Раздел 4
Элементы коммутативной алгебры

§14. Целые расширения колец

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

14.1. Целые элементы. Рассмотрим коммутативное кольцо B и его подкольцо $A \subset B$. Элемент $b \in B$ называется *целым* над A, если он удовлетворяет условиям идущей далее лем. 14.1.

Лемма 14.1
Следующие три свойства элемента $b \in B$ попарно эквивалентны:

(1) $b^m = a_1\, b^{m-1} + \cdots + a_{m-1}\, b + a_m$ для некоторого $m \in \mathbb{N}$ и некоторых $a_1, a_2, \ldots, a_m \in A$;

(2) A-линейная оболочка всех целых неотрицательных степеней b^m (с $m \geqslant 0$) линейно порождается над A конечным числом элементов;

(3) существует конечно порожденный A-подмодуль $M \subset B$, такой что $bM \subset M$ и для каждого $b' \in B$ из $b'M = 0$ вытекает, что $b' = 0$ (это последнее условие иногда называют B-*точностью* подмодуля M)

Доказательство. Импликации (1) $\Rightarrow$ (2) $\Rightarrow$ (3) очевидны. Чтобы вывести (1) из (3), допустим, что $e_1, e_2, \ldots, e_m$ порождают M над A и что A-линейный оператор умножения на b:

$$M \xrightarrow{\;m \mapsto bm\;} M$$

представляется в этих образующих матрицей $Y \in \mathrm{Mat}_m(A)$, т. е. действует по правилу

$$(be_1, be_2, \ldots, be_m) = (e_1, e_2, \ldots, e_m) \cdot Y\,. \tag{14-1}$$

Из матричного тождества $\det X \cdot E = X \cdot X^\vee$, где X — произвольная квадратная матрица, E — единичная матрица того же размера, что и X, а $X^\vee$ — присоединённая к матрице X матрица из алгебраических дополнений к элементам матрицы X^t, вытекает, что образ оператора умножения на $\det X$ содержится в линейной оболочке столбцов матрицы X. Поэтому образ оператора умножения всех элементов модуля M на число $\det(bE - Y) \in B$ содержится в линейной оболочке векторов $(e_1, e_2, \ldots, e_m) \cdot (bE - Y)$, которая равна нулю согласно (14-1). Таким образом, $\det(bE - Y) \cdot M = 0$, откуда $\det(bE - Y) = 0$ в силу B-точности M. Так как все элементы матрицы Y лежат в A, соотношение $\det(bE - Y) = 0$ имеет вид, требуемый в условии (1). □

Определение 14.1
Множество всех $b \in B$, целых над данным подкольцом $A \subset B$, называется *целым замыканием* A в B. Если оно не содержит ничего, кроме элементов самого A, то A называется *целозамкнутым* в B. Наоборот, если все $b \in B$ целы над A, то B называется *целым расширением* кольца A или *целой A-алгеброй*.

Предложение 14.1
Целое замыкание $\overline{A} \subset B$ любого подкольца $A \subset B$ является подкольцом в B. Для любого кольца $C \supset B$ всякий элемент $c \in C$, целый над $\overline{A}$, цел и над A.

Доказательство. Если $p^m = x_{m-1}\,p^{m-1} + \cdots + x_1\,p + x_0$, $q^n = y_{n-1}\,q^{n-1} + \cdots + y_1\,q + y_0$ для $p, q \in B$, $x_\nu, y_\mu \in A$, то $A-$модуль, натянутый на $p^i q^j$ с $0 \leqslant i < m$, $0 \leqslant j < n$, является B-точным (ибо содержит 1) и переходит в себя при умножении как на $p+q$, так и на 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 $0 \leqslant j_k < m_k$. □

Следствие 14.1 (лемма Гаусса – Кронекера – Дедекинда)
Пусть $A \subset B$ — произвольное расширение коммутативных колец, и $f, g \in B[x]$ — приведённые многочлены положительной степени. Тогда все коэффициенты произведения $h(x) = f(x)g(x)$ целы над A если и только если все коэффициенты и у $f(x)$ и у $g(x)$ целы над A.

