Алгебраическая геометрия.

Лектор — Иван Александрович Панин
Создатель конспекта — Глеб Минаев *

TODOs

Содержание

Литература:

- Хартсхорн, “Алгебраическая геометрия”.
- Атья, Макдональд, “Введение в коммутативную алгебру”.

Замечание 1. Все кольца ассоциативны, коммутативны и с единицей.

1 Коммутативноалгебраическое введение

Определение 1. Пусть I — частично упорядоченное по порядку $\leqslant$ множество, т.е.

$$a \leqslant b \leqslant c \quad \Longrightarrow \quad a \leqslant c.$$

ОВУ: всякая последовательности элементов $i_1 \leqslant i_2 \leqslant \dots$ стабилизируется с некоторого момента (т.е. последовательность имеет константный хвост).

Наличие минимального элемента. Для всякого $J \subseteq I$ существует $j_{max} \in J$, что для всякого $j \in J$ имеет место следствие $j_{max} \leqslant j \Rightarrow j = j_{max}$.

Лемма 1. *I удовлетворяет ОВУ тогда и только тогда, когда I удовлетворяет наличию минимального элемента.*

*Оригинал конспекта расположен на GitHub. Также на GitHub доступен репозиторий с другими конспектами.

Доказательство.

$\Rightarrow$) Предположим, что максимального элемента, т.е. для всякого элемента есть строго больший. Тогда мы можем построить строго возрастающую последовательность, что противоречит ОВУ.

$\Leftarrow$) Пусть дана нестрого возрастающая последовательность $(i_m)_{m=1}^{\infty}$. Тогда применяя свойство наличия максимального элемента для $J := \{i_m\}_{m=1}^{\infty}$, получаем, что есть $j_M \in J$ (для некоторого M), для которого нет строго большего в J. Значит после j_M все элементы с ним совпадают.

$\square$

Определение 2. Пусть A — кольцо, а M — A-модуль. Тогда $\mathrm{mod}(A)$ — множество всех подмодулей в M, упорядоченных по включению ($(0), M \in \mathrm{mod}(M)$).

M *нётеров*, если $\mathrm{mod}(A)$ удовлетворяет ОВУ (или наличию максимального элемента).

Лемма 2.

1. *Если M нётеров, то любой подмодуль $N \subseteq M$ конечнопорождён (как A-модуль).*

2. *Если любой подмодуль M конечнопорождён, то M нётеров.*

Доказательство.

$1 \Rightarrow 2$) Пусть M нётеров, $N \subseteq M$ — подмодуль. Пусть I — все конечнопорождённые модули в N.

I непуст, так как $(0) \in I$. Следовательно, в I есть максимальный элемент, пусть N_{max}. Если $N_{max} = N$, то N конечнопорождён. Если $N_{max} \neq N$, то существует $x \in N \setminus N_{max}$, что $N_{max} \nsubseteq N_{max} + x \cdot A \subseteq N$ — противоречие.

$2 \Rightarrow 1$) Пусть имеется последовательность $M_1 \subseteq M_2 \subseteq \ldots$ подмодулей M. Определим

$$M_\infty := \bigcup_{m=1}^{\infty} M_m.$$

M_∞ тоже подмодуль M. Значит M_∞ конечнопорождён. $x_1, \ldots, x_n \in M_\infty$, значит есть n_0, что $x_1, \ldots, x_n \in M_{n_0}$. Следовательно,

$$M_{n_0} = M_{n_0+1} = M_{n_0+2} = \ldots$$

$\square$

Лемма 3. *M' — подмодуль M и есть сюръективный гомоморфизм $\pi : M \to M/M' = M''$. Тогда M нётеров тогда и только тогда, когда M' и M'' нётеровы.*

Доказательство. Пусть M — нётерово. Покажем, что M' нётерово. Пусть есть цепочка $M'_1 \subseteq M'_2 \subseteq \ldots$ подмодулей M. M нётерово, значит цепочка стабилизируется, значит M' нётерова.

Покажем, что M'' нётерово. Пусть есть цепочка подмодулей $M''_1 \subseteq M''_2 \subseteq \ldots$. Следовательно $[\pi(\pi^{-1}(M''_1) \subseteq \pi^{-1}(M''_2) \subseteq \ldots)] \subseteq M$. Значит цепочка стабилизируется. Значит стабилизируется изначальная цепочка, значит M'' нётерово.

Теперь предположим, что M' и M'' нётеровы.

Дописать.

$\square$

Определение 3. Кольцо A *нётерово*, если как модуль над собой нётерово.

Замечание 2. 1 — образующая A как A-модуля. Всякий идеал I является подмодулем A, но может не иметь одного образующего.

Определение 4. *Идеал* I кольца A — непустое подмножество A, что для всяких $a, b \in I$ $a + b \in I$ и для всяких $a \in I$, $k \in A$ $ak \in I$.

Лемма 4. *Пусть дано кольцо A. TFAE*

1. *A нётерово.*
2. *Любая цепочка идеалов $I_1 \subseteq I_2 \subseteq \dots$ стабилизируется.*
3. *Всякий идеал I конечнопорождён.*

Доказательство.

$1 \Leftrightarrow 2)$ По определению.

$1 \Leftrightarrow 3)$ По лемме 2.

□

Лемма 5. *Пусть дано нётерово кольцо A. Тогда для всякого $n \geqslant 0$ A^n — нётеров модуль.*

Доказательство. (0) — нётеров. $A^1 = A$ — нётеров. Далее легко провести по индукции, что A^{n-1} нётерово и $A^n/A^{n-1} = A$ нётерово, а тогда A^n нётерово. □

Следствие 5.1. *Если A — нётерово кольцо, то всякий конечнопорождённый A-модуль M нётеров.*

Доказательство. Пусть $m_1, \dots, m_r \in M$ — система порождающих модуля M. Тогда имеем сюръективный гомоморфизм $A^r \to M$, порождённый $e_i \mapsto m_i$. Следовательно, по лемме 3 из нётеровости A^r следует нётеровость M. □

Следствие 5.2. *Если M — конечнопорождённый модуль и N — подмодуль M, то N конечнопорождён. В частности всякий подмодуль $N \subseteq A^r$ конечнопорождён.*

Доказательство.

Дописать.

