[t]$-модуля для K^n.

Задача 6.26. Проверьте, что умножения $\mu_t:\ v \longmapsto tv$ и $\mu_A:\ v \longmapsto Av$ являются гомоморфизмами $K[t]$-модулей.

Поскольку $K[t] \supset K$, как $K[t]$-модуль K^n будет по прежнему порождаться стандартными базисными столбцами $(e_1, e_2, \dots, e_n)$, однако над $K[t]$ они уже не будут линейно независимы, ибо $te_j = a_{1j}e_1 + a_{2j}e_2 + \dots + a_{nj}e_n$ для каждого $j = 1, 2, \dots, n$.

Из этих соотношений следует, в частности, что гомоморфизм $\alpha = \mu_t - \mu_A:\ K^n \longrightarrow K^n$, заданный правилом $v \overset{\alpha}{\longmapsto} tv - Av$, отображает каждую из образующих e_i, а значит, и весь модуль K^n в нуль. Из равенства $(\, \alpha(e_1),\, \alpha(e_2),\, \dots,\, \alpha(e_n)\,) = (e_1, e_2, \dots, e_n)(tE - A)$ (квадратная матрица $(tE - A)$ получается из $-A$ прибавлением t ко всем элементам главной диагонали) по Сл.4.3.6 вытекает, что умножение на на $\det(tE - A)$ также должно аннулировать K^n. Тем самым, справедливо

4.4.1. Предложение. (Тождество Гамильтона-Кэли.) *При подстановке матрицы A вместо переменной t в многочлен $\det(tE - A) \in K[t]$ получается нулевая матрица.*

---

[8] K-алгеброй называется любое кольцо, которое одновременно является K-модулем, причём кольцевые операции перестановочны с умножением на элементы из K. $Mat_n(K)$ имеет каноническую структуру K-модуля, в которой умножение матрицы на число есть умножение всех элементов матрицы на это число, и это умножение, очевидно, перестановочно с кольцевыми операциями в $Mat_n(K)$.

□

Многочлен $\chi_A(t) = \det(tE - A)$ называется *характеристическим многочленом* матрицы A. Поэтому тождество Гамильтона-Кэли часто формулируют словами: *над произвольным коммутативным кольцом всякая квадратная матрица аннулируется своим характеристическим многочленом.*

Задача 6.27. Пусть $\det(tE - A) = \sigma_0 t^n + \sigma_1 t^{n-1} + \cdots + \sigma_{n-1} t + \sigma_n$. Докажите, что $\sigma_0 = 1$, а при $1 \le k \le (n-1)$ коэффициент $(-1)^k \sigma_k$ равен сумме всех миноров k-того порядка, главная диагональ которых совпадает с главной диагональю A (такие миноры называются *главными*). В частности, $s_1 = -\sum\limits_{i=1}^{n} a_{ii}$ (величина $\mathrm{tr}\,(A) \stackrel{\mathrm{def}}{=} \sum\limits_{i=1}^{n} a_{ii}$ называется *следом* матрицы A) и $\sigma_n = (-1)^n \det(A)$.

Задача 6.28. Вычислите $\left.\dfrac{d}{dt}\right|_{t-0} \det(E + tA)$.

Задача 6.29. Проверьте, что матрицы A и $C^{-1}AC$ имеют одинаковые характеристические многочлены для любой обратимой матрицы $C \in Mat_n(K)$. Выведите отсюда, что если $V \xrightarrow{\varphi} V$ — эндомомрфизм свободного модуля V с базисом e_i, то характеристический многочлен матрицы Φ_e гомоморфизма φ в этом базисе в действительности от выбора базиса не зависит (он называется *характеристическим многочленом гомоморфизма* φ.

Лекция 7
Строение некоторых модулей

▷Прямые суммы ▷Фактор-модули ▷Разложение гомоморфизма ▷О сизигиях ▷Взаимные базисы ▷Инвариантные множители ▷Элементарные делители ▷Строение конечно порождённых модулей над кольцом главных идеалов ▷Строение конечно-порождённых абелевых групп ▷Целозначные многочлены

§1. Некоторые конструкции с модулями

1.1. Прямые суммы модулей. Прямая сумма модулей определяется аналогично прямой сумме колец. Если $V_1, V_2, \dots, V_m$ — некоторый набор K-модулей, то их *прямой суммой* называется модуль, обозначаемый

$$\bigoplus_{i=1}^{m} V_i = V_1 \oplus V_2 \oplus \cdots \oplus V_m$$

и состоящий из всевозможных наборов $(v_1, v_2, \dots, v_m)$, где $v_i \in V_i$, с покомпонентным сложением и умножением на числа:

$$\begin{aligned}(u_1, u_2, \dots, u_m) + (v_1, v_2, \dots, v_m) &\overset{\text{def}}{=} (u_1 + v_1\,,\ u_2 + v_2\,,\ \dots\,,\ u_m + v_m\,)\\ \lambda \cdot (v_1, v_2, \dots, v_m) &\overset{\text{def}}{=} (\lambda v_1, \lambda v_2, \dots, \lambda v_m)\end{aligned}$$

Задача 7.1. Проверьте, что прямая сумма K-модулей является K-модулем.

Говорят, что модуль V является *прямой суммой своих подмодулей*, $U_1, U_2, \dots, U_m \subset U$, если гомоморфизм сложения

$$\alpha\colon U_1 \oplus U_2 \oplus \cdots \oplus U_m \longrightarrow V : \quad (u_1, u_2, \dots, u_m) \longmapsto \sum u_i$$

является изоморфизмом. Это равносильно тому, что каждый вектор $v \in V$ допускает единственное разложение вида $v = \sum u_i$ с $u_i \in U_i$. Модуль, не представимый в виде прямой суммы своих собственных[1] подмодулей называется *неразложимым.*

[1] т. е. ненулевых и отличных от самого модуля

1.1.1. Лемма. *Для того чтобы модуль V распадался в прямую сумму двух своих подмодулей U и W необходимо и достаточно, чтобы подмодули U, W порждали V и пересекались только по нулевому вектору.*

Доказательство. Необходимость очевидна. Достаточность: то что U и W порождают V означает, что всякий $v \in V$ представим в виде $v = u + w$, а единственность такого представления вытекает из условия $U \cap W = 0$, ибо $v = u + w = u' + w'$ означает, что $u - u' = w - w' \in U \cap W$. □

1.1.2. Пример: свободный модуль K^n есть прямая сумма свободных модулей единичного ранга:

$$K^n = \underbrace{K \oplus K \oplus \cdots \oplus K}_{n} .$$

В частности, теорема о существовании базиса в векторном пространстве означает, что неразложимые модули над полем — это одномерные векторные пространства и только они.

1.1.3. Пример. Если число $m \in \mathbb{Z}$ разложено в произведение попарно взаимно простых множителей $m = q_1 q_2 \cdots q_s$, то построенный в лекции 2 изоморфизм колец

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \bigoplus_i (\mathbb{Z}/q_i\mathbb{Z})$$

задаёт заодно разложение $\mathbb{Z}$-модуля $\mathbb{Z}/m\mathbb{Z}$ в прямую сумму $\mathbb{Z}$-модулей $\mathbb{Z}/q_i\mathbb{Z}$.

> Задача 7.2. Вложите $\mathbb{Z}/q_i\mathbb{Z}$ в $\mathbb{Z}/m\mathbb{Z}$ в качестве подмодулей так, чтобы предыдущее разложение превратилось в разложение в прямую сумму *подмодулей*.

1.1.4. Пример: дополнительное подпространство. Если V — (конечномерное) векторное пространство над полем k, и $W \subset V$ — некоторое подпространство, то всегда можно (многими разными способами) подобрать подпространство $W' \subset V$, так чтобы $V = W \oplus W'$. Например, можно фиксировать какой-либо базис $(w_1, w_2, \dots, w_m)$ в W и как-то дополнить его (по Сл.3.7.6 из лек. 5) до базиса $(w_1, w_2, \dots, w_n)$ в V. После этого в качестве W' можно взять подпространство, порождённое последними $(n - m)$ базисными векторами $(w_{m+1}, \dots, w_n)$.

> Задача 7.3. Проверьте, что всякий вектор $v \in V$ действительно допускает единственное разложение $v = w + w'$ с $w \in W$, $w' \in W'$.

> Задача 7.4. Проверьте, что в качестве W' можно взять любое подпространство в V, удовлетворяющее условиям $W' \cap W = 0$ и $\dim W' + \dim W = \dim V$.

Подпространство $W' \subset V$, такое что $V = W \oplus W'$, называется *дополнительным подпространством* к W в V.

1.1.5. Пример-предупреждение. Если кольцо K не является полем, то *неверно* что всякий подмодуль W в K-модуле V имеет дополнительный подмодуль, даже в случае, когда $V = K^n$ – свободен. Например, подмодуль $W = 2\mathbb{Z} \subset \mathbb{Z}$ чётных чисел не имеет никакого дополнительного подмодуля $W' \subset \mathbb{Z}$. Действительно, как и всякий подмодуль в $\mathbb{Z}$, W' был бы тогда главным идеалом: $W' = d\mathbb{Z}$, и изоморфизм $\mathbb{Z} = W \oplus W'$ означал бы, что всякое целое число m *единственным способом* разложимо в сумму $m = 2x + dy$, что невозможно.

> Задача 7.5. Убедитесь, что представлений числа m в виде $m = 2x + dy$ либо нет вообще, либо бесконечно много.

Тем не менее, с парой $W \subset V$ всегда можно связать новый модуль, V/W называемый *фактор-модулем V по подмодулю W*. Этот модуль обладает многими интуитивными свойствами "дополнения" к W в в V, с той только разницей, что он не будет подмодулем в V, а будет "отдельно стоящим".

1.2. Факторизация K-модуля V по подмодулю $W \subset V$, опять-таки, аналогична факторизации кольца по идеалу. А именно, рассмотрим разбиение V на классы эквивалентности, относя два элемента $v_1, v_2 \in V$ в один класс $[v_1] = [v_2]$, если и только если их разность $(v_1 - v_2)$ лежит в W. Это действительно разбиение, ибо если классы $[v_1]$ и $[v_2]$ пересекаются по некоторому u, то $v_1 - u = w_1$ и $v_2 - u = w_2$ для каких-то $w_1, w_2 \in W$, и значит, $v_1 - v_2 = w_1 - w_2 \in W$, т. е. $[v_1] = [v_2]$. Класс $[v]$ называется *смежным классом элемента $v \in V$ по подмодулю W*. Два элемента v_1, v_2, лежащие в одном кдассе, называются *сравнимыми по подмодулю W*. Множество смежных классоы обозначается V/W и наделяется структурой K-модуля, инуцированной с V:

$$\begin{aligned} [v_1] + [v_2] &\stackrel{\text{def}}{=} [v_1 + v_2] \qquad \forall\, v_1, v_2 \in V \\ \lambda[v] &\stackrel{\text{def}}{=} [\lambda v] \qquad \forall\, \lambda \in K \ , \quad \forall\, v \in V \end{aligned}$$

Эти правила корректны, поскольку из равенств $[u_1] = [v_1]$, $[u_2] = [v_2]$ и $[u] = [v]$, означающих что $u_1 = v_1 + w_1$, $u_2 = v_2 + w_2$ и $u = v + w$, где w_1, w_2, $w \in V$, следует, что

$$\begin{aligned} u_1 + u_2 &= v_1 + v_2 + (w_1 + w_2) \equiv v_1 + v_2 \bmod (W) \\ \lambda u &= \lambda v + \lambda w \equiv \lambda v \bmod (W) \end{aligned}$$

Модуль V/W называется *фактор-модулем V по W*.

Задача 7.6. Проверьте выполнение аксиом модуля для V/W.

Задача 7.7. Проверьте, что каноническое отображение

$$\pi\colon V \longrightarrow V/W \ , \quad v \longmapsto [v]$$

является гомоморфизмом модулей (он называется *эпиморфизмом редукции по модулю W*).

Задача 7.8. Докажите, что фактор-множество модуля V по какому-либо разбиению тогда и только тогда корректно наследует модульную структуру с V, когда это разбиение является разбиением на смежные классы по некоторому подмодулю.

Подсказка: следуйте рассуждению из лекции 2 (т. е. убедитесь, что клясс $[0]$ — это подмодуль и т. д.).

1.3. Строение гомоморфизмов. Пусть $V \xrightarrow{\varphi} W$ — гомоморфизм модулей. Тогда имеется канонический изоморфизм $V/\ker(\varphi) \xrightarrow{\tilde{\varphi}} \mathrm{im}\,(\varphi)$, индуцированный гомоморфизмом φ, т. е. заданный правилом $v \bmod (\ker\varphi) \xmapsto{\tilde{\varphi}} f(v) \in W$. Это правило корректно, поскольку выбирая другой $u = v + w$ (где $\varphi(w) = 0$), мы получим $f(u) = f(v) + f(w) = f(v)$. Биективность $\tilde{\varphi}$ вытекает из равносильности условий $f(v_1) = f(v_2)$ и $f(v_1 - v_2) = 0$ (последнее, означает, что $v_1 \equiv v_2 \bmod (\ker\varphi)$). Мы доказали

1.3.1. Предложение. (Теорема о строении гомоморфизма модулей.) *Всякий гомоморфизм* $\varphi\colon V \longrightarrow W$ *может быть разложен в композицию*

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "\pi"'] & W \\ V/ker(\varphi) \arrow[r, "\tilde{\varphi}"] & \mathrm{im}\,(\varphi) \arrow[u, "\iota"'] \end{tikzcd} ,$$

где $V \xrightarrow{\pi} V/ker(f)$ *– канонический эпиморфизм редукции по модулю* $\ker(f)$, $\tilde{\varphi}$ *– изоморфизм, а* ι *– вложение.*

□

1.3.2. Пример: линейные уравнения. Пусть $Ax = b$ — система из m линейных уравнений от n неизвестных над кольцом K. Рассмотрим гомоморфизм $K^n \xrightarrow{\mu_A} K^m$, переводящий вектор-столбец $v \in K^n$ в вектор-столбец $Av \in K^m$. Система $Ax = b$ разрешима тогда и только тогда, когда $b \in \mathrm{im}\,\mu_A$, что равносильно тому, что столбец b лежит в линейной оболочке столбцов матрицы A (если $K = k$ – поле, то последнее означает, что *ранг расширенной матрицы системы равен рангу матрицы* A).

Если $b \in \mathrm{im}\,\mu_A$, то множество решений есть *полный прообраз* вектора b относительно μ_A, и стало быть, представляет собой смежный класс по подмодулю $\ker\mu_A$, т. е. имеет вид

$$\{\, x = c + w \,\} ,$$

где c – произвольное фиксированное решение системы $Ax = b$, а w пробегает множество решений однородной системы $Ax = 0$. Если модуль $\ker\mu_A$ свободен (например, если $K = k$ – поле), то выбирая в нём базис $(e_1, e_2, \dots, e_d)$, мы получаем для каждого решения единственное представление в виде $x = c + \lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_d e_d$, где c – какое-либо одно фиксированное решение системы $Ax = b$, а λ_i – произвольные постоянные.

1.3.3. Пример: сизигии. Всякий конечно порождённый K-модуль V является фактором свободного модуля. В самом деле, пусть V порождается набором векторов $(v_1, v_2, \dots, v_{n_0})$. Тогда отображение, переводящее стандартный базисный вектор $e_i \in K^{n_0}$ в вектор v_i можно продолжить по линейности до гомоморфизма модулей $K^{n_0} \xrightarrow{\varphi_0} V$. Поскольку v_i порождают V, получаем, что $V = K^{n_0}/\ker(\varphi_0)$. Подмодуль $\ker\varphi_o \subset K^{n_0}$ называется *модулем соотношений* или 0-*сизигий* между образующими v_i. Название связано с тем, что всякий элемент $\sum x_i e_i \in \ker\varphi_0$ соответствует линейной зависимости $\sum x_i v_i = 0$ в модуле V, и это соответствие, очевидно, биективно.

Если модуль соотношений $\ker\varphi_0$ также конечно порождён, то его тоже можно представить как образ сюрьективного гомоморфизма $K^{n_1} \xrightarrow{\varphi_1} \ker\varphi_0$ из свободного модуля, базисные векторы которого соответствуют *образующим соотношениям* между $v_i \in V$ (т. е. соотношениям, из которых вытекают все остальные соотношения). Ядро $\ker\varphi_1$ называется *модулем 1-сизигий* между образующими v_i. Интуитивно, 1-сизигии это “соотношения между соотношениями”.

Процедуру можно итерировать и далее, построив последовательность гомоморфизмов

$$\cdots \xrightarrow{\varphi_{k+1}} K^{n_k} \xrightarrow{\varphi_k} K^{n_{k-1}} \xrightarrow{\varphi_{k-1}} \cdots \xrightarrow{\varphi_2} K^{n_1} \xrightarrow{\varphi_1} K^{n_0} \xrightarrow{\varphi_0} V \to 0 ,$$

в которой каждый раз $\ker(\varphi_k) = \operatorname{im}(\varphi_{k+1})$. Этот модуль называется модулем k-сизигий. Если процесс оборвётся на m-том шагу, т. е. очередной гомоморфизм $K^{n_m} \xrightarrow{\varphi_m} \ker(\varphi_{m-1})$ окажется изоморфизмом (что ознаачает, что модуль $(n-1)$-сизигий свободен), то говорят что исходный модуль V имел *когомологическую размерность* $\leq m$. Когомологическая размерность измеряет, таким образом, насколько данный модуль V далёк от свободного модуля.

1.4. Факторизация прямых сумм. Факторизация согласована с взятием прямых сумм в следующем смысле.

1.4.1. Предложение. *Пусть в каждом из модулей $(V_1, V_2, \dots, V_m)$ задано по подмодулю $W_i \subset V_i$, $i = 1, 2, \dots, m$. Тогда $W = \bigoplus\limits_i W_i$ — подмодуль в $V = \bigoplus\limits_i V_i$ и $V/W = \bigoplus\limits_i (V_i/W_i)$.*

Доказательство. То, что наборы вида $(w_1, w_2, \dots, w_m)$ составляют подмодуль в V, — очевидно. Легко видеть, что отображение $\alpha\colon V/W \longrightarrow \bigoplus\limits_i (V_i/W_i)$:

$$(v_1, v_2, \dots, v_m) \bmod W \longmapsto \Big(v_1(\bmod W_1),\ v_2(\bmod W_2),\ \dots,\ v_m(\bmod W_m)\Big)\,.$$

является корректно определённым эпиморфизмом с нулевым ядром.

Задача 7.9. Проверьте это.

□

1.4.2. Следствие. *Свободные модули K^m и K^n над произвольным коммутативным кольцом K изоморфны только при $k = m$.*

Доказательство. Пусть $V = K^n$, $W = K^m$, и пусть $\alpha\colon V \longrightarrow W$ — изоморфизм. Рассмотрим какой-нибудь максимальный идеал $\mathfrak{m} \subset K$, так что фактор-кольцо $k = K/\mathfrak{m}$ является полем. Ясно, что α отождествляет подмодуль $\mathfrak{m}V = \{\, w = \lambda v \mid \lambda \in \mathfrak{m}, v \in V \,\} \subset V$ с аналогичным подмодулем $\mathfrak{m}W \subset W$, и стало быть, индуцирует изоморфизм фактор-модулей $V/\mathfrak{m}V \xrightarrow{\sim} W/\mathfrak{m}W$.

Задача 7.10. Пусть V – произвольный K-модуль и $\mathfrak{q} \subset K$ – любой идеал. Убедитесь, что $\mathfrak{q}V$ является подмодулем в V и что правило

$$\lambda \bmod (q) \cdot v \bmod (qV) \overset{\text{def}}{=} \lambda v \bmod (qV)$$

корректно задаёт на $V/\mathfrak{q}V$ структуру модуля над кольцом $K/\mathfrak{q}$.

Поскольку $V = \underbrace{K \oplus K \oplus \dots \oplus K}_{n}$, имеем $\mathfrak{m}V = \mathfrak{m}K \oplus \mathfrak{m}K \oplus \dots \oplus \mathfrak{m}K = \mathfrak{m} \oplus \mathfrak{m} \oplus \dots \oplus \mathfrak{m}$, и по предыдущему предложению $V/\mathfrak{m}V = \underbrace{K/\mathfrak{m}K \oplus K/\mathfrak{m}K \oplus \dots \oplus K/\mathfrak{m}K}_{n} = k^n$ является n-мерным векторным пространством над полем k. Аналогично, $W/\mathfrak{m}W = k^m$. Поскольку α индуцирует отождествление этих пространств, должно выполняться равенство $n = m$.

□

Задача 7.11. Пусть U — подмодуль в V, а W — подмодуль в U. Убедитесь, что W является подмодулем в V и что U/W можно рассматривать как подмодуль в V/W. Постройте изоморфизм $\big(V/W\big)/\big(U/W\big) \xrightarrow{\sim} V/U$.

