

А. Л. Городенцев*

Теория Галуа

Теория Галуа изучает связь между алгебраическими расширениями полей и группами их симметрий. Она является исторической прародительницей значительной части современной алгебры (коммутативная алгебра, линейная алгебра, теория групп) и фундаментальной идеи привлечения групп симметрий для классификации и описания свойств самых разных математических объектов (Эрлангенская программа Ф. Клейна в геометрии, дифференциальная теория Галуа в анализе и т. п.). Теория Галуа является важным инструментом в современной теории чисел, алгебраической и диофантовой геометрии. Предлагаемый курс является доступным для начинающих введением в классическую теорию Галуа и служит идейным прологом для дальнейших занятий всеми перечисленными дисциплинами. Для его понимания достаточно владения алгеброй и геометрией в объеме первого года бакалавриата, например, моими курсами <http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2526/list.html> и http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/list.html, на записки лекций которых мы будем далее ссылаться как [Алг 1] и [Гео 1].

Факультет математики НИУ ВШЭ
осень 2026 г

* ВШЭ, ИТЭФ, НМУ, [e-mail:gorod@itep.ru](mailto:gorod@itep.ru), <http://gorod.bogomolov-lab.ru/>

Оглавление

Оглавление	2
§1 Целые, алгебраические и трансцендентные элементы	3
1.1 Расширения колец	3
1.2 Целые элементы	4
1.3 Конечно порождённые алгебры над полем	8
1.4 Базисы трансцендентности	10
§2 Алгебраические расширения полей	13
2.1 Башни примитивных расширений	13
2.2 Сепарабельные расширения	14
2.3 Продолжение гомоморфизмов	16
2.4 Поле разложения многочлена	17
2.5 Алгебраическое замыкание	18
2.6 Нормальные расширения	20
2.7 Композиты	21
Ответы и указания к некоторым упражнениям	22

§1. Целые, алгебраические и трансцендентные элементы

Всюду этом курсе слово «кольцо» по умолчанию означает коммутативное кольцо с единицей¹, а « $\mathbb{K}$ -алгебра» — коммутативную ассоциативную алгебру² с единицей над полем $\mathbb{K}$.

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 многочленов³ $A[x]$, 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 модулю⁴ 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 $f \in A[x]$ — приведённый⁵ 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 $f = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ таков, что

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

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

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

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

¹См. раздел 1.1 на с. 22 лекций [Алг 1].

²См. Пример 4.5 на с. 72 лекций [Алг 1].

³См. раздел 2.1 на с. 38 лекций [Алг 1].

⁴Ср. с разделом 2.3.1 на с. 44 лекций [Алг 1].

⁵Т. 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 $\sqrt{5} \cdot \sqrt{5} = 5$:

$$\begin{aligned}(a + b\sqrt{5}) + (c + d\sqrt{5}) &= (a + c) + (b + d)\sqrt{5} \\ (a + b\sqrt{5})(c + d\sqrt{5}) &= (ac + 5bd) + (cb + ad)\sqrt{5}.\end{aligned}$$

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. $\square$

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 элемент¹ 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.

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

для некоторых $m \in \mathbb{N}$ и $a_1, \dots, a_m \in A$, 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

¹Такие 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 $b: M \rightarrow M, t \mapsto bt$, действует на эти образующие по правилу

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

где $Y \in \text{Mat}_m(A)$ — 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 матрица¹, 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 факториальное² кольцо A целозамкнуто в своём поле частных³ $Q_A \supset A$. Если многочлен $a_0 t^m + \dots + a_{m-1} t + a_m \in A[t]$ аннулирует дробь $p/q \in Q_A$ с $\text{нод}(p, q) = 1$, 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 $\mathbb{k}[x]$, где $\mathbb{k}$ — любое поле, целозамкнуто в поле $\mathbb{k}(x)$.

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 $0 \leq i \leq m-1$ и $0 \leq j \leq n-1$ 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 .

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

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

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

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 $z_0^{j_0} z_1^{j_1} \dots z_r^{j_r}$, где $0 \leq j_0 \leq r-1$ и $0 \leq j_k \leq m_k-1$ при $k > 0$. $\square$

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 множители¹, 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 . $\square$

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

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 $b : V \rightarrow V, x \mapsto bx$, сюръективен, так как имеет нулевое ядро. Обратный к b элемент b^{-1} является прообразом единицы $1 \in V$. $\square$

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 многочлен² $\mu_\vartheta \in \mathbb{Q}[x]$ 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 многочлен³ $\chi_\vartheta \in \mathbb{Q}[x]$ оператора умножения $\vartheta : K \rightarrow K, x \mapsto \vartheta x$, на алгебраическое число $\vartheta \in K$ имеет в поле $\mathbb{C}$ те же корни, что и минимальный многочлен⁴ μ_ϑ . Если $\vartheta \in \mathcal{O}_K$, то

¹См. [лем. 1.1](#) на стр. 4.

²Т. 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 [н° 1.3](#) на стр. 8 ниже.

³См. раздел 9.1.4 на с. 146 лекций [\[Алг 1\]](#).

⁴См. 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 $a_0 \xi^n + \dots + a_{n-1} \xi + a_n = 0$ с коэффициентами $a_i \in \mathbb{Z}$. Так как число $\zeta = a_0 \xi$ удовлетворяет уравнению

$$\zeta^n + a_1 \zeta^{n-1} + a_0 a_2 \zeta^{n-2} + \dots + a_0^{n-1} a_n = 0,$$

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 $e_1, \dots, e_d$ 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* $\operatorname{sp} : K \times K \rightarrow \mathbb{Q}$, значение которой на элементах $\xi, \vartheta \in K$ равно следу $\operatorname{tr}(\xi \vartheta)$ оператора умножения на $\xi \vartheta : K \rightarrow K, x \mapsto \xi \vartheta x$.

УПРАЖНЕНИЕ 1.4. Убедитесь, что форма sp симметрична и невырождена¹.

Пусть целые элементы $e_1, \dots, e_n \in \mathcal{O}_K$ образуют базис поля K над $\mathbb{Q}$, а $e_1^\times, \dots, e_n^\times \in K$ — двойственный к нему базис относительно формы следа². 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 $e_1^\times, \dots, e_n^\times$. Поэтому он своден и имеет ранг не выше n . А так как векторы $e_1, \dots, e_n \in \mathcal{O}_K$ 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 $\zeta \in K \setminus \mathbb{Q}$ 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 квадратов³ 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 $\mathbb{Q}[\sqrt{d_1}] \neq \mathbb{Q}[\sqrt{d_2}]$ для свободных от квадратов $d_1 \neq d_2$.

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

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

³Целое 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 $s = \text{Sp}(\xi) = \text{tr } \xi$ 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 $\sqrt{d} \in \mathcal{O}_K$, 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.

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

$$\pi : \mathbb{k}[x_1, \dots, x_m] \twoheadrightarrow B.$$

В этом случае образы переменных $b_i = \pi(x_i) \in B$ называются *образующими* алгебры B , а ядро $\ker \pi \subset \mathbb{k}[x_1, \dots, x_m]$ называется *идеалом соотношений* между ними. Элемент $b \in B$ цел над полем $\mathbb{k}$ если и только если гомоморфизм вычисления $\text{ev}_b : \mathbb{k}[x] \rightarrow B, f \mapsto f(b)$, имеет ненулевое ядро, т. е. $f(b) = 0$ для какого-нибудь ненулевого $f \in \mathbb{k}[x]$. Такие элементы b обычно называют *алгебраическими* над $\mathbb{k}$. Поскольку все идеалы в $\mathbb{k}[x]$ главные, $\ker(\text{ev}_b) = (\mu_b)$, где образующая $\mu_b \in \mathbb{k}[x]$ однозначно определяется алгебраическим элементом b как приведённый многочлен наименьшей степени, аннулирующий b . Этот многочлен называется *минимальным* *многочленом* элемента b над $\mathbb{k}$. Элемент $b \in B$, не являющийся алгебраическим, называется *трансцендентным* над $\mathbb{k}$.

Обозначим через $\mathbb{k}[b] = \text{im } \text{ev}_b \subset B$ наименьшую $\mathbb{k}$ -подалгебру в B , содержащую элементы 1 и b . Если b трансцендентен, подалгебра $\mathbb{k}[b]$ изоморфна кольцу многочленов $\mathbb{k}[x]$. В частности, она бесконечномерна как векторное пространство над $\mathbb{k}$ и не является полем. Если же b алгебраичен, алгебра $\mathbb{k}[b] \simeq \mathbb{k}[x]/(\mu_b)$ имеет размерность $\deg \mu_b$ как векторное пространство над $\mathbb{k}$. Она является полем если и только если многочлен μ_b неприводим² в $\mathbb{k}[x]$.

