Лекция 1
Идеалы в кольцах многочленов

▷Задание идеалов образующими ▷Нётеровость ▷Теоремы Гильберта о базисе и нулях полиномиального идеала ▷Нули однородных идеалов ▷Теория исключения и проблема построения результантов ▷Алгебраическая зависимость ▷Лемма о примитивном элементе ▷Конечно-порождённые расширения поля $\mathbb{C}$

§1 Теоремы Гильберта

1.1. Полиномиальные уравнения и идеалы. Пусть $\mathbb{A}_n$ – n-мерное аффинное пространство над полем $\mathbb{C}$ с координатами $(x_1, x_2, \ldots, x_n)$. Множество всех общих нулей какой-либо (возможно, бесконечной) системы алгебраических уравнений

$$f_\nu(x_1, \ldots, x_n) = 0 \ ; \quad f_\nu \in \mathbb{C}[x_1, \ldots, x_n] \tag{1-1}$$

называется *алгебраическим подмножеством* в $\mathbb{A}_n$. Алгебраическая геометрия изучает алгебраические множества или, если угодно, *геометрические свойства систем алгебраических уравнений*. В этом курсе мы остановимся на самых общих качественных свойствах подобного рода. А именно, мы будем пытаться упрощать системы уравнений и подыскивать критерии их совместности. Методы наши будут более алгебраическими, чем геометрическими, но геометрическую картинку всегда следует держать в голове.

Прежде всего ясно, что вместе с системой уранений (1-1) имеет смысл рассмотреть и все её следствия, коими являются уравнения вида $g(x) = 0$, где g пробегает всевозможные *конечные* линейные комбинации вида

$$g(x) = g_1(x) \cdot f_{\nu_1}(x) + g_2(x) \cdot f_{\nu_2}(x) + \cdots g_s(x) \cdot f_{\nu_s}(x) \ , \quad g_i \in \mathbb{C}[x_1, \ldots, x_n] \ .$$

Задача 1.1. Убедитесь, что такие g составляют идеал в кольце $\mathbb{C}[x_1, \ldots, x_n]$.

Этот идеал называется идеалом, *порождённым* семейством полиномов f_ν и обозначается (f_ν). Сами f_ν называются его *образующими*. Таким образом, мы всегда можем считать, что правые части системы (1-1) составляют идеал, а вопрос об упрощении системы уравнений превращается в вопрос о выборе хорошей системы образующих в данном идеале. Например, интересно, во всяком ли идеале можно выделить конечную систему образующих?

Задача 1.2. Докажите, что в кольце $k[x]$, где k – поле, каждый идеал является *главным* (порождается одним элементом).

Указание. В качестве образущей можно взять приведённый многочлен наименьшей степени.

Задача 1.3. Докажите, что идеалы $(x, y) \subset k[x, y]$, где k – поле, и $(2, x) \subset \mathbb{Z}[x]$ не являются главными.

1.1.1. Лемма. *Следующие условия на коммутативное кольцо R попарно-равносильны:*

(i) Всякий идеал $I \subset R$ конечно-порождён.

(ii) В произвольном семействе элементов f_ν из R можно выделить конечное подмножество $\{f_1, f_2, \dots, f_k\}$, через которое любой f_ν выражается в виде $f_\nu = \sum_{i=1}^{k} g_i f_i$ с подходящими $g_i \in R$ (разными для разных ν).

(iii) Всякая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subset I_2 \subset I_3 \subset \cdots$ в R стабилизируется, т.е. $\exists N \in \mathbb{N} : I_k = I_{k+1} \quad \forall\, k \geq N$

Доказательство. Очевидно, что из (ii) следует (i). Чтобы вывести (iii) из (i) рассмотрим объединение $I = \bigcup_k I_k$. Это идеал в R (проверьте!), и по (i) он порождается конечным набором элементов $\{f_1, f_2, \dots, f_k\}$. В качестве I_N в (iii) надо взять идеал, содержащий все f_i.

Наконец, чтобы из (iii) получить (ii) выберем среди f_ν какое либо f_1 и рассмотрим идеал $I_1 = (f_1)$. Если все f_ν лежат в I_1, то (ii) выполнено с $k = 1$. Если нет, фиксируем $f_2 \notin I_1$ и рассмотрим $I_2 = (f_1, f_2) \supset I_1$ и т.д. Если мы таким образом не построим конечную ситему, удовлетворяющую условию (ii), то получим бесконечную возрастающую цепочку *строго* вложенных друг в друга идеалов, что противоречит (iii).

□

1.1.2. Определение. *Кольцо R называется нётеровым если оно удовлетворяет перечисленным в Лм.1.1.1 равносильным условиям.*

1.2. Теорема. (Теорема Гильберта о базисе.) *Если кольцо R нётерово, то кольцо $R[x]$ также нётерово.*

Доказательство. Пусть $I \subset R[x]$ – любой идеал. Мы построим в I конечную систему образующих.

Задача 1.4. Убедитесь, что старшие коэффициенты всех многочленов из I составляют идеал в R.

Пусть этот идеал порождается старшими коэффициентами многочленов $f_1, f_2, \dots, f_k$ Включим все f_i в конструируемую нами ситему образующих идеала I. Пусть n – максимальная из степеней этих многочленов. Легко видеть, что всякий многочлен из I представляется по модулю идеала $(f_1, f_2, \dots, f_k)$ многочленом степени $\leq (n-1)$ (если $\deg g = d \geq n$, то старший член g можно сократить, вычтя подходящую линейную комбинацию многочленов $x^{d-\deg f_i} \cdot f_i$).

Задача 1.5. Убедитесь, что старшие коэффициенты всех многочленов степени $n-1$ из I составляют идеал в R.

Как и предыдущий, этот идеал порождается конечным числом элементов — старших коэффициентов многочленов $g_1, g_2, \dots, g_l$. Добавим и их к нашей системе образующих. Легко видеть, что по модулю всех f_i и g_j любой многочлен из I представляется многочленом степени $\leq (n-2)$. И так далее.

□

1.2.1. Следствие. *Кольцо многочленов $R[x_1, \dots, x_n]$ над нётеровым кольцом нётерово.*

□

1.2.2. Следствие. *Любая бесконечная система полиномиальных уравненений над нётеровым кольцом равносильна некоторой своей конечной подсистеме.*

□

Задача 1.6. Докажите, что фактор-кольцо нётерова кольца нётерово.
Указание: воспользуйтесь свойством (iii) из Лм.1.1.1.

1.2.3. Следствие. *Всякая конечно-порождённая алгебра A над нётеровым кольцом R нётерова.*

□

1.3. Алгебраические подмножества и идеалы. Обозначим через $V(I) \subset \mathbb{A}_n$ алгебраическое подмножество, заданное как множество всех общих нулей идеала $I \subset \mathbb{C}[x_1, \dots, x_n]$. Спрашивается, насколько однозначно восстанавливается I по $V(I)$? Ясно, что тут не всё так просто: скажем, над полем $\mathbb{R}$ несобственный идеал (1) и главный идел (x^2+1) задают одно и то же (пустое) алгебраическое множество. Над алгебраически-замкнутым полем на однозначное соответствие надежды тоже нет: множества нулей идеалов (x) и (x^2) совпадают.

Тем не менее, всякому алгебраическому множеству V можно канонически сопоставить некий идеал $I(V)$, называемый *идеалом алгебраического множества* V. По определению, он состоит из всех полиномов, зануляющихся в каждой точке V;

$$I(V) \stackrel{\text{def}}{=} \{g \in \mathbb{C}[x_1, \dots, x_n] \mid g(p) = 0 \ \forall\, p \in V\ \}\ .$$

Задача 1.7. Убедитесь, что $I(V)$ действительно идеал.

Очевидно, всегда имеет место включение $I \subset I(V(I))$. Спрашивается, как алгебраически характеризуются те идеалы, для которых имеет место равенство, и как описать соответствие $I \longmapsto I(V(I))$ в алгебраических терминах? Над полем $\mathbb{C}$ ответ даёт знаменитая теорема Гильберта о нулях.

1.4. Теорема. (Der Nullstellensatz.) *Для любого идеала $I \subset \mathbb{C}[x_1, \dots, x_n]$ справедливы следующие два утверждения:*

(i) $V(I) = \emptyset$ тогда и только тогда, когда $1 \in I$;

(ii) если f обращается в нуль во всех точках $V(I)$, то $f^k \in I$ для некоторого $k \in \mathbb{N}$.

Таким образом, $I(V(I))$ состоит из всех многочленов, некоторая степень которых лежит в I. В коммутативной алгебре совокупность

$$\{f \mid f^k \in I \text{ для некоторого } k\}$$

называется *радикалом* идеала I и обозначается $\mathrm{Rad}\,(I)$.

Задача 1.8. Убедитесь (не прибегая к теореме Гильберта), что радикал идеала является идеалом.

Идеалы, совпадающие со своими радикалами, называются *радикальными*. Тем самым, алгебраические подмножества в $\mathbb{A}_n(\mathbb{C})$ взаимно-однозначно соответствуют радикальным идеалам.

1.5. Доказательство теоремы Гильберта о нулях займёт остаток этого параграфа. Мы разобьём его на несколько шагов. По ходу дела нам понадобится алгебраическое описание всех конечнопорождённых расширений поля $\mathbb{C}$. Это описание будет получено нами в §3 (ибо оно находится в рамках не завищаей от теоремы Гильберта теории).

1.5.1. Редукция утверждения (ii) к утверждению (i) — это формальный трюк с уравнениями.

Пусть $f \in \mathbb{C}[x_1, \dots, x_n]$ обращается в нуль во всех точках $V(I) \subset \mathbb{A}_n$. Вложим $\mathbb{C}[x_1, \dots, x_n]$ в $\mathbb{C}[x_1, \dots, x_n, t]$ и рассмотрим в этом большем кольце идеал J, порождённый многочленами из I и ещё одним многочленом $g = 1 - t \cdot f$. Алгебраическое подмножество $V(J)$ в аффинном пространстве $\mathbb{A}_{n+1}$ с координатами $(x_1, \dots, x_n, t)$ пусто, ибо общие нули многочленов из I имеют вид (x, t), где $x \in V(I) \subset \mathbb{A}_n$, а в таких точках $g = 1$. Из утверждения (i) теоремы Гильберта следует тогда, что $1 \in J$.

Это означает, что найдутся конечные наборы многочленов $\{q_0, q_1, \dots, q_s\} \subset \mathbb{C}[x_1, \dots, x_n, t]$ и $\{f_1, f_2, \dots, f_s\} \subset I \subset \mathbb{C}[x_1, \dots, x_n]$ такие, что

$$q_0(x,t)(1 - tf(x)) + q_1(t,x)f_1(x) + \cdots + q_s(x,t)f_s(x) = 1 \ .$$

Написанное равенство есть равенство в кольце многочленов $\mathbb{C}[x_1, \dots, x_n, t]$. Если вместо переменных в него подставить "числа" из произвольного расширения $K \supset \mathbb{C}$, то получится верное равенство в поле K. Возьмём в качестве K поле рациональных функций $\mathbb{C}(x_1, \dots, x_n)$, а в качестве "числовых значений" x_ν и t подставим, соответственно, сами x_ν и дробь $1/f(x)$. Получим равенство

$$q_1(\frac{1}{f(x)}, x)f_1(x) + \cdots + q_s(\frac{1}{f(x)}, t)f_s(x) = 1 \ ,$$

справедливое в поле $\mathbb{C}(x_1, \dots, x_n)$. Все знаменатели в этом равенстве имеют вид f^d, и от них можно избавиться, умножая обе части на достаточно большую степень f^k. В результате получится равенство в кольце многочленов $\mathbb{C}[x_1, \dots, x_n]$, выражающее f^k через $f_1, f_2, \dots, f_s$ с полиномиальными коэффициентами. Это доказывает, что $f^k \in I$.

1.5.2. Доказательство утверждения (i). Мы должны проверить, что всякий идеал $I \subset \mathbb{C}[x_1, \dots, x_n]$, не содержащий 1 (т.е. отличный от всего кольца многочленов или, как ещё говорят, *собственный*) имеет нуль в $\mathbb{A}_n(\mathbb{C})$. Ясно, что такую проверку достаточно провести только для максимальных идеалов (напомню, что идеал $\mathfrak{m}$ называется *максимальным*, если он собственный и не содержится ни в каком большем собственном идеале).

> Задача 1.9. Убедитесь, что всякий собственный идеал содержится в некотором максимальном идеале.
>
> Указание: примените *лемму Цорна*[1] к совокупности всех собственных идеалов.
>
> Задача 1.10. Докажите, что идеал $\mathfrak{m}$ в коммутативном кольце R максимален тогда и только тогда, когда фактор-кольцо $R/\mathfrak{m}$ является полем.
>
> Указание: Полный прообраз в R собственного ненулевого идеала из $R/\mathfrak{m}$ является собственным идеалом, содержащим $\mathfrak{m}$.

Итак, мы должны предъявить нуль для любого максимального идеала $\mathfrak{m}$. Обозначим поле $\mathbb{C}[x_1, \dots, x_n]/\mathfrak{m}$ через K, и пусть

$$\mathbb{C}[x_1, \dots, x_n] \xrightarrow{\pi} K$$

каноническая проекция. Её ограничение на константы задаёт вложение поля $\mathbb{C}$ в K, так что мы можем рассматривать K как расширение поля $\mathbb{C}$. В частности, имеет смысл говорить о множестве нулей идеала $\mathfrak{m}$ в аффинном пространстве $\mathbb{A}_n(K)$ над полем K. Это множество не пусто: точка $\xi = (\xi_1, \xi_2, \dots, \xi_n)$, где $\xi_i = \pi(x_i)$, является общим нулём для всех многочленов из $\mathfrak{m}$, ибо $f(\xi) = f(\pi(x)) = \pi(f(x)) = f \pmod{\mathfrak{m}}$.