□

Теорема 6 (Гильберта)**.** *Если кольцо A нётерово, то $A[t]$ нётерово.*

Доказательство. Пусть фиксирован некоторый идеал I в $A[t]$. Как только мы покажем, что I конечнопорождён, то применяя лемму 4, получим нётеровость $A[t]$.

Пусть $\mathcal{A} \subseteq A$ — множество старших членов многочленов из I.

Лемма 6.1. *$\mathcal{A}$ — идеал. И, следовательно, конечнопорождено.*

Доказательство. Действительно, для всяких $a, b \in \mathcal{A}$ есть многочлены $f_a, f_b \in I$ со старшими коэффициентами a и b соответственно. Следовательно $f_a t^{\deg(f_b)} + f_b t^{\deg(f_a))}$ лежит в I и имеет старший коэффициент $a+b$ (если только $a+b \neq 0$; иначе очевидно). Также если $a \in \mathcal{A}$, а $k \in A$, то есть многочлен $f_a \in I$ с данным старшим коэффициентом. Но тогда kf_a (если $ak \neq 0$; иначе очевидно) лежит в I и имеет старший член ak. □

Рассмотрим $a_1, \ldots, a_r$ — система порождающих $\mathcal{A}$, а $f_1, \ldots, f_r$ — многочлены из I с данными старшими коэффициентами.

Тогда всякий $f \in I$ порождается тогда и только тогда, когда порождается соответствующий ему $g \in I$ степени меньше $n := \max_k \deg(f_k)$, так как иначе с помощью старших членов f_i можно породить старший член f, вычесть его из f и тем самым понизить степень. Значит вопрос свёлся к порождаемости многочленов из I степени не выше n.

Заметим, что описанные многочлены образуют модуль $I \cap (A \oplus At \oplus \cdots \oplus At^{n-1})$ — подмодуль A^n. Значит $I \cap (A \oplus At \oplus \cdots \oplus At^{n-1})$ конечнопорождён, а отсюда I конечнопорождён. $\square$

Лемма 7. *Если B — нётерово кольцо, C — кольцо, а $\varphi : B \to C$ — гомоморфизм колец, то $\varphi(B)$ — нётерово.*

Доказательство. Пусть дана последовательность идеалов $I_1 \subseteq I_2 \subseteq \ldots$ в $\varphi(B)$. Тогда $\varphi^{-1}(I_i)$ — идеалы и

$$\varphi^{-1}(I_1) \subseteq \varphi^{-1}(I_2) \subseteq \ldots.$$

Значит с какого-то момента эта цепочка стабилизируется, а значит стабилизируется образ этой цепочки по φ, т.е. изначальная цепочка. $\square$

Лемма 8. *Если $\psi : A \to C$ — гомоморфизм колец, такой что C — конечная A-алгебра, порождённая элементами $x_1, \ldots, x_n$. Тогда C нётеров.*

Доказательство. Мы можем рассмотреть нативное вложение A в $A[t_1, \ldots, t_n]$ и гомоморфизм A-алгебр $\varphi : A[t_1, \ldots, t_n] \to C$, порождённый ψ и соотношениями $\varphi(t_i) = x_i$.

$$\begin{tikzcd}
A \arrow[rr, "\psi"] \arrow[dr, hook] & & C \\
& A[t_1, \ldots, t_n] \arrow[ur, two heads, "\varphi"'] &
\end{tikzcd}$$

φ сюръективен, а $A[t_1, \ldots, t_n]$ нётерово. Таким образом $\varphi(B) = C$ нётерово. $\square$

Замечание 3. Всякое поле нётерово.

Следствие 8.1. *Любая конечнопорождённая F-алгебра, где F — поле, нётерова.*

Замечание 4.
- $\mathbb{Z}$ — нётерово кольцо.
- Всякое кольцо является $\mathbb{Z}$-кольцом.
- Если кольцо R — конечнопорождённая $\mathbb{Z}$-алгебра, то оно нётерово.

Лемма 9. *Пусть A — нётерово кольцо, а M'' — A-модуль. Тогда M конечнопорождён тогда и только тогда, когда нётеров.*

Доказательство. Если M'' нётеров, то уже доказано, что M'' конечнопорождён, так как является собственным подмодулем (см. лемму).

Если M'' конечнопорождено, то есть система порождающих $m_1, \ldots, m_s$. Тогда есть сюръективный гомоморфизм

$$\varphi : A^s \to M'', e_i \mapsto m_i.$$

При этом A^s нётеров, значит M'' нётеров. $\square$

Лемма 10. *Пусть даны кольца $A \subseteq B \subseteq C$, что A — нётерово, C — конечнопорождённый B-модуль и конечнопорождённая A-алгебра. Тогда B — конечнопорождённая A-алгебра.*

Доказательство. Пусть $y_1, \ldots, y_n$ — система порождающих C как A-алгебру, а $x_1, \ldots, x_m$ — система порождающих C как B-модуль. Тогда есть $b_{i,j} \in B$, что

$$y_i = \sum b_{i,j} x_j,$$

и $b_{i,j,k} \in B$, что

$$x_i x_j = \sum b_{i,j,k} x_k.$$

Пусть B_0 — это A-подалгебра в B, порождённая всеми $b_{i,j}$ и $b_{i,j,k}$. Заметим, что количество перечисленных порождающих конечно, т.е. B_0 — конечнопорождённая алгебра. Следовательно, B_0 нётерова.

Поймём, что C порождается уже над B_0 элементами $x_1, \ldots, x_n$. Действительно, для всякого $c \in C$ есть $F \in A[t_1, \ldots, t_n]$, что $c = F(y_1, \ldots, y_n)$. При этом $y_i = \sum b_{i,j} x_j$. Значит

$$c = G(x_1, \ldots, x_m) \in B_0 x_1 + \cdots + B_0 x_m,$$

так как при раскрытии скобок каждый квадратный $x_i x_j$ член заменяется на линейную сумму $\sum b_{i,j,k} x_k$, т.е. можно запустить банальный алгоритм понижения степени и получить линейное по x_i выражение.