УПРАЖНЕНИЕ 1.7. Убедитесь, что следующие три свойства алгебраического над полем $\mathbb{k}$ элемента $b \in B$ с минимальным многочленом $\mu_b \in \mathbb{k}[x]$ эквивалентны друг другу: а) $\mathbb{k}[b]$

¹Иначе говоря, коммутативная $\mathbb{k}$ -алгебра — это векторное пространство B над $\mathbb{k}$ с билинейным умножением $B \times B \rightarrow B$, которое ассоциативно и коммутативно, см. раздел 5.2 на с. 90 лекций [\[Алг 1\]](#).

²См. предложение 2.5 на с. 45 лекций [\[Алг 1\]](#).

является полем б) $\mathbb{k}[b]$ не имеет делителей нуля в) μ_b неприводим в $\mathbb{k}[x]$.

ТЕОРЕМА 1.1

Если конечно порождённая $\mathbb{k}$ -алгебра является полем, то все её элементы алгебраичны над $\mathbb{k}$.

Доказательство. Пусть алгебра B является полем и порождается над $\mathbb{k}$ 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 $\mathbb{k}$, то алгебра $\mathbb{k}[b_m]$ является полем. Тогда по предположению индукции поле B алгебраично над $\mathbb{k}[b_m]$, а значит и над $\mathbb{k}$ по [предл. 1.1](#) на стр. 5. Остаётся убедиться, что образующая b_m не может быть трансцендентна над $\mathbb{k}$. Допустим противное. Тогда изоморфизм $\mathbb{k}[x] \xrightarrow{\sim} \mathbb{k}[b_m]$ продолжается до изоморфизма поля рациональных функций $\mathbb{k}(x)$ с наименьшим содержащим элемент b_m подполем $\mathbb{k}(b_m) \subset B$. По предположению индукции поле B алгебраично над полем $\mathbb{k}(b_m)$, т. е. каждая из образующих $b_1, \dots, b_{m-1}$ удовлетворяет некоторому полиномиальному уравнению с коэффициентами из $\mathbb{k}(b_m)$. Умножая эти уравнения на подходящие многочлены от b_m , сделаем их коэффициенты лежащими в $\mathbb{k}[b_m]$, а все старшие коэффициенты — равными одному и тому же многочлену $p(b_m) \in \mathbb{k}[b_m]$. Поле B цело над подалгеброй $F \subset B$, порождённой над $\mathbb{k}$ 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

$$(1 + p(b_m)) g(b_m, 1/p(b_m)) = 1 \quad (1-2)$$

для некоторого многочлена $g \in \mathbb{k}[x_1, x_2]$. Записывая рациональную функцию $g(x, 1/p(x))$ в виде $h(x)/p^k(x)$, где $h \in \mathbb{k}[x]$ не делится в $\mathbb{k}[x]$ 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 $\mathbb{k}[x]$. $\square$

ПРИМЕР 1.5 (конечные расширения полей)

Если $\mathbb{k}$ -алгебра A конечномерна как векторное пространство над $\mathbb{k}$, то каждый элемент $\xi \in A$ алгебраичен¹ над $\mathbb{k}$, так как бесконечное множество целых неотрицательных степеней ξ^k линейно зависимо. Поэтому алгебра A цела² над $\mathbb{k}$. Если в ней нет делителей нуля, то A является полем по [предл. 1.2](#) на стр. 6. Конечномерные как векторные пространства над $\mathbb{k}$ поля $\mathbb{F} \supset \mathbb{k}$ называются *конечными расширениями* поля $\mathbb{k}$. Размерность конечного расширения $\mathbb{F}$ поля $\mathbb{k}$ как векторного пространства над $\mathbb{k}$ называется *степенью расширения* $\mathbb{F} \supset \mathbb{k}$ и обозначается $\deg \mathbb{F}/\mathbb{k}$ или $[\mathbb{F} : \mathbb{k}]$.

УПРАЖНЕНИЕ 1.8. Пусть в башне расширений колец $\mathbb{k} \subset \mathbb{K} \subset \mathbb{F}$ 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 $\mathbb{k}$. Покажите, что mn произведений $f_i t_j$ образуют базис $\mathbb{F}$ над $\mathbb{k}$, откуда $\deg \mathbb{F}/\mathbb{k} = \deg \mathbb{F}/\mathbb{K} \cdot \deg \mathbb{K}/\mathbb{k}$.

ПРЕДЛОЖЕНИЕ 1.3

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

¹См. [п. 1.3](#) на стр. 8.

²См. [опр. 1.1](#) на стр. 5.

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

Следствие 1.2

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

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

Элементы $a_1, \dots, a_m \in A$ называются *алгебраически независимыми* над $\mathbb{k}$, если гомоморфизм вычисления $\text{ev}_{(a_1, \dots, a_m)}: \mathbb{k}[x_1, \dots, x_m] \rightarrow A, f \mapsto f(a_1, \dots, a_m)$ инъективен, т. е. на элементы $a_1, \dots, a_m$ нет нетривиальных полиномиальных соотношений. В этом случае гомоморфизм вычисления продолжается до изоморфизма полей $\mathbb{k}(x_1, \dots, x_m) \simeq \mathbb{k}(a_1, \dots, a_m) \subset Q_A$, 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 $\mathbb{k}$, если каждый элемент алгебры A алгебраичен над $\mathbb{k}(a_1, \dots, a_m)$. В этом случае поле Q_A тоже алгебраично над $\mathbb{k}(a_1, \dots, a_m)$, так как целое замыкание $\mathbb{k}(a_1, \dots, a_m)$ в Q_A является полем по [предл. 1.2](#) на стр. 6 и содержит A , а значит, по универсальному свойству поля частных¹, и Q_A .

Алгебраически независимый набор элементов $a_1, \dots, a_m$ алгебры A , трансцендентно порождающий A над $\mathbb{k}$, называется *базисом трансцендентности* алгебры A над $\mathbb{k}$. 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 $\mathbb{k}$, то $n \leq m$ 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 $\mathbb{k}$.

Доказательство. Поскольку b_1 алгебраичен над $\mathbb{k}(a_1, \dots, a_m)$, имеется содержащее b_1 полиномиальное соотношение $f(b_1, a_1, \dots, a_m) = 0$, и так как b_1 трансцендентен над $\mathbb{k}$, в это соотношение входит какое-нибудь a_i . Перенумеруем a_i так, чтобы это было a_1 . Тогда алгебра A алгебраична над $\mathbb{k}(b_1, a_2, \dots, a_m)$. Пусть по индукции элементы $b_1, \dots, b_k, a_{k+1}, \dots, a_m$ трансцендентно порождают алгебру A над $\mathbb{k}$, и при этом $k < n$. Поскольку b_{k+1} алгебраичен над полем $\mathbb{k}(b_1, \dots, b_k, a_{k+1}, \dots, a_m)$, имеется содержащее b_{k+1} полиномиальное соотношение

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

¹См. Пример 3.2 на с. 56 лекций [\[Алг 1\]](#).

Так как $b_1, \dots, b_n$ алгебраически независимы над $\mathbb{k}$, 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 $\mathbb{k}(b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_m)$, что воспроизводит индуктивное предположение. $\square$

СЛЕДСТВИЕ 1.3 (ТЕОРЕМА О БАЗИСЕ)

Все базисы трансцендентности конечно порождённой $\mathbb{k}$ -алгебры состоят из одинакового числа элементов, не превосходящего число образующих, причём любой набор элементов, трансцендентно порождающий A над $\mathbb{k}$, содержит в себе базис трансцендентности, а любой алгебраически независимый набор элементов можно дополнить до базиса трансцендентности. $\square$

ОПРЕДЕЛЕНИЕ 1.2

Число элементов в базисе трансцендентности конечно порождённой алгебры A над $\mathbb{k}$ называется *степенью трансцендентности* этой алгебры и обозначается $\text{tr deg}_{\mathbb{k}} A$.

ПРИМЕР 1.6 (ПОДАЛГЕБРЫ ПОЛЯ РАЦИОНАЛЬНЫХ ФУНКЦИЙ)

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

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

Мы заключаем, что поле $\mathbb{k}(t)$ является конечным расширением поля $\mathbb{k}(\psi)$ степени

$$[\mathbb{k}(t) : \mathbb{k}(\psi)] = \max(\deg f, \deg g),$$

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

ТЕОРЕМА 1.2 (ТЕОРЕМА ЛЮРОТА)

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

ДОКАЗАТЕЛЬСТВО. Из предыдущего [прим. 1.6](#) вытекает, что элемент t алгебраичен над $\mathbb{K}$. Обозначим через

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

его минимальный многочлен над $\mathbb{K}$, а через $d \in \mathbb{k}[t]$ — наименьший общий знаменатель всех коэффициентов a_v . Многочлен $\tilde{f}(x, t) = df$ лежит в $\mathbb{k}[t][x]$ и имеет содержание¹ 1 как многочлен от x с коэффициентами в факториальном кольце $\mathbb{k}[t]$, а его степень по t равна максимальной из степеней многочленов $da_v \in \mathbb{k}[t]$. Пусть она равна $m = \deg da_i$ и $a_i = b/c$, где $b, c \in \mathbb{k}[t]$ взаимно просты. Покажем, что $m = n$.

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

Поскольку элемент t является корнем многочлена $a_i(t)c(x) - b(x) \in \mathbb{k}(a_i)[x] \subset \mathbb{K}[x]$, 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 $c(t) \in \mathbb{K}[t]$, получаем

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

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

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

в $\mathbb{k}[x, t]$. 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 $\mathbb{k}[x]$, а так как $c(x)$ и $b(x)$ взаимно просты в $\mathbb{k}[x]$, многочлен g не зависит и от x , т. е. является константой из $\mathbb{k}$. 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 $\deg \mathbb{k}(t)/\mathbb{k}(a_i) = \max(\deg b, \deg c)$. Поэтому

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

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

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

§2. Алгебраические расширения полей

2.1. Башни примитивных расширений. Для любого отличного от константы неприводимого многочлена $f \in \mathbb{k}[x]$ степени $n \geq 1$ алгебра $\mathbb{k}[x]/(f)$ не имеет делителей нуля и n -мерна над $\mathbb{k}$. Поэтому она является полем. Элементы этого поля однозначно записываются в виде

$$b_0 + b_1\vartheta + \dots + b_{n-1}\vartheta^{n-1},$$

где $b_i \in \mathbb{k}$, а класс $\vartheta \stackrel{\text{def}}{=} [x]_f$ является корнем многочлена f . Поле $\mathbb{k}[x]/(f)$ называется *примитивным* расширением поля $\mathbb{k}$, полученным *присоединением* к полю $\mathbb{k}$ корня ϑ неприводимого многочлена f .

УПРАЖНЕНИЕ 2.1. Покажите, что для любого многочлена $f \in \mathbb{k}[x]$ последовательными примитивными расширениями можно получить из поля $\mathbb{k}$ такое поле $\mathbb{F} \supset \mathbb{k}$, над которым многочлен f полностью разложится в произведение линейных множителей.

ПРИМЕР 2.1 (КУБИЧЕСКИЕ РАСШИРЕНИЯ)

Пусть $f = x^3 + a_1x^2 + a_2x + a_3 \in \mathbb{k}[x]$ неприводим над $\mathbb{k}$. Примитивное расширение $\mathbb{K} = \mathbb{k}[x]/(f)$ имеет степень 3 над $\mathbb{k}$ и его элементы однозначно записываются в виде

$$b_0 + b_1\vartheta + b_2\vartheta^2,$$

где $b_i \in \mathbb{k}$, а $\vartheta \in \mathbb{K}$ означает класс $[x]_f$ многочлена x по модулю f . Такие записи перемножаются и складываются по стандартным правилам раскрытия скобок с учётом соотношения $f(\vartheta) = 0$.

УПРАЖНЕНИЕ 2.2. Пусть $\mathbb{k} = \mathbb{Q}$ и $f(x) = x^3 + x + 1$. Запишите $(1 + 2\vartheta)^{-1}$ и $(1 + \vartheta + \vartheta^2)^{-1}$ в виде $b_0 + b_1\vartheta + b_2\vartheta^2$.

Так как $f(\vartheta) = 0$, многочлен $f(x)$ раскладывается в $\mathbb{K}[x]$ в произведение $f(x) = (x - \vartheta)q(x)$, где $q(x) = x^2 + c_1x + c_2 \in \mathbb{K}[x]$ либо приводим над $\mathbb{K}$, и тогда существуют такие $\vartheta_1, \vartheta_2 \in \mathbb{K}$, что

$$q(x) = (x - \vartheta_1)(x - \vartheta_2), \quad (2-1)$$

либо неприводим, и тогда разложение (2-1) имеет место над полем $\mathbb{L} = \mathbb{K}[x]/(q)$, степень которого над $\mathbb{k}$ равна 6. Чтобы выяснить, какой из этих двух случаев имеет место, заметим, что *дискриминант*

$$D(f) = (\vartheta - \vartheta_1)^2(\vartheta - \vartheta_2)^2(\vartheta_1 - \vartheta_2)^2 = q^2(\vartheta) \cdot D(q), \quad (2-2)$$

будучи симметрическим многочленом от корней, является многочленом от коэффициентов f и лежит в $\mathbb{k}$.

УПРАЖНЕНИЕ 2.3. Убедитесь, что $D(x^2 + px + q) = p^2 - 4q$, а $D(x^3 + px + q) = -4p^3 - 27q^2$.

Приводимость q в $\mathbb{K}[x]$ равносильна тому, что $D(q) = (\vartheta_1 - \vartheta_2)^2$ является квадратом в $\mathbb{K}$. Согласно (2-2), это эквивалентно тому, что квадратом в $\mathbb{K}$ является $D(f)$. Но если $D(f) = \delta^2$ квадрат в $\mathbb{K}$, то он квадрат и в $\mathbb{k}$, так как в противном случае многочлен $g(x) = x^2 - D(f)$ был бы неприводим над $\mathbb{k}$, и квадратичное расширение $\mathbb{k}[x]/(g)$ поля $\mathbb{k}$ вкладывалось бы в $\mathbb{K}$ по правилу

$$[h]_g \mapsto h(\delta) \in \mathbb{k},$$

что невозможно по [упр. 1.8](#), ибо $\deg \mathbb{K}/\mathbb{k} = 3$. Мы заключаем, что неприводимый кубический многочлен $f \in \mathbb{k}[x]$ полностью разлагается на линейные множители над кубическим расширением $\mathbb{k}[x]/(f)$ если и только если $D(f)$ квадрат в $\mathbb{k}$.

ЛЕММА 2.1

Любое конечное расширение $\mathbb{F} \supset \mathbb{K}$ можно получить в качестве верхнего этажа башни

$$\mathbb{K} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F} \quad (2-3)$$

примитивных расширений $\mathbb{L}_i = \mathbb{L}_{i-1}[x]/(f_i)$, где $f_i \in \mathbb{L}_{i-1}[x]$ неприводим над $\mathbb{L}_{i-1}$.

Доказательство. Пусть поле $\mathbb{L}_i \subset \mathbb{F}$ уже построено. Если $\mathbb{L}_i \neq \mathbb{F}$, возьмём в качестве $f_{i+1} \in \mathbb{L}_i[x]$ минимальный многочлен любого элемента $\vartheta \in \mathbb{F} \setminus \mathbb{L}_i$ над полем $\mathbb{L}_i$ и вложим примитивное расширение $\mathbb{L}_i[x]/(f)$ в поле $\mathbb{F}$ по правилу $[x]_f \mapsto \vartheta$. Обозначим через $\mathbb{L}_{i+1} \supsetneq \mathbb{L}_i$ образ этого вложения. Поскольку степень поля $\mathbb{F}$ над $\mathbb{L}_{i+1}$ строго меньше, чем над $\mathbb{L}_i$, через конечное число шагов оно исчерпается. $\square$

2.2. Сепарабельные расширения. Напомню¹, что многочлен $f \in \mathbb{K}[x]$ называется *сепарабельным*, если у него нет кратных корней ни в каком расширении поля $\mathbb{K}$, что равносильно равенству

$$\text{нод}(f, f') = 1,$$

которое можно проверить при помощи алгоритма Евклида над самим полем $\mathbb{K}$. Алгебраическое расширение² $\mathbb{F} \supset \mathbb{K}$ называется *сепарабельным*, если минимальный над $\mathbb{K}$ многочлен $\mu_\vartheta \in \mathbb{K}[x]$ любого элемента $\vartheta \in \mathbb{F} \setminus \mathbb{K}$ сепарабелен.

УПРАЖНЕНИЕ 2.4. Убедитесь, что все примитивные расширения простых полей $\mathbb{F}_p$ и любого поля характеристики нуль сепарабельны.

УПРАЖНЕНИЕ 2.5. Пусть $\mathbb{K} = \mathbb{F}_p(t)$. Покажите что многочлен $f(x) = x^p - t \in \mathbb{K}[x]$ неприводим над $\mathbb{K}$ и несепарабелен.

