§9. Расширения коммутативных колец

9.1. Целые элементы. Всюду этом параграфе термин «кольцо» по умолчанию подразумевает *коммутативное кольцо с единицей*, а все гомоморфизмы колец предполагаются отображающими единицу в единицу. Если кольцо A является подкольцом кольца B, то мы называем B *расширением* кольца A. В этой ситуации элемент $b \in B$ называется *целым* над A, если он удовлетворяет перечисленным в лем. 9.1 условиям.

Лемма 9.1 (характеризация целых элементов)
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 некоторых $m \in \mathbb{N}$ и $a_1, \ldots, a_m \in A$

(2) A-линейная оболочка всех целых неотрицательных степеней b^m линейно порождается над A конечным числом элементов

(3) существует конечно порождённый A-подмодуль $M \subset B$, который не аннулируется умножением ни на какой ненулевой элемент из B, и такой, что $bM \subset M$.

Доказательство. Импликации (1) $\Rightarrow$ (2) $\Rightarrow$ (3) очевидны. Покажем, что (3) $\Rightarrow$ (1). Пусть элементы $e_1, \ldots, e_m$ линейно порождают M над A и A-линейный оператор $b : M \to M$, $m \mapsto bm$, умножения на b действует на эти образующие по правилу

$$(be_1, \ldots, be_m) = (e_1, \ldots, e_m) \cdot Y\,, \tag{9-1}$$

где $Y \in \mathrm{Mat}_m(A)$ — некоторая матрица. Для любой квадратной матрицы X над любым коммутативным кольцом с единицей выполняется тождество $\det X \cdot E = X \cdot X^\vee$, где $X^\vee$ — присоединённая к X матрица[1], а E — единичная матрица того же размера, что X. Согласно этому тождеству, образ оператора умножения на $\det X$ содержится в линейной оболочке столбцов матрицы X. Мы заключаем, что $\det(bE - Y) \cdot M$ содержится в линейной оболочке векторов $(e_1, \ldots, e_m) \cdot (bE - Y)$, которая равна нулю в силу (9-1). Поскольку умножение на ненулевой элемент кольца B не может аннулировать модуль M, равенство $\det(bE - Y) \cdot M = 0$ влечёт равенство $\det(bE - Y) = 0$. Так как все элементы матрицы Y лежат в A, последнее равенство имеет требуемый в условии (1) вид. □

Определение 9.1
Множество всех $b \in B$, целых над подкольцом $A \subset B$, называется *целым замыканием* A в B. Если оно совпадает с A, подкольцо A называется *целозамкнутым* в B. Если оно совпадает с B, расширение колец $A \subset B$ называется *целым* и кольцо B называется *целой A-алгеброй*.

Пример 9.1 (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 $q = \pm 1$.

[1] Она состоит из алгебраических дополнений $x^\vee_{ij} = (-1)^{i+j} X_{ji}$ к элементам матрицы X^t, см. теорему 8.1 на стр. 114 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_08.pdf.

Пример 9.2 (инварианты действия конечной группы)
Пусть конечная группа G действует на кольце B кольцевыми автоморфизмами. Покажем, что кольцо B цело над *подкольцом инвариантов* $B^G \stackrel{\text{def}}{=} \{a \in B \mid \forall\, g \in G\ \ ga = a\}$. Если G-орбита элемента $b \in B$ состоит из элементов $b_1, \dots, b_n$, где $b = b_1$, то элемент b является корнем приведённого[1] многочлена $B(t) = \prod(t - b_i) \in B^G[t]$.

Предложение 9.1
Целое замыкание любого подкольца $A \subset B$ является подкольцом в B. В любом расширении колец $C \supset B$ всякий элемент $c \in C$, целый над целым замыканием A в B, цел и над A.

