§13. Алгебраические расширения полей

13.1. Конечные расширения. Поле $\mathbb{F} \supset \Bbbk$, конечномерное как векторное пространство над полем $\Bbbk$, называется *конечным расширением* поля $\Bbbk$. Его размерность $\dim_{\Bbbk} \mathbb{F}$ называется *степенью* $\mathbb{F}$ над $\Bbbk$ и обозначается $\deg \mathbb{F} / \Bbbk$ или $[\mathbb{F} : \Bbbk]$.

Упражнение 13.1. Пусть расширения полей $\Bbbk \subset \mathbb{K} \subset \mathbb{F}$ конечны и $f_1, f_2, