§1. Целые, алгебраические и трансцендентные элементы

Всюду этом курсе слово «кольцо» по умолчанию означает коммутативное кольцо с единицей[1], а «$\Bbbk$-алгебра» — коммутативную ассоциативную алгебру[2] с единицей над полем $\Bbbk$.

1.1. Расширения колец. Пусть кольцо A является подкольцом кольца B, и у этих колец общая единица. Мы будем называть такую пару $A \subset B$ *расширением колец*. Например, поле $\mathbb{Q}$ является расширением кольца $\mathbb{Z} \subset \mathbb{Q}$. Из всякого кольца A можно изготовить кольцо многочленов[3] $A[x]$, куда A вложено в качестве подкольца констант (многочленов нулевой степени и нулевого многочлена). Таким образом, кольцо $A[x]$ является расширением кольца A. Для любого многочлена $f \in A[x]$ можно построить кольцо $A[x]/(f)$ вычетов по модулю[4] f. Если старший коэффициент многочлена f не делит нуль в кольце A, то для любого многочлена $g \in A[x]$ старший коэффициент произведения fg равен произведению старших коэффициентов многочленов f и g, откуда $\deg(fg) = \deg f + \deg g$. В этом случае степени всех ненулевых многочленов из идеала (f) не меньше, чем у f, и если $\deg f > 0$, то никакие две различные константы не сравнимы по модулю f. Таким образом, для отличного от константы многочлена $f \in A[x]$, старший коэффициент которого не является делителем нуля в A, кольцо A вкладывается в кольцо вычетов $A[x]/(f)$ в качестве классов констант, т. е. кольцо $A[x]/(f)$ является расширением кольца A.

Упражнение 1.1. Опишите факторкольца $A[x]/(f)$ для а) $A = \mathbb{Z}/(6)$, $f = 3x^2$ б) $A = \mathbb{Z}/(6)$, $f = 2x^3 + 1$ в) $A = \mathbb{Z}$, $f = 5x - 1$ и выясните, вкладывается ли в них кольцо A по правилу $a \mapsto [a]_f$.

Расширения вида $A \subset A[x]/(f)$, где $f \in A[x]$ — приведённый[5] многочлен, называются *примитивными*. Примитивное расширение $B = A[x]/(f)$ кольца A замечательно тем, что многочлен f имеет в кольце B корень. А именно, класс $\vartheta = [x]_f$ одночлена x по модулю многочлена $f = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ таков, что

$$f(\vartheta) = a_0 + a_1[x]_f + \ldots + a_{n-1}[x]_f^{n-1} = [a_0 + a_1x + \ldots + a_{n-1}x^{n-1}]_f = [f]_f = 0\,.$$

В частности, многочлен f делится в кольце $B[x]$ на линейный двучлен $x - \vartheta$.

Упражнение 1.2. Пусть $f \in A[x]$ — приведённый многочлен положительной степени. Убедитесь, что каждый многочлен $g \in A[x]$ однозначно представляется в виде $g = fh + r$, где $h, r \in A[x]$ и $\deg r < \deg f$.

Из упражнения вытекает, что в каждом классе $[g]_f = g + (f)$ имеется единственный представитель $r \in [g]_f$ степени $\deg r < \deg f$. Поэтому каждый элемент примитивного расширения $B = A[x]/(f)$ однозначно записывается в виде

$$[a_0 + a_1x + \ldots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}\,,\ \text{где } \vartheta = [x]_f,\ a_i \in A,\ n = \deg f\,.$$

Элементы $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1} \in B$ складываются и перемножаются по стандартным правилам раскрытия скобок и приведения подобных слагаемых с учётом соотношения $f(\vartheta) = 0$.

[1] См. раздел 1.1 на с. 22 лекций [Алг 1].
[2] См. Пример 4.5 на с. 72 лекций [Алг 1].
[3] См. раздел 2.1 на с. 38 лекций [Алг 1].
[4] Ср. с разделом 2.3.1 на с. 44 лекций [Алг 1].
[5] Т. е. со старшим коэффициентом 1.

