

## §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  $\vartheta$  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  $[x]_f$  одночлена  $x$  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.** Напомню<sup>1</sup>, 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 расширение<sup>2</sup>  $\mathbb{F} \supset \mathbb{K}$  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  $\mu_n(\mathbb{K})$  циклическая<sup>3</sup>. 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  $\zeta^m$  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  $f$ .

<sup>1</sup>См. раздел 2.3.4 на с. 47 лекций [Алг 1].

<sup>2</sup>В том числе и не обязательно конечное.

<sup>3</sup>См. 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  $\mathbb{K}^\times$  циклическая<sup>1</sup>. Пусть  $\vartheta \in \mathbb{K}$  — её образующая. Тогда<sup>2</sup>  $\mathbb{K} = \mathbb{k}[\vartheta]$ .

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  $\alpha, \beta$ . 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  $\vartheta$  алгебраичен над  $\mathbb{k}$ , и алгебра  $\mathbb{k}[\vartheta]$  является полем. Достаточно добиться того, чтобы оно содержало элемент  $\beta$ : тогда и  $\alpha = \vartheta - t\beta$  тоже будет в нём лежать. Обозначим через  $f_\alpha(x)$  и  $f_\beta(x)$  минимальные многочлены элементов  $\alpha$  и  $\beta$  над полем  $\mathbb{k}$ . Элемент  $\beta$  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  $f_\alpha$  и  $f_\beta$ , а с ними и  $g$ , полностью разлагаются на линейные множители. Если  $t$  таков, что  $\beta$  является единственным общим корнем многочленов  $f_\beta$  и  $g$  в поле  $\mathbb{F}$ , то выразив  $(x - \beta) = \text{нод}(f_\beta, g)$  через многочлены  $f_\beta$  и  $g$  по алгоритму Евклида, мы получим искомое представление элемента  $\beta$  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  $f_\alpha$  и  $f_\beta$  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  $\alpha$  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  $\beta$ . 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 элементов<sup>3</sup> 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  $\mathbb{K}$ .  $\square$

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

<sup>2</sup>Хотя 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.

<sup>3</sup>Напомню, что *степенью* алгебраического элемента называется степень его минимального многочлена.

**2.3. Продолжение гомоморфизмов.** Поскольку у полей нет ненулевых собственных идеалов<sup>1</sup>, а ядро гомоморфизма колец является идеалом<sup>2</sup>, всякий ненулевой гомоморфизм из поля в кольцо инъективен.

Предложение 2.1

Если поле  $\mathbb{K} \supset \mathbb{k}$  алгебраично<sup>3</sup> 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  $\varphi$  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  $\varphi$  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  $\varphi$  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  $\varphi$  на подполе  $\mathbb{k} \subset \mathbb{K}$ , находятся в канонической биекции с корнями многочлена  $f^\varphi$  в поле  $\mathbb{F}$ . В частности, таких вложений не более  $d$ , и их ровно  $d$  если и только если многочлен  $f^\varphi$  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  $\alpha$  является корнем многочлена  $f^\varphi \in \mathbb{F}[x]$ , то  $f \in \ker \varphi_\alpha$ , и  $\varphi_\alpha$  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  $\varphi$  на подполе  $\mathbb{k} \subset \mathbb{K}$ , переводит  $\vartheta$  в некоторый корень многочлена  $f^\varphi$ , 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 расширение<sup>4</sup>  $\mathbb{K} \supset \mathbb{k}$  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  $\mu_\vartheta^\varphi$  существует такое совпадающее с  $\varphi$  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  $\vartheta$  в  $\xi$ . Множество всех продолжений  $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$  отображения  $\varphi_\xi$  на всевозможные подполя  $\mathbb{k}[\vartheta] \subseteq \mathbb{L} \subseteq \mathbb{K}$  непусто, ибо содержит  $\varphi_\xi$ , и частично упорядочено отношением  $(\mathbb{L}'', \psi'') \geq (\mathbb{L}', \psi')$ , означаящим, что  $\mathbb{L}'' \supseteq \mathbb{L}'$  и  $\psi''|_{\mathbb{L}'} = \psi'$ .

<sup>1</sup>См. Предложение 4.1 на с. 68 лекций [Алг 1].

<sup>2</sup>См. раздел 4.1 на с. 68 лекций [Алг 1].

<sup>3</sup>Но не обязательно конечно.

<sup>4</sup>Не обязательно конечно.

УПРАЖНЕНИЕ 2.6. Убедитесь, что это полный чум<sup>1</sup>, к которому применима Лемма Цорна<sup>2</sup>.

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  $\mu_\vartheta^\varphi$  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  $\psi$  продолжается 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  $\varphi$  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  $\varphi$  вложений  $\psi$  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  $f_i^\varphi$  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  $\mu_\vartheta^\varphi$  минимального многочлена  $\mu_\vartheta$  любого элемента  $\vartheta \in \mathbb{K}$  раскладывается над  $\mathbb{F}$  в произведение  $\deg \mu_\vartheta$  различных линейных множителей. В частности,  $\mu_\vartheta$  сепарабелен. Наоборот, если все элементы  $\vartheta \in \mathbb{K}$  сепарабельны, а образы  $\mu_\vartheta^\varphi$  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  $\mu_{\vartheta_i}$  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  $\xi_v$  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  $\mathbb{K}$ .

<sup>1</sup>См. Определение 0.3 на с. 21 лекций [Алг 1].

<sup>2</sup>См. 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 множители<sup>1</sup>, 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 элемент<sup>2</sup>  $\vartheta \in \{\alpha_1, \dots, \alpha_m\}$ . 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  $\vartheta$ , 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  $\mathbb{k}$ .

<sup>1</sup>См. упр. 2.1 на стр. 13.

<sup>2</sup>Отметим, 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  $\varphi'$  и  $\varphi''$  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  $\vartheta$  в некотором конечном расширении  $\mathbb{L} \supset \overline{\mathbb{k}}_{\mathbb{K}}$ . Так как  $\vartheta$  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 пространств<sup>1</sup>  $A = \bigotimes_f \mathbb{L}_f$ . 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  $\vartheta$ . Поле  $\mathbb{k}$  тоже вкладывается в  $A$  как  $\mathbb{k}$ -линейная оболочка единицы  $\bigotimes_f 1 \in A$ . Выберем любой максимальный собственный идеал<sup>2</sup>  $\mathfrak{m} \subset A$  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  $\vartheta$  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  $\mathbb{L}_1 \subset \mathbb{L}_3$ .  $\square$

<sup>1</sup>Тензорное произведение бесконечного семейства векторных пространств  $V_\mu$ , где  $\mu$  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*.

<sup>2</sup>См. 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  $\vartheta$  в алгебраическом расширении  $\mathbb{K} \supset \mathbb{k}$ , является минимальным многочленом элемента  $\vartheta$  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  $\xi$  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  $\vartheta$  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 многочлена<sup>1</sup>  $f \in \mathbb{k}[x]$ .

**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  $\alpha_i$  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 имеется  $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}]$  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 поля<sup>2</sup> 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  $\mathbb{K} \hookrightarrow \mathbb{K}'$ .  $\square$

<sup>1</sup>Возможно приводимого над  $\mathbb{k}$ .

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

### Ответы и указания к некоторым упражнениям

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](#).