

§12. Алгебраические расширения полей

12.1. Конечные расширения. Поле \mathbb{F} , конечномерное как векторное пространство над своим подполем $\mathbb{k} \subset \mathbb{F}$, называется *конечным расширением* поля \mathbb{k} . Размерность $\dim_{\mathbb{k}} \mathbb{F}$ этого векторного пространства называется *степенью* поля \mathbb{F} над \mathbb{k} и обозначается $\deg \mathbb{F}/\mathbb{k}$ или $[\mathbb{F} : \mathbb{k}]$.

УПРАЖНЕНИЕ 12.1. Пусть расширения полей $\mathbb{k} \subset \mathbb{K} \subset \mathbb{F}$ конечны и $f_1, \dots, f_m \in \mathbb{F}$ 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 $f_i t_j$ составляют базис \mathbb{F} над \mathbb{k} . В частности,

$$\deg \mathbb{F}/\mathbb{k} = \deg \mathbb{F}/\mathbb{K} \cdot \deg \mathbb{K}/\mathbb{k}. \quad (12-1)$$

Поскольку целость и алгебраичность элемента над полем означают одно и то же, из доказанных в н° 9.1 на стр. 128 свойств целых элементов вытекает, что всякая коммутативная \mathbb{k} -алгебра A , конечномерная как векторное пространство над \mathbb{k} , алгебраична над \mathbb{k} , и если в A нет делителей нуля, то A является полем. Наоборот, любое поле $\mathbb{K} \supset \mathbb{k}$, конечно порождённое как \mathbb{k} -алгебра, является конечным расширением поля \mathbb{k} . В частности, любая конечно порождённая \mathbb{k} -подалгебра $\mathbb{k}[a_1, \dots, a_m]$ в любом поле $\mathbb{F} \supset \mathbb{k}$ конечной степени над \mathbb{k} тоже является полем конечной степени над \mathbb{k} , причём эта степень делит $\deg \mathbb{F}/\mathbb{k}$ по [упр. 12.1](#).

УПРАЖНЕНИЕ 12.2. Убедитесь, что любое конечное поле \mathbb{F} имеет положительную характеристику $\text{char}(\mathbb{F}) = p > 0$, является конечным расширением своего простого подполя¹ $\mathbb{F}_p = \mathbb{Z}/(p)$ и имеет порядок $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}$.

12.1.1. Примитивные расширения. Для любого отличного от константы неприводимого многочлена $f \in \mathbb{k}[x]$ 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 $\vartheta = x \pmod{f}$ 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 . Если понятно, какой многочлен f имеется в виду, примитивное расширение $\mathbb{k}[x]/(f)$ часто обозначают² $\mathbb{k}[\vartheta]$ или $\mathbb{k}(\vartheta)$. Так, запись $\mathbb{k}[\sqrt[m]{a}]$ по определению означает примитивное расширение $\mathbb{k}[x]/(x^m - a)$, где $a \in \mathbb{k}$ таков, что многочлен $x^m - a$ неприводим в $\mathbb{k}[x]$.

ПРИМЕР 12.1 (КУБИЧЕСКИЕ РАСШИРЕНИЯ)

Для любого поля \mathbb{k} и неприводимого над \mathbb{k} многочлена $f = x^3 + a_1x^2 + a_2x + a_3 \in \mathbb{k}[x]$ поле $\mathbb{K} = \mathbb{k}[x]/(f)$ 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 $x \pmod{f}$. Такие записи перемножаются и складываются по стандартным правилам раскрытия скобок с учётом соотношения $f(\vartheta) = 0$.

УПРАЖНЕНИЕ 12.3. 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 $f(x) = (x - \vartheta) \cdot q(x)$, где квадратный трёхчлен $q(x) = x^2 + c_1x + c_2 \in \mathbb{K}[x]$ либо приводим над \mathbb{K} , и тогда

$$q(x) = (x - \vartheta_1)(x - \vartheta_2) \quad (12-2)$$

¹Напомню, что *простым подполем* поля \mathbb{F} называется наименьшее по включению подполе в \mathbb{F} , см. раздел 2.8.1 на стр. 32 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_02.pdf.

²Однако без явного указания многочлена f обозначение $\mathbb{k}[\vartheta]$ мало осмысленно.

для некоторых $\vartheta_1, \vartheta_2 \in \mathbb{K}$, либо неприводим, и тогда разложение (12-2) пишется лишь над квадратичным расширением $\mathbb{L} = \mathbb{K}[x]/(q)$ поля \mathbb{K} , степень которого над исходным полем \mathbb{K} равна 6. Чтобы выяснить, какой из этих двух случаев имеет место, заметим, что *дискриминант*¹

$$D(f) = (\vartheta - \vartheta_1)^2(\vartheta - \vartheta_2)^2(\vartheta_1 - \vartheta_2)^2 = q^2(\vartheta) \cdot D(q), \quad (12-3)$$

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

УПРАЖНЕНИЕ 12.4. 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 (12-3), это эквивалентно тому, что квадратом в \mathbb{K} является $D(f)$. Но если $D(f)$ квадрат в \mathbb{K} , то он квадрат и в \mathbb{k} : иначе многочлен $x^2 - D(f)$ был неприводим над \mathbb{k} , и квадратичное расширение $\mathbb{k}[x]/(x^2 - D(f))$ поля \mathbb{k} вкладывалось бы в поле \mathbb{K} по правилу $x \bmod (x^2 - D(f)) \mapsto \sqrt{D(f)} \in \mathbb{K}$, что невозможно по упр. 12.1, так как $\deg \mathbb{K}/\mathbb{k} = 3$. Итак, неприводимый кубический многочлен $f \in \mathbb{k}[x]$ тогда и только тогда полностью разлагается на линейные множители над кубическим расширением $\mathbb{k}[x]/(f)$, когда $D(f)$ квадрат в \mathbb{k} .