§2. Конечно порождённые модули над кольцом главных идеалов

2.1. Некоторые напоминания. Всюду в этом параграфе мы будем предполагать, что K — это кольцо главных идеалов, т. е. целостное коммутативное кольцо с единицей, каждый идеал $I \subset K$ в котором имеем вид $I = (d) = dK$ для некоторого $d \in K$. Основными модельными примерами для нас будут случаи $K = \mathbb{Z}$ и $K = k[x]$, где k – поле. Читателю настоятельно рекомендуется отдельно проговаривать все формулировки и доказательства в конкретных терминах этих колец.

Образующая d идеала $\mathfrak{I}$ называется *наибольшим общим делителем* элементов этого идеала и обозначается *НОД* $(\mathfrak{I})$. Напомню (см. лекции 2, 3), *НОД* $(\mathfrak{I})$ определяется идналом $\mathfrak{I}$ однозначно с точностью до умножения на обратимые элементы кольца[2]. В лекции 3 мы видели, что всякое кольцо главных идеалов нётерово и факториально. Из первого вытекает, в частности

2.1.1. Следствие. *Псякое множество идеалов в кольце главных идеалов содержит по меньшей мере один идеал, не содержащийся (строго) ни в каком другом идеале из этого множества.*

□

Второе же означает, что в кольце главных идеалов каждый элемент m допускает разложение на простые множители
$$m = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s} ,$$
в котором $p_1, p_2, \dots, p_s$ – попарно неассоциированные простые (= неприводимые) элементы кольца и неупорядоченная совокупность степеней $p_\nu^{d_\nu}$ определяются по m однозначно с точностью до умножения любого p_i на обратимый элемент кольца K.

2.2. Теорема. (Теорема о взаимных базисах) *Пусть $U \subset V$ — произвольный подмодуль в свободном K-модуле $V \simeq K^n$. Тогда U тоже свободен, и существуют такие базисыв $(u_1, u_2, \dots, u_r)$ в U и $(v_1, v_2, \dots, v_n)$ в V, что $u_i = m_i v_i$, $1 \le i \le r$, для некоторых $m_i \in K$, таких что m_i делит m_j при $i < j$.*

Терминологическое замечание. Базисы, о которых идёт речь в теореме, называются *взаимными базисами* модуля V и подмодуля U, а числа m_i называются *инвариантными множителями* подмодуля U.

Доказательство. Индукция по n. При $n = 1$ теорема в утверждает в точности то, что K является кольцом главных идеалов.

Пусть $n \ge 2$ и $e = (e_1, e_2, \dots, e_n)$ – какой-либо базис в V. Подмножество $I(e) \subset K$, состоящее из первых координат всевозможных векторов $u \in U$ в базисе e является идеалом в K (проверьте!). Пусть $f = (f_1, f_2, \dots, f_n)$ – такой базис в V, что идеал $I(f)$ не содержится в качестве собственного подмножества ни в одном из идеалов семейства $I(e)$, где e пробе-

[2] в $\mathbb{Z}$ и $k[x]$ этот произвол можно устранить требуя чтобы *НОД* был неотрицательным числом или соответственно приведённым многочленом.

гает все базисы V (существование f гарантировано предыдущим следствием). Пусть m_1 — образующая идеала $I(f)$, и пусть это m_1 служит первой координатой вектора $u_1 \in U$.

Заметим, что все координаты вектора u_1 в базисе f делятся на m_1. В самом деле, если, скажем, вторая координата x вектора $u_1 = m_1 f_1 + x f_2 + \cdots$ не лежит в идеале $(m_1) = I(f)$, то идеал $I(f')$, построенный по базису

$$f' = (f_2, (f_1 + f_2), f_3, f_4, \ldots, f_n) ,$$

будет (вопреки выбору f) строго содержать $I(f)$, поскольку первая координата вектора $xf_2 - u_1$ будет равна m_1, а первая координата вектора u_1 будет равна $x - m_1 \notin (m_1)$ (обязательно проверьте!).

Таким образом, $u_1 = m_1 v_1$ для некоторого $v_1 \in V$. Подчеркнём, что первая координата вектора v в базисе f равна 1, и обозначим через V' свободный подмодуль ранга $(k-1)$, порождённый векторами $f_2, f_3, \ldots, f_n$, а через U' – пересечение $V' \cap U$. Я утверждаю, что $V = Kv_1 \oplus V'$ и $U = Ku_1 \oplus U'$.

Первое следует из того, что подмодули Kv_1 и V' пересекаются только по нулю (ибо вектор вида xv_1 в разложении по базису f содержит xf_1, а стало быть лежит в V' лишь при $x = 0$) и порождают V (ибо всякий $v = \sum x_i f_i = x_1 v_1 + v'$ с $v' \in V'$).

Второе устанавливается аналогично: очевидно, что $Ku_1 \cap U' = 0$, а u_1 и U' порождают U потому, что первая координата всякого $u \in U$ в базисе f делится на первую координату вектора u_1 (по определению $I(f)$, f и u_1), и значит, может быть обнулена вычитанием из u подходящего кратного u_1.

Применяя к $U' \subset V'$ предположение индукции, мы можем построить для этих модулей взаимные базисы $(u_2, \ldots, u_r)$ и $(v_2, \ldots, v_n)$ с $u_i = m_i v_i$ при $i = 2, \ldots, r$, где $r' \leq (n-1)$ и целые числа m_i таковы, что m_i делит m_j при $i < j$. Добавляя к этим базисам построенные выше v_1 и $u_1 = m_1 v_1$ мы получим базисы в исходных модулях U и V и для проверки того, что они будут взаимными нам остаётся только показать, что все m_i с $i \geq 2$ делятся на m_1.

Для этого покажем сначала, что *все* координаты *всех* векторов $u' \in U'$ в базисе f делятся на m_1. Действительно, пусть, к примеру, координата x вектора $u' = xf_2 + \cdots$ не лежит в идеале $(m_1) = I(f)$ и пусть $u_1 = m_1 f_1 + y f_2 + \cdots$. Тогда идеал $I(f'')$, построенный по базису

$$f'' = (f_2, (f_1 + f_2), f_3, f_4, \ldots, f_n) ,$$

опять-таки, будет строго содержать $I(f)$, поскольку первая координата вектора $yf_2 - u_1$ будет равна m_1, а первая координата вектора u' будет равна $x \notin (m_1)$ (обязательно проверьте!).

Заметим теперь, что каждое m_i есть координата вектора u_i в базисе $(v_1, v_2, \ldots, v_n)$, а потому является k-линейной комбинацией координат вектора u_i в базисе f (при замене базиса столбец координат умножается на матрицу перехода). Так как последние делятся на m_1, мы получаем, что m_i также делится на m_1.

□

Задача 7.12. Убедитесь, что приведённое только что рассуждение по-существу дублирует доказательство теоремы о приведении матрицы к строгому ступенчатому виду.

Задача 7.13. Докажите такой вариант теоремы о ранге матрицы: пусть A – матрица размера $m \times n$ над кольцом главных идеалов K; тогда ее столбцы порождают свободный подмодуль в K^m, а строки — свободный подмодуль в K^n, причём ранги этих подмодулей совпадают и равны числу ненулевых диагональных элементов, возникающих в результате приведения матрицы A к строгому диагональному виду элементарными преобразованиями строк и столбцов.

2.3. Теорема. (Теорема об инвариантных множителях.) *Каждый из инвариантных множителей $m_i \in K$ в предыдущей теореме однозначно с точностью до умножения на обратимый элемент кольца K определяется самими модулями U и V, и не зависит от выбора взаимных базисов.*

Доказательство. Пусть $\{v_1, v_2, \ldots, v_n\} \subset K^n$ и $\{u_1, u_2, \ldots, u_r\} \subset U \subset K^n$ — какая-то пара взаимных базисов, так что $u_i = m_i v_i$, $m_i \in K$. Мы дадим независящее от выбора взаимных базисов описание для каждого из произведений

$$M_i = m_1 m_2 \ldots m_i \quad , \qquad 1 \le i \le r$$

(тем самым, $m_i = M_i / M_{i-1}$ тоже будут описаны инвариантно).

Для каждого набора $w = \{w_1, w_2, \ldots, w_i\} \subset U$ из i векторов и каждого базиса $e = (e_1, e_2, \ldots, e_n)$ модуля V обозначим через $C_i(e, w) \in Mat_i(K)$ матрицу, j-тый столбец которой сотоит из первых i координат вектора w_j в базисе e, и положим $D_i(e, w) = \det(C_i(e, w)) \in K$ (при $i = 1$ $C_1(e, w) = D_1(e, w)$ — это в точности первая координата вектора $w = w_1$ в базисе e). Матрица $C_i(e, w)$ есть подматрица, составленная из верхних i строк матрицы перехода C_{ew}, которая, напомню, имеет размер $(n \times i)$ и однозначно определяется равенством

$$(w_1, w_2, \ldots, w_i) = (e_1, e_2, \ldots, e_n) C_{ew} \, .$$

Отметим, что $M_i = D_i(v, u)$, где $(v, u) = \big((v_1, v_2, \ldots, v_n) , \ (u_1, u_2, \ldots, u_i) \big)$ происходит из зафиксированных выше взаимных базисов. Инвариантная характеризация M_i состоит в том, что M_i *является наибольшим общим делителем всех чисел $D_i(e, w)$ по всем w, e*. Чтобы доказать это, нам остаётся проверить, что M_i делит каждое из чисел $D_i(e, w)$.

Пусть произвольный набор $(w_1, w_2, \ldots, w_i)$ векторов подмудуля U раскладывается по векторам из зафиксированных выше взаимных базисов по формулам

$$w_j = \sum_{\alpha=1}^{r} c_{\alpha j} u_\alpha = \sum_{\alpha=1}^{r} m_\alpha c_{\alpha j} v_\alpha \, .$$

Если для любого вектора $g \in V$ обозначить через $g^{(i)} \in K^i$ вектор-столбец высоты i, состоящий из первых i координат вектора g относительно произвольно выбранного базиса $(e_1, e_2, \ldots, e_n)$ в V, то согласно предыдущей формуле, j-тый столбец матрицы $C_i(e, w)$ можно представить в виде линейной комбинации $w_j^{(i)} = \sum\limits_{\alpha=1}^{r} m_\alpha c_{\alpha j} v_\alpha^{(i)}$, откуда пользуясь полилинейностью и кососимметричностью определителя получаем

$$D_i(e, w) = \det(w_1^{(i)}, w_2^{(i)}, \ldots, w_i^{(i)}) =$$

$$\sum_{1\le\alpha_1<\alpha_2<\cdots<\alpha_i\le r}\ \sum_{\sigma\in\mathfrak{S}_i} sgn\,(\sigma) m_{\alpha_{\sigma(1)}} m_{\alpha_{\sigma(2)}} \cdots m_{\alpha_{\sigma(i)}} \cdot c_{\alpha_{\sigma(1)}j} c_{\alpha_{\sigma(2)}j} \cdots c_{\alpha_{\sigma(i)}j} \cdot \det\left(v^{(i)}_{\alpha_1}, v^{(i)}_{\alpha_2}, \dots, v^{(i)}_{\alpha_i}\right).$$

Так как m_α делит m_β при $\alpha<\beta$, каждое слагаемое суммы делится на $M_i = m_1 m_2 \cdots m_i$, что и требовалось.

□

Задача 7.14. Докажите, что две прямоугольные матрицы одинакового размера над кольцом главных идеалов тогда и только тогда приводятся к одинаковому строгому диагональному виду элементарными преобразованиями строк и столбцов, когда при всех k у этих матриц совпадает наибольший общий делитель всех миноров k-того порядка.

2.4. Элементарные делители. Пусть теперь $(m_1, m_2, \dots, m_r)$ – упорядоченная последовательность элементов кольца, в которой m_i делит m_j при $i<j$. Если разложить каждый из них на простые множители

$$m_i = p_{i_1}^{d_{i_1}} p_{i_2}^{d_{i_2}} \cdots p_{i_{s_i}}^{d_{i s_i}} ,$$

то исходная упорядоченная последовательность $(m_1, m_2, \dots, m_r)$ будет однозначно восстанавливаться по неупорядоченному набору, полученному *дизъюнктным объединением* всех степеней p^d из всех этих разложений (дизъюнктность означает, что каждая степень присутствует в итоговом неупорядоченном наборе столько раз, сколько она появляется во всевозможных разложениях). В самом деле, все степени одного и того же простого элемента p из итогового набора можно выстроить в ряд так, чтобы показатели монотонно невозрастали слева направо. Тогда первый слева элемент этого ряда входит в разложение числа m_r, второй – в разложение m_{r-1} и т. д. пока ряд не кончится. В результате мы однозначно восстанавливаем разложение каждого m_i в отдельности. Нами доказана

2.4.1. Лемма. *Произвольный набор (возможно повторяющихся) степеней p^d простых элементов возникает из единственной последовательности $(m_1, m_2, \dots, m_r)$, в которой m_i делит m_j при $i<j$, как дизъюнктное объединение всех степеней простых элементов, входящих в разложения m_i на простые множители.*

□

В ситуации, когда набор $(m_1, m_2, \dots, m_r)$ является набором инвариантных множителей подмодуля U в свободном модуле V, соответствующее ему дизъюнктное объединение степеней простых сомножителей p^d, входящих в разложения m_i, называется *набором элементарных делителей* подмодуля U в свободном модуле V.

2.5. Теорема. *Всякий конечно порождённый модуль V над кольцом главных идеалов K допускает конечное разложение вида*

$$V = K^n \oplus \bigoplus_\nu \frac{K}{p_\nu^{d_\nu} K} \tag{7-1}$$

где $p_\nu \in K$ – простые элементы. Число n и совокупность степеней $p_\nu^{s_\nu}$ не зависят (с точностью до умножения p_ν на обратимые элементы кольца) от способа разложения[3] *и определяются*

[3]таких способов, разумеется, много: например способов представить свободный модуль V в виде $V = K^n$ имеется столько же, сколько базисов в V

модулем V однозначно.

Доказательство. Пусть V порождается элементами $e_1, e_2, \dots, e_N$. Тогда $V = K^N/\ker(\varphi)$, где $K^N \xrightarrow{\varphi} V$ — эпиморфизм, переводящий стандартный базис координатного модуля K^N в образующие e_i. Выберем в $\ker(\varphi) \subset K^N$ взаимные базисы $\{u_1, u_2, \dots, u_r\}$ и $\{v_1, v_2, \dots, v_N\}$, где $u_i = m_i v_i$. В этих базисах

$$V = \underbrace{\frac{K \oplus K \oplus \cdots \oplus K \oplus K \oplus \cdots \oplus K}{m_1 K \oplus m_2 K \oplus \cdots \oplus m_r K \oplus 0 \oplus \cdots \oplus 0}}_{N} = \frac{K}{(m_1)} \oplus \frac{K}{(m_2)} \oplus \cdots \frac{K}{(m_r)} .$$

Раскладывая каждый из инвариантных множителей m_i в произведение степеней простых элементов $m_i = p_{i_1}^{d_{i_1}} p_{i_2}^{d_{i_2}} \cdots p_{i_{s_i}}^{d_{i_{s_i}}}$ по китайской теореме об остатках (см. с Сл.1.6.2 лекции 3), получаем дальнейшее разложение

$$\frac{K}{(m_i)} = \frac{K}{(p_{i_1}^{d_{i_1}})} \oplus \frac{K}{(p_{i_2}^{d_{i_2}})} \oplus \cdots \frac{K}{(p_{i_{s_i}}^{d_{i_{s_i}}})} .$$

Это доказывает существование разложения.

Для доказательства единственности отметим прежде всего несколько следствий из факта существования разложения (7-1).

2.5.1. Следствие. *Всякий конечно порождённый модуль над кольцом главных идеалов является прямой суммой свободного модуля и подмодуля кручения*[4].

□

2.5.2. Следствие. *Всякий конечно порождённый модуль без кручения над кольцом главных идеалов свободен.*

□

Из этого следствия сразу же вытекает, что число n в (7-1) однозначно определяется по модулю V как ранг свободного модуля $V/\mathit{Tors}(V)$.

Если p и q — простые неассоциированные элементы, то p^k взаимно-прост с q^d, а стало быть, обратим в $K/(q^d)$, и значит, гомоморфизм $K/(p^d) \xrightarrow{\mu_{p^k}} K/(p^d)$ умножения на p^k в модуле $K/(p^d)$ является изоморфизмом. Напротив, гомоморфизм μ_{p^k} в модуле $K/(p^d)$ тождественно нулевой, если $k \geq d$, и $\ker \mu_{p^k} = p^{d-k} K/(p^d)$, если $k < d$. Таким образом, прямая сумма всех слагаемых из (7-1) вида $K/(p^s)$ с $s \leq d$ инвариантно характеризуется как множество всех векторов, которые аннулируются умножением на p^d. Но тогда число слагаемых вида $K/(p^s)$ с фиксированным s есть логарифм по модулю p^s от числа элементов в фактор модуле $\dfrac{\ker \mu_{p^s}}{\ker \mu_{p^{s-1}}}$, где через $V \xrightarrow{\mu_\alpha} V$ мы на этот раз обозначаем гомоморфизм умножения на α в модуле V.

Теорема доказана.

□

[4]напомню, что подмодуль кручения $\mathit{Tors}(V) = \{\, v \neq 0 \mid \exists \lambda \neq 0 : \lambda v - 0 \,\}$

2.6. Пример: конечно порождённые абелевы группы. При $K = \mathbb{Z}$ предыдущая теорема утверждает, что всякая конечно порождённая абелева группа изоморфна

$$\mathbb{Z}^n \oplus \bigoplus_{\nu} \frac{\mathbb{Z}}{p_\nu^{d_\nu}\mathbb{Z}} \;,$$

где $\mathfrak{p}_\nu$ – простые числа, и две группы такого вида изоморфны, если и только если совпадают числа n и наборы степеней $p_\nu^{d_\nu}$.

Если абелева группа задана в терминах образующих и соотношений, т. е. в виде K^N/R, где модуль соотношений $R \subset K^N$ также задан образующими соотношениями $(r_1, r_2, \ldots, r_k)$, то для определения её канонического разложения в прямую сумму циклических фактор-групп можно воспользоваться явными процедурами из доказательств предыдущих теорем, а именно, составить из вектор-столбцов r_i прямоугольную матрицу, элементарными преобразованиями строк и столбцов привести её к строгому диагональному виду, тогда числа $(m_1, m_2, \ldots, m_r)$, стоящие на диагонали, будут не чем иным как инвариантными множителями подмодуля соотношений R, и набор их элементарных делителей будет совпадать с набором знаменателей, участвующих в каноническом разложении (а n будет равно $N - r$),

Разумеется, на практике часто удаётся избежать полномасштабного вычисления по только что описанному алгоритму и найти базис $\mathbb{Z}$-модуля используя специфику его изначального определения.

2.6.1. Пример: базис в модуле целозначных многочленов. Целозначными называются такие многочлены из $\mathbb{Q}[x]$, которые принимают целые значения при целых значениях x. Поскольку сумма двух целозначных многочленов и целое кратное целозначного многочлена также будут целозначными, эти многочлены образуют $\mathbb{Z}$-модуль. Отметим, что коэффициенты целозначного многочлена вовсе не обязаны быть целыми, как показывает пример многочлена $T(x) = x(x+1)/2$, задающего треугольные числа. Мы собираемся доказать, что *многочлены*

$$b_i(x) = \frac{1}{i!} x(x-1)\ldots(x-i+1) \quad , \qquad i = 0, 1, 2, \ldots$$

(при $i = 0$ мы считаемем $b_i(x) \equiv 1$) составляют базис модуля целозначных многочленов над $\mathbb{Z}$.

Для этого заметим прежде всего, что многочлены $b_i(x)$ составляют базис векторного пространства $\mathbb{Q}[x]$ над полем $\mathbb{Q}$.

Задача 7.15. Докажите это (ср. с зад.5.21).

Стало быть, любой многочлен g степени $\le n$ допускает разложение

$$g(x) = \sum_{i=0}^{n} \lambda_i b_i(x)$$

с рациональными коэффициентами λ_i. Покажем, что если $g(x)$ – целозначен, то эти коэффициенты обязаны быть целыми.

Для этого рассмотрим линейный гомоморфизм

$$\nabla \;:\; f(x) \longmapsto \nabla f(x) \stackrel{\text{def}}{=} f(x) - f(x-1) \;.$$

Он переводит целозначные многочлены в целозначные и действует на базисные многочлены $b_i(x) = \binom{x+i}{i}$ по правилу

$$\nabla b_i(x) = \binom{x+i}{i} - \binom{x+i-1}{i} = \binom{x+i-1}{i-1} = b_{i-1}(x) \,.$$

Поскольку $b_i(0) = \begin{cases} 1\,, & \text{при} \quad i=0 \\ 0\,, & \text{при} \quad i>0 \end{cases}$, мы заключам, что

$$\lambda_i = \underbrace{\nabla\nabla\cdots\nabla}_{i}\, g\,(0) \,\in\, \mathbb{Z}\,,$$

что и требовалось.

Задача 7.16. Докажите, что многочлены

$$c_i^n(x) \stackrel{\text{def}}{=} \binom{x+i+n}{n} = \frac{1}{n!}(x+i)(x+i+11)...(x+i+n)\,,$$

с $i = 0,\, 1,\, \ldots,\, n$ составляют базис модуля целозначных многочленов степени $\leq n$ над $\mathbb{Z}$.