По этой причине кольцо $B = A[x]/(f)$ иногда обозначают «$A[\vartheta]$, где $f(\vartheta) = 0$». Например, расширение $\mathbb{Q}[x]/(x^2 - 5)$ поля $\mathbb{Q}$ обычно обозначают $\mathbb{Q}[\sqrt{5}]$, где $\sqrt{5}$ — это класс переменной x по модулю многочлена $x^2 - 5$. Он удовлетворяет равенству $\sqrt{5} \cdot \sqrt{5} = 5$ (проверьте!), а всё кольцо $\mathbb{Q}[\sqrt{5}]$ состоит из элементов вида $a + b\sqrt{5}$ с $a, b \in \mathbb{Q}$, которые складываются и перемножаются по обычным правилам раскрытия скобок с учётом соотношения $\sqrt{5} \cdot \sqrt{5} = 5$:

$$(a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + (b + d)\sqrt{5}$$
$$(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (cb + ad)\sqrt{5}\,.$$

Упражнение 1.3. Проверьте, что кольцо $\mathbb{Q}[\sqrt{5}]$ является полем.

Лемма 1.1
Для любого кольца A и любого приведённого многочлена $f \in A[x]$ положительной степени существует такое расширение колец $A \subset B$, что многочлен f раскладывается в $B[x]$ в произведение $\deg f$ приведённых линейных множителей (не обязательно различных), причём кольцо B можно получить из A конечным числом последовательных примитивных расширений.

Доказательство. Индукция по $\deg f$. Если $\deg f = 1$, то доказывать нечего. Если $\deg f > 1$, то f имеет корень $\vartheta = [x]_f$ в примитивном расширении $C = A[x]/(f) \supset A$, и в кольце $C[x]$ многочлен f раскладывается в произведение $f(x) = (x - \vartheta)\, f_1(x)$, где $f_1 \in C[x]$ тоже приведён и $\deg f_1 = \deg f - 1$. По индукции, существует такое расширение $C \subset B$, получающееся из C последовательными примитивными расширениями, что многочлен f_1 является в $B[x]$ произведением $\deg f_1$ линейных приведённых двучленов. □

1.2. Целые элементы. Покажем, что следующие три свойства элемента $b \in B$ в расширении колец $A \subset B$ эквивалентны друг другу:

(1) b является корнем приведённого многочлена из $A[x]$

(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 M не аннулируется умножением ни на какой ненулевой элемент[1] из B.

Элементы $b \in B$, обладающие этими свойствами, называются *целыми* над A.

В самом деле, свойство (1) равносильно тому, что некоторая степень элемента b линейно выражается через меньшие степени с коэффициентами из A, т. е.

$$b^m = a_1\, b^{m-1} + \ldots + a_{m-1}\, b + a_m$$

для некоторых $m \in \mathbb{N}$ и $a_1, \ldots, a_m \in A$, откуда сразу следует свойство (2). Если выполнено свойство (2), то A-линейная оболочка всех целых неотрицательных степеней элемента b удовлетворяет свойству (3), поскольку конечно порождена и содержит единицу $b^0 = 1$. Ну а если

[1] Такие модули называются *B-точными* (по-английски *faithful*).

выполняется свойство (3), и элементы $e_1, \dots, e_m \in M$ линейно порождают M, то A-линейный оператор умножения на b: $M \to M$, $m \mapsto bm$, действует на эти образующие по правилу

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

где $Y \in \mathrm{Mat}_m(A)$ — квадратная матрица с элементами из A. Из 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[1], вытекает, что образ оператора умножения на $\det X$ содержится в линейной оболочке столбцов матрицы X. Поэтому модуль $\det(bE - Y)\,M$ содержится в линейной оболочке векторов $(e_1, \dots, e_m) \cdot (bE - Y)$, нулевой в силу соотношения (1-1). Из равенства $\det(bE - Y)\,M = 0$ и B-точности модуля M вытекает, что $\det(bE - Y) = 0$. Так как все элементы матрицы Y лежат в A, её характеристический многочлен $\chi_Y(x) = \det(xE - Y)$ лежит в $A[x]$. Он приведён, и b является его корнем.

