§10. Расширения коммутативных колец

10.1. Целые элементы. Всюду этом параграфе слово «кольцо» по умолчанию означает *коммутативное кольцо с единицей*, а все гомоморфизмы колец предполагаются отображающими единицу в единицу. В частности, *расширением колец* $A \subset B$ мы называем ситуацию, когда коммутативное кольцо A является подкольцом коммутативного кольца B, и у этих колец общая единица. В этой ситуации элемент $b \in B$ называется *целым* над A, если он удовлетворяет условиям идущей ниже леммы.

Лемма 10.1 (определяющие свойства целых элементов)
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 $a_1, a_2, \dots, a_m \in A$

(2) A-линейная оболочка всех целых неотрицательных степеней b^m 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[1] $b' = 0$.

Доказательство. Импликации (1) ⇒ (2) ⇒ (3) очевидны. Чтобы вывести (1) из (3), допустим, что $e_1, e_2, \dots, e_m$ порождают M над A и что A-линейный оператор умножения на $b : M \to M$, $m \mapsto bm$, представляется в этих образующих матрицей $Y \in \mathrm{Mat}_m(A)$, т. е. действует по правилу

$$(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y . \tag{10-1}$$

Из матричного тождества $\det X \cdot E = X \cdot X^{\vee}$, где X — произвольная квадратная матрица, E — единичная матрица того же размера, а $X^{\vee}$ — присоединённая к X матрица[2], вытекает, что образ оператора умножения на $\det X$ содержится в линейной оболочке столбцов матрицы X. Поэтому умножение элементов модуля M на число $\det(bE - Y) \in B$ посылает их в линейную оболочку векторов $(e_1, e_2, \dots, e_m) \cdot (bE - Y)$, нулевую согласно (10-1). В силу B-точности модуля M обнуление $\det(bE - Y) \cdot M$ влечёт равенство $\det(bE - Y) = 0$. Поскольку все элементы матрицы Y лежат в A, это равенство имеет такой вид, как в условии (1). □

Определение 10.1
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*.

---

[1] модуль M со свойством $\forall\, b' \in B \quad b'M = 0 \Rightarrow b' = 0$ называется *точным* (по-английски *faithful*) над B

[2] состоящая из алгебраических дополнений к элементам матрицы X^t

Пример 10.1 (целозамкнутость $\mathbb{Z}$ в $\mathbb{Q}$)
Покажем, что кольцо $\mathbb{Z}$ целозамкнуто в поле $\mathbb{Q} \supset \mathbb{Z}$. 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 $q = \pm 1$.

Пример 10.2 (инварианты действия конечной группы)
Если конечная группа G действует на кольце B кольцевыми автоморфизмами, то кольцо B цело над *подкольцом инвариантов* $B^G \overset{\text{def}}{=} \{a \in B \mid ga = a \ \forall g \in G\}$: если G-орбита элемента $b \in B$ состоит из элементов $b_1 = b, b_2, b_3, \dots, b_n$, то элемент b является корнем приведённого[1] многочлена $B(t) = \prod (t - b_i) \in B^G[t]$.

Предложение 10.1
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.

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

$$p^m = x_1 p^{m-1} + \cdots + x_{m-1} p + x_m \quad \text{и} \quad q^n = y_1 q^{n-1} + \cdots + y_{n-1} q + y_n$$

для некоторых $x_\nu, y_\mu \in A$, то произведения $p^i q^j$ с $0 \leqslant i < m-1$ и $0 \leqslant j < n-1$ порождают точный над B A-модуль, выдерживающий умножение и на p, и на q, а значит, и на $p+q$, и на pq. Аналогично, если

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

для всех $1 \leqslant k \leqslant r$ и некоторых $a_{k,\ell} \in A$, то умножение на c сохраняет A-линейную оболочку всех произведений $c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}$ с $0 \leqslant i < r-1$ и $0 \leqslant j_k < m_k - 1$. □

Следствие 10.1 (лемма Гаусса – Кронекера – Дедекинда)
Для любого расширения колец $A \subset B$ и произвольных приведённых многочленов $f, g \in B[x]$ положительной степени все коэффициенты произведения $f(x)g(x)$ целы над A, если и только если все коэффициенты и у $f(x)$ и у $g(x)$ целы над A.

