§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

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

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 $f_1, \ldots, f_m$ из какого-либо идеала $I \subset A$ называются *образующими* этого идеала, если $I = (f_1, \ldots, f_m)$, т. е. $f_1, \ldots, f_m$ 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 $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ существует $n \in \mathbb{N}$ такое, что $I_\nu = I_n$ для всех $\nu \geqslant n$.

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 $f_1, \ldots, f_m \in I$. Все эти элементы содержатся в некотором идеале I_n из цепочки. Следовательно, $I_\nu = I_n = I$ для всех $\nu \geqslant n$. Чтобы вывести (1) из (3), рассмотрим цепочку идеалов $I_n = (f_1, \ldots, f_n)$, которая строится по индукции следующим образом: в качестве f_1 возьмём произвольный элемент множества M. При $i > 1$ и $(M) \neq (f_1, \ldots, f_{i-1})$ в качестве f_i возьмём любой элемент из M, не лежащий в $(f_1, \ldots, f_{i-1})$. 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 $(M) = (f_1, \ldots, f_i)$. □

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 $\leqslant d$ 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_∞) являются идеалами в A.

Поскольку кольцо A нётерово, все идеалы L_d конечно порождены. Для каждого d (включая $d = \infty$) обозначим через $f_1^{(d)}, \ldots, f_{m_d}^{(d)} \in A[x]$ 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^∞ и многочленами $f_j^{(d)}$ с $0 \leqslant d < D$.

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_∞, он имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in A$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. При $\deg g \geqslant D$ все разности $m_i = \deg g - \deg f_i^{(\infty)}$ неотрицательны, и мы можем образовать многочлен $h = g - \sum \lambda_i \cdot f_i(x) \cdot x_i^{m_i}$, сравнимый с g по модулю I и имеющий строго меньшую, чем g степень. Заменим 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 $0 \leqslant d < D$, мы сможем сокращать его старший моном, строго уменьшая степень, до тех пор, пока не получим нуль. □

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 $\mathbb{C} \to \mathbb{C}$, обращающихся в нуль на множествах $\mathbb{Z} \smallsetminus \{1, \dots, k\}$, 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[1] $b' = 0$.

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

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

Матричное тождество $\det X \cdot E = X \cdot X^\vee$, где $X \in \mathrm{Mat}_m(B)$ — произвольная квадратная матрица, $X^\vee$ — присоединённая к ней матрица[2], а E — единичная матрица того же размера, показывает,

[1] Последнее условие в (3) иногда называют *B-точностью* подмодуля M.

[2] 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). □

Определение 4.1
Множество всех элементов $b \in B$, целых над подкольцом $A \subset B$, называется *целым замыканием* A в B и обозначается $\overline{A}_B$. Если $\overline{A}_B = A$, кольцо A называется *целозамкнутым* в B. Если $\overline{A}_B = B$, 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

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

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

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

Подкольцо $B^G \overset{\text{def}}{=} \{a \in B \mid ga = a \ \ \forall g \in G\ \}$ 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[1] 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 ζ векторное подпространство $W \subset \mathbb{K}$ над полем $\mathbb{Q}$, что оператор умножения на ζ: $W \to W$, $x \mapsto \zeta x$, 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 $\overline{A}_B \subset B$ любого подкольца $A \subset B$ является подкольцом в B. Для любого кольца $C \supset B$ всякий элемент $c \in C$, целый над $\overline{A}_B$, цел и над A.

[1] 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

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

для некоторых $x_\nu, y_\mu \in A$, то A-модуль, порождённый произведениями $p^i q^j$ с $0 \leqslant i < m$, $0 \leqslant j < n$, 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

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

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

Предложение 4.2 (лемма Гаусса – Кронекера – Дедекинда)
Пусть $A \subset B$ — произвольное расширение коммутативных колец, и $f, g \in B[x]$ — приведённые[1] 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[2], 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. □

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 $a^{-m} = \alpha_1\, a^{1-m} + \cdots + \alpha_{m-1}\, a^{-1} + \alpha_0$, где все $\alpha_\nu \in A$. Умножая обе части на a^{m-1}, получаем $a^{-1} = \alpha_1 + \cdots + \alpha_{m-1}\, a^{m-2} + \alpha_0\, a^{m-1} \in A$.