Лекция 8
Алгебраические функции

▷Лексикографическое упорядочение мономов ▷Формулы Виета ▷Разложение на множители результанта и дискриминанта ▷Базисы в модуле симметрических многочленов ▷Основная теорема о симметрических функциях ▷Рациональные функции ▷Разложение на простейшие дроби ▷Поле частных ▷Ряды Лорана и дробно-степенные ряды ▷Разложение неявной алгебраической функции в формальный дробно-степенной ряд

Функции, как правило, задаются алгебраическими формулами. При работе с такими функциями возникают два вопроса: первый – как определить значение функции в точке, или более общо, как придать смысл высказыванию: "такая-то алгебраическая формула определяет нам функцию"; второй – как с такими формулами производить вычисления, то есть устанавливать для таких функций те или иные тождества. Первое поле деятельности традиционно относится к анализу, а второе - к алгебре. Ближайшие две лекции мы будем заниматься именно этой второй задачей — обсудим как производить вычисления над функциями (образующими, как правило, некую стандартную алгебраическую структуру), и установим ряд классических соотношений.

§1. Многочлены от многоих переменных

В этом пункте мы применим векторную машинерию к тому, чтобы систематизировать наши представления о $K[x_1, x_2, \dots, x_n]$ как о K-модуле. Кольцо K теперь будет произвольным коммутативным кольцом с единицей.

1.1. Упорядочение мономов. Базис в K-модуле $K[x_1, x_2, \dots, x_n]$ составляют (по определению многочленов) всевозможные мономы $x_1^{d_1}, x_2^{d_2}, \dots, x_n^{d_n}$. Целое неотрицательное число $|d| \overset{\text{def}}{=} \sum_i d_i$ называется *степенью* монома, а сам набор $d = (d_1, d_2, \dots, d_n)$ – *мультистепенью*. Мы часто будем сокращать запись $x_1^{d_1}, x_2^{d_2}, \dots, x_n^{d_n}$ до x^d. При этом удобно представлять себе $d = (d_1, d_2, \dots, d_n)$ как вектор, лежащий в первом координатном октанте решётки $\mathbb{Z}^n$.

Выше мы привыкли иметь дело с базисами, векторы в которых линейно упорядочены: $e_1, e_2, \dots$. Линейная упорядоченность базисных векторов необходима, к например, для того чтобы записывать гомоморфизмы матрицами. На множестве наборов $d = (d_1, d_2, \ldots, d_n)$ имеется стандартный линейный порядок, который называется *лексикографическим*, ибо основан на том же принципе, что и расположение слов в словаре: мультистепень $a = (a_1, a_2, \ldots, a_n)$ называется *лексикографически большей*, чем мультистепень $b = (b_1, b_2, \ldots, b_n)$, если для некоторого i имеем $a_\nu = b_\nu$ при $\nu < i$, но $a_i > b_i$. В этом случае мы будем писать $a > b$.

Задача 8.1. Убедитесь, что мы действительно определили на множестве мультистепеней отношение полного линейного порядка (т. е. проверьте, что $\forall a, b$ имеются в точности 3 взаимо исключающие возможности: $a < b$, $a = b$, $b < a$, что из неравенств $a > b$ и $b > c$ следует неравенство $a > c$ и что в каждом непустом множестве мультииндексов есть наименьший элемент).

1.1.1. Пример: однородные многочлены степени d — это многочлены, каждый моном которых имеет степень d. Они составляют свободный подмодуль в $K[x_1, x_2, \ldots, x_n]$ ранга $\binom{d+n-1}{n}$ (почему?). Лекикографически старшим мономом в этом модуле является x_1^d, а лексикографически младшим - моном x_n^d.

Задача 8.2. Докажите, что $f \in K[x_1, x_2, \ldots, x_n]$ тогда и только тогда однороден степени d, когда в кольце $K[t, x_1, x_2, \ldots, x_n]$ выполнено равенство $f(tx_1, tx_2, \ldots, tx_n) = tf(x_1, x_2, \ldots, x_n)$.

Задача 8.3. (Теорема Эйлера об однородных функциях.) Докажите, что $f \in K[x_1, x_2, \ldots, x_n]$ тогда и только тогда однороден степени d, когда в кольце $K[x_1, x_2, \ldots, x_n]$ выполнено равенство $\sum\limits_{i=1}^{n} \dfrac{\partial f}{\partial x_i} = d \cdot f$ (через $\dfrac{\partial f}{\partial x_i}$ обозначается производный многочлен от $f(x_1, x_2, \ldots, x_n)$, рассматриваемого, как многочлен от x_i с коэффициентами из кольца многочленов от остальных переменных).

1.2. Сравнение соответственных мономов. Наличие линейного порядка на мономах позволяет распространить на кольцо $K[x_1, x_2, \ldots, x_n]$ стандартные свойства умножения в $K[x]$.

Задача 8.4. Убедитесь, что старший и младший мономы в произведении равны, соответственно, произведениям старших и младших мономов сомножителей.

В частности, отсюда следует, что в $K[x_1, x_2, \ldots, x_n]$ не будет делителей нуля, если их не было в K, и что обратимыми элементами в $K[x_1, x_2, \ldots, x_n]$ являются обратимые константы и только они.

При доказательстве различных тождеств часто очень эффективным оказывается *сравнение старших членов*. Стандартная схема такова. Допустим, что нам надо разложить многочлен f на множители, и мы из каких-то соображений знаем, что f делится на многочлены $g_1, g_2, \ldots, g_k$. Тогда, если старший моном у произведения $g_1 g_2 \cdots g_k$ имеет ту же мультистепень, что и старший моном в f, то $f = c \cdot g_1 g_2 \cdots g_k$, где $c \in K$ – константа, и для нахождения точного значения c, опять же, достаточно сравнить лишь коэффициенты при старших мономах.

1.2.1. Пример: определитель ван дер Монда

$$\det\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \prod_{i>j}(x_i - x_j) \quad .$$

Действительно, обе части являются элементами $\mathbb{Z}[\,x_1, x_2, \dots, x_n\,]$, причём левый многочлен делится на правый, ибо он делится на каждый из попарно взаимно простых линейных двучленов $(x_i - x_j)$ (чтобы убедиться в этом надо отнять из i-того столбца j-тый и вынести $(x_i - x_j)$ из каждогой разности $x_i^k - x_j^k$). Остаётся заметить, что старшие мономы слева и справа одинаковы – это $(-1)^{\frac{n(n-1)}{2}} x_1^{n-1} x_2^{n-2} x_3^{n-3} \cdots x_{n-1}$.

Задача 8.5. Убедитесь в этом!

1.3. Формулы Виета. Пусть $\{x_1, x_2, \dots, x_n\}$ – корни многочлена $f(t) = a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n \in K[t]$, где K – произвольное коммутативное кольцо. Тогда, как мы знаем, $f(t)$ делится на произведение $(t - x_1)(t - x_2) \cdots (t - x_n)$, и сравнивая старшие степени t, мы получаем разложение:

$$a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n = a_0 (t - x_1)(t - x_2) \cdots (t - x_n) \ ,$$

которое позволяет выразить коэффициенты $a_1, a_2, \dots, a_n$ через a_0 и корни $x_1, x_2, \dots, x_n$. Действительно, сравнивая коэффициент при t^{n-k}, мы получаем

1.3.1. Предложение. (Теорема Виета.)

$$a_k = (-1)^k a_0 e_k(x_1, x_2, \dots, x_n) \ ,$$

где $e_k(x_1, x_2, \dots, x_n) \stackrel{\text{def}}{=} \sum\limits_{1 \le \nu_1 < \nu_2 < \dots < \nu_k \le n} x_{\nu_1} x_{\nu_2} \cdots x_{\nu_n}$ *есть сумма всех возможных произведений из k попарно разных переменных ($k = 1, 2, \dots, n$).*

□

Многочлены $e_k(x_1, x_2, \dots, x_n)$ называются *элементарными симметрическими многочленами.*

Задача 8.6. Пусть $s_i = x_i^{-1}$, $i = 1, 2, \dots, n$ — величины, обратные к корням. Убедитесь, что имеется разложение

$$a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n = a_n (1 - s_1 t)(1 - s_2 t) \cdots (1 - s_n t)$$

и докажите формулы $a_k = (-1)^{n-k} a_n e_{n-k}(s_1, s_2, \dots, s_n)$.

1.4. Разложение результанта и дискриминанта. Пусть K – произвольное коммутативное кольцо. Рассмотрим кольцо многочленов $\mathcal{K} = K[\,x_1, x_2, \dots, x_n\,,\ y_1, y_2, \dots, y_m\,]$ и будем воспринимать переменные $x_1, x_2, \dots, x_n$ как формальные корни многочлена

$$f(t) = a_0 \prod_{\nu=1}^{n} (t - x_\nu) = a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n \in \mathcal{K}[t] \ ,$$

а переменные $y_1, y_2, \dots, y_m$ — как формальные корни многочлена

$$g(t) = b_0 \prod_{\mu=1}^{n} (t - y_\mu) = b_0 m^t + b_1 m^{t-1} + \dots + b_{t-1} m + b_t \in \mathcal{K}[t] \, .$$

Мы собираемся разложить на множители результант $R(f,g)$ как элемент кольца

$$\mathcal{K}' = K[\, a_0, a_1, \dots, a_n \, , \; b_0, b_1, \dots, b_m \,] \, .$$

Для этого заметим, что при подстановке y_j вместо x_i, многочлены f и g приобретают общий корень, а стало быть, результант в этом случае обратится в ноль.

Задача 8.7. Убедитесь, что если многочлен от x, y (с коэффициентами в любом коммутативном кольце) обращается в ноль при замене всех входящих в него x'ов на y, то он делится нацело на $x - y$.

Указание. Это вполне аналогично Сл.2.2.1 из лекции 3.

Поскольку все разности $x_i - y_j$ попарно взаимно просты, и все коэффициенты f делятся на a_0, а все коэффициенты g делятся на b_0, результант $R(f,g)$ делится в кольце

$$K[\, x_1, x_2, \dots, x_n \, , \; y_1, y_2, \dots, y_m \, , \, a_0, \, b_0] \supset \mathcal{K}'$$

на произведение

$$P = a_0^m b_0^n \prod_{\substack{1 \le \nu \le n \\ 1 \le \mu \le m}} (x_\nu - y_\mu) = a_0^m \prod_{\nu=1}^{n} g(x_\nu) = (-1)^{mn} b_0^n \prod_{\mu=1}^{m} f(y_\mu) \, .$$

Из последних двух перезаписей видно, что P как элемент $\mathcal{K}'$ является однородным степени n по переменным b_i, и однородным степени m по переменным a_j.

Задача 8.8. Убедитесь, что результант $R(F,G)$ любых двух многочленов F и G однороден степени $\deg G$ по коэффициентам F и однороден степени $\deg F$ по коэффициентам G.

Таким образом, $R(f,g) = \text{const} \cdot P$. Сравнение коэффициена при $a_0^m b_m^n$ в $R(f,g)$ и P показывает, что константа равна единице.

Задача 8.9. Чему точно равны сравниваемые коэффициенты?

Итак, мы доказали

1.4.1. Предложение. *Результант $R(f,g)$ пары многочленов f и g (над произвольным коммутативным кольцом), имеющих корни $x_1, x_2, \dots, x_n$ и $y_1, y_2, \dots, y_m$ и старшие коэффициенты a_0 и b_0 допускает разложения*

$$R(f,g) = a_0^m b_0^n \prod_{\substack{1 \le \nu \le n \\ 1 \le \mu \le m}} (x_\nu - y_\mu) = a_0^m \prod_{\nu=1}^{n} g(x_\nu) = (-1)^{mn} b_0^n \prod_{\mu=1}^{m} f(y_\mu) \, .$$

□

1.4.2. Следствие. *Дискриминант $D(f)$ многочлена f (над произвольным коммутативным кольцом), имеющего корни $x_1, x_2, \dots, x_n$ и старший коэффициент a_0 допускает разложение*

$$D(f) = a_0^{2n-2} \prod_{i>j}(x_i - x_j)^2 = a_0^{2n-2} \det^2 \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{pmatrix} .$$

Доказательство. По определению, $D(f) = (-1)^{\frac{n(n-1)}{2}} R(f, f')$. Но выше мы видели, что $R(f, f') = a_0^{n-1} \prod\limits_i f'(x_i)$. Но по формуле для дифференцирования произведения мы имеем

$$f'(x_i) = \left.\frac{d}{dt}\right|_{t=x_i} a_0 \prod_\nu (t - x_\nu) = a_0 \prod_{\nu \neq i} (x_i - x_\nu) ,$$

откуда после перемножения и получается нужное равенство.
□

Задача 8.10. Докажите, что дискриминант и результант являются неприводимыми многочленами от коэффициентов исходных многочленов.

Задача 8.11. Докажите, что дискриминант $D(a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n)$ как функция от коэффициентов a_i удовлетворяет дифференциальному уравнению

$$n a_0 + (n-1) a_1 \frac{\partial D}{\partial a_2} + (n-2) a_2 \frac{\partial D}{\partial a_3} + \dots + \frac{\partial D}{\partial a_n} .$$

Указание: Проверьте сначала, что дискриминант инвариантен относительно сдвигов переменной, т. е. $D\big(f(t)\big) = D\big(f(t+a)\big) \;\; \forall\, a \in K$.

§2. Симметрические многочлены

2.1. Определение. *Многочлен $f(x_1, x_2, \dots, x_n)$ называется симметрическим, если он не изменяется при любой перенумерации переменных, т. е. если*

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = f(x_1, x_2, \dots, x_n) \qquad \forall\, \sigma \in \mathfrak{S}_n \ .$$

Ясно, что симметрические многочлены из $K[x_1, x_2, \dots, x_n]$ образуют K-модуль (над произвольным коммутативным кольцом K).

Из теоремы Виета следуетет, что коэффициенты и дискриминант приведенного многочлена $t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n \in k[t]$ являются симметрическими многочленами от его корней. Оказывается, имеет место следующее

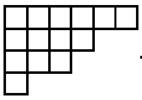
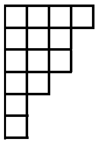
2.1.1. Предложение. *Всякий симметрический многочлен от корней приведенного многочлена из $k[t]$ может быть выражен в виде многочлена от коэффициентов (а стало быть, его значения можно найти не решая уравнения).*

Мы докажем сейчас несколько более сильный результ: проверим, что многочлены вида

$$e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n} ,$$

где $e_k(x_1, x_2, \ldots, x_n) = \sum\limits_{1 \le \nu_1 < \nu_2 < \cdots < \nu_k \le n} x_{\nu_1} x_{\nu_2} \cdots x_{\nu_n}$ суть элементарные симметрические многочлены, составляют *базис* модуля симметрических многочленов. Обозначим через $Sym^d = Sym^d(x_1, x_2, \ldots, x_n)$ подмодуль, состоящий из однородных симметрических многочленов степени d и нулевого многочлена. Поскольку элементарный симметрический многочлен e_k однороден степени k, нам достаточно будет проверить, что многочлены вида $e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n}$ с $\sum\limits_k k d_k = m$ образуют базис в Sym^m при каждом m. В процессе проверки нам понадобится одно очень полезное обозначение.

2.2. Разбиения и диаграммы Юнга. Упорядоченный набор монотонно невозрастающих неотрицательных целых чисел $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_k \ge 0$, с суммой $\sum \lambda_i = n$ называется *разбиением числа* n. Число n называется *весом* разбиения λ и обозначается также через $|\lambda|$. Число k называется *длиной* разбиения и обозначается $l(\lambda)$.

Визуализируется разбиение при помощи картинки, которая называется *диаграммой Юнга* и сосотоит из расположенных друг под другом и выровненных по левому краю клетчатых полосок длины $\lambda_1, \lambda_2, \ldots, \lambda_k$ (удобно рисовать на клетчатой бумаге). Например, разбиение $\lambda = (6431)$ изображается диаграммой . Разбиение, отвечающее *транспонированной* (т. е. симметричной относительно главной диагонали) диаграмме  называется *сопряжённым* к исходжному и обозначается λ' (в нашем случае $\lambda' = (4, 3, 3, 2, 1, 1)$).

Задача 8.12. Убедитесь, что $\lambda'_i =$ (количество строк длины $\le i$ в λ).

2.3. Симметрические многочлены e_λ. Соответсвие

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \longmapsto e_\lambda \overset{\text{def}}{=} e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}$$

устанавливает биекцию между всевозможными многочленами вида $e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n}$ лежащими в Sym^d и всевозможными разбиениями λ веса d, такими что $l(\lambda') = n$ (обратное отображение сопоставляет каждому многочлену вида $e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n}$ разбиение

$$\lambda = (\underbrace{n, n, \ldots, n}_{d_n}, \underbrace{(n-1), (n-1), \ldots, (n-1)}_{d_{n-1}}, \ldots \underbrace{1, 1, \ldots, 1}_{d_1}) ,$$

в котором количество строк длины i равно показателю при e_i).

2.3.1. Лемма. *Лексикографически старший моном многочлена $e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}$ равен $x_1^{\lambda'_1} x_2^{\lambda'_2} \cdots x_n^{\lambda'_n}$, где $\lambda' = (\lambda'_1, \lambda'_2, \ldots, \lambda'_n)$ – сопряжённое к λ разбиение.*

Доказательство. Поскольку старший моном в e_i есть $x_1x_2\cdots x_i$, степень, в которой переменная x_m войдет в старший моном произведения $e_{\lambda_1}e_{\lambda_2}\cdots e_{\lambda_k}$ равна количеству строк в λ, длина которых не меньше, чем m.
□

2.4. Симметрические многочлены f_λ. Для прозвольного разбиения $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_n)$ обозначим через $f_\lambda\in Sym^{|\lambda|}$ сумму всех попарно различных мономов, которые можно получить из монома $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$ всевозможными перенумерациями переменных. Симметрические многочлены f_λ называются *мономиальными* симметрическими многочленами.

2.4.1. Лемма. *Sym^d является свободным K-модулем конечного ранга, и всевозможные многочлены f_λ с $l(\lambda)=n$, $|\lambda|=d$ составляют базис в Sym^d.*

Доказательство. Всякий полином $g\in Sym^d$ вместе с каждым мономом содержит и все мономы, получающиеся из него перенумерациями переменных, причём все эти мономы входят в g с одним итем же коэффициентом, и лексикографически старшим из них будет единственный моном $c_\lambda\cdot x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$, показатели которого невозрастают: $\lambda_1\ge\lambda_2\ge\ldots\ge\lambda_n$. Стало быть, сумма всех этих мономов есть $c_\lambda\cdot f_\lambda$, где $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_n)$, $c_\lambda\in K$. Это показыает, что g распадается и притом единственным образом в линейную комбинацию многочленов f_λ с коэффициентами из K.
□

2.5. Матрица перехода от e_λ к f_λ. Введём лексикографический порядок на множестве всех разбиений $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_n)$ веса d и длины n. Тогда согласно Лм.2.3.1 разложение многочлена e_λ по базису f_λ имеет вид

$$e_\lambda=f_{\lambda'}+\text{ члены младших степеней },$$

где λ' — разбиение, двойственное к λ. Таким образом, если ввести на множестве всех разбиений веса d, удовлетворяющих условию $l(\lambda')=n$, линейное упорядочение полагая $\lambda<\mu$ если λ' лексикографически меньше μ', то мы получим

2.5.1. Следствие. *Матрица, по столбцам которой стоят координаты многочленов $e_\lambda\in Sym^n$ в базисе из мономиальных симметрических многочленов, является квадратной верхнетреугольной матрицей с единицами по главной диагонали.*

□

Но всякая матрица $H=(h_{ij}\in Mat_N(K)$, у которой $h_ij=0$ при $i>j$ и $h_{ii}=1$ $\forall i$ обратима над любым кольцом K.

Задача 8.13. Докажите это и получите (хотя бы при малых N) общую формулу для обратной матрицы.

Ответ: обратная матрица $H^{-1}=(g_{ij})$ имеет

$$g_{ij}=\begin{cases}0\quad\text{при}\quad i>j\\ 1\quad\text{при}\quad i=j\\ -h_{ij}+\sum\limits_{i<\nu_1<j}h_{i\nu_1}h_{\nu_1 j}-\sum\limits_{i<\nu_1<\nu_2<j}h_{i\nu_1}h_{\nu_1\nu_2}h_{\nu_1 j}+\sum\limits_{i<\nu_1<\nu_2<\nu_3<j}\cdots\qquad\text{при}\quad i<j\end{cases}.$$

Как мы знаем, обратимость матрицы перехода равносильно тому, что e_λ также составляет базис в Sym^d.