Определение 1.1 (целое замыкание)
Множество всех целых над A элементов кольца $B \supset A$ называется *целым замыканием* подкольца A в B. Если оно совпадает с A, кольцо A называется *целозамкнутым* в B. Если оно совпадает с B, кольцо B называется *целым расширением* кольца A или *целой A-алгеброй*.

Пример 1.1 (целозамкнутость факториального кольца в поле частных)
Покажем, что каждое факториальное[2] кольцо A целозамкнуто в своём поле частных[3] $Q_A \supset A$. Если многочлен $a_0 t^m + \dots + a_{m-1} t + a_m \in A[t]$ аннулирует дробь $p/q \in Q_A$ с нод$(p, q) = 1$, то $a_0 p^m + a_1 q p^{m-1} + \dots + a_{m-1} q^{m-1} p + a_m q^m = 0$, откуда $q \mid a_0$, и если $a_0 = 1$, то q обратим, и $p/q \in A$. В частности, кольцо $\mathbb{Z}$ целозамкнуто в поле $\mathbb{Q}$, а кольцо $\Bbbk[x]$, где $\Bbbk$ — любое поле, целозамкнуто в поле $\Bbbk(x)$.

Пример 1.2 (инварианты действия конечной группы)
Если конечная группа G действует на кольце B кольцевыми автоморфизмами, то B цело над *подкольцом инвариантов* $B^G \stackrel{\text{def}}{=} \{\, a \in B \mid ga = a \ \ \forall\, g \in G \,\}$, поскольку каждый элемент $b \in B$ является корнем приведённого многочлена $B(t) = \prod_{\beta \in Gb} (t - \beta)$, где произведение берётся по всем различным элементам β из G-орбиты Gb элемента b, и коэффициенты этого многочлена, будучи симметрическими многочленами от элементов G-орбиты, G-инвариантны.

Предложение 1.1
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.

[1] Т. е. транспонированная к матрице алгебраических дополнений элементов матрицы X, см. раздел 8.4 на с. 138 лекций [Алг 1].

[2] См. раздел 4.4 на с. 74 лекций [Алг 1].

[3] См. раздел 3.1 на с. 55 лекций [Алг 1].

Аналогично, если $z_0^r = z_1 z_0^{r-1} + \cdots + z_{r-1} z_0 + z_r$, где каждый z_k с $k > 0$ удовлетворяет равенству

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

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 1.1 (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[1], 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 1.2
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 $a^{-m} = \alpha_1 a^{1-m} + \cdots + \alpha_{m-1} a^{-1} + \alpha_0$, 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 1.3 (целые алгебраические числа)
Пусть поле $K \supset \mathbb{Q}$ конечномерно как векторное пространство над $\mathbb{Q}$. Элементы таких полей называются *алгебраическими числами*. По предл. 1.1 целые над $\mathbb{Z}$ алгебраические числа образуют в поле K подкольцо. Оно называется *кольцом целых* поля K и обозначается $\mathcal{O}_K$. Если число $\vartheta \in \mathcal{O}_K$ является корнем приведённого многочлена $f \in \mathbb{Z}[x]$, то f делится в $\mathbb{Q}[x]$ на минимальный многочлен[2] $\mu_\vartheta \in \mathbb{Q}[x]$ числа ϑ над $\mathbb{Q}$. По сл. 1.1 коэффициенты многочлена μ_ϑ целы над $\mathbb{Z}$, а поскольку $\mathbb{Z}$ целозамкнуто в $\mathbb{Q}$, они лежат в $\mathbb{Z}$. Мы заключаем, что минимальный над полем $\mathbb{Q}$ многочлен целого алгебраического числа имеет целые коэффициенты. Характеристический многочлен[3] $\chi_\vartheta \in \mathbb{Q}[x]$ оператора умножения $\vartheta\colon K \to K$, $x \mapsto \vartheta x$, на алгебраическое число $\vartheta \in K$ имеет в поле $\mathbb{C}$ те же корни, что и минимальный многочлен[4] μ_ϑ. Если $\vartheta \in \mathcal{O}_K$, то

[1] См. лем. 1.1 на стр. 4.
[2] Т. е. приведённый многочлен наименьшей степени с коэффициентами в $\mathbb{Q}$, зануляющийся на элементе ϑ, см. раздел 5.7.2 на с. 72 лекций [Гео 1] или n° 1.3 на стр. 8 ниже.
[3] См. раздел 9.1.4 на с. 146 лекций [Алг 1].
[4] См. разделы 9.1.4-9.1.5 на с. 146-147 лекций [Алг 1].