ПРИМЕР 2.2 (корни из единицы)

Корни уравнения $x^n = 1$ в произвольном поле $\mathbb{K}$ образуют конечную мультипликативную подгруппу, которая обозначается $\mu_n(\mathbb{K})$ и называется *группой корней n -й степени из единицы* поля $\mathbb{K}$. Как и всякая конечная мультипликативная подгруппа в поле, группа $\mu_n(\mathbb{K})$ циклическая³. Если её порядок равен n , то говорят, что поле $\mathbb{K}$ *содержит все $\sqrt[n]{1}$* , и буде это так, образующие группы $\mu_n(\mathbb{K}) \simeq \mathbb{Z}/(n)$ называются *первообразными корнями степени n из единицы*. Всего имеется $\varphi(n)$ первообразных корней, и если $\zeta \in \mathbb{K}$ — один из них, все степени ζ^m с $0 \leq m \leq n-1$ различны. Поэтому следующие три условия эквивалентны:

- поле $\mathbb{K}$ допускает расширение, содержащее все $\sqrt[n]{1}$
- многочлен $x^n - 1$ сепарабелен над $\mathbb{K}$
- $\text{char}(\mathbb{K}) \nmid n$.

При их выполнении каждый многочлен $f(x) = x^n - a$ с ненулевым $a \in \mathbb{K}$ сепарабелен, так как $f'(x) = nx^{n-1}$ имеет единственный корень нуль, не являющийся корнем f .

¹См. раздел 2.3.4 на с. 47 лекций [Алг 1].

²В том числе и не обязательно конечное.

³См. следствие 2.3 на с. 53 лекций [Алг 1].

ТЕОРЕМА 2.1 (ТЕОРЕМА О ПРИМИТИВНОМ ЭЛЕМЕНТЕ)

Всякое конечное сепарабельное расширение $\mathbb{K} \supset \mathbb{k}$ примитивно, т. е. имеет вид $\mathbb{K} = \mathbb{k}[x]/(f)$, где $f \in \mathbb{k}[x]$ — неприводимый многочлен степени $\deg \mathbb{K}/\mathbb{k}$.

Доказательство. Если поле $\mathbb{k}$ конечно, то поле $\mathbb{K}$ тоже конечно, и его мультипликативная группа $\mathbb{K}^\times$ циклическая¹. Пусть $\vartheta \in \mathbb{K}$ — её образующая. Тогда² $\mathbb{K} = \mathbb{k}[\vartheta]$.

Всюду далее мы считаем поле $\mathbb{k}$ бесконечным. Индукция по длине башни из [лем. 2.1](#) сводит теорему к случаю, когда поле $\mathbb{K} = \mathbb{k}[\alpha, \beta] \supset \mathbb{k}[\alpha] \supset \mathbb{k}$ является башней двух примитивных расширений. Как $\mathbb{k}$ -алгебра такое поле $\mathbb{K}$ порождается над $\mathbb{k}$ двумя сепарабельными алгебраическими элементами α, β . Подберём $t \in \mathbb{k}^\times$ так, чтобы подалгебра $\mathbb{k}[\vartheta] \subset \mathbb{K}$, порождённая над $\mathbb{k}$ элементом $\vartheta = \alpha + t\beta$, совпала с $\mathbb{K}$. При любом t элемент ϑ алгебраичен над $\mathbb{k}$, и алгебра $\mathbb{k}[\vartheta]$ является полем. Достаточно добиться того, чтобы оно содержало элемент β : тогда и $\alpha = \vartheta - t\beta$ тоже будет в нём лежать. Обозначим через $f_\alpha(x)$ и $f_\beta(x)$ минимальные многочлены элементов α и β над полем $\mathbb{k}$. Элемент β является общим корнем многочлена $f_\beta(x) \in \mathbb{k}[x]$ и многочлена $g(x) = f_\alpha(\vartheta - tx)$, коэффициенты которого лежат в зависящем от параметра t поле $\mathbb{k}[\vartheta]$. Рассмотрим любое поле $\mathbb{F} \supset \mathbb{K}$, над которым f_α и f_β , а с ними и g , полностью разлагаются на линейные множители. Если t таков, что β является единственным общим корнем многочленов f_β и g в поле $\mathbb{F}$, то выразив $(x - \beta) = \text{нод}(f_\beta, g)$ через многочлены f_β и g по алгоритму Евклида, мы получим искомое представление элемента β в виде рациональной функции от лежащих в $\mathbb{k}[\vartheta]$ коэффициентов этих многочленов. Остаётся найти такое t .

Пусть $\deg f_\alpha = m$, $\deg f_\beta = \deg g = k$. Обозначим через $\alpha_1, \dots, \alpha_m$ и $\beta_1, \dots, \beta_k$ корни многочленов f_α и f_β в $\mathbb{F}$, считая, что $\alpha = \alpha_1$ и $\beta = \beta_1$. Тогда корни g суть $(\vartheta - \alpha_i)/t = \beta_1 + (\alpha_1 - \alpha_i)/t$, где $1 \leq i \leq m$. Мы хотим, чтобы

$$\beta_j \neq \beta_1 + (\alpha_1 - \alpha_i)/t \quad (2-4)$$

при всех i, j кроме $i = j = 1$. В силу сепарабельности элемента α разности $\alpha_1 - \alpha_i \neq 0$ при $i \neq 1$. Поэтому каждое неравенство (2-4), в котором $i \neq 1$, запрещает ровно одно значение $t = (\beta_j - \beta_1)/(\alpha_1 - \alpha_i)$. При $i = 1$ запреты (2-4) требуют, чтобы $\beta_1 \neq \beta_j$ при $j \neq 1$, что обеспечивается сепарабельностью β . Тем самым, исключается лишь конечное множество значений t , что доказывает теорему для бесконечного поля $\mathbb{k}$. $\square$

СЛЕДСТВИЕ 2.1

Если поле $\mathbb{K}$ является сепарабельным алгебраическим расширением поля $\mathbb{k}$ и степени всех его элементов³ ограничены, то $\mathbb{K}$ конечно над $\mathbb{k}$, и $\deg \mathbb{K}/\mathbb{k} = \max_{\vartheta \in \mathbb{K}} \deg_{\mathbb{k}} \vartheta$.

Доказательство. Если $\beta \in \mathbb{K}$ не лежит в примитивном расширении $\mathbb{k}[\alpha] \supset \mathbb{k}$, порождённом каким-либо другим элементом $\alpha \in \mathbb{K}$, то $[\mathbb{k}[\alpha, \beta] : \mathbb{k}] > \deg_{\mathbb{k}} \alpha$, и степень примитивного элемента поля $\mathbb{k}[\alpha, \beta]$ строго больше $\deg \alpha$. Поэтому подполе в $\mathbb{K}$, порождённое элементом максимальной степени, совпадает со всем $\mathbb{K}$. $\square$

¹См. всё то же следствие 2.3 на с. 53 лекций [\[Алг 1\]](#).

²Хотя это рассуждение не использует сепарабельности поля $\mathbb{k}$ напрямую, из [лем. 2.1](#) на стр. 14 и [упр. 2.4](#) вытекает, что каждое конечное поле сепарабельно над своим простым подполем.

³Напомню, что *степенью* алгебраического элемента называется степень его минимального многочлена.

2.3. Продолжение гомоморфизмов. Поскольку у полей нет ненулевых собственных идеалов¹, а ядро гомоморфизма колец является идеалом², всякий ненулевой гомоморфизм из поля в кольцо инъективен.

Предложение 2.1

Если поле $\mathbb{K} \supset \mathbb{k}$ алгебраично³ над $\mathbb{k}$, то любое вложение $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$, тождественное на подполе $\mathbb{k}$, является автоморфизмом поля $\mathbb{K}$.

Доказательство. Достаточно убедиться, что $\varphi(\mathbb{K}) = \mathbb{K}$. Пусть $\vartheta \in \mathbb{K}$ имеет над $\mathbb{k}$ минимальный многочлен $f \in \mathbb{k}[x]$. Вложение φ переводит корни многочлена f в корни многочлена f . Поэтому $\varphi^m \vartheta = \varphi^n \vartheta$ для некоторых $m > n$, где $\varphi^k = \varphi \circ \dots \circ \varphi$ означает k -кратную итерацию вложения $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$. Из инъективности φ вытекает, что $\vartheta = \varphi^{m-n} \vartheta \in \text{im } \varphi$. $\square$

Каждое вложение полей $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ продолжается до вложения $\mathbb{k}[x] \hookrightarrow \mathbb{F}[x]$, $f \mapsto f^\varphi$, где многочлен $f^\varphi \in \mathbb{F}[x]$ получается из $f \in \mathbb{k}[x]$ применением φ к каждому коэффициенту многочлена f .

Лемма 2.2

Пусть $\mathbb{K} = \mathbb{k}[x]/(f)$ — примитивное расширение поля $\mathbb{k}$ степени $d = \deg f = [\mathbb{K} : \mathbb{k}]$, и $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ — любое вложение $\mathbb{k}$ в произвольное поле. Вложения $\tilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, совпадающие с φ на подполе $\mathbb{k} \subset \mathbb{K}$, находятся в канонической биекции с корнями многочлена f^φ в поле $\mathbb{F}$. В частности, таких вложений не более d , и их ровно d если и только если многочлен f^φ полностью раскладывается над $\mathbb{F}$ в произведение d попарно разных линейных множителей.