Доказательство. Если коэффициенты многочленов f и g целы над A, то коэффициенты их произведения $h = fg$ тоже целы над A, поскольку целые элементы образуют кольцо. Чтобы показать обратное, рассмотрим какое-нибудь кольцо $C \supset B$, над которым f и g полностью разлагаются на линейные множители[2]:

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

[1] напомню, что многочлен называется *приведённым*, если его старший коэффициент равен единице

[2] 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 $C \supset F \supset B$

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

Предложение 10.2
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 к произвольному ненулевому $a \in A$ элемент $a^{-1} \in B$ удовлетворяет уравнению

$$a^{-m} = \alpha_1 \, a^{1-m} + \cdots + \alpha_{m-1} \, a^{-1} + \alpha_0 \,,$$

в котором $\alpha_\nu \in A$. Умножая обе его 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 $b : V \to V$, $x \mapsto bx$, не имеет ядра и, стало быть, биективен. Прообраз $1 \in V$ и есть b^{-1}. □

10.1.1. Целые алгебраические числа . Пусть поле $K \supset \mathbb{Q}$ конечномерно как векторное пространство над $\mathbb{Q}$. Элементы таких полей называются *алгебраическими числами*. По предл. 10.1 целые над $\mathbb{Z}$ алгебраические числа образуют в поле K подкольцо. Оно называется *кольцом целых* поля K и обозначается $\mathcal{O}_K$.

Упражнение 10.1. Покажите, что для любого $\xi \in K$ существует такое $n \in \mathbb{N}$, что $n\xi$ цело над $\mathbb{Z}$.

Из упражнения вытекает, что K является полем частных кольца $\mathcal{O}_K$, и для любого базиса $\{e_i\}$ поля K как векторного пространства над $\mathbb{Q}$ существует такое $n \in \mathbb{N}$, что все $ne_i \in \mathcal{O}_K$.

Упражнение 10.2. Покажите, что $\mathcal{O}_K$ является свободным $\mathbb{Z}$-модулем ранга $\dim_{\mathbb{Q}} K$, и выведите из этого, что число $z \in K$ является целым , если и только если оператор умножения на z записывается целочисленной матрицей *в каком-нибудь* базисе[1] K над $\mathbb{Q}$.

Определение 10.2
Вычисленный в произвольном базисе свободного $\mathbb{Z}$-модуля $\mathcal{O}_K$ определитель Грама билинейной *формы следа* $\mathrm{Sp} : K \times K \to \mathbb{Q}$, сопоставляющей числам $\alpha, \beta \in K$ след оператора умножения на $\alpha\beta$, называется *дискриминантом* поля K.

Упражнение 10.3. Убедитесь, что дискриминант является целым числом и не зависит от выбора базиса кольца целых как модуля над $\mathbb{Z}$.

[1]именно таким образом целые алгебраические числа и были впервые определены в XIX веке Дедекиндом

Пример 10.3 (целые числа Кронекера)
Покажем, что целые элементы поля $\mathbb{Q}[\omega]$, где $\omega^2+\omega+1=0$, исчерпываются *целыми числами Кронекера* $a+b\omega$ с $a,b\in\mathbb{Z}$. Каждое число из $\mathbb{Q}[\omega]\smallsetminus\mathbb{Q}$ можно записать как

$$\xi=\frac{p_1+p_2\omega}{q}\,,\quad \text{где } p_1,p_2\in\mathbb{Z},\ q\in\mathbb{N},\ p_2\neq 0 \text{ и } \text{нод}(p_1,p_2,q)=1\,. \tag{10-2}$$

Если оператор умножения на ξ имеет целочисленную матрицу в некотором базисе пространства K над $\mathbb{Q}$, то его след $\operatorname{tr}(\xi)$ и определитель $\det(\xi)$ лежат в $\mathbb{Z}$ и не зависят от выбора базиса. В базисе 1, ω умножение на ξ записывается матрицей

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

Поэтому $2p_1-p_2=q\cdot\operatorname{tr}(\xi)$ делится на q, а $p_1^2-p_1p_2+p_2^2=q^2\cdot\det(\xi)$ делится на q^2. Тем самым, разность $(2p_1-p_2)^2-(p_1^2-p_1p_2+p_2^2)=3p_1(p_1-p_2)$ делится на q^2, что возможно лишь тогда, когда каждый простой делитель α числа q делит p_1 или p_1-p_2. Если α делит p_1, то поскольку $2p_1-p_2$ делится на q, α делит также и p_2, что противоречит условию $\text{нод}(p_1,p_2,q)=1$. Аналогично, если α делит p_1-p_2, то α делит и p_1, что также невозможно. Следовательно, у q нет простых делителей, т. е. $q=1$.