УПРАЖНЕНИЕ 12.5. Покажите, что следующие три условия на вещественный трёхчлен $f(x) = x^3 + px + q \in \mathbb{R}[x]$ попарно эквивалентны: а) $D(f) > 0$ б) все комплексные корни f вещественны в) при некотором $\lambda \in \mathbb{R}$ подстановка $x = \lambda t$ превращает уравнение $f(x) = 0$ в уравнение $4t^3 - 3t = c$ с $|c| \leq 1$, корнем которого является $x = \cos\left(\frac{1}{3} \arccos(c)\right)$.

12.1.2. Сепарабельность. Если в рассмотренном выше прим. 12.1 характеристика исходного поля \mathbb{K} равна 3, некоторые из корней ϑ, ϑ_1 и ϑ_2 многочлена f могут совпасть, хотя он и неприводим над \mathbb{k} . Скажем, над полем $\mathbb{k} = \mathbb{F}_3(t)$ рациональных функций с коэффициентами в поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ многочлен $f(x) = x^3 - t \in \mathbb{k}[x]$ неприводим, так как не имеет корней в \mathbb{k} , однако над примитивным расширением $\mathbb{K} = \mathbb{k}[\sqrt[3]{t}] = \mathbb{k}[x]/(f)$ он становится полным кубом²: $x^3 - t = \left(x - \sqrt[3]{t}\right)^3$.

ОПРЕДЕЛЕНИЕ 12.1

Многочлен $f \in \mathbb{k}[x]$ называется *сепарабельным*, если у него нет кратных корней ни в каком расширении $\mathbb{K} \supset \mathbb{k}$. Алгебраическое расширение $\mathbb{F} \supset \mathbb{k}$ (возможно, бесконечное) 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 12.6. Покажите, что корень $\alpha \in \mathbb{F} \supset \mathbb{k}$ многочлена $f \in \mathbb{k}[x]$ является кратным если и только если $f'(\alpha) = 0$.

Тем самым, многочлен $f \in \mathbb{k}[x]$ сепарабелен если и только если $\text{нод}(f, f') = 1$, и это условие проверяемо при помощи алгоритма Евклида над исходным полем \mathbb{k} .

УПРАЖНЕНИЕ 12.7. Убедитесь, что все неприводимые многочлены над любым полем характеристики нуль сепарабельны.

¹Напомним, что *дискриминантом* приведённого многочлена $f(x) = \prod (x - \vartheta_i)$ называется произведение $D(f) \stackrel{\text{def}}{=} \prod_{i < j} (\vartheta_i - \vartheta_j)^2$ квадратов разностей его корней.

²Напомним, что $(a + b)^3 = a^3 + b^3$ в любом поле характеристики 3.

ПРИМЕР 12.2 (СЕПАРАБЕЛЬНОСТЬ КОНЕЧНЫХ ПОЛЕЙ)

Если многочлен f неприводим, то он не может иметь отличных от констант общих делителей ни с каким ненулевым многочленом меньшей степени. Поэтому неравенство $\text{нод}(f, f') \neq 1$ возможно только когда $f' = 0$. Над полем \mathbb{k} характеристики p это равенство означает, что показатели всех мономов, входящих в f с ненулевым коэффициентом, делятся на p . Для простого поля $\mathbb{k} = \mathbb{F}_p = \mathbb{Z}/(p)$, в котором $\alpha^p = \alpha$ для каждого $\alpha \in \mathbb{k}$, последнее условие означает, что многочлен $f(x) = a_n x^{np} + \dots + a_1 x^p + a_0 = a_n^p x^{np} + \dots + a_1^p x^p + a_0^p = (a_n x^n + \dots + a_1 x + a_0)^p$ является чистой p -той степенью. Поэтому все неприводимые многочлены над \mathbb{F}_p сепарабельны. В частности, каждое конечное поле сепарабельно над своим простым подполем.

УПРАЖНЕНИЕ 12.8. 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 12.3 (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 -той степени из единицы* поля \mathbb{k} . Как и всякая конечная мультипликативная подгруппа в поле, группа $\mu_n(\mathbb{k})$ циклическая. 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: (1) поле \mathbb{k} допускает расширение, содержащее все $\sqrt[n]{1}$; (2) многочлен $x^n - 1$ сепарабелен над \mathbb{k} ; (3) $\text{char}(\mathbb{k})$ не делит n . При выполнении этих условий 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 .

ЛЕММА 12.1

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

$$\mathbb{k} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \dots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F} \quad (12-4)$$

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 $x \pmod{f} \mapsto \vartheta$. Обозначим через $\mathbb{L}_{i+1} \supseteq \mathbb{L}_i$ 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

ЛЕММА 12.2

Для любого многочлена $f \in \mathbb{k}[x]$ существует конечное расширение $\mathbb{F} \supset \mathbb{k}$, над которым f полностью раскладывается на линейные множители.

Доказательство. Разложим f в $\mathbb{k}[x]$ на неприводимые множители. Если хоть один из них, назовём его q , не линеен, перейдём от \mathbb{k} к расширению $\mathbb{K} = \mathbb{k}[x]/(q) \supset \mathbb{k}$ и повторим процедуру. Поскольку над \mathbb{K} многочлен f имеет строго большее число линейных множителей, чем над \mathbb{k} , после нескольких таких итераций мы получим требуемое расширение. \square