Таким образом C как B_0-модуль конечнопорождён (а B_0 нётеров), значит всякий B_0-подмодуль в C конечнопорождён, значит B — конечнопорождённый B_0-модуль. Поскольку $B_0 \subseteq B$, то B — конечнопорождённая B_0-алгебра. Следовательно, B — конечнопорождённая B_0-алгебра, а B_0 — конечнопорождённая A-алгебра, и тогда B — конечнопорождённая A-алгебра. □

1.1 Алгебраические и чисто трансцендентные расширения полей

Определение 5. Пусть есть поле F, содержащееся в поле E. Элемент $x \in E$ называется *алгебраическим над F*, если есть $g \in F[t]$, что $g(x) = 0 \in E$. Иначе x называется *трансцендентным над F*.

Лемма 11. *Если x алгебраический над F, то рассмотрим F-подалгебру $F[x]$ в E, порождённую x, т.е. есть гомоморфизм алгебр $\varphi : F[t] \to E$, порождённый соотношением $\varphi(t) = x$, определяет алгебру $\varphi(F[t])$. Тогда существует неприводимый многочлен $f \in F[t]$, что $f(x) = 0$ и $F[x] = \varphi(F[t]) = F[t]/(f)$.*

Доказательство. φ — гомоморфизм алгебр, а значит гомоморфизм колец, значит $\mathrm{Ker}(\varphi) \subseteq F[t]$ непуст (из-за алгебраичности x) и является идеалом. Но всякий идеал в $F[t]$ является главным, следовательно $\mathrm{Ker}(\varphi) = (f(t))$ для некоторого $f \in F[t]$. При этом, так как E поле, $\mathrm{Ker}(\varphi)$ — простой идеал, т.е. $f(t)$ неприводим. Отсюда получаем искомое. □

Следствие 11.1. *Уже $F[x]$ является подполем в E.*

Следствие 11.2. $\dim_F F[x] = \deg f(t) < \infty$.

Следствие 11.3. *$F[x]$ порождается как векторное пространство над F элементами (базисом) $1, x, \ldots, x^d$ для некоторого $d \in \mathbb{N}$.*

Определение 6. Пусть $K \subseteq L$ — поля. Если $y_1, ..., y_m \in L$ алгебраичны над K и

$$K \subseteq K[y_1] \subseteq K[y_1][y_2] \subseteq \cdots \subseteq K[y_1] \ldots [y_m] = L,$$

то L называется *конечнопорождённым алгебраически порождённым алгебраическим расширением поля K*.

Лемма 12. *Если даны поля $K \subseteq L$, что L — конечнопорождённое алгебраическое расширение K, то $\dim_K L < \infty$.*

Доказательство. Если $m = 1$, то утверждение превращается в следствие 11.2.

По следствию 11.3 $1, \ldots, y_2^{d_2}$ порождают $K[y_1][y_2]$ как векторное пространство над $K[y_1]$. При этом $K[y_1]$ порождается $1, \ldots, y_1^{d_1}$ как векторное пространство над K. Следовательно, все элементы вида $y_1^{\alpha_1} y_2^{\alpha_2}$, $\alpha_1 \in \{0; \ldots; d_1\}$, $\alpha_2 \in \{0; \ldots; d_2\}$, порождают $K[y_1][y_2]$ как векторное пространство над K. Следовательно

$$\dim_K K[y_1][y_2] = \dim_K K[y_1] \cdot \dim_{K[y_1]} K[y_1][y_2] < \infty.$$

□

Упражнение 1. Верно и обратное: если $\dim_K L < \infty$, то L — конечнопорождённое алгебраическое расширение поля K.

Определение 7. Пусть даны поля $F \subseteq E$ и $x \in E$, трансцендентный в F. Тогда

$$F(x) := \{\frac{f(x)}{g(x)} \mid f, g \in F[t], g(t) \neq 0\}.$$

Лемма 13. *1. $F(x)$ корректно определено.*

2. $F(x)$ — поле.

Доказательство.

1. Если $g(x) = 0$, то x алгебраично. Значит $f(x)/g(x)$ определено.

2. Операции наследуются от поля. Несложно видеть, что $F(x)$ относительно них замкнуто.

□

Лемма 14. *$F(x) \cong F(t)$ как поля, где $F(t)$ — поле рациональных функций.*

Доказательство. Построим понятный гомоморфизм полей

$$\varphi : F(t) \to F(x), f/g \mapsto f(x)/g(x).$$

По построению φ сюръективен. $\operatorname{Ker}(\varphi)$ — идеал в поле, т.е. либо (0), либо всё $F(t)$. Но φ сохраняет F, значит $\operatorname{Ker}(\varphi) = 0$, т.е. φ инъективен. Итого φ — изоморфизм. □

Лемма 15. *Пусть x трансцендентно. Тогда 1, x, x^2, ... линейно независимы.*

Доказательство. В противном случае это означает, что есть некоторое $n \in \mathbb{N}$ и $a_0, \ldots, a_n \in F$, что

$$\sum_{k=0}^{n} a_k x^k = 0.$$

Тогда $f(x) = 0$, где

$$f(t) := \sum_{k=0}^{n} a_k t^k.$$

Это противоречит с трансцендентностью x. □

Лемма 16. *Пусть даны поле L и независимая переменная t. Тогда*

$$L(t) := \{\frac{f(t)}{g(t)} \mid f(t), g(t) \in L[t], g(t) \neq 0\}$$

не является конечнопорождённой L-алгеброй.

Доказательство. Предположим противное. Пусть $L(t) = L[y_1, \dots, y_s]$ — конечнопорождённая L-алгебра, где $y_i = \frac{f_i(t)}{g_i(t)}$. Тогда есть гомоморфизм

$$\varphi : L[T_1, \dots, T_s] \to L(t), T_i \mapsto y_i.$$

Понятно, что

$$L[y_1, \dots, y_s] = \varphi(L[T_1, \dots, T_s]).$$

Тогда рассмотрим $h(t)$ — неприводимый делитель значения

$$1 - \prod_{i=1}^{s} q_i(t).$$

Поскольку $L = L[y_1, \dots, y_s]$, то $1/h(t) \in L[y_1, \dots, y_s]$, то есть $G(T_1, \dots, T_s) \in L[T_1, \dots, T_s]$, что $G(y_1, \dots, y_s) = \frac{1}{h(t)}$. Понятно, что есть некоторое $N \in \mathbb{N}$, что

$$G(y_1, \dots, y_s) = \frac{F(t)}{(\prod q_i(t))^N}.$$

Тогда

$$\left(\prod q_i(t)\right)^N = h(t)F(t).$$

Вспомним, что

$$\prod g_i(t) - 1 = h(t) \cdot h_1(t) \quad \Longrightarrow \quad \prod g_i(t) \equiv 1 \pmod{h(t)} \quad \Longrightarrow \quad \left(\prod g_i(t)\right)^N \equiv 1 \pmod{h(t)},$$
$$\left(\prod g_i(t)\right)^N = h(t)F(t) \quad \Longrightarrow \quad \left(\prod g_i(t)\right)^N \equiv 0 \pmod{h(t)},$$