$\mu_\vartheta \in \mathbb{Z}[x]$, и стало быть, все эти корни целы над $\mathbb{Z}$. Поэтому все коэффициенты характеристического многочлена целого алгебраического числа целы над $\mathbb{Z}$ и, будучи рациональными числами, лежат в $\mathbb{Z}$. В частности определитель $\det\vartheta$ и след $\operatorname{tr}\vartheta$ оператора умножения на целое алгебраическое число $\vartheta \in \mathcal{O}_K$ лежат в $\mathbb{Z}$. Они называются *нормой* и *следом* алгебраического числа ϑ и обозначаются $N(\vartheta) \stackrel{\text{def}}{=} \det\vartheta$ и $\operatorname{Sp}(\vartheta) \stackrel{\text{def}}{=} \operatorname{tr}\vartheta$.

Поскольку целые неотрицательные степени ξ^m любого числа $\xi \in K$ линейно зависимы над $\mathbb{Q}$, каждое алгебраическое число ξ удовлетворяет уравнению $a_0\xi^n + \ldots + a_{n-1}\xi + a_n = 0$ с коэффициентами $a_i \in \mathbb{Z}$. Так как число $\zeta = a_0\xi$ удовлетворяет уравнению

$$\zeta^n + a_1\zeta^{n-1} + a_0a_2\zeta^{n-2} + \ldots + a_0^{n-1}a_n = 0\,,$$

оно цело над $\mathbb{Z}$, т. е. подходящее целое кратное любого алгебраического числа цело над $\mathbb{Z}$. Мы заключаем, что каждое конечномерное над $\mathbb{Q}$ поле $K \supset \mathbb{Q}$ является полем частных своего кольца целых $\mathcal{O}_K$, и для любого базиса $e_1, \ldots, e_d$ поля K как векторного пространства над $\mathbb{Q}$ существует такое $n \in \mathbb{N}$, что все $ne_i \in \mathcal{O}_K$. Таким образом, поле K имеет базис из целых алгебраических чисел.

Целые алгебраические числа образуют модуль над кольцом $\mathbb{Z}$. Покажем, что он изоморфен $\mathbb{Z}^n$, где $n = \dim_{\mathbb{Q}} K$. Для этого рассмотрим *билинейную форму следа* $\operatorname{sp}: K\times K \to \mathbb{Q}$, значение которой на элементах $\xi, \vartheta \in K$ равно следу $\operatorname{tr}(\xi\vartheta)$ оператора умножения на $\xi\vartheta\colon K \to K, x \mapsto \xi\vartheta x$.

Упражнение 1.4. Убедитесь, что форма sp симметрична и невырождена[1].

Пусть целые элементы $e_1, \ldots, e_n \in \mathcal{O}_K$ образуют базис поля K над $\mathbb{Q}$, а $e_1^\times, \ldots, e_n^\times \in K$ — двойственный к нему базис относительно формы следа[2]. Произвольный элемент $\vartheta \in K$ раскладывается по второму базису как [формулой]13.2175 $\vartheta = \sum_{i+1}^n \operatorname{sp}(e_i, \vartheta)e_i^\times$. Так как $e_i \in \mathcal{O}_K$ и для любого $\vartheta \in \mathcal{O}_K$ след произведения $\vartheta e_i \in \mathcal{O}_K$ лежит в $\mathbb{Z}$, мы заключаем, что $\mathcal{O}_K$ содержится в свободном $\mathbb{Z}$-модуле с базисом $e_1^\times, \ldots, e_n^\times$. Поэтому он своден и имеет ранг не выше n. А так как векторы $e_1, \ldots, e_n \in \mathcal{O}_K$ линейно независимы над $\mathbb{Q}$, а значит, и над $\mathbb{Z}$, ранг $\operatorname{rk}_{\mathbb{Z}} \mathcal{O}_K = n$.