2.5.2. Следствие. *Многочлены $e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}$, где λ пробегает разбиения веса d, у которых $l(\lambda') = n$, или (что то же самое) многочлены вида $e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n}$ с $\sum\limits_k k d_k = d$ составляют базис модуля $\sum^d$ однородных симметрических многочленов степени d над произвольным коммутативным кольцом K.*

□

Переформулировкой этого следствия является

2.6. Теорема. (Основная теорема о симметрических функциях.) *Гомоморфизм*

$$K[t_1, t_2, \dots, t_n] \to K[x_1, x_2, \dots, x_n]\ ,$$

переводящий многочлен $p(t_1, t_2, \dots, t_n)$ в многочлен $p(e_1(x), e_2(x), \dots, e_n(x))$ отождествляет $K[xt1, t_2, \dots, t_n]$ с подкольцом симметрических многочленов в $K[x_1, x_2, \dots, x_n]$, т. е. всякий симметрический многочлен может быть представлен в виде многочлена от элементарных симметрических многочленов

$$e_i(x) \in K[x_1, x_2, \dots, x_n]\ ,$$

и такое представление единственно.

□

2.7. Практическое отыскание представления $g(x) = p(e)$ данного симметрического многочлена $g \in Sym^d$ в виде многочлена от элементарных симметрических многочленов осуществляется обычно так. В $g(x)$ отыскивается лексикографически старший моном

$$\alpha \cdot x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$$

Его показатели автоматически невозрастают: $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, и многочлен $g(x) - \alpha \cdot e_{\lambda'}(x)$, где λ' – разбиение, двойственное к $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$, имеет лексикографически меньший старший моном, чем $g(x)$. Далее процесс продолжается по индукции.

Задача 8.14. Пусть x_+ и x_- – корни уравнения $at^2 + bt + c = 0$. Не прибегая к определителям, выразите $D = a(x_+ - x_-)^2$ через a, b, и c и выведите из этого всю школьную теорию квадратных уравнений.

Задача 8.15. Пусть x_1, x_2, x_3 – корни уравнения $x^3 + px + q = 0$. Не прибегая к определителям, выразите $D = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ через p и q.

§3. Рациональные функции

3.1. Терминология. Класс эквивалентных дробей P/Q, где P, $Q \in k[\,x_1, x_2, \dots, x_n\,]$, $Q \neq 0$ и P/Q и F/G считаются эквивалентными, если $P(x)G(x) = F(x)Q(x)$ в $k[x_1, x_2, \dots, x_n]$, называется *рациональной функцией* от n переменных над полем k. Про эквивалентные дроби P/Q

и F/G говорят, что они задают одну и туже рациональную функцию. Множество рациональных функций обозначается $k(\,x_1, x_2, \ldots, x_n\,)$ (скобки круглые). Определим в $k(\,x_1, x_2, \ldots, x_n\,)$ сложение и умножение формулами

$$\begin{gathered}\frac{P_1}{Q_1}+\frac{P_2}{Q_2}\overset{\text{def}}{=}\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}\\ \frac{P_1}{Q_1}\cdot\frac{P_2}{Q_2}\overset{\text{def}}{=}\frac{P_1P_2}{Q_1Q_2}\,.\end{gathered}\tag{8-1}$$

Задача 8.16. Проверьте, что эти определения корректны, (т. е. не зависят от выбора представителя в классе эквивалентных дробей).

Задача 8.17. Убедитесь (прямой проверкой всех аксиом надлежащими явными вычислениями), что $k(\,x_1, x_2, \ldots, x_n\,)$ является полем.

Запись рациональной функции дробью P/Q называется *несократимой*, если полиномы P и Q не имеют нетривиальных общих делителей. Дробь P/Q называется *правильной*, если $\deg P < \deg Q$.

Задача 8.18. Убедитесь, что свойство дроби быть правильной сохраняется при переходе к эквивалентной дроби.

3.2. Разложение рациональных функций от одной переменной. При вычислениях с рациональными функциями от одной переменной над полем часто бывает полезной следующая

3.2.1. Лемма. *Пусть k – поле, и путь знаменатель дроби $P(t)/Q(t) \in k(t)$ разложен в произведение попарно взаимно простых многочленов:*

$$Q(t) = q_1(t)q_2(t)\ldots q_m(t)\,.$$

Тогда существует разложение

$$\frac{P(t)}{Q(t)} = h(t) + \frac{p_1(t)}{q_1(t)} + \frac{p_2(t)}{q_2(t)} + \cdots + \frac{p_m(t)}{q_m(t)}\,,\tag{8-2}$$

в котором $\deg h = \deg P - \deg Q$, $\deg p_i < \deg q_i$ и набор многочленов $h,\ p_1, p_2, \ldots, p_m \ \in k[t]$ однозначно определяется этими условиями по P и Q.

Доказательство. Пусть требуемое равенство выполнено. Домножая обе его части на Q, получим в $k[t]$ равенство:

$$P = hQ + p_1Q_1 + p_2Q_2 + \cdots + p_mQ_m\,,\tag{8-3}$$

где через Q_i обозначено произведение всех многочленов q_ν кроме i-того (в частности, Q_i взаимно прост с q_i и делится на все $q\nu$ с $\nu \neq i$). Из условия леммы вытекает неравенство $\deg(\sum p_\nu Q_\nu) < \deg Q$, показывающее, что h и $r \overset{\text{def}}{=} \sum p_\nu Q_\nu$ однозначно определяются как неполное частное и остаток от деления P на Q. Поскольку Q_i обратим в кольце $k[t]/(q_i)$, каждый из p_i однозначно определяется как единственный многочлен степени $< \deg q_i$, представляющий класс вычета $[r][Q_i]^{-1} = [P][Q_i]^{-1}$ в кольце $k[t]/(q_i)$ вычетов по $\bmod q_i$.

Это рассуждение показывает не только единственность, но и существование. Действительно, деля P на Q с остатком, можем написать, что $P/Q = h + r/Q$, где $\deg P < \deg Q$.

Далее, подбирая $p_1 \in k[t]$ с $\deg p_1 < \deg q_1$, представляющий в $k[t]/(q_1)$ класс $[P][Q_1]^{-1}$, можем написать, что $r = p_1 Q_1 + q_1 r_1$, с некоторым $r_1 \in k[t]$, имеющим $\deg r_1 < \deg Q_1$ (ибо $\deg r < \deg Q$). Отсюда $r/Q = p_1/q_1 + r_1/Q_1$, где знаменатель Q_1 уже не содержит q_1, но по-прежнему $\deg r_1 < \deg Q_1$, так что процедуру можно повторить с r_1/Q_1 и так далее.
□

3.2.2. Практическое отыскание разложения (8-2) удобно производить методом неопределенных коэффициентов: поскольку мы знаем оценки сверху на степени h и p_i, мы можем записать эти многочлены с неопределенными коэффициентами, и воспринимать соотношение (8-3) как систему линейных уравнений на эти коэффициенты. При этом извлекать из (8-3) уравнения можно двумя способами: либо приравнивать коэффициенты при одинаковых степенях t в левой и правой части, либо подставлятьть в левую и правую часть конкретные значения $t \in k$ (в качестве таковых особенно удобны корни многочленов q_i, ибо они аннулируют все Q_ν кроме i-того).

3.2.3. Пример: Найдём 1996-ю производную от $f(x) = x^3/(1+x^2)$, для чего воспользуемся разложением

$$\frac{x^3}{x^2+1} = x + \frac{\alpha}{x+i} + \frac{\beta}{x-i}$$

с подходящими $\alpha, \beta \in \mathbb{C}$. Чтобы их найти, подставим в равенство

$$x^3 = x(x^2+1) + \alpha(x-i) + \beta(x+i)$$

значения $x = i$ и $x = -i$. Получим $2i\beta = -i$ и $-2i\alpha = i$, т. е. $\alpha = \beta = -1/2$. Для 1996-й производной получаем выражение

$$-1995!\left((x+i)^{-1996} + (x-i)^{-1996}\right) = -1995! \cdot 2 \cdot \frac{x^{1996} + \binom{1996}{2} x^{1994} + \binom{1996}{4} x^{1992} + \cdots + 1}{(x^2+1)^{1996}} .$$

Задача 8.19. Докажите, что правильная дробь вида P/Q^d, однозначно записывается в виде

$$\frac{P}{Q^d} = \frac{P_1}{Q} + \frac{P_2}{Q^2} + \cdots + \frac{P_d}{Q^d} ,$$

где $\deg P_i < \deg Q \quad \forall i$.

Указание. Это не что иное как введение на кольце многочленов Q-ической позиционной системы счисления, что вполне аналогично хорошо известной всем программистам деятельности с натуральными числами (см. задачу ниже).

Задача 8.20. Докажите, что всякое натуральное число p, не превосходящее некоторой степени q^k произвольным образом фиксированного натурального числа q, единственным образом представляется в виде

$$p = a_0 + a_1 q + \cdots + a_{k-1} q^{k-1} .$$

Пример: при $q = 10$ это позволяет записать всякое $n \in \mathbb{N}$, $n < 10^k$, k-значным десятичным числом.

3.3. Поле частных, подобное $k(x_1, x_2, \dots, x_n)$ или $\mathbb{Q}$, можно построить исходя из любого *целостного* коммутативного кольца K. А именно, обозначим через a/b $(a, b \in K)$ класс возможных пар

$$\{(c, d) \in K \times K : \, ad = bc\} \, .$$

Эти классы разбивают $K \times K$ в объединение непересекающихся подмножеств, ибо если (c, d) входит и в a_1/b_1 и в a_2/b_2, то вычитая из равенства $a_1db_2 = b_1cb_2$ (полученного умножением обеих частей $a_1d = b_1c$ на b_2) аналогичное равенство $a_2db_1 = b_2cb_1$, получим $d(a_1b_2 - b_2a_1) = 0$, что ввиду целостности K влечёт равенство $a_1b_2 = b_2a_1$, означающее, что классы a_1/b_1 и a_2/b_2 совпадают.

Фактор-множество $K \times K$, состоящее из описанных только что классов a/b называется *полем частных* целостного коммутативного кольца K. Операции в этом поле определяются, как и ранее, правилами (8-1).

Задача 8.21. Проверьте, что опреации определены корректно и удовлетворяют всем аксиомам поля.

3.3.1. Пример: поле рядов Лорана. Пусть в предыдущей конструкции $K = k[[t]]$ будет кольцом формальных степенных рядов над полем k. Поле частных обозначается в этом случае $k((t))$. Напомню (см. лекцию 2), что каждый элемент $f(t) \in k[[t]]$ единственным образом представим в виде $f(t) = t^d f_0(t)$, где $d \in \mathbb{N}$, а $f_0(t)$ имеет ненулевой свободный член, и стало быть, обратим в $k[[t]]$. Поэтому всякий элемент $f/g \in k((t))$ может быть (также единственным способом) записан в виде $f(t)/g(t) = t^m r_0(t)$, где $m \in \mathbb{Z}$, а $r_0(t)$ – обратимый степенной ряд. Таким образом, всякий $l \in k((t))$ представляется рядом $l(t) = \sum\limits_{\nu \geq \nu_{\min}} a_\nu t^\nu$ по целым степеням переменной, в котором допускается лишь конечное число отрицательных степеней. Такие ряды называются *степенными рядами Лорана.*

Задача 8.22. Убедитесь непосредственным вычислением, что степенные ряды Лорана составляют поле.

Итак, поле частных кольца $k[[t]]$ изоморфно полю рядов Лорана.

3.4. Факториальность кольца многочленов. Пусть A – факториальное кольцо, и K – его поле частных. Внимательный анализ доказательств из лекции 3 показывает, что между разложением на множители в кольце $A[x]$ и разложением на множители в кольце $K[x]$ должна быть точно такая же связь как и в случае $A = \mathbb{Z}$, $K = \mathbb{Q}$.

Действительно, для любого набора элементов $a_1, a_2, \dots, a_n \in A$ можно определить их наибольший общий делитель *НОД* $(a_1, a_2, \dots, a_n)$ как максимальную общую часть разложений всех этих элементов на простые множители (как и в кольце главных идеалов, такой *НОД* будет определён однозначно с точностью до умножения на обратимые элементы кольца). После этого мы также как в лекции 3 можем определить *содержание* $\operatorname{cont}(f)$ многочлена $f \in A[x]$ и дословно теми же рассуждениями доказать лемму Гаусса.

Задача 8.23. Докажите, что:

(i) для любых двух многочленов $f, g \in A[x]$ выполнено равенство

$$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g) \, ;$$

(ii) любой многочленов $f(x) \in K[x]$ представляется в виде $\dfrac{\widehat{f}(x)}{a}$, где $a \in A$ и $\widehat{f}(x) \in A[x]$ – многочлен содержания 1, причём a и $\widehat{f}$ определяются по f однозначно с точностью до умножения на обратимый элемент кольца A;

(iii) всякий многочлен $f \in A[x]$, который раскладывается в $K[x]$ в произведение двух многочленов меньшей степени, будет и в $A[x]$ раскладываться в произвеедение двух многочленов тех же степеней.

Таким образом, множество неприводимых элементов кольца $A[x]$ состоит из неприводимых констант из A и неприводимых над полем K многочленов содержания 1. Из этого вытекает

3.4.1. Предложение. *Неприводимые элементы $A[x]$ просты.*

Доказательство. Надо проверить, что если gh делится на неприводимый многочлен f, то либо g либо h делится на f.

Если $f \equiv p = \mathrm{const} \in A$ — неприводимое число, то оно просто вследствие факториальности A, и либо $\mathrm{cont}(g)$, либо $\mathrm{cont}(h)$ делится на p (ибо $\mathrm{cont}(g)\mathrm{cont}(h) = \mathrm{cont}(gh)$ делится на p). Тем самым, p выносится из всех коэффициентов одного из многочленов, что и требовалось.

Если $f(x) \in A[x]$ – неприводимый над K многочлен содержания 1, то либо g, либо h делится на f в $K[x]$ (ибо неприводимые многочлены над полем просты). Если это, к примеру, g, то записывая частное в виде $\dfrac{g(x)}{f(x)} = \dfrac{q(x)}{a}$, где $q(x) \in A[x]$ – многочлен содержания 1, а $a \in A$, получим

$$a \cdot g(x) = f(x) \cdot q(x) \,.$$

Сравнивая содержание обеих частей по лемме Гаусса находим, что a – обратим в A (ибо $a\,\mathrm{cont}\,g = \mathrm{cont}\,f\,\mathrm{cont}\,q = 1$), и значит, $g/f \in A[x]$, что и требовалось.

□

3.4.2. Следствие. *Кольцо многочленов над факториальным кольцом факториально.*

□

По индукции отсюда немедленно вытекает

3.4.3. Следствие. *Кольцо многочленов от n переменных над факториальным кольцом факториально.*

□

§4. Разложение алгебраической функции в дробно-степенной ряд

4.1. Неявные алгебраические функции. Под *неявной формальной алгебраической функцией* от переменной t мы будем понимать корень $x(t)$ многочлена

$$f_t(x) = a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_{n-1}(t)x + a_n(t)$$

коэффициенты которого являются формальными степенными рядами от t.

Если t пробегает какую-либо область в $\mathbb{R}$ или $\mathbb{C}$ и ряды $a_i(t)$ сходятся в этой области, то корень $x(t)$ представляет “настоящую” (мноозначную) функцию от t. Простейшими примерами таких функций являются, скажем, $x(t) = \sqrt{1+t^2}$ и $x(t) = \dfrac{1}{1+t^2}$, представляющие собой, соответственно, корени квадратного многочлена $x^2 - a(t)$ и линейного многочлена $a(t)x - 1$, где $a(t) = 1 + t^2$.

Таким образом, функции, которые мы собираемся рассматривать, есть алгебраические функции наиболее общего вида, влючающие в себя, в частности, рациональные функции и радикалы. Остаток лекции будет посвящён тому, чтобы показать, что всякая такая функция может быть разложена в формальный степенной рядом Лорана от $\sqrt[d]{t}$ для подходящего $d \in \mathbb{N}$. Этот ряд называется *рядом Пюизо* рассматриваемой алгебраической функции. Интуитивное значение этого результата может быть выражено словами “всякая функция, записанная формулой, формально раскладывается в дробно-степенной ряд”.

Задача 8.24. Разложите $\sqrt{1+t+t^2}$ и $1/(1+t+t^2)$ в формальные степенные ряды по натуральным степеням t

Сразу оговоримся, что мы не будем здесь заниматься вопросами сходимости и остановимся только на алгебраической стороне дела: существовании такого ряда $\vartheta(\sqrt[d]{t})$, что после подстановки $x = \vartheta(t)$ в многочлен $a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_n(x)$ получится тождественно нулевой ряд от $\sqrt[d]{t}$. Точное утверждение таково:

4.2. Теорема. *Пусть k – алгебраически-замкнутое поле характеристики нуль и пусть $K = k((t))$ – поле рядов Лорана над k. Тогда для любого многочлена $f(x) \in K[x]$,*

$$f(x) = a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_n(x)$$

существует такой ряд $\vartheta(s) \in k((s))$ и такое число $d \in \mathbb{N}$, что в поле $k((s))$ выполнено тождество

$$f(\vartheta(s)) = a_0(s^d)\vartheta(s)^n + a_1(s^d)\vartheta(s)^{n-1} + \cdots + +a_n(s^d) \equiv 0\ .$$

4.3. Доказательство теоремы основывается на следующем фундаментальном факте, известном как *лемма Гензеля.*

4.3.1. Лемма. *Пусть k — любое поле, а*

$$G(t,x) = x^m + g(t)_1 x^{m-1} + \cdots + g(t)_{m-1}x + g(t)_m \in k[[t]][x]$$

– многочлен от x со старшим коэффициентом единица и прочими коэффициентами из кольца формальных степенных рядов $k[[t]]$. Если многочлен

$$G(0,x) = x^m + g(0)_1 x^{m-1} + \cdots + g(0)_{m-1}x + g(0)_m \in k[x]$$

раскладывается в $k[x]$ на два взаимно простых множителя $a(x)$ и $b(x)$ с $\deg a \geq 1$ и $\deg b \geq 1$, то $G(t,x)$ раскладывется на два взаимно-простых множителя $A(t,x)$ и $B(t,x)$ в $k[[t]][x]$, причём $\deg A \geq 1$, $\deg B \geq 1$ и $A(0,x) = a(x)$, $B(0,x) = b(x)$.

Доказательство. Воспользуемся методом неопределенных коэффициентов, т. е. будем искать $A(t,x)$ и $B(t,x)$ в виде

$$\begin{aligned} A(t,x) &= a_0(x) + a_1(x)t + a_2(x)t^2 + \cdots \\ B(t,x) &= b_0(x) + b_1(x)t + b_2(x)t^2 + \cdots \ , \end{aligned}$$

где $a_i(x)$ и $b_i(x)$ – многочлены из $k[x]$ степени *не больше, чем* $\deg(G) - 1$. В качестве $a_0(x)$ и $b_0(x)$ выберем $a(x)$ и $b(x)$, дающие разложение $G(0,x)$ из условия леммы. Для нахождения остальных a_i, b_i переразложим $G(t,x)$ по степеням t

$$G(t,x) = g_0(x) + g_1(x)t + g_2(x)t^2 + \cdots \quad ,$$

и приравнивая коэффициенты при одинаковых степенях t в равенстве $G(t,x) = A(t,x)B(t,x)$, получим рекурентную формулу

$$a_0(x)b_k(x) + b_0(x)a_k(x) = g_k(x) - \sum_{i+1}^{k-1} a_i(x)b_{k-i}(x) \ ,$$

позволяющую по индукции найти $a_k(x)$ и $b_k(x)$. Действительно, многочлен

$$r(x) = g_k(x) - \sum_{i+1}^{k-1} a_i(x)b_{k-i}(x)$$

в правой части зависит только от предыдущих a_i, b_i с $i < k$, многочлены a_0 и b_0 взаимно просты по условию леммы, и стало быть a_k есть единственный многочлен степени $< \deg a_0$, представляющий класс $[r][b_0]^{-1} \bmod a_0 \in k[x]/(a_0(x))$, а b_k есть единственный многочлен степени $< \deg b_0$, представляющий класс $[r][a_0]^{-1} \bmod b_0 \in k[x]/(b_0(x))$.
□

4.3.2. Окончание доказательства теоремы. Вернемся к полю $K = k((t))$ формальных рядов Лорана над алгебраически замкнутым полем k характеристики нуль, и пусть

$$f_t(x) = a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_n(x) \in K[x]$$

– какой-либо многочлен над K. Мы собираемся найти его корень, возможно после некоторой параметризации $t = s^d$.

Заметим прежде всего, что достаточно рассмотреть только случай, когда старший коэффициент a_0 многочлена f равен единице, а остальные коэффициенты лежат в кольце $k[[t]]$. Действительно, после умножения обеих частей уравнения $f(x) = 0$ на достаточно большую степень t^N, можно считать, что все $a_i \in k[[t]]$, и затем, умножив обе части на $a_0(x)^{n-1}$ и сделав линейную замену $z = a_0(t)x$, получить на z уравнение со старшим коэффициентом 1, умение решать которое в поле K равносильно умению решать в поле K исходное уравнение.

Итак, пусть $f_t(x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(x) \in k[[t]][x]$. Поскольку линейные уравнения (отвечающие $n = 1$) решаются над $K = k((t))$ без проблем, нам достаточно (благодаря индукции по n) разложить f в $k[[t]][x]$ на множители строго меньшей степени. Я утверждаю, что это всегда возможно, может быть, после некоторой замены параметра $t = s^d$.