ТЕОРЕМА 12.1 (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, поле \mathbb{K} тоже конечно, и его ненулевые элементы образуют циклическую мультипликативную группу. Если $\vartheta \in \mathbb{K}$ — образующая этой группы¹, то $\mathbb{K} = \mathbb{k}[\vartheta]$. Поэтому далее мы считаем поле \mathbb{k} бесконечным. Индукция по длине башни из лем. 12.1 сводит теорему к случаю, когда поле $\mathbb{K} = \mathbb{k}[\alpha, \beta] \supset \mathbb{k}[\alpha] \supset \mathbb{k}$ является башней двух примитивных расширений и как \mathbb{k} -алгебра порождается двумя сепарабельными алгебраическими элементами α, β . Мы собираемся подобрать $t \in \mathbb{k}^*$ так, чтобы порождённая над \mathbb{k} элементом $\vartheta = \alpha + t\beta$ подалгебра $\mathbb{k}[\vartheta] \subset \mathbb{K}$ совпала со всем полем \mathbb{K} . Так как ϑ алгебраичен над \mathbb{k} , алгебра $\mathbb{k}[\vartheta]$ является полем. Достаточно добиться того, чтобы в это поле попал 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 $(x - \beta) = \text{нод}(f_\beta(x), g(x))$ 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. Пусть $\deg f_\alpha = m$, $\deg f_\beta = \deg g = k$. Обозначим через $\alpha_1, \dots, \alpha_m$ и β_1, \dots, β_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 $\beta_j \neq \beta_1 + (\alpha_1 - \alpha_i)/t$ для всех i, j кроме $i = j = 1$. В силу сепарабельности элемента α разность $\alpha_1 - \alpha_i \neq 0$ при $i \neq 1$. Поэтому каждое неравенство с $i \neq 1$ запрещает ровно одно значение $t = (\beta_j - \beta_1)/(\alpha_1 - \alpha_i)$. При $i = 1$ запреты означают, что $\beta_1 \neq \beta_j$ при $j \neq 1$, и это так в силу сепарабельности β . Тем самым, исключается лишь конечное множество значений t , что и доказывает теорему для бесконечного поля \mathbb{k} . \square

Следствие 12.1

Если поле \mathbb{K} является сепарабельным алгебраическим расширением поля \mathbb{k} и степени всех его элементов² 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

12.2. Продолжение гомоморфизмов. Поскольку у полей нет ненулевых собственных идеалов, все ненулевые гомоморфизмы полей в кольца инъективны. Каждое вложение полей $\varphi : \mathbb{k} \hookrightarrow \mathbb{F}$ продолжается до вложения колец многочленов $\mathbb{k}[x] \hookrightarrow \mathbb{F}[x]$, переводящего многочлен $f \in \mathbb{k}[x]$ в многочлен $f^\varphi \in \mathbb{F}[x]$, получающийся из $f \in \mathbb{k}[x]$ применением φ к каждому коэффициенту f .

¹Это рассуждение показывает, что каждое конечное поле как алгебра над любым своим подполем всегда порождается одним элементом — образующей своей мультипликативной группы. Хотя сепарабельность не использовалась в нашем рассуждении явно, в прим. 12.2 мы видели, что все конечные поля сепарабельны над своими простыми подполями.

²Напомним, что степень алгебраического элемента называется степенью его минимального многочлена.

ЛЕММА 12.3

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 $\vartheta = x \pmod{f}$ 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 12.4

Пусть алгебраическое расширение¹ $\mathbb{K} \supset \mathbb{k}$ 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. 12.3 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 $(\mathbb{L}'', \psi'') \geq (\mathbb{L}', \psi')$ когда $\mathbb{L}'' \supseteq \mathbb{L}'$ и $\psi''|_{\mathbb{L}'} = \psi'$.

Упражнение 12.9. Убедитесь, что этот чум удовлетворяет условиям леммы Цорна.

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. 12.3, и вложение ψ продолжается на строго большее подполе $\mathbb{L}[\vartheta] = \mathbb{L}[x]/(\mu_{\vartheta, \mathbb{L}})$. \square

ПРЕДЛОЖЕНИЕ 12.1

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 (12-4) примитивных расширений

$$\mathbb{k} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \dots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \quad (12-5)$$

¹Не обязательно конечное.

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. 12.3 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 (12-5) 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 (12-5) 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 12.10. Пусть в условиях предл. 12.1 поле \mathbb{K} как алгебра над \mathbb{k} порождается элементами ξ_1, \dots, ξ_m . Покажите, что наличие ровно $[\mathbb{K} : \mathbb{k}]$ продолжений равносильно тому, что каждый элемент ξ_ν сепарабелен и его минимальный многочлен полностью раскладывается в $\mathbb{F}[x]$ на линейные множители.

Предложение 12.2

Если поле $\mathbb{K} \supset \mathbb{k}$ алгебраично¹ 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

12.3. Поле разложения и алгебраическое замыкание. В этом разделе мы установим существование у любого поля \mathbb{k} некоторых специальных расширений, единственных с точностью до неканонического изоморфизма, тождественно действующего на \mathbb{k} .

Определение 12.2 (поле разложения)

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} .

Пример 12.4 (поле разложения кубического многочлена)

В прим. 12.1 на стр. 169 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 он не квадрат и в \mathbb{K} , и полем разложения f в этом случае служит квадратичное расширение поля \mathbb{K} при помощи $\sqrt{D(f)}$, имеющее над полем \mathbb{k} степень 6.

¹Но не обязательно конечно.

ТЕОРЕМА 12.2

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 (12-4) примитивных расширений

$$\mathbb{k} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \dots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{L}_f, \quad (12-6)$$

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 (12-6) до тождественного на \mathbb{k} вложения $\mathbb{L}_f \hookrightarrow \mathbb{K}$ по лем. 12.4: 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. 12.2 обе композиции $\varphi \circ \varphi'$ и $\varphi' \circ \varphi$ биективны. Поэтому каждое из вложений является изоморфизмом. \square

ПРИМЕР 12.5 (КЛАССИФИКАЦИЯ КОНЕЧНЫХ ПОЛЕЙ)

Согласно упр. 12.2 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.

ОПРЕДЕЛЕНИЕ 12.3 (АЛГЕБРАИЧЕСКОЕ ЗАМКНУТОЕ ПОЛЕ)

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

УПРАЖНЕНИЕ 12.11. Покажите, что любое конечное расширение $\mathbb{K} \supset \mathbb{k}$ допускает тождественное на \mathbb{k} вложение в любое алгебраическое замыкание $\overline{\mathbb{k}}$ поля \mathbb{k} .

ТЕОРЕМА 12.3

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. лем. 12.2 на стр. 171.