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 $b : V \to V$, $x \mapsto bx$, имеет нулевое ядро и, тем самым, биективен. Прообраз $1 \in V$ относительно этого оператора и есть b^{-1}. □

Следствие 4.2
Если поле $\mathbb{F}$ является конечномерным векторным пространством над своим подполем $\Bbbk \subset \mathbb{F}$, то все элементы $\mathbb{F}$ алгебраичны над $\Bbbk$, и $\Bbbk$-подалгебра в $\mathbb{F}$, порождённая любым набором элементов $a_1, \ldots, a_m \in \mathbb{F}$, является полем. □

[1] Т. е. со старшим коэффициентом единица.

[2] 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)
Напомню, 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[1] 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 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 $A[x]$. □

Доказательство. Это вытекает прямо из определений и предл. 4.2. □

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[2] μ_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 μ_b лежат в A. □

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

4.3.1. Алгебраичность элементов. Каждый элемент b любой $\Bbbk$-алгебры B задаёт *гомоморфизм вычисления*

$$\mathrm{ev}_b : \Bbbk[x] \to B, \quad f \mapsto f(b), \tag{4-2}$$

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

[1] См. лекцию .

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

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

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

Теорема 4.2
Конечно порождённая $\Bbbk$-алгебра B может быть полем лишь при условии, что все её элементы алгебраичны над $\Bbbk$, и в этом случае она конечномерна как векторное пространство над $\Bbbk$.

Доказательство. Пусть алгебра B порождается над $\Bbbk$ элементами $b_1, \dots, b_m$ и является полем. Доказывать её алгебраичность над $\Bbbk$ мы будем индукцией по m. Случай $m = 1$, $B = \Bbbk[b_1]$ уже был разобран выше. Пусть $m > 1$. Если элемент b_m алгебраичен над $\Bbbk$, то $\Bbbk[b_m]$ — поле, и по предположению индукции поле B алгебраично над $\Bbbk[b_m]$ и конечномерно как векторное пространство над $\Bbbk[b_m]$. По предл. 4.1 поле B тогда алгебраично и над $\Bbbk$. Его конечномерность как векторного пространства над $\Bbbk$ 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 $\Bbbk$. Допустим противное. Тогда по универсальному свойству поля частных инъективный гомоморфизм вычисления $\mathrm{ev}_{b_m} : \Bbbk[x] \to B$, $f \mapsto f(b_m)$, продолжается до изоморфизма поля рациональных функций $\Bbbk(x)$ с наименьшим содержащим элемент b_m подполем $\Bbbk(b_m) \subset B$. По предположению индукции поле B алгебраично над $\Bbbk(b_m)$. Поэтому каждая из образующих $b_1, \dots, b_{m-1}$ поля B как алгебры над $\Bbbk$ удовлетворяет некоторому полиномиальному уравнению с коэффициентами из $\Bbbk(b_m)$. Умножая эти уравнения на подходящие многочлены от b_m, сделаем так, чтобы все их коэффициенты лежали в $\Bbbk[b_m]$, а все старшие коэффициенты стали равны друг другу. Обозначая этот общий для всех уравнений старший коэффициент через $p(b_m) \in \Bbbk[b_m]$, заключаем, что поле B цело над подалгеброй $F = \Bbbk[b_m, 1/p(b_m)] \subset B$, порождённой над $\Bbbk$ 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 $g \in \Bbbk[x_1, x_2]$, что

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

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

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

[1] Поскольку кольцо $\Bbbk[x]$ является областью главных идеалов.

Оно нетривиально, так как $h(x)(1+p(x))$ не делится в $\Bbbk[x]$ на $p(x)$, и противоречит трансцендентности элемента b_m. □

4.3.2. Базисы трансцендентности. Пусть $\Bbbk$-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

$$\mathrm{ev}_{a_1,\dots,a_m} : \Bbbk[x_1, \dots, x_m] \to A\,, \quad f \mapsto f(a_1, \dots, a_m)\,, \tag{4-4}$$

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

Упражнение 4.8. Покажите, что $\Bbbk(a_1, \dots, a_m) \simeq Q_{\Bbbk[a_1,\dots,a_m]}$.

Элементы $a_1, \dots, a_m \in A$ называются *алгебраически независимыми* над $\Bbbk$, 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 $\Bbbk(x_1, \dots, x_m) \xrightarrow{\sim} \Bbbk(a_1, \dots, a_m) \subset Q_A$, 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[1] над подполем $\Bbbk(a_1, \dots, a_m) \subset Q_A$.