Упражнение 10.4. Опишите кольца целых в полях $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ и $\mathbb{Q}[\sqrt{-1}]$ и вычислите дискриминанты этих полей.

10.2. Приложения к теории представлений. Пусть G — конечная группа. Значение характера χ_ϱ любого конечномерного представления ϱ группы G на любом элементе $g\in G$ цело над $\mathbb{Z}$ в силу того, что оператор $\varrho(g)$ аннулируется многочленом $t^{|G|}-1$, все корни которого целы над $\mathbb{Z}$, а $\chi_\varrho(g)$ это сумма некоторых из них[1].

Теорема 10.1
Если комплексное представление $\varrho:\mathbb{C}[G]\to\operatorname{End}V$ конечной группы G неприводимо, то $\dim V$ делит индекс $[G:Z(G)]$ центра $Z(G)$ группы G.

Доказательство. Покажем сначала, что $\dim V$ делит $|G|$. Согласно прим. 10.1 для этого достаточно убедиться, что рациональное число $|G|/\dim V$ цело над $\mathbb{Z}$. Так как V неприводимо, скалярный квадрат характера χ_V равен единице:

$$1=(\chi_V,\chi_V)=\frac{1}{|G|}\sum_{g\in G}\operatorname{tr}\varrho(g^{-1})\cdot\operatorname{tr}\varrho(g)\,. \tag{10-3}$$

Функция $g\mapsto\operatorname{tr}\varrho(g^{-1})$ постоянна на классах сопряжённых элементов и принимает целые над $\mathbb{Z}$ значения. Обозначим её значение на классе $K\in\operatorname{Cl}(G)$ через $\tau(K)\in\mathbb{C}$ и перепишем (10-3) как

$$\frac{|G|}{\dim V}=\frac{1}{\dim V}\sum_{g\in G}\operatorname{tr}\varrho(g^{-1})\cdot\operatorname{tr}\varrho(g)=\sum_{K\in\operatorname{Cl}G}\tau(K)\cdot\frac{1}{\dim V}\cdot\operatorname{tr}\sum_{g\in K}\varrho(g)\,. \tag{10-4}$$

[1] напомню, что собственные числа оператора содержатся среди корней любого аннулирующего этот оператор многочлена

Остаётся 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 над $\mathbb{Z}$. Элемент $g_K = \sum\limits_{g \in K} g \in \mathbb{Z}[G] \cap Z(\mathbb{C}[G])$ лежит в конечно порождённом $\mathbb{Z}$-модуле центральных элементов групповой алгебры, являющихся целочисленными линейными комбинациями элементов группы. Неприводимое представление $\varrho : \mathbb{C}[G] \to \operatorname{End} V$ переводит этот $\mathbb{Z}$-модуль в конечно порождённый $\mathbb{Z}$-подмодуль алгебры $\operatorname{End} V$, причём все его операторы, будучи перестановочными с неприводимым действием группы, являются по лемме Шура скалярными гомотетиями. Коэффициенты этих гомотетий составляют таким образом конечно порождённый $\mathbb{Z}$-подмодуль в $\mathbb{C}$, выдерживающий умножение на каждый из коэффициентов. Следовательно, все эти коэффициенты целы над $\mathbb{Z}$. Но коэффициент гомотетии $\varrho(g_K)$ как раз и равен $\operatorname{tr} \varrho(g_K)/\dim V$, что и завершает доказательство целостности $|G|/\dim V$.