Доказательство. Если коэффициенты f и g целы над A, то коэффициенты fg тоже целы над A, так как целые элементы образуют кольцо. Чтобы показать обратное, рассмотрим какое-нибудь кольцо $C \supset B$, над которым f и g полностью разлагаются на линейные множители[1]:

$$f(x) = \prod(x - \alpha_\nu)\,, \quad g(x) = \prod(x - \beta_\mu)\,, \quad \text{для некоторых } \alpha_\nu, \beta_\mu \in C\,.$$

Если все коэффициенты $h(x) = \prod(x-\alpha_\nu)\prod(x-\beta_\mu)$ целы над A, то α_ν, β_μ целы над целым замыканием A в C, а значит и целы и над самим A. Поскольку коэффициенты f и g являются многочленами от α_ν и β_μ, они тоже целы над A. □

14.1.1. Пример: кольцо $\mathbb{Z}$ целозамкнуто в поле $\mathbb{Q} \supset \mathbb{Z}$. Действительно, если дробь p/q с взаимно простыми $p, q \in \mathbb{Z}$ такова, что

$$\frac{p^m}{q^m} = a_1\,\frac{p^{m-1}}{q^{m-1}} + \cdots + a_{m-1}\frac{p}{q} + a_m$$

с $a_i \in \mathbb{Z}$, то $p^m = a_1 q p^{m-1} + \cdots + a_{m-1} q^{m-1} p + a_m q^m$ делится на q, что при взаимно простых p и q возможно только если $q = \pm 1$.

14.1.2. Пример: целые алгебраические числа. Пусть $K \supset \mathbb{Q}$ — поле, конечномерное как векторное пространство над $\mathbb{Q}$. Элементы $z \in K$ называются *алгебраическими числами*. Условие (3) лем. 14.1 означает, что алгебраическое число z является целым над $\mathbb{Z}$ тогда и только тогда, когда существует инвариантное относительно умножения на z подпространство $W \subset K$ и некоторый базис в нём, такие что оператор умножения на z

$$z : W \xrightarrow{\;x \mapsto zx\;} W$$

записывается в этом базисе целочисленной матрицей. Именно таким образом *целые алгебраические числа* и были впервые определены в XIX веке Дедекиндом. Введённое выше понятие *целого элемента* исторически возникло как обобщение определения Дедекинда на произвольные коммутативные кольца.

Опишем, для примера, все целые числа в поле $K = \mathbb{Q}[\omega]$, где $\omega^2 + \omega + 1 = 0$. Поскольку все целые над $\mathbb{Z}$ элементы $\mathbb{Q}$ лежат в $\mathbb{Z}$, достаточно исследовать только числа $\xi \in \mathbb{Q}[\omega] \smallsetminus \mathbb{Q}$. Такое число можно записать в виде

$$\xi = \frac{p_1 + p_2\omega}{q}\,, \quad \text{где } p_1, p_2 \in \mathbb{Z},\ q \in \mathbb{N},\ p_2 \neq 0 \text{ и } \operatorname{НОД}(p_1, p_2, q) = 1\,. \tag{14-2}$$

Если существует ненулевой вектор $w \in W$, такой что $\xi \cdot w = z \cdot w$ с $z \in \mathbb{Z}$, то $\xi = z \in \mathbb{Z}$. Если же умножение на ξ записывается целочисленной матрицей в некотором базисе всего пространства

[1] такое кольцо C можно построить индукцией по $\deg h$: если $h \neq 1$, то B вкладывается в фактор кольцо $F = B[x]/(h)$ как подкольцо классов констант, и поскольку класс $\varkappa = x \pmod h \in F$ является корнем h, то $h(x) = (x - \varkappa) \cdot h_1(x)$ в $F[x]$, и либо $h_1 = 1$, либо по индукции $h_1 = \prod(x - c_\nu)$ над некоторым кольцом $C \supset F \supset B$

K, то след $\operatorname{tr}(\xi)$ и определитель $\det(\xi)$ оператора умножения на ξ лежат в $\mathbb{Z}$. Так как след и определитель линейного оператора не зависят от выбора базиса, а в базисе $1, \omega$ оператор умножения на ξ имеет матрицу

$$\begin{pmatrix} p_1/q & -p_2/q \\ p_2/q & (p_1-p_2)/q \end{pmatrix}$$

мы заключаем, что $2p_1 - p_2 = q \cdot \operatorname{tr}(\xi)$ делится на q, а $p_1^2 - p_1p_2 + p_2^2 = q^2 \cdot \det(\xi)$ делится на q^2. Но тогда разность $(2p_1 - p_2)^2 - (p_1^2 - p_1p_2 + p_2^2) = 3p_1(p_1 - p_2)$ тоже делится на q^2. Это возможно только тогда, когда каждый простой делитель α числа q делит p_1 или $p_1 - p_2$. Если α делит p_1, то в силу того, что $2p_1 - p_2$ делится на q, α будет делить также и p_2, что противоречит условию $\text{нод}(p_1, p_2, q) = 1$. Если α делит $p_1 - p_2$, то опять же, в силу того, что $2p_1 - p_2$ делится на q, α будет делить p_1, что, как мы уже видели, невозможно. Мы заключаем, что у q нет простых делителей, т. е. $q = 1$. Таким образом, целые элементы поля $\mathbb{Q}[\omega]$ исчерпываются *целыми числами Кронекера* $a + b\omega$ с $a, b \in \mathbb{Z}$.