В самом деле, по лемме Гензеля достаточно уметь раскладывать $f_0(x) = f_t(x)|_{t=0}$ на два нетривиальных взаимно простых множителя в $k[x]$. Поскольку поле k алгебраически замкнуто (и стало быть, каждый многочлен является произведением линейных), такое разложение невозможно только в случае, когда $f_0(x) = (x-\alpha)^n$ является чистой степенью линейного. Это можно исправить подходящим сдвигом переменной x и сменой параметра $t = s^d$.

Действительно, заменяя x на $x - a_1(t)/n$, можно считать, что $f_t(x)$ не содержит члена с $x^n - 1$. Если при при таком сдвиге исчезнут и все меньшие степени, т. е. $f_t(x)$ превратится в x^n, то мы получаем тривиальное решение $x = \vartheta(t) \equiv 0$ и больше делать нечего. Если же после сдвига останутся какие-то ненулевые коэффициенты

$$a_m(t) = \alpha_{\nu_m} t^{\nu_m} + \text{члены большей степени по } t\ ,$$

то мы выберем наименьшую из всех дробей $\frac{\alpha_{\nu_m}}{m}$ (ν_m пробегает младшие степени всех ненулевых рядов a_m) и рассмотрим её несократимую запись p/q. Отметим, что по построению $q\nu_m \geq pm$ при всех $m \geq 2$. Сделаем теперь замену $t = s^q$, $x = s^p y$. Получим

$$\begin{aligned} p_t(x) &= x^n + \sum_{m=2}^{n} (\alpha_{\nu_m} t^{\nu_m} + \cdots) x^{n-m} = \\ &= s^{pn} y^n + \sum_{m=2}^{n} s^{p(n-m)+q\nu_m} (\alpha_{\nu_m} + \cdots) y^{n-m} = \\ &= s^{np}\Big(y^n + \sum_{m=2}^{n} s^{q\nu_m - pm} (\alpha_{\nu_m} + \cdots) y^{n-m} \Big) \end{aligned}$$

где все ряды-коэффициенты справа содержат неотрицательные степени s (поскольку $q\nu_m \geq pm$), и хотя бы один из них (у которого $q\nu_m = pm$) имеет ненулевой свободный член. а стало быть гарантированно не занулится при $s = 0$. Таким образом, после сокращения на s^{pn} мы получаем на y уравнение, правая часть которого не является чистой степенью линейной формы при $s = 0$, поскольку будет содержать при $s = 0$ некий член y^i с $i < n$, но не будет содержать y^{n-1} (над полем характеристики нуль $(y - \alpha)^n$ либо совпадает с y^n (при $a = 0$) либо содержит *все без исключения* члены y^m с $0 \leq m \leq n$). Из сказанного ранее вытекает, что это уравнение разрешимо над полем $k((s))$.

Теорема доказана.

Лекция 9
Формальные функции

▷Формальные операции над степенными рядами ▷Экспоненты, логарифмы и логарифмичесие производные ▷Формула Ньютона для бинома ▷Действие $k[[d/dx]]$ на $k[x]$ ▷Числа Бернулли и многочлены Бернулли, суммирование степеней ▷Метод производящих функций: числа Каталана и формулы Ньютона для выражения степенных сумм через многочлены $e_i(x_1, x_2, \dots, x_n)$

§1. Экспонента, логарифм, бином

1.1. Формальные операции над формальными рядами. Под *формальной операцией* в кольце $k[[t]]$ мы будем понимать правило, сопоставляющее некоторым конечным наборам рядов $f_1, f_2, \dots, f_n$ с теми или иными свойствами (например, *всем* наборам из двух рядов f_1, f_2) новые ряды $g = g(f_1, f_2, \dots, f_n) \in k[[t]]$ так, что для вычисления каждого из коэффициентов ряда $g(f_1, f_2, \dots, f_n)$ достаточно произвести конечное число действий сложения, вычитания, умножения и деления над конечным числом коэффициентов рядов из набора $f_1, f_2, \dots, f_n$.

Два примера формальных операций, — сложение и умножение, – нам давно знакомы. Ниже мы приведем другие примеры.

1.1.1. Подстановка ряда в ряд. Если $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots$ – любой ряд, а

$$s(t) = s_k t^k + s_{k+1} t^{k+1} + \cdots \;, \quad k \geq 1 \;,$$

– ряд без свободного члена, то определен результат *подстановки* s в $f(t)$ вместо t:

$$f(s(t)) = \sum_{\nu \geq 0} a_\nu (s_k t^k + s_{k+1} t^{k+1} + \cdots)^\nu \in k[[t]] \;.$$

Действительно, каждый из рядов $a_\nu s(t)^\nu$ начинается с $t^{k\nu}$, и каждый коэффициент в них может быть вычислен за конечное число операций. Поэтому для вычисления каждого коэффициента в $f(s(t))$ также требуется только конечное число операций.

1.1.2. Дифференцирование в $k[[t]]$ определяется также, как в $k[t]$. Поскольку

$$\frac{x^k - y^k}{x - y} = x^{k-1} + x^{k-2} y + \cdots + x y^{k-2} + y^{k-1} \;,$$

ряд $f(x)-f(y)$ делится на $(x-y)$ в $k[[x,y]]$ для любого ряда $f(t)\in k[[t]]$. Обозначим частное от деления $f(x)-f(y)$ на $x-y$ через $D_f(x,y)$. Ряд $\dfrac{d}{dt}f=f'(t)\overset{\text{def}}{=}D_f(t,t)$ называется *производной* от $f(t)$.

Задача 9.1. Убедитесь, что $\left(a_0+a_1t+a_2t^2+\cdots\right)'=\sum\limits_{\nu\ge1}\nu a_{nu}t^{\nu-1}$.

1.1.3. Лемма. *Операция $f(t)\xrightarrow{d/dt}f'(t)$ удовлетворяет обычным правилам дифференцирования суммы, разности, произведения, частного (если оно определено) и композиции (если она определена).*

Доказательство. Пусть $f=a_0+a_1t+a_2t^2+\cdots$ и $g=\sum\limits_{\nu\ge1}b_\nu t^\nu$. Правило Лейбница для дифференцирования произведения доказывается дословно также, как и для многочленов:

$$D_{fg}(x,y)=\frac{f(x)g(x)-f(y)g(y)}{x-y}=f(x)\frac{g(x)-g(y)}{x-y}+\frac{f(x)-f(y)}{x-y}g(y)=$$

$$=f(x)D_g(x,y)+g(y)D_f(x,y)\ ,$$

что при $x=y=t$ даёт $(fg)'=f'g+g'f$.

Задача 9.2. Убедитесь, что $(f^m)'=mf^{m-1}f'$ для любого рядя f.

Докажем ещё правило дифференцирования композиции.

$$D_{f\cdot g}(x,y)=\sum_{i\ge0}a_i\frac{g(x)^i-f(x)^i}{x-y}$$

(сумма справа определена, ибо коэффициент при каждой степени $x^\alpha y^\beta$ является конечной суммой). Это равенство показывает, что

$$(f{\cdot}g)'=\sum_{i\ge0}a_i(g^i)'=\sum_{i\ge0}ia_ig^{i-1}g'=f'(g(t))g'(t)$$

(мы воспользовались предыдущей задачей).

Задача 9.3. Докажите остальные правила дифференцирования.

□

1.1.4. Первообразный ряд ряда $f(t)=a_0+a_1t+a_2t^2+\cdots$ определяется как ряд без свободного члена, производная от которого равна $f(t)$. Легко видеть, что этим он определяется однозначно:

$$\int f(t)dt=\sum_{k\ge1}\frac{a_{k-1}}{k}t^k\ .$$

1.2. Экспоненты и логарифмы. Всякий ряд $f(t)$, удовлетворяющий дифференциальному уравнению $f'=f$, называется *показательным*. Записывая такой ряд f с неопределенными коэффициентами

$$f=a_0+a_1t+a_2t^2+\cdots\ ,$$

получаем, что $ka_k = a_{k-1} \quad \forall\, k \geq 1$, откуда $a_k = \dfrac{a_0}{k!}$, и

$$f(t) = a_0 e^t \ , \quad \text{где} \quad e^t \stackrel{\text{def}}{=} \sum_{k \geq 0} \frac{t^k}{k!} \ .$$

Ряд e^t называется *экспонентой*. Отметим, что можно рассматривать экспоненту от любого ряда без свободного члена (подставляя этот ряд вместо t в e^t).

Определим ряд $\ln(1+t)$ как первообразный от ряда

$$\frac{1}{1+t} = \sum_{k \geq 0} (-1)^k t^k = 1 - t + t^2 - t^3 + \cdots \ .$$

Таким образом, $\ln(1+t) \stackrel{\text{def}}{=} \int dt/(1+t) = \sum\limits_{k \geq 1} (-1)^{k+1} \dfrac{x}{k}$.

Заметим, что для любого ряда $g(t) \in k[[t]]$ со свободным членом 1 можно определить его *логарифм* $\ln(g(t))$, как результат подстановки ряда $g(t) - 1$ (у этого ряда нет свободного члена!) вместо t в ряд $\ln(1+t)$. Ряд

$$\frac{d}{dt} \ln(g(t)) = \frac{g'(t)}{g(t)}$$

называется *логарифмической производной* ряда $g(t)$. Как и логарифм, логарифмическая производная определена только для рядов со свободным членом 1.

1.2.1. Лемма. *Для любых двух рядов $f(t)$ и $g(t)$ со свободным членом 1 равенства*

$$f(x) = g(x) \quad , \qquad \ln(f(x)) = \ln(g(x)) \quad , \qquad \frac{d}{dt} \ln(f(t)) = \frac{d}{dt} \ln(g(t))$$

попарно эквивалентны.

Доказательство. Импликации слева направо тривиальны, так что достаточно будет вывести первое равенство из третьего. Пусть $f(t) = 1 + a_1 t + a_2 t^2 + \cdots$ и $g(t) = 1 + b_1 t + b_2 t^2 + \cdots$ и пусть $\dfrac{d}{dt} \ln(f(t)) = \dfrac{d}{dt} \ln(g(t))$, т. е. $f'(t) g(t) = f(t) g'(t)$. Сравнивая коэффициенты при одинаковых степенях t, получаем равенства

$$\begin{array}{rcl}
a_1 \cdot 1 & = & 1 \cdot b_1 \\
2a_2 + a_1 b_1 & = & a_1 b_1 + 2b_2 \\
& \cdots & \\
ka_k \ + \sum\limits_{i=1}^{k-1} i a_i b_{k-i-1} & = & \sum\limits_{i=1}^{k-1} (k-i) a_{i-1} b_{k-i} \ + \ kb_k \\
& \cdots &
\end{array}$$

которые по индукции показывают, что $a_k = b_k \quad \forall\, k \in \mathbb{N}$.

$\square$

1.2.2. Лемма. *В $k[[t]]$ между рядами e^t и $\ln(1+t)$ выполняются обычные соотношения $e^{\ln(1+t)} = 1+t$ и $\ln(e^t) = t$.*

Доказательство. Продифференцируем ряд $\ln(e^t)$ как композицию рядов $f(t) = \ln(1+t)$ и $g(t) = e^t - 1$. Получим

$$(\ln(e^t))' = (f \cdot g)' = f'(g(t))g'(t) = \frac{1}{1+g(t)}g'(t) = \frac{e^t}{e^t} = 1 \ .$$

Таким образом, $\ln(e^t) = c+t$, где $c \in k$ — константа. Непосредственная подстановка $t + t^2/2 + t^3/6 + \cdots$ вместо t в ряд $t - t^2/2 + t^3/3 - \cdots$ показывает, что $c = 0$.

Первое равенство следует из второго по предыдущей лемме (в обеих частях стоят ряды со свободным членом 1 и второе равенство есть результат логарифмирования обеих частей первого равенства).

□

Задача 9.4. Докажите, что взятие экспоненты и логарифма суть взаимно обратные биекции между множеством рядов без свободного члена и множеством рядов со свободным членом 1.

1.2.3. Лемма. *Для рядов $f(t)$ и $g(t)$ со свободным членом 1 выполняется "основное свойство логарифма": $\ln(fg) = \ln(f)+\ln(g)$. Кроме того, $\ln(1/g) = -\ln(g)$ и $\ln(g^k) = k\ln(g) \quad \forall\, k \in \mathbb{Z}$.*

Доказательство. Левая и правая части равенства $\ln(fg) = \ln(f) + \ln(g)$ являются рядами без свободного члена, поэтому их совпадение равносильно совпадению их производных. Дифференцируя, получаем

$$\frac{(fg)'}{fg} = \frac{f'g + fg'}{fg} = \frac{f'}{f} + \frac{g'}{g} \ .$$

Аналогично, дифференцируя $\ln(1/g)$ и $-\ln(g)$, получаем равные ряды

$$(\ln(1/g))' = \frac{(1/g)'}{1/g} = \frac{-g'/g^2}{1/g} = -g/g' = (-\ln(g))' \ .$$

Последнее утверждение леммы есть следствие двух первых.

□

Задача 9.5. Докажите, что двух рядов $f(t)$ и $g(t)$ без свободного члена выполено основное свойство экспоненты $e^{f+g} = e^f e^g$.

Задача 9.6. Убедитесь, что биекции из зад.9.4 являются гомоморфными в том смысле, что они переводят сложение на множестве рядов без свободного члена в умножение рядов со свободным членом 1

1.3. Степень $(1+t)^\alpha$ с произвольным показателем $\alpha \in k$ можно определить формально распространяя равенство $\ln(1+t)^n = n\ln(1+t)$ с целых n на произвольные $\alpha \in k$. Итак, по определению, полагаем

$$(1+t)^\alpha \stackrel{\text{def}}{=} e^{\alpha\ln(1+t)} \ .$$

Свойства экспоненты гарантируют, что эта функция оправдывает своё обозначение, т. е. удовлетворяет основному соотношению

$$(1+t)^{\alpha+\beta} = e^{(\alpha+\beta)\ln(1+t)} = e^{\alpha\ln(1+t)}e^{\beta\ln(1+t)} = (1+t)^{\alpha}(1+t)^{\beta} \qquad \forall\, a,b\in k\ .$$

Задача 9.7. Убедитесь, что если показатель α – целый, то из нашего определения вытекают равенста

$$(1+t)^n = \underbrace{(1+t)\cdot\,\cdots\,\cdot(1+t)}_{n}\,, \qquad \text{и} \qquad (1+t)^{-n} = \underbrace{(1+t)^{-1}\cdot\,\cdots\,\cdot(1+t)^{-1}}_{n}$$

(здесь $n\in\mathbb{N}$ и $(1+t)^{-1} = 1 - t + t^2 - t^3 + \cdots$ — элемент обратный к $(1+t)$ в $k[[t]]$).

Для того чтобы отыскать явные значения коэффициентов ряда

$$(1+t)^{\alpha} = a_0 + a_1 t + a_2 t^2 + \cdots \in k[[t]]\ ,$$

заметим, что $a_0 = 1$ (это усматривается прямо из определения – обязательно убедитесь!) и вычислим логарифмическую призводную:

$$\frac{d}{dt}\ln(1+t)^{\alpha} = \frac{d}{dt}\ln e^{\alpha}\ln(1+t) = \frac{d}{dt}\Big(\alpha\ln(1+t)\Big) = \frac{\alpha}{(1+t)}\ .$$

Таким образом, $\Big((1+t)^{\alpha}\Big)'\cdot(1+t) = \alpha\cdot(1+t)^{\alpha}$, и сравнивая коэффициенты при t^{k-1}, мы получаем на искомые коэффициенты a_i соотношения:

$$ka_k + (k-1)a_{k-1} = \alpha a_{k-1}\ ,$$

откуда $a_k = \dfrac{a_{k-1}}{k}(\alpha-k+1) = \dfrac{a_0}{k!}\underbrace{\alpha(\alpha-1)\cdots(\alpha-k+1)}_{k}$. Вспоминая, что $a_0 = 1$ и вводя обозначение

$$\binom{\alpha}{k} \overset{\text{def}}{=} \frac{\overbrace{\alpha(\alpha-1)\cdots(\alpha-k+1)}^{k}}{k!}\ ,$$

получаем следующий результат:

1.4. Теорема. (Формула Ньютона для бинома.)

$$(1+t)^{\alpha} = \sum_{\nu\geq 0}\binom{\alpha}{\nu}t^{\nu} = 1 + \alpha t + \frac{\alpha(\alpha-1)}{2}t^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6}t^3 + \cdots \qquad \forall\,\alpha\in k\ .$$

□

Именно эта теорема и была открыта И. Нютоном и известна как *бином Ньютона.* Числа $\binom{\alpha}{\nu}$ называются *биномиальными коэффициентами.* Отметим, что формула Ньютона даёт явное разложение для алгебраических функций, выражаемых в радикалах (надо взять $\alpha = 1/n$). В своём учебнике по анализу Л. Эйлер писал, что любая функция может быть разложена в ряд, в чём каждый сомневающийся легко может удостовериться, разобрав несколько примеров. Доказанная в конце прошлой лекции теорема может восприниматься как один из способов придания точного смысла этим словам Эйлера, а бином Ньютона – как один из наиболее убедительных примеров.

§2. Разностные операторы на кольце многочленов

2.1. Обозначения. Пусть k – поле характеристики нуль. Рассмотрим кольцо многочленов $k[x]$ как (бесконечномерное) векторное пространство над полем k. Будем называть *линейным оператором* на $k[x]$ всякий k-линейный эндоморфизм $k[x] \xrightarrow{\varphi} k[x]$ как векторного пространства[1] над k. Всякий линейный оператор Φ на $k[x]$ однозначно определяется заданием последовательности многочленов

$$\varphi_n(x) \stackrel{\text{def}}{=} \Phi(x^n) \quad , \qquad n = 0\,,\ 1\,,\ 2\ \dots\ .$$

В самом деле, вследствие линейности

$$\Phi(a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m) = a_0\varphi_n(x) + a_1\varphi_{n-1}(x) + \ \cdots\ a_m\varphi_0(x)\ .$$

Примерами линейных операторов на кольце многочленов являются:

оператор сдвига $T_a:\ f(x) \longrightarrow T_af(x) \stackrel{\text{def}}{=} f(x+a)$;

разностный оператор $\Delta_a = T_a - 1:\ f(x) \longrightarrow \Delta_af(x) \stackrel{\text{def}}{=} f(x+a) - f(x)$;

и оператор дифференцирования $\dfrac{d}{dx}:\ f(x) \longrightarrow f'(x)$.

Через T и Δ мы будем далее обозначать, соответственно, операторы T_1 и $\Delta_1 = T - 1$, так что

$$Tf(x) \stackrel{\text{def}}{=} f(x+1) \qquad , \qquad \Delta f(x) \stackrel{\text{def}}{=} f(x+1) - f(x)\ .$$

2.2. Действие $k\left[\left[\dfrac{d}{dx}\right]\right]$ на $k[x]$. Для каждого формального ряда $F(t) = \sum\limits_{\nu\geq 0} a_\nu t^\nu \in k[[t]]$ определим оператор

$$F\left(\frac{d}{dx}\right)\,:\ k[x] \longrightarrow k[x]:\quad f \longmapsto F\left(\frac{d}{dx}\right) f \stackrel{\text{def}}{=} \sum_{\nu\geq 0} \frac{d^\nu f}{dx^\nu}$$

(правая часть имеет смысл поскольку $\dfrac{d^\nu f}{dx^\nu}$ при $k > \deg(f)$, и стало быть, сумма справа конечна для каждого конкретного f).

Задача 9.8. Проверьте, что тем самым мы определили гомоморфизм из кольца $k[[t]]$ в кольцо линейных операторов на $k[x]$ (кольцевыми операциями в последнем являются сложение и композиция).

Совокупность всех операторов на $k[x]$, представимых в виде ряда от $\dfrac{d}{dx}$, является коммутативным подкольцом, котров мы обозначим через $\mathcal{A}$ и будем называть *кольцом разностных операторов* на $k[x]$ (смысл этого названия мы объясним чуть позже).

[1] это означает, что $\varphi(\alpha f + \beta g) = \alpha\varphi(f) + \beta\varphi(g)\ \forall\,\alpha,\beta \in k$ и $\forall\, f, g \in k[x]$, но вообще говоря, $\varphi(fg) \neq \varphi(f)\varphi(g)$

2.2.1. Лемма. (Формула Тейлора[2] .) $T_a = e^{a\frac{d}{dx}}$.

Доказательство. Поскольку действие линейного оператора однозначно определяется его действием на базис, достаточно проверить, что $e^{a\frac{d}{dx}}x^n = T_a x^n = (x+a)^n$. Это следует из разложения бинома:

$$e^{a\frac{d}{dx}}x^n = \sum_{\nu=0}^{n} \frac{a^\nu d^\nu x^n}{\nu! dx^\nu} = \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu x^{n-\nu} = (x+a)^\nu \ .$$

□

Линейные операторы $\Phi \in \mathcal{A}$ замечательны тем, что к ним применима вся предыдущая машинерия формальных тождеств в $k[[t]]$. Мы проиллюстрируем это на одном классическом примере.