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. 12.2](#) 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 несколько итераций. Пусть поле \mathbb{k} содержится в алгебраически замкнутом поле \mathbb{K} . Тогда множество $\overline{\mathbb{k}}$ алгебраических над \mathbb{k} элементов поля \mathbb{K} является полем по [предл. 9.2](#) на [стр. 129](#). Любой многочлен из $\overline{\mathbb{k}}[x] \subset \mathbb{K}[x]$ имеет корень ϑ в \mathbb{K} . Поскольку ϑ алгебраичен над $\overline{\mathbb{k}}$, он алгебраичен и над \mathbb{k} , а значит, лежит в $\overline{\mathbb{k}}$. Тем самым, поле $\overline{\mathbb{k}}$ алгебраически замкнуто и является алгебраическим замыканием поля \mathbb{k} . Остаётся убедиться в наличии какого-нибудь алгебраически замкнутого поля $\mathbb{K} \supset \mathbb{k}$. Сначала построим поле $\mathbb{F}_1 \supset \mathbb{k}$, над которым каждый многочлен $f \in \mathbb{k}[x]$ полностью разлагается на линейные множители. Для этого рассмотрим множество \mathcal{L} , элементами которого являются следующие наборы данных: (1) линейно упорядоченное множество многочленов $L \subset \mathbb{k}[x]$ (2) множество таких занумерованных многочленами $f \in L$ полей $\mathbb{L}_f(L) \supset \mathbb{k}$, что f полностью разлагается на линейные множители над $\mathbb{L}_f(L)$ и $\mathbb{L}_f(L) \subseteq \mathbb{L}_g(L)$ при $f \leq g$. Введём на \mathcal{L} частичный порядок, полагая $L_1 \leq L_2$ если $L_1 \subseteq L_2$ с сохранением порядка и $L_f(L_1) = L_f(L_2)$ для всех $f \in L_1$.

УПРАЖНЕНИЕ 12.12. Убедитесь, что \mathcal{L} является непустым полным чумом.

По лемме Цорна¹ в \mathcal{L} имеется максимальный элемент L . Если существует отличный от константы многочлен $h \notin L$, то множество L можно увеличить, добавив к нему h в качестве максимального элемента и положив \mathbb{L}_h равным полю разложения многочлена h над полем $\bigcup_{f \in L} \mathbb{L}_f$. Таким образом, множество многочленов L содержит все многочлены положительной степени, и все они полностью разлагаются на линейные множители над полем $\mathbb{F}_1 = \bigcup_{f \in L} \mathbb{L}_f$, что и требовалось. Заменяя \mathbb{k} на \mathbb{F}_1 и повторяя процедуру, мы получим бесконечную цепочку вложенных полей $\mathbb{k} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \dots$, в которой каждый многочлен из $\mathbb{F}_i[x]$ полностью разлагается на множители над полем \mathbb{F}_{i+1} . Поле $\mathbb{K} = \bigcup_i \mathbb{F}_i$ алгебраически замкнуто и содержит \mathbb{k} . \square

Следствие 12.2

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. 12.1](#) 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. 12.1](#) означает сепарабельность расширения $\mathbb{L}_1 \subset \mathbb{L}_3$. \square

12.4. 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 12.13. Покажите, что неприводимый над \mathbb{k} приведённый многочлен $f \in \mathbb{k}[x]$,

¹См. предложение 1.5 на [стр. 19](#) лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_01.pdf.

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 любого элемента $\vartheta \in \mathbb{K}$ над \mathbb{k} полностью раскладывается в $\mathbb{K}[x]$ на линейные множители.

УПРАЖНЕНИЕ 12.14. Убедитесь, что любое квадратичное расширение нормально.

ЛЕММА 12.5

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. 12.4 на стр. 173 существует тождественное на подполе \mathbb{k} вложение $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$. Поэтому мы можем 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. 12.4 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 12.6

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. 12.5: 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 12.1. 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. 12.14, однако само оно 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 из двойки: $\pm\sqrt[4]{2} \in \mathbb{R}$ и $\pm i\sqrt[4]{2} \notin \mathbb{R}$, и образы этих вложений суть два разных подполя в \mathbb{C} — одно содержится в \mathbb{R} , другое нет.

Предложение 12.3

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

¹Возможно приводимого над \mathbb{k} .

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. 12.10](#) поле \mathbb{K} вкладывается в любое другое поле, над которым f полностью раскладывается на линейные множители. Следовательно, \mathbb{K} является полем разложения многочлена f . Наоборот, если $\mathbb{K} \supset \mathbb{k}$ является полем разложения некоторого многочлена $f \in \mathbb{k}[x]$, то любое тождественное на подполе \mathbb{k} вложение \mathbb{K} в фиксированное алгебраическое замыкание $\overline{\mathbb{k}}$ является изоморфизмом \mathbb{K} на подполе $\mathbb{k}[\alpha_1, \dots, \alpha_k] \subset \overline{\mathbb{k}}$, порождённое всеми корнями $\alpha_1, \dots, \alpha_k$ многочлена f в $\overline{\mathbb{k}}$. Поэтому \mathbb{K} нормально по [лем. 12.5](#) на стр. 177. \square

12.4.1. Композиты. Зафиксируем алгебраическое замыкание $\overline{\mathbb{k}}$ поля \mathbb{k} . Для любого набора содержащих \mathbb{k} и содержащихся в $\overline{\mathbb{k}}$ полей $\mathbb{K}_1, \dots, \mathbb{K}_m$ наименьшее подполе в $\overline{\mathbb{k}}$, которое содержит все поля \mathbb{K}_i , называется *композитом* этих полей и обозначается $\mathbb{K}_1 \dots \mathbb{K}_m$. Иначе композит можно описать как пересечение всех подполей в $\overline{\mathbb{k}}$, 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 12.4