т.е. $0 \equiv 1 \pmod{h(t)}$. □

Лемма 17. *Пусть $F \subseteq E$ — поля, и $E = F[x_1, \dots, x_n]$ конечнопорождёно как F-алгебра. Тогда $[x_1, \dots, x_n]$ алгебраичны над F и $\dim_F E < \infty$.*

Доказательство. Среди $x_1, \dots, x_n$ может оказаться элемент трансцендентный над F, WLOG x_1. Получим

$$F \subseteq F(x_1) \subseteq E.$$

Среди оставшихся может оказаться элемент, трансцендентный над $F(x_1)$, WLOG x_2. Получим

$$F \subseteq F(x_1) \subseteq F(x_1)(x_2) \subseteq E.$$

Будем повторять данную операцию до конца. Таким образом выделим $x_1, \dots, x_r$, получим

$$F \subseteq F(x_1) \subseteq F(x_1)(x_2) \subseteq \dots \subseteq \underbrace{F(x_1)\dots(x_r)}_{K} \subseteq E,$$

что все $x_{r+1}, \dots, x_n$ алгебраичны над K. Тогда E как векторное пространство над K конечномерно (лемма 12).

Тогда имеем, что
$$F \subseteq K \subseteq E,$$
где E — конечнопорождённый K-модуль и конечнопорождённая F-алгебра. Следовательно, по лемме 10 K — конечнопорождённая F-алгебра.

Пусть $r \neq 0$. Пусть $L = F(x_1)\dots(x_{r-1})$. Тогда $L(x_r) = K$, где $x_r \in K$ трансцендентен над L. Следовательно, $L(x_r) \cong L(t)$, т.е. $K = L(x_r)$ — не конечнопорожденная L-алгебра, и тем более не конечнопорождённая F-алгебра. Противоречие. □

Следствие 17.1. *Пусть $F \to A$ — конечнопорождённая F-алгебра, а $\mathcal{M}$ — максимальный идеал A. Тогда $F \hookrightarrow A/\mathcal{M}$ — конечное алгебраическое расширение поля.*

Доказательство.

Дописать?

□

Следствие 17.2. *Пусть F — алгебраически замкнутое поле, а $F \to A$ — конечнопорождённая F-алгебра. Тогда $F \to A/\mathcal{M}$ — изоморфизм.*

Доказательство. $A/\mathcal{M}$ — конечное алгебраическое расширение поля F, т.е. совпадает с F. □

Упражнение 2. Пусть R — кольцо, $I \subseteq J \subseteq R$ — два иделала в R. Тогда TFAE.

1. $I = J$.
2. $\overline{\varphi} : R/I \to R/J, r \bmod I \mapsto r \bmod J$ — изоморфизм колец.

Доказательство. Если $I = J$, то очевидно что $r \bmod I = r \bmod J$, а $R/I = R/J$, а тогда $\overline{\varphi}$, являясь тождественным отображением, является изоморфизмом колец.

Пусть $\overline{\varphi}$ — изоморфизм колец. Рассмотрим вложения $\pi_I : R \to R/I, r \mapsto r \bmod I$ и $\pi_J : R \to R/J, r \mapsto r \bmod J$. Следовательно, имеем коммутативность диаграммы

$$\begin{tikzcd} & R \arrow[dl, "p_I"'] \arrow[dr, "p_J"] & \\ R/I \arrow[rr, "\sim", "\overline{\varphi}"'] & & R/J \end{tikzcd}$$

Следовательно,
$$r \in I \quad \Leftrightarrow \quad r \in \mathrm{Ker}(p_I) \quad \Leftrightarrow \quad p_I(r) = 0 \quad \Leftrightarrow \quad p_J(r) = 0 \quad \Leftrightarrow \quad r \in \mathrm{Ker}(p_J) \quad \Leftrightarrow \quad r \in J,$$
т.е. $I = J$. □

Упражнение 3. Пусть $\mathcal{M} \subseteq R$ — идеал. Тогда TFAE.

1. $\mathcal{M}$ максимален.
2. $R/\mathcal{M}$ — поле.

Теорема 18 (Гильберта о нулях, Nullstellensatz (слабая))**.** *Пусть K — алгебраически замкнутое поле (например, $\mathbb{C}$), $\mathcal{M} \subseteq K[t_1, \dots, t_n]$ — максимальный идеал. Тогда $\mathcal{M} = (t_1 - x_1, \dots, t_n - x_n)$, где $x_i \in F$.*

Доказательство. Зафиксируем некоторые значения $x_1, \dots, x_n \in K$ и рассмотрим идеал $I := (t_1 - x_1, \dots, t_n - x_n)$. Также рассмотрим следующие гомоморфизмы:

$$in : K \to K[t_1, \dots, t_n], r \mapsto r,$$
$$\pi_{\mathcal{M}} : K[t_1, \dots, t_n] \to K[t_1, \dots, t_n]/\mathcal{M}, r \mapsto r \bmod \mathcal{M}, \qquad i_{\mathcal{M}} := \pi_{\mathcal{M}} \circ in,$$
$$\pi_I : K[t_1, \dots, t_n] \to K[t_1, \dots, t_n]/I, r \mapsto r \bmod I, \qquad i_I := \pi_I \circ in.$$

$$\begin{tikzcd}
 & & K[t_1, \dots, t_n]/\mathcal{M} \arrow[dd, dashed, "\varphi"] \\
K \arrow[r, "in"] \arrow[urr, bend left, "i_{\mathcal{M}}", "\sim"'] \arrow[drr, bend right, "i_I"', "\sim"] & K[t_1, \dots, t_n] \arrow[ur, "\pi_{\mathcal{M}}"'] \arrow[dr, "\pi_I"] & \\
 & & K[t_1, \dots, t_n]/I
\end{tikzcd}$$