Докажем теперь утверждение теоремы, а именно установим целость над $\mathbb{Z}$ рационального числа $q = [G : Z(G)]/\dim V$. Для этого достаточно убедиться, что все его натуральные степени q^n лежат в конечно порождённом $\mathbb{Z}$-подмодуле поля $\mathbb{Q}$. Рассмотрим представление группы $G^n = G \times G \times \cdots \times G$ в пространстве $W = V^{\otimes n}$, заданное правилом $(g_1, g_2, \dots, g_n) : v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto \varrho(g_1)v_1 \otimes \varrho(g_2)v_2 \otimes \cdots \varrho(g_n)v_n$.

Упражнение 10.5. Убедитесь, что это представление неприводимо.

Подгруппа $C \subset G^n$, состоящая из элементов $(c_1, c_2, \dots, c_n)$ с $c_i \in Z(G)$ и $c_1 c_2 \dots c_n = 1$, 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 $\varrho(c_1 c_2 \dots c_n) = 1$ произведение этих констант равно единице. Подгруппа C имеет порядок $|Z(G)|^{n-1}$ и нормальна, поскольку лежит в центре группы G^n. Пространство W размерности $(\dim V)^n$ является неприводимым представлением фактор группы G^n/C порядка $|G|^n/|Z(G)|^{n-1}$. По уже доказанному

$$\frac{|G|^n}{(\dim V)^n |Z(G)|^{n-1}} = |Z(G)| \cdot q^n \in \mathbb{Z}.$$

Тем самым, все степени q^n лежат в конечно порождённом $\mathbb{Z}$-подмодуле $|Z(G)|^{-1} \cdot \mathbb{Z}$ поля $\mathbb{Q}$, что и требовалось. □

10.3. Алгебраические элементы. Коммутативная $\Bbbk$-алгебра B называется *конечно порожденной*, если она является фактором кольца многочленов, т. е. имеется эпиморфизм $\Bbbk$-алгебр $\pi : \Bbbk[x_1, x_2, \dots, x_m] \twoheadrightarrow B$. В этом случае образы переменных $b_i = \pi(x_i) \in B$ называются *образующими* алгебры B, а ядро $\ker \pi \subset \Bbbk[x_1, x_2, \dots, x_m]$ называется *идеалом соотношений* между ними. Целость элемента $b \in B$ над полем $\Bbbk$ равносильна его *алгебраичности*, т. е. тому, что b удовлетворяет какому-нибудь — необязательно приведённому — уравнению $f(b) = 0$ с ненулевым $f \in \Bbbk[x]$. Иначе алгебраичность элемента $b \in B$ над $\Bbbk$ можно охарактеризовать тем, что *гомоморфизм вычисления*

$$\operatorname{ev}_b : \Bbbk[x] \to B, \quad f \mapsto f(b) \tag{10-5}$$

имеет ненулевое ядро. Так как все идеалы в $\Bbbk[x]$ главные, $\ker(\mathrm{ev}_b) = (\mu_b)$. Образующая $\mu_b \in \Bbbk[x]$ однозначно определяется по b как приведённый многочлен наименьшей степени, аннулирующий b. Этот многочлен называется *минимальным многочленом* элемента b над $\Bbbk$. Элемент $b \in B$, не являющийся алгебраическим, называется *трансцендентным* над $\Bbbk$.

Мы будем обозначать через $\Bbbk[b] = \operatorname{im} \mathrm{ev}_b \subset B$ наименьшую $\Bbbk$-подалгебру в B, содержащую 1 и b. Если b трансцендентен, эта подалгебра изоморфна кольцу многочленов $\Bbbk[x]$. В частности, она бесконечномерна как векторное пространство над $\Bbbk$ и не является полем. Если элемент b алгебраичен, размерность подалгебры $\Bbbk[b] = \Bbbk[x]/(\mu_b)$ как векторного пространства над $\Bbbk$ равна $\dim_\Bbbk \Bbbk[b] = \deg \mu_b$, и эта подалгебра является полем , если и только если минимальный многочлен μ_b неприводим.

Упражнение 10.6. Убедитесь, что следующие три свойства алгебраического над $\Bbbk$ элемента $b \in B$ с минимальным минимальный многочленом $\mu_b \in \Bbbk[x]$ эквивалентны друг другу: а) $\Bbbk[b]$ является полем б) $\Bbbk[b]$ не имеет делителей нуля в) μ_b неприводим в $\Bbbk[t]$.