Доказательство. Каждый элемент $\alpha \in \mathbb{F}$ задаёт гомоморфизм $\varphi_\alpha : \mathbb{k}[x] \rightarrow \mathbb{F}$, $g(x) \mapsto g^\varphi(\alpha)$. Если α является корнем многочлена $f^\varphi \in \mathbb{F}[x]$, то $f \in \ker \varphi_\alpha$, и φ_α корректно факторизуется до вложения полей $\tilde{\varphi}_\alpha : \mathbb{k}[x]/(f) \hookrightarrow \mathbb{F}$, переводящего примитивный элемент $\vartheta = [x]_f$ поля $\mathbb{K}$ в $\alpha \in \mathbb{F}$. При этом разные корни $\alpha \neq \beta$ задают разные вложения $\tilde{\varphi}_\alpha \neq \tilde{\varphi}_\beta$. С другой стороны, любое вложение $\tilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, совпадающее с φ на подполе $\mathbb{k} \subset \mathbb{K}$, переводит ϑ в некоторый корень многочлена f^φ , так как $f^\varphi(\tilde{\varphi}(\vartheta)) = \tilde{\varphi}(f(\vartheta)) = \varphi(0) = 0$. Поэтому $\tilde{\varphi}$ совпадает с одним из вложений $\tilde{\varphi}_\alpha$. $\square$

Лемма 2.3

Пусть алгебраическое расширение⁴ $\mathbb{K} \supset \mathbb{k}$ и вложение $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ таковы, что для любого элемента $\vartheta \in \mathbb{K}$ с минимальным над $\mathbb{k}$ многочленом $\mu_\vartheta \in \mathbb{k}[x]$ многочлен $\mu_\vartheta^\varphi \in \mathbb{F}[x]$ полностью раскладывается в $\mathbb{F}[x]$ на линейные множители. Тогда для любого элемента $\vartheta \in \mathbb{K}$ и любого корня $\xi \in \mathbb{F}$ многочлена μ_ϑ^φ существует такое совпадающее с φ на подполе $\mathbb{k}$ вложение $\tilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, что $\tilde{\varphi}(\vartheta) = \xi$.

Доказательство. По лем. 2.2 вложение $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ продолжается до вложения $\varphi_\xi : \mathbb{k}[\vartheta] \hookrightarrow \mathbb{F}$, переводящего ϑ в ξ . Множество всех продолжений $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$ отображения φ_ξ на всевозможные подполя $\mathbb{k}[\vartheta] \subseteq \mathbb{L} \subseteq \mathbb{K}$ непусто, ибо содержит φ_ξ , и частично упорядочено отношением $(\mathbb{L}'', \psi'') \geq (\mathbb{L}', \psi')$, означаящим, что $\mathbb{L}'' \supseteq \mathbb{L}'$ и $\psi''|_{\mathbb{L}'} = \psi'$.

¹См. Предложение 4.1 на с. 68 лекций [Алг 1].

²См. раздел 4.1 на с. 68 лекций [Алг 1].

³Но не обязательно конечно.

⁴Не обязательно конечное.

УПРАЖНЕНИЕ 2.6. Убедитесь, что это полный чум¹, к которому применима Лемма Цорна².

Покажем, что его максимальный элемент $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$ имеет область определения $\mathbb{L} = \mathbb{K}$. Если имеется элемент $\vartheta \in \mathbb{K} \setminus \mathbb{L}$, то его минимальный многочлен $\mu_\vartheta \in \mathbb{K}[x]$ над полем $\mathbb{K}$ делится в $\mathbb{L}[x]$ на его минимальный многочлен $\mu_{\vartheta, \mathbb{L}}$ над полем $\mathbb{L}$. Коль скоро многочлен μ_ϑ^φ полностью раскладывается в $\mathbb{F}[x]$ на линейные множители, его делитель $\mu_{\vartheta, \mathbb{L}}^\varphi$ тоже обладает этим свойством. Поэтому к примитивному расширению $\mathbb{L} \subset \mathbb{L}[\vartheta]$ применима лем. 2.2, и вложение ψ продолжится на строго большее подполе $\mathbb{L}[\vartheta] = \mathbb{L}[x]/(\mu_{\vartheta, \mathbb{L}})$. $\square$

Предложение 2.2

Если расширение $\mathbb{K} \supset \mathbb{k}$ конечно, то вложение полей $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ продолжается до вложения $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ не более, чем $[\mathbb{K} : \mathbb{k}]$ различными способами. Наличие ровно $[\mathbb{K} : \mathbb{k}]$ продолжений равносильно тому, что расширение $\mathbb{K} \supset \mathbb{k}$ сепарабельно и образ $\mu_\vartheta^\varphi \in \mathbb{F}[x]$ минимального над $\mathbb{k}$ многочлена $\mu_\vartheta \in \mathbb{k}[x]$ любого элемента $\vartheta \in \mathbb{K}$ полностью раскладывается в $\mathbb{F}[x]$ на линейные множители.

Доказательство. Разложим $\mathbb{K}$ в башню (2-3) примитивных расширений

$$\mathbb{k} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \quad (2-5)$$

где $\mathbb{L}_i = \mathbb{L}_{i-1}[\vartheta_i] \simeq \mathbb{L}_{i-1}[x]/(f_i)$ и многочлен $f_i \in \mathbb{L}_{i-1}[x]$ является минимальным над $\mathbb{L}_{i-1}$ многочленом элемента $\vartheta_i \in \mathbb{L}_i \setminus \mathbb{L}_{i-1}$. Ограничения продолжающего φ вложения $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ на подполя $\mathbb{L}_i \subset \mathbb{K}$ образуют цепочку последовательно продолжающих друг друга вложений $\psi_i : \mathbb{L}_i \hookrightarrow \mathbb{F}$. Так как по лем. 2.2 каждый шаг этой цепочки можно осуществить не более, чем $\deg f_i = [\mathbb{L}_i : \mathbb{L}_{i-1}]$ способами, продолжающих φ вложений ψ имеется не более $\prod_i [\mathbb{L}_i : \mathbb{L}_{i-1}] = [\mathbb{K} : \mathbb{k}]$, и их будет ровно столько если и только если каждый многочлен f_i^φ имеет $\deg f_i$ различных корней в поле $\mathbb{F}$. Поскольку башню (2-5) можно начать присоединением любого элемента $\vartheta = \vartheta_1 \in \mathbb{K}$, из наличия $[\mathbb{K} : \mathbb{k}]$ продолжений вытекает, что образ μ_ϑ^φ минимального многочлена μ_ϑ любого элемента $\vartheta \in \mathbb{K}$ раскладывается над $\mathbb{F}$ в произведение $\deg \mu_\vartheta$ различных линейных множителей. В частности, μ_ϑ сепарабелен. Наоборот, если все элементы $\vartheta \in \mathbb{K}$ сепарабельны, а образы μ_ϑ^φ их минимальных многочленов полностью раскладываются над $\mathbb{F}$ на линейные множители, то эти множители будут различны, и в любой цепочке (2-5) каждый многочлен f_i , будучи делителем многочлена μ_{ϑ_i} в кольце $\mathbb{L}_{i-1}[x]$, переведётся вложением $\psi_{i-1} : \mathbb{L}_{i-1} \hookrightarrow \mathbb{F}$ в многочлен, полностью разлагающийся над $\mathbb{F}$ в произведение попарно различных линейных множителей. Поэтому вложение $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ будет продолжаться вдоль такой цепочки ровно $[\mathbb{K} : \mathbb{k}]$ способами. $\square$

УПРАЖНЕНИЕ 2.7. Пусть в условиях предл. 2.2 поле $\mathbb{K}$ как алгебра над $\mathbb{k}$ порождается элементами $\xi_1, \dots, \xi_m$. Покажите, что наличие ровно $[\mathbb{K} : \mathbb{k}]$ продолжений равносильно тому, что каждый элемент ξ_v сепарабелен и его минимальный многочлен полностью раскладывается в $\mathbb{F}[x]$ на линейные множители.

2.4. Поле разложения многочлена. Поле $\mathbb{L}_f \supset \mathbb{k}$ называется *полем разложения* многочлена $f \in \mathbb{k}[x]$, если f полностью раскладывается в $\mathbb{L}_f[x]$ на линейные множители, и для любого расширения $\mathbb{F} \supset \mathbb{k}$, в котором f полностью раскладывается на линейные множители, существует вложение $\mathbb{L}_f \hookrightarrow \mathbb{F}$, тождественное на подполе $\mathbb{k}$.