[1]См. *Ван дер Варден Алгебра* М."Наука" (1975) стр. 246 или *П. С. Александров Введение в теорию множеств и общую топологию* М."Наука" (1977) стр. 62 – 84

Таким образом, все многочлены из $\mathfrak{m}$ имеют общий нуль над некоторым конечно-порождённым расширением $K \supset \mathbb{C}$. Для того, чтобы спустить этот нуль в $\mathbb{A}_n(\mathbb{C})$ мы воспользуемся следующим описанием всех конечно-порождённых расширений поля $\mathbb{C}$.

1.5.3. Предложение. *Всякое конечно-порождённое расширение $K \supset \mathbb{C}$ изоморфно расширению поля рациональных функций $R = \mathbb{C}(t_1, \dots, t_m)$ при помощи одного алгебраического над R элемента ζ.*

Иными словами, $K = R[z]/(\varphi(z))$, где

$$\varphi(z) = z^r + a_1 z^{r-1} + \dots + a_{r-1} z + a_r \in R[z]$$

есть минимальный многочлен элемента ζ (неприводимый над R).

Доказательство. См. n° 3.4.

1.5.4. Завершение доказательства утверждения (i). Пусть в обозначениях предыдущего предложения координаты $(\xi_1, \xi_2, \dots, \xi_n)$ общего нуля в K^n всех многочленов из $\mathfrak{m}$ представляются как элементы кольца $R[z]/(\varphi(z))$ в виде $\xi_\nu = \xi_\nu(z) \pmod{\varphi(z)}$ с $\xi_\nu \in R[z]$. Пусть $f \in \mathbb{C}[x_1, \dots, x_n]$ пробегает конечную систему образующих идеала $\mathfrak{m}$. Равенство $f(\xi) = 0$ в K означает, что найдётся $\psi_f(z) \in R[z]$ (зависящий от f), такой что

$$f(\xi_1(z), \xi_2(z), \dots, \xi_n(z)) = \varphi(z) \cdot \psi_f(z) \tag{1-2}$$

Коэффициенты многочленов $\xi_\nu(z), \varphi(z), \psi_f(z)$ лежат в $R = \mathbb{C}(t_1, \dots, t_m)$. Если вместо t_i подставить конкретные числовые значения так, чтобы знаменатели этих коэффициентов не обратились в нуль, то мы получим многочлены $\tilde{\xi}_\nu(z), \tilde{\varphi}(z), \tilde{\psi}_f(z)$ с комплексными коэффициентами. Если после этого подставить в них всместо z какой-либо комплексный корень z_0 многочлена $\tilde{\varphi}(z)$, то равенства (1-2) превратяться в числовые рвенства

$$f(\tilde{\xi}_1(z_0), \tilde{\xi}_2(z_0), \dots, \tilde{\xi}_n(z_0)) = 0 ,$$

означающие, что точка в $\mathbb{C}^n$ с координатами $x_\nu = \tilde{\xi}_\nu(z_0)$ является общим нулём всех образующих f идеала $\mathfrak{m}$, т.е. общим нулём для всех многочленов этого идеала.

Проделанный выше выбор значений t_i, не зануляющий знаменателей, возможен вследствие того, что поле $\mathbb{C}$ бесконечно, а знаменателей — конечное число. Взяв произведение всех знаменателей, мы получим некий ненулевой многочлен из $\mathbb{C}[t_1, \dots, t_m]$, и нам достаточно найти в $\mathbb{C}_m$ точку, где он не обращается в нуль.

> Задача 1.11. Докажите, что ненулевой многочлен от m переменных над бесконечным полем не может тождественно зануляться как функция на аффинном пространстве $\mathbb{A}_m$.

Теорема Гильберта доказана.

□

§2 Простейшие следствия из теорем Гильберта

2.1. Максимальные идеалы в кольце многочленов. В качестве первого следствия теоремы о нулях мы сейчас опишем все максимальные идеалы в кольце многочленов $\mathbb{C}[x_1, \dots, x_n]$. Пусть $p \in \mathbb{A}_n$ – произвольная точка. Идеал $I(p)$ всех полиномов, обращающихся в нуль в точке p, максимален, ибо фактор по нему – поле $(\mathbb{C}[x_1, \dots, x_n]/I(p) \cong \mathbb{C}$ и каноническая проекция

$\mathbb{C}[x_1,\dots,x_n]/I(p) \xrightarrow{\pi} \mathbb{C}$ сопоставляет многочлену f его значение $f(p)$). Наоборот, по теореме Гильберта всякий максимальный идеал $\mathfrak{m}$ имеет нуль в некоторой точке $p \in \mathbb{A}_n$, а стало быть, $\mathfrak{m} \subset I(p)$, и из-за максимальности $\mathfrak{m}$ это включение в действительности является равенством.

Итак, максимальные идеалы в $\mathbb{C}[x_1,\dots,x_n]$ — это идеалы точек, и только они. Спрашивается, а как устроены идеалы $I \in \mathbb{C}[x_1,\dots,x_n]$, для которых $V(I)$ состоит из одной точки $p \in \mathbb{A}_n$, т.е. такие идеалы, радикалы которых максимальны? Для удобства давайте считать, что $p = (0,0,\dots,0)$ – начало координат. Обозначим через $S^k \cong S^k(\mathbb{C}^{n*})$ пространство всех однородных многочленов степени k от $x_1, x_2, \dots, x_n$.

Задача 1.12. Вычислите размерность S^k.

Задача 1.13. Пусть $V \cong \mathbb{C}^n$ – векторное пространство, подлежащее рассматриваемому нами аффинному пространству $\mathbb{A}_n$. Постройте естественный изоморфизм между пространством однородных многочленов степени k на V (т.е. фукций f из V в $\mathbb{C}$, таких что $f(\lambda v) = \lambda^k f(v)\ \ \forall\, v \in V\ ,\ \ \forall\, \lambda \in \mathbb{C}$) и пространством полилинейных симметричных k-форм на V (т.е. k-той симметрической степенью V^*).

По традиции мы будем называть многочлены из S^k *однородными формами* степени k.

2.1.1. Предложение. *$V(I)$ тогда и только тогда совпадает с началом координат, когда $\exists N$, такое что $S^k \subset I\ \forall k \geq N$.*

Доказательство. Пусть $V(I)$ содержит точку, отличную от начала координат, и пусть у этой точки, скажем, $x_1 \neq 0$. Тогда форма x_1^k не лежит в I ни при каком k, т.е. $S^k \not\subset I\ \ \forall\, k \in \mathbb{N}$.

Наоборот, пусть $V(I)$ — это начало координат. Тогда все координатные функции x_ν зануляются на $V(I)$, и по теореме Гильберта существует m такое, что $x_\nu^m \in I$ при всех $\nu = 1,2,\dots,n$. Но тогда $S^k \subset I$ при всех $k \geq N = n(m-1)+1$.

□

При помощи параллельного переноса системы координат мы сразу же получаем из этого предложения, что радикал идеала I тогда и только тогда совпадает с максимальным идеалом $I(p)$, где $p = (p_1,p_2,\dots,p_n) \in \mathbb{A}_n$, когда в I лежат все однородные формы от $(x_i - p_i)$ достаточно высокой степени. В частности, отсюда вытекает

2.1.2. Следствие. *Для максимальности идеала $\mathfrak{m}! \subset \mathbb{C}[x_1,\dots,x_n]$ необходимо и достаточно, чтобы он порождался n линейными многочленами вида $x_\nu - p_\nu$.*

□

2.2. Проективные алгебраические многообразия. С точки зрения проективного пространства $\mathbb{P}_n$ с однородными координатами $(t_0,t_1,t_2,\dots,t_n)$ геометрический смысл имеют лишь *однородные* многочлена $f(t_0,t_1,\dots,t_n) \in \mathbb{C}[t_0,\dots,t_n]$, ибо только их нули корректно определяют геометрические фигуры в $\mathbb{P}_n$.

Задача 1.14. Докажите, что $f(t) \in \mathbb{C}[t_0,\dots,t_n]$ тогда и только тогда однороден степени d, когда $\forall\, \lambda \in \mathbb{C}\ \ f(\lambda t) = \lambda^d f(t)$.

Идеал $I \in \mathbb{C}[t_0,\dots,t_n]$ называется *однородным*, если его можно задать системой образующих, являющихся однородными формами (возможно, разных степеней).

Задача 1.15. Докажите, что идеал I тогда и только тогда однороден, когда вместе с каждым (неоднородным) многочленом $f \in I$ в I будут содержаться и все его однородные компоненты (*однородной компонентой* степени d многочлена f называется сумма всех одночленов степени d входящих в f).

Множество нулей однородного идеала $I \in \mathbb{C}[t_0,\dots,t_n]$ корректно определяет геометрическую фигуру в $\mathbb{P}_n$. Мы будем называть такие фигуры *проективными алгебраическими* *многообразиями* и обозначать $\mathbb{P}V(I)$. Проективное многообразие, задаваемое однородным идеалом I тогда и только тогда непусто, когда соответствующее аффинное алгебраическое множество $V(I) \subset \mathbb{A}_{n+1}$ во-первых непусто, а во-вторых отлично от начала координат. Как мы видели выше, это равносильно тому, что пространство однородных форм степени k не содержится в I ни при каком $k \in \mathbb{N}$. Напротив, если $\mathbb{P}V(I)$ пусто, то $S^k \subset I$ *при всех* k начиная с некоторого $k = N$.

Задача 1.16. Докажите, что радикал однородного идеала однороден.

2.3. Теория исключения. Интуитивно-геометрически, дописывание очередного однородного уравнения в систему однородных полиномиальных уравнений либо никак не влияет на множество решений (если уравнение является следствием предыдущих), либо уменьшает его размерность на 1 (ибо пересекает его с гиперповерхностью). Поэтому естественно ожидать, что $n+1$ однородных многочленов $\{f_1, f_2, \dots, f_{n+1}\}$ в общем случае определяют пустое проективное многообразие в $\mathbb{P}_n$ (т.е. $(n+1)$ гиперповерхностей общего положения не имеют общих точек). Теория исключения (в классическом варианте) описывает то подмножество "необщих" наборов $\{f_1, f_2, \dots, f_{n+1}\}$, которые определяют непустое алгебраическое многообразие.

В чуть более общей постановке фиксируем число уравнений s, размерность проективного пространства n и набор степеней $d_1, d_2, \dots, d_s$. Рассмотрим произведение

$$S^{d_1} \times S^{d_2} \times \cdots \times S^{d_s} .$$

Точки этого пространства взаимно-однозначно соответствуют наборам из s однородных форм $\{f_1, f_2, \dots, f_s\}$ степеней $d_1, d_2, \dots, d_s$ соответственно.

2.3.1. Предложение. *Совокупность тех наборов форм, для которых система однородных уравнений $f_\nu = 0$ (где $1 \le \nu \le s$) задаёт непустое многообразие в $\mathbb{P}_n$, является алгебраическим подмножеством в аффинном пространстве $S^{d_1} \times S^{d_2} \times \cdots \times S^{d_s}$ и может быть описано конечной системой однородных полиномиальных уравнений на коэффициенты форм.*

Доказательство. Непустота прективного многообразия, задаваемого формами f_ν равносильна, как мы видели, тому, что $\forall\, k \in \mathbb{N}$ пространство S^k однородных форм степени k не содержится в идеале $I = (f_1, f_2, \dots, f_s)$, порождённом этими формами. Но пересечение $S^k \cap I$ является образом $\mathbb{C}$-линейного оператора

$$\begin{aligned} \mu_k : \quad & S^{k-d_1} \times S^{k-d_2} \times \cdots \times S^{k-d_s} \longrightarrow S^k \\ & (g_1, g_2, \dots, g_s) \longmapsto \sum_{i=1}^{s} g_i \cdot f_i \end{aligned} \tag{1-3}$$

действующего из векторного пространства размерности

$$D_k = \binom{n+k-d_1}{n} + \binom{n+k-d_2}{n} + \cdots + \binom{n+k-d_2}{n}$$

в векторное пространство размерности $\binom{n+k}{n}$. Он заведомо неэпиморфен при $\binom{n+k}{n} > D_k$, а при $\binom{n+k}{n} \le D_k$ его неэпиморфность равносильна обращению в нуль всех миноров порядка $\binom{n+k}{n}$ его матрицы в каких-либо базисах.

Если в качестве базисов взять стандартные базисы из мономов, то элементами этой матрицы будут коэффициенты форм $f_1, f_2, \dots, f_s$. Приравнивая к нулю все указанные миноры

для всех $k \in \mathbb{N}$ мы получим искомую систему однородных полиномиальных уравнений на коэффициенты форм. По теореме Гильберта о базисе, эта бесконечная система полиномиальных уравнений равносильна некоей своей конечной подсистеме.
□

2.3.2. Замечание. Название "теория исключения" связано с тем, что Пр.2.3.1 позволяет исключать переменные из систем однородных полиномиальных уравнений. В самом деле, пусть мы решаем систему уравнений $f_\nu(t_0, \dots, t_n) = 0$. Предположим, что многочлены системы однородны по какой-то группе переменных. Тогда можно рассмотреть их как многочлены только от этих переменных с коэффициентами, зависящими от оставшихся переменных. Согласно предложению эти коэффициенты обязаны удовлетворять некому набору полиномиальных соотношений. Выписывая их явно, получаем систему с меньшим числом переменных.