Обратите внимание, что всякий базис модуля $\mathcal{O}_K$ над $\mathbb{Z}$ одновременно является базисом векторного пространства K над $\mathbb{Q}$, и умножение на любой элемент $\vartheta \in \mathcal{O}_K$ записывается в этом базисе целочисленной матрицей. Именно так целые алгебраические числа и были впервые определены Дедекиндом в XIX веке: как числа $\vartheta \in K$, умножение на которые записывается целочисленной матрицей в подходящем базисе поля K над $\mathbb{Q}$.

Пример 1.4 (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 1.5. Покажите, что $\mathbb{Q}[\sqrt{d_1}] \not\simeq \mathbb{Q}[\sqrt{d_2}]$ для свободных от квадратов $d_1 \neq d_2$.

[1] См. раздел 13.2 на с. 173 лекций [Гео 1].

[2] Это означает, что $\operatorname{sp}(e_i, e_j^\times) = \delta_{ij}$, см. раздел 13.2.1 на с. 175 лекций [Гео 1].

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

Пусть число $\xi = a+b\sqrt{d}$, где $a, b \in \mathbb{Q}$, цело над $\mathbb{Z}$. Обозначим через $s = \mathrm{Sp}(\xi) = \operatorname{tr}\xi$ и $n = N(\xi) = \det\xi$ его след и норму, т. е. след и определитель оператора умножения на ξ в поле $K = \mathbb{Q}[\sqrt{d}]$. В прим. 1.3 выше мы видели, что $t, n \in \mathbb{Z}$. 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 1.6. Убедитесь, что $(1+\sqrt{d})/2 \in \mathcal{O}_K$ при $d \equiv 1 \pmod 4$.

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 $d \equiv 2 \pmod 4$, то $t^2 \equiv 2s^2 \pmod 4$, а если $d \equiv 3 \pmod 4$, то $t^2 + s^2 \equiv 0 \pmod 4$. В обоих случаях числа t и s чётны, и $\xi = a + b\sqrt{d}$ имеет $a, b \in \mathbb{Z}$. Так как $\sqrt{d} \in O_K$, 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.

1.3. Конечно порождённые алгебры над полем. Пусть $\Bbbk$ — произвольное поле. Расширения $\Bbbk \subset B$, где B — коммутативное кольцо, называются *коммутативными $\Bbbk$-алгебрами*[1]. Такая $\Bbbk$-алгебра B называется *конечно порожденной*, если существует эпиморфизм $\Bbbk$-алгебр

$$\pi : \Bbbk[x_1, \dots, x_m] \twoheadrightarrow B.$$

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* $\mathrm{ev}_b : \Bbbk[x] \to B$, $f \mapsto f(b)$, имеет ненулевое ядро, т. е. $f(b) = 0$ для какого-нибудь ненулевого $f \in \Bbbk[x]$. Такие элементы b обычно называют *алгебраическими* над $\Bbbk$. 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. Если же 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[2] в $\Bbbk[x]$.

Упражнение 1.7. 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) $\Bbbk[b]$

[1] Иначе говоря, коммутативная $\Bbbk$-алгебра — это векторное пространство B над $\Bbbk$ с билинейным умножением $B \times B \to B$, которое ассоциативно и коммутативно, см. раздел 5.2 на с. 90 лекций [Алг 1].

[2] См. предложение 2.5 на с. 45 лекций [Алг 1].

является полем б) $\Bbbk[b]$ не имеет делителей нуля в) μ_b неприводим в $\Bbbk[x]$.