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

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

для некоторых $x_\nu, y_\mu \in A$, то произведения $p^i q^j$ с $0 \leqslant i \leqslant m-1$ и $0 \leqslant j \leqslant n-1$ порождают A-модуль, который выдерживает умножение и на p, и на q, а значит, и на $p+q$, и на pq. Поскольку он содержит единицу, его нельзя аннулировать умножением ни на какой элемент из B. Аналогично, если $z_0^r = z_1 z_0^{r-1} + \dots + z_{r-1} z_0 + z_r$, где каждый z_k с $k > 0$ удовлетворяет равенству

$$z_k^{m_k} = a_{k,1}\, z_k^{m_k - 1} + \dots + a_{k,m_k - 1}\, z_k + a_{k,m_k}$$

для некоторых $a_{k,\ell} \in A$, то умножение на элемент z_0 переводит в себя A-линейную оболочку всех произведений $z_0^{j_0} z_1^{j_1} \cdots z_r^{j_r}$, где $0 \leqslant j_0 \leqslant r-1$ и $0 \leqslant j_k \leqslant m_k - 1$ при $k > 0$. □

Следствие 9.1 (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 обоих многочленов $f(x)$ и $g(x)$ 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], т. е. $f(x) = \prod(x - \alpha_\nu)$ и $g(x) = \prod(x - \beta_\mu)$ в $C[x]$ для некоторых $\alpha_\nu, \beta_\mu \in C$. Если все коэффициенты многочлена $h(x) = \prod(x - \alpha_\nu) \prod(x - \beta_\mu)$ целы над A, то все его корни α_ν и β_μ целы над целым замыканием A в C, а значит, и над самим A. Поскольку коэффициенты многочленов f и g являются многочленами от α_ν и β_μ, они тоже целы над A. □

Предложение 9.2
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.

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

[2] Кольцо $C \supset B$, над которым заданный приведённый многочлен $f \in B[x]$ полностью раскладывается на линейные множители, строится индукцией по $\deg f$. Если $\deg f > 0$, то B вкладывается в фактор кольцо $F = B[x]/(f)$ как подкольцо, образованное классами констант. В кольце F многочлен f имеет корень $\gamma = x \pmod f$. Поэтому $f(x) = (x - \gamma) \cdot f_1(x)$, где $f_1 \in F[x]$ тоже приведён и $\deg f_1 < \deg f$. По индукции, $f_1 = \prod(x - \gamma_i)$ для подходящих элементов γ_i из подходящего расширения $C \supset F \supset B$.

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

Обратно, если A — поле, и B — целая A-алгебра, то все неотрицательные целые степени b^i любого ненулевого элемента $b \in B$ порождают конечномерное векторное пространство V над полем A. Если в B нет делителей нуля, то линейный оператор $b\colon V \to V$, $x \mapsto bx$, сюръективен, так как имеет нулевое ядро. Обратный к b элемент b^{-1} является прообразом единицы $1 \in V$. □

Пример 9.3 (целые алгебраические числа)
Пусть поле $K \supset \mathbb{Q}$ конечномерно как векторное пространство над $\mathbb{Q}$. Элементы таких полей называются *алгебраическими числами*. По предл. 9.1 целые над $\mathbb{Z}$ алгебраические числа образуют в поле K подкольцо. Оно называется *кольцом целых* поля K и обозначается $\mathcal{O}_K$. Поскольку целые неотрицательные степени ξ^m любого числа $\xi \in K$ линейно зависимы над $\mathbb{Q}$, каждое алгебраическое число ξ удовлетворяет уравнению $a_0\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0$ с коэффициентами $a_i \in \mathbb{Z}$, откуда вытекает, что число $a_0\xi$ цело[1] над $\mathbb{Z}$. Таким образом, для каждого алгебраического числа ξ и для любого базиса $e_1, \ldots, e_d$ поля K как векторного пространства над $\mathbb{Q}$ существует такое $n \in \mathbb{N}$, что $n\xi$ и все ne_i целы над $\mathbb{Z}$. В частности, каждое конечномерное над $\mathbb{Q}$ поле $K \supset \mathbb{Q}$ является полем частных своего кольца целых $\mathcal{O}_K$.

Упражнение 9.1. Покажите, что кольцо целых $\mathcal{O}_K \subset K$ является свободным $\mathbb{Z}$-модулем ранга $d = \dim_{\mathbb{Q}} K$, а число $\zeta \in K$ является целым над $\mathbb{Z}$ если и только если оператор умножения на ζ записывается в подходящем базисе K над $\mathbb{Q}$ целочисленной матрицей[2].