2.3.3. Системы результантов. Система полиномиальных уравнений на коэффициенты форм, равносильная непустоте множества их общих нулей в $\mathbb{P}_n$, называется *системой результантов* для данных значений n, s, $d_1, d_2, \dots, d_k$. Подчеркнём, что доказанное только что предложение гарантирует лишь *существование* системы результантов, но мало что даёт для её практического отыскания и даже не позволяет ничего сказать о том, из скольких уравнений она состоит.

В случае, когда результантное уравнение только одно, оно называется просто *результантом*.

2.3.4. Пример. Если $s = n + 1$ и $d_1 = d_2 = \dots = d_{n+1} = 1$, то мы имеем дело с ситемой из $n + 1$ однородных линейных уравнений от $n + 1$ переменных. Условие существования ненулевого решения такой системы хорошо известно из начального курса алгебры — это обращение в нуль определителя матрицы системы. В контексте доказательства Пр.2.3.1 эта матрица является матрицей оператора μ_2 из (1-3). Таким образом, $n+1$ линейных форм тогда и только тогда не порождают максимальный идеал $I(0)$, когда они не порождают $S^2 \cap I(0)$.

2.3.5. Пример. Если $n = s = 2$, то речь идёт об общих нулях пары однородных форм

$$\begin{aligned} f_1(t_0, t_1) &= a_0 t_0^\alpha + a_1 t_0^{\alpha-1} t_1 + a_2 t_0^{\alpha-2} t_1^2 + \dots + a_{\alpha-1} t_0 t_1^{\alpha-1} + a_\alpha t_1^\alpha \\ f_2(t_0, t_1) &= b_0 t_0^\beta + b_1 t_0^{\beta-1} t_1 + b_2 t_0^{\beta-2} t_1^2 + \dots + b_{\beta-1} t_0 t_1^{\beta-1} + b_\beta t_1^\beta \end{aligned}$$

степеней $d_1 = \alpha$ и $d_2 = \beta$ на $\mathbb{P}_1$. В обозначениях из доказательства Пр.2.3.1 для этого случая размерность $D_k = 2k + 2 - (\alpha + \beta)$, и размерность $\dim S^k = k + 1$. Поэтому первое нетривиальное условие возникает при $k = \alpha + \beta - 1$ и заключается в том, что отображение

$$\mu_{\alpha+\beta-1} \colon S^{\beta-1} \times S^{\alpha-1} \longrightarrow S^{\alpha+\beta-1} ,$$

переводящее пару форм g_1, g_2 в $f_1 \cdot g_1 + f_2 \cdot g_2$ неэпиморфно. Этот линейный оператор в стандартных базисах из мономов задаётся квадратной матрицей порядка $\alpha + \beta$.

Задача 1.17. Напишите эту матрицу.

Оказывается, что её определитель и будет в этом случае единственным результантным соотношением (тот, кто решил задачу и знает формулу для результанта двух многочленов уже понял это!). Действительно, из-за совпадения размерностей неэпиморфность оператора $\mu_{\alpha+\beta-1}$ равносильна его немономорфности, а нетривиальность ядра $\mu_{\alpha+\beta-1}$ равносильно наличию общего нуля у f_1 и f_2 на $\mathbb{P}_1$ вследствие задачи

Задача 1.18. Докажите, что однородные формы f_1 и f_2 тогда и только тогда имеют общий линейный множитель, когда существует форма g_1 степени $\deg f_2 - 1$ и форма g_2 степени $\deg f_1 - 1$, такие что $g_1 f_1 = g_2 f_2$.

Одной из целей этого курса является изучение техники, позволяющей, если уж не выписывать явно, то во всяком случае подробно исследовать системы результантов для других наборов форм.

Задача 1.19. Попытайтесь найти результант системы трёх однородных форм на $\mathbb{P}_2$ (в этой ситуации результантное условие тоже только одно) в случаях

а) когда все три формы — квадратичные;

б) когда одна из форм линейна, а две другие имеют произвольные степени d_1 и d_2.

§3 Кое что о расширениях полей

3.1. Терминология. Пусть $k \subset K$ – два поля. В этом случае говорят, что K является *расширением* k. Для любого набора элементов $a = \{a_1, a_2, \dots, a_m\}$ можно рассмотреть *гомоморфизм вычисления*

$$\mathrm{ev}_{(a_1,a_2,\dots,a_m)}\colon\ k[x_1, \dots, x_n] \to K \qquad f(x) \longmapsto f(a) \in K\ . \tag{1-4}$$

Если этот гомоморфизм эпиморфен, то говорят, что элементы $(a_1, a_2, \dots, a_m)$ *порождают* K над k, и называют такого сорта расширения *конечно-порождёнными*. Таким образом, все элементы конечно-порождённого расширения поля k представляются многочленами с коэффициентами из k от какого-то фиксированного конечного набора элементов.

Набор элементов $\{a_1, a_2, \dots, a_m\}$ называется *алгебраически независимым* или *трансцендентным*, если гомоморфизм (1-4) инъективен. В противном случае набор называется *алгебраически зависимым*. Алгебраическая (не)зависимость набора $\{a_1, a_2, \dots, a_m\} \subset K$ означает, тем самым, (не)существование многочлена с коэффициентами из k, зануляющегося на этом наборе.

Если элементы $\{a_1, a_2, \dots, a_m\}$ алгебраически независимы, то сопоставление $t_\nu \longmapsto a_\nu$ продолжает гоморфизм (1-4) до вложения поля рациональных функций

$$k(t_1, \dots, t_m) \hookrightarrow K\ .$$

3.2. Алгебраические расширения. Элемент $\zeta \in K$ называется *алгебраическим* над k, если если он алгебраически зависим сам с собой, т.е. вычисление

$$\mathrm{ev}_\zeta\colon\ k[z] \to K \qquad f(z) \longmapsto f(\zeta) \in K\ . \tag{1-5}$$

имеет ненулевое ядро. Поскольку $k[z]$ – это область главных идеалов, ядро $\ker \mathrm{ev}_\zeta$, буде оно ненулевое, состоит из всех многочленов, делящихся на некий многочлен $f_\zeta(z) \in k[z]$, однозначно определяемый как многочлен наименьшей степени со старшим коэффициентом 1, для которого ζ является корнем. Этот многочлен называется *минимальным многочленом* элемента $\zeta \in K$ над k.

Задача 1.20. Докажите, что минимальный многочлен неприводим в $k[z]$.

Из задачи вытекает, что $k[z]/(f_\zeta(z))$ является полем, и сопоставление $z \longmapsto \zeta$ задаёт изоморфизм этого поля с наименьшим подполем в K, содержащим k и ζ. Поле $k[z]/(f_\zeta(z))$ называется *примитивным расширением* поля k при помощи *присоединения* корня ζ неприводимого многочлена $f_\zeta(z)$ и обозначается $k(\zeta)$.

Задача 1.21. Докажите, что следующие условия на элемент $\zeta \in K \supset k$ равносильны:

а) ζ алгебраичен над k;

б) набор вкторов $\{\zeta^\nu\}_{\nu\in\mathbb{N}} \subset K$ линейно-зависим над k;

в) наименьшее подполе в K, содержащее k и ζ, является конечномерным векторным пространством над k.

Напоминание: линейная зависимость набора векторов означает, по определению, зануление некоей конечной нетривиальной линейной комбинации этих векторов.

Подсказка. Чтобы вывести а) из в) рассмотрите оператор умножения на элемент ζ в конечномерном подполе, задайте его матрицей в удобном базисе, и вспомните про тождество Гамильтона-Кэли.

Расширение полей $k \subset K$ называется *алгебраическим*, если каждый элемент $\zeta \in K$ алгебраичен над k, и *конечным*, – если K является конечномерным векторным пространством над k. Из предыдущей задачи сразу следует, что конечное расширение всегда является алгебраическим. Обратное, разумеется, неверно. Тем не менее:

Задача 1.22. Докажите, что композиция конечных расширений является конечным расширением.

Задача 1.23. Докажите, что композиция алгебраических расширений является алгебраическим расширением (т.е. если $\zeta \in K' \supset K$ алгебраичен над K, и $K \supset k$ – алгебраическое расширение, то ζ алгебраичен над k).

3.3. Теорема. *Всякое конечное расширение поля k характеристики нуль является примитивным, т.е. изоморфно $k[z]/(\varphi(z))$, где $\varphi(z) \in k[z]$ – неприводимый многочлен.*

Доказательство. Всякое конечное расширение можно получить при помощи нескольких последовательных примитивных расширений. Предыдущая задача показывает, что без ограничения общности можно считать, что при каждом из этих последовательных расширений присоединяется элемент, алгебраичный над исходным полем, т.е. присоединяется корень некого неприводимого многочлена из $k[z]$. Ввиду того, что неприводимый многочлен над полем нулевой характеристики взаимно прост со своей производной, он не может иметь кратных корней ни в каком расширении основного поля. Теперь очевидная индукция по количеству промежуточных расширений выводит нашу теорему из приводимой ниже леммы, известной как *лемма о примитивном элементе*.

3.3.1. Лемма. *Пусть k – бесконечное поле, $\varphi(z)$ и $\psi(z)$ — неприводимые многочлены, причём φ не имеет кратных корней ни в каком расширении поля k. Тогда поле K, полученное последовательным присоединением корня многочлена φ и корня многочлена ψ является примитивным расширением, т.е. может быть получено присоединением одного элемента $\zeta \in K$.*

Доказательство. Пусть K' – такое расширение k, где и φ и ψ полностью раскладываются на линейные множители (его можно построить последовательно присоединяя недостающие корни). Пусть $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ – это все (попарно-разные) корни φ, а $\{\beta_1, \beta_2, \dots, \beta_m\}$ – все корни ψ.

Задача 1.24. Докажите, что K изоморфно наименьшему подполю в K', содержащему α_1 и β_1.

Отождествим K с указанным в задаче подполем в K'. Будем искать нужный нам $\zeta \in K$ в виде $\zeta = \alpha_1 \cdot c + \beta_1$, где $c \in k$. Нам надо подобрать c так, чтобы и α_1 и β_1 содержались в примитивном расширении $k(\zeta)$. Поскольку $\beta_1 = \zeta - c\alpha_1$, достаточно следить лишь за тем, что $\alpha_1 \in k(\zeta)$. Мы собираемся показать, что α_1 является корнем линейного уравнения над $k(\zeta)$.

Заметим, что α_1 является корнем двух многочленов с коэффициентами из $k(\zeta)$, а именно $\varphi(z)$ и $\psi(\zeta - cz)$ (где z – переменная). Следовательно, α_1 является корнем и их наибольшего общего делителя (также многочлена с коэффициентами из $k(z)$). Этот НОД будет линеен, если мы сумеем подобрать c так, чтобы многочлены не имели других общих корней кроме α_1, т.е. чтобы для прочих корней α_ν, $(\nu \geq 2)$ многочлена φ числа $\zeta - c\alpha_\nu$ не совпали ни с одним из корней β_μ многочлена ψ. Для этого мы должны удовлетворить конечной системе неравенств

$$c(\alpha_1 - \alpha_\nu) + \beta_1 \neq \beta_\mu \,,$$

где $\mu = 1, 2, \ldots, m$ и $\nu = 2, 3 \ldots, n$. Но это всегда возможно над бесконечным полем!

Лемма и теорема доказаны.

□

Задача 1.25. Где в доказательстве использовалось требование, чтобы все корни φ были попарно-различны?

Задача 1.26. Постройте примитивный элемент расширения поля $\mathbb{Q}$ при помощи последовательного присоединения $\sqrt{3}$ и $\sqrt{5}$. Найдите размерность (над $\mathbb{Q}$) этого расширения. Выпишите минимальный многочлен предлагаемого Вами примитивного элемента.

Задача 1.27. Докажите, что конечное расширение конечного поля примитивно.
Указание: Воспользуйтесь тем, что ненулевые элементы конечного поля составляют циклическую группу по умножению.

3.4. Конечно-порождённые расширения поля $\mathbb{C}$. Вернёмся теперь к использованному нами при доказательстве теоремы Гильберта о нулях Пр.1.5.3, которое описывает все конечно-порождённые расширения поля комплексных чисел. Итак, пусть поле K порождается над $\mathbb{C}$ элементами $\{a_1, a_2, \ldots, a_n\}$. Перенумеруем их, если надо, так, чтобы первые m элементов $\{a_1, a_2, \ldots, a_m\}$ составляли трансцендентный над $\mathbb{C}$ набор, но любой набор $\{a_1, \ldots, a_m, a_{m+s}\}$ был бы алгебраически зависимым. Отметим, что такая алгебраическая зависимость обязана фактически содержать a_{m+s}, а стало быть, она означает, что a_{m+s} алгебраичен над наименьшим подполем в K, содержащем $\mathbb{C}$ и $a_1, a_2, \ldots, a_m$. Но, как мы видели в начале параграфа, такое подполе изоморфно полю рациональных функций от m переменных.

Итак, K является расширением поля рациональных функций $\mathbb{C}(t_1, \ldots, t_m)$ при помощи конечного числа элементов $a_{m+1}, \ldots, a_n$, алгебраических над этим полем. По лемме о примитивном элементе, K будет примитивным расширением поля рациональных функций, что и утверждалось в Пр.1.5.3.