Упражнение 4.9. Убедитесь, что если все элементы $a \in A \subset Q_A$ алгебраичны над полем $\Bbbk(a_1, \dots, a_m) \subset Q_A$, 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 $\Bbbk$. 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 $m \geqslant k$ 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 порождать Q_A.

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

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

[1] 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 $\Bbbk(u_1, \dots, u_{i+1}, a_{i+2}, \dots, a_m)$. Следовательно $u_1, \dots, u_{i+1}, a_{i+2}, \dots, a_m$ алгебраически порождают Q_A, что воспроизводит индуктивное предположение. □

Следствие 4.4
В конечно порождённой $\Bbbk$-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. □

Определение 4.3 (степень трансцендентности)
Число элементов в базисе трансцендентности конечно порождённой $\Bbbk$-алгебры A называется *степенью трансцендентности* алгебры A над $\Bbbk$ и обозначается $\operatorname{tr}\deg_{\Bbbk} A$

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

4.4. Нули многочленов. Любая система полиномиальных уравнений

$$f_\nu(x_1, \dots, x_n) = 0\,, \quad f_\nu \in \Bbbk[x_1, \dots, x_n]\,, \tag{4-5}$$

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

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

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

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

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

(1) *слабая теорема о нулях*: $V(J) = \varnothing \iff 1 \in J$

(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[1] идеала $J \subset \Bbbk[x_1, \dots, x_n]$ 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 $h \in \Bbbk[x_1, \dots, x_n]$ 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 $\Bbbk[x_1, \dots, x_n]/J$ является полем, что мы и будем далее предполагать.

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

$$f(x_1, \dots, x_n) \in \Bbbk[x_1, \dots, x_n]$$

сравним по модулю идеала J с некоторой константой. Рассмотрим точку $p = (p_1, \dots, p_n) \in \mathbb{A}^n$, каждая координата $p_i \in \Bbbk$ 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 $f(p) \in \Bbbk$. Тем самым, $f(p) = 0$ для всех $f \in J$, что и требовалось.

Докажем теперь второе утверждение. Поскольку при $J = \Bbbk[x_1, \dots, x_n]$ и $V(J) = \varnothing$ оно тривиально, мы будем считать, что $V(J) \neq \varnothing$ 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

$$f \in \Bbbk[x_1, \dots, x_n] \subset \Bbbk[t, x_1, \dots, x_n]$$

тождественно обращается в нуль на $V(J)$, то идеал $J' \subset \Bbbk[t, x_1, \dots, x_n]$, порождённый J и многочленом $g(t, x) = 1 - t\,f(x)$, 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 $q_0, q_1, \dots, q_s \in \Bbbk[t, x_1, \dots, x_n]$ и $f_1, \dots, f_s \in J$, такие что

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

Применим к этому равенству гомоморфизм $\Bbbk[t, x_1, \dots, x_n] \to \Bbbk(x_1, \dots, x_n)$, заданный правилами $t \mapsto 1/f(x)\,, \quad x_\nu \mapsto x_\nu$. Получим равенство

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

[1] Т. е. отличного от всего кольца многочленов

в поле рациональных функций $\Bbbk(x_1, \dots, x_n)$. Так как идеал J не содержит единицы, среди рациональных функций $q_\nu\big(1/f(x), x\big)$ есть функции с нетривиальными знаменателями, причём все их можно сократить умножением на некоторую степень f^m. После умножения обеих частей равенства на эту степень получаем искомое выражение $f^m(x) = \tilde{q}_1(x) \cdot f_1(x) + \dots + \tilde{q}_s(x) \cdot f_s(x)$ с $\tilde{q}_\nu \in \Bbbk[x_1, \dots, x_n]$. □

4.5. Системы результатнтов. Рассматриваемые с точностью до пропорциональности ненулевые решения системы однородных полиномиальных уравнений

$$\begin{cases} f_1(x_0, x_1, \dots, x_n) = 0 \\ f_2(x_0, x_1, \dots, x_n) = 0 \\ \quad \dots\dots\dots\dots\dots\dots \\ f_m(x_0, x_1, \dots, x_n) = 0\,, \end{cases} \tag{4-6}$$