Пусть поля \mathbb{F} и \mathbb{K} содержат \mathbb{k} и содержатся в $\overline{\mathbb{k}}$. 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 $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$ продолжается по \mathbb{F} -линейности до тождественного на \mathbb{F} вложения $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\mathbb{k}}$, между первыми и вторыми вложениями имеется каноническая биекция. Если \mathbb{K} сепарабельно над \mathbb{k} , то по [сл. 12.2](#) на стр. 176 оба расширения башни $\mathbb{k} \subset \mathbb{F} \cap \mathbb{K} \subset \mathbb{K}$ сепарабельны, и по [предл. 12.1](#) на стр. 173 имеется $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}]$ тождественных на $\mathbb{F} \cap \mathbb{K}$ вложений $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$. Поэтому тождественных на \mathbb{F} вложений $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\mathbb{k}}$ тоже имеется $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}] = [\mathbb{F}\mathbb{K} : \mathbb{F}]$, что по той же [предл. 12.1](#) означает сепарабельность $\mathbb{F}\mathbb{K}$ над \mathbb{F} . Если поле \mathbb{K} нормально над \mathbb{k} , то по [лем. 12.5](#) на стр. 177 образы всех вложений $\mathbb{K} \hookrightarrow \overline{\mathbb{k}}$ совпадают с \mathbb{K} . Поэтому образы всех \mathbb{F} -линейных вложений $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\mathbb{k}}$ совпадают с $\mathbb{K}\mathbb{F}$, что по [лем. 12.5](#) означает нормальность $\mathbb{K}\mathbb{F}$ над \mathbb{F} . \square

Теорема 12.4 (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 поля¹ конечны над \mathbb{k} и (не канонически) изоморфны друг другу над \mathbb{k} .

Доказательство. Зафиксируем алгебраическое замыкание $\overline{\mathbb{k}} \supset \mathbb{k}$ и возьмём в качестве \mathbb{K} композит образов всех $n = \deg \mathbb{F}/\mathbb{k}$ различных вложений $\mathbb{F} \hookrightarrow \overline{\mathbb{k}}$. 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

12.5. Автоморфизмы полей и соответствие Галуа. Автоморфизмы поля \mathbb{K} , тождественно действующие на его подполе $\mathbb{k} \subset \mathbb{K}$, называются *автоморфизмами \mathbb{K} над \mathbb{k}* . Все такие автоморфизмы образуют группу $\text{Aut}_{\mathbb{k}} \mathbb{K} \stackrel{\text{def}}{=} \{ \varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K} \mid \varphi(t) = t \ \forall t \in \mathbb{k} \}$. Так как каждый автоморфизм

¹Они называются *нормальными замыканиями* сепарабельного расширения $\mathbb{F} \supset \mathbb{k}$.

поля \mathbb{K} над \mathbb{k} является продолжением включения $\mathbb{k} \subset \mathbb{K}$ на расширение $\mathbb{K} \supset \mathbb{k}$, порядок группы автоморфизмов конечного расширения $\mathbb{K} \supset \mathbb{k}$ удовлетворяет неравенству $|\text{Aut}_{\mathbb{k}} \mathbb{K}| \leq \deg \mathbb{K}/\mathbb{k}$ из [предл. 12.1](#) на стр. 173. Конечные расширения, для которых это неравенство превращается в равенство, называются *расширениями Галуа*. Из [предл. 12.1](#) вытекает, что конечное расширение является расширением Галуа если и только если оно нормально и сепарабельно. Группа автоморфизмов расширения Галуа $\mathbb{K} \supset \mathbb{k}$ называется *группой Галуа* и обозначается

$$\text{Gal } \mathbb{K}/\mathbb{k} \stackrel{\text{def}}{=} \text{Aut}_{\mathbb{k}} \mathbb{K}.$$

Для любой группы G автоморфизмов поля \mathbb{K} элементы $t \in \mathbb{K}$, неподвижные относительно всех преобразований из G , образуют в \mathbb{K} подполе $\mathbb{K}^G \stackrel{\text{def}}{=} \{t \in \mathbb{K} \mid \forall \varphi \in G \varphi(t) = t\}$, которое называется *полем инвариантов группы G* . Отметим, что \mathbb{K}^G содержит простое подполе поля \mathbb{K} , изоморфное \mathbb{Q} , когда $\text{char}(\mathbb{k}) = 0$, или $\mathbb{F}_p = \mathbb{Z}/(p)$, когда $\text{char}(\mathbb{k}) = p > 0$.

ТЕОРЕМА 12.5

Для любой конечной группы G автоморфизмов произвольного поля \mathbb{K} расширение $\mathbb{K} \supset \mathbb{K}^G$ является расширением Галуа степени $|G|$, и $\text{Aut}_{\mathbb{K}^G} \mathbb{K} = G$.

Доказательство. Пусть элементы $\vartheta_1, \dots, \vartheta_m \in \mathbb{K}$ попарно различны и составляют G -орбиту элемента $\vartheta = \vartheta_1 \in \mathbb{K}$. Многочлен $f_\vartheta(x) = (x - \vartheta_1) \dots (x - \vartheta_m)$ имеет коэффициенты в \mathbb{K}^G и неприводим над \mathbb{K}^G , поскольку группа G переводит в себя множество корней любого многочлена положительной степени из $\mathbb{K}^G[x]$ и не может транзитивно действовать на корнях произведения двух таких многочленов. Тем самым, f_ϑ является минимальным многочленом элемента ϑ над полем \mathbb{K}^G . Так как f_ϑ полностью разлагается над \mathbb{K} в произведение попарно различных линейных множителей, расширение $\mathbb{K}^G \subset \mathbb{K}$ алгебраично, нормально и сепарабельно, причём степень над \mathbb{K}^G любого элемента $\vartheta \in \mathbb{K}$ не выше $|G|$. По [сл. 12.1](#) на стр. 172 расширение $\mathbb{K}^G \subset \mathbb{K}$ конечно и $\deg \mathbb{K}/\mathbb{K}^G \leq |G|$. С другой стороны, $|G| \leq |\text{Aut}_{\mathbb{K}^G} \mathbb{K}| \leq \deg \mathbb{K}/\mathbb{K}^G$. Поэтому все написанные неравенства являются равенствами, и $G = \text{Aut}_{\mathbb{K}^G} \mathbb{K}$. \square

СЛЕДСТВИЕ 12.3

Для любых конечного расширения полей $\mathbb{k} \subset \mathbb{K}$ и подгруппы $G \subset \text{Aut}_{\mathbb{k}} \mathbb{K}$ равенства $\mathbb{K}^G = \mathbb{k}$ и $|G| = \deg \mathbb{K}/\mathbb{k}$ эквивалентны друг другу, и в случае их выполнения $G = \text{Aut}_{\mathbb{k}} \mathbb{K}$.