Лекция 3
Алгебраические многообразия и схемы

▷Общая концепция многообразия ▷Топология Зарисского ▷Максимальный спектр ▷Регулярные отображения ▷Структурный пучок ▷Абстрактные алгебраические многообразия ▷Аффинные схемы ▷Изоморфизмы и замкнутые вложения ▷Целые расширения колец ▷Лемма Гаусса-Дедекинда-Кронекера ▷Целые алгебраические числа ▷Ещё одно доказательство der Nullstellensatz ▷Конечные морфизмы схем ▷Нётерова нормализация

§1 Многообразия

1.1. Что такое многообразие? Говоря философски, многообразие — это та среда, где уместно заниматься геометрией в широком смысле слова (включая геометрические аспекты алгебры, анализа и топологии). Такая среда всегда является результатом взаимодействия двух неотъемлемых компонент — топологического пространства и кольца *регулярных* функций на нём. Взаимодействие это происходит по двум направлениям. Во-первых, в локальной окрестности каждой точки топология подлежащего пространства целиком определяется аналитическими свойствами функций, регулярных в данной точке. Поэтому вблизи каждой точки многообразие устроено неким стандартным способом. Во-вторых, алгебраические свойства кольца регулярных функций имеют адекватное отражение в глобальной геометрии подлежащего пространства.

Так, *гладкое многообразие* — это топологическое пространство X, каждая точка x которого имеет окрестность U, снабжённую гомеоморфизмом $B^n \xrightarrow{\varphi} U$ с шаром $B^n \subset \mathbb{R}^n$. Эта окрестность всегда рассматривается вместе с кольцом *гладких* функций. По определению, таковыми являются все вещественнозначные функции f на U, для которых композиция $f\varphi$ будет гладкой функцией на B^n. Вблизи каждой точки с такими функциями можно заниматься анализом точно также, как в $\mathbb{R}^n$, а глобальная геометрия X (количества дырок, компактность, и т. п.) отвечают за глобальную алгебру кольца функций на всём X (индексы дифференциальных операторов, когомологии Де Рама и т. п.).

Аналогично, *аналитическая геометрия* (не путать с названием одного из вводных мехматских курсов!) занимается топологическими пространствами, локально устроенными как открытое подмножество в $\mathbb{C}^n$, и исследует с их помощью *аналитические* функции комплексных переменных.

Цель настоящей лекции — объяснить, что такое *алгебраическое многообразие*, т. е. описать среду, где уместно изображать геометрически всё то, что связано с исследованием алгебраических уравнений. Описание будет идти по стандартной схеме: Сначала мы опишем локальное топологическое устройство, потом объясним с какими функциями мы собираемся иметь дело, и наконец, опишем по каким правилам локальные куски можно склеивать в глобальные объекты.

1.2. Топология Зарисского на алгебраическом множестве. Комплексное алгебраическое многообразие, по определению, локально устроено как алгебраическое множество в аффинном пространстве $\mathbb{A}_n(\mathbb{C})$. Однако локальность мы будем понимать не в смысле стандартной топологии на $\mathbb{C}_n$, известной из анализа и аналитической геометрии, а в смысле другой топологии, называемой *топологией Зарисского*. В отличие от обычной топологии, топология Зарисского приспособлена не к метрической геометрии и предельным переходам, а к отражению алгебраических свойств кольца функций, таких как делимость, взаимное расположение идеалов внутри кольца и т. п. Она гораздо грубее обычной, но зато может быть введена на любом алгебраическом множестве над любым (в том числе конечным) полем.

Итак, пусть $V \subset \mathbb{A}_n(k)$ — алгебраическое множество, и

$$I(V) = \{f \in k[x_1, \dots, x_n] \mid f(p) = 0 \; \forall \, p \in V \}$$

— его идеал. Фактор-кольцо $k[V] \stackrel{\text{def}}{=} k[x_1, \dots, x_n]/I(V)$ называется *координатной алгеброй* или *стуктурным кольцом* алгебраического множества V. Для любого $f \pmod{I(V)} \in k[V]$ множество $V(f)$ нулей многочлена f на V корректно определено (т. е. зависит лишь от класса f в фактор-кольце). Для любого идеала $J \subset k[V]$ обозначим через $V(J) \stackrel{\text{def}}{=} \bigcap\limits_{f \in J} V(f)$ множество его нулей на V.

Задача 3.1. Убедитесь, что построенное соответствие между подмножествами в V и идеалами координатного кольца обладает следующими свойствами:
а) $V(J_1) \cup V(J_2) = V(J_1 \cap J_2)$;
б) $\bigcap\limits_{\nu} V(J_\nu) = V(\sum\limits_{\nu} J_\nu)$, где под суммой идеалов понимается их сумма как векторных подпространств над k;
в) $V(0) = V$ и $V(1) = \emptyset$;
г) $V(J_1) \subset V(J_2) \iff J_1 \supset J_2$.

Из задачи сразу следует, что объявив все подмножества вида $V(J)$ *замкнутыми* мы зададим на V *топологию*. Это и есть топология Зарисского.

Задача 3.2. Покажите, что объединение бесконечного семейства замкнутых по Зарисскому подмножеств может быть незамкнуто.

Задача 3.3. Докажите, что дополнения $D(f) \stackrel{\text{def}}{=} V \setminus V(f)$ до множеств вида $V(f)$, $f \in k[V]$, составляют базу открытых множеств топологии Зарисского.

Для того, чтобы получить представление об отличии топологии Зарисского от классической, рассмотрим три характерных примера.

1.2.1. Большие открытые множества. Базисные открытые множества вида $D(f)$, будучи дополнениями до гиперповерхностей, как правило, являются всюду плотными и попарно пересекаются. Поэтому топология Зарисского сильно неотделима, и слова “система сужающихся окрестностей” выражают не то, что эти окрестности стягиваются в точку, а то, что дополнение до них задаётся многочленом всё более высокой степени. Непример, если $V = \mathbb{A}_1$ – аффинная прямая (так что $k[V] = k[x]$), то замкнутыми будут конечные множества точек и только они. Поэтому топология Зарисского на прямой попросту совпадает с *дискретной топологией*.

Задача 3.4. Приведите пример алгебраического множества и двух собственных непересекающихся открытых подмножеств вида $D(f)$ на нём.

1.2.2. Неприводимость. Топологическое пространство называется *неприводимым*, если оно не представимо в виде объединения двух своих собственных замкнутых подмножеств. Разумеется, в классической вещественной метрической топологии неприводимых замкнутых множеств, отличных от точки, не бывает. Однако, в алгебраической по природе топологии Зарисского неприводимые замкнутые множества играют такую же роль, как простые числа в арифметике.

Допустим, что замкнутое множество $V = V(J)$ приводимо. Тогда V содержит собственное замкнутое подмножество $V_1 = V(J_1)$. Если и оно приводимо, то $V_1 \supset V_2 = V(J_2)$ и т. д. Цепочке строго вложенных друг в друга замкнутых подмножеств $V \supset V_1 \supset V_2 \supset \cdots$ соответствует возрастающая цепочка строго вложенных идеалов $J \subset J_1 \subset J_2 \subset \cdots$, которая в нётеровом кольце не может быть бесконечной. Таким образом, всякая убывающая цепочка вложенных замкнутых подмножеств стабилизируется, и как следствие, мы получаем, что всякое замкнутое алгебраическое множество V является объединением конечного числа своих замкнутых неприводимых подмножеств. Они называются *неприводимыми компонентами* V.

Задача 3.5. Докажите, любые два непустых открытых подмножества неприводимого алгебраического множества V имеют непустое (и даже всюду плотное в V) пересечение.

Задача 3.6. Докажите, что замкнутое подмножество $W \subset V$ тогда и только тогда неприводимо, когда его идеал $I(W) \subset k[V]$ *прост* (т. е. фактор кольцо $k[W] = k[V]/I(W)$ не имеет делителей нуля или, как говорят, является *целостным*).

Задача 3.7. Докажите, что набор неприводимых компонент алгебраического множества V определяется по V однозначно (это довольно грубый аналог теоремы о единственности разложения на простые множители).

Подсказка: Неприводимыа компонента не может лежать в объединении других (отличных от неё) компонент.

1.2.3. Топология Зарисского на произведении. Не вдаваясь в подробное объяснение, почему декартово произведение алгебраических множеств имеет естественную структуру алгебраического множества, мы отметим здесь, что топология Зарисского на таком произведении не совпадает с произведением топологий Зарисского на сомножителях, а является более тонкой. Например, в произведении топологий Зарисского на $\mathbb{A}_2 = \mathbb{A}_1 \times \mathbb{A}_1$ замкнутыми будут лишь конечные объединения точек и прямых, параллельным осям координат, тогда как в своей "родной" топологии Зарисского на $\mathbb{A}_2$ замкнуты любые плоские алгебраические кривые, скажем, гипербола $V(xy - 1)$.

Связано это с тем, что координатная алгебра произведения алгебраических множеств естественно изоморфна тензорному произведению координатных алгебр $k[V \times W] \simeq k[V] \otimes_k k[W]$, а далеко не все идеалы в тензорном произведении колец являются тензорными произведениями идеалов сомножителей.

Задача 3.8. Попытайтесь чётко обосновать два этих факта.

1.3. Регулярные функции. После того, как мы определили топологию на алгебраическом множестве $V \subset \mathbb{A}_n(k)$, мы должны для каждого открытого множества $U \subset V$ описать класс *регулярных* функций на нём. По определению, мы будем считать регулярными *рациональные* функции, определённые на U, т. е. функции, которые в глобальных координатах на $\mathbb{A}_n$ представляются в виде отношения $f(x)/g(x)$ двух полиномов $f,g \in k[x_1,\dots,x_n]$, причём g не обращается в нуль на U. Регулярные на U функции составляют кольцо, которое мы будем обозначать $k[U]$.

Если U является объединением конечного числа базисных открытых множеств $D(f_\nu)$, а поле k – алгебраически замкнуто, то из теоремы Гильберта о нулях вытекает, что знаменатель g регулярной функции $f/g \in k[\bigcup\limits_\nu D(f_\nu)]$ лежит в радикале идеала, порождённого всеми f_ν, а стало быть является произведением каких-то степеней многочленов, участвующих в разложениях f_ν на простые множители.

В частности, мы получаем, что над алгебраически замкнутым полем кольцо всех функций регулярных на всём алгебраическом множестве V совпадает со структурным кольцом $k[V]$. Поэтому $k[V]$ иногда называют также *кольцом регулярных функций*. Замечательно, что топологическое пространство V однозначно восстанавливается по кольцу регулярных функций.

1.4. Алгебраическая характеризация точек. Далее мы предполагаем, что основное поле k алгебраически замкнуто (желающие могут считать, что $k = \mathbb{C}$), так что для него справедлива теорема Гильберта о нулях[1]. С каждой точкой $p \in V$ связан (очевидно, эпиморфный) гомоморфизм вычисления $\mathrm{ev}_p\colon\ k[V] \longrightarrow k$, переводящий $f \pmod{I(V)}$ в $f(p) \in k$. Его ядро, следовательно, будет максимальным идеалом в $k[V]$. Он обозначается $\mathfrak{m}_p$ и называется *максимальным идеалом точки* p.

1.4.1. Предложение. *Соответствие $p \longmapsto \mathfrak{m}_p$ между множеством точек алгебраического множества V и множеством максимальных идеалов структурного кольца $k[V]$ взаимно-однозначно (над алгебраически замкнутым полем!).*

Доказательство. Обратное отображение немедленно доставляется теоремой Гильберта о нулях: всякий максимальный идеал в $k[V]$ имеет нуль $q \in V$, откуда $\mathfrak{m} \subset \mathfrak{m}_q$, что в действительности означает равенство (из-за максимальности $\mathfrak{m}$).
□

> Задача 3.9. Докажите, что точки отрезка взаимно-однозначно соответствуют максимальным идеалам в кольце вещественно-значных непрерывных функций на отрезке. Обобщается ли это
>
> а) на компактные б) на любые подмножества в $\mathbb{R}_n$?
>
> Задача 3.10. Пусть U — открытое подмножество алгебраического множества V. Покажите, что сопоставляя точкам U их максимальные идеалы, мы получим, вообще говоря, не все максимальные идеалы кольца $k[U]$, а также, что это кольцо может и не быть конечно порождённым над k.

Топология Зарисского на V также однозначно восстанавливается по алгебраическим свойствам координатного кольца. А именно, обращение в нуль регулярной функции $f \in k[V]$ в точке $p \in V$ означает в точности принадлежность $f \in \mathfrak{m}_p$. Поэтому базис открытых множеств в топологии Зарисского на “пространстве максимальных идеалов” составляют множества вида $D(f) \overset{\text{def}}{=} \{\mathfrak{m} \mid f \notin \mathfrak{m}\}$. Соответственно, замкнутыми будут все множества вида $V(I) \overset{\text{def}}{=} \{\mathfrak{m} \mid I \subset \mathfrak{m}\}$.

[1] В прошлой лекции мы доказали der Nullstellenzatz только для поля $\mathbb{C}$, однако желающие могут легко удостовериться, что доказательство годится для любого алгебраически замкнутого поля характеристики нуль. Ниже, в n° 3.4.3 мы слегка модифицируем это доказательство так, что оно будет проходить для любой характеристике.

Таким образом, мы можем строить алгебраическое множество V исходя из произвольного абстрактно заданного кольца! Опишем теперь класс колец, которые реально возникают как $k[V]$ для "настоящих" геометрических аффинных алгебраических подмножеств $V \subset \mathbb{A}_n(k)$. Прежде всего, по построению, эти кольца являются конечно порождёнными k- алгебрами. Во-вторых, из-за того, что идеалы вида $I(V)$ радикальны по теореме о нулях, эти кольца будут *приведёнными*, т. е. без *нильпотентов*[2]. Мы приходим к следующему определению.

1.4.2. Определение. *Пусть A — коммутативное кольцо. Множество максимальных идеалов кольца A с описанной выше топологией Зарисского на нём называется максимальным спектром кольца A и обозначается $Spm(A)$. Пара $A, Spm(A)$, где A — приведённая конечнопорождённая алгебра над алгебраически-замкнутым полем k, называется абстрактным аффинным алгебраическим многообразием над полем k.*

1.5. Регулярные отображения. Итак, "элементарные куски" из которых мы будем собирать общие алгебраические многообразия, — это (абстрактные) аффинные многообразия. Уговоримся теперь, какие отображения между аффинными многообразиями мы собираемся рассматривать, и какие многообразия мы объявляем изоморфными.