Упражнение 14.1. Опишите все целые над $\mathbb{Z}$ числа в полях $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ и $\mathbb{Q}[i]$, где $i^2 = -1$.

Отметим, что подходящее целочисленное кратное произвольного алгебраического числа $\xi \in K \supset \mathbb{Q}$ является целым алгебраическим числом, поскольку если ξ удовлетворяет уравнению

$$a_0\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0$$

с целыми коэффициентами $a_i \in \mathbb{Z}$, то число n-тая степень числа $\zeta = a_0\xi$ будет выражаться через меньшие свои степени с целыми коэффициентами:

$$\zeta^n = a_0^n\xi^n = -a_0^n a_1\xi^{n-1} - a_0^n a_2\xi^{n-2} - \cdots - a_0^n a_n = -a_0a_1 \cdot \zeta^{n-1} - a_0^2a_2 \cdot \zeta^{n-2} - \cdots - a_0^n a_n \cdot \zeta^0 .$$

В частности, у любого конечномерного как векторное пространство над $\mathbb{Q}$ поля $K \supset \mathbb{Q}$ всегда можно выбрать базис над $\mathbb{Q}$, состоящий из целых алгебраических чисел.

14.1.3. Пример: инварианты действия конечной группы. Пусть конечная группа G действует на кольце B кольцевыми автоморфизмами $g : B \xrightarrow{\sim} B$. Подкольцо

$$B^G \stackrel{\text{def}}{=} \{a \in B \mid ga = a \ \forall\, g \in G\}$$

называется *подкольцом инвариантов* действия G на B. Если G-орбита элемента $b \in B$ состоит из элементов $b_1 = b$, b_2, b_3, $\ldots$, b_n, то элемент b является корнем приведённого многочлена

$$B(t) = \prod (t - b_i) \in B^G[t] .$$

Таким образом, B цело над подкольцом инвариантов $B^G \subset B$.

14.1.4. Пример: характер конечномерного представления конечной группы G над полем $\mathbb{C}$ является целым алгебраическим числом. В самом деле, поскольку каждый оператор $g \in G$ аннулируется многочленом $t^{|G|} - 1$, все собственные значения оператора g являются корнями этого многочлена и, стало быть, целы над $\mathbb{Z}$. Поэтому след $\operatorname{tr} g$ тоже цел над $\mathbb{Z}$.

Теорема 14.1
Размерность любого комплексного неприводимого представления конечной группы G делит индекс $[G : Z(G)]$ центра $Z(G)$ группы G.

Доказательство. Пусть представление $\varrho : \mathbb{C}[G] \longrightarrow \operatorname{End}(V)$ неприводимо. Покажем сначала, что $\dim V$ делит $|G|$. Согласно n° 14.1.1, для этого достаточно показать, что число $|G|/\dim V \in \mathbb{Q}$ является целым над $\mathbb{Z}$.

Поскольку представление ϱ неприводимо, скалярный квадрат его характера равен единице:

$$1 = (\chi_V, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \varrho(g^{-1}) \cdot \operatorname{tr} \varrho(g) . \tag{14-3}$$

Функция $g \mapsto \operatorname{tr} \varrho(g^{-1})$ постоянна на классах сопряжённых элементов. Обозначим её значение на классе $K \in \mathrm{cl}(G)$ через $\tau(K) \in \mathbb{C}$. Будучи суммой комплексных корней степени $|G|$ из единицы, $\tau(K)$ является целым над $\mathbb{Z}$ комплексным числом. Из (14-3) вытекает, что

$$\frac{|G|}{\dim V} = \frac{1}{\dim V} \sum_{g \in G} \operatorname{tr} \varrho(g^{-1}) \cdot \operatorname{tr} \varrho(g) = \sum_{K \in \mathrm{cl}G} \tau(K) \cdot \frac{1}{\dim V} \cdot \operatorname{tr} \sum_{g \in K} \varrho(g)\,. \tag{14-4}$$