где каждый $f_i \in \Bbbk[x_0, x_1, \dots, x_n]$ однороден степени d_i, образуют проективное многообразие — пересечение проективных гиперповерхностей $S_i = V(f_i) \subset \mathbb{P}(V)$. Проективные гиперповерхности степени d являются точками проективного пространства $\mathbb{P}(S^d V^*)$. Наборы гиперповерхностей $(S_1, \dots, S_m)$ заданных степеней $d_1, \dots, d_m$ с непустым пересечением $\bigcap_i S_i \neq \varnothing$, составляют фигуру

$$\mathcal{R}(n+1;\, d_1, \dots, d_m) \subset \mathbb{P}(S^{d_1} V^*) \times \dots \times \mathbb{P}(S^{d_m} V^*)\,, \tag{4-7}$$

которая называется *результантным множеством* системы (4-6). Например, когда число уравнений равно числу переменных и все уравнения линейны, система (4-6) превращается в систему однородных линейных уравнений $Ax = 0$ с квадратной матрицей $A = (a_{ij})$ и имеет ненулевое решение если и только если $\det(a_{ij}) = 0$. Поэтому для $m = n+1$ и $d_1 = \dots = d_{n+1} = 1$ результантное множество является проективным алгебраическим многообразием, заданным одним полиномиальным уравнением на коэффициенты $a_{i,j}$ линейных форм $f_1, \dots, f_{n+1}$.

Покажем, что результантное множество (4-7) всегда является проективным алгебраическим многообразием, т. е. задаётся конечной системой полиномиальных уравнений на коэффициенты многочленов f_i, однородных по коэффициентам каждого из многочленов и зависящих только от числа переменных и набора степеней. Для этого рассмотрим идеал

$$J = (f_1, \dots, f_m) \subset \Bbbk[x_0, x_1, \dots, x_n]\,.$$

Отсутствие у системы (4-6) ненулевых решений означает, что аффинное алгебраическое многообразие $V(J) \subset \mathbb{A}(V)$ пусто или совпадает с началом координат. В обоих случаях каждая из координатных функций x_i тождественно зануляется на $V(J)$, и по теореме Гильберта о нулях существует такое $m \in \mathbb{N}$, что $x_i^m \in J$ для все i. Наоборот, если J содержит некоторую степень каждой из переменных, то система уравнений с левыми частями из идеала J включает в себя уравнения $x_0^m = x_1^m = \dots = x_n^m = 0$, имеющие только нулевое решение. Таким образом, отсутствие ненулевых решений у системы (4-6) равносильно тому, что для некоторого m идеал J содержит все x_i^m. Последнее означает, что любой многочлен, степень которого больше $(n+1)(m-1)$, лежит в J, т. е. J содержит все $S^d V^*$ с $d \gg 0$. Пересечение $J \cap S^d V^*$ является образом линейного отображения

$$\mu_d : S^{d-d_1} V^* \oplus \dots \oplus S^{d-d_m} V^* \to S^d\,, \quad (g_1, \dots, g_m) \mapsto \sum g_\nu f_\nu\,, \tag{4-8}$$

задаваемого в стандартных базисах из мономов матрицей, ненулевые элементы которой суть коэффициенты многочленов f_ν. При $d \gg 0$ размерность левой части (4-8) ведёт себя как

$$\sum_{\nu=1}^{m} \binom{n+d-d_\nu}{n} \sim \frac{m}{n!}\, d^n$$

и становится больше, чем размерность правой части, ведущая себя как $\binom{n+d}{n} \sim \frac{1}{n!}\, d^n$. Для всех таких d неэпиморфность отображения (4-8), т. е. неравенство $J \cap S^d V^* \neq S^d V^*$, равносильно обнулению всех максимальных миноров матрицы μ_d.

Итак, наличие ненулевых решений у системы (4-6) эквивалентно обращению в нуль всех максимальных миноров матриц μ_d для всех таких d, что размерность левой части (4-8) не меньше, чем размерность правой. В силу нётеровости кольца многочленов, эта бесконечная система полиномиальных уравнений эквивалентна некоторой конечной подсистеме, называемой *системой результантов*.