Заметим, что $i_{\mathcal{M}}$ — изоморфизм колец, так как $\mathcal{M}$ максимален. При этом для всякого многочлена $F \in K[t_1, \dots, t_n]$ по теореме Безу $F(t_1, \dots, t_n) \equiv F(x_1, \dots, x_n) \pmod{I}$, а значит i_I инъективен, так как K поле, и сюръективен, так как $[F]_I = [F(x_1, \dots, x_n)]_I = i_I(F(x_1, \dots, x_n))$. Следовательно i_I тоже изоморфизм колец. Следовательно есть изоморфизм колец $\varphi = i_{\mathcal{M}}^{-1} \circ i_I$, т.е. для всякого $r \in K$

$$\varphi(r \bmod \mathcal{M}) = r \bmod I.$$

Осталось показать, что $\varphi \circ \pi_{\mathcal{M}} = \pi_I$, т.е. для всякого $F \in K[t_1, \dots, t_n]$ $\varphi : F \bmod \mathcal{M} \mapsto F \bmod I$.

На деле для случайных x_1, …, x_n это не верно. Поэтому возьмём $x_k := i_{\mathcal{M}}^{-1}(t_k \bmod \mathcal{M})$, т.е. чтобы $t_k - x_k \in \mathcal{M}$. Тогда получим, что

$$\varphi(t_k \bmod \mathcal{M}) = \varphi(x_k \bmod \mathcal{M}) = x_k \bmod I = t_k \bmod I.$$

Поскольку φ — гомоморфизм колец, а всякий многочлен представляется в виду суммы произведений элементов K и t_1, …, t_n, то теперь это верно для всех многочленов. Значит $\mathcal{M} = I$. $\square$

2 Аффинная геометрия

Замечание. Глава I. §1. Замкнутые подмножества A_k^n.

Обозначить это по-нормальному.

Определение 8. Пусть фиксировано поле k. *Аффинное пространство* над полем k размерности n — есть пространство

$$\mathbb{A}^n = \mathbb{A}_k^n := \{x = (x_1, \dots, x_n) \mid x_i \in k\} = k^n.$$

Пусть $A := k[T_1, \dots, T_n]$, $f \in A$. Тогда f — отображение $\mathbb{A}^n \to k$. Пусть фиксировано $S \subseteq A$. Тогда *множеством общих нулей многочленов из* S (также “общие нули многочленов из S” или “нули S”) — это множество

$$Z(S) := \{x \in \mathbb{A}^n \mid \forall f \in S \ f(x) = 0\}.$$

Все подмножества $Z(S)$ называются *замкнутыми подмножествами в* $\mathbb{A}^n$ или *аффинными подмножествами в* $\mathbb{A}^n$.

Пример 1.

1. $\varnothing = Z(\{a\}_{a \in k}) = Z(A)$.

2. $\mathbb{A}^n = Z(\varnothing) = Z(\{0\})$.

3. $\{(x_1, \ldots, x_n)\} = Z(\{T_1 - x_1, \ldots, T_n - x_n\})$.

4. Замкнутые подмножества в $\mathbb{A}^1$ — это $\mathbb{A}$, $\varnothing$ и любое конечное подмножество.

5. Если $n = 2$, то $Z(f)$ называется *плоской кривой*.

Лемма 19.

1. *Если $S \subseteq S'$, то $Z(S') \subseteq Z(S)$.*

2. *Пусть I — идеал, порождённый многочленами из S. Тогда $Z(I) = Z(S)$.*

3. *Для всякого S есть конечное S', что $Z(S) = Z(S')$.*

4. *Пусть есть семейство $\{S_i\}_{i \in I}$. Тогда*

$$Z\left(\bigcup_{i \in I} S_i\right) = \bigcap_{i \in I} Z(S_i).$$

5. *Пусть дано семейство идеалов $\{I_j\}_{j \in J}$. Тогда*

$$Z\left(\sum_{j \in J} I_j\right) = \bigcap_{j \in J} Z(I_j).$$

6. *Пусть дано семейство $\{S_i\}_{i=1}^n$. $S' := S_1 S_2 \ldots S_n = \{f_1 \ldots f_n \mid f_1 \in S_1 \wedge \cdots \wedge f_n \in S_n\}$. Тогда*

$$Z(S') = \bigcup_{i=1}^{n} Z(S_i).$$

7. *Пусть дано семейство идеалов $\{I_j\}_{j=1}^n$. Тогда*

$$Z\left(\bigcap_{j=1}^{n} I_j\right) = \bigcup_{j=1}^{n} Z(I_j).$$

Доказательство.

1. Действительно, для всякой точки $x \in Z(S')$ верно, что для всякого $f \in S'$ $f(x) = 0$, а значит то же верно для всякого $f \in S$ (так как $S \subseteq S'$), т.е. $x \in Z(S)$.

2. Поскольку $S \subseteq I$, то $Z(I) \subseteq Z(S)$. При этом для всякого $x \in Z(S)$ верно, что для всякого $f \in S$ $f(x) = 0$, а значит то же верно для всех $f \in I$ (так как I — идеал, порождённый S), т.е. $x \in Z(I)$. Т.е. $Z(S) \subseteq Z(I)$. Следовательно, $Z(S) = Z(I)$.

3. Если известно, что S и S' порождают одинаковые идеалы, то $Z(S) = Z(S')$. Но всякий идеал в $k[T_1, \ldots, T_n]$ конечнопорождён, а значит у идеала, порождённого S, есть конечное порождающее множество S' — искомое S'.

4. Заметим, что $x \in Z(\bigcup_{i\in I} S_i)$ тогда и только тогда, когда на x зануляются все многочлены из $\bigcup_{i\in I} S_i$, что равносильно тому, что на x зануляются все многочлены из каждого S_i, что равносильно тому, что x лежит в каждом $Z(S_i)$, что равносильно тому, что $x \in \bigcap_{i\in I} Z(S_i)$. Отсюда следует требуемое.

5. По прошлому пункту.
$$Z\left(\bigcup_{j\in J} I_j\right) = \bigcap_{j\in J} Z(I_j).$$
Но также несложно видеть, что идеал, порождённый $\bigcup_{j\in J} I_j$, есть $\sum_{j\in J} I_j$. Отсюда сиюминутно следует искомое (по ранее доказанному пункту).