Теорема 10.2
Если конечно порожденная $\Bbbk$-алгебра B является полем, то все её элементы алгебраичны над $\Bbbk$.

Доказательство. Пусть B имеет образующие $\{b_1, b_2, \dots , b_m\}$ и является полем. Доказывать алгебраичность B будем индукцией по m. Когда $m = 1$, т. е. $B = \Bbbk[b]$, всё очевидно: если b трансцендентен, гомоморфизм (10-5) 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 по предположению индукции B алгебраично над $\Bbbk[b_m]$, а значит, по предл. 10.1 B алгебраично и над $\Bbbk$. Таким образом, достаточно показать, что b_m алгебраичен над $\Bbbk$.

Допустим, что b_m трансцендентен. Тогда гомоморфизм (10-5) продолжается до изоморфизма поля рациональных функций $\Bbbk(x)$ с наименьшим содержащим b_m подполем $\Bbbk(b_m) \subset B$. По предположению индукции, B алгебраично над $\Bbbk(b_m)$, т. е. каждая из образующих $b_1, b_2, \dots , b_{m-1}$ 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. 10.2 эта подалгебра F должна быть полем, что невозможно, поскольку, к примеру, $1 + p(b_m)$ не обратим в F: если есть такой многочлен $g \in \Bbbk[x_1, x_2]$, что $g\left(b_m\, , 1/p(b_m)\right) \cdot (1 + p(b_m)) = 1$, то, записывая рациональную функцию $g\left(x\, , 1/p(x)\right)$ 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 10.2
Всякое поле $\mathbb{F}$, которое конечно порождено как алгебра над своим подполем $\Bbbk \subset \mathbb{F}$, конечномерно как векторное пространство над $\Bbbk$.

Доказательство. Индукция по числу образующих: добавление очередной алгебраической образующей приводит к конечномерному пространству над полем, порождённым предыдущими образующими. □

Определение 10.3 (нормальные кольца)
Коммутативное кольцо A без делителей нуля называется *нормальным*, если оно целозамкнуто в своём поле частных Q_A. В частности, каждое поле нормально.

Пример 10.4 (факториальные кольца нормальны)
Дословно то же рассуждение, что и в прим. 10.1, показывает, что любое факториальное[1] кольцо 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.

Предложение 10.3 (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 10.2
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. 10.1 все коэффициенты μ_b целы над A. □

Следствие 10.3
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 над полем Q_A лежит в $A[x]$. □

[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 $a = p_1p_2 \cdots p_n = q_1q_2 \cdots q_m$ 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

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

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

$$\mathrm{ev}_{(a_1,a_2,\dots,a_m)} : \Bbbk[x_1, x_2, \dots, x_m] \to A\,, \quad f \mapsto f(a_1, a_2, \dots, a_m)$$

инъективно. В этом случае оно продолжается до изоморфизма полей

$$\Bbbk(x_1, x_2, \dots, x_m) \simeq \Bbbk(a_1, a_2, \dots, a_m) \subset Q_A\,,$$

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

Элементы $a_1, a_2, \dots, a_m \in A$ называются *алгебраически порождающими* A над $\Bbbk$, если каждый элемент алгебры A алгебраичен над $\Bbbk(a_1, a_2, \dots, a_m)$. В этом случае всё поле Q_A тоже алгебраично над $\Bbbk(a_1, a_2, \dots, a_m)$, т. к. по предл. 10.2 целое замыкание $\Bbbk(a_1, a_2, \dots, a_m)$ в Q_A является полем, содержащим A, а значит, и Q_A.

Алгебраически независимый набор элементов $a_1, a_2, \dots, a_m$ из алгебры A, алгебраически порождающий A над $\Bbbk$, называется *базисом трансцендентности* A над $\Bbbk$. Поскольку собственные подмножества любого базиса трансцендентности алгебраически независимы, но не являются базисами трансцендентности, базис трансцендентности можно иначе охарактеризовать либо как такой минимальный по включению набор $a_1, a_2, \dots, a_m$, что алгебра A алгебраична над $\Bbbk(a_1, a_2, \dots, a_m)$, либо как максимальный по включению алгебраически независимый набор $a_1, a_2, \dots, a_m$. Доказательство того, что все базисы трансцедентности состоят из одинакового числа элементов совершенно аналогично доказательству оответствующей теоремы о базисах векторных пространств.