Теорема 1.1
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. 1.7 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. 1.1 на стр. 5. 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. 1.2 подалгебра F является полем. Покажем, что элемент $1 + p(b_m) \in F$ не обратим в F. Пусть это не так, и

$$\big(1 + p(b_m)\big)\, g\big(b_m, 1/p(b_m)\big) = 1 \tag{1-2}$$

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 (1-2) на $p^k(b_m)$, мы получим на b_m полиномиальное уравнение $h(b_m)\,(1 + p(b_m)) = p^k(b_m)$. Оно нетривиально, поскольку $h(1 + p) = h + hp$ не делится на p в $\Bbbk[x]$. □

Пример 1.5 (конечные расширения полей)
Если $\Bbbk$-алгебра A конечномерна как векторное пространство над $\Bbbk$, то каждый элемент $\xi \in A$ алгебраичен[1] над $\Bbbk$, так как бесконечное множество целых неотрицательных степеней ξ^k линейно зависимо. Поэтому алгебра A цела[2] над $\Bbbk$. Если в ней нет делителей нуля, то A является полем по предл. 1.2 на стр. 6. Конечномерные как векторные пространства над $\Bbbk$ поля $\mathbb{F} \supset \Bbbk$ называются *конечными расширениями* поля $\Bbbk$. Размерность конечного расширения $\mathbb{F}$ поля $\Bbbk$ как векторного пространства над $\Bbbk$ называется *степенью* расширения $\mathbb{F} \supset \Bbbk$ и обозначается $\deg \mathbb{F}/\Bbbk$ или $[\mathbb{F} : \Bbbk]$.

Упражнение 1.8. Пусть в башне расширений колей $\Bbbk \subset \mathbb{K} \subset \mathbb{F}$ элементы $f_1, \dots, f_m \in \mathbb{F}$ составляют базис $\mathbb{F}$ как векторного пространства над $\mathbb{K}$, а $t_1, \dots, t_n \in \mathbb{K}$ — базис $\mathbb{K}$ над $\Bbbk$. Покажите, что mn произведений $f_i t_j$ образуют базис $\mathbb{F}$ над $\Bbbk$, откуда $\deg \mathbb{F}/\Bbbk = \deg \mathbb{F}/\mathbb{K} \cdot \deg \mathbb{K}/\Bbbk$.

Предложение 1.3
Всякое поле $\mathbb{F}$, являющееся конечно порождённой алгеброй над подполем $\Bbbk \subset \mathbb{F}$, является конечным расширением поля $\Bbbk$.

[1] См. n° 1.3 на стр. 8.
[2] См. опр. 1.1 на стр. 5.

Доказательство. Индукция по числу образующих. Если $\mathbb{F}$ порождается над $\Bbbk$ одним элементом a, то a алгебраичен, а $\mathbb{F} = \Bbbk[x]/(\mu_a)$, где $\mu_a \in \Bbbk[x]$ — минимальный многочлен элемента a, и размерность $\mathbb{F}$ над $\Bbbk$ равна $\deg \mu_a$. Пусть $\mathbb{F}$ порождается n элементами $a_1, \dots, a_m$. Поскольку все элементы поля $\mathbb{F}$ алгебраичны над $\Bbbk$, поле $\mathbb{F}$ цело над $\Bbbk$, а значит и над подалгеброй $\mathbb{L} = \Bbbk[a_2, \dots, a_n] \subset \mathbb{F}$, порождённой над $\Bbbk$ элементами $a_2, \dots, a_n$. По предл. 1.2 на стр. 6 эта подалгебра — поле. По индукции расширение $\Bbbk \subset \mathbb{L}$ конечно. Так как $\mathbb{F}$ порождается над $\mathbb{L}$ одним элементом a_1, расширение $\mathbb{L} \subset \mathbb{F}$ тоже конечно. По упр. 1.8 $\mathbb{F}$ конечномерно над $\Bbbk$. □

Следствие 1.2
Любая конечно порождённая $\Bbbk$-подалгебра любого конечного расширения $\mathbb{F} \supset \Bbbk$ является полем конечной степени над $\Bbbk$, делящей степень $\deg \mathbb{F}/\Bbbk$. □

1.4. 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 $\mathrm{ev}_{(a_1,\dots,a_m)} \colon \Bbbk[x_1, \dots, x_m] \to A$, $f \mapsto f(a_1, \dots, a_m)$ 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.

