

## §4. Порция коммутативной алгебры

Всюду в этом параграфе слово «кольцо» означает по умолчанию *коммутативное кольцо с единицей*, а гомоморфизмы колец всегда предполагаются отображающими единицу в единицу.

**4.1. Нётеровы кольца.** Любое множество элементов  $M \subset A$  коммутативного кольца  $A$  порождает в  $A$  идеал  $(M)$ , состоящий из всевозможных конечных сумм

$$g_1 f_1 + \dots + g_m f_m,$$

в которых  $g_\nu \in A$ , а  $f_\nu \in M$ . Как  $A$ -модуль, идеал  $(M)$  представляет собою  $A$ -линейную оболочку элементов множества  $M$ . Элементы  $f_1, \dots, f_m$  из какого-либо идеала  $I \subset A$  называются *образующими* этого идеала, если  $I = (f_1, \dots, f_m)$ , т. е.  $f_1, \dots, f_m$  линейно порождают  $I$  как  $A$ -модуль. Коммутативное кольцо  $A$  называется *нётеровым*, если каждый его идеал допускает конечное множество образующих. Условие нётеровости имеет несколько эквивалентных переформулировок.

ЛЕММА 4.1

Следующие свойства коммутативного кольца  $A$  попарно эквивалентны:

- (1) любое множество элементов  $M \subset A$  содержит некоторое конечное подмножество, порождающее тот же идеал, что и  $M$
- (2) любой идеал в  $A$  допускает конечное множество образующих
- (3) для любой бесконечной цепочки вложенных идеалов  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$  существует  $n \in \mathbb{N}$  такое, что  $I_\nu = I_n$  для всех  $\nu \geq n$ .

*Доказательство.* Ясно, что (1)  $\Rightarrow$  (2). Для доказательства импликации (2)  $\Rightarrow$  (3) заметим, что объединение  $I = \bigcup_\nu I_\nu$  всех идеалов возрастающей цепочки также является идеалом, и стало быть, линейно порождается над  $A$  конечным числом элементов  $f_1, \dots, f_m \in I$ . Все эти элементы содержатся в некотором идеале  $I_n$  из цепочки. Следовательно,  $I_\nu = I_n = I$  для всех  $\nu \geq n$ . Чтобы вывести (1) из (3), рассмотрим цепочку идеалов  $I_n = (f_1, \dots, f_n)$ , которая строится по индукции следующим образом: в качестве  $f_1$  возьмём произвольный элемент множества  $M$ . При  $i > 1$  и  $(M) \neq (f_1, \dots, f_{i-1})$  в качестве  $f_i$  возьмём любой элемент из  $M$ , не лежащий в  $(f_1, \dots, f_{i-1})$ . Тогда идеалы  $I_{i-1} \subsetneq I_i$  будут строго возрастать, что в силу (3) не может продолжаться бесконечно, т. е. на каком-то шагу мы придём к равенству  $(M) = (f_1, \dots, f_i)$ .  $\square$

ТЕОРЕМА 4.1 (ТЕОРЕМА ГИЛЬБЕРТА О БАЗИСЕ)

Если  $A$  нётерово, то кольцо многочленов  $A[x]$  также нётерово.

*Доказательство.* Рассмотрим произвольный идеал  $I \subset A[x]$  и обозначим через  $L_d \subset A$  множество старших коэффициентов всех многочленов степени  $\leq d$  из  $I$ , а через  $L_\infty = \bigcup_d L_d$  — множество старших коэффициентов вообще всех многочленов из  $I$ .

УПРАЖНЕНИЕ 4.1. Убедитесь, что все  $L_d$  (включая  $L_\infty$ ) являются идеалами в  $A$ .

Поскольку кольцо  $A$  нётерово, все идеалы  $L_d$  конечно порождены. Для каждого  $d$  (включая  $d = \infty$ ) обозначим через  $f_1^{(d)}, \dots, f_{m_d}^{(d)} \in A[x]$  многочлены, старшие коэффициенты которых порождают соответствующий идеал  $L_d$  в  $A$ . Пусть наибольшая из степеней многочленов  $f_i^{(\infty)}$ , старшие коэффициенты которых порождают идеал  $L_\infty \subset A$ , равна  $D \in \mathbb{N}$ . Покажем, что идеал  $I$  порождается многочленами  $f_i^\infty$  и многочленами  $f_j^{(d)}$  с  $0 \leq d < D$ .

Произвольный многочлен  $g \in I$  сравним по модулю многочленов  $f_1^{(\infty)}, \dots, f_{m_\infty}^{(\infty)}$  с многочленом, степень которого строго меньше  $D$ . В самом деле, поскольку старший коэффициент многочлена  $g$  лежит в идеале  $L_\infty$ , он имеет вид  $\sum \lambda_i a_i$ , где  $\lambda_i \in A$ , а  $a_i$  — старшие коэффициенты многочленов  $f_i^{(\infty)}$ . При  $\deg g \geq D$  все разности  $m_i = \deg g - \deg f_i^{(\infty)}$  неотрицательны, и мы можем образовать многочлен  $h = g - \sum \lambda_i f_i(x) x^{m_i}$ , сравнимый с  $g$  по модулю  $I$  и имеющий строго меньшую, чем  $g$  степень. Заменяем  $g$  на  $h$  и повторим эту процедуру, пока не получим многочлен  $h \equiv g \pmod{(f_1^{(\infty)}, \dots, f_{m_\infty}^{(\infty)})}$  степени  $\deg h < D$ . Теперь старший коэффициент многочлена  $h$  находится в идеале  $L_d$  с  $d < D$ . Тем же способом вычитая из него подходящие комбинации многочленов  $f_j^{(d)}$  с  $0 \leq d < D$ , мы сможем сокращать его старший моном, строго уменьшая степень, до тех пор, пока не получим нуль.  $\square$

Следствие 4.1

Если кольцо  $A$  нётерово, то кольцо многочленов  $A[x_1, \dots, x_n]$  тоже нётерово.