Итак, достаточно проверить, что каждое из чисел

$$\frac{1}{\dim V} \cdot \operatorname{tr} \sum_{g \in K} \varrho(g) = \frac{1}{\dim V} \cdot \operatorname{tr}\, \varrho\Big(\sum_{g \in K} g\Big)$$

является целым. Элемент $g_K = \sum\limits_{g \in K} g$ лежит в конечно порождённом $\mathbb{Z}$-подмодуле центра групповой алгебры $\mathbb{C}[G]$, образованном всеми центральными элементами $m = \sum z_g g$ с $z_g \in \mathbb{Z}$. Умножение на любой такой элемент m переводит этот подмодуль в себя. В представлении ϱ каждый такой элемент m действует оператором $\varrho(m)$, перестановочным со всеми операторами из группы G. Из неприводимости представления ϱ и леммы Шура вытекает, что все операторы $\varrho(m)$ являются скалярными гомотетиями: $\varrho(m) = \lambda_m \cdot \mathrm{Id}_V$, причём коэффициенты λ_m этих гомотетий составляют конечно порождённый $\mathbb{Z}$-подмодуль в $\mathbb{C}$, а умножение на каждое из чисел λ_m переводит этот подмодуль в себя. Таким образом, все числа λ_m являются целыми над $\mathbb{Z}$. В частности, цел над $\mathbb{Z}$ и коэффициент λ гомотетии $\varrho(g_K) = \lambda \cdot \mathrm{Id}_V$. Но

$$\frac{1}{\dim V} \cdot \operatorname{tr} \sum_{g \in K} \varrho(g) = \frac{\operatorname{tr} \varrho(g_K)}{\dim V} = \frac{\operatorname{tr}\, (\lambda \cdot \mathrm{Id}_V)}{\dim V} = \lambda\,.$$

Итак, правая часть (14-4) цела над $\mathbb{Z}$, что и требовалось.

Докажем теперь утверждение теоремы. Достаточно убедиться, что все натуральные степени

$$\left(\frac{[G : Z(G)]}{\dim V}\right)^n$$

рационального числа $[G : Z(G)]/\dim V$ содержатся в конечно порождённом $\mathbb{Z}$-подмодуле

$$\mathbb{Z} \cdot \frac{1}{\dim V} \subset \mathbb{Q}\,.$$

Для этого рассмотрим представление группы $G^n = G \times G \times \cdots \times G$ в пространстве $W = V^{\otimes n}$, заданное правилом $(g_1, g_2, \ldots, g_n) : v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto \varrho(g_1)v_1 \otimes \varrho(g_2)v_2 \otimes \cdots \varrho(g_n)v_n$.

Упражнение 14.2. Убедитесь, что это представление неприводимо.

Подгруппа $C \subset G^n$, состоящая из элементов $(c_1, c_2, \ldots, c_n)$ с $c_i \in Z(G)$ и $c_1 c_2 \ldots c_n = 1$, содержится в ядре этого представления, поскольку по лемме Шура каждый центральный элемент c_i действует в неприводимом представлении ϱ умножением на некоторую константу, и в силу равенства $\varrho(c_1 c_2 \ldots c_n) = 1$ произведение этих констант равно единице. Подгруппа C лежит в центре G^n и имеет порядок $|Z(G)|^{n-1}$. Таким образом, пространство W размерности $(\dim V)^n$ является неприводимым представлением фактор группы G^n/C порядка $|G|^n/|Z(G)|^{n-1}$. По уже доказанному

$$\frac{|G|^n}{(\dim V)^n |Z(G)|^{n-1}} = |Z(G)| \cdot \left(\frac{[G : Z(G)]}{\dim V}\right)^n \in \mathbb{Z},$$

что и требовалось. □

14.2. Алгебраические элементы. Пусть теперь кольцо $A = \Bbbk$ является полем. В этой ситуации всякое кольцо $B \supset \Bbbk$ называется *коммутативной* $\Bbbk$*-алгеброй*. Коммутативная $\Bbbk$-алгебра B называется *конечно порожденной*, если она является фактор алгеброй кольца многочленов от конечного числа переменных с коэффициентами из $\Bbbk$, т. е. если имеется эпиморфизм $\Bbbk$-алгебр $\pi : \Bbbk[x_1, x_2, \ldots, x_m] \twoheadrightarrow B$. В этом случае образы переменных $b_i = \pi(x_i) \in B$ называются *образующими* алгебры B, а ядро $\ker \pi \subset \Bbbk[x_1, x_2, \ldots, x_m]$ называется *идеалом соотношений* между ними.