¹См. Определение 0.3 на с. 21 лекций [Алг 1].

²См. Следствие 0.1 на с. 21 лекций [Алг 1].

ПРИМЕР 2.3 (поле разложения кубического многочлена)

В прим. 2.1 на стр. 13 мы видели, что полем разложения неприводимого кубического многочлена $f \in \mathbb{k}[x]$, дискриминант $D(f)$ которого является квадратом в $\mathbb{k}$, служит примитивное кубическое расширение $\mathbb{K} = \mathbb{k}[x]/(f)$, а если $D(f)$ не квадрат в $\mathbb{k}$, то полем разложения является его квадратичное расширение $\mathbb{K}[\sqrt{D(f)}]$, имеющее степень 6 над $\mathbb{k}$.

ТЕОРЕМА 2.2

У любого многочлена $f \in \mathbb{k}[x]$ есть поле разложения $\mathbb{L}_f$, и между любыми двумя полями разложения многочлена f имеется (не канонический) изоморфизм, тождественно действующий на подполе $\mathbb{k}$.

Доказательство. Рассмотрим любое конечное расширение $\mathbb{F} \supset \mathbb{k}$, в котором f полностью раскладывается на линейные множители¹, и обозначим через $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ корни f , а через $\mathbb{L}_f$ — наименьшее подполе в $\mathbb{F}$, содержащее $\mathbb{k}$ и все эти корни. Поле $\mathbb{L}_f$ раскладывается в башню (2-3) примитивных расширений

$$\mathbb{k} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{L}_f, \quad (2-6)$$

на каждом этаже которой присоединяется какой-нибудь элемент² $\vartheta \in \{\alpha_1, \dots, \alpha_m\}$. Если поле $\mathbb{K} \supset \mathbb{k}$ таково, что f полностью раскладывается над ним на линейные множители, то включение $\mathbb{k} \subset \mathbb{K}$ продолжается вдоль башни (2-6) до тождественного на $\mathbb{k}$ вложения $\mathbb{L}_f \hookrightarrow \mathbb{K}$ по лем. 2.3: минимальный многочлен каждого присоединяемого элемента ϑ , будучи делителем многочлена f , полностью раскладывается над $\mathbb{K}$ на линейные множители. Тем самым, $\mathbb{L}_f$ является полем разложения. Для любого другого поля разложения $\mathbb{L}'_f$ имеются вложения $\varphi: \mathbb{L}_f \hookrightarrow \mathbb{L}'_f$ и $\varphi': \mathbb{L}'_f \hookrightarrow \mathbb{L}_f$. По предл. 2.1 обе композиции $\varphi \circ \varphi'$ и $\varphi' \circ \varphi$ биактивны. Поэтому каждое из вложений является изоморфизмом. $\square$

ПРИМЕР 2.4 (классификация конечных полей)

Каждое конечное поле $\mathbb{F}$ характеристики p является конечным расширением своего простого подполя $\mathbb{F}_p = \mathbb{Z}/(p)$ и состоит из $q = p^n$ элементов, где $n = [\mathbb{F} : \mathbb{F}_p]$. Так как ненулевые элементы поля $\mathbb{F}$ образуют конечную мультипликативную группу порядка $q - 1$, все они удовлетворяют уравнению $x^{q-1} = 1$. Следовательно, элементы поля $\mathbb{F}$ суть q различных корней многочлена $f(x) = x^q - x \in \mathbb{F}_p[x]$, сепарабельного, поскольку $f' = 1$. Таким образом, поле $\mathbb{F}$ является полем разложения многочлена f и единственно с точностью до (не канонического) изоморфизма.

2.5. Алгебраическое замыкание. Алгебраическое над $\mathbb{k}$ алгебраически замкнутое поле $\bar{\mathbb{k}} \supset \mathbb{k}$ называется *алгебраическим замыканием* поля $\mathbb{k}$.

УПРАЖНЕНИЕ 2.8. Покажите, что любое конечное расширение $\mathbb{K} \supset \mathbb{k}$ допускает тождественное на $\mathbb{k}$ вложение в любое алгебраическое замыкание $\bar{\mathbb{k}}$ поля $\mathbb{k}$.

ТЕОРЕМА 2.3

У каждого поля $\mathbb{k}$ есть алгебраическое замыкание, и между любыми двумя алгебраическими замыканиями поля $\mathbb{k}$ имеется (не канонический) изоморфизм, тождественно действующий на подполе $\mathbb{k}$.

¹См. упр. 2.1 на стр. 13.

²Отметим, что число k этажей башни может оказаться меньше, чем число корней m многочлена f , поскольку присоединение очередного корня может привести к автоматическому присоединению ещё нескольких.

Доказательство. Для любых двух алгебраических замыканий $\mathbb{L}', \mathbb{L}''$ поля $\mathbb{K}$ включение $\mathbb{K} \subset \mathbb{L}'$ продолжается до тождественного на $\mathbb{K}$ вложения $\varphi' : \mathbb{L}' \hookrightarrow \mathbb{L}''$. Симметричным образом имеется тождественное на $\mathbb{K}$ вложение $\varphi'' : \mathbb{L}'' \hookrightarrow \mathbb{L}'$. По [предл. 2.1](#) композиции $\varphi' \circ \varphi''$ и $\varphi'' \circ \varphi'$ биективны. Поэтому φ' и φ'' тоже биективны, и $\mathbb{L}' \simeq \mathbb{L}''$. Существование алгебраического замыкания устанавливается в два шага.

Пусть поле $\mathbb{K} \supset \mathbb{k}$ алгебраично над $\mathbb{k}$ и каждый многочлен из $\mathbb{k}[x]$ полностью разлагается в $\mathbb{K}[x]$ на линейные множители. Алгебраические над $\mathbb{k}$ элементы поля $\mathbb{K}$ образуют подполе $\overline{\mathbb{k}}_{\mathbb{K}} \subset \mathbb{K}$. Покажем, что оно алгебраически замкнуто и тем самым является алгебраическим замыканием поля $\mathbb{k}$. Каждый многочлен $f \in \overline{\mathbb{k}}_{\mathbb{K}}[x]$ имеет корень ϑ в некотором конечном расширении $\mathbb{L} \supset \overline{\mathbb{k}}_{\mathbb{K}}$. Так как ϑ алгебраичен над $\overline{\mathbb{k}}_{\mathbb{K}}$, он алгебраичен и над $\mathbb{k}$, т. е. $g(\vartheta) = 0$ для некоторого многочлена $g \in \mathbb{k}[x]$. Так как g полностью распадается в $\mathbb{K}[x]$ на линейные множители, все корни многочлена g лежат в $\overline{\mathbb{k}}_{\mathbb{K}} \subset \mathbb{K} \subset \mathbb{L}$. В частности, $\vartheta \in \overline{\mathbb{k}}_{\mathbb{K}}$, что и требовалось.

Чтобы построить алгебраическое расширение $\mathbb{K} \supset \mathbb{k}$, в котором каждый многочлен из $\mathbb{k}[x]$ полностью разложим, сопоставим каждому многочлену $f \in \mathbb{k}[x]$ его поле разложения $\mathbb{L}_f \supset \mathbb{k}$ и рассмотрим тензорное произведение векторных пространств¹ $A = \bigotimes_f \mathbb{L}_f$. На A имеется естественная структура коммутативной $\mathbb{k}$ -алгебры, в которой разложимые тензоры перемножаются покомпонентно: $(\bigotimes_f \xi_f) \cdot (\bigotimes_f \zeta_f) \stackrel{\text{def}}{=} \bigotimes_f (\xi_f \zeta_f)$. Каждое поле $\mathbb{L}_f$ вкладывается в A сопоставлением элементу $\vartheta \in \mathbb{L}_f$ разложимого тензора, единственным отличным от единицы сомножителем которого является f -й сомножитель, равный ϑ . Поле $\mathbb{k}$ тоже вкладывается в A как $\mathbb{k}$ -линейная оболочка единицы $\bigotimes_f 1 \in A$. Выберем любой максимальный собственный идеал² $\mathfrak{m} \subset A$ и рассмотрим поле $\mathbb{K} = A/\mathfrak{m}$. Поскольку в идеале $\mathfrak{m}$ нет обратимых элементов, он имеет нулевое пересечение с $\mathbb{k}$, и со всеми подполями $\mathbb{L}_f$. Поэтому эти поля вкладываются в поле $\mathbb{K}$. При этом любой многочлен $f \in \mathbb{k}[x]$ полностью разложим в $\mathbb{L}_f \subset \mathbb{K}$. $\square$

Следствие 2.2

В любой башне конечных расширений $\mathbb{L}_1 \subset \mathbb{L}_2 \subset \mathbb{L}_3$ расширение $\mathbb{L}_1 \subset \mathbb{L}_3$ сепарабельно если и только если сепарабельны оба расширения $\mathbb{L}_1 \subset \mathbb{L}_2$ и $\mathbb{L}_2 \subset \mathbb{L}_3$.