УПРАЖНЕНИЕ 4.2. Покажите, что все факторкольца нётерова кольца нётеровы.

УПРАЖНЕНИЕ 4.3. Заменяя в доказательстве теор. 4.1 старшие коэффициенты младшими, покажите, что кольцо формальных степенных рядов  $A[[t]]$  над нётеровым кольцом  $A$  тоже нётерово.

Замечание 4.1. Подкольцо нётерова кольца не обязательно является нётеровым. Например, кольцо  $\mathbb{C}[[t]]$  нётерово по упр. 4.3, однако, его подкольцо, образованное рядами, сходящимися всюду в  $\mathbb{C}$ , нётеровым не является.

УПРАЖНЕНИЕ 4.4. Покажите, что идеалы  $I_k$ , состоящие из аналитических функций  $\mathbb{C} \rightarrow \mathbb{C}$ , обращающихся в нуль на множествах  $\mathbb{Z} \setminus \{1, \dots, k\}$ , образуют бесконечную цепочку строго увеличивающихся идеалов.

**4.2. Целые элементы.** Пусть имеется расширение колец  $A \subset B$ . Элемент  $b \in B$  называется *целым* над  $A$ , если он удовлетворяет условиям лем. 4.2.

Лемма 4.2

Следующие три свойства элемента  $b \in B$  попарно эквивалентны:

- (1)  $b^m = a_1 b^{m-1} + \dots + a_{m-1} b + a_m$  для некоторых  $m \in \mathbb{N}$  и  $a_1, \dots, a_m \in A$
- (2)  $A$ -линейная оболочка всех целых неотрицательных степеней  $b^m$  линейно порождается над  $A$  конечным числом элементов
- (3) существует такой конечно порождённый  $A$ -подмодуль  $M \subset B$ , что  $bM \subset M$  и для каждого  $b' \in B$  из  $b'M = 0$  вытекает, что  $b' = 0$ .

Доказательство. Импликации (1)  $\Rightarrow$  (2)  $\Rightarrow$  (3) очевидны. Покажем, что (3)  $\Rightarrow$  (1). Пусть элементы  $e_1, \dots, e_m$  линейно порождают  $M$  над  $A$ , и  $A$ -линейный оператор  $M \rightarrow M$ ,  $t \mapsto bt$ , умножения на  $b$  имеет в этих образующих матрицу  $Y \in \text{Mat}_{m \times m}(A)$ , т. е.

$$(be_1, be_2, \dots, be_m) = (e_1, \dots, e_m) \cdot Y. \quad (4-1)$$

Матричное тождество  $\det X \cdot E = X \cdot X^V$ , где  $X \in \text{Mat}_m(B)$  — произвольная квадратная матрица,  $X^V$  — присоединённая к ней матрица<sup>2</sup>, а  $E$  — единичная матрица того же размера, показывает,

<sup>1</sup>Последнее условие в (3) иногда называют *B-точностью* подмодуля  $M$ .

<sup>2</sup>Т. е. транспонированная к матрице алгебраических дополнений к элементам матрицы  $X$ .

что образ оператора умножения на  $\det X$  в  $B^m$  содержится в линейной оболочке столбцов матрицы  $X$ . Поэтому образ оператора умножения всех элементов модуля  $M$  на число  $\det(bE - Y) \in B$  лежит в линейной оболочке векторов  $(e_1, \dots, e_m) \cdot (bE - Y)$ , а она нулевая в силу (4-1). Тем самым,  $\det(bE - Y) \cdot M = 0$ , а значит,  $\det(bE - Y) = 0$  в силу  $B$ -точности модуля  $M$ . Так как элементы матрицы  $Y$  лежат в  $A$ , равенство  $\det(bE - Y) = 0$  имеет вид, требуемый в условии (1).  $\square$

#### ОПРЕДЕЛЕНИЕ 4.1

Множество всех элементов  $b \in B$ , целых над подкольцом  $A \subset B$ , называется *целым замыканием*  $A$  в  $B$  и обозначается  $\bar{A}_B$ . Если  $\bar{A}_B = A$ , кольцо  $A$  называется *целозамкнутым* в  $B$ . Если  $\bar{A}_B = B$ , кольцо  $B$  называется *целым расширением* кольца  $A$  или *целой  $A$ -алгеброй*.

#### ПРИМЕР 4.1 ( $\mathbb{Z}$ ЦЕЛОЗАМКНУТО В $\mathbb{Q}$ )

Если дробь  $p/q$  с взаимно простыми  $p, q \in \mathbb{Z}$  удовлетворяет приведённому уравнению

$$\frac{p^m}{q^m} = a_1 \frac{p^{m-1}}{q^{m-1}} + \dots + a_{m-1} \frac{p}{q} + a_m, \quad \text{где } a_1, \dots, a_m \in \mathbb{Z},$$

то  $p^m = a_1 q p^{m-1} + \dots + a_{m-1} q^{m-1} p + a_m q^m$  делится на  $q$ , что возможно только при  $q = \pm 1$ .

#### ПРИМЕР 4.2 (ИНВАРИАНТЫ КОНЕЧНОЙ ГРУППЫ)

Пусть конечная группа  $G$  действует на кольце  $B$  кольцевыми автоморфизмами

$$g : B \xrightarrow{\simeq} B, \quad g \in G.$$

Подкольцо  $B^G \stackrel{\text{def}}{=} \{a \in B \mid ga = a \ \forall g \in G\}$  называется *кольцом инвариантов* этого действия. Пусть  $G$ -орбита элемента  $b \in B$  состоит из элементов  $b_1, \dots, b_n$ , где  $b_1 = b$ . Тогда  $b$  является корнем приведённого многочлена  $B(t) = \prod (t - b_i) \in B^G[t]$ . Поэтому  $B$  цело над  $B^G$ .