Элементы $a_1, \dots, a_m \in A$ называются *трансцендентно 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. 1.2 на стр. 6 и содержит A, а значит, по универсальному свойству поля частных[1], и Q_A.

Алгебраически независимый набор элементов $a_1, \dots, a_m$ алгебры A, трансцендентно 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 минимальный по включению трансцендентно порождающий набор, либо как максимальный по включению алгебраически независимый набор. Доказательство того, что все базисы трансцендентности состоят из одинакового числа элементов совершенно аналогично доказательству соответствующей теоремы о базисах векторных пространств.

Лемма 1.2 (о замене)
Если $b_1, \dots, b_n \in A$ алгебраически независимы, а $a_1, \dots, a_m \in A$ трансцендентно 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 трансцендентно 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 $b_1, \dots, b_k, a_{k+1}, \dots, a_m$ трансцендентно 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

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

[1] См. Пример 3.2 на с. 56 лекций [Алг 1].

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

Определение 1.2
Число элементов в базисе трансцендентности конечно порождённой алгебры A над $\Bbbk$ называется *степенью трансцендентности* этой алгебры и обозначается $\operatorname{tr\,deg}_{\Bbbk} A$.

Пример 1.6 (подалгебры поля рациональных функций)
Степень трансцендентности любой строго большей, чем поле $\Bbbk$ подалгебры $A \subset \Bbbk(t)$ в поле рациональных функций $\Bbbk(t)$ равна единице. В самом деле, если $\psi = f(t)/g(t) \in A \smallsetminus \Bbbk$ и $f, g \in \Bbbk[t]$ взаимно просты, то элемент t алгебраичен над наименьшим содержащим ψ подполем $\Bbbk(\psi) \subset \Bbbk(t)$, ибо удовлетворяет уравнению $\psi \cdot g(x) - f(x) = 0$ с коэффициентами в $\Bbbk(\psi)$. Поэтому ψ трансцендентен над $\Bbbk$ (иначе t был бы алгебраичен над $\Bbbk$), и поле $\Bbbk(\psi)$ само по себе изоморфно полю рациональных функций.

Упражнение 1.9. Убедитесь, что многочлен $\psi \cdot g(x) - f(x)$ неприводим в $\Bbbk(\psi)[x]$ и тем самым является минимальным многочленом элемента t над $\Bbbk(\psi)$.

Мы заключаем, что поле $\Bbbk(t)$ является конечным расширением поля $\Bbbk(\psi)$ степени

$$[\Bbbk(t) : \Bbbk(\psi)] = \max(\deg f, \deg g),$$

равной максимуму степеней числителя и знаменателя несократимого представления $\psi = f/g(t)$ с $f, g \in \Bbbk[t]$.

Теорема 1.2 (теорема Люрота)
Для любого поля $\Bbbk$ всякое строго содержащее его подполе $\Bbbk \subsetneq \mathbb{K} \subset \Bbbk(t)$ поля рациональных функций само изоморфно полю рациональных функций $\Bbbk(x)$.

Доказательство. Из предыдущего прим. 1.6 вытекает, что элемент t алгебраичен над $\mathbb{K}$. Обозначим через

$$f(x,t) = x^n + a_1 x^{n-1} + \dots + a_n \in \mathbb{K}[x], \quad \text{где} \quad a_\nu \in \Bbbk(t), \tag{1-3}$$

его минимальный многочлен над $\mathbb{K}$, а через $d \in \Bbbk[t]$ — наименьший общий знаменатель всех коэффициентов a_ν. Многочлен $\tilde{f}(x,t) = df$ лежит в $\Bbbk[t][x]$ и имеет содержание[1] 1 как многочлен от x с коэффициентами в факториальном кольце $\Bbbk[t]$, а его степень по t равна максимальной из степеней многочленов $da_\nu \in \Bbbk[t]$. Пусть она равна $m = \deg da_i$ и $a_i = b/c$, где $b, c \in \Bbbk[t]$ взаимно просты. Покажем, что $m = n$.

[1] Напомню, что *содержанием* многочлена над факториальным кольцом (в данном случае над $\Bbbk[t]$) называется наибольший общий делитель всех его коэффициентов, см. раздел 4.5 на с. 78 лекций [Алг 1].