Доказательство. По [теор. 12.5](#) в башне $\mathbb{k} \subset \mathbb{K}^G \subset \mathbb{K}$ степень $\deg \mathbb{K}/\mathbb{K}^G = |G|$, откуда всё и следует. Поучительно, однако, дать другое доказательство, не использующее теорему о примитивном элементе, скрытую в ссылке на [сл. 12.1](#), данной при доказательстве [теор. 12.5](#).

Итак, пусть $|G| = \deg \mathbb{K}/\mathbb{k}$. Из неравенств $|G| \leq \deg \mathbb{K}/\mathbb{K}^G \leq \deg \mathbb{K}/\mathbb{k}$ вытекает, что $\deg \mathbb{K}/\mathbb{K}^G = \deg \mathbb{K}/\mathbb{k} = \deg \mathbb{K}/\mathbb{K}^G \cdot \deg \mathbb{K}^G/\mathbb{k}$, откуда $\deg \mathbb{K}^G/\mathbb{k} = 1$ и $\mathbb{K}^G = \mathbb{k}$. Наоборот, пусть $\mathbb{K}^G = \mathbb{k}$. Те же рассуждения, что и в [теор. 12.5](#) показывают, что расширение $\mathbb{K} \supset \mathbb{k}$ нормально и сепарабельно. Поэтому тождественное вложение $\mathbb{k} \hookrightarrow \mathbb{K}$ продолжается до автоморфизма поля \mathbb{K} над \mathbb{k} ровно $\deg \mathbb{K}/\mathbb{k}$ способами, и $|\text{Aut}_{\mathbb{k}} \mathbb{K}| = \deg \mathbb{K}/\mathbb{k}$. Остаётся показать, что $\text{Aut}_{\mathbb{k}} \mathbb{K} = G$. Поскольку коэффициенты минимального многочлена f_ϑ любого элемента $\vartheta \in \mathbb{K}$ инвариантны относительно $\text{Aut}_{\mathbb{k}} \mathbb{K}$, каждый автоморфизм $\varphi \in \text{Aut}_{\mathbb{k}} \mathbb{K}$ переводит ϑ в один из корней многочлена f_ϑ . Так как f_t неприводим, эти корни составляют орбиту группы G . Таким образом, для каждого $\vartheta \in \mathbb{K}$ и каждого $\varphi \in \text{Aut}_{\mathbb{k}} \mathbb{K}$ существует такой элемент $g \in G$, что $g(\vartheta) = \varphi(\vartheta)$. Поэтому для каждого $\varphi \in \text{Aut}_{\mathbb{k}} \mathbb{K}$ поле \mathbb{K} является объединением по всем $g \in G$ конечного числа подмножеств $V_g = \{\vartheta \in \mathbb{K} \mid g(\vartheta) = \varphi(\vartheta)\}$, каждое из которых является подпространством

конечномерного векторного пространства \mathbb{K} над полем \mathbb{k} . Если поле \mathbb{k} бесконечно, то конечномерное пространство над ним не представимо в виде объединения конечного числа собственных подпространств¹, и значит, одно из подпространств V_g совпадает с \mathbb{K} , откуда² $\varphi = g$. Если поле \mathbb{k} конечно, то \mathbb{K} тоже конечно и порождается над \mathbb{k} образующей ϑ циклической мультипликативной группы \mathbb{K}^* . В этом случае $\varphi = g$ для такого $g \in G$, что $\varphi(\vartheta) = g(\vartheta)$. \square

Пример 12.6 (поле инвариантов группы треугольника)

Рассмотрим проективную прямую $\mathbb{P}_1 = \mathbb{P}(\mathbb{k}^2)$ над произвольным полем \mathbb{k} . Группа треугольника $G = S_3$ действует на ней дробно линейными преобразованиями, переставляющими точки $0 = (0 : 1)$, $1 = (1 : 1)$, $\infty = (1 : 0)$. Тожждественное преобразование, циклы $\tau = (0, 1, \infty)$, $\tau^{-1} = (\infty, 1, 0)$ и транспозиции $\sigma_0, \sigma_1, \sigma_\infty$, оставляющие на месте точки $0, 1, \infty$ соответственно, преобразуют аффинную координату $t = t_0/t_1$ по формулам:

$$\begin{aligned} \text{Id} : t &\mapsto t & \tau : t &\mapsto 1/(1-t) & \tau^{-1} : t &\mapsto (t-1)/t \\ \sigma_0 : t &\mapsto t/(t-1) & \sigma_1 : t &\mapsto 1/t & \sigma_\infty : t &\mapsto 1-t. \end{aligned} \quad (12-7)$$