Пусть $V \subset \mathbb{A}_n(k)$ и $W \subset \mathbb{A}_m(k)$ — алгебраические множества. Всякое теоретико-множественное отображение $V \xrightarrow{\varphi} W$ идуцирует гомоморфизм поднятия φ^*, действующий из кольца всех k-значных функций на W в кольцо всех k-значных функций на V по правилу $f \longmapsto f \circ \varphi$. Мы будем называть φ *регулярным отображением* или *морфизмом алгебраических многообразий*, если φ^* переводит регулярные функции на W в регулярные функции на V, т. е. индуцирует гомомрфизм $k[W] \to k[W]$, который мы также будем обозначать φ^*.

> Задача 3.11. Докажите, что отображение φ отрезка в отрезок тогда и только тогда измеримо (непрерывно, гладко, ...), когда композиция φ с любой измеримой (непрерывной, гладкой, ...) функцией будет измеримо (непрерывно, гладко, ...).

1.5.1. Предложение. *Пусть $V \subset \mathbb{A}_n(k)$ и $W \subset \mathbb{A}_m(k)$ — алгебраические множества над алгебраически-замкнутым полем. Тогда для любого гомомрфизма колец $\varphi^*\colon\ k[W] \longrightarrow k[V]$ существует единственное регулярное отображение $\varphi\colon\ V \longrightarrow W$, для которого φ^* служит гомоморфизмом поднятия.*

Доказательство. Полный прообраз $\mathfrak{q} = \varphi^{*-1}(\mathfrak{m}_p)$ максимального идеала $\mathfrak{m}_p \in k[V]$ точки $p \in V$ является максимальным идеалом в $k[W]$ (это сразу следует из того, что композиция $k[W] \xrightarrow{\varphi^*} k[V] \xrightarrow{\pi} k[V]/\mathfrak{m}_p \simeq k$ является эпиморфизмом на поле с ядром $\mathfrak{q}$). Поэтому $\mathfrak{q}$ является идеалом некоторой точки $q \in W$.

> Задача 3.12. Докажите, что $p \longmapsto q$ является искомым регулярным отображением.

□

Регулярное отображение $\varphi\colon\ V \longrightarrow W$ называется *изоморфизмом*, если φ^* является изоморфизмом координатных колец. Изоморфизм, очевидно, биективен, и всякая регулярная биекция, по предыдущему предложению, является изоморфизмом. Подчекнём, что алгебраическая замкнутость поля существенна для столь хорошего соответствия между алгеброй и геометрией.

> Задача 3.13. Убедитесь, что отображение $\mathbb{R}_1 \xrightarrow{t \longmapsto t^3} \mathbb{R}_1$ регулярно, биективно, но не изоморфизм.

[2]Элемент a коммутативного кольца A называется *нильпотентным*, если $a \neq 0$, но $a^m = 0$ для некоторого $\forall\, m \in \mathbb{N}$.

1.5.2. Вложение абстрактного аффинного многообразия в $\mathbb{A}_n$ тавтологически получается из предыдущего предложения. Если A – приведённая k-алгебра с конечным числом образующих, то для некоторого $n \in \mathbb{N}$ существует эпиморфизм $k[x_1, \dots, x_n] \xrightarrow{\pi^*} A$, ядро которого — радикальный идеал $I \subset k[x_1, \dots, x_n]$. Соответствующее регулярное отображение $Spm(A) \xrightarrow{\pi} \mathbb{A}_n$ будет изоморфизмом с алгебраическим подмножеством $V(I) \subset \mathbb{A}_n$ (ибо π^* индуцирует изоморфизм $k[x_1, \dots, x_n]/I$ с A).

1.5.3. Алгебраический смысл регулярных отображений Чтобы задать регулярное отображение из аффинного многообразия $V \subset \mathbb{A}_n = Spm(k[x_1, \dots, x_n])$ в афинное многообразие $W \subset \mathbb{A}_m = Spm(k[y_1, \dots, y_m])$, мы должны построить гомоморфизм колец

$$k[y_1, \dots, y_m]/I(W) \xrightarrow{\varphi^*} k[x_1, \dots, x_n]/I(V) .$$

Для этого надо задать образы образующих координатного кольца $y_i \longmapsto f_i(x_1, \dots, x_n)$, причём сделать это так, чтобы всякая функция $f(y)$ из идеала $I(W)$ при подстановке $f_i(x)$ вместо y_i превращалась в функцию из идеала $I(V)$ (иначе не получится гомоморфизма фактор-колец). Таким образом, наличие регулярного отображения из V в W на языке уравнений означает, что существует алгебраическая замена переменных, превращающая систему уравнений, задающую W, в систему, которая является следствием системы уравнений, задающей V.

1.6. Склейка. Теперь, наконец, мы можем дать определение произвольного (не аффинного) абстрактного алгебраического многообразия.

Аффинной картой на топологическом пространстве X называется открытое подмножество $V \subset X$, наделённое структурой абстрактного аффинного алгебраического многообразия. Это означает наличие гомеоморфизма $Spm(A) \xrightarrow{\varphi} U$ с абстрактным аффинным многообразием (рассматриваемым с топологией Зарисского) и фиксацию в качестве колца регулярных функций на любом открытом подмножестве $W \subset U$ таких k-значных функций f, для которых композиция $f\varphi$ лежит в $k[\varphi^{-1}(W)]$.

Покрытие топологического пространства X аффинными картами V_ν называется *алгебраическим атласом*, если любые две карты V_1 и V_2 *согласованы* в том смысле, что кольца регулярных функций на открытом множестве $V_1 \cap V_2$ индуцированные структурами на V_1 и на V_2 изоморфны. Два алгебраических атласа на X называются *эквивалентными*, если их карты попарно-согласованы, т. е. объединение их карт также является алгебраическим атласом.

1.6.1. Определение. *Абстрактным алгебраическим многообразием называется топологическое пространство вместе с непустым классом эквивалентных алгебраических атласов на нём.*

Задача 3.14. Докажите, что следующие многообразия являются алгебраическими:
а) проективное пространство $\mathbb{P}_n(k)$;
б) множество нулей любого однородного полинома в $\mathbb{P}_n(k)$;
в) множество нулей любого однородного идеала в $\mathbb{P}_n(k)$;
г) аффинная прямая с раздвоенной точкой, т.е. результат замены одной из точек на $\mathbb{A}_1$ на пару дизъюнктных точек.

1.6.2. Структурный пучок. k-значная функция f на открытом подмножестве U алгебраического многообразия X называется *регулярной*, если её ограничение на пересечение $U \cap V$ с любой аффинной картой V принадлежит кольцу регулярных функций $k[U \cap V]$. Регулярные функции на открытом подмножестве U составляют кольцо, обозначаемое $k[U]$.

Сопоставление $U \longmapsto k[U]$ называется *структурным пучком* алгебраического многообразия X и обозначается $\mathcal{O}_X$. В таком контексте элементы кольца $k[U]$назыаются *сечениями* структурного пучка над открытыми множествами U и их совокупность обозначаются через $\Gamma(U;\mathcal{O}_X)$ или $H^0(\mathcal{O}_x;U)$. Отметим, что для каждого вложения открытых множеств $V \hookrightarrow U$ имеются гомоморфизмы ограничения $r_V^U\colon\ k[U] \longrightarrow k[V]$.

Отображение $X \xrightarrow{\varphi} Y$ между произвольными алгебраическими многообразиями называется *регулярным*, если оно непрерывно, и для любого открытого подмножества $U \subset Y$ гомоморфизм подъёма индуцирует отображение колец регулярных функций $k[U] \xrightarrow{\varphi^*} k[\varphi^{-1}(U)]$.

> Задача 3.15. Убедитесь, что для регулярности отображения из произвольного алгебраического многообразия X в аффинное многообразие Y необходимо и достаточно, чтобы сужение этого отображения на каждую аффинную карту X было регулярным морфизмом аффинных многообразий.

> Задача 3.16. Проверьте, что проекция проективного пространства из подпространства на дополнительное подпространство является регулярным отображением алгебраических многообразий.

> Задача 3.17. (Трудная!) Докажите, что $k[\mathbb{P}_n] = k$, т.е. регулярные функции, определённые на всём проективном пространстве — это константы и только они (основное поле — алгебраически замкнуто!).

§2 Схемы

2.1. Расширение концепции точки. Алгебраические многообразия, определённые в предыдущем параграфе, являются изображениями колец специального вида, а именно, конечно порождённых целостных алгебр над алгебраически замкнутым полем. Пытливый ум формального склада не замедлит пойти дальше в рисовании алгебры и разработать "геометрический" язык для описания гомомрфизмов произвольных колец. Слово "геометрический" взято в кавычки, потому что в действительности мы уже изобразили точками всё, что изображается настоящими геометрическими точками в настоящем аффинном пространстве над полем. Тем не менее, существует некоторое расширение концепции точки, которое позволяет, если не рисовать последние, то пользоваться при работе с ними вполне геометрической интуицией, причём на языке этих обобщённых точек можно будет оперировать с произвольными кольцами.

Мы будем исходить из того, что точке многообразия V в аффинном пространстве над полем k соответствует гомомрфизм вычисления $k[V] \xrightarrow{\text{ev}} k$. Разумеется, мы можем вычислять значение и над каким-нибудь другим полем k'. Получим гомомрфизм $k[V] \xrightarrow{\text{ev}} k'$. Заменяя $k[V]$ произвольным коммутативным кольцом A, мы можем, таким образом, считать *вычислением значения* элементов из A над полем K произвольный гомоморфизм $A \longrightarrow K$. Точки A должны как-то параметризовать все такие гомоморфизмы во всевозможные поля K во внутренних терминах кольца A. Естественно осуществить такую параметризацию сопоставляя каждому гомомрфизму его ядро – идеал в A, автоматически являющийся *простым*, поскольку образ гомомрфизма в поле является кольцом без делителей нуля.

2.2. Простой спектр. Совокупность всех простых идеалов коммутативного кольца A называется *простым спектром* этого кольца и обозначается $Spec(A)$. В точности также, как и на максимальном спектре, на $Spec(A)$ можно ввести *топологию Зарисского*, объявив *замкнутыми* всевозможные множества вида $V(I) \overset{\text{def}}{=} \{\mathfrak{p} \subset A \mid I \subset \mathfrak{p}\}$, где I – идеал в A.

Задача 3.18. Докажите, что и в самом деле получится топология.

Задача 3.19. Докажите, что замкнутое подмножество $V(I)$ неприводимо тогда и только тогда, когда I – простой идеал.

Задача 3.20. Докажите, что точка $\mathfrak{p} \in Spec(A)$ замкнута тогда и только тогда, когда идеал $\mathfrak{p} \subset A$ максимален, и убедитесь, что замыкание незамкнутой точки $\mathfrak{p}$ есть неприводимое множество $V(\mathfrak{p})$ нулей идеала $\mathfrak{p}$.

Элементы кольца A называются *глобальными регулярными функциями* на $Spec(A)$. Название это, скорее, условно, но тем не менее, с каждой точкой $\mathfrak{p} \in Spec(A)$ связан гомоморфизм вычисления $A \xrightarrow{\mathrm{ev}_\mathfrak{p}} K_\mathfrak{p}$ со значениями в целостном кольце $K_\mathfrak{p} \overset{\text{def}}{=} A/\mathfrak{p}$. Таким образом, область значений функций $f \in A$ меняется от точки к точке. И всё же, каждая $f \in A$ определяет замкнутое подмножество $V(f) = \{\mathfrak{p} \in Spec(A) \mid f \in \mathfrak{p}\}$, называемое *множеством нулей функции* f, и дополнительное к нему открытое подмножество $D(f) = Spec(A) \setminus V(f)$.

Задача 3.21. Убедитесь, что открытые подмножества $D(f)$ составляют базис открытых множеств топологии Зарисского на $Spec(A)$.

Как мы видели, число рациональных функций, регулярных на открытом подмножестве алгебраического множества, увеличивается с измеьчением множества за счёт того, что появляется большее количество не обращающихся в нуль знаменателей. Чтобы отразить это явление в случае простого спектра используется

2.2.1. Локализация. Пусть A – любое кольцо, а $\mathfrak{p} \subset A$ – произвольный простой идеал. Дополнение $S = A \setminus \mathfrak{p}$ до этого идеала в A не содержит нуля, содержит 1 и замкнуто относительно умножения, т. е. $s_1 s_2 \in S \quad \forall s_1, s_2 \in S$. Для всякого такого множества S можно рассмотреть *кольцо частных* $A[S^{-1}]$, определяемое аналогично полю частных[3] как множество классов эквивалентных записей a/s, где $a \in A$, $s \in S$ и две записи a_1/s_1 и a_2/s_2 эквивалентны, если и только если $s(a_1 s_2 - a_2 s_1) = 0$ для некоторого $s \in S$.

Задача 3.22. Убедитесь, что это действительно отношение эквивалентности, продумайте, почему оно именно такое, и докажите, что оперции

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \overset{\text{def}}{=} \frac{a_1 \cdot a_2}{s_1 \cdot s_2} \qquad \text{и} \qquad \frac{a_1}{s_1} + \frac{a_2}{s_2} \overset{\text{def}}{=} \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$$

корректно определяют на $A[S^{-1}]$ структуру коммутативного кольца с единицей, а отображение $A \xrightarrow{\mathrm{loc}_S} A[S^{-1}]$, переводящее a в $a/1$, является гоморфизмом колец, ядро которого совпадает с множеством *S-делителей нуля* в A (т. е. таких $a \neq 0$, что $sa = 0$ для некого $s \in S$).