#### ПРИМЕР 4.3 (ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ЧИСЛА)

Пусть  $\mathbb{K} \supset \mathbb{Q}$  — поле, конечномерное<sup>1</sup> как векторное пространство над  $\mathbb{Q}$ . Элементы  $z \in \mathbb{K}$  называются *алгебраическими числами*. Условие (3) из лем. 4.2 на стр. 58 утверждает, что алгебраическое число  $\zeta \in K$  цело над  $\mathbb{Z}$ , если и только если существует такое инвариантное относительно умножения на  $\zeta$  векторное подпространство  $W \subset \mathbb{K}$  над полем  $\mathbb{Q}$ , что оператор умножения на  $\zeta: W \rightarrow W, x \mapsto \zeta x$ , записывается в некотором базисе целочисленной матрицей. Именно таким образом *целые алгебраические числа* и были впервые определены в XIX веке Дедекиндом. Отметим, что каждое алгебраическое число  $\xi \in \mathbb{K}$  становится целым после умножения на подходящее число из  $\mathbb{Z}$ . В частности, у  $\mathbb{K}$  существует базис над  $\mathbb{Q}$ , состоящий из целых алгебраических чисел.

УПРАЖНЕНИЕ 4.5\*. Покажите, что целые алгебраические числа в расширении  $\mathbb{K} \supset \mathbb{Q}$  составляют свободный  $\mathbb{Z}$ -модуль ранга  $\deg \mathbb{K}/\mathbb{Q}$ .

#### ПРЕДЛОЖЕНИЕ 4.1

Целое замыкание  $\bar{A}_B \subset B$  любого подкольца  $A \subset B$  является подкольцом в  $B$ . Для любого кольца  $C \supset B$  всякий элемент  $c \in C$ , целый над  $\bar{A}_B$ , цел и над  $A$ .

<sup>1</sup>Размерность  $\mathbb{K}$  как векторного пространства над  $\mathbb{Q}$  обычно обозначается  $\deg \mathbb{K}/\mathbb{Q}$  и называется *степенью расширения*  $\mathbb{K} \supset \mathbb{Q}$ .

Доказательство. Если элементы  $p, q \in B$  таковы, что

$$p^m = x_{m-1} p^{m-1} + \dots + x_1 p + x_0, \quad q^n = y_{n-1} q^{n-1} + \dots + y_1 q + y_0$$

для некоторых  $x_\nu, y_\mu \in A$ , то  $A$ -модуль, порождённый произведениями  $p^i q^j$  с  $0 \leq i < m, 0 \leq j < n$ , является  $B$ -точным (ибо содержит 1) и переходит в себя при умножении и на  $p$ , и на  $q$ , а значит, и при умножении на  $p + q$  и  $pq$ . Аналогично, если

$$c^r = z_{r-1} c^{r-1} + \dots + z_1 c + z_0, \quad z_k^{m_k} = a_{k,m_k-1} z_k^{m_k-1} + \dots + a_{k,1} z_k + a_{k,0}$$

где  $0 \leq k \leq (r-1)$  и все  $a_{k,\ell} \in A$ , то умножение на  $c$  сохраняет  $B$ -точный  $A$ -подмодуль, порождённый произведениями  $c^i z_1^{j_1} z_2^{j_2} \dots z_r^{j_r}$  с  $0 \leq i < r$  и  $0 \leq j_k < m_k$ .  $\square$

Предложение 4.2 (лемма Гаусса–Кронекера–Дедекинда)

Пусть  $A \subset B$  — произвольное расширение коммутативных колец, и  $f, g \in B[x]$  — приведённые<sup>1</sup> многочлены положительной степени. Тогда все коэффициенты произведения  $h(x) = f(x)g(x)$  целы над  $A$ , если и только если все коэффициенты как  $f$ , так и  $g$  целы над  $A$ .

Доказательство. Рассмотрим любое кольцо  $C \supset B$ , над которым  $f$  и  $g$  полностью разлагаются на линейные множители<sup>2</sup>, т. е. в кольце  $C[x]$  выполняются равенства

$$f(x) = \prod_{\nu} (x - \alpha_{\nu}), \quad g(x) = \prod_{\mu} (x - \beta_{\mu}), \quad h(x) = \prod_{\mu, \nu} (x - \alpha_{\nu})(x - \beta_{\mu}).$$

Целость над  $A$  всех коэффициентов многочлена  $h$  равносильна тому, что все корни  $\alpha_{\nu}, \beta_{\mu} \in C$  многочлена  $h$  целы над целым замыканием  $A$  в  $C$ , а значит, и над самим  $A$ . Это, в свою очередь, эквивалентно одновременной целости над  $A$  всех коэффициентов как  $f$ , так и  $g$ .  $\square$

Предложение 4.3

Пусть кольцо  $B$  цело над подкольцом  $A \subset B$ . Если  $B$  — поле, то  $A$  также является полем. Наоборот, если  $A$  — поле, и в  $B$  нет делителей нуля, то  $B$  — поле.

Доказательство. Если  $B$  — поле, целое над  $A$ , то обратный элемент  $a^{-1} \in B$  к произвольному ненулевому  $a \in A$  удовлетворяет уравнению  $a^{-m} = \alpha_1 a^{1-m} + \dots + \alpha_{m-1} a^{-1} + \alpha_0$ , где все  $\alpha_\nu \in A$ . Умножая обе части на  $a^{m-1}$ , получаем  $a^{-1} = \alpha_1 + \dots + \alpha_{m-1} a^{m-2} + \alpha_0 a^{m-1} \in A$ .

Обратно, если  $A$  — поле, и  $B$  — целая  $A$ -алгебра, то все неотрицательные целые степени  $b^i$  любого  $b \in B$  порождают конечномерное векторное пространство  $V$  над  $A$ . Если  $b \neq 0$ , и в  $B$  нет делителей нуля, то линейный оператор умножения на  $b: V \rightarrow V, x \mapsto bx$ , имеет нулевое ядро и, тем самым, биективен. Прообраз  $1 \in V$  относительно этого оператора и есть  $b^{-1}$ .  $\square$

Следствие 4.2

Если поле  $\mathbb{F}$  является конечномерным векторным пространством над своим подполем  $\mathbb{k} \subset \mathbb{F}$ , то все элементы  $\mathbb{F}$  алгебраичны над  $\mathbb{k}$ , и  $\mathbb{k}$ -подалгебра в  $\mathbb{F}$ , порождённая любым набором элементов  $a_1, \dots, a_m \in \mathbb{F}$ , является полем.  $\square$

<sup>1</sup>Т. е. со старшим коэффициентом единица.