Поскольку элемент t является корнем многочлена $a_i(t)c(x) - b(x) \in \Bbbk(a_i)[x] \subset \mathbb{K}[x]$, этот многочлен делится в $\mathbb{K}[x]$ на минимальный многочлен (1-3) элемента t, т. е.

$$a_i(t)c(x) - b(x) = f(x,t)\,q(x)$$

для некоторого $q(x) \in \mathbb{K}[x]$. Умножая обе части этого равенства на $c(t) \in \Bbbk[t]$, получаем

$$b(t)c(x) - b(x)c(t) = f(x,t)q(x)c(t)\,.$$

Так как в $\Bbbk(t)[x]$ многочлен $f \in \Bbbk(t)[x]$ делится на $\tilde{f} = df \in \Bbbk[t][x]$, левая часть этого равенства, лежащая в $\Bbbk[t][x]$, делится на $\tilde{f}$ в $\Bbbk(t)[x]$, а значит, и в $\Bbbk[t][x]$, так как содержание $\tilde{f}$ равно 1. Стало быть, существует такой многочлен $g(x,t) \in \Bbbk[x,t]$, что

$$b(t)c(x) - b(x)c(t) = \tilde{f}(x,t)g(x,t)$$

в $\Bbbk[x,t]$. Так как степень левой части по t не превышает m, а степень $\tilde{f}$ по t в точности равна m, многочлен g не зависит от t и лежит в $\Bbbk[x]$, а так как $c(x)$ и $b(x)$ взаимно просты в $\Bbbk[x]$, многочлен g не зависит и от x, т. е. является константой из $\Bbbk$. Мы заключаем, что $\tilde{f}(x,t)$ знакопеременен по x и t, а значит, имеет по ним одинаковую степень $n = m$.

Далее, в прим. 1.6 мы видели, что $\deg \Bbbk(t)/\Bbbk(a_i) = \max(\deg b, \deg c)$. Поэтому

$$\deg \Bbbk(t)/\Bbbk(a_i) \leqslant \deg da_i = m = n = \deg \Bbbk(t)/\mathbb{K}\,,$$

и поскольку $\Bbbk(a_i) \subset \mathbb{K}$, мы заключаем, что $\Bbbk(a_i) = \mathbb{K}$. □

Упражнение 1.10. Покажите, что $\mathbb{K} = \Bbbk(a_v)$ для любого отличного от константы коэффициента многочлена (1-3).

Ответы и указания к некоторым упражнениям

Упр. 1.2. Модифицируйте рассуждение из доказательства см. Предложения 2.2 на с. 41 лекций [Алг 1].

Упр. 1.3. Обратным элементом к произвольному ненулевому $a + b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ является $\frac{a}{a^2-5b^2} - \frac{b}{a^2-5b^2}\sqrt{5}$.

Упр. 1.4. Первое очевидно, второе вытекает из того, что $\operatorname{sp}(\vartheta, \vartheta^{-1}) = \operatorname{tr}(1) = \dim_{\mathbb{Q}} K$ для любого $\vartheta \neq 0$.

Упр. 1.5. 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 $a = 0$, $b = 1$, $d_1 = d_2$.

Упр. 1.9. Многочлен $x_1\, g(x_2) - f(x_2) \in \Bbbk[x_1, x_2]$ от независимых переменных x_1, x_2 неприводим в $\Bbbk[x_1, x_2]$. Поскольку ψ трансцендентен, кольцо $\Bbbk[x_1, x_2]$ изоморфно кольцу $\Bbbk[\psi][x]$ посредством гомоморфизма $x_1 \mapsto \psi$, $x_2 \mapsto x$, переводящего многочлен $x_1\, g(x_2) - f(x_2) \in \Bbbk[x_1, x_2]$ в многочлен $\psi \cdot g(x) - f(x)$, тем самым неприводимый в $\Bbbk[\psi][x]$. По лемме Гаусса[1], он будет неприводим и в $\Bbbk(\psi)[x]$.

[1] См. Следствие 4.5 на с. 78 лекций [Алг 1].