Любой набор элементов $b_1, b_2, \ldots, b_m$ любой $\Bbbk$-алгебры B порождает $\Bbbk$-подалгебру

$$\Bbbk[b_1, b_2, \ldots, b_m] \subset B$$

которая представляет собою образ гомоморфизма вычисления

$$\mathrm{ev}_{b_1,b_2,\ldots,b_m} \,:\, \Bbbk[x_1, x_2, \ldots, x_m] \xrightarrow{f(x_1,x_2,\ldots,x_m)\mapsto f(b_1,b_2,\ldots,b_m)} B\,, \tag{14-5}$$

и состоит из всех элементов, что можно получить из $\Bbbk$ и $b_1, b_2, \ldots, b_m$ при помощи операций сложения и умножения. Это наименьшая $\Bbbk$-подалгебра в B, содержащая $\Bbbk$ и $b_1, b_2, \ldots, b_m$.

Целость над $\Bbbk$ элемента $b \in B$ равносильна его *алгебраичности* над $\Bbbk$, т. е. тому, что b удовлетворяет какому-нибудь — необязательно приведённому — уравнению $f(b) = 0$ с ненулевым $f \in \Bbbk[x]$. Алгебраичность элемента $b \in B$ над $\Bbbk$, в свою очередь, равносильна тому, что *гомоморфизм вычисления*

$$\mathrm{ev}_b \,:\, \Bbbk[x] \xrightarrow{f(x)\mapsto f(b)} B \tag{14-6}$$

имеет ненулевое ядро. Элемент $b \in B$, не являющийся алгебраическим, называется *трансцендентным* над $\Bbbk$. В этом случае гомоморфизм вычисления (14-6) является изоморфизмом алгебры $\Bbbk[b]$ кольцом многочленов. В частности, $\Bbbk[b]$ не является полем и бесконечномерна как векторное пространство над $\Bbbk$.

Если элемент $b \in B$ алгебраичен над подполем $\Bbbk \subset B$, ядро гомоморфизма вычисления (14-6), будучи идеалом в кольце главных идеалов $\Bbbk[x]$, представляет собой ненулевой главный идеал

$$\ker(\mathrm{ev}_b) = (\mu_b)\,,$$

образующая которого $\mu_b \in \Bbbk[x]$ однозначно определяется по b как приведённый многочлен наименьшей степени, аннулирующий b. Этот многочлен называется *минимальным многочленом* элемента b над $\Bbbk$. Алгебра $\Bbbk[b] = \Bbbk[x]/(\mu_b)$ в этом случае конечномерна как векторное пространство над $\Bbbk$ и $\dim_{\Bbbk} \Bbbk[b] = \deg \mu_b$.

Предложение 14.2
Пусть элемент b из алгебры B над полем $\Bbbk$ алгебраичен и имеет минимальный многочлен $\mu_b \in \Bbbk[x]$. Тогда следующие три свойства эквивалентны друг другу:

(1) подалгебра $\Bbbk[b] = \Bbbk[x]/(\mu_b) \subset B$ является полем

(2) подалгебра $\Bbbk[b] = \Bbbk[x]/(\mu_b) \subset B$ не имеет делителей нуля

(3) минимальный многочлен $\mu_b(t) \in \Bbbk[t]$ элемента b над $\Bbbk$ неприводим в $\Bbbk[t]$

Доказательство. Импликация (1) $\Rightarrow$ (2) очевидна. Импликация (2) $\Rightarrow$ (3) доказывается от противного: если $\mu_b = f \cdot g$ с $\deg f, \deg g < \deg \mu_b$, то оба класса $[f]$, $[g]$ в кольце вычетов $\Bbbk[t]/(\mu_b)$ отличны от нуля, а их произведение $[f] \cdot [g] = [fg] = [\mu_b] = 0$, что противоречит (2). Для доказательства импликации (3) $\Rightarrow$ (1) достаточно убедиться, что всякий ненулевой вычет $[f]$ в фактор кольце $\Bbbk[t]/(\mu_b)$ обратим. Поскольку μ_b неприводим и f не делится на μ_b, многочлены μ_b и f не имеют общих неприводимых делителей, а значит, взаимно просты, т. е. существуют такие $h, q \in \Bbbk[t]$, что $h(t) \cdot \mu_b(t) + q(t) \cdot f(t) = 1$ в $\Bbbk[t]$. Но тогда $[q] \cdot [f] = 1$ в $\Bbbk[t]/(\mu_b)$. □