Доказательство. Если поле $\mathbb{L}_3$ сепарабельно над $\mathbb{L}_1$, то сепарабельно и его подполе $\mathbb{L}_2$. Так как минимальный многочлен над $\mathbb{L}_2$ любого элемента $\vartheta \in \mathbb{L}_3$ делит сепарабельный минимальный многочлен элемента ϑ над $\mathbb{L}_1$, то $\mathbb{L}_3$ сепарабельно над $\mathbb{L}_2$. Наоборот, если оба расширения $\mathbb{L}_1 \subset \mathbb{L}_2$ и $\mathbb{L}_2 \subset \mathbb{L}_3$ сепарабельны, то по [предл. 2.2](#) тождественное вложение $\mathbb{L}_1$ в алгебраическое замыкание $\overline{\mathbb{L}}_1$ допускает ровно $\deg \mathbb{L}_2 / \mathbb{L}_1$ продолжений до вложения $\mathbb{L}_2 \hookrightarrow \overline{\mathbb{L}}_1$, и каждое из них ровно $\deg \mathbb{L}_3 / \mathbb{L}_2$ способами продолжается до вложения $\mathbb{L}_3 \hookrightarrow \overline{\mathbb{L}}_1$, так что всего имеется $\deg \mathbb{L}_2 / \mathbb{L}_1 \cdot \deg \mathbb{L}_3 / \mathbb{L}_2 = \deg \mathbb{L}_3 / \mathbb{L}_1$ продолжений тождественного вложения $\mathbb{L}_1 \hookrightarrow \overline{\mathbb{L}}_1$ до вложения $\mathbb{L}_3 \hookrightarrow \overline{\mathbb{L}}_1$, что по [предл. 2.2](#) означает сепарабельность расширения $\mathbb{L}_1 \subset \mathbb{L}_3$. $\square$

¹Тензорное произведение бесконечного семейства векторных пространств V_μ , где μ пробегает произвольное множество M , определяется точно также, как для конечного семейства (см. раздел 13.1 на с. 210 лекций [\[Алг 1\]](#)), а именно, как фактор векторного пространства $\mathcal{V}$ с базисом $\mathcal{B} = \prod_{\mu \in M} V_\mu$ по подпространству $\mathcal{R} \subset \mathcal{V}$, линейно порождённому всевозможными трёхчленными линейными комбинациями базисных векторов $a^{(m)} - xb^{(m)} - yc^{(m)}$, в которых $x, y \in \mathbb{k}$, а базисные семейства $a^{(m)} = (a_\mu)_{\mu \in M}$, $b^{(m)} = (b_\mu)_{\mu \in M}$, $c^{(m)} = (c_\mu)_{\mu \in M}$ из $\mathcal{B}$ таковы, что $a_\mu = b_\mu = c_\mu$ при всех $\mu \neq m$, а $a_m = xb_m + yc_m$, где индекс $m \in M$ тоже может быть любым. Класс базисного вектора $(v_\mu)_{\mu \in M}$ по модулю $\mathcal{R}$ обозначается $\bigotimes_\mu v_\mu$ и называется *разложимым тензором*.

²См. Пример 4.3 на с. 71 лекций [\[Алг 1\]](#).

2.6. Нормальные расширения. Алгебраическое расширение $\mathbb{K} \subset \mathbb{K}$ называется *нормальным*, если любой неприводимый над $\mathbb{k}$ многочлен $f \in \mathbb{k}[x]$, имеющий корень в $\mathbb{K}$, полностью разлагается в $\mathbb{K}[x]$ на линейные множители.

УПРАЖНЕНИЕ 2.9. Покажите, что неприводимый над $\mathbb{k}$ приведённый многочлен $f \in \mathbb{k}[x]$, имеющий корень ϑ в алгебраическом расширении $\mathbb{K} \supset \mathbb{k}$, является минимальным многочленом элемента ϑ над $\mathbb{k}$.

Таким образом, нормальность алгебраического расширения $\mathbb{K} \subset \mathbb{K}$ равносильна тому, что минимальный многочлен над $\mathbb{k}$ любого элемента $\vartheta \in \mathbb{K}$ полностью раскладывается в $\mathbb{K}[x]$ на линейные множители.

УПРАЖНЕНИЕ 2.10. Убедитесь, что любое квадратичное расширение нормально.

ЛЕММА 2.4

Фиксируем произвольное алгебраическое замыкание $\overline{\mathbb{k}}$ поля $\mathbb{k}$. Алгебраическое расширение $\mathbb{K} \subset \mathbb{K}$ нормально тогда и только тогда, когда образы всех тождественных на $\mathbb{k}$ вложений $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$ совпадают друг с другом.

Доказательство. По лем. 2.3 на стр. 16 существует вложение $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$, тождественное на подполе $\mathbb{k}$. Поэтому мы можем и будем считать, что $\mathbb{k} \subset \mathbb{K} \subset \overline{\mathbb{k}}$. Любое тождественное на $\mathbb{k}$ вложение $\psi: \mathbb{K} \hookrightarrow \overline{\mathbb{k}}$ переводит каждый элемент $\vartheta \in \mathbb{K}$ в один из корней его минимального над полем $\mathbb{k}$ многочлена $\mu_\vartheta \in \mathbb{k}[x]$. Если все эти корни лежат в $\mathbb{K}$, то $\psi(\mathbb{K}) \subset \mathbb{K}$. Наоборот, по лем. 2.3 для каждого корня ξ минимального многочлена $\mu_\vartheta \in \mathbb{k}[x]$ любого элемента $\vartheta \in \mathbb{K}$ имеется такое вложение $\psi_{\vartheta, \xi}: \mathbb{K} \hookrightarrow \overline{\mathbb{k}}$, что $\psi_{\vartheta, \xi}(\vartheta) = \xi$. Если образы всех этих вложений лежат в $\mathbb{K}$, то все корни минимальных многочленов элементов поля $\mathbb{K}$ лежат в $\mathbb{K}$. $\square$

ЛЕММА 2.5

Пусть в башне алгебраических расширений $\mathbb{k} \subset \mathbb{L} \subset \mathbb{K}$ поле $\mathbb{K}$ нормально над $\mathbb{k}$. Тогда $\mathbb{K}$ нормально и над $\mathbb{L}$, а вот $\mathbb{L}$ нормально над $\mathbb{k}$ если и только если образ любого тождественного на $\mathbb{k}$ вложения $\mathbb{L} \hookrightarrow \mathbb{K}$ совпадает с $\mathbb{L}$.

Доказательство. Минимальный над $\mathbb{L}$ многочлен любого элемента $\vartheta \in \mathbb{K}$ делит в $\mathbb{L}[x]$ минимальный многочлен элемента ϑ над $\mathbb{k}$, и если в $\mathbb{K}[x]$ второй из них полностью раскладывается на линейные множители, то и первый раскладывается. Поэтому $\mathbb{K}$ нормально над $\mathbb{L}$. Второе утверждение вытекает из лем. 2.4: фиксируем алгебраическое замыкание $\overline{\mathbb{k}} \supset \mathbb{K} \supset \mathbb{L} \supset \mathbb{k}$ и заметим, что образы всех вложений $\mathbb{L} \hookrightarrow \overline{\mathbb{k}}$ лежат в $\mathbb{K}$, поскольку каждое такое вложение продолжается до вложения $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$, образ которого совпадает с $\mathbb{K}$. $\square$

Предостережение 2.1. Башня $\mathbb{F} \supset \mathbb{L} \supset \mathbb{k}$ нормальных расширений $\mathbb{F} \supset \mathbb{L}$ и $\mathbb{L} \supset \mathbb{k}$ может не быть нормальным расширением. Например, расширение $\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q}[x]/(x^4 - 2)$ раскладывается в башню квадратичных расширений $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$, каждое из которых нормально по упр. 2.10, однако само нормальным не является, так как четыре его вложения в алгебраическое замыкание $\overline{\mathbb{Q}} \subset \mathbb{C}$ переводят примитивный элемент $\vartheta = x \pmod{x^4 - 2}$ поля $\mathbb{Q}[x]/(x^4 - 2)$ в четыре разных комплексных корня $\pm \sqrt[4]{2} \in \mathbb{R}$ и $\pm i \sqrt[4]{2} \notin \mathbb{R}$ из двойки, и образами этих вложений являются два разных подполя в $\mathbb{C}$ — одно из них содержит оба вещественных корня и содержится в $\mathbb{R}$, а другое содержит оба мнимых корня и не содержится в $\mathbb{R}$.

Предложение 2.3

Конечное расширение $\mathbb{K} \supset \mathbb{k}$ нормально если и только если $\mathbb{K}$ является полем разложения некоторого многочлена¹ $f \in \mathbb{k}[x]$.