Пример 9.4 (целые квадратичные иррациональности)
Расширение $K \supset \mathbb{Q}$ называется *квадратичным*, если K двумерно как векторное пространство над $\mathbb{Q}$. В этом случае для любого $\zeta \in K \smallsetminus \mathbb{Q}$ числа 1 и ζ образуют базис K над $\mathbb{Q}$, и $\zeta^2 = b\zeta + c$ для некоторых $b, c \in \mathbb{Q}$, откуда $\zeta = x + y\sqrt{d}$ для подходящих $x, y \in \mathbb{Q}$ и свободного от квадратов[3] целого d. Поэтому $K = \mathbb{Q}[\sqrt{d}] = \mathbb{Q}[x]/(x^2 - d)$. Таким образом, каждое квадратичное расширение получается присоединением к $\mathbb{Q}$ квадратного корня из свободного от квадратов целого числа.

Упражнение 9.2. Покажите, что $\mathbb{Q}[\sqrt{d_1}] \not\simeq \mathbb{Q}[\sqrt{d_2}]$ для свободных от квадратов $d_1 \neq d_2$.

Пусть число $\xi = a + b\sqrt{d}$, где $a, b \in \mathbb{Q}$, цело над $\mathbb{Z}$. Обозначим через $t = \operatorname{tr}(\xi)$ и $n = N(\xi)$ след и определитель оператора умножения на ξ в поле $K = \mathbb{Q}[\sqrt{d}]$. Так как в подходящем базисе поля Kнад $\mathbb{Q}$ этот оператор имеет целочисленную матрицу, оба числа $t, n \in \mathbb{Z}$. В базисе $1, \sqrt{d}$ умножение на ξ имеет матрицу

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Поэтому $t = 2a \in \mathbb{Z}$ и $n = a^2 - db^2 = t^2/4 - db^2 \in \mathbb{Z}$. Полагая $s = 2b$, мы заключаем, что $s \in \mathbb{Z}$ и $t^2 - ds^2 \equiv 0 \pmod 4$. Если $d \equiv 1 \pmod 4$, то $t^2 \equiv s^2 \pmod 4$, откуда $t \equiv s \pmod 2$. Пусть $s = t + 2r$, где $r \in \mathbb{Z}$. Тогда $\xi = t + r(1 + \sqrt{d})/2$.

Упражнение 9.3. Убедитесь, что $(1 + \sqrt{d})/2 \in \mathcal{O}_K$ при $d \equiv 1 \pmod 4$.

[1] Ибо $\zeta = a_0\xi$ удовлетворяет уравнению $\zeta^n = -a_1 \cdot \zeta^{n-1} - a_0 a_2 \cdot \zeta^{n-2} - \cdots - a_0^{n-1} a_n$.

[2] Именно так целые алгебраические числа были впервые определены Дедекиндом в XIX веке.

[3] Целое число называется *свободным от квадратов*, если оно отлично от нуля и единицы и не делится на отличные от единицы целые квадраты.

Мы заключаем, что при $d \equiv 1 \pmod 4$ базис $\mathbb{Z}$-модуля $\mathcal{O}_K$ образуют 1 и $(1+\sqrt{d})/2$. В частности, *числа Кронекера*, т. е. целые элементы поля $\mathbb{Q}[\sqrt{-3}] = \mathbb{Q}[\omega]/(\omega^2+\omega+1)$, исчерпываются целочисленными линейными комбинациями вида $a+b\omega$, где $\omega = (-1+\sqrt{-3})/2$ — первообразный комплексный кубический корень из единицы. Если $d \equiv 2 \pmod 4$ или $d \equiv 3 \pmod 4$, то соответственно $t^2 \equiv 2s^2 \pmod 4$ или $t^2 + s^2 \equiv 0 \pmod 4$, и оба числа t, s чётны, а $\xi = a + b\sqrt{d}$ имеет $a, b \in \mathbb{Z}$. Так как $\sqrt{d} \in \mathcal{O}_K$, базис $\mathbb{Z}$-модуля $\mathcal{O}_K$ при $d \equiv 2, 3 \pmod 4$ составляют 1 и $\sqrt{d}$. В частности, *гауссовы числа*, т. е. целые элементы поля $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]/(i^2+1)$исчерпываются целочисленными линейными комбинациями вида $a+bi$, где $i = \sqrt{-1}$ — первообразный комплексный корень четвёртой степени из единицы.

9.2. 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 значение $\chi_\varrho(g)$ равно сумме некоторых из этих корней[1].

Теорема 9.1
Если конечная группа G имеет нормальную абелеву подгруппу $A \lhd G$, то размерности всех комплексных неприводимых линейных представлений группы G делят индекс $[G : A]$.