6. Покажем утверждение для $n = 2$. Заметим, что если $x \in Z(S_1)$, то на x зануляются все многочлены из S_1, а значит и из $S_1 \cdot S_2$, т.е. $x \in Z(S_1S_2)$. Следовательно $Z(S_1) \subseteq Z(S_1S_2)$. Из аналогичного утверждения получаем, что $Z(S_1) \cup Z(S_2) \subseteq Z(S_1S_2)$. При этом если $x \in Z(S_1S_2) \setminus Z(S_1)$, то есть многочлен $f \in S_1$, что $f(x) \neq 0$. Но для всякого $g \in S_2$ верно $fg \in S_1S_2$, а значит $f(x)g(x) = 0$, а тогда $g(x) = 0$, т.е. $x \in Z(S_2)$. Итого $Z(S_1S_2) = Z(S_1) \cup Z(S_2)$. Утверждение для всякого n получается по индукции с помощью данного.

7. Покажем для $n = 2$; общий случай получается по индукции. Пусть даны идеалы I и J. Имеем по прошлому пункту
$$Z(I \cdot J) = Z(I) \cup Z(J).$$
При этом $I \cdot J \subseteq I \cap J$, а $I \cap J \subseteq I$, $I \cap J \subseteq J$. Следовательно $Z(I \cdot J) \supseteq Z(I \cap J)$, $Z(I \cap J) \supseteq Z(I)$, $Z(I \cap J) \supseteq Z(J)$. Итого
$$Z(I \cdot J) \supseteq Z(I \cap J) \supseteq Z(I) \cup Z(J),$$
откуда
$$Z(I \cdot J) = Z(I \cap J) = Z(I) \cup Z(J).$$

□

Следствие 19.1. *Мораль такова.*

1. *Замкнутые идеалы образуют топологию, где они являются замкнутыми. Т.е. их дополнения образуют топологию (являясь открытыми).*

2. *Каждое замкнутое подмножество имеет вид $Z(I)$, где I — идеал.*

3. *Сумма идеалов соответствует пересечению замкнутых множеств (и наоборот). Т.е. для всякого семейства идеалов $\{I_j\}_{j\in J}$ верно, что*
$$\bigcap_{j\in J} Z(I_j) = Z\left(\sum_{j\in J} I_j\right).$$

4. *Конечные пересечения идеалов соответствуют конечным объединениям замкнутых множеств. Т.е. для всякого семейства идеалов $\{I_j\}_{j=1}^n$ верно, что*
$$\bigcup_{j=1}^{n} Z(I_j) = Z\left(\bigcap_{j=1}^{n} I_j\right).$$

Определение 9. Пусть имеется множество точек $X \subseteq A^n_k$. Определим множество

$$I(X) := \{f \in A \mid \forall x \in X\ f(x) = 0\}.$$

Лемма 20.

1. *$I(X)$ — идеал.*

2. *Если $X \subseteq Y$, то $I(X) \supseteq I(Y)$.*

3. *$I(X) = I(\overline{X})$ ($\overline{X}$ — замыкание X в смысле рассмотренной топологии).*

4. *Написать леммы про пересечения и объединения $I(X)$:*

   (a) $\sum_{j \in J} I(X_j) = I(\bigcap_{j \in J} X_j)$?

   (b) $\bigcap_{j \in J} I(X_j) = I(\bigcup_{j \in J} X_j)$?

5. *Если $X \subseteq Y$, то $ZI(X) \subseteq ZI(Y)$.*

6. *Если $S \subseteq T$, то $IZ(S) \subseteq IZ(T)$.*

7. *$ZI(X) \supseteq X$.*

8. *$IZ(S) \supseteq S$.*

Доказательство.

1. Если $f, g \in I(X)$, то для всякой точки $x \in X$ верно $f(x) = g(x) = 0$, а тогда $(f+g)(x) = 0$, т.е. $f + g \in I(X)$. Если же $f \in I(X)$, $g \in A$, то для всякой точки $x \in X$ верно $f(x) = 0$, а значит $(fg)(x) = 0$, т.е. $fg \in I(X)$.

2. Если $f \in I(Y)$, то $f(Y) = 0$, значит $f(X) = 0$, тогда $f \in I(X)$.

3. Понятно, что $X \subseteq \overline{X}$, а значит $I(\overline{X}) \subseteq I(X)$. Покажем обратное. Пусть есть $x \in \overline{X} \setminus X$. Если есть какой-то многочлен $f \in A$, что f зануляется на X, но не на x, то $Y := Z(f)$ является замкнутым, $X \subseteq Y$, а $x \notin Y$. Следовательно, так как $\overline{X} \subseteq Y$, то $x \notin \overline{X}$ — противоречие. Это значит, что всякий многочлен, зануляющийся на X, зануляется на всякой точке из $\overline{X} \setminus X$, а значит на всём $\overline{X}$. Следовательно $I(X) \subseteq I(\overline{X})$.

4. $X \subseteq Y \Rightarrow I(X) \supseteq I(Y) \Rightarrow ZI(X) \subseteq ZI(Y)$.

5. $S \subseteq T \Rightarrow Z(S) \supseteq Z(T) \Rightarrow IZ(S) \subseteq IZ(T)$.

6. Поскольку $I(X)$ — множество всех многочленов, зануляющихся на X, то всё $I(X)$ зануляется на X, т.е. $ZI(X) \supseteq X$.

7. Поскольку $Z(S)$ — множество всех точек, на которых зануляется S, то S на нём зануляется, а тогда $IZ(S) \supseteq S$.

$\square$

Определение 10. Пусть I — некоторый идеал. *Радикал из иделала I* — $\sqrt{I} := \{h \in A \mid \exists N\colon\ h^N \in I\}$.

Идеал I называется *радикальным* тогда и только тогда, когда для всякого $g \in A$, что есть $m \geqslant 1$, что $g^m \in I$ верно, что $g \in I$.

Лемма 21.

1. *$\sqrt{I}$ — идеал.*

2. *$Z(\sqrt{I}) = Z(I)$.*

3. *Идеал I радикален тогда и только тогда, когда $\sqrt{I} \subseteq I$.*

4. *$\sqrt{I}$ радикален.*

5. *$I(X)$ радикален.*

Доказательство.