2.3. Пример: обращение Бернулли. Разностный оператор Δ представим в виде

$$\Delta = T - 1 = e^{\frac{d}{dx}} - 1 = U\left(\frac{d}{dx}\right) \cdot \frac{d}{dx} \ ,$$

где $U(t) = \dfrac{e^t - 1}{t} \in k[[t]]$ является обратимым рядом со свободным членом 1, а стало быть, $U\left(\dfrac{d}{dx}\right)$ является изоморфизмом векторного пространства $k[x]$ на себя. Оператор

$$B\left(\frac{d}{dx}\right) = U^{-1}\left(\frac{d}{dx}\right)$$

называется *оператором Бернулли*. Он получается подстановкой $t = \dfrac{d}{dx}$ в формальный ряд $B(t) = \dfrac{t}{e^t - 1}$. Явное разложение $B(t)$ по степеням t традиционно записывают в виде

$$B(t) = \frac{t}{e^t - 1} = \sum_{\nu \ge 0} \frac{b_\nu}{\nu!} t^\nu \ .$$

Числа[3] $b_\nu \in \mathbb{Q}$ называются *числами Бернулли* и возникают в самых различных областях математики. Для их вычисления имеется простая реккурентная формула. Прежде всего, понятно, что $b_0 = 1$. Далее, раскладывая $B(t)$ в сумму чётной и нечетной составляющей

$$B(t) = B_+(t) + B_-(t) \quad , \qquad \text{где} \quad B_\pm(t) = \frac{B(t) \pm B(-t)}{2} \ ,$$

---

[2]В более традиционных терминах формула Тейлора означает, что для любого многочлена $f \in k[x]$ степени n и любого $a \in k$ выполнено тождество

$$f(x+a) = \sum_{\nu=0}^{n} \frac{1}{\nu!} f^{(\nu)}(x) a^\nu = f(x) + f'(x)a + \frac{1}{2} f''(x)a^2 + \frac{1}{6} f'''(x)a^3 + \cdots \ .$$

[3]очевидно, что b_ν находятся в простом подполе поля k, которое по нашему предположению ($\mathrm{char}\, k = 0$) можно канонически отождествить с полем рациональных чисел

немедленно получаем, что

$$B_-(t) = \frac{1}{2}\left(\frac{t}{e^t - 1} + \frac{t}{e^{-t} - 1}\right) = -\frac{t}{2} ,$$

что означает, что за исключением $b_1 = -1/2$ все прочие коэффициенты b_ν с *нечётными* номерами равны нулю[4]. Наконец, приравнивая коэффициенты при t^{n+1} в формуле

$$t = (e^t - 1)B(t) = \Big(\sum_{\mu \geq 1} \frac{1}{\mu!}t^\mu\Big)\Big(\sum_{\nu \geq 0} \frac{b_\nu}{\nu!}t^\nu\Big) ,$$

получаем соотношение

$$\sum_{\nu=0}^{n} \frac{b_\nu}{\nu!(n-\nu+1)!} = 0 \qquad (\text{при } n \geq 2) ,$$

Из которого получается реккурентная формула

$$b_n = -n!\sum_{\nu=0}^{n-1} \frac{b_\nu}{\nu!(n-\nu+1)!} = -\frac{1}{n+1}\sum_{\nu=0}^{n-1} \binom{n+1}{\nu} b_\nu , \tag{9-1}$$

справедливая при $n \geq 2$.

Задача 9.9. Вычислите первые 10 чисел Бернулли.

Ответ: отличные от нуля b_ν с $\nu \leq 10$ суть

$$b_0 = 1 , \quad b_1 = -\frac{1}{2} , \quad b_2 = \frac{1}{6} , \quad b_4 = -\frac{1}{30} , \quad b_6 = \frac{1}{42} , \quad b_8 = -\frac{1}{30} , \quad b_6 = \frac{5}{66} .$$

Задача 9.10. Докажите, что последовательность чисел Бернулли с чётными номерами является знакопеременной.

Предыдущее вычисление впервые было предпринято Якобом Бернулли для решения следующей задачи:

2.3.1. Задача Бернулли: получить формулу, выражающую сумму

$$S_k(n) = 0^k + 1^k + 2^k + \cdots + n^k$$

в виде многочлена от n (при фиксированном k).

Для получения явного выражения для целозначного многочлена $S_k(x) \in \mathbb{Q}[x]$, вычисляющего предыдущую сумму при подстановке целых $x = n \in \mathbb{Z}$, Бернулли заметил, что прямо по определению S_k имеем

$$\Delta S_k(x) = (x+1)^k$$

[4] напротив, для чётных коэффициентов имеем

$$B_+(t) = \frac{1}{2}\left(\frac{t}{e^t - 1} - \frac{t}{e^{-t} - 1}\right) = \frac{t}{2}\cdot\frac{e^t - e^{-t}}{e^t - 2 + e^{-t}} = \frac{t}{2}\cdot\frac{\left(e^{\frac{t}{2}} + e^{-\frac{t}{2}}\right)\left(e^{\frac{t}{2}} - e^{-\frac{t}{2}}\right)}{\left(e^{\frac{t}{2}} - e^{-\frac{t}{2}}\right)^2} = \frac{t}{2}\cdot\frac{e^{\frac{t}{2}} + e^{-\frac{t}{2}}}{e^{\frac{t}{2}} - e^{-\frac{t}{2}}} \stackrel{\text{def}}{=} \frac{t}{2}\cdot \operatorname{cth}\left(\frac{t}{2}\right) ;$$

ряд $\operatorname{cth}(t) = \sum_{\alpha \geq 1} \frac{2^{2\alpha-1}}{(2\alpha-1)!} b_{2\alpha} t^{2\alpha-1}$ называется *гиперболическим котангенсом*.

(эта фомула выполняется для всех $x \in \mathbb{N}$, и следовательно является тождеством в $\mathbb{Q}[x]$). Поскольку $\Delta = B^{-1}\left(\frac{d}{dx}\right)\cdot\frac{d}{dx}$, мы получаем на $S_k(x)$ дифференциальное уравнение

$$S'_k(x) = B\left(\frac{d}{dx}\right)(x+1)^k = B_k(x+1)\ ,$$

где $B_k(x) \stackrel{\text{def}}{=} B\left(\frac{d}{dx}\right)x^k = \sum\limits_{\nu\geq 0}\frac{b_\nu}{\nu!}\frac{d^\nu x^k}{dx^\nu} = \sum\limits_{\nu=0}^{k}\binom{k}{\nu}b_\nu x^{k-\nu}$ — многочлены[5], определяющие действие оператора B на стандартный базис в $k[x]$. Сами B_k также связаны дифференциальным соотношением

$$B'_{k+1}(x) = \frac{d}{dx}B\left(\frac{d}{dx}\right)x^{k+1} = B\left(\frac{d}{dx}\right)\frac{d}{dk}x^{k+1} = (k+1)B\left(\frac{d}{dx}\right)x^k = (k+1)B_k(x)\ ,$$

из которого следует, что $S'_k(x) = \frac{1}{k+1}B'_{k+1}(x+1)$, т. е. $S_k(x)$ и $\frac{1}{k+1}B_{k+1}(x+1)$ различаются на константу. Подставляя $x=1$ получаем $S_k(1)=1$ и

$$\frac{1}{k+1}B_{k+1}(1) = \frac{1}{k+1}\sum_{\nu=0}^{k}\binom{k}{\nu}b_\nu = b_k - \frac{1}{k+1}\binom{k+1}{k}b_k - \frac{1}{k+1}\binom{k+1}{k+1}b_{k+1} = -\frac{b_{k+1}}{k+1}$$

(мы воспользовались реккурентной формулой (9-1) для чисел Бернулли). Нами доказано

2.3.2. Предложение. (Формула Бернулли.)

$$S_k(n) = 0^k + 1^k + 2^k + \cdots + n^k = \frac{B_{k+1}(n+1) - b_{k+1}}{k+1}\ .$$

□

Задача 9.11. Вычислите первые 11 многочленов Бернулли.

Подсказка:
$B_0(x) = 1$
$B_1(x) = x - \frac{1}{2}$
$B_2(x) = x^2 - x + \frac{1}{6}$
$B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$
$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}$
$B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x$

Задача 9.12. Докажите, что для многочленов Бернулли имеется рекурентная формула

$$B_k(x) = x^k - \frac{1}{k+1}\sum_{\nu=1}^{k}\binom{k+1}{\nu+1}B_{k-\nu}(x)\ .$$

Задача 9.13. Решив свою задачу, Якоб Бернулли не без гордости записал, что "сумел вычислить сумму десятых степеней первой тысячи натуральных чисел менее, чем за половину четверти часа". Сумеете ли Вы повторить его результат?

[5] они называются *многочленами Бернулли*

Подсказка: $B_{11}(x) = x^{11} - \frac{11}{2}x^{10} + \frac{55}{6}x^9 - 11x^7 + 11x^5 - \frac{5}{3}x^3 + \frac{5}{6}x.$

2.4. Объяснение термина "разностный оператор". Поскольку $\forall f \in k[x]$ имеем $\deg(\Delta f) < \deg(f)$,

Задача 9.14. Убедитесь в этом.

для каждого формального ряда $F(t) = f_0 + f_1 t + f_2 t^2 + \cdots \in k[[t]]$ можно, как и выше, определить оператор

$$f(\Delta): \quad f(x) \longmapsto \sum_{\nu \geq 0} f_\nu \Delta^\nu f\ .$$

Благодаря тождеству $\ln(e^t) = t$ мы можем представить оператор дифференцирования $\frac{d}{dx}$ в виде ряда по $\Delta = T - 1 = e^{-\frac{d}{dx}} - 1$:

$$Dx = \ln(e^{\frac{d}{dx}} = \ln(1+\Delta) = \sum_{\nu \geq 1} (-1)^{\nu-1} \frac{\Delta^\nu}{\nu} = \Delta - \frac{\Delta^2}{2} + \frac{\Delta^3}{3} - \cdots\ .$$

Таким образом, всякий линейный оператор, представимый в виде ряда по $\frac{d}{dx}$, представим и в виде ряда по степеням разностного оператора Δ, т. е. алгебра $\mathcal{A}$ есть алгебра степенных рядов от разного оператора.

2.5. Теорема. *Следующие условия на линейный оператор $k[x] \xrightarrow{\Phi} k[x]$ попарно эквивалентны:*

(i) Φ перестановочен с Δ: $\Phi\Delta = \Delta\Phi$;

(ii) Φ перестановочен с T: $\Phi T = T\Phi$;

(iii) Φ перестановочен со всеми операторами сдвига: $\Phi T_a = T_a \Phi \quad \forall\, a \in k$;

(iv) Φ имеет вид $\Phi = F\left(\frac{d}{dx}\right)$ для некоторого $F \in k[[t]]$;

(v) Φ имеет вид $\Phi = F(\Delta)$ для некоторого $F \in k[[t]]$.

Доказательство. Замечания перед теоремой делают тривиальными все импликации сницу вверх. Поэтому достаточно проверить, что из первого условия следует последнее. Для этого мы выберем в пространстве $k[x]$ специальный базис, состоящий из многочленов

$$f_0 \overset{\text{def}}{=} 1 \qquad \text{и} \qquad f_k(x) \overset{\text{def}}{=} \binom{x}{k} = \frac{1}{k!} \underbrace{x(x-1)\cdots(x-k+1)}_{k},$$

которые замечательны тем, что $\Delta f_k = f_{k-1} \quad \forall\, k \geq 1$.

Задача 9.15. Проверьте это соотношение и убедитесь, что f_k и в самом деле составляют базис пространства $k[x]$ над k.

Для каждого $k \geq 0$ обозначим через $a_k \in k$ значение многочлена $\Phi(f_k)$ при $x = 0$ (т. е. свободный член этого многочлена). Так как все многочлены $f_k(x)$ с $k \geq 1$ обращаются в нуль при $x = 0$, коэффициенты λ_ν из разложения

$$\Phi(f_k) = \sum_{\nu \geq 0} \lambda_\nu f_\nu$$

равны $\lambda_\nu = \Delta^\nu \Phi\, f_k\,(0) = \Phi \Delta^\nu\, f_k\,(0) = \Phi\, f_{k-\nu}(0) = a_{k-nu}$ (и в частности, все $a_\nu = 0$ при $\nu > k$). Но тогда

$$\Phi(f_k) = \sum_{\nu=0}^{k} a_{k-\nu} f_\nu = \sum_{\alpha \geq 0} a_\alpha \Delta^\alpha\, f_k\ ,$$

откуда $\Phi = \sum a_\alpha \Delta^\alpha$.
□

§3. Производящие функции

3.1. Описание метода. Пусть $(a_\nu) = a_0,\ a_1,\ a_2,\ \dots$ – последовательность элементов произвольного коммутативного кольца K. Формальный степенной ряд

$$A(t) = a_0 + a_1 t + a_2 t^2 + \cdots \in K[[t]]$$

называется *производящей функцией* для последовательности (a_ν). Производящая функция исключительно полезна в ситуации, когда какие-либо свойства последовательности (a_ν) приводят к алгебраическому или дифференциальному уравнению на $A(t)$ в кольце $K[[t]]$. В этом случае использование техники формальных функций обычно позволяет устанавливать новые нетривиальные свойства последовательности $(a_\nu$, невидные непосредственно из её определения.

Мы проиллюстрируем этот метод исследования несколькими примерами.

3.2. Пример: числа Каталана. Чтобы вычислить сумму $(n+1)$ чисел

$$a_0 + a_1 + a_2 + \ \cdots\ + a_n\ ,$$

мы должны выполнить n написанных выше операций "+" в той или иной допустимой последовательности. Количество таких последовательностей (или иначе, количество допустимых расстановок $n+1$ пар скобок в предыдущей сумме) называется n-ым *числом Каталана* c_n. Очевидно, что $c_n < n!$. Мы собираемся получить явную формулу, выражающую c_n через n.

Заметим, прежде всего, что количество способов упорядочения действий, приводящих к тому, что последним выполняется i-тый слева знак "+" (где $i = 1,\ 2,\ \dots,\ n$), равно $c_{i-1}c_{n-i-1}$. Это приводит к рекурентной формуле

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \ \cdots\ + c_{n-2} c_1 + c_{n-1} c_0$$

(где мы для единоообразия положили $c_0 \stackrel{\text{def}}{=} 1$). Эта формула означает, что производящая функция

$$C(t) = c_0 + c_1 t + c_2 t^2 + \cdots \in \mathbb{Q}[[t]]$$

удовлетворяет квадратному уравнению $C(t)-1 = tC(t)^2$ (написанная выше рекурентная формула сравнивает коэффициенты при t^n в левой и правой части). Решая это уравнение относительно $C(t)$, получаем

$$C(t) = \frac{1 \pm \sqrt{1-4t}}{2t} ,$$

где $\pm\sqrt{1-4t}$ суть два решения уравнения $x^2 = 1-4t$ в целостном кольце $\mathbb{Q}[[t]]$. Одним из этих решений будет, очевидно, бином

$$(1-4t)^{1/2} = \sum_{\nu\geq 0} \frac{(-1)^{\nu-1}}{\nu!} 4^\nu \underbrace{\frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-\nu+1\right)}_{\nu} t^\nu ,$$

а другое отличается от него знаком. Поскольку $c_0 = 1$, искомая нами функция $C(t)$ получится при выборе знака "+". Получаем окончательно:

$$\begin{aligned} C(t) &= \frac{1}{2t}\sum_{\nu\geq 1} \frac{(-1)^{\nu-1}}{\nu!} 4^\nu \frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-\nu+1\right) t^\nu = \\ &= \sum_{\nu\geq 1} 2^{\nu-1} \frac{1\cdot(2\cdot 1-1)\cdot(4\cdot 1-1)\cdot\cdots\cdot(2(\nu-1)-1)}{\nu!} t^{\nu-1} = \\ &= \sum_{\nu\geq 1} \frac{\big(2(\nu-1)\big)!}{\nu!(\nu-1)!} t^{\nu-1} = \sum_{k\geq 0} \binom{2k}{k} \frac{t^k}{k+1} \end{aligned}$$

(при переходе от первой строки ко второй мы умножили каждый из ν множителей в числителе дроби на 2, отщепив эти ν двоек из 4^ν, и сменили знак последних $(\nu-1)$ множителях; при переходе от второй строчки к третьей — домножили и числитель и знаменатель на $(\nu-1)!$, что в сочетании с $2^{\nu-1}$ дополняет числитель до полного факториала).

Итак,

$$c_n = \frac{1}{n+1}\binom{2n}{n}$$

(в частоности, это число всегда является целым!).

3.3. Пример: формулы Ньютона для выражения симметрических многочленов

$$p_k(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} x_1^k + x_2^k + \cdots + x_n^k$$

через элементарные симметрические многочлены $e_i(x)$ получаются следующим образом.

Рассмотрим кольцо $K = \mathbb{Q}[\, x_1, x_2, \ldots, x_n \,]$. Элементарные симметрические многочлены $e_0, e_1, \ldots, e_n$ (мы полагаем $e_0 \equiv 1$) представляют собой конечную последовательность элементов этого кольца. Производящей функцией для этой последовательности является

$$E(t) = (1+x_1t)(1+x_2t)\ldots(1+x_nt) \in K[t] \subset K[[t]] .$$

Степенные суммы p_k, $k \geq 1$, составляют бесконечную последовательность в K. Удобно записать производящую функцию для p_k в виде ряда

$$P(t) = \sum_{\nu \geq 0} p_{\nu+1} t^\nu = \sum_{i=1}^{n} \sum_{\nu \geq 0} x_i^{\nu+1} t^\nu = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t}$$

(последнее равенство получается по формуле суммирования геометрической прогрессии). Из свойств логарифма получаем, что

$$P(t) = \frac{d}{dt} \ln E(-t) = \frac{E'(-t)}{E(-t)} .$$

Сравнивая в раенстве $P(t)E(-t) = E'(-t)$ коэффициенты при t^{k-1} слева и справа, получаем

$$\sum_{\nu=0}^{k-1} (-1)^\nu e_\nu p_{k-\nu} = (-1)^{k-1} k e_k$$

(мы считаеи, что $e_\nu = 0$ при $\nu > n$). Таким образом возникает рекурентная формула, позволяющая последовательно выразить p_1, p_2, p_3, $\ldots$ через элементарные симметрические функции:

$$p_k = (-1)^{k-1} e_k - \sum_{\nu=1}^{k-1} (-1)^\nu e_\nu p_{k-\nu} \quad , \qquad \text{где} \quad e_\nu = 0 \quad \text{при} \quad \nu > n \ .$$

Это и есть *формула Ньютона для степенных сумм.*

Отметим, что и наоборот, можно выразить элементарные симметрические функции через суммы степеней, но правда, с рациональными коэффициентами:

$$e_k = -\frac{1}{k} \sum_{\nu=0}^{k-1} (-1)^\nu p_{\nu+1} e_{k-1-\nu} \ .$$

Задача 9.16. Докажите, что произведения степенных сумм

$$p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$$

составляют $\mathbb{Q}$-базис пространства симметрических многочленов над полем $\mathbb{Q}$ (т. е. что всякий симметрический многочлен из $\mathbb{Q}[\, x_1, x_2, \ldots, x_n \,]$ можно единственным образом представить в виде многочлена с рациональными коэффициентами от первых n степенных сумм $p_1, p_2, \ldots, p_n$).

Лекция 10
Группы

▷Автоморфизмы и симметрии ▷Групповой закон композиции ▷Симметрические группы ▷Группы Галуа ▷Группы многогранников ▷Смежные классы и теорема Лагранжа ▷Действие группы на множестве: формула для длины орбиты ▷Фактор-группы, нормальные подгруппы и строение гомоморфизмов ▷Цикловой тип подстановки ▷Строение групп $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{A}_3$, $\mathfrak{A}_4$, $\mathfrak{A}_5$ ▷Простота знакопеременных групп $\mathfrak{A}_n$ с $n \geq 5$

§1. Что такое группа

Все познаётся в сравнении, и основным источником информации о математических объектах является исследование их взаимодействия между собой. Если мы рассматриваем множества, наделённые той или иной структурой, то их взаймодействия друг с другом — это отображения из одних в другие, сохраняющие эту структуру. Изучать такие взаймодействия можно по двум направлениям: выяснять внутреннее устройство каждого отдельно взятого отображения, либо описать строение всего множества взаймодействий, рассматривая его как некий новый математический объект. Первую возможность демонстрируют теоремы о гомоморфизмах полей и колец, доказанные нами в первых лекциях. В этой лекции мы обсудим вторую возможность.

1.1. Эндоморфизмы и симметрии. Сразу ясно, что множество отображений наделено естественной алгебраической структурой. А именно, последовательно выполняя два отображения:

$$f\colon X \longrightarrow Y \quad \text{и} \quad g\colon Y \longrightarrow Z$$

мы получаем новое отображение $g \circ f : X \longrightarrow Z$, называемое *композицией* f и g (обратите внимание на то, что *первое* из двух последовательно выполнямых отображений в обозначении $g \circ f$ записано *справа*). Операция композиции, очевидно, определена не для любых пар (f, g), но уж если определена, то ассоциативна: $(h \circ g) \circ f = h \circ (g \circ f)$, хотя и не коммутативна. Мы уже встречались с подобной ситуацией, когда изучали алгебру матриц (что не удивительно, ибо матрицы представляют собой лишь удобное алгебраическое обозначение для *линейных отображений* векторных пространств и модулей).