Доказательство. Пусть $\varrho : \mathbb{C}[G] \to \operatorname{End} W$ — неприводимое комплексное представление. Сначала докажем теорему для единичной подгруппы $A = \{e\}$, т. е. покажем, что $\dim W$ делит $|G|$. В силу прим. 9.1 достаточно убедиться, что рациональное число $|G|/\dim W$ цело над $\mathbb{Z}$. Так как представление ϱ неприводимо, скалярный квадрат его характера равен единице:

$$1 = (\chi_\varrho, \chi_\varrho) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \varrho(g^{-1}) \cdot \operatorname{tr} \varrho(g)\,. \tag{9-2}$$

Функция $g \mapsto \operatorname{tr} \varrho(g^{-1})$ постоянна на классах сопряжённости, и её значения целы над $\mathbb{Z}$. Обозначим через $\tau(K) \in \mathbb{C}$ её значение на классе $K \in \operatorname{Cl}(G)$ и перепишем (9-2) как

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

Достаточно проверить, что каждое из чисел

$$\frac{1}{\dim W} \operatorname{tr} \sum_{g \in K} \varrho(g) = \frac{\operatorname{tr} \varrho(g_K)}{\dim W}\,, \quad \text{где} \quad g_K \stackrel{\text{def}}{=} \sum_{g \in K} g \in Z(\mathbb{Z}[G])\,,$$

цело над $\mathbb{Z}$. Неприводимое представление ϱ переводит конечно порождённый $\mathbb{Z}$-модуль центральных элементов подкольца $\mathbb{Z}[G] \subset \mathbb{C}[G]$ в конечно порождённый $\mathbb{Z}$-подмодуль кольца $\operatorname{End} W$. По лемме Шура все элементы последнего подмодуля являются скалярными гомотетиями, ибо перестановочны со всеми элементами группы. Коэффициенты этих гомотетий образуют 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 $\operatorname{tr} \varrho(g_K)/\dim W$. Итак, $|G|/\dim W \in \mathbb{Z}$.

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

Теперь рассмотрим случай, когда $A = Z(G)$ является центром группы G, т. е. покажем, что рациональное число $q = [G : Z(G)]/\dim W$ тоже цело над $\mathbb{Z}$. Для этого достаточно убедиться, что все его натуральные степени q^n лежат в конечно порождённом $\mathbb{Z}$-подмодуле поля $\mathbb{Q}$. Рассмотрим действие группы $G^n = G \times \dots \times G$ на $W^{\otimes n}$ по правилу

$$(g_1, \dots, g_n)\colon w_1 \otimes \dots \otimes w_n \mapsto \varrho(g_1)w_1 \otimes \dots \otimes \varrho(g_n)w_n\,.$$

Упражнение 9.4. Убедитесь, что это неприводимое линейное представление.

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

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

Тем самым, все степени q^n лежат в $\mathbb{Z}$-модуле $|Z(G)|^{-1}\,\mathbb{Z} \subset \mathbb{Q}$ ранга 1.

Наконец, рассмотрим произвольную нормальную абелеву подгруппу $A \lhd G$ и изотипное разложение $\operatorname{res}_A W = \bigoplus W_\chi$ ограничения представления ϱ на A. Каждая изотипная компонента W_χ является прямой суммой одномерных представлений абелевой группы A, отвечающих некоторому мультипликативному характеру[1] $\chi\colon A \to \mathbb{C}^*$, т. е. $aw = \chi(a)w$ для всех $a \in A$ и $w \in W_\chi$. Поскольку подгруппа A нормальна в G, группа G действует на её мультипликативных характерах: элемент $g \in G$ переводит характер $\chi\colon A \to \mathbb{C}^*$ в композицию $\chi^g = \chi \circ \operatorname{Ad}_{g^{-1}}$, принимающую на элементах $a \in A$ значения $\chi^g(a) = \chi(g^{-1}ag)$. Так как $agw = gg^{-1}agw = g\chi^g(a)w = \chi^g(a)gw$ для всех $w \in W_\chi$, $a \in A$, $g \in G$, в представлении ϱ каждый элемент $g \in G$ изоморфно отображает изотипную компоненту W_χ в компоненту W_{χ^g}. Поскольку представление ϱ неприводимо, действие G на изотипных компонентах W_χ транзитивно. Поэтому все компоненты имеют одну и ту же размерность, которая делит $\dim W$. Если компонента всего одна, то все элементы подгруппы A действуют на W скалярно, и образ $\varrho(A)$ лежит в центре $Z(\varrho(G))$ образа всего представления. По уже доказанному индекс центра $[\varrho(G) : Z(\varrho(G))]$ делится на $\dim W$. Но этот индекс делит индекс $[\varrho(G) : \varrho(A)]$ центральной подгруппы $\varrho(A)$, а последний в свою очередь делит индекс[2] $[G : A]$. Остаётся рассмотреть случай, когда изотипных компонент несколько. Пусть W_χ — одна из них. Обозначим через $H = \{g \in G \mid g(W_\chi) = W_\chi\}$ её стабилизатор в G. Тогда общее число изотипных компонент равно $[G : H]$, подгруппа $H \subsetneq G$ является собственной, содержит A, и её линейное представление в пространстве W_χ неприводимо.