Доказательство. Пусть нормальное над $\mathbb{k}$ поле $\mathbb{K} \supset \mathbb{k}$ порождается как алгебра над $\mathbb{k}$ элементами $\alpha_1, \dots, \alpha_k$, и пусть $f_i \in \mathbb{k}[x]$ — минимальный многочлен элемента α_i над полем $\mathbb{k}$. Тогда многочлен $f = \prod f_i$ полностью раскладывается над $\mathbb{K}$ на линейные множители, и по [упр. 2.7](#) поле $\mathbb{K}$ вкладывается в любое другое поле, над которым f полностью раскладывается на линейные множители. Следовательно, $\mathbb{K}$ является полем разложения многочлена $f \in \mathbb{k}[x]$, то любое тождественное на подполе $\mathbb{k}$ вложение $\mathbb{K}$ в фиксированное алгебраическое замыкание $\bar{\mathbb{k}}$ является изоморфизмом $\mathbb{K}$ на подполе $\mathbb{k}[\alpha_1, \dots, \alpha_k] \subset \bar{\mathbb{k}}$, порождённое всеми корнями $\alpha_1, \dots, \alpha_k$ многочлена f в $\bar{\mathbb{k}}$. Поэтому $\mathbb{K}$ нормально по [лем. 2.4](#). $\square$

2.7. Композиты. Зафиксируем алгебраическое замыкание $\bar{\mathbb{k}}$ поля $\mathbb{k}$. Для любого набора содержащих $\mathbb{k}$ и содержащихся в $\bar{\mathbb{k}}$ полей $\mathbb{K}_1, \dots, \mathbb{K}_m$ наименьшее подполе в $\bar{\mathbb{k}}$, которое содержит все поля $\mathbb{K}_i$, называется *комполитом* этих полей и обозначается $\mathbb{K}_1 \dots \mathbb{K}_m$. Иначе композит можно описать как пересечение всех подполей в $\bar{\mathbb{k}}$, содержащих каждое из полей $\mathbb{K}_i$, или как $\mathbb{k}$ -линейную оболочку всевозможных произведений $\vartheta_1 \dots \vartheta_m$, где $\vartheta_i \in \mathbb{K}_i$ для каждого i .

Предложение 2.4

Пусть поля $\mathbb{F}$ и $\mathbb{K}$ содержат $\mathbb{k}$ и содержатся в $\bar{\mathbb{k}}$. Если поле $\mathbb{K}$ нормально (соотв. сепарабельно) над $\mathbb{k}$, то композит $\mathbb{F}\mathbb{K}$ нормален (соотв. сепарабелен) над $\mathbb{F}$.

Доказательство. Поскольку базис поля $\mathbb{K}$ как векторного пространства над $\mathbb{F} \cap \mathbb{K}$ является одновременно и базисом композита $\mathbb{F}\mathbb{K}$ как векторного пространства над $\mathbb{F}$, имеет место равенство степеней $[\mathbb{F}\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F} \cap \mathbb{K}]$. Так как любое тождественное на $\mathbb{F} \cap \mathbb{K}$ вложение $\mathbb{K} \hookrightarrow \bar{\mathbb{k}}$ продолжается по $\mathbb{F}$ -линейности до тождественного на $\mathbb{F}$ вложения $\mathbb{K}\mathbb{F} \hookrightarrow \bar{\mathbb{k}}$, между первыми и вторыми вложениями имеется каноническая биекция. Если $\mathbb{K}$ сепарабельно над $\mathbb{k}$, то по [сл. 2.2](#) на стр. 19 оба расширения башни $\mathbb{k} \subset \mathbb{F} \cap \mathbb{K} \subset \mathbb{K}$ сепарабельны, и по [предл. 2.2](#) на стр. 17 имеет место $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}]$ тождественных на $\mathbb{F} \cap \mathbb{K}$ вложений $\mathbb{K} \hookrightarrow \bar{\mathbb{k}}$. Поэтому тождественных на $\mathbb{F}$ вложений $\mathbb{K}\mathbb{F} \hookrightarrow \bar{\mathbb{k}}$ тоже имеется $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}] = [\mathbb{F}\mathbb{K} : \mathbb{F}]$, что по той же [предл. 2.2](#) означает сепарабельность $\mathbb{F}\mathbb{K}$ над $\mathbb{F}$. Если поле $\mathbb{K}$ нормально над $\mathbb{k}$, то по [лем. 2.4](#) на стр. 20 образы всех вложений $\mathbb{K} \hookrightarrow \bar{\mathbb{k}}$ совпадают с $\mathbb{K}$. Поэтому образы всех $\mathbb{F}$ -линейных вложений $\mathbb{K}\mathbb{F} \hookrightarrow \bar{\mathbb{k}}$ совпадают с $\mathbb{K}\mathbb{F}$, что по [лем. 2.4](#) означает нормальность $\mathbb{K}\mathbb{F}$ над $\mathbb{F}$. $\square$

Теорема 2.4 (нормальное замыкание)

Для любого конечного сепарабельного расширения $\mathbb{F} \supset \mathbb{k}$ существует нормальное и сепарабельное над $\mathbb{k}$ поле $\mathbb{K} \supset \mathbb{F}$, которое вкладывается над $\mathbb{F}$ в любое другое нормальное и сепарабельное над $\mathbb{k}$ поле $\mathbb{K}' \supset \mathbb{F}$. Все такие поля² конечны над $\mathbb{k}$ и (не канонически) изоморфны друг другу над $\mathbb{k}$.

Доказательство. Зафиксируем алгебраическое замыкание $\bar{\mathbb{k}} \supset \mathbb{k}$ и возьмём в качестве $\mathbb{K}$ композит образов всех $n = \deg \mathbb{F}/\mathbb{k}$ различных вложений $\mathbb{F} \hookrightarrow \bar{\mathbb{k}}$. Тогда $\deg \mathbb{K}/\mathbb{F} \leq n$, и $\mathbb{F}$ нормально и сепарабельно как над $\mathbb{F}$, так и над $\mathbb{k}$, а любое вложение $\mathbb{F}$ в любое нормальное сепарабельное расширение $\mathbb{K}' \supset \mathbb{k}$ продолжается до вложения $\mathbb{K} \hookrightarrow \mathbb{K}'$. $\square$

¹Возможно приводимого над $\mathbb{k}$.

²Они называются *нормальными замыканиями* сепарабельного расширения $\mathbb{F} \supset \mathbb{k}$.

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 $\text{sp}(\vartheta, \vartheta^{-1}) = \text{tr}(1) = \dim_{\mathbb{Q}} K$ для любого $\vartheta \neq 0$.
- Упр. 1.5. Если $\mathbb{Q}[\sqrt{d_1}] \sim \mathbb{Q}[\sqrt{d_2}]$, то $d_2 = (a + b\sqrt{d_1})^2 = a^2 + d_1b^2 + 2ab\sqrt{d_1}$ для некоторых $a, b \in \mathbb{Q}$, откуда $ab = 0$ и $a^2 + d_1b^2 = d_2$, что возможно только при $a = 0, b = 1, d_1 = d_2$.
- Упр. 1.9. Многочлен $x_1 g(x_2) - f(x_2) \in \mathbb{k}[x_1, x_2]$ от независимых переменных x_1, x_2 неприводим в $\mathbb{k}[x_1, x_2]$. Поскольку ψ трансцендентен, кольцо $\mathbb{k}[x_1, x_2]$ изоморфно кольцу $\mathbb{k}[\psi][x]$ посредством гомоморфизма $x_1 \mapsto \psi, x_2 \mapsto x$, переводящего многочлен $x_1 g(x_2) - f(x_2) \in \mathbb{k}[x_1, x_2]$ в многочлен $\psi \cdot g(x) - f(x)$, тем самым неприводимый в $\mathbb{k}[\psi][x]$. По лемме Гаусса¹, он будет неприводим и в $\mathbb{k}(\psi)[x]$.
- Упр. 2.1. Уточните доказательство [лем. 1.1](#) на стр. 4, см. также теорему 2.1 на с. 46 лекций [\[Алг 1\]](#).
- Упр. 2.4. Неприводимый многочлен f не сепарабелен, если и только если $f' = 0$. Над полем характеристики нуль такого не бывает, а над простым полем $\mathbb{F}_p$ равенство $f' = 0$ равносильно тому, что $f = g(x^p) = g(x)^p$ для некоторого многочлена $g \in \mathbb{F}_p[x]$, см. раздел 2.3.4 на с. 47 лекций [\[Алг 1\]](#).
- Упр. 2.8. Это вытекает из [лем. 2.3](#).

¹См. Следствие 4.5 на с. 78 лекций [\[Алг 1\]](#).