1. Пусть $h \in \sqrt{I}$. Тогда есть N, что $h^N \in I$. Значит для всякого $f \in A$
$$(hf)^N = h^n f^n \in IA \subseteq I.$$
Т.е. $hf \in \sqrt{I}$. Значит $hA \subseteq \sqrt{I}$.
Пусть $h_1, h_2 \in \sqrt{I}$. Тогда есть N_1 и N_2, что $h_1^{N_1}, h_2^{N_2} \in I$. Тогда
$$(h_1 + h_2)^{N_1+N_2} = \sum_{k=0}^{N_1+N_2} h_1^k h_2^{N_1+N_2-k} \binom{N_1+N_2}{N_1}.$$
При этом при $k \leqslant N_1$
$$h_2^{N_2} \in I, \qquad h_1^k h_2^{N_1-k} \binom{N_1+N_2}{N_1} \in A, \qquad \Longrightarrow \qquad h_1^k h_2^{N_1+N_2-k} \binom{N_1+N_2}{N_1} \in I;$$
аналогично для $k \geqslant N_1$.

2. Поскольку $I \subseteq \sqrt{I}$, то $Z(\sqrt{I}) \subseteq Z(I)$. При этом для всякого $x \in Z(I)$ верно, что для всякого $f \in S$ $f(x) = 0$, а значит для всякого $f \in \sqrt{I}$ есть N, что $f^N(x) = 0$, а тогда $f(x) = 0$, т.е. $x \in Z(\sqrt{I})$. Т.е. $Z(I) \subseteq Z(\sqrt{I})$. Следовательно, $Z(\sqrt{I}) = Z(I)$.

3. Определение по-другому написанное.

4. Несложно видеть, что $\sqrt{\sqrt{I}} = \sqrt{I}$ по определению радикала. Значит $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$, т.е. $\sqrt{I}$ радикален.

5. $I(X)$ — максимальный идеал, что $X \subseteq Z(I(X))$. При этом $Z(\sqrt{I(X)}) = Z(I(X))$, значит $\sqrt{I} \subseteq I$. Таким образом I максимален.

□

Лемма 22. *Если X замкнуто, то $ZI(X) = X$.*

Доказательство. Как мы уже знаем, $X \subseteq ZI(X)$; покажем обратное. Заметим, что $X = Z(S)$. Тогда $I(X) = IZ(X) \supseteq S$. Тогда $ZI(X) \subseteq Z(S) = X$. □

Теорема 23 (Гильберта о нулях, Nullstellensatz)**.** *Если I — радикальный идеал, то $IZ(I) = I$.*

Следствие 23.1. *I и Z — биекции из множества замкнутых множеств в A и обратно. При этом $Z \circ I$ и $I \circ Z$ — тождественные отображения.*

Доказательство. Как мы уже знаем, I — функция из множества замкнутых множеств в A, а Z — наоборот. При этом по следствию двух предыдущих утверждений ZI и IZ — тождественные функции из множества замкнутых функций в себя и из A в себя. Из первого следует, что I инъективно, а Z сюръективно; из второго следует, что Z инъективно, а I сюръективно. Т.е. I и Z — биекции. $\square$

Следствие 23.2.

1. $ZI(X) = \overline{X}$.
2. $IZ(I) = \sqrt{I}$.

Доказательство.

1. $ZI(X) = ZI(\overline{X}) = \overline{X}$.
2. $IZ(I) = IZ(\sqrt{I}) = \sqrt{I}$.

$\square$

Замечание 5. Точки в $\mathbb{A}^n$ находятся во взаимнооднозначном соответствии с максимальными идеалами в A — это говорит слабая теорема Гильберта о нулях. Т.е. всякой точке $x \in \mathbb{A}^n$ сопоставляется $I(x)$, а максимальному идеалу $\mathcal{M}$ сопоставляется $Z(\mathcal{M})$, которое является точкой, так как $\mathcal{M} = (T_1 - x_1, \ldots, T_n - x_n)$, а значит подходит только точка $(x_1; \ldots; x_n)$.

Определение 11. Пусть X замкнуто. Тогда $k[X] := A/I(X)$ — *кольцо регулярных функций на* X.

Лемма 24. *Пусть* X_1 *и* X_2 *замкнуты.*

1. $X := X_1 \sqcup X_2$ *замкнуто.*
2. *Отображение*

$$\varphi : k[X] \to k[X_1] \times k[X_2], F \bmod I(X) \mapsto (F \bmod I(X_1), F \bmod I(X_2))$$

задаёт изоморфизм колец.

Определение 12. Пусть X — замкнутое множество. Функция $f : X \to k$ называется *регулярной*, если есть $F \in A$, что $f = F|_X$.

Замечание 6. Множество $k[X]$ регулярных функций на X является кольцом и даже k-алгеброй.

При этом $T_i \in A = k[T_1, \ldots, T_n]$ образуют A, значит функции $t_i : X \to k, x \mapsto T_i(x)$ образуют $k[X]$. Значит получается сюръективный гомоморфизм $\varphi : A \to k[X], F \mapsto F|_X$, который на деле порождается соотношениями $T_i \mapsto t_i$.

Лемма 25. *Рассмотрим гомоморфизм* $\varphi : A \to k[X], F \to F|_X$.

1. $\operatorname{Ker}(\varphi) = I(X)$.
2. $A/I(X) \underset{\sim}{\xrightarrow{\varphi}} k[X]$.

Доказательство.

1. $\varphi(F) = 0$ iff $F|_X \equiv 0$, iff $F(X) = 0$, iff $F \in I(X)$.

2. φ, очевидно, сюръективно. Следовательно, φ индуцирует изоморфизм

$$A/I(X) = A/\mathrm{Ker}(\varphi) \to k[X].$$

$\square$

Лемма 26. *Пусть даны замкнутые множества X_1 и X_2. Тогда $X_1 \cap X_2 = \varnothing$ равносильно $I(X_1) + I(X_2) = A$.*

Доказательство. Понятно, что если $X_1 \cap X_2 = \varnothing$

$$A = I(\varnothing) = I(X_1 \cap X_2) = I(ZI(X_1) \cap ZI(X_2)) = IZ(I(X_1) + I(X_2)) = I(X_1) + I(X_2).$$

А если $A = I(X_1) + I(X_2)$, то

$$X_1 \cap X_2 = ZI(X_1) \cap ZI(X_2) = Z(I(X_1) + I(X_2)) = Z(A) = \varnothing.$$

$\square$

Теорема 27. *Пусть X_1, X_2 — замкнутые множества, $X_1 \cap X_2 = \varnothing$, а $X := X_1 \sqcup X_2$. $\psi : k[X] \to k[X_1] \times k[X_2], f \mapsto (f|_{X_1}, f|_{X_2})$ — изоморфизм колец (и даже алгебр).*

Доказательство. Понятно, что ψ определено корректно и является гомоморфизмом алгебр. Также понятно, что ψ инъективно, так как всякая функция f, зануляющаяся на X_1 и X_2, зануляется на X, т.е. ядро ψ тривиально.