Пример 4.5 (результант пары бинарных форм)
Над алгебраически замкнутым полем $\Bbbk$ каждый однородный многочлен степени d от двух переменных $A(t_0, t_1) = a_0\, t_1^d + a_1\, t_0 t_1^{d-1} + \ldots + a_{d-1}\, t_0^{d-1} t_1 + a_d\, t_0^d$ полностью раскладывается на линейные множители:

$$A(t_0, t_1) = \prod_{i=0}^{d} (\alpha_i'' t_0 - \alpha_i' t_1) = \prod_{i=0}^{d} \det \begin{pmatrix} t_0 & t_1 \\ \alpha_i' & \alpha_i'' \end{pmatrix}$$

биективно соответствующие d нулям[1] $\alpha_i = (\alpha_i' : \alpha_i'')$ многочлена A на проективной прямой $\mathbb{P}_1 = \mathbb{P}_1(\Bbbk)$. Коэффициенты многочлена A выражаются через однородные координаты его нулей по *формуле Виета* $a_k = (-1)^{d-k} \sigma_k(\alpha', \alpha'') \overset{\text{def}}{=} (-1)^{d-k} \sum_{\#I=k} \left(\prod_{i \in I} \alpha_i' \cdot \prod_{j \notin I} \alpha_j'' \right)$, где I пробегает все строго возрастающие подмножества из k индексов. В частности, a_k биоднороден бистепени $(k, d-k)$ по (α', α''). Для фиксированных степеней $m, n \in \mathbb{N}$ рассмотрим в кольце многочленов $\Bbbk[\alpha', \alpha'', \beta', \beta'']$ от четырёх наборов переменных

$$\alpha' = (\alpha_1', \ldots, \alpha_n'),\ \alpha'' = (\alpha_1'', \ldots, \alpha_n''),\ \beta' = (\beta_1', \ldots, \beta_m'),\ \beta'' = (\beta_1'', \ldots, \beta_m'')$$

произведение $R_{AB} \overset{\text{def}}{=} \prod_{i,j} \left(\alpha_i' \beta_j'' - \alpha_i'' \beta_j' \right) = \prod_{j=1}^{n} A(\beta_j) = (-1)^{mn} \prod_{i=1}^{m} B(\alpha_i)$. Оно обращается в нуль если и только если многочлены $A(t_0, t_1) = \sum_{i=0}^{n} a_i\, t_0^i t_1^{n-i}$ и $B(t_0, t_1) = \sum_{j=0}^{m} b_j\, t_0^j t_1^{m-j}$ с коэффициентами $a_i = (-1)^{n-i} \sigma_i(\alpha', \alpha'')$ и $b_j = (-1)^{m-j} \sigma_j(\beta', \beta'')$ имеют общий нуль на $\mathbb{P}_1$. Многочлен $R_{A,B}$ биоднороден бистепени (mn, mn) по (α, β) и явно выражается через коэффициенты форм A, B по *формуле Сильвестра*

$$R_{AB} = \det \underbrace{\begin{pmatrix} a_0 & a_1 & \ldots & \ldots & a_n & & & \\ & a_0 & a_1 & \ldots & \ldots & a_n & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & \ldots & \ldots & a_n \\ b_0 & b_1 & \ldots & \ldots & b_m & & & \\ & b_0 & b_1 & \ldots & \ldots & b_m & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & b_0 & b_1 & \ldots & \ldots & b_m \end{pmatrix}}_{m+n} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \end{matrix} \tag{4-9}$$

[1] Эти нули не обязательно различны.

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 $\mu_{m+n-1} : S^{m-1}V^* \oplus S^{n-1}V^* \to S^{m+n-1}V^*$ и в стандартных базисах из мономов задаётся квадратной матрицей, транспонированной к матрице Сильвестра (4-9).

Упражнение 4.11. Убедитесь в этом.

Если точка (α, β) 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 $\operatorname{im}\mu_{m+n-1} \neq S^{m+n-1}V^*$. 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 результантное многообразие задаётся одним уравнением[1] $R_{AB} = 0$ 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 результант двух неоднородных многочленов $A(x)$ и $B(x)$. В предположении, что $a_0 b_0 \neq 0$, такой результант обращается в нуль если и только если неоднородные многочлены A и B имеют общий корень в $\mathbb{A}^1 = \mathbb{P}_1 \smallsetminus \{(0 : 1)\}$.

[1] В **??** на стр. **??** 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 $m \geqslant n$, 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 αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 4.2. Пусть $\pi : A \twoheadrightarrow B$ — гомоморфизм факторизации. Полный прообраз $\pi^{-1}(I)$ любого идеала $I \subset B$ является конечно порождённым идеалом в A. Образы его образующих в B продят 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 $\Bbbk(a_1, \dots, a_m)$ в Q_A является полем. Если оно содержит A, то содержит и Q_A.