В кольце $A[S^{-1}]$ имеется ровно один максимальный идеал $\mathfrak{p}[S^{-1}] \overset{\text{def}}{=} \mathrm{loc}_S(\mathfrak{p})$, ибо по построению все элементы вне $\mathfrak{p}[S^{-1}]$ обратимы в $A[S^{-1}]$. Кольца, обладающие таким свойством, называются *локальными*, и переход от “глобального” кольца A к кольцу частных $A[S^{-1}]$ называется *локализацией относительно мультипликативного множества* S. Если в качестве S, как в нашем случае, берётся дополнение до простого идеала $\mathfrak{p} \subset A$, то результат локализации часто называют *локальным кольцом точки* $\mathfrak{p} \in Spec(A)$ и обозначают $A_\mathfrak{p}$ или $\mathcal{O}_{Spec(A)}, \mathfrak{p}$. Название интуитивно оправдывается тем, что формально обращая все функции, не зануляющиеся в данной точке $\mathfrak{p}$, мы как бы ограничиваем себя той окрестностью этой точки, где соответствующие знаменатели не имеют полюсов.

[3]с поправкой на возможное наличие делителей нуля в A (но не в S !)

2.2.2. Структурный пучок $\mathcal{O}_{Spec(A)}$ на $Spec(A)$ наделяет каждое открытое множество $U \subset Spec(A)$ кольцом $\Gamma(U, \mathcal{O}_{Spec(A)})$, которое, по определению, состоит из всевозможных отображений s, сопоставляющих каждой точке $\mathfrak{p} \in U$ локальную функцию $s(\mathfrak{p}) = f_\mathfrak{p}/g_\mathfrak{p} \in A_\mathfrak{p}$, и *непрерывных* в в следующем смысле: $\forall\, \mathfrak{q} \in U \;\; \exists$ открытая окрестность $\mathfrak{q} \in U' \subset U$ и пара функций $f, g \in A$ таких, что g не обращатся в нуль нигде на U' и $\forall\, \mathfrak{p} \in U' \;\; s(\mathfrak{p}) = f/g$ в $A_\mathfrak{p}$. Элементы s кольца $\Gamma(U, \mathcal{O}_{Spec(A)})$ называются *сечениями пучка* $\mathcal{O}_{Spec(A)}$ над открытым множеством U.

Задача 3.23. Убедитесь, что $\Gamma(U, \mathcal{O}_{Spec(A)})$ действительно является кольцом, и постройте для каждой пары вложенных открытых множеств $V \subset U$ *гомомрфизм ограничения* $\Gamma(U, \mathcal{O}_{Spec(A)}) \xrightarrow{r_V^U} \Gamma(V, \mathcal{O}_{Spec(A)})$, Докажите далее, что гомомрфизмы ограничения обладают следующими свойствами:
а) $r_W^V r_V^U = r_W^U$ для любой упорядоченной тройки $W \subset V \subset U$.
б) Для каждого покрытия произвольного открытого множества U набором открытых множеств V_ν и для каждого набора сечений $s_\nu \in \Gamma(V_\nu, \mathcal{O}_{Spec(A)})$, которые "совпадают" на пересечениях в том смысле, что $\forall i, j \;\; r^{V_i}_{V_i \cap V_j}(s_i) = r^{V_j}_{V_i \cap V_j}(s_j)$ в $\Gamma(V_i \cap V_j, \mathcal{O}_{Spec(A)}$, существует и притом единственное сечение над U, ограничение которого на каждое из V_ν совпадает с s_ν.

Таким образом, сечения структурного пучка над открытыми множествами обладают всеми формальными признаками локально определённых рациональных функций. Например, мы тоже можем вычислять их "значения", беря класс вычетов

$$s(\mathfrak{p}) \,(\mathrm{mod}\, \mathfrak{p}) \;\stackrel{\mathrm{def}}{=}\; \frac{f_\mathfrak{p}}{g_\mathfrak{p}} \,(\mathrm{mod}\, \mathfrak{p}A_\mathfrak{p}) \,\in A[S^{-1}]/\mathfrak{p}A[S^{-1}] \simeq A/\mathfrak{p} = K_\mathfrak{p}\;.$$

2.2.3. Определение. *Пара* $Spec(A), \mathcal{O}_{Spec(A)}$, *где* A *– произвольное коммутативное кольцо, называется аффинной схемой.*

Задача 3.24. Подумайте, как определить склейку аффинных схем и общие (неаффинные) схемы, а также регулярные функции на них и регулярные отображения между ними.

Мы не будем глубже уходить в тонкости теории схем, поскольку в этом курсе схемы нам потребуются лишь как средство привлечения геометрической интуиции к изучению свойств коммутативных колец и их гомоморфизмов.

2.3. Геометрический анализ гоморфизмов колец. Язык схем даёт вполне адекватную геометризованную переформулировку всей алгебры, связанной с коммутативными кольцами и их гомоморфизмами. Например, по произвольному гомоморфизму $A \xrightarrow{\varphi^*} B$ произвольных коммутативных колец строится непрерывное отображение $Spec(B) \xrightarrow{\varphi} Spec(A)$, переводящее $\mathfrak{q} \in B$ в полный прообраз $\varphi^{*-1}(\mathfrak{q}) \in A$. Такие отображения спектров называются *регулярными*.

Задача 3.25. Проверьте, что полный прообраз простого идеала относительно произвольного гомомрфизма произвольных коммутативных колец всегда является простым идеалом.

Задача 3.26. (Необязятельная.) Приведите примеры, показывающие, что для максимальных идеалов это неверно.

Предупреждение. Мы видели выше, что в геометрической ситуации прообраз максимального идеала максимален. Поэтому контрпримеры надо искать не среди алгебр над полем!

Задача 3.27. Проверьте, что регулярное отображение спектров действительно непрерывно.

2.3.1. Пример: изоморфизм схем. Как и в случае алгебраических многообразий, изоморфизм произвольных колец индуцирует, очевидно, гомеоморфизм из спектров. В этом случае соответствующие схемы называются *изоморфными*.

2.3.2. Пример: замкнутое вложение. Эпиморфизм колец $A \xrightarrow{\varphi^*} B$ также имеет простую геометрическую интерпретацию. Идеал $I = \ker(\varphi^*) \subset A$ определяет замкнутое подмножество $V(I) \subset Spec(A)$, причём его топология, индуцированная со $Spec(A)$ совпадает (убедитесь!) с топологией его как схемы $Spec(A/I)$. Поскольку φ^* индуцирует изоморфизм A/I с B, схема $Spec(B)$ отождествляется с $V(I)$. В этом случае говорят, что $Spec(B)$ является *замкнутой подсхемой* в $Spec(A)$ и называют $Spec(B) \xrightarrow{\varphi} Spec(A)$ *замкнутым вложением*.

Задача 3.28. Пусть $A \xrightarrow{\varphi^*} B$ – гоморфизм колец, $Spec(B) \xrightarrow{\varphi} Spec(A)$ – соответствующее регулярное отображение аффинных схем и $V(I) \subset Spec(B)$ – замкнутое подмножество в B. Докажите, что замыкание $\varphi(V(I))$ в $Spec(A)$ есть $V(J) \subset Spec(A)$, где J – полный прообраз I относительно φ^*.

Предупреждение. Образ замкнутого множества, вообще говоря, незамкнут (спроектируйте, например, гиперболу $xy = 1$ на прямую $y = 0$ вдоль оси OY).

2.3.3. Пример: расширения колец. Вопреки ожиданиям, геометрическая интерпретация вложения колец $A \subset B$ оказывается не такой простой, как интерпретация эпиморфизмов. Соответствующее отображение спектров переводит каждую точку $\mathfrak{q} \subset B$ в точку $\mathfrak{q} \cap A \subset A$. Тот же пример с проекцией гиперболы, которому отвечает вложение $k[x]$ в $k[x,y]/(xy-1)$ по правилу $x \longmapsto x \pmod{xy-1}$, показывает, что отображение спектров вложенных колец, вообще говоря, не эпиморфно. На языке идеалов это означает, что не у всякого простого (а в примере – даже и максимального) идеала $\mathfrak{p} \subset A$ имеется *подъём* в расширение $B \subset A$. Анализу тех случаев, когда такой подъём всё же имеет место, посвящён следующий параграф. В частности, мы увидим, что казус с проекцией гиперболы всегда исправляется малым шевелением направления проекции.

§3 Целые элементы

3.1. Арифметическая мотивировка. При изучении многочленов с рациональными коэффициентами важную роль играют соображения делимости в кольце $\mathbb{Z} \subset \mathbb{Q}$, ибо умножая многочлен из $\mathbb{Q}[x]$ на подходящее целое, мы получаем многочлен из $\mathbb{Z}[x]$, к которому применима довольно развитая арифметическая машинерия.

Задача 3.29. Докажите, что несократимая дробь $p/q \in \mathbb{Z}$ может быть корнем многочлена из $\mathbb{Z}[t]$ лишь в случае, когда p делит свободный член, а q делит старший коэффициент этого многочлена.

Задача 3.30. Докажите, что неприводимый многочлен из $\mathbb{Z}[t]$ неприводим и в $\mathbb{Q}[t]$.

Комментарий. Это утверждение известно как *Лемма Гаусса* и, как правило, доказывается в первом семестре университетского курса алгебры. Ниже в n° 3.2 мы докажем её обобщение.

Возникает естественное желание сконструировать нечто подобное в произвольном поле алгебраических чисел, т. е. построить в произвольном конечном расширении $K \supset \mathbb{Q}$ некое подкольцо $K \supset \mathfrak{O}_K \supset \mathbb{Z}$, которое бы выполняло роль кольца $\mathbb{Z}$. Интуитивно, хотелось бы, чтобы эти обобщённые целые числа составляли решётку в K и одновременно кольцо, и чтобы K было полем частных для $\mathfrak{O}_K$. Косвенным указанием на полезность такой конструкции являются целые Гауссовы числа $\{n+im \mid m,n \in \mathbb{Z}\} \subset \mathbb{Q}[i]$, при помощи которых решается ряд красивых арифметических задач (связанных с квадратичной формой x^2+y^2, для разложения которой на множители и приходится присоединять $i=\sqrt{-1}$).

Итак, мы должны решить, какие числа в конечномерном поле $K \supset \mathbb{Q}$ правильно считать целыми?

> Задача 3.31. Прежде чем читать дальше, предложите свой вариант ответа на этот вопрос.

Решение (предложенное во второй половине прошлого века) сотоит в том, что умножения на числа поля K можно рассматривать как линейные операторы на конечномерном векторном пространстве K над полем Q. В координатах над $\mathbb{Q}$ эти операторы записываются матрицами с рациональными элементами. Назовём оператор ζ *целым*, если в K найдется ζ-инвариантное подпространство L, в некотором базисе которого над $\mathbb{Q}$ ограничение $\zeta|_L$ записывается *целочисленной* матрицей.

Это условие допускает ряд переформулировок, пригодных и для произвольных расширений произвольных коммутативных колец.

3.1.1. Лемма. *Пусть $A \subset B$ – произвольные коммутативные кольца. Следующие условия на элемент $b\in B$ попарно эквивалентны:*

(i) существует A-модуль $M \subset B$, который b-инвариантен[4]*, эффективен*[5] *и конечно порождён*[6]

(ii) A-линейная оболочка бесконечного набора векторов $\{1, b, b^2, b^3, \dots\}$ является конечно порождённым A-модулем.

(iii) Некоторая степень b^n A-линейно выражается через меньшие степени, т. е. b удовлетворяет уравнению

$$b^n = a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_{n-1} b + a_n \,, \quad a_\nu \in A$$

(которое называется уравнением целой зависимости b над A).

Доказательство. Очевидно, что из (iii) следует (ii) и из (ii) следует (i). Чтобы вывести (iii) из (i), выберем в M систему образующих над A и запишем оператор умножения на b в виде матрицы с элементами из A. Характеристический многочлен $\chi(t)$ этой матрицы также будет иметь коэффициенты из A старший коэффициент 1. В силу тождества Гамильтона-Кэли оператор умножения на $\chi(b)$ аннулирует M, откуда $\chi(b)=0$, что и даёт уравнение целой зависимости.

□

---

[4]т. е. $bM \subset M$

[5]т. е. $\mathrm{Ann}_A(M) \overset{\text{def}}{=} \{a\in A \mid am=0 \;\; \forall\, m\in M\} = \{0\}$

[6]Конечно порождённые *модули* не следует путать с конечно порождёнными *алгебрами*. То, что A-*модуль* M порождается элементами $\{\zeta_1, \zeta_2, \dots, \zeta_k\}$, означает, по определению, что любой $\zeta \in M$ является *линейной комбинацией* $\zeta = \sum a_\nu \zeta_\nu$ с $a_\nu \in A$. В частности, в случае $A=\mathbb{Z}$, $B=K\supset\mathbb{Q}$ первое условие леммы в точности описывает ситуацию, когда умножение на b переводит $\mathbb{Q}$-линейную оболочку M в себя и записывается *целочисленной матрицей* в любом $\mathbb{Z}$-базисе M.

В противоположность этому, конечная порождённость A-*алгебры* R, скажем, элементами $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ означает, что произвольный $\alpha \in A$ является *многочленом* от α_ν, т. е. A-линейно выражается лишь через *всевозможные степени* α_ν.

3.1.2. Определение. *Элементы b удовлетворяющие условиям предыдущей леммы называются целыми над кольцом A.*

Кольцо B называется *целым* над кольцом A, если все его элементы целы над A. Расширения $B \supset A$, в которых B цело над A, называются *целыми*.