Задача 10.1. Придумайте пример двух некоммутирующих отображений из некоторого множества X в себя.

Если ограничиться рассмотрением одного единственного объекта X,то композиция уже будет определена для любых $f, g : X \longrightarrow X$. Множество всех отображений из X в себя (сохраняющих алгебраическую структуру на X, буде таковая имеется) наазывается *полугруппой эндоморфизмов* объекта X и обозначается $\mathrm{End}(X)$. Взаимно-однозначные эндоморфизмы $f : X \longrightarrow X$ называются *автоморфизмами* или *симметриями* объекта X и их совокупность (группа) обозначается $\mathrm{Aut}\,(X)$.

Множество симметрий отражает взаймодействие объекта X самого с собой, т. е. его «внутренний характер», а потому является важнейшим источником информации об X. Способы судить об X глядя на $\mathrm{Aut}\,(X)$ называются *соображениями симметрии*. С древнейших времён они имеют статус наиболее изящных среди физических и математических рассуждений. Говоря по-учёному, свойства X адекватно кодируются алгебраической структурой на $\mathrm{Aut}\,(X)$. Изучению этой структуры и будет посвящена настоящая лекция. Прежде всего заметим, что ввиду взаимной однозначности у каждой симметрии $X \xrightarrow{f} X$ имеется *обратная симметрия* $X \xleftarrow{f^{-1}} X$.

Задача 10.2. Докажите, что если X является кольцом (или модулем) и $X \xrightarrow{f} X$ является взаимно-одноэначным гомоморфизмом, то обратное отображение также будет гомоморфизмом.

Множества симметрий с первой половины XIX века стали называть *группами*. Понятие абстрактной группы возникло в XX веке и служит для аксиоматизации алгебраических свойств групп симметрий (которые в XIX веке не считали нужным уточнять, ибо они были всем очевидны из контекста.)

1.2. Определение. *Группой называется всякое множество G, на элементах которого определена бинарная операция $G \times G \longrightarrow G : \quad (f, g) \longmapsto fg$, называемая композицией (а в последнее время чаще – умножением), удовлетворяющая аксиомам:*

(аксиомы группового закона композиции)

(i) ассоциативность:

$$(fg)h = f(gh) \qquad \forall f, g, h$$

(ii) существование единицы (тождественного отображения):

$$\exists e \in G\colon \quad eg = ge = g \quad \forall g \in G$$

(iii) существование обратного:

$$\forall g \in G \quad \exists g^{-1}\colon \quad gg^{-1} = g^{-1}g = e$$

Задача 10.3. Докажите, что единичный элемент единственен, а обратный элемент g^{-1} однозначно определяется по g.

1.3. Определение. *Абелевой группой называется всякая группа G, в которой композиция коммутативна: $fg = gf \quad \forall f, g \in G$.*

В этом случае в аксиомах (ii) и (iii) можно отбросить левое равенство, и аксиомы композиции превратятся в аксиомы сложения векторов. Поэтому операцию в абелевой группе обычно обозначают знаком «+».

1.4. Определение. *Отображение групп $\varphi\colon\ G_1 \longrightarrow G_2$ называется **гомоморфизмом групп**, если в группе G_2 имеем $\varphi(gh) = \varphi(g)\varphi(h) \quad \forall g, h \in G_1$. **Эпи-**, **моно-** и **изоморфизмы** определяются как обычно.*

§2. Примеры групп

2.1. Подгруппы. Как уже говорилось, группы чаще всего реализуются как подмножества в множестве $\mathrm{Aut}\,(X)$ всех взаимно-однозначных отображений того или иного множества X в себя. Очевидно, что $\mathrm{Aut}\,(X)$ само является группой. Для того чтобы подмножество H группы G составляло группу относительно имеющейся в G композиции необходимо и достаточно, чтобы $\forall h \in H$ обратное отображение h^{-1} также лежало в H и чтобы $\forall h_1, h_2 \in G$ их композиция $h_1h_2 \in G$. Такие $H \subset G$ называются *подгруппами* в G. Как всегда, эти два условия можно заменить одним.

Задача 10.4. Докажите, что подмножество H в группе G тогда и только тогда составляет группу относительно композиции, имеющейся в G, когда

$$h_1h_2^{-1} \in H \qquad \forall h_1, h_2 \in H\ .$$

2.2. Симметрическая группа $\mathfrak{S}_n \overset{\text{def}}{=} \mathrm{Aut}\,(\{1, 2, \dots, n\})$ — это группа всех взаимно-однозначных отображений множества из n элементов[1] в себя. Каждое такое отображение осуществляет попросту перестановку чисел в строчке $(1, 2, 3, \dots, n)$, поэтому $\mathfrak{S}_n$ иногда называют *группой перестановок*.

Мы уже встречались с группой $\mathfrak{S}_n$ в лекции 6 при исследовании полилинейных косых форм. Эта группа также незримо присутствовала в лекции 8, когда мы занимались симметрическими многочленами. Поскольку перенумерацию переменных в многочлене $f(x_1, \dots, x_n)$ можно воспринимать как результат подстановки в f вместо набора переменных $(x_1, \dots, x_n)$ нового набора переменных $(y_1, \dots, y_n)$, полученного из него перестановкой букв, группу $\mathfrak{S}_n$ называют также *группой подстановок* n аргументов.

Задача 10.5. Вспомните, колько всего подстановок имеется в $\mathfrak{S}_n$.
Ответ: $n!$.

2.2.1. Предложение. *Любая конечная группа из n элементов допускает гомоморфное вложение в $\mathfrak{S}_n$.*

Доказательство. Занумеруем элементы группы G и сопоставим каждому элементу $h \in G$ взаимно-однозначное отображение множества этих номеров на себя, индуцированное умножением на h: номер k, соответствующий элементу $g \in G$, переведем в номер элемента hg.

[1] в качестве которых обычно берут первые n натуральных чисел

Отображение номеров будет взаимно-однозначным, поскольку взаимно-однозначным будет отображение $g \mapsto hg$ (ибо $hg_1 = hg_2$ после умножения слева на h^{-1} превращается в $g_1 = g_2$). Построенное отображение $G \longrightarrow \mathfrak{S}_n$, очевидно, является гомоморфизмом и инъективно, поскольку если h_1 и h_2 одинаково переставляют элементы G, то в частности и $h_1 e = h_2 e$, т. е. $h_1 = h_2$.
□

Задача 10.6. Докажите что любая абстрактная группа изоморфна некоторой подгруппе группы всех взаимно-однозначных отображений подходящего множества X в себя.

2.3. Группа Галуа. Пусть $f \in \mathbb{Q}[x]$ - неприводимый многочлен и $K \supset \mathbb{Q}$ - поле разложения f (т. е. поле, в котором f раскладывается на линейные множители, и которое вкладывается в любое другое такое поле). Поле K можно получить, последовательно присоединяя к $\mathbb{Q}$ недостающие корни f (см. лекцию 3). Группа автоморфизмов поля K называется *группой Галуа* многочлена f над $\mathbb{Q}$ и обозначается $\mathrm{Gal}(f/\mathbb{Q})$ или $\mathrm{Gal}(K/\mathbb{Q})$ или просто $\mathrm{Gal}(f)$.

Пусть $(\vartheta_1, \ldots, \vartheta_n)$ — множество всех (автоматически попарно-различных) корней f в K. Любой элемент из K может быть выражен в виде значения некоторого многочлена $F(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ на наборе $(\vartheta_1, \ldots, \vartheta_n)$, поэтому действие любого автоморфизма $\sigma \colon K \longmapsto K$ из группы Галуа однозначно опредеыяется тем, как он действует на ϑ_i. С другой стороны, всякий автоморфизм поля K действует тождественно на простом подполе $\mathbb{Q} \subset K$, в частности, переводит в себя коэффициенты f, а стало быть отображает корни f в корни f. Следовательно, группа Галуа $\mathrm{Gal}(f)$ отождествляется с подгруппой в группе $\mathfrak{S}_n$ перестановок корней $(\vartheta_1, \ldots, \vartheta_n)$.

Группы Галуа были впервые рассмотрены Лагранжем в 1770г для того, чтобы описать такие полиномиальные выражения от $x_1, \ldots, x_n$, значения которых на корнях $(\vartheta_1, \ldots, \vartheta_n)$ данного многочлена лежат в $\mathbb{Q}$. Если значение $F(\vartheta_1, \ldots, \vartheta_n) \in \mathbb{Q}$, то (по определению группы Галуа) оно не меняется при всех перестановках корней ϑ_i из группы Галуа. *Теорема Лагранжа* утверждает, что верно и обратное:

2.3.1. Предложение. (Теорема Лагранжа) *Если функция не меняет значение при всех перестановках из группы Галуа, то это значение рационально.*

2.3.2. Комментарий: Из основной теоремы о симметрических многочленах тривиально следует, что таковыми заведомо являются функции от $\vartheta_1, \ldots, \vartheta_n$, инвариантные относительно *вообще всех* перестановок ϑ_i, ибо такие функции выражаются через коэффициенты уравнения. Теорема Лагранжа является более тонким фактом, поскольку устанавливает рациональность не только симметрических функций, но функций, инвариантных относительно, вообще говоря, меньшей, группы Галуа. Поэтому равенство $F(\vartheta_1, \ldots, \vartheta_n) = q \in \mathbb{Q}$ для такой функции F означает наличие *нетривиального* соотношения между корнями, не вытекающего из теоремы Виета. Ясно, что чем меньше группа Галуа, тем больше у нас таких соотношений, и тем проще решать уравнение. И наоборот, уравнения, группа которых совпадает с $\mathfrak{S}_n$, максимально трудны для решения, ибо между их корнями нет никаких соотношений, кроме вытекающих из теоремы Виета.

2.3.3. Набросок доказательства теоремы Лагранжа. В терминах полей теорема

Лагранжа утверждает, что если элемент $\alpha \in K$ инвариантен относительно всех автоморфизмов K, то $\alpha \in \mathbb{Q}$. Чтобы убедиться в этом, надо уметь строить для каждого $\alpha \notin \mathbb{Q}$ автоморфизм поля K, сдвигающий α. Мы наметим доказательство в серии задач:

Задача 10.7. Докажите, что K конечномерно как векторное пространство над $\mathbb{Q}$.
Указание: вспомните явное построение K.

Задача 10.8. Докажите, что все элементы $\alpha \in K \setminus \mathbb{Q}$ алгебраичны над $\mathbb{Q}$ и имеют степень ≥ 2.
Указание: векторы $1, \alpha, \alpha^2, \ldots$ не могут быть линейно независимы, ибо $\dim(K) < \infty$.

Задача 10.9. Пусть $\alpha \in K \setminus \mathbb{Q}$ и $f \in \mathbb{Q}[x]$ — минимальный многочлен для α. Докажите, что отображение, переводящее α в любой другой корень f, единственным образом продолжается до автоморфизма поля $\mathbb{Q}[\alpha]$ (наименьшего подполя в K , содержащего α).

Задача 10.10. Докажите, что автоморфизм из предыдущей задачи можно продолжить с $\mathbb{Q}[\alpha]$ на всё поле K.
Указание: надо вместо расширения $K \supset \mathbb{Q}$ рассмотреть расширение $K \supset \mathbb{Q}[\alpha]$ и проделать с ним всё то же самое.

2.4. Группы многогранников. Отображение пространства на себя, сохраняющее расстояние между точками, называется *движением.* Очевидно, движения составляют подгруппу в группе всех взаимно-однозначных отображений $\mathbb{R}^3$ на себя. Движения бывают *собственные* и *несобственные*, смотря по тому, переводят они стандартно ориентированный базис в $\mathbb{R}^3$ в стандартный, или в нестандартный (см. рис.3 на стр. 90). Движение F тогда и только тогда является собственным, когда его можно непрерывно продеформировать в тождественное, т. е. построить такое непрерывно зависящее от $t \in [0,1]$ семейство движений $F(t)$, что $F(0) =$ тождественmому движению, а $F(1) = F$. Собственные движения составляют подгруппу в группе движений. Движения (соответственно собственные движения), переводящие в себя фиксированную фигуру $\mathfrak{F} \subset \mathbb{R}^3$ составляют подгруппу в группе всех движепий (соответственно всех собственных движений). Она называется *группой фигуры* $\mathfrak{F}$ (соответственно *собственной группой фигуры* $\mathfrak{F}$)

2.4.1. Пример. Группа самосовмещений правильного плоского n-угольника в пространстве называется *группой диэдра порядка* $2n$ и обозначается $Д_n$. Она состоит из $2n$ элементов: n поворотов на углы $2\pi k/n \quad (k = 0, 1, \ldots n-1)$ и n симметрий (т. е. поворотов на $180°$ вокруг прямых в пространстве). При чётном n оси симметрий бывают двух типов: соединяющие противоположные вершины и соединяющие середины противоположных рёбер. При нечётном n все оси одинаковы (см. рис.1)

2.4.2. Пример. Группа собственных самосовмещений правильного тетраэдра состоит из 12 вращений вокруг его центра: тождественного самосовмещения, восьми поворотов на $\pm 120°$ вокруг осей, проходящих через вершину и центр противоположной грани (см. рис.2), и трёх поворотов на $180°$ вокруг осей, проходящих через середины противоположных рёбер. Никаких других собственных симметрий нет.

В самом деле, зафиксируем какие-либо четыре вращения t_1, t_2, t_3, t_4, переводящие вершину

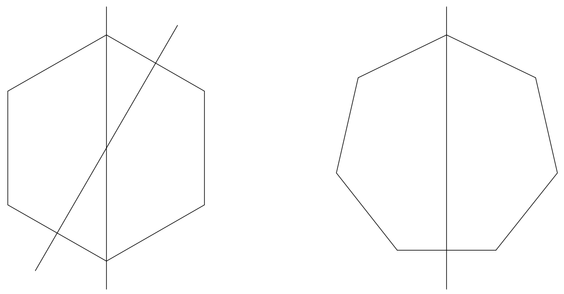


Рис. 1. Геометрически различные оси диэдров.

1 соответственно в вершины 1, 2, 3 и 4, и пусть s_0, s_1, s_2 – это три (с учётом тождественного) вращения тетраэдра, сохраняющие вершину 1 на месте. Поскольку движение вполне определяется тем, куда оно переводит вершины, каждое вращение можно единственным способом записать в виде $g = s_i t_j$, так что мы действительно имеем ровно $3 \cdot 4 = 12$ вращений. Нетрудно дать явное описание всех подгрупп группы тетраэдра. Ясно, что она содержит 4 подгруппы, состоящие каждая из трёх (с учётом тождественного) поворотов вокруг прямой, проходящей через вершину и центр противоположной грани. Кроме того, три поворота на 180° вокруг прямых, соединяющих середины противоположных ребер, вместе с тождественным преобразованием составляют подгруппу из 4 элементов (убедитесь в этом!). Она называется *квадратичной группой Клейна.*

Задача 10.11. Убедитесь, что других подгрупп в группе тетраэдра нет.

Задача 10.12. Сколько вращений имеется в собственной группе куба?

Задача 10.13. Сколько движений в полной группе тетраэдра?

2.5. Разбиение группы на смежные классы. Пусть $H \subset G$ - подгруппа в группе. Тогда мы можем рассмотреть множество всех «параллельных переносов» gH подгруппы H на всевозможные $g \in G$. Множество

$$gH \stackrel{\text{def}}{=} \{gh:\ h \in H\}$$

называется *левым смежным классом* группы G по подгруппе H. Смежные классы составляют разбиение G на *непересекающиеся подмножества*. Действительно, если $g_1H \bigcap g_2H \neq \emptyset$ и $g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in H$, то $g_1 = g_2h_2h_1^{-1}$, а т. к. H – подгруппа, то $h_2h_1^{-1} = h \in H$. Поэтому $g_1 \in g_2H$, а стало быть $g_1H \subset g_2H$. По аналогичным причинам имеется и обратное включение $g_2H \subset g_1H$, так что $g_1H = g_2H$, если только $g_1H \bigcap g_2H \neq \emptyset$.

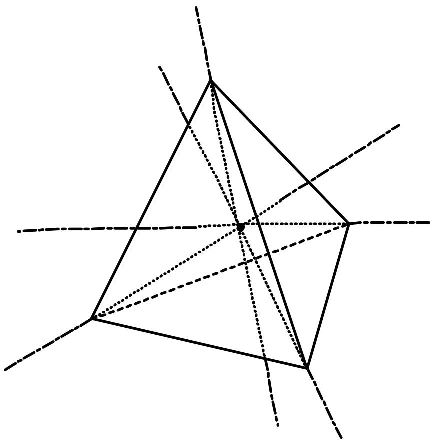


Рис. 2. Оси третьего порядка в правильном тетраэдре

Кроме того, все смежные классы состоят из "одинакового числа элементов", а точнее говоря, умножение на g слева: $h \mapsto gh$ задает взаимно-однозначное соответствие между H и gH (обратным к нему будет умножение элементов gH слева на g^{-1}). Следствием такого разбиения G на непересекающиеся биективно соответствующие друг другу смежные классы является

2.6. Теорема. (Теорема Лагранжа.) *Число элементов конечной группы G делится нацело на число элементов любой её подгруппы $H \subset G$.*

2.7. Порядок и индекс. Число элементов в конечной группе G называется *порядком группы* и обозначается $|G|$. Число смежных классов группы G по подгруппе H называется *индекспм подгруппы* H в G и обозначается $|G : H|$.

2.7.1. Следствие. *Если $|G| < \infty$, то $|H| \cdot |G : H| = |G| \quad \forall$ подгруппы $G \subset H$.*

2.8. Циклические группы. Произведения $\underbrace{\varrho \cdot \varrho \cdot \dots \cdot \varrho}_{n}$ и $\underbrace{\varrho^{-1} \cdot \varrho^{-1} \cdot \dots \cdot \varrho^{-1}}_{n}$ обозначаются через ϱ^n и ϱ^{-n} соответственно. Группа G называется *циклической*, если все её элементы являются целыми степенями некоторого одного элемента $\varrho \in G$, называемого *образующей*.

Множество всех степеней ϱ^n, $n \in \mathbb{Z}$), произвольного элемента ϱ в любой группе составляет циклическую подгруппу, называемую *циклической подгруппой, порождённой ϱ*. Если порядок этой группы конечен, то он называется также *порядком элемента ϱ* (и сам ϱ называется в этом случае *элементом конечного порядка*).

> Задача 10.14. Докажите, что порядок элемента $g \in G$ можно иначе описать как наименьшее $n \in \mathbb{N}$, такое что $g^n = e$.

2.8.1. Следствие. *Всякий элемент конечной группы имеет конечный порядок и этот порядок делит порядок группы.*

2.8.2. Следствие. *Группа простого порядка не содержит нетривиальных подгрупп (отличных от $\{e\}$ и от самой себя).*

> Задача 10.15. Докажите, что всякая циклическая группа порядка n изоморфна аддитивной группе кольца $\mathbb{Z}/n\mathbb{Z}$ (в частности все её элементы представляются *натуральными* степенями образующей.

§3. Действие группы на множестве

Ситуация, когда абстрактная группа G выступает как группа отображений какого-либо множества X в себя, формализуется так:

3.1. Определение. *Действием группы G на множестве X называется отображение*

$$G \times X \longrightarrow X \; : \quad (g, x) \mapsto g(x) \; ,$$

удовлетворяющее условиям: $gh(x) = g(h(x)) \quad \forall\, g, h \in G$ и $e(x) = x \quad \forall\, x \in X$.

3.2. Терминология. Поскольку каждый элемент $g \in G$ обладает обратным, все отображения $X \xrightarrow{g} X$, индуцированные действием, являются взаимно-однозначными. Поэтому действие группы G на множестве X можно иначе описать как гомоморфизм $G \longrightarrow \operatorname{Aut} X$ из G в группу $\operatorname{Aut} X$ всех биекций X на себя.

Действие называется *точным*, если этот гомоморфизм инъективен, т. е. разные элементы $g \in G$ задают разные отображения $X \xrightarrow{g} X$.

Действие называется *транзитивным*, если $\forall x_1, x_2 \in X \quad \exists g \in G: \quad g(x_1) = x_2$, т. е. любой элемент из X можно перевести в любой другой подходящим преобразованием из G.

Множество всех $g \in G$, оставляющих на месте некий фиксированный элемент $x \in X$ (т. е. таких что $g(x) = x$) называется *стабилизатором* элемента x и обозначается G_x. Стабилизатор, очевидно, является подгруппой в G.

3.3. Орбиты. Множество $x \in X$, которые можно получить из данного элемента $x_0 \in X$ при помощи преобразований из G называется *орбитой* элемента x_0 и обозначается $G(x_0)$. Таким образом, действие транзитивно, если орбита каждого элемента совпадает со всем X. В общем случае множество X, на котором действует группа G, *распадается в объединение непересекающихся орбит*.