Упражнение 9.5. Убедитесь в этом.

Применяя индукцию по порядку $|G|$, мы можем считать, что $\dim W_\chi$ делит индекс $[H : A]$. Но тогда и $\dim W = [G : H]\,\dim W_\chi$ делит $[G : A] = [G : H]\,[H : A]$. □

[1] См. n° 5.4.1 на стр. 71.

[2] Ибо гомоморфизм ϱ корректно задаёт эпиморфизм фактор групп $G/A \twoheadrightarrow \varrho(G)/\varrho(A)$.

9.3. Алгебраические элементы. Коммутативная $\Bbbk$-алгебра B называется *конечно порожденной*, если существует эпиморфизм $\Bbbk$-алгебр $\pi\colon \Bbbk[x_1,\dots,x_m] \twoheadrightarrow B$. В этом случае образы переменных $b_i = \pi(x_i) \in B$ называются *образующими* алгебры B, а ядро $\ker\pi \subset \Bbbk[x_1,\dots,x_m]$ называется *идеалом соотношений* между ними. Элемент $b \in B$ цел над полем $\Bbbk$ если и только если *гомоморфизм вычисления* $\mathrm{ev}_b\colon \Bbbk[x] \to B$, $f \mapsto f(b)$, имеет ненулевое ядро, т. е. $f(b) = 0$ для какого-нибудь ненулевого $f \in \Bbbk[x]$. Такие элементы b также называют *алгебраическими* над полем $\Bbbk$. Поскольку все идеалы в $\Bbbk[x]$ главные, $\ker(\mathrm{ev}_b) = (\mu_b)$, где образующая $\mu_b \in \Bbbk[x]$ однозначно определяется алгебраическим элементом 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 $\Bbbk$.

Обозначим через $\Bbbk[b] = \operatorname{im}\mathrm{ev}_b \subset B$ наименьшую $\Bbbk$-подалгебру в B, содержащую элементы 1 и b. Если b трансцендентен, подалгебра $\Bbbk[b]$ изоморфна кольцу многочленов $\Bbbk[x]$. В частности, она бесконечномерна как векторное пространство над $\Bbbk$ и не является полем. Когда b алгебраичен, алгебра $\Bbbk[b] \simeq \Bbbk[x]/(\mu_b)$ имеет размерность $\deg\mu_b$ как векторное пространство над $\Bbbk$. Она является полем если и только если многочлен μ_b неприводим в $\Bbbk[x]$.

Упражнение 9.6. Убедитесь, что следующие три свойства алгебраического над полем $\Bbbk$ элемента $b \in B$ с минимальным 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 $\Bbbk[x]$.

Теорема 9.2
Если конечно порождённая $\Bbbk$-алгебра является полем, то все её элементы алгебраичны над $\Bbbk$.