Совокупность всех целых над A элементов произвольного расширения $A \subset R$ называется *целым замыканием* A в R. Целостное (т. е. без делителей нуля) кольцо называется *целозамкнутым* или *нормальным*, если его целое замыкание в его поле частных совпадает с ним самим.

3.1.3. Пример. Кольцо $\mathbb{Z}$ целозамкнуто. Это сразу следует из зад.3.29: если рациональное число является корнем уравнения с целыми коэффициентами и старшим коэффициентом 1, то знаменатель в его несократимом представлении может быть только ± 1.

3.1.4. Пример: конечные расширения. Пусть $A \subset B$ и B конечно порождено как A-*модуль*. Тогда B цело над A. Это сразу следует из Лм.3.1.1 (i). По аналогии с конечными расширениями полей, разбиравшимися в прошлой лекции, такие расширения колец также называются *конечными*.

3.1.5. Пример: инварианты конечной группы. Пусть конечная группа G действует кольцевыми автоморфизмами на кольце A. Подкольцо $A^G \overset{\text{def}}{=} \{a \in A \mid g(a) = a \ \ \forall g \in G\}$ называется кольцом G-*инвариантов*.

Задача 3.32. Убедитесь, что это и вправду подкольцо.

Легко видеть, что A цело над A^G. Действительно, пусть $\{a_1, a_2, \dots, a_k\}$ – G-орбита произвольного элемента $a_1 \in A$. Тогда a_1 – корень многочлена $f(t) = (t - a_1)(t - a_2) \cdots (t - a_k)$, имеющего старший коэффициент 1 и прочие коэффициенты из A^G (ибо они будут симметрическими функциями от a_ν, которые просто переставляются группой G). Одно из применений подобного рассуждения см. ниже в n° 3.2.

3.1.6. Предложение. *Целое замыкание A в $B \supset A$ всегда является кольцом.*

Доказательство. Всё немедленно следует из сопоставления условий (i) и (ii) Лм.3.1.1: если все целые неотрицательные степени элементов b_1 и b_2 содержатся в A-модулях, порождённых, соответственно, конечными наборами b_1^ν с $0 \le \nu < n$ и b_2^μ с $0 \le \mu < m$, то операторы умножения на $b_1 b_2$ и на $(b_1 + b_2)$ переводят в себя конечный A-модуль, порождённый набором $b_1^\nu b_2^\mu$ с $0 \le \nu < n$, $0 \le \mu < m$.
□

3.1.7. Предложение. *Пусть $C \supset B \supset A$ – коммутативные кольца, B цело над A и $c \in C$ цел над B. Тогда c цел над A.*

Доказательство. Пусть $b_1, b_2, \dots, b_n$ — коэффициенты правой части уравнения целой зависимости c над B, и пусть для каждого $i = 1, 2, \dots, n$ все степени b_i A-линейно выражаются через конечное число первых нескольких степеней $b_i^{\nu_i}$, $0 \le \nu_i < m_i$. Тогда умножение на c переводит в себя конечный A-модуль, порождённый всевозможными произведениями

$$c^\mu \cdot b_1^{\nu_1} \cdot b_2^{\nu_2} \cdot \dots \cdot b_n^{\nu_n} ,$$

где $0 \le \mu < n$, $0 \le \nu_i < m_i$.
□

3.2. Лемма Гаусса-Дедекинда-Кронекера. Пусть

$$\alpha(t) \;=\; a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n$$

$$\begin{aligned}\beta(t) &= b_0t^m + b_1t^{m-1} + \cdots + b_{m-1}t + b_m\\ \gamma(t) = \alpha(t)\cdot\beta(t) &= c_0t^{n+m} + c_1t^{n+m-1} + \cdots + c_{n+m-1}t + c_{n+m}\end{aligned}$$

— многочлены, рассматриваемые *формально*, т. е. как элементы кольца

$$B = \mathbb{Z}[t, a_0, \dots, a_n, b_0, \dots, b_m]\,.$$

Коэффициенты $c_\nu \in B$ выражаются через a_ν и b_μ по известным формулам и порождают подкольцо $A \simeq \mathbb{Z}[c_0, \dots, c_{n+m}] \subset B$.

3.2.1. Предложение. *В описанной выше ситуации все попарные произведения $a_ib_j \in B$ целы над A.*

Доказательство. Вложим B в большее кольцо $R = \mathbb{Z}[t, a_0, b_0, x_1, \dots, x_{n+m}]$, порождённое формальными корнями многочленов $\alpha(t)$ и $\beta(t)$. Это вложение задаётся сопоставлением

$$\begin{aligned} a_\nu &\longmapsto (-1)^\nu a_0\sigma_\nu(x_1, \dots, x_n)\\ b_\mu &\longmapsto (-1)^\mu b_0\sigma_\mu(x_{n+1}, \dots, x_{n+m}) \quad ,\end{aligned}$$

где $\nu, \mu \geq 1$. В R все наши многочлены раскладываются на линейные множители:

$$\alpha(t) = a_0\prod_{\nu=1}^{n}(t - x_\nu) \qquad \beta(t) = b_0\prod_{\nu=n+1}^{n+m}(t - x_\nu) \qquad \gamma(t) = c_0\prod_{\nu=1}^{n+m}(t - x_\nu)$$

Симметрическая группа $\mathfrak{S}_{n+m}$ действует на R перестановками формальных корней. Как и в n° 3.1.5, рассмотрим орбиту $\{p_1, p_2, \dots, p_s\}$ элемента $p_1 = \sigma_i(x_1, \dots, x_n)\cdot\sigma_j(x_{n+1}, \dots, x_{n+m})$ и составим целое уравнение $(t - p_1)(t - p_2)\cdots(t - p_s) = 0$ на p_1. Коэффициенты этого уравнения лежат, очевидно, в $\mathbb{Z}[c_0, \dots, c_{n+m}]$, так что умножив обе части на подходящую степень $(-1)^{i+j}c_0$, получим уравнение целой зависимости на $a_ib_j = (-1)^{i+j}c_0p_1$.
□

Задача 3.33. Убедитесь, что если b цел над A, то и все его A-кратные целы над A.

Задача 3.34. Пусть $\mathfrak{O}$ — целостное целозамкнутое кольцо с полем частных K. Используя n° 3.2 докажите, что:

а) если приведённый многочлен из $\mathfrak{O}[t]$ раскладывается в $K[t]$ в произведение двух многочленов со старшими коэффициентами 1, то оба этих многочлена в действительности лежат в $\mathfrak{O}[t]$;

б) если многочлен из $\mathfrak{O}[t]$ неприводим в $\mathfrak{O}[t]$, то он неприводим и в $K[t]$.

3.3. Целые алгебраические числа. Обратимся опять к случаю, когда $A = \mathbb{Z}$ — кольцо целых рациональных чисел, а $B = \mathfrak{O}_K \subset K$ — его целое замыкание в конечном алгебраическом расширении $K \supset \mathbb{Q}$. Кольцо $\mathfrak{O}_K$ называется *кольцом целых (алгебраических) чисел* поля K.

3.3.1. Лемма. $\forall\,\zeta \in K$ *можно подобрать целое рациональное число $m \in \mathbb{N}$, так чтобы $m\zeta \in \mathfrak{O}_K$. В частности, любой базис поля K над $\mathbb{Q}$ можно после домножения на подходящее натуральное число считать состоящим из целых алгебраических чисел.*

Доказательство. Если минимальное уравнение на ζ над $\mathbb{Q}$ имеет вид

$$\zeta^n + \frac{p_1}{q_1}\zeta^{n-1} + \frac{p_2}{q_2}\zeta^{n-2} + \cdots + \frac{p_n}{q_n} = 0\;,$$

то полагая $q = HOK(q_1, q_2, \dots, q_n)$ и умножая обе части на q^n, мы получаем уравнение целой зависимости на $q\zeta$ над $\mathbb{Z}$.
□

3.3.2. След. Для всякого $\zeta \in K$ обозначим через $\mathrm{Sp}(\zeta)$ *след* оператора умножения на ζ в K. Поскольку след единицы $\mathrm{Sp}(1) = \underbrace{1+1+\dots+1}_{\dim K} = \dim K$, след является ненулевым[7] $\mathbb{Q}$-значным линейным функционалом на векторном пространстве K.

3.3.3. Лемма. *Минимальный многочлен целого алгебраического числа имеет целые коэффициенты, и след целого алгебраического числа — цел.*

Доказательство. Пусть $\zeta \in \mathfrak{O}_K$ — цел, и $f(\zeta) = 0$ — его уравнение целой зависимости над $\mathbb{Z}$, а $\varphi(\zeta) = \zeta^k + q_1\zeta^{k-1} + \dots + q_{k-1}\zeta + q_k$ — его минимальный многочлен над $\mathbb{Q}$. Поскольку φ делит f в $\mathbb{Q}[t]$ и оба они имеют старший коэффициент 1, по лемме Гаусса (зад.3.34) все остальные коэффициенты q_i также будут целыми.

Пусть $L \simeq \mathbb{Q}[t]/(\varphi(t))$ — наименьшее подполе в K, содержащее $\mathbb{Q}$ и ζ. Поскольку K — это векторное пространство над L, мы имеем ζ-инвариантное разложение

$$K = \underbrace{L \oplus L \oplus \dots \oplus L}_{\dim_L(K)} .$$

Таким образом, $\mathrm{Sp}(\zeta)$ есть умноженный на $\dim_L(K)$ след оператора умножения на ζ в поле $\mathbb{Q}[t]/(\varphi(t))$. Последний, очевидно, равен q_1 и по доказанному выше цел.
□

Для произвольных $\eta, \zeta \in K$ обозначим через $\mathrm{Sp}(\eta, \zeta)$ след произведения $\eta\zeta$. Очевидно, что $\mathrm{Sp}(\eta, \zeta)$ является $\mathbb{Q}$-значной симметричной билинейной формой на $K \times K$, причём она принимает целые значения на $\mathbb{Z}$-подмодуле $\mathfrak{O}_K \times \mathfrak{O}_K$.

Легко усмотреть, что эта форма невырождена. Если вектор $\kappa \neq 0$ находился в ядре *билинейной формы* следа и имеет нулевые скалярные произведения со всеми векторами некоторого базиса $\{\zeta_1, \zeta_2, \dots, \zeta_n\}$ поля K над $\mathbb{Q}$, то в базисе $\{\kappa\zeta_1, \kappa\zeta_2, \dots, \kappa\zeta_n\}$ *функционал* следа имеет нулевые коэффициенты, что невозможно.

3.3.4. Предложение. *Пусть $K \supset \mathbb{Q}$ – конечное расширение и $\dim_{\mathbb{Q}}(K) = n$. Кольцо целых алгебраических чисел $\mathfrak{O}_K$ составляет n-мерную целочисленную подрешётку в K (т. е. является свободным $\mathbb{Z}$-модулем ранга n).*

Доказательство. Выберем базис $\{\zeta_1, \zeta_2, \dots, \zeta_n\}$ поля K над $\mathbb{Q}$, состоящий из элементов $\mathfrak{O}_K$. Пусть $\{\hat{\zeta}_1, \hat{\zeta}_2, \dots, \hat{\zeta}_n\}$ – двойственный базис относительно следа, определяемый условиями $\mathrm{Sp}(\hat{\zeta}_i, \zeta_j) = \delta_{ij}$ (он существует вследствии невырожденности формы). Тогда $\mathfrak{O}_K$ содержится в свободном $\mathbb{Z}$-модуле, порождённом $\{\hat{\zeta}_1, \hat{\zeta}_2, \dots, \hat{\zeta}_n\}$. Действительно, коэффициенты разложения целого алгебраического числа по этому базису являются целыми, ибо они суть скалярные произведения с векторами двойственного базиса, который цел.

Как подмодуль свободного $\mathbb{Z}$-модуля, модуль $\mathfrak{O}_K$ также будет свободен, а так как его $\mathbb{Q}$-линейная оболочка совпадает с K, $\mathrm{rk}\,\mathfrak{O}_K = n$.
□

---

[7] Если вместо $\mathbb{Q}$ рассматривается поле конечной характеристики, то это, вообще говоря, неверно. Однако, наша выкладка показывает, что след ненулевой, если степень расширения не делится на характеристику поля. Расширения, для которых функционал следа нетривиален, называются *сепарабельными*. Расширения, в которых след тождественно нулевой, называются *несепарабельными*.

Задача 3.35. Опишите кольцо целых чисел в расширениях $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{-3}]$, $\mathbb{Q}[\sqrt{3}]$ и $\mathbb{Q}[\sqrt{5}]$. Попытайтесь дать ответ для произвольного квадратичного расширения $\mathbb{Q}[\sqrt{d}]$, где d – натуральное, свободное от квадратов (вид ответа зависит от вычета $d \pmod 4$).

3.4. Целость и обратимость. Вернёмся вновь к произвольным целым расширениям $B \supset A$. Интуитивно ясно, что элемент, обратный к целому, редко когда бывает целым.

3.4.1. Лемма. *Пусть $B \supset A$ цело над A. Тогда*

(i) если B — поле, то и A — поле;

(ii) если A — поле и в B нет делителей нуля, то и B — поле.

Доказательство. Если B – поле, то всякий элемент $a \in A$ обратим в B, и по условию $a^{-1} \in B$ цел над A, т. е.

$$a^{-n} = a_1 a^{-n+1} + a_2 b^{-n+2} + \cdots + a_{-1} b + a_n \;, \quad a_\nu \in A \;.$$

Умножая обе части на a^{n-1}, получаем, что $a^{-1} \in A$.