<sup>2</sup>Такое кольцо  $C$  можно построить индукцией по  $\deg h$ . Если  $\deg h > 0$ , то  $B$  вкладывается в фактор кольцо  $F = B[x]/(h)$  как подкольцо классов констант. Поскольку класс  $\vartheta = x \pmod{h} \in F$  является корнем  $h$ , то  $h(x) = (x - \vartheta) \cdot h_1(x)$  в  $F[x]$ . По индукции  $h_1 = \prod (x - c_\nu)$  над некоторым кольцом  $C \supset F \supset B$ .

## ОПРЕДЕЛЕНИЕ 4.2 (НОРМАЛЬНЫЕ КОЛЬЦА)

Коммутативное кольцо  $A$  без делителей нуля называется *нормальным*, если оно целозамкнуто в своём поле частных  $Q_A$ . Отметим, что любое поле нормально.

## ПРИМЕР 4.4 (НОРМАЛЬНОСТЬ ФАКТОРИАЛЬНЫХ КОЛЕЦ)

Напомним, что кольцо  $A$  называется *факториальным*, если в нём нет делителей нуля, и каждый необратимый элемент  $a \in A$  является произведением конечного числа неприводимых, причём для любых двух таких разложений  $a = p_1 \dots p_n = q_1 \dots q_m$  выполняются равенства  $m = n$  и (возможно, после надлежащей перенумерации сомножителей)  $p_i = s_i q_i$  для некоторых обратимых  $s_i \in A$ . Например, факториальными являются<sup>1</sup> все кольца главных идеалов и кольца многочленов  $K[x_1, \dots, x_n]$  над факториальными кольцами  $K$ . Каждое факториальное кольцо  $A$  нормально. Это устанавливается дословно тем же рассуждением, что и в [прим. 4.1](#) на стр. 59.

УПРАЖНЕНИЕ 4.6. Убедитесь, что приведённый многочлен  $t^m + a_1 t^{m-1} + \dots + a_m$  с коэффициентами в факториальном кольце  $A$  не может аннулировать дробь  $p/q \in Q_A$  с необратимым знаменателем  $q$  и  $\text{нод}(p, q) = 1$ .

## ПРЕДЛОЖЕНИЕ 4.4 (ЛЕММА ГАУССА)

Пусть  $A$  — нормальное кольцо с полем частных  $Q_A$ . Если многочлен  $f \in A[x]$  раскладывается в  $Q_A[x]$  в произведение приведённых множителей, то эти множители лежат в  $A[x]$ .  $\square$

Доказательство. Это вытекает прямо из определений и [предл. 4.2](#).  $\square$

## СЛЕДСТВИЕ 4.3

Пусть  $A$  — нормальное кольцо с полем частных  $Q_A$ , и  $B$  — произвольная  $Q_A$ -алгебра. Если элемент  $b \in B$  цел над  $A$ , то его минимальный многочлен<sup>2</sup>  $\mu_b$  над полем  $Q_A$  лежит в  $A[x]$ .

Доказательство. Поскольку элемент  $b$  цел над  $A$ , он является корнем приведённого многочлена  $f \in A[x]$ . Тогда  $f = \mu_b \cdot q$  в кольце  $Q_A[x]$ . По [предл. 4.4](#) все коэффициенты  $\mu_b$  лежат в  $A$ .  $\square$

**4.3. Конечно порождённые алгебры над полем.** Если кольцо  $A = \mathbb{k}$  является полем, то содержащие его кольца  $B \supset \mathbb{k}$  называются *коммутативными  $\mathbb{k}$ -алгебрами*. Факторкольца алгебры многочленов  $\mathbb{k}[x_1, \dots, x_n]$  называются *конечно порождёнными  $\mathbb{k}$ -алгебрами*. Каждая такая алгебра  $B$  является образом эпиморфизма  $\pi : \mathbb{k}[x_1, \dots, x_m] \twoheadrightarrow B$ , который называется *представлением* алгебры  $B$  образующими и соотношениями: элементы  $b_i = \pi(x_i) \in B$  называются *образующими* алгебры  $B$ , а ядро  $\ker \pi \subset \mathbb{k}[x_1, \dots, x_m]$  называется *идеалом соотношений* между ними. Отметим, что по [сл. 4.1](#) и [упр. 4.2](#) все конечно порождённые  $\mathbb{k}$ -алгебры нётеровы, и идеал соотношений между образующими конечно порождённой  $\mathbb{k}$ -алгебры всегда конечно порождён.

**4.3.1. Алгебраичность элементов.** Каждый элемент  $b$  любой  $\mathbb{k}$ -алгебры  $B$  задаёт *гомоморфизм вычисления*

$$\text{ev}_b : \mathbb{k}[x] \rightarrow B, \quad f \mapsto f(b), \quad (4-2)$$

образ которого обозначается через  $\mathbb{k}[b] \subset B$  и представляет собой наименьшую  $\mathbb{k}$ -подалгебру с единицей в  $B$ , содержащую  $b$ , т. е. всё, что можно получить из  $b$  и элементов поля  $\mathbb{k}$  конечным числом сложений и умножений.

<sup>1</sup>См. лекцию .

<sup>2</sup>Т. е. такой приведённый многочлен  $\mu_b \in Q_A[x]$  наименьшей положительной степени, что  $\mu_b(b) = 0$ .

Элемент  $b$  называется *трансцендентным* над  $\mathbb{k}$ , если гомоморфизм вычисления (4-2) инъективен. В этом случае алгебра  $\mathbb{k}[b] \simeq \mathbb{k}[x]$  не является полем и бесконечномерна как векторное пространство над  $\mathbb{k}$ .