Эти шесть замен переменной задают действие группы G на поле $\mathbb{K} = \mathbb{k}(t)$ рациональных функций по правилу $g : \varphi(t) \mapsto \varphi(g^{-1}(t))$. Поле инвариантов \mathbb{K}^G этого действия состоит из функций $\varphi(t)$, не меняющихся при подстановках (12-7). Согласно теор. 12.5, расширение $\mathbb{K}^G \subset \mathbb{K}$ является расширением Галуа степени 6. Опишем поле \mathbb{K}^G явно. Если рациональная функция $\psi(t) = p(t)/q(t)$ G -инвариантна, то любая рациональная функция от ψ тоже G -инвариантна. Такие функции образуют подполе $\mathbb{k}(\psi) \subset \mathbb{K}^G$, и функция $t \in \mathbb{K}$ является корнем многочлена $\psi \cdot q(x) - p(x)$ с коэффициентами в этом подполе. Поэтому $\dim_{\mathbb{k}(\psi)} \mathbb{K} \leq \max(\deg p, \deg q)$. Так как левая часть неравенства делится на $\dim_{\mathbb{K}^G} \mathbb{K} = 6$, мы заключаем, что $\max(\deg p, \deg q) \geq 6$, где равенство означает, что $\mathbb{K}^G = \mathbb{k}(\psi)$. Инвариантную функцию ψ с $\deg p = \deg q = 6$ нетрудно построить из геометрических соображений. Рассмотрим однородный многочлен $f(t_0, t_1)$ без кратных неприводимых множителей, нули которого на \mathbb{P}_1 образуют одну G -орбиту. Подстановки (12-7) переводят его в многочлен с тем же множеством нулей, т. е. умножают на константы: $f(g^{-1}t) = \lambda(g) \cdot f(t)$, где $\lambda : G \rightarrow \mathbb{k}^*$, $g \mapsto \lambda(g)$, является одномерным характером группы G , коих имеется ровно два: тривиальный и знаковый. Поэтому f либо инвариантен относительно всех постановок (12-7), либо сохраняется поворотами и меняет знак при отражениях. Из трёхточечной орбиты $\{0, 1, \infty\}$ таким образом получается знакопеременный многочлен $p = t_0 t_1 (t_0 - t_1)$, квадрат которого G -инвариантен, а из двухточечной, образованной собственными векторами поворотов³ — G -инвариантный многочлен $q = t_0^2 - t_0 t_1 + t_1^2$. Минимальный лоранов моном полной степени нуль⁴ по $(t_0 : t_1)$, который можно соорудить из p^2 и q , это

$$\psi(t) = \frac{p^2}{q^3} = \frac{t_0^2 t_1^2 (t_0 - t_1)^2}{(t_0^2 - t_0 t_1 + t_1^2)^3} = \frac{t^2 (t-1)^2}{(t^2 - t + 1)^3}$$

так как это отношение многочленов степени ≤ 6 , поле инвариантов $\mathbb{K}^G = \mathbb{k}(\psi)$.

Упражнение 12.15. Убедитесь прямым вычислением, что замены (12-7) не меняют $\psi(t)$.

¹ См. упр. 10.12 на стр. 146.

² Полезно сопоставить это рассуждение с тем, что использовалось в теор. 12.1 на стр. 172.

³ Отметим, что сами точки могут быть и не определены над полем \mathbb{k} , но инвариантный многочлен, корнями которого они являются, лежит в $\mathbb{k}[t_0, t_1]$.

⁴ А именно, они являются рациональными функциями от $t = t_0/t_1$.

Пример 12.7 (автоморфизмы и вложения конечных полей)

Пусть $q = p^n$, где $p \in \mathbb{N}$ — простое. Поскольку расширение $\mathbb{F}_p \subset \mathbb{F}_q$ нормально и сепарабельно¹, $|\text{Aut}_{\mathbb{F}_p} \mathbb{F}_q| = [\mathbb{F}_q : \mathbb{F}_p] = n$. Итерации $F_p^0 = \text{Id}, F_p, F_p^2, \dots, F_p^{n-1}$ автоморфизма Фробениуса $F_p : \vartheta \mapsto \vartheta^p$ различны, так как равенство $F_p^k = F_p^m$ означает, что все p^n элементов поля \mathbb{F}_q являются корнями многочлена $x^{p^k} - x^{p^m}$, что невозможно при $k, m < n$. Поэтому $\text{Aut}_{\mathbb{F}_p} \mathbb{F}_q$ — циклическая группа порядка n , порождённая F_p . Для каждого $k|n$ подгруппа $G_k \subset \text{Aut}_{\mathbb{F}_p} \mathbb{F}_q$, порождённая автоморфизмом F_p^k , имеет порядок n/k , а её неподвижные точки суть корни многочлена $x^{p^k} - x$. Поэтому $\mathbb{F}_q^{G_k} = \mathbb{F}_{p^k} \subset \mathbb{F}_{p^n}$ является полем разложения многочлена $x^{p^k} - x$, и $G_k \simeq \text{Aut}_{\mathbb{F}_{p^k}} \mathbb{F}_{p^n}$. Любое вложение $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^n}$ является изоморфизмом на подполе $\mathbb{F}_q^{G_k}$, ибо переводит элементы \mathbb{F}_{p^k} в корни многочлена $x^{p^k} - x$. Всего таких вложений имеется k , и они образуют одну орбиту группы $\text{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^k}$.

Упражнение 12.16. Покажите, что в $\mathbb{F}_p[x]$ многочлен $x^{p^n} - x$ является произведением всех неприводимых над \mathbb{F}_p приведённых многочленов, степени которых делят n .

ТЕОРЕМА 12.6 (соответствие Галуа)

Для любого конечного расширения Галуа $\mathbb{k} \subset \mathbb{K}$ с группой Галуа $G = \text{Aut}_{\mathbb{k}} \mathbb{K}$ отображение, сопоставляющее подгруппе $H \subseteq G$ её поле инвариантов $\mathbb{K}^H \subseteq \mathbb{K}$, и отображение, сопоставляющее содержащему \mathbb{k} подполю $\mathbb{L} \subseteq \mathbb{K}$ подгруппу $\text{Aut}_{\mathbb{L}} \mathbb{K} \subseteq G$, являются взаимно обратными биекциями между множеством подгрупп $H \subseteq G$ и множеством таких полей \mathbb{L} , что $\mathbb{k} \subseteq \mathbb{L} \subseteq \mathbb{K}$. При этом нормальные подгруппы $H \trianglelefteq G$ взаимно однозначно соответствуют содержащимся в \mathbb{K} расширениям Галуа $\mathbb{L} \supseteq \mathbb{k}$, и в этом случае $\text{Gal } \mathbb{L}/\mathbb{k} \simeq G/H$.