Лемма 10.3 (о замене)
Если $b_1, b_2, \dots, b_n \in A$ алгебраически независимы, а $a_1, a_2, \dots, a_m \in A$ алгебраически порождают A над $\Bbbk$, то $n \leqslant m$ и элементы a_i можно перенумеровать так, что набор $b_1, \dots, b_n, a_{n+1}, \dots, a_m$ будет алгебраически порождать A над $\Bbbk$.

Доказательство. Поскольку b_1 алгебраичен над $\Bbbk(a_1, a_2, \dots, a_m)$, имеется содержащее b_1 полиномиальное соотношение $f(b_1, a_1, a_2, \dots, a_m) = 0$, и т. к. b_1 трансцендентен над $\Bbbk$, в это соотношение входит какое-нибудь a_i. Перенумеруем a_i так, чтобы это было a_1. Тогда a_1, а с ним и вся алгебра A алгебраичны над $\Bbbk(b_1, a_2, \dots, a_m)$. Пусть по индукции элементы $b_1, \dots, b_k, a_{k+1}, \dots, a_m$ алгебраически порождают алгебру A над $\Bbbk$, и при этом $k < n$. Поскольку b_{k+1} алгебраичен над $\Bbbk\left(b_1, \dots, b_k, a_{k+1}, \dots, a_m\right)$, имеется содержащее b_{k+1} полиномиальное соотношение

$$f\left(\left(b_1, \dots, b_k, b_{k+1}, a_{k+1}, \dots, a_m\right)\right) = 0\,,$$

и т. к. набор $b_1, b_2, \dots, b_n$ алгебраически независим над над $\Bbbk$, в это соотношение входит какое-нибудь a_i, откуда, в частности, следует что $m > k$. Перенумеровывая оставшиеся a_i так, чтобы это было a_{k+1}, мы как и выше заключаем, что a_{k+1}, а с ним и вся алгебра A алгебраичны над $\Bbbk\left(b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_m\right)$, т. е. воспроизводим индуктивное предположение. □

Следствие 10.4 (теорема о базисе)
Все базисы трансцендентности конечно порождённой $\Bbbk$-алгебры состоят из одинакового числа элементов, не превосходящего число образующих, причём любой набор элементов, алгебраически порождающий A над $\Bbbk$, содержит в себе базис трансцендентности, а любой алгебраически независимый набор элементов можно дополнить до базиса трансцендентности. □

Определение 10.4
Число элементов в базисе трансцендентности конечно порождённой алгебры A над $\Bbbk$ называется *степенью трансцендентности* этой алгебры и обозначается $\operatorname{tr}\deg_{\Bbbk} A$).

Ответы и указания к некоторым упражнениям

Упр. 10.1. В силу конечномерности K над $\mathbb{Q}$ целые неотрицательные степени ξ^m линейно зависимы над $\mathbb{Q}$. Умножая эту линейную зависимость на общий знаменатель всех коэффициентов, получаем на ξ уравнение $a_0\xi^n + a_1\xi^{n-1} + \dots + a_{n-1}\xi + a_n = 0$ с $a_i \in \mathbb{Z}$. Тогда $\zeta = a_0\xi$ цел, т. к. $\zeta^n = -a_1 \cdot \zeta^{n-1} - a_0a_2 \cdot \zeta^{n-2} - \dots - a_0^{n-1}a_n$.

Упр. 10.2. Будучи подмодулем поля, модуль $\mathcal{O}_K$ не имеет кручения, и стало быть, свободен. Его ранг не выше d, поскольку любые $d+1$ его векторов линейно зависимы над $\mathbb{Q}$, а значит, и над $\mathbb{Z}$. С другой стороны, подходящие натуральные кратности любых d базисных векторов пространства K дают линейно независимую над $\mathbb{Q}$ систему векторов из $\mathcal{O}_K$. Поэтому ранг $\mathcal{O}_K$ не меньше d. В базисе модуля целых оператор умножения на целое алгебраическое число записывается целочисленной матрицей.