Элемент  $b$  называется *алгебраическим* над  $\mathbb{k}$ , если гомоморфизм вычисления (4-2) имеет ненулевое ядро. В этом случае  $\ker(\text{ev}_b) = (\mu_b) \subset \mathbb{k}[x]$  является главным идеалом<sup>1</sup>, порождённым аннулирующим  $b$  приведённым многочленом  $\mu_b$  наименьшей положительной степени. Многочлен  $\mu_b \in \mathbb{k}[x]$  однозначно определяется этим свойством и называется *минимальным многочленом* элемента  $b$  над  $\mathbb{k}$ . Отметим, что алгебраичность элемента  $b \in B$  означает, что он цел над подполем  $\mathbb{k} \subset B$ . В этом случае подалгебра  $\mathbb{k}[b] \simeq \mathbb{k}[x]/(\mu_b)$  как векторное пространство над  $\mathbb{k}$  имеет конечную размерность  $\dim_{\mathbb{k}} \mathbb{k}[b] = \deg \mu_b$ , и по [предл. 4.3](#) является полем, если и только если в ней нет делителей нуля.

#### ТЕОРЕМА 4.2

Конечно порождённая  $\mathbb{k}$ -алгебра  $B$  может быть полем лишь при условии, что все её элементы алгебраичны над  $\mathbb{k}$ , и в этом случае она конечномерна как векторное пространство над  $\mathbb{k}$ .

*Доказательство.* Пусть алгебра  $B$  порождается над  $\mathbb{k}$  элементами  $b_1, \dots, b_m$  и является полем. Доказывать её алгебраичность над  $\mathbb{k}$  мы будем индукцией по  $m$ . Случай  $m = 1$ ,  $B = \mathbb{k}[b_1]$  уже был разобран выше. Пусть  $m > 1$ . Если элемент  $b_m$  алгебраичен над  $\mathbb{k}$ , то  $\mathbb{k}[b_m]$  — поле, и по предположению индукции поле  $B$  алгебраично над  $\mathbb{k}[b_m]$  и конечномерно как векторное пространство над  $\mathbb{k}[b_m]$ . По [предл. 4.1](#) поле  $B$  тогда алгебраично и над  $\mathbb{k}$ . Его конечномерность как векторного пространства над  $\mathbb{k}$  вытекает из следующего упражнения.

**УПРАЖНЕНИЕ 4.7** (мультипликативность степени конечного расширения). Пусть в расширении полей  $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$  элементы  $x_1, \dots, x_n \in \mathbb{K}$  составляют базис  $\mathbb{K}$  как векторного пространства над  $\mathbb{F}$ , а элементы  $y_1, \dots, y_m \in \mathbb{L}$  — базис  $\mathbb{L}$  как векторного пространства над  $\mathbb{K}$ . Покажите, что  $mn$  произведений  $x_i y_j$  образуют базис  $\mathbb{L}$  как векторного пространства над  $\mathbb{F}$ .

Для завершения доказательства остаётся убедиться, что элемент  $b_m$  не может быть трансцендентен над  $\mathbb{k}$ . Допустим противное. Тогда по универсальному свойству поля частных инъективный гомоморфизм вычисления  $\text{ev}_{b_m} : \mathbb{k}[x] \rightarrow B, f \mapsto f(b_m)$ , продолжается до изоморфизма поля рациональных функций  $\mathbb{k}(x)$  с наименьшим содержащим элемент  $b_m$  подполем  $\mathbb{k}(b_m) \subset B$ . По предположению индукции поле  $B$  алгебраично над  $\mathbb{k}(b_m)$ . Поэтому каждая из образующих  $b_1, \dots, b_{m-1}$  поля  $B$  как алгебры над  $\mathbb{k}$  удовлетворяет некоторому полиномиальному уравнению с коэффициентами из  $\mathbb{k}(b_m)$ . Умножая эти уравнения на подходящие многочлены от  $b_m$ , сделаем так, чтобы все их коэффициенты лежали в  $\mathbb{k}[b_m]$ , а все старшие коэффициенты стали равны друг другу. Обозначая этот общий для всех уравнений старший коэффициент через  $p(b_m) \in \mathbb{k}[b_m]$ , заключаем, что поле  $B$  цело над подалгеброй  $F = \mathbb{k}[b_m, 1/p(b_m)] \subset B$ , порождённой над  $\mathbb{k}$  элементами  $b_m$  и  $1/p(b_m)$ . По [предл. 4.3](#) подалгебра  $F$  является полем. В частности, элемент  $1 + p(b_m)$  обратим в  $F$ , т. е. существует такой многочлен  $g \in \mathbb{k}[x_1, x_2]$ , что

$$g(b_m, 1/p(b_m)) \cdot (1 + p(b_m)) = 1. \quad (4-3)$$

Записывая рациональную функцию  $g(x, 1/p(x))$  в виде  $h(x)/p^k(x)$ , где  $h \in \mathbb{k}[x]$  не делится на  $p$ , и умножая обе части (4-3) на  $p^k(b_m)$ , получаем на  $b_m$  полиномиальное уравнение

$$h(b_m) \cdot (p(b_m) + 1) = p^{k+1}(b_m).$$

<sup>1</sup>Поскольку кольцо  $\mathbb{k}[x]$  является областью главных идеалов.