Доказательство. Пусть алгебра B является полем и порождается над $\Bbbk$ элементами $b_1,\dots,b_m$. Воспользуемся индукцией по m. Случай $m = 1$ был разобран перед упр. 9.6 выше. Пусть $m > 1$. Если b_m алгебраичен над $\Bbbk$, то алгебра $\Bbbk[b_m]$ является полем. Тогда по предположению индукции поле B алгебраично над $\Bbbk[b_m]$, а значит и над $\Bbbk$ по предл. 9.1 на стр. 128. Остаётся убедиться, что образующая b_m не может быть трансцендентна над $\Bbbk$. Допустим противное. Тогда изоморфизм $\Bbbk[x] \xrightarrow{\sim} \Bbbk[b_m]$ 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 полем $\Bbbk(b_m)$, т. е. каждая из образующих $b_1,\dots,b_{m-1}$ удовлетворяет некоторому полиномиальному уравнению с коэффициентами из $\Bbbk(b_m)$. Умножая эти уравнения на подходящие многочлены от b_m, сделаем их коэффициенты лежащими в $\Bbbk[b_m]$, а все старшие коэффициенты — равными одному и тому же многочлену $p(b_m) \in \Bbbk[b_m]$. Поле B цело над подалгеброй $F \subset B$, порождённой над $\Bbbk$ элементами b_m и $1/p(b_m)$. По предл. 9.2 подалгебра F является полем. Покажем, что элемент $1 + p(b_m) \in F$ не обратим в F. Пусть это не так, и

$$\big(1 + p(b_m)\big)\, g\big(b_m, 1/p(b_m)\big) = 1 \tag{9-3}$$

для некоторого многочлена $g \in \Bbbk[x_1,x_2]$. Записывая рациональную функцию $g\big(x, 1/p(x)\big)$ в виде $h(x)/p^k(x)$, где $h \in \Bbbk[x]$ не делится в $\Bbbk[x]$ на p, и умножая обе части (9-3) на $p^k(b_m)$, мы получим на b_m полиномиальное уравнение $h(b_m)\,(1 + p(b_m)) = p^{k+1}(b_m)$. Оно нетривиально, поскольку $h(1+p) = h + hp$ не делится на p. □

Следствие 9.2
Всякое поле $\mathbb{F}$, являющееся конечно порождённой алгеброй над 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 9.2 (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 9.5 (факториальные кольца нормальны)
Дословно то же рассуждение, что и в прим. 9.1, 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 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.

Следствие 9.3 (лемма Гаусса)
Пусть A — нормальное кольцо с полем частных Q_A. Если в $Q_A[x]$ многочлен $f \in A[x]$ раскладывается в произведение приведённых множителей, то все эти множители лежат в $A[x]$.

Доказательство. Это вытекает из сл. 9.1 на стр. 128. □

Следствие 9.4
Пусть A — целостное[2] кольцо с полем частных Q_A, и B — произвольная Q_A-алгебра. Если элемент $b \in B$ цел над A, то все коэффициенты его минимального многочлена над полем Q_A целы над A.

Доказательство. Поскольку b цел над A, он аннулируется приведённым многочленом $f \in A[x]$, который делится в $Q_A[x]$ на минимальный многочлен элемента b над полем Q_A. Поэтому все коэффициенты минимального многочлена целы над A в силу сл. 9.1 на стр. 128. □

Следствие 9.5
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 $A[x]$. □

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

Элементы $a_1,\dots,a_m \in A$ называются *алгебраически независимыми* над $\Bbbk$, если гомоморфизм вычисления $\mathrm{ev}_{(a_1,\dots,a_m)} : \Bbbk[x_1,\dots,x_m] \to A$, $f \mapsto f(a_1,\dots,a_m)$ инъективен, т. е. на элементы $a_1,\dots,a_m$ нет нетривиальных полиномиальных соотношений. В этом случае гомоморфизм вычисления 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 на элементах a_i.

[1] Напомню, что кольцо называется *факториальным*, если в нём нет делителей нуля, каждый необратимый элемент является произведением конечного числа неприводимых, и если $p_1\dots p_n = q_1\dots q_m$, где все p_i и q_j неприводимы, то $m = n$ и после надлежащей перенумерации $p_i = s_iq_i$, где все s_i обратимы. Поля, кольца главных идеалов и кольца многочленов с коэффициентами в факториальном кольце факториальны. См. лекцию http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_05.pdf.

[2] Т. е. без делителей нуля.

Элементы $a_1, \dots, a_m \in A$ называются *алгебраически порождающими* A над $\Bbbk$, если каждый элемент алгебры A алгебраичен над $\Bbbk(a_1, \dots, a_m)$. В этом случае поле Q_A тоже алгебраично над $\Bbbk(a_1, \dots, a_m)$, так как целое замыкание $\Bbbk(a_1, \dots, a_m)$ в Q_A является полем по предл. 9.2 на стр. 128 и содержит A, а значит, и Q_A.