Доказательство. Для любого такого поля \mathbb{L} , что $\mathbb{k} \subseteq \mathbb{L} \subseteq \mathbb{K}$, расширение $\mathbb{L} \subset \mathbb{K}$ нормально по лем. 12.6 на стр. 177 и сепарабельно по сл. 12.2 на стр. 176. Тем самым, оно является расширением Галуа с группой Галуа $H = \text{Aut}_{\mathbb{L}} \mathbb{K}$, причём $|H| = \deg \mathbb{K}/\mathbb{L}$. Очевидно, что H является подгруппой в G . По сл. 12.3 на стр. 179 её поле инвариантов $\mathbb{K}^H = \mathbb{L}$. Наоборот, для любой подгруппы $H \subseteq G$ расширение $\mathbb{K}^H \subseteq \mathbb{K}$ является по теор. 12.5 на стр. 179 расширением Галуа с группой Галуа H . Это доказывает утверждение о биекции. Для доказательства второго утверждения рассмотрим действие группы $G = \text{Gal } \mathbb{K}/\mathbb{k}$ на содержащихся в \mathbb{K} подполях $\mathbb{L} \supset \mathbb{k}$. По уже доказанному, централизатор $C_{\mathbb{L}} \stackrel{\text{def}}{=} \{g \in G \mid g|_{\mathbb{L}} = \text{Id}_{\mathbb{L}}\} = \text{Aut}_{\mathbb{L}} \mathbb{K}$ каждого такого поля \mathbb{L} совпадает с подгруппой $H \subseteq G$, соответствующей по Галуа полю \mathbb{L} . Поскольку расширение $\mathbb{K} \supset \mathbb{L}$ нормально и сепарабельно, любое тождественное на \mathbb{k} вложение $\varphi : \mathbb{L} \hookrightarrow \mathbb{K}$ продолжается до автоморфизма $g : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ над \mathbb{k} . Тем самым, $\varphi(\mathbb{L}) = g(\mathbb{L})$ для некоторого $g \in G$, и централизатор поля $\varphi(\mathbb{L})$ в G сопряжён подгруппе $H : C_{\varphi(\mathbb{L})} = C_{g(\mathbb{L})} = gC_{\mathbb{L}}g^{-1} = gHg^{-1}$. Согласно лем. 12.6 на стр. 177 и сл. 12.2 на стр. 176 расширение $\mathbb{L} \supset \mathbb{k}$ всегда сепарабельно, а нормально если и только если $\varphi(\mathbb{L}) = \mathbb{L}$ для всех тождественных на \mathbb{k} вложений $\varphi : \mathbb{L} \hookrightarrow \mathbb{K}$. Последнее равносильно тому, что все подгруппы, сопряжённые с H , совпадают с H , т. е. нормальности H . В этом случае группа $\text{Gal } \mathbb{K}/\mathbb{k}$ переводит \mathbb{L} в себя, и возникает сюръективный гомоморфизм $\text{Gal } \mathbb{K}/\mathbb{k} \rightarrow \text{Gal } \mathbb{L}/\mathbb{k}$ с ядром $\text{Gal } \mathbb{K}/\mathbb{L}$. Таким образом, $\text{Gal } \mathbb{L}/\mathbb{k} = (\text{Gal } \mathbb{K}/\mathbb{k}) / (\text{Gal } \mathbb{K}/\mathbb{L})$. \square

Упражнение 12.17. Убедитесь, что соответствие Галуа оборачивает включения:

$$H \subset K \subset \text{Gal } \mathbb{K}/\mathbb{k} \iff \mathbb{K}^H \supset \mathbb{K}^K \supset \mathbb{k}$$

¹См. прим. 12.5 на стр. 175.

и что пересечению подгрупп $H_1 \cap H_2$ отвечает композит $\mathbb{K}_1 \mathbb{K}_2$ соответствующих им полей $\mathbb{K}_1 = \mathbb{K}^{H_1}$ и $\mathbb{K}_2 = \mathbb{K}^{H_2}$, а пересечению $\mathbb{K}_1 \cap \mathbb{K}_2$ — наименьшая подгруппа в G , содержащая H_1 и H_2 .

Ответы и указания к некоторым упражнениям

Упр. 12.2. В силу конечности \mathbb{F} гомоморфизм колец $\mathbb{Z} \rightarrow \mathbb{F}$, переводящий $1 \in \mathbb{Z}$ в $1 \in \mathbb{F}$, имеет ненулевое ядро $(p) \subset \mathbb{Z}$, и его образ изоморфен $\mathbb{Z}/(p) \subset \mathbb{F}$. Поскольку в нём нет делителей нуля, число p простое, и образ — поле \mathbb{F}_p совпадающее с простым подполем в \mathbb{F} .

Упр. 12.6. Если $f(x) = (x - \alpha) \cdot g(x)$, то по правилу Лейбница $f'(x) = g(x) + (x - \alpha) \cdot g'(x)$, откуда $g(\alpha) = f'(\alpha) = 0$.

Упр. 12.7. Поскольку $\deg f \geq 2$, производная $f' \neq 0$ и $\deg f' < \deg f$. Так как f не имеет отличных от константы делителей, степень которых меньше $\deg f$, $\text{нод}(f, f') = 1$.

Упр. 12.11. Это вытекает из лем. 12.4.

Упр. 12.16. Корни многочлена $x^{p^n} - x$ распадаются на орбиты группы $G = \text{Aut } \mathbb{F}_{p^n} \simeq \mathbb{Z}/(n)$. Длина m каждой орбиты $\alpha_1, \dots, \alpha_m$ делит n , а произведение $\prod (x - \alpha_i)$ по всем элементам G -орбиты является неприводимым приведённым многочленом с коэффициентами из $\mathbb{F}_p = \mathbb{F}_{p^n}^G$. Поскольку многочлен $x^{p^n} - x$ сепарабелен, его разложение на простые множители в $\mathbb{F}_p[x]$ имеет вид произведения попарно различных приведённых неприводимых многочленов, степени которых делят n . С другой стороны, неприводимый приведённый многочлен $g \in \mathbb{F}_p[x]$ степени m делит $x^{p^n} - x$ тогда и только тогда, когда он имеет корень в поле разложения \mathbb{F}_{p^n} многочлена $x^{p^n} - x$. Это равносильно наличию вложения $\mathbb{F}_p[x]/(g) = \mathbb{F}_{p^m}$ в \mathbb{F}_{p^n} , т. е. тому, что $m|n$.