Предложение 14.3
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 $a^{-m} = \alpha_1 a^{1-m} + \cdots + \alpha_{m-1} a^{-1} + \alpha_0$ с $\alpha_\nu \in A$. 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 $V \xrightarrow{x \mapsto bx} V$ не имеет ядра, а потому — биективен. Прообраз $1 \in V$ относительно этого оператора и есть b^{-1}. □

Следствие 14.2
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 $a_1, a_2, \ldots, a_m \in \mathbb{F}$, является полем.

Теорема 14.2
Конечно порожденная $\Bbbk$-алгебра B может быть полем только при условии, что все её элементы алгебраичны над $\Bbbk$.

Доказательство. Пусть B имеет образующие $\{b_1, b_2, \ldots, b_m\}$ и является полем. Доказывать алгебраичность B будем индукцией по m. Случай $m = 1$, $B = \Bbbk[b]$ уже разбирался в n° 14.2: если b трансцендентен, то гомоморфизм (14-6) отождествляет B с кольцом многочленов $\Bbbk[x]$, которое не является полем.

Пусть $m > 1$. Если b_m алгебраичен над $\Bbbk$, то $\Bbbk[b_m]$ — поле и B алгебраично над $\Bbbk[b_m]$ по предположению индукции. Тогда по предл. 14.1 B алгебраично и над $\Bbbk$. Таким образом, достаточно показать, что b_m алгебраичен над $\Bbbk$.

Допустим, что b_m трансцендентен. Тогда гомоморфизм (14-6) продолжается до изоморфизма поля рациональных функций $\Bbbk(x)$ с наименьшим подполем $\Bbbk(b_m) \subset B$, содержащим b_m. По предположению индукции, B алгебраично над $\Bbbk(b_m)$, так что каждая из образующих $b_1, b_2, \ldots, b_{m-1}$ удовлетворяет некоторому полиномиальному уравнению с коэффициентами из $\Bbbk(b_m)$. Умножая эти уравнения на подходящие многочлены от b_m, мы можем добиться того, чтобы все их коэффициенты лежали в $\Bbbk[b_m]$, а также сделать все их старшие коэффициенты равными одному и тому же многочлену, который мы обозначим через $p(b_m) \in \Bbbk[b_m]$. В результате поле B оказывается целым над подалгеброй $F = \Bbbk[b_m\,,\, 1/p(b_m)] \subset B$, порожденной над $\Bbbk$ элементами b_m и $1/p(b_m)$. По лемме предл. 14.3 эта подалгебра F должна быть полем, что невозможно, поскольку, скажем, $1 + p(b_m)$ не обратим в F.

Действительно, если есть многочлен $g \in \Bbbk[x_1, x_2]$, такой что $g\,(\,b_m\,,\,1/p(b_m)\,) \cdot (1 + p(b_m)) = 1$, то, 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 предыдущего равенства на $p^k(b_m)$, мы получим на b_m полиномиальное уравнение $h(b_m) \cdot (p(b_m) + 1) = p^{k+1}(b_m)$, нетривиальное, поскольку $h(x)(1 + p(x))$ не делится в $\Bbbk[x]$ на $p(x)$. □

Следствие 14.3
Всякое поле $\mathbb{F}$, которое конечно порождено как алгебра над своим подполем $\Bbbk \subset \mathbb{F}$, конечномерно как векторное пространство над $\Bbbk$.

14.3. Нормальные кольца. Коммутативное кольцо A без делителей нуля называется *нормальным*, если оно целозамкнуто в своём поле частных Q_A. Отметим, что любое поле нормально. Дословно также, как в примере n° 14.1.1, устанавливается, что любое факториальное[1] кольцо

[1] 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 разложений

A нормально: многочлен $a_0t^m + a_1t^{m-1} + \cdots + a_{m-1}t + a_m \in A[t]$ аннулирует дробь $p/q \in Q_A$ с $\text{нод}(p,q) = 1$, только если $q|a_0$ и $p|a_m$, поэтому из $a_0 = 1$ вытекает, что $q = 1$. В частности, кольцо многочленов от любого числа переменных над факториальным кольцом нормально.

Прямо из определений и леммы Гаусса – Кронекера – Дедекинда (сл. 14.1) вытекают следующие полезные свойства, отчасти проясняющие эпитет «нормальный».