Алгебраически независимый набор элементов $a_1, \dots, a_m$ алгебры A, алгебраически порождающий A над $\Bbbk$, называется *базисом трансцендентности* алгебры 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 $a_1, \dots, a_m$, что алгебра A алгебраична над $\Bbbk(a_1, \dots, a_m)$, либо как максимальный по включению алгебраически независимый набор. Доказательство того, что все базисы трансцедентности состоят из одинакового числа элементов совершенно аналогично доказательству оответствующей теоремы о базисах векторных пространств.

Лемма 9.2 (о замене)
Если $b_1, \dots, b_n \in A$ алгебраически независимы, а $a_1, \dots, a_m \in A$ 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 $\Bbbk(a_1, \dots, a_m)$, имеется содержащее b_1 полиномиальное соотношение $f(b_1, a_1, \dots, a_m) = 0$, и так как b_1 трансцендентен над $\Bbbk$, в это соотношение входит какое-нибудь a_i. Перенумеруем a_i так, чтобы это было a_1. Тогда алгебра A алгебраична 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 полем $\Bbbk(b_1, \dots, b_k, a_{k+1}, \dots, a_m)$, имеется содержащее b_{k+1} полиномиальное соотношение

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

Так как $b_1, \dots, b_n$ алгебраически независимы над $\Bbbk$, в это соотношение входит какое-нибудь a_i. Поэтому $m > k$, и после надлежащей перенумерации можно считать, что в последнем соотношении участвует элемент a_{k+1}. Тогда этот элемент, а с ним и вся алгебра A алгебраичны над полем $\Bbbk(b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_m)$, что воспроизводит индуктивное предположение. □

Следствие 9.6 (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 9.3
Число элементов в базисе трансцендентности конечно порождённой алгебры A над $\Bbbk$ называется *степенью трансцендентности* этой алгебры и обозначается $\operatorname{tr\,deg}_{\Bbbk} A$.

Пример 9.6 (теорема Люрота)
Степень трансцендентности любой отличной от поля $\Bbbk$ подалгебры $A \subset \Bbbk(t)$ в поле рациональных функций $\Bbbk(t)$ равна единице. В самом деле, если $\psi = f(t)/g(t) \in A \smallsetminus \Bbbk$, то элемент t алгебраичен над наименьшим содержащим ψ подполем $\Bbbk(\psi) \subset \mathbb{Q}_A$, ибо удовлетворяет уравнению $\psi \cdot g(x) - f(x) = 0$ с коэффициентами в $\Bbbk(\psi)$.

Упражнение 9.7. Убедитесь, что многочлен $\psi \cdot g(x) - f(x)$ отличен от нуля в $\Bbbk(\psi)[x]$.

Поэтому ψ трансцендентен над $\Bbbk$ (иначе t был бы алгебраичен над $\Bbbk$), и поле $\Bbbk(t)$ алгебраично над полем $\Bbbk(\psi)$, причём последнее поле изоморфно полю рациональных функций. Это наблюдение известно как *теорема Люрота*.

Ответы и указания к некоторым упражнениям

Упр. 9.1. Будучи подмодулем в поле, модуль $\mathcal{O}_K$ не имеет кручения и, стало быть, свободен. Его ранг не выше d, поскольку любые $d+1$ векторов из $\mathcal{O}_K$ 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 в $\mathcal{O}_K$. Поэтому ранг $\mathcal{O}_K$ не меньше d. Всякий базис модуля $\mathcal{O}_K$ над $\mathbb{Z}$ одновременно является базисом K над $\mathbb{Q}$, и в таком базисе оператор умножения на любой элемент $\zeta \in \mathcal{O}_K$ записывается целочисленной матрицей, ибо умножение на ζ переводит $\mathcal{O}_K$ в себя.

Упр. 9.2. Если $\mathbb{Q}[\sqrt{d_1}] \simeq \mathbb{Q}[\sqrt{d_2}]$, то $d_2 = (a + b\sqrt{d_1})^2 = a^2 + d_1 b^2 + 2ab\sqrt{d_1}$ для некоторых $a, b \in \mathbb{Q}$, откуда $ab = 0$ и $a^2 + d_1 b^2 = d_2$, что возможно только при $a = 0$, $b = 1$, $d_1 = d_2$.