Действительно, если $G(x_1) \bigcap G(x_2) \neq \emptyset$ и $x = gx_1 = hx_2$ для каких-то $g, h \in G$, то $x_1 = g^{-1}hx_2$. Потому $x_1 \in G(x_2)$, а значит $G(x_1) \subset G(x_2)$. Аналогично, $G(x_2) \subset G(x_1)$, — так что пересекающиеся орбиты в действительности совпадают, и действие группы G на X можно изучать отдельмо на каждой орбите (где оно транзитивно).

3.3.1. Лемма. *Пусть группа G действует на некоторпм множестве X. Тогда орбита каждого элемента $x \in X$ находится в биективном соответствии с левыми смежными классами группы G по подгруппе G_x.*

Доказательство. Сопоставим каждому элементу gx смежный класс gG_x. Это сопоставление корректно, поскольку из равенства $g_1x = g_2x$ вытекает, что $g_1^{-1}g_2 \in G_x$, а значит

$$g_1G_x = g_1(g_1^{-1}g_2)G_x = g_2G_x.$$

Обратное отображение, переводящее смежный класс gG_x в элемент gx также, очевидно, корректно, а потому мы имеем дело с биекцией.

□

3.3.2. Следствие. (Формула для длины орбиты.) *Если G конечна, то $|G(x)| = |G| : |G_x|$.*

□

3.3.3. Следствие. *Стабилизаторы всех элементов одной орбиты состоят из одного и того же числа элементов.*

□

Это следствие можно уточнить. А именно, пусть H - это стабилизатор элемента x, а $y = g(x)$. Тогда стабилизатор y есть $gHg^{-1} = \{ghg^{-1} \quad \forall h \in H\}$. Действительно,

$$gHg^{-1}y = gHg^{-1}gx = gHx = gx = y$$

и если $hy = y$, то

$$g^{-1}hgx = g^{-1}hy = g^{-1}y = x$$

т. е. $g^{-1}hg \in H$, а значит $h \in gHg^{-1}$. Легко видеть, что отображение $G \xrightarrow{\mathrm{Ad}\,(g)} G$, заданное правилом $h \longmapsto ghg^{-1}$, является *автоморфизмом*[2] группы G. Наше уточнение предыдущего следствия теперь можно сформулировать так:

3.3.4. Следствие. *Стабилизаторы элементов x и gx сопряжены при помощи g:*

$$G_{gx} = gG_xg^{-1}\ .$$

□

Задача 10.16. Докажите, что отображение $G \xrightarrow{\mathrm{Ad}} \mathrm{Aut}\, G$, переводящее элемент $g \in G$ в автоморфизм сопряжения $G \xrightarrow{\mathrm{Ad}(g)} G$ является гомоморфизмом[3].

3.4. Нормальные подгруппы и простота. Подгруппа $H \subset G$ называется *инвариантной* (или *нормальной*), если $gHg^{-1} = H \quad \forall g \in G$, т. е. если все внутренние автоморфизмы группы G сохраняют H (в этом случае пишут $H \triangleleft G$). Группа G называется *простой*, если у неё нет нормальных подгрупп, отличных от $\{e\}$ и G. В частности, све конечные группы простого порядка являются простыми.

§4. Факторизация

4.1. Корректность группового закона на факторе. Выясним, когда на фактор-множестве группы G по какому-либо разбиению на классы можно ввести структуру группы, индуцированную с G, т. е. определив групповую операцию над классами разбиения формулой $[h][g] = [hg]$.

Как и в случае колец, легко видеть, что главное препятствие состоит в возможной *некорректности* этого определения, поскольку если оно корректно, аксиомы группы будут тривиально переноситься с группы G на фактор, в частности, единицей в факторе будет класс $[e]$, а обратным классом к классу $[g]$ будет класс $[g^{-1}]$.

Для корректности правила $[h][g] = [hg]$ необходимо прежде всего, чтобы класс $[e]$ *составлял нормальную подгруппу* в G. Действительно, $\forall g \in [e]$ класс $[g^{-1}]$ должен совпасть с $[e^{-1}] = [e]$, и стало быть, $g^{-1} \in [e]$. Аналогично, $\forall g, h \in [e]$ класс $[gh] = [g][h] = [e][e] = [e]$, т. е. $gh \in [e]$. Поэтому $[e]$ – подгруппа в G. Более того, $\forall g \in G$ и $\forall h \in [e]$ имеем

$$[ghg^{-1}] = [g][h][g^{-1}] = [g][e][g^{-1}] = [geg^{-1}] = [e]$$

откуда $g[e]g^{-1} \subset [e] \quad \forall g \in G$, а значит $g[e]g^{-1} = [e]$ (т. к. заменив g на g^{-1}, получим обратное включение).Поэтому $[e]$ – нормальная подгруппа.

Второе необходимое условие — классы разбиения должны совпадать с левыми смежными классами по $[e]$. Действительно, если $h \in [g]$, то

$$[e] = [gg^{-1}] = [g][g^{-1}] = [h][g^{-1}] = [hg^{-1}]$$

---

[2]он называется *автоморфизмом сопряжения* элементом g

[3]его образ называется группой *внутренних автоморфизмов* группы G

поэтому $hg^{-1} \in [e]$, а значит $h \in g[e]$. Наоборот, если $h \in g[e], h = gt$ (где $t \in [e]$), то

$$[h] = [gt] = [g][t] = [g][e] = [ge] = [g],$$

т. е. $h \in [g]$.

4.2. Теорема. *Фактор-множество группы G, по некоторому разбиению тогда и только тогда является группой, когда это разбиение есть разбиение на (левые) смежные классы по некоторой нормальной подгруппе $H \triangleleft G$.*

Доказательство. Осталось проверить лишь корректность определения композиции классов $g_1H \circ g_2H = (g_1g_2)H$. Пусть $t_1 \in g_1H$, скажем $t_1 = g_1h_1$, и $t_2 \in g_2H$, скажем $t_2 = g_2h_2$. Тогда $t_1t_2 = g_1h_1g_2h_2$. Поскольку H нормальна, элемент $g_2^{-1}h_1g_2 \in H$, т. е. $g_2^{-1}h_1g_2 = h$ для некоторого $h \in H$, а потому $h_1g_2 = g_2h$, и стало быть $t_1t_2 = g_1g_2hh_2$. Но тогда $t_1t_2H = g_1g_2H$. Теорема доказана.
□

Слово "левый" в условии теоремы взято в скобки, поскольку имеет место

Задача 10.17. Докажите, что подгруппа $H \subset G$ тогда и только тогда нормальна, когда всякий левый смежный класс gH совпадает с правым смежным классом Hg.

4.3. Определение. *Группа смежных классов группы G по нормальной подгруппе H называется фактор-группой G по H и обозначается G/H.*

4.4. Строение гомоморфизмов. Отображение $G \longrightarrow G/H: \quad g \longmapsto gH$ является сюръективным гомоморфизмом группы G на фактор-группу G/H. Он называется *гомоморфизмом приведения по модулю H* или *гомоморфизмом факторизации.*

С произвольным гомоморфизмом $G \xrightarrow{\varphi} G$ можно, как обычно, связать

$$\begin{array}{lcl} \textit{ядро} \ \ \ker\varphi & = & \{g_1 \in G_1 \mid \ \ \varphi(g_1) = e\} \\ \textit{образ} \ \ \operatorname{im}\varphi & = & \{g_2 \in G_2 \mid \ \ \exists g_1 \in G_1: \quad \varphi(g_1) = g_2\} \end{array}$$

4.4.1. Лемма. $\operatorname{im}\varphi$ *является подгруппой в G_2, а $\ker\varphi$ — нормальной подгруппой в G_1.*

Доказательство. Поскольку $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, умножив обе части этого равенства на $\varphi(e)^{-1}$, мы получим $\varphi(e) = e$. Но тогда $\forall g \in G_1$ имеем

$$e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$$

откуда $\varphi(g^{-1}) = \varphi(g)^{-1}$. Поэтому $\forall g, h \in G_1$ имеем $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1}$, а стало быть, $\operatorname{im}\varphi \subset G_2$ — подгруппа.

Если $h_1, h_2 \in \ker\varphi$, то $\varphi(h_1h_2^{-1}) = \varphi(h_1)\varphi(h_2)^{-1} = e \cdot e = e$, а значит $\forall h_1, h_2 \in ker\varphi \quad h_1h_2^{-1}$ также лежит в $\ker\varphi$, и $\ker\varphi$ — подгруппа в G_1. Более того,

$$\forall g \in G_1 \qquad \varphi(g(\ker\varphi)g^{-1}) = \varphi(g)\varphi(\ker\varphi)\varphi(g)^{-1} = \varphi(g)e\varphi(g)^{-1} = e$$

поэтому $\ker\varphi$ — нормальна.

Последнее можно было бы проверить и иначе: $\operatorname{im}\varphi$ есть фактор-группа G_1 по разбиению, относящему в один класс все элементы, имеющие один и тот же образ относительно φ. По теореме, доказанной в предыдущем параграфе, это означает, что $\operatorname{im}\varphi$ есть фактор группы G_1 по (автоматически нормальной) подгруппе $\ker(\varphi)$, что и требовалось.

4.4.2. Следствие. *Каноническое отображение*

$$\tilde{\varphi}\colon \operatorname{im}\varphi \longrightarrow G_1/\ker\varphi$$

переводящее каждый $\varphi(g) \in \operatorname{im}\varphi$ в класс $[g] \bmod \ker\varphi$ является корректно определённым изоморфизмом между образом и фактором по ядру.

4.4.3. Следствие. *Простая группа не имеет нетривиальных фактор-групп, а всякий гомоморфизм из простой группы является либо вложением, либо отображением в единицу.*

4.4.4. Следствие. (Теорема о стороении гомоморфизма групп) *Всякий гомоморфизм групп $\varphi\colon\ G_1 \longrightarrow G_2$ может быть разложен в композицию эпиморфизма факторизации по ядру, изоморфизма этого фактора с образом и вложения образа:*

$$\begin{tikzcd}
G_1 \arrow[r, "\varphi"] \arrow[d, "\text{эпи}"'] & G_2 \\
G_1/\ker\varphi \arrow[r, "\tilde{\varphi}", "\text{изо}"'] & \operatorname{im}\varphi \arrow[u, "\text{моно}"']
\end{tikzcd}$$

§5. Симметрические группы

5.1. Группы многогранников Следующие ниже примеры служат неплохой иллюстрацией всех предыдущих конструкций с группами.

5.1.1. Изоморфизм $Д_3 \tilde{\to} \mathfrak{S}_3$. Группа $\mathfrak{S}_3$ перестановок множества $\{123\}$ состоит из шести перестановок:

$$E = (123), \qquad T = (231), \qquad T^{-1} = (312),$$

$$\sigma_{12} = (213), \qquad \sigma_{13} = (321), \qquad \sigma_{23} = (132).$$

Перестановки E, T, T^{-1} составляют нормальную циклическую подгруппу.

Группа треугольника $Д_3$ (т. е. множество всех движений трёхмерного пространства, переводящих в себя данный правильный треугольник) также состоит из шести элементов: трёх (с учётом тождественного) поворотов относительно центра, составляющих нормальную подгруппу, и ещё трёх симметрий. Если занумеровать вершины треугольника и сопоставить каждому самосовмещению треугольника соответствующую перестановку номеров вершин, мы получим (очевидно, инъективный) гомоморфизм из $Д_3$ в $\mathfrak{S}_3$. Следовательно, $Д_3$ и $\mathfrak{S}_3$ изоморфны.

Задача 10.18. Составьте таблицы умножения для $\mathfrak{S}_3$ и $Д_3$, и явным сравнением этих таблиц убедитесь, что $Д_3$ и $\mathfrak{S}_3$ изоморфны .

5.1.2. $\mathfrak{S}_4$ и тетраэдр. Обобщая предыдущую конструкцию на тетраэдр, мы можем построить гомоморфизм из полной группы тетраэдра в группу $\mathfrak{S}_4$ перестановок номеров его вершин. Он инъективен, поскольку имеет тривиальное ядро: если движение оставляет на месте все 4 вершины некоторого тетраэдра, то это движение тождественное (почему?). В группе $\mathfrak{S}_4$ имеется 24 перестановки. Но в полной группе тетраэдра также 24 движения: все вершины составляют одну орбиту нашей группы, а стабилизатор вершины состоит из трёх поворотов вокруг высот тетраэдра, проходящих через эту вершину, и трёх симметрий в плоскостях, проходящих через примыкающее к вершине ребро и середину противоположного ребра.

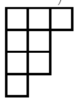
Задача 10.19. Докажите, что стабилизатор вершины изоморфен группе треугольника.

Следовательно, по формуле для длины орбиты (Сл.3.3.2), всего в группе тетраэдра имеется $4 \cdot 6 = 24$ движения, и стало быть, полная группа тетраэдра изоморфна $\mathfrak{S}_4$.

Собственные (сохраняющие ориентацию) вращения тетраэдра составляют, очевидно, нормальную подгруппу в группе тетраэдра. Соответствующая подгруппа в $\mathfrak{S}_4$ называется *знакопеременной группой* на четырёх элементах и обозначается $\mathfrak{A}_4$. Другое название для $\mathfrak{A}_4$,— *группа чётных перестановок*, — обусловлено тем, что каждая из 12 перестановок, составляющих $\mathfrak{A}_4$, может быть получена чётным числом транспозиций, т. е. перестановок какой-либо пары элементов. Действительно, этим свойством обладают все 8 циклов длины 3 (переставляющих по циклу какие-либо 3 элемента, а четвёртый не меняющие), соответствующие поворотам вокруг высот тетраэдра, а также три подстановки (2143), (4321), (3412) из квадратичной группы Клейна.

5.1.3. $\mathfrak{S}_4$ и собственная группа куба. Группа собственных самосовмещений куба состоит из 24 вращений (ибо у куба 8 вершин, а стабилизатор вершины состоит из трёх поворотов на $0°$ и $\pm 120°$ вокруг диагонали, проходящей через вершину). Занумеровав 4 диагонали куба цифрами 1 , 2 , 3 и 4 мы, как и выше, определяем инъективный гомоморфизм из группы куба в $\mathfrak{S}_4$. Поэтому $\mathfrak{S}_4$ изоморфна собственной группе куба.

Задача 10.20. Опишите явно все подгруппы в группе вращений куба. В частности, опишите, каким вращениям куба отвечают несобственные самосовмещения тетраэдра, а каким - собственные.

5.2. Цикловой тип перестановки. Рассмотрим в $\mathfrak{S}_n$ циклическую подгруппу, порождённую элементом g (обозначим её $\langle g \rangle$). Группа $\langle g \rangle$ действует на множестве $\{1, 2, \ldots, n\}$ символов, переставляемых группой $\mathfrak{S}_n$. По n° 3.3 это действие разбивает всё множество $\{1, 2, \ldots, n\}$ в объединение непересекающихся орбит относительно действия g. Эти орбиты называются *независимыми циклами*, поскольку каждая из них состоит из элементов $\{i, gi, g^2 i, \ldots\}$, циклически переставляемых элементом g, и действие g на каждом таком цикле происходит независимо. В частности, это означает, что $g = h_1 h_2 \ldots h_m$, где m - количество циклов, а h_i — циклическая перестановка элементов i-того цикла на 1 шаг. Такое разложение называется *разложением g в произведение независимых циклов*. Набор длин циклов составляет разбиение числа n и называется *цикловым типом* g. Удобно представлять его диаграммой Юнга. Например, перестановка $g \in \mathfrak{S}_8$, переводящая (12345678) в (51682374), распадается в произведение циклов $1 \to 5 \to 2 \to 1$ длины 3, $3 \to 6 \to 3$ длины 2, $4 \to 8 \to 4$ длины 2, $7 \to 7$ длины 1, и её цикловой тип изображается диаграммой Юнга:  .

Задача 10.21. Убедитесь, что две перестановки тогда и только тогда сопряжены в $\mathfrak{S}_n$, когда они имеют одинаковый цикловой тип.

Указание. Запишем в строки диаграммы Юнга номера элементов, циклически переставляемых соответствующими циклами перестановки g, в том порядке, в каком они переходят друг в друга при действии g. Если g и g_1 имеют одинаковый цикловой тип, то $g = hg_1h^{-1}$, где h отображает элемент $\alpha \in \{1, \ldots, n\}$ в элемент, стоящий в той же клеточке диаграммы g, в которой α стоит на диаграмме g_1.

5.3. Знакопеременная подгруппа $\mathfrak{A}_n \subset \mathfrak{S}_n$. Определённый нами в лекции 6 *знак перестановки* является, очевидно гомоморфизмом из симметрической группы $\mathfrak{S}_n$ в группу из двух элементов $\{\pm 1\}$ с операцией умножения. Ядро $\ker(sgn)$ состоит из всех чётных перестановок, которые, тем самым, образуют нормальную подгруппу индекса 2 в $\mathfrak{S}_n$. Она обозначается $\mathfrak{A}_n$ и называется *знакопеременной группой* или *группой чётных подстановок*.

Термин «знакопеременный» связан с тем, что подгруппа $\mathfrak{A}_n$ является *централизатором*[4] множества *знакопеременных* функций — таких функций от n переменных, которые меняют знак при транспозиции любой пары аргументов. Примером знакопеременного многочлена является произведение упорядоченных разностей:

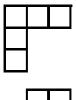
$$\delta(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) \, .$$

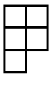
Задача 10.22. Докажите, что всякий знакопеременный многочлен делится (в кольце многочленов от n переменных) на произведение упорядоченных разностей, и частное от этого деления будет симметрическим многочленом.

Задача 10.23. Докажите, что перестановка тогда и только тогда чётна, когда в её цикловом типе число циклов чётной длины чётно.

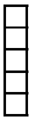
5.3.1. Строение группы $\mathfrak{A}_5$ Опишем классы сопряжённых элементов в $\mathfrak{A}_5$. Для этого сначала опишем классы элементов $\mathfrak{A}_5$, сопряжённых в $\mathfrak{S}_5$. Согласно предыдущему, такие классы соответствуют диаграммам Юнга веса 5 с чётным количеством строк чётной длины. Таких диаграмм имеется всего 4:

 – циклы длины 5, всего $4! = 24$шт. (почему?);

 – циклы длины 3, всего $2 \cdot \binom{5}{2} = 20$шт. (почему?);

 – пары независимых транспозиций, всего $5 \cdot 3 = 15$шт. (почему?);

[4]т. е. поточечно оставляет на месте все элементы

 – тождественная подстановка, 1шт.

Задача 10.24. Докажите, что все циклы длины 3 сопряжены между собой в $\mathfrak{A}_5$.

Задача 10.25. Докажите, что все пары транспозиций сопряжены между собой в $\mathfrak{A}_5$.

Задача 10.26. Докажите, что все циклы длины 5 образуют два класса сопряжённости в $\mathfrak{A}_5$: циклы, сопряжённые циклу $1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$, и циклы, сопряжённые циклу $2 \longrightarrow 1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$.

5.4. Теорема. *Группа $\mathfrak{A}_5$ проста.*

Доказательство. Если подгруппа $H \subset A$ — нормальная, то вместе с каждым элементом она содержит весь класс сопряжённых ему элементов. Всего таких классов в $\mathfrak{A}_5$,— как мы видели в задачах зад.10.24–зад.10.26,— имеется 5, и состоят они из 1, 12, 12, 20 и 15 элементов. Т.к. единица лежит в любой подгруппе, имеем:

$$|H| = 1 + 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4,$$

где все ε_k равны либо 1, либо 0. Непосредственная проверка показывает, что |H| делит $|\mathfrak{A}_5| = 60$ лишь в двух случаях: $\varepsilon_k = 1 \quad \forall k$ и $\varepsilon_k = 0 \quad \forall k$ (убедитесь!), так что непростота $\mathfrak{A}_5$ противоречит теореме Лагранжа (Теор.2.6).

Задача 10.27. Докажите, что все группы $\mathfrak{A}_n$ с $n \geq 5$ просты.

Указание. Воспользуйтесь индукцией. Вложите $\mathfrak{A}_{n-1}$ в $\mathfrak{A}_n$ как стабилизатор символа n, и докажите, что нетривиальная нормальная подгруппа в $\mathfrak{A}_n$ обязана иметь нетривиальное пересечение с $\mathfrak{A}_{n-1}$ (автоматически нормальное в $\mathfrak{A}_{n-1}$)), что противоречит индуктивному предположению о простоте $\mathfrak{A}_{n-1}$.

Задача 10.28. Докажите, что внутренние автоморфизмы составляют подгруппу индекса 2 в группе всех автоморфизмов группы $\mathfrak{A}_5$.

Указание. Всякий автоморфизм $\mathfrak{A}_5$ переводит цикл длины 5 в цикл длины 5 и является внутренним тогда и только тогда, когда переводит циклы длины 5 в сопряжённые циклы длины 5.

Задача 10.29. Докажите, что группа A_5 изоморфна собственной группе икосаэдра.

Указание. Найдите у икосаэдра 5 геометрических подконфигураций, переставляемых его вращениями.

Предметный указатель

Р

С

Я