Предложение 14.4 (лемма Гаусса – 2)
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 $A[x]$. □

Лемма 14.2
Пусть $\Bbbk = Q_A$ является полем частных коммутативного кольца A без делителей нуля. Если элемент b какой-либо Q_A-алгебры B цел над A, то он алгебраичен над Q_A и все коэффициенты его минимального многочлена $\mu_b \in Q_A[x]$ целы над A.

Доказательство. Поскольку b цел над A, он удовлетворяет уравнению $f(b) = 0$, в котором $f \in A[x]$ приведён. Тем самым, $\ker \mathrm{ev}_b \neq 0$ и $f = \mu_b \cdot q$ в кольце $Q_A[x]$. По сл. 14.1 все коэффициенты μ_b целы над A. □

Следствие 14.4
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 над полем Q_A лежит в $A[x]$. □

14.4. Базисы трансцендентности. Пусть $\Bbbk$-алгебра A не имеет делителей нуля. Обозначаем через Q_A её поле частных, а через $\Bbbk(a_1, a_2, \ldots, a_m) \subset Q_A$ — наименьшее подполе, содержащее заданные элементы $a_1, a_2, \ldots, a_m \in A$.

Элементы $a_1, a_2, \ldots, a_m \in A$ называются *алгебраически независимыми* над $\Bbbk$, если между ними нет никаких полиномиальных соотношений вида $f(a_1, a_2, \ldots, a_m) = 0$ с $f \in A[x_1, x_2, \ldots, x_m]$, т. е. если отображение вычисления

$$\mathrm{ev}_{(a_1,a_2,\ldots,a_m)} : \Bbbk[x_1, x_2, \ldots, x_m] \xrightarrow{x_i \mapsto a_i} A$$

инъективно. В этом случае отображение вычисления продолжается до изоморфизма полей

$$\Bbbk(x_1, x_2, \ldots, x_m) \xrightarrow{\sim} \Bbbk(a_1, a_2, \ldots, a_m) \subset Q_A,$$

переводящего рациональную функцию $f(x_1, x_2, \ldots, x_m)$ в её значение $f(a_1, a_2, \ldots, a_m)$ на элементах a_i.

Алгебраически независимый набор элементов $a_1, a_2, \ldots, a_m \in A$ называется *базисом трансцендентности* алгебры A над $\Bbbk$, если любой $p \in A$ алгебраичен над $\Bbbk(a_1, a_2, \ldots, a_m)$. В этом случае, любой $q \in Q_A$ также алгебраичен над $\Bbbk(a_1, a_2, \ldots, a_m)$, поскольку по предл. 14.3 целое замыкание $\Bbbk(a_1, a_2, \ldots, a_m)$ в Q_A является полем, содержащим A, а значит, и Q_A.

Отметим, что любое собственное подмножество любого базиса трансцендентности алгебраически независимо, однако, не является базисом трансцендентности. Поэтому базис трансцендентности можно иначе определить как минимальный по включению набор $a_1, a_2, \ldots, a_m \in A$, такой что алгебра A алгебраична над $\Bbbk(a_1, a_2, \ldots, a_m)$, или же как максимальный по включению алгебраически независимый набор $a_1, a_2, \ldots, a_m \in A$.

$a = p_1p_2\cdots p_n = q_1q_2\cdots q_m$ в произведение неприводимых множителей $m = n$ и (после надлежащей перенумерации) $p_i = s_iq_i$ для некоторых обратимых $s_i \in A$; например, факториальными являются любое поле, любое кольцо главных идеалов (в частности, кольцо целых чисел $\mathbb{Z}$) и кольца многочленов $K[x_1, x_2, \ldots, x_n]$ над любым факториальным кольцом K

Лемма 14.3
Любой набор элементов $a_1, a_2, \ldots, a_n \in A$, такой что A алгебраична над $\Bbbk(a_1, a_2, \ldots, a_m)$, содержит в себе некоторый базис трансцендентности A над $\Bbbk$ (пустой, если алгебра A алгебраична над $\Bbbk$). В частности, любая система образующих A как $\Bbbk$-алгебры содержит в себе некоторый базис трансцендентности.