Оно нетривиально, так как  $h(x)(1 + p(x))$  не делится в  $\mathbb{k}[x]$  на  $p(x)$ , и противоречит трансцендентности элемента  $b_m$ .  $\square$

**4.3.2. Базисы трансцендентности.** Пусть  $\mathbb{k}$ -алгебра  $A$  не имеет делителей нуля. Обозначим через  $Q_A$  её поле частных. С каждым набором элементов  $a_1, \dots, a_m \in A$  связан гомоморфизм вычисления

$$\text{ev}_{a_1, \dots, a_m} : \mathbb{k}[x_1, \dots, x_m] \rightarrow A, \quad f \mapsto f(a_1, \dots, a_m), \quad (4-4)$$

образ которого обозначается через  $\mathbb{k}[a_1, \dots, a_m] \subset A$  и состоит из всех элементов, что можно получить из  $a_1, \dots, a_m$  и элементов поля  $\mathbb{k}$  при помощи конечного числа сложений и умножений. Это наименьшая по включению  $\mathbb{k}$ -подалгебра в  $A$ , содержащая поле  $\mathbb{k}$  и все элементы  $a_i$ . Через  $\mathbb{k}(a_1, \dots, a_m) \subset Q_A$  мы обозначим наименьшее подполе, содержащее поле  $\mathbb{k}$  и заданные элементы  $a_1, \dots, a_m \in A$ .

УПРАЖНЕНИЕ 4.8. Покажите, что  $\mathbb{k}(a_1, \dots, a_m) \simeq Q_{\mathbb{k}[a_1, \dots, a_m]}$ .

Элементы  $a_1, \dots, a_m \in A$  называются *алгебраически независимыми* над  $\mathbb{k}$ , если между ними нет никаких полиномиальных соотношений вида  $f(a_1, \dots, a_m) = 0$ , где  $f \in A[x_1, \dots, x_m]$ , т. е. гомоморфизм вычисления (4-4) инъективен. В этом случае вложение (4-4) продолжается до изоморфизма полей  $\mathbb{k}(x_1, \dots, x_m) \simeq \mathbb{k}(a_1, \dots, a_m) \subset Q_A$ , переводящего рациональную функцию  $f(x_1, \dots, x_m)$  в её значение  $f(a_1, \dots, a_m)$  на элементах  $a_i$ .

Элементы  $a_1, \dots, a_m \in A$  называются *алгебраически порождающими*  $Q_A$ , если поле  $Q_A$  алгебраично<sup>1</sup> над подполем  $\mathbb{k}(a_1, \dots, a_m) \subset Q_A$ .

УПРАЖНЕНИЕ 4.9. Убедитесь, что если все элементы  $a \in A \subset Q_A$  алгебраичны над полем  $\mathbb{k}(a_1, \dots, a_m) \subset Q_A$ , то элементы  $a_1, \dots, a_m \in A$  алгебраически порождают  $Q_A$ .

Алгебраически независимый набор элементов  $a_1, \dots, a_m \in A$ , алгебраически порождающий  $Q_A$ , называется *базисом трансцендентности* алгебры  $A$  над  $\mathbb{k}$ . Любое собственное подмножество базиса трансцендентности алгебраически независимо, однако, не является базисом трансцендентности. Поэтому базис трансцендентности можно иначе определить либо как минимальный по включению набор  $a_1, \dots, a_m \in A$ , алгебраически порождающий  $Q_A$ , либо как максимальный по включению алгебраически независимый набор  $a_1, \dots, a_m \in A$ .

ЛЕММА 4.3 (ЛЕММА О ЗАМЕНЕ)

Если  $a_1, \dots, a_m \in A$  алгебраически порождают  $Q_A$ , а  $u_1, \dots, u_k \in A$  алгебраически независимы, то  $t \geq k$  и  $a_i$  можно перенумеровать так, что набор элементов

$$u_1, \dots, u_k, a_{k+1}, a_{k+2}, \dots, a_m$$

(полученный заменой первых  $k$  элементов  $a_i$  на элементы  $u_i$ ) также будет алгебраически порожждать  $Q_A$ .

Доказательство. Так как элемент  $u_1$  алгебраичен над  $\mathbb{k}(a_1, \dots, a_m)$ , имеется полиномиальное соотношение  $f(u_1, a_1, \dots, a_m) = 0$ , в которое входит  $u_1$ . Поскольку  $u_1$  трансцендентен над  $\mathbb{k}$ , в это соотношение входит и какой-нибудь из элементов  $a_i$ . Перенумеруем их так, чтобы это был  $a_1$ . Тогда  $a_1$  алгебраичен над  $\mathbb{k}(u_1, a_2, \dots, a_m)$ , и  $u_1, a_2, \dots, a_m$  алгебраически порождают  $Q_A$ . Далее действуем по индукции. Пусть для очередного  $i$  в пределах  $1 \leq i < k$  элементы  $u_1, \dots, u_i, a_{i+1}, \dots, a_m$  алгебраически порождают  $Q_A$ . Так как  $u_{i+1}$  алгебраичен над

$$\mathbb{k}(u_1, \dots, u_i, a_{i+1}, \dots, a_m),$$

<sup>1</sup>Или, что то же самое, цело.

имеется содержащее  $u_{i+1}$  полиномиальное соотношение  $f(u_1, \dots, u_{i+1}, a_{i+1}, \dots, a_m) = 0$ . Поскольку  $u_1, \dots, u_k$  алгебраически независимы, в этом соотношении присутствует один из элементов  $a_j$ . Тем самым,  $m > i$ , и мы можем занумеровать оставшиеся  $a_j$  так, чтобы  $a_{i+1}$  был алгебраичен над  $\mathbb{k}(u_1, \dots, u_{i+1}, a_{i+2}, \dots, a_m)$ . Следовательно  $u_1, \dots, u_{i+1}, a_{i+2}, \dots, a_m$  алгебраически порождают  $Q_A$ , что воспроизводит индуктивное предположение.  $\square$

#### Следствие 4.4

В конечно порождённой  $\mathbb{k}$ -алгебре  $A$  без делителей нуля любой алгебраически порождающий  $Q_A$  набор элементов содержит в себе некоторый базис трансцендентности для  $A$ , а любой набор алгебраически независимых элементов можно дополнить до базиса трансцендентности, причём все базисы трансцендентности состоят из одинакового числа элементов.  $\square$

#### Определение 4.3 (степень трансцендентности)

Число элементов в базисе трансцендентности конечно порождённой  $\mathbb{k}$ -алгебры  $A$  называется *степенью трансцендентности* алгебры  $A$  над  $\mathbb{k}$  и обозначается  $\text{tr deg}_{\mathbb{k}} A$

Упражнение 4.10. Покажите, что следующие условия на конечно порождённую  $\mathbb{k}$ -алгебру  $A$  без делителей нуля эквивалентны друг другу: а)  $\text{tr deg } A = 0$  б)  $A = Q_A$  в)  $A$  — поле г)  $\dim_{\mathbb{k}} A < \infty$ .