Покажем, что ψ сюръективно. Пусть $(f_1, f_2) \in k[X_1] \times k[X_2]$. Тогда есть $F_1, F_2 \in A$, что $f_1 = F_1|_{X_1}$, $f_2 = F_2|_{X_2}$. Мы знаем, что $I(X_1)+I(X_2) = A$. Тогда $F_1-F_2 = H_1-H_2$, где $H_1 \in I(X_1)$, $H_2 \in I(X_2)$. Тогда $F_1 - H_1 = F_2 - H_2 =: F$. Имеем, что $F|_{X_1} = (F_1 - H_1)|_{X_1} = f_1 - 0 = f_1$; аналогично $F|_{X_2} = f_2$. $\square$

Определение 13. Кольцо R называется *редуцированным*, если для всякого $a \in R$ и всякого $m \geqslant 1$ из того, что $a^m = 0$ следует, что $a = 0$.

Замечание. $k[X]$ редуцированно.

Лемма 28. *Любая конечнопорождённая редуцируемая k-алгебра B изоморфна k-алгебра $k[X]$ регулярных функций для некоторых замкнутого подмножества $X \subseteq A$.*

Доказательство. Пусть $B = k[t_1, \dots, t_m]$, где $t_1, \dots, t_m = B$ (они порождают B над k). Рассмотрим гомоморфизм $\varphi : k[T_1, \dots, T_m] \to B, T_i \mapsto t_i$ алгебр. Понятно, что φ сюръективен. Пусть $I := \mathrm{Ker}(\varphi)$. Тогда есть изоморфизм $\overline{\varphi} : A/I \to B$. Поскольку B редуцированно, то I радикален:

$$f^m \in I \qquad \Longrightarrow \qquad \varphi(f)^m = \varphi(f^m) = 0 \qquad \Longrightarrow \qquad \varphi(f) = 0 \qquad \Longrightarrow \qquad f \in I.$$

Тогда пусть $X := Z(I)$. Следовательно $I = I(X)$, а тогда $B \cong A/I = A/I(X) = k[X]$. $\square$

Лемма 29. *Пусть R — кольцо, I — радикальный идеал в R,*

$$\pi : R \to \overline{R} := R/I, f \mapsto f \pmod I.$$

Тогда имеется взаимнооднозначное соответствие между множеством радикальных идеалов $J \supseteq I$ в R и множеством радикальных идеалов $\mathfrak{A}$ в $\overline{R}$, заданное отображениями $J \mapsto \overline{J} := J/I$ и $\mathfrak{A} \mapsto \pi^{-1}(\mathfrak{A})$.

Доказательство. Обозначим

- множество радикальных идеалов $J \supseteq I$ в R за D_R,
- множество радикальных идеалов $\mathfrak{A}$ в $\overline{R}$ за $D_{\overline{R}}$.

Тогда заданные в условии отображения $D_R \to D_{\overline{R}}$ и $D_{\overline{R}} \to D_R$ индуцируются π и π^{-1}. Но непонятна их корректность и биективность; это и обсудим.

Пусть $J \supseteq I$ — радикальный идеал в R. Тогда $\pi(J) = J/I$. При этом если $\overline{f}^m \in J/I$ в $\overline{R}$, где $\overline{f} = f \pmod I$, то $(f+I)^m \subseteq J$. При этом $f^m \in (f+I)^m \subseteq J$, т.е. $f^m \in J$, значит $f \in J$. Следовательно $f + I \subseteq J$. Тогда $\overline{f} \in J/I$. Таким образом J/I радикален в $\overline{R}$.

Пусть $\mathfrak{A}$ — радикальный идеал в $\overline{R}$. Тогда $J := \pi^{-1}(\mathfrak{A})$. Следовательно, $\mathfrak{A} = J/I$. Если $f^m \in J$, то $\overline{f}^m \in \mathfrak{A}$. Тогда $\overline{f} \in J/I$. Следовательно, $f + I \subseteq J$, т.е. $f \in J$. Следовательно J радикален.

Таким образом π и π^{-1} индуцируют корректные отображения $D_R \to D_{\overline{R}}$ и $D_{\overline{R}} \to D_R$. Таким образом осталось показать, что они образуют взаимнооднозначное соответствие.

Заметим, что π и π^{-1} образуют взаимнооднозначное соответствие между $\{f + I \mid f \in R\}$ и $\overline{R}$. Так как π переводит идеал, содержащий I, в идеал, а π^{-1} идеал в идеал, содержащий I, то π и π^{-1} образует взаимнооднозначное соответствие между идеалами $J \supseteq I$ в R и идеалами $\mathfrak{A}$ в $\overline{R}$. Значит, аналогично, они образуют взаимнооднозначное соответствие между D_R и $D_{\overline{R}}$. $\square$

Определение 14. Пусть X — замкнутое множество в $\mathbb{A}^n$. *Замкнутые подмножества в X* — это множества вида $Z' \cap X$, где Z' — замкнутое в $\mathbb{A}^n$.

Замечание. Сравнить с топологией, индуцированной на (замкнутом) подмножестве.

Замечание. Замкнутые подмножества в X — замкнутые подмножества Z в $\mathbb{A}^n$, что $Z \subseteq X$.

Следствие 29.1. *Пусть X замкнуто в $\mathbb{A}^n$. Тогда имеется взаимнооднозначное соответствие между множеством замкнутых $Z \subseteq X$ и радикальными идеалами $\overline{J}$ в $A/I(X)$, заданное отображениями $Z \mapsto \overline{I(Z)}$ и $\mathfrak{B} \mapsto Z(\pi^{-1}(\mathfrak{B}))$.*