Пусть A – поле. Оператор умножения на произвольное ненулевое $b \in B$ переводит в себя подпространство, порождённое векторами $1, b, b^2, \ldots$. Это подпространство конечномерно (b – цел) и b действует на нём инъективно (в B нет делителей нуля). Поэтому b – изоморфизм и прообраз 1 есть не что иное как b^{-1}.

□

3.4.2. Предложение. *Пусть B – кончно-порождённая алгебра над произвольным полем k. Если B – поле, то B алгебраично над k.*

Доказательство. Индукция по числу образующих B над k. Пусть B порождается (как алгебра) элементами $a_1, a_2, \ldots, a_m$. Применяя индуктивное предположение к паре $k(a_m) \subset B$, где $k(a_m)$ – наименьшее подполе в B, содержащее k и a_m, мы можем считать, что остальные образующие $a_1, a_2, \ldots, a_{m-1}$ алгебраичны над $k(a_m)$. Это означает, что при $1 \le \nu \le (m-1)$ образующая a_ν является корнем (возможно, неприведённого) многочлена $f_\nu(z)$, коэффициенты которого — *многочлены* от a_m.

Пусть $p = p(a_m)$ – произведение старших коэффициентов всех многочленов $f_\nu(z)$, а $A \subset B$ — k-подалгебра, порождённая элементом p^{-1} (обратными к p в B). Т. к. B цело над A, A является полем (по Лм.3.4.1). Но наличие в A обратного элемента, скажем, к $1 + p^{-1}$ означает наличие соотношения

$$\left(1 + \frac{1}{p(a_m)}\right) \cdot g\left(\frac{1}{p(a_m)}\right) = 1 \quad , \qquad p, g \in k[t] \;. \tag{3-1}$$

Рациональная функция одного переменного $g\left(\dfrac{1}{p(t)}\right) \in k(t)$ может быть переписана в виде $\dfrac{h(t)}{p(t)^d}$, где $h(t) \in k[t]$ — многочлен, который не делится на $p(t)$ в $k[t]$. Умножив обе части (3-1) на $p(a_m)^{d+1}$, получаем, что a_m является корнем полиномиального уравнения

$$\Big(p(t) + 1\Big) \cdot h(t) = p(t)^{d+1}$$

над k. Это уравнение нетривиально (не есть тождество в $k[t]$), поскольку левая часть не делится на $p(t)$. Стало быть, a_m алгебраичен над k, а значит, и B алгебраично над k, что и требовалось.

□

3.4.3. Уточнения к доказательству der Nullstellensatz. Теперь мы в можем значительно прояснить доказательство "трудной части" теоремы Гильберта о нулях. Я напомню, что мы должны были построить точку в $\mathbb{A}_n(k)$, в которой бы обращались в нуль все полиномы из некоторого максимального идеала $\mathfrak{m} \in k[x_1, \dots, x_n]$. Мы убедились, что такая точка существует над конечно порождённым расширением $K = k[x_1, \dots, x_n]/\mathfrak{m}$ поля k. Заметим теперь, что поле K конечно порождено над k не *как поле*, а *как алгебра*, т. е. состоит из k-линейных целых *неотрицательных* степеней своих образующих. По предыдущему предложению K алгебраично над k, и если k алгебраически замкнуто, то $K = k$, что и доказывает теорему Гильберта.

Отметим, что тем самым мы доказали der Nullstellensatz над алгебраически замкнутым полем произвольной характеристики.

3.5. Конечные морфизмы. Вернёмся к примеру, на котором мы остановились в n° 2.3.3. Мы собираемся доказать, что вложению колец $A \hookrightarrow B$ при котором B цело над образом A соответствует *эпиморфизм* аффинных схем, а в геометрической ситуации — конечное накрытие (вообще говоря, разветвлённое).

Напомню, что морфизм $Spec(B) \longrightarrow Spec(A)$, индуцированный вложением $A \hookrightarrow B$, отображает простой идеал $\mathfrak{q} \subset B$ в его пересечение с образом A. Поэтому наши геометрические утверждения эквивалентны следующему предложению.

3.5.1. Лемма о подъёме. *Пусть $B \supset A$ цело над A. Тогда:*

(i) для любого простого идеала $\mathfrak{p} \subset A$ существует простой идеал $\mathfrak{q} \subset B$ такой, что $\mathfrak{p} = \mathfrak{q} \cap A$ (он называется подъёмом $\mathfrak{p}$ в B);

(ii) для любого максимального идеала $\mathfrak{m} \subset A$ всякий простой идеал $\mathfrak{q} \subset B$ такой, что $\mathfrak{q} \cap A = \mathfrak{m}$, автоматически является максимальным в B;

(iii) для любого максимального идеала $\mathfrak{q} \subset B$ идеал $\mathfrak{q} \cap A$ максимален в A;

(iv) если B конечно порождено как A-модуль, то у каждого простого идеала $\mathfrak{p} \subset A$ имеется лишь конечное число простых подъёмов.

Доказательство. Доказательство (iii). Если $\mathfrak{q} \subset B$ – максимальный идеал, то. поле $B/\mathfrak{q}$ цело над подкольцом $A/(\mathfrak{q} \cap A)$, которое по Лм.3.4.1 также будет полем. Следовательно, $\mathfrak{q} \cap A$ – максимальный идеал в A.

Доказательство (ii). Если $\mathfrak{q} \subset B$ – простой идеал, для которого $\mathfrak{q} \cap A = \mathfrak{m}$ – максимален в A, то целостное кольцо $B/\mathfrak{q}$ цело над полем $A/\mathfrak{m}$ и по Лм.3.4.1 является полем. Поэтому $\mathfrak{q}$ – максимален.

Доказательство (i) и (iv). Прежде всего заметим, что из (ii) и (iii) следует, что в специальном частном случае, когда A – локальное кольцо, а $\mathfrak{p} = \mathfrak{m}$ – его максимальный идеал, утверждение (i) имеет место, и простые идеалы кольца B, высекающие в пересечении с A единственный в A максимальный идеал $\mathfrak{m}$ – это всевозможные максимальные идеалы B и только они. Эти максимальные идеалы находятся во взимно-однозначном соответствии с максимальными идеалами алгебры $B/\mathfrak{m}B$ над полем $A/\mathfrak{m}$. Если B – конечнопорождённый A-модуль, то $B/\mathfrak{m}B$ конечномерна над $A/\mathfrak{m}$, а значит (iv) также справедливо в силу задачи:

> Задача 3.36. Пусть F – k-алгебра, конечномерная как векторное пространство над k (такие алгебры называются *артиновыми*). Докажите, что все простые идеалы в F максимальны и их имеется лишь конечное число.
>
> Совет: используйте Лм.3.4.1.

Общий случай сводится к разобранному частному при помощи *локализации*. А именно, пусть A – любое кольцо, и $\mathfrak{p} \subset A$ – произвольный простой идеал. Рассмотрим *кольца частных* $A[S^{-1}]$ и $B[S^{-1}]$ по мультипликативному подмножеству $S = A \setminus \mathfrak{p} \subset A \subset B$ (см. n° 2.2.1) .

> Задача 3.37. Убедитесь, что $A[S^{-1}] \subset B[S^{-1}]$ — целое расширение колец и что $B[S^{-1}]$ конечно порождено как $A[S^{-1}]$-модуль, если B было конечно порождённым A-модулем.

Кольцо $A[S^{-1}]$ является локальным с единственным максимальным идеалом $\mathfrak{p}[S^{-1}] \stackrel{\text{def}}{=} \operatorname{loc}_S(\mathfrak{p})$, где $\operatorname{loc}_S\colon\ A \longrightarrow A[S^{-1}]$ – естественный гомоморфизм. По доказанному выше, простой идеал $\mathfrak{q}_S \subset B[S^{-1}]$, пересечение которого с подкольцом $A[S^{-1}]$ совпадает с $\mathfrak{p}[S^{-1}]$ существует[8]. Пусть $\mathfrak{q} \subset B$ – полный прообраз одного из таких идеалов относительно естественного отображения $B \xrightarrow{\operatorname{loc}_S} B[S^{-1}]$. По зад.3.25 $\mathfrak{q}$ – простой идеал. Очевидно, что $\mathfrak{p} \subset \mathfrak{q} \cap A$. Наоборот, для любого $f \in \mathfrak{q} \cap A$ условие $f/1 \in \mathfrak{p}[S^{-1}]$ означает, что $s \cdot (f \cdot s_2 - p \cdot 1) = 0$ для неких $s, s_2 \in S$ и $p \in \mathfrak{p}$. Поэтому $sfs_2 \in \mathfrak{p}$, откуда $f \in \mathfrak{p}$ и $\mathfrak{p} = \mathfrak{q} \cap A$.

Это доказывает (i). Для завершения доказательства (iv) остаётся заметить, что всякий подъём $\mathfrak{q} \subset B$ простого идеала $\mathfrak{p} \subset A$ при локализации по S превращается в подъём $\mathfrak{q}[S^{-1}] \supset B[S^{-1}]$ простого идеала $\mathfrak{p}[S^{-1}] \subset A[S^{-1}]$ (см. задачу ниже), так что (iv) следует из сделанной выше сноски ([8]).

> Задача 3.38. Докажите, что образы простых идеалов при любой локализации остаются простыми идеалами.

□

Регулярное отображение аффинных алгебраических многообразий $V \xrightarrow{\varphi} W$ называется *конечным морфизмом*, если $k[W] \xrightarrow{\varphi^*} k[V]$ – вложение и $k[W]$ конечно порождено как модуль над $k[V]$. Из доказанного предложения следует, что конечный морфизм является локально-конечным накрытием. Замечательно, что любое аффинное алгебраическое мнообразие можно реализовать как такого сорта накрытие над аффинным пространством.

3.6. Нётерова нормализация. Пусть k – бесконечное поле, и $A = k[x_1, \dots, x_m]/I$ — произвольная конечно порождённая k-алгебра. Можно воспринимать её как структурное кольцо замкнутой подсхемы в $\mathbb{A}_m(k)$, заданной как множество нулей идеала $I \subset k[x_1, \dots, x_m]$. Если $I \neq (0), (1)$, то эта подсхема непуста и отлична от всего пространства, а значит мы можем параллельно спроектировать её на какую-нибудь гиперплоскость. Если направление проекции выбрать неассимптотическим для для нашей подсхемы, то ограничение проекции на подсхему будет конечным морфизмом. Если его образ отличен от всей гиперплоскости, то процедуру можно будет повторить, и далее продолжать до тех пор, пока не получим конечного накрытия над аффинным пространством подходящей размерности.

На языке формул это означает следующее.

3.6.1. Лемма Эмми Нётер о нормализации. *Всякая конечно порождённая алгебра над бесконечным полем k является конечно порождённым модулем над кольцом многочленов $k[t_1, \dots, t_n]$ от подходящего числа переменных.*

Доказательство. Индукция по числу образующих алгебры A над k. Пусть A порождается m образующими $a_1, a_2, \dots, a_m$. Если они алгебраически независимы, то A есть кольцо многочленов, и доказывать нечего. Если между ними есть алгебраическая зависимость $f(a_1, \dots, a_m) = 0$, то мы разложим f в сумму однородных компонент $f = f_d + f_{d-1} + \dots + f_0$, где $\deg f_\nu = \nu$ и предположим, что a_m явно входит в форму старшей степени f_d.

---

[8]Как мы видели, этим свойством обладают все максимальные идеалы кольца $B[S^{-1}]$ и только они. Их число конечно, если B конечно порождено как модуль над A.

Если в $f_d(a_1, a_2, \ldots, a_m)$ имеется чистая степень $\alpha \cdot a_m^d$, где $\alpha \in k$, то деля соотношение $f(a_1, a_2, \ldots, a_m) = 0$ на α, мы получим уравнение целой зависимости для a_m над подкольцом, порождённым $a_1, a_2, \ldots, a_{m-1}$, которое по индукции можно считать конечным модулем над кольцом многочленов. Поскольку целый элемент над целым расширением цел и над исходным кольцом, присоединяя a_m мы вновь получим конечный модуль над кольцом многочленов. Так что в этом случае всё доказано (а индуктивный переход геометрически изображается проекцией вдоль m-той координатной оси на гиперплоскость, натянутую на остальные оси).

Если в $f_d(a_1, a_2, \ldots, a_m)$ нет чистой степени $\alpha \cdot a_m^d$, то надо чуть-чуть пошевелить направление проекции. А именно, заменим образующие $a_1, a_2, \ldots, a_{m-1}$ на новые образующие $b_1, b_2, \ldots, b_{m-1}$, связанные со старыми формулами $a_\nu = b_\nu + \lambda_\nu \cdot a_m$, где $1 \leq \nu \leq (m-1)$ и $\lambda_\nu \in k$. Подставляя выражения a_ν через b_ν в f, получим

$$0 = f(b_1, b_2, \ldots, b_{m-1}, a_m) = f_d(\lambda_1, \ldots, \lambda_{m-1}, 1) \cdot a_m^d + \text{члены меньшей степени по } a_m .$$

Таким образом, чистая степень a_m^d после нашего шевеления будет входить с коэффициентом $f_d(\lambda_1, \ldots, \lambda_{m-1}, 1)$ и над бесконечным полем иы можем подобрать константы λ_ν так, чтобы этот коэффициент не занулился. Но тогда a_m будет цел над подкольцом, порождённым $b_1, b_2, \ldots, b_{m-1}$, и доказательство завершается как в предыдущем случае.
□

3.6.2. Следствие. *Для произвольного аффинного алгебраического многообразия V над произвольным алгебраически замкнутым полем k существует конечный морфизм $V \longrightarrow \mathbb{A}_m(k)$ на аффинное пространство подходящей размерности.*

□