Доказательство. Если имеется полиномиальное соотношение $f(a_1, a_2, \ldots, a_m) = 0$, скажем, содержащее a_m, то мы удалим a_m. Если остающиеся $a_1, a_2, \ldots, a_{m-1}$ удовлетворяют полиномиальному соотношению, содержащему a_{m-1}, мы удалим a_{m-1} и т. д. В конечном счете мы получим либо алгебраически независимый набор элементов, скажем, $a_1, a_2, \ldots, a_r$, либо все a_i, а значит, и вся алгебра A, окажутся алгебраичны над $\Bbbk$. В первом случае все выкинутые a_i (а значит, и алгебра A) алгебраичны над $\Bbbk(a_1, a_2, \ldots, a_r)$. □

Лемма 14.4
Если A алгебраична над $\Bbbk(a_1, a_2, \ldots, a_m)$, где $a_1, a_2, \ldots, a_n \in A$, то любой алгебраически независимый набор элементов $b_1, b_2, \ldots, b_n \in A$ состоит из $n \leqslant m$ элементов и может быть дополнен до базиса трансцендентности A над $\Bbbk$ подходящими элементами из набора $a_1, a_2, \ldots, a_m$.

Доказательство. По лем. 14.3 набор $a_1, a_2, \ldots, a_m$ содержит базис трансцендентности. Будем считать, что это $a_1, a_2, \ldots, a_r$. Поскольку b_1 алгебраичен над $\Bbbk(a_1, a_2, \ldots, a_r)$, имеется полиномиальное соотношение $f(b_1, a_1, a_2, \ldots, a_r) = 0$. Так как b_1 трансцендентен, а $a_1, a_2, \ldots, a_r$ алгебраически независимы, в этом соотношении реально присутствуют как b_1, так и какие-нибудь a_i, например, a_1. Тогда a_1 алгебраичен над $\Bbbk(b_1, a_2, a_3, \ldots, a_r)$, а значит, алгебра A алгебраична над $\Bbbk(b_1, a_2, a_3, \ldots, a_r)$. Элементы $b_1, a_2, a_3, \ldots, a_r$ алгебраически независимы, поскольку $a_2, a_3, \ldots, a_r$ алгебраически независимы и b_1 не может быть алгебраичен над $\Bbbk(a_2, a_3, \ldots, a_r)$: в противном случае A была бы алгебраична над $a_2, a_3, \ldots, a_r$, и элементы $a_1, a_2, \ldots, a_r$ были бы алгебраически зависимы. Тем самым, набор $b_1, a_2, a_3, \ldots, a_r$ тоже является базисом трансцендентности для A.

Элемент b_2 алгебраичен над $\Bbbk(b_1, a_2, a_3, \ldots, a_r)$, и значит, существует полиномиальное соотношение $f(b_1, b_2, a_2, a_3, \ldots, a_r) = 0$. Так как b_2 трансцендентен, а набор b_1, b_2 и каждое собственное подмножество набора $b_1, a_2, a_3, \ldots, a_r$ алгебраически независимы, в этом соотношении реально присутствуют как b_2, так и какие-нибудь из a_i — скажем, a_2. Тогда a_2 алгебраичен над $\Bbbk(b_1, b_2, a_3, \ldots, a_r)$, а значит, алгебра A алгебраична над $\Bbbk(b_1, b_2, a_3, \ldots, a_r)$. Элементы $b_1, b_2, a_3, \ldots, a_r$ алгебраически независимы, поскольку $b_1, a_3, \ldots, a_r$ алгебраически независимы и b_2 не может быть алгебраичен над $\Bbbk(b_1, a_3, \ldots, a_r)$: в противном случае A была бы алгебраична над $b_1, a_3, \ldots, a_r$, и элементы $b_1, a_2, a_3, \ldots, a_r$ были бы алгебраически зависимы. Тем самым, набор $b_1, b_2, a_3, \ldots, a_r$ тоже является базисом трансцендентности для A.

Продолжая в том же духе (и, если необходимо, перенумеровывая по ходу дела элементы a_i), мы по индукции получим для каждого $i \leqslant n$ базис трансцендентности $b_1, \ldots, b_i, a_{i+1}, \ldots, a_r$ алгебры A над $\Bbbk$. Отсюда получаются неравенства $n \leqslant r \leqslant m$, и при $i = n$ мы приходим к искомому базису трансцендентности вида $b_1, \ldots, b_n, a_{n+1}, \ldots, a_r$. □

Следствие 14.5
Все базисы трансцендентности конечно порождённой коммутативной алгебры A над полем $\Bbbk$ состоят из одинакового числа элементов (это число называется *степенью трансцендентности* алгебры A над $\Bbbk$ и обозначается $\operatorname{tr\,deg}_{\Bbbk} A$). □