#### 4.4. Нули многочленов. Любая система полиномиальных уравнений

$$f_v(x_1, \dots, x_n) = 0, \quad f_v \in \mathbb{k}[x_1, \dots, x_n], \quad (4-5)$$

эквивалентна системе, левые части которой образуют в  $\mathbb{k}[x_1, \dots, x_n]$  идеал  $J = (f_v)$ , порождённый многочленами  $f_v$ . Эта большая система получается добавлением к уравнениям (4-5) всех уравнений, которые можно получить умножая уравнения (4-5) на произвольные полиномы и складывая их друг с другом. В силу нётеровости кольца многочленов такая большая система, в свою очередь, эквивалентна конечной системе уравнений, левые части которых порождают идеал  $J$ , причём этот конечный набор уравнений может быть выбран из уравнений первоначальной системы (4-5). Таким образом, любая (в том числе бесконечная) система полиномиальных уравнений равносильна, с одной стороны, некоторой своей конечной подсистеме, а с другой стороны, системе, левые части которой образуют в кольце многочленов идеал.

Множество  $V(J) \stackrel{\text{def}}{=} \{a \in \mathbb{A}^n \mid f(a) = 0 \quad \forall f \in J\}$  всех решений системы (4-5), левые части  $f_v$  которой пробегают идеал  $J \subset \mathbb{k}[x_1, \dots, x_n]$ , называется *аффинным алгебраическим многообразием*, задаваемым идеалом  $J$ . Отметим, что это множество может оказаться пустым: например, когда  $J = (1) = \mathbb{k}[x_1, \dots, x_n]$  содержит уравнение  $1 = 0$ .

Для произвольной фигуры  $\Phi \subset \mathbb{A}^n$  множество всех многочленов, тождественно зануляющихся на  $\Phi$ , образует в кольце многочленов идеал, который обозначается

$$I(\Phi) = \{f \in \mathbb{k}[x_1, \dots, x_n] \mid f(p) = 0 \quad \forall p \in \Phi\}.$$

Множество нулей  $V(I(\Phi))$  этого идеала — это наименьшее аффинное алгебраическое многообразие, содержащее  $\Phi$ .

Для любого идеала  $J \subset \mathbb{k}[x_1, \dots, x_n]$  имеется тавтологическое включение  $J \subset I(V(J))$ . Вообще говоря, это включение строгое. Например, при  $n = 1$  для идеала  $J = (x^2)$  многообразие  $V(J) = \{0\}$ , а идеал  $I(V(J)) = (x) \supsetneq (x^2) = J$ .

ТЕОРЕМА 4.3 (NULLSTELLENSATZ, или ТЕОРЕМА ГИЛЬБЕРТА О НУЛЯХ)

Для любого идеала  $J \subset \mathbb{k}[x_1, \dots, x_n]$  над произвольным алгебраически замкнутым полем  $\mathbb{k}$  справедливы следующие два утверждения:

- (1) *слабая теорема о нулях*:  $V(J) = \emptyset \iff 1 \in J$
- (2) *сильная теорема о нулях*:  $f \in I(V(J)) \iff f^m \in J$  для некоторого  $m \in \mathbb{N}$ .

Доказательство. Чтобы доказать первое утверждение, достаточно для каждого собственного<sup>1</sup> идеала  $J \subset \mathbb{k}[x_1, \dots, x_n]$  указать точку  $p \in \mathbb{A}^n$ , в которой зануляются все многочлены из  $J$ . Поскольку увеличение идеала  $J$  только усложняет эту задачу, мы без ограничения общности можем считать, что идеал  $J$  максимален, т. е. любой многочлен  $g \notin J$  обратим по модулю  $J$ . Действительно, если существует необратимый по модулю  $J$  многочлен  $g \notin J$ , то уравнение  $gh + f = 1$  неразрешимо относительно  $h \in \mathbb{k}[x_1, \dots, x_n]$  и  $f \in J$ , а значит, идеал  $J' = (J, g)$  не содержит 1, т. е. является строго большим, чем  $J$  собственным идеалом, и мы можем расширить  $J$  до  $J' \supsetneq J$ . В силу нётеровости кольца многочленов после конечного числа таких расширений мы получим такой собственный идеал  $J$ , что  $\mathbb{k}[x_1, \dots, x_n]/J$  является полем, что мы и будем далее предполагать.

Так как поле  $\mathbb{k}[x_1, \dots, x_n]/J \supset \mathbb{k}$  конечно порождено как  $\mathbb{k}$ -алгебра, каждый элемент  $\vartheta$  этого поля по теор. 4.2 алгебраичен над  $\mathbb{k}$ , т. е. является корнем некоторого неприводимого приведённого многочлена из  $\mathbb{k}[x]$ . Поскольку для алгебраически замкнутого поля  $\mathbb{k}$  все такие многочлены линейны,  $\vartheta \in \mathbb{k}$ . Таким образом,  $\mathbb{k}[x_1, \dots, x_n]/J \simeq \mathbb{k}$ , т. е. каждый многочлен

$$f(x_1, \dots, x_n) \in \mathbb{k}[x_1, \dots, x_n]$$

сравним по модулю идеала  $J$  с некоторой константой. Рассмотрим точку  $p = (p_1, \dots, p_n) \in \mathbb{A}^n$ , каждая координата  $p_i \in \mathbb{k}$  которой сравнима по модулю  $J$  с одночленом  $x_i$ . Тогда произвольный многочлен  $f(x_1, \dots, x_n)$  будет сравним по модулю  $J$  с константой  $f(p) \in \mathbb{k}$ . Тем самым,  $f(p) = 0$  для всех  $f \in J$ , что и требовалось.

Докажем теперь второе утверждение. Поскольку при  $J = \mathbb{k}[x_1, \dots, x_n]$  и  $V(J) = \emptyset$  оно тривиально, мы будем считать, что  $V(J) \neq \emptyset$  и  $J \neq (1)$ . Вложим  $\mathbb{A}^n$  в большее пространство  $\mathbb{A}^{n+1}$  с координатами  $(t, x_1, \dots, x_n)$  в качестве гиперплоскости  $t = 0$ . Если многочлен

$$f \in \mathbb{k}[x_1, \dots, x_n] \subset \mathbb{k}[t, x_1, \dots, x_n]$$

тождественно обращается в нуль на  $V(J)$ , то идеал  $J' \subset \mathbb{k}[t, x_1, \dots, x_n]$ , порождённый  $J$  и многочленом  $g(t, x) = 1 - tf(x)$ , имеет пустое множество нулей в  $\mathbb{A}^{n+1}$ , поскольку  $g(x, t) \equiv 1$  вдоль цилиндра  $V(J) \subset \mathbb{A}^{n+1}$ . Тем самым, по слабой теореме о нулях, идеал  $J'$  содержит единицу, т. е. существуют  $q_0, q_1, \dots, q_s \in \mathbb{k}[t, x_1, \dots, x_n]$  и  $f_1, \dots, f_s \in J$ , такие что

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

Применим к этому равенству гомоморфизм  $\mathbb{k}[t, x_1, \dots, x_n] \rightarrow \mathbb{k}(x_1, \dots, x_n)$ , заданный правилами  $t \mapsto 1/f(x)$ ,  $x_v \mapsto x_v$ . Получим равенство

$$q_1(1/f(x), x) \cdot f_1(x) + \dots + q_s(1/f(x), x) \cdot f_s(x) = 1$$

<sup>1</sup>Т. е. отличного от всего кольца многочленов





В самом деле, линейное отображение (4-8) для векторного пространства  $V^*$  с базисом  $t_0, t_1$  переводит пару однородных многочленов  $(h_1, h_2)$  в  $Ah_1 + Bh_2$ . При  $d = m + n - 1$  оно имеет вид  $\mu_{m+n-1} : S^{m-1}V^* \oplus S^{n-1}V^* \rightarrow S^{m+n-1}V^*$  и в стандартных базисах из мономов задаётся квадратной матрицей, транспонированной к матрице Сильвестра (4-9).

УПРАЖНЕНИЕ 4.11. Убедитесь в этом.

Если точка  $(\alpha, \beta)$  лежит на квадрике  $\alpha'_i \beta''_j - \alpha''_i \beta'_j = 0$ , то с точностью до постоянного множителя  $(\alpha''_i t_0 - \alpha'_i t_1) = (\beta''_i t_0 - \beta'_i t_1)$ . Так как эта линейная форма делит все многочлены вида  $Ah_1 + Bh_2$ , образ  $\text{im } \mu_{m+n-1} \neq S^{m+n-1}V^*$ . Поэтому определитель Сильвестра (4-8) зануляется на каждой квадрике  $\alpha'_i \beta''_j - \alpha''_i \beta'_j = 0$ . По теореме о нулях, некоторая степень многочлена  $R_{A,B}$  делится на произведение уравнений квадрик. В силу неприводимости этих уравнений и факториальности кольца многочленов такое возможно только когда  $R_{A,B}$  делится на произведение уравнений квадрик. Сравнение степеней и коэффициента при старшем мономе показывает, что частное равно 1.

УПРАЖНЕНИЕ 4.12. Убедитесь в этом.

Таким образом, для пары бинарных форм результатное многообразие задаётся одним уравнением<sup>1</sup>  $R_{AB} = 0$  на коэффициенты многочленов  $A, B$ . Многочлен  $R_{A,B}$  называется *результантом* форм  $A$  и  $B$ . Если положить  $t_0 = 1, t_1 = x$ , мы получим результат двух неоднородных многочленов  $A(x)$  и  $B(x)$ . В предположении, что  $a_0 b_0 \neq 0$ , такой результат обращается в нуль если и только если неоднородные многочлены  $A$  и  $B$  имеют общий корень в  $\mathbb{A}^1 = \mathbb{P}_1 \setminus \{(0 : 1)\}$ .

<sup>1</sup>В прим. 6.9 на стр. 99 ниже мы обобщим этот результат на случай произвольной системы однородных полиномиальных уравнений, в которой число уравнений равно числу неизвестных.

### Ответы и указания к некоторым упражнениям

- Упр. 4.1. Если  $a$  и  $b$  являются старшими коэффициентами многочленов  $f(x)$  и  $g(x)$  из идеала  $I$ , причём  $\deg f = m$  и  $\deg g = n$ , где  $m \geq n$ , то  $a + b$  либо равно нулю, либо является старшим коэффициентом многочлена  $f(x) + x^{m-n} \cdot g(x) \in I$  степени  $m$ . Аналогично, для любого  $\alpha \in A$  произведение  $\alpha a$  является старшим коэффициентом многочлена  $\alpha f(x) \in I$  степени  $m$ .
- Упр. 4.2. Пусть  $\pi : A \rightarrow B$  — гомоморфизм факторизации. Полный прообраз  $\pi^{-1}(I)$  любого идеала  $I \subset B$  является конечно порождённым идеалом в  $A$ . Образы его образующих в  $B$  просят идеал  $I$ .
- Упр. 4.8. В силу универсального свойства поля частных, любой ненулевой гомоморфизм алгебры  $A$  без делителей нуля в любое поле однозначно продолжается до вложения в это поле поля частных алгебры  $A$ .
- Упр. 4.9. По предл. 4.3 целое замыкание  $\mathbb{k}(a_1, \dots, a_m)$  в  $Q_A$  является полем. Если оно содержит  $A$ , то содержит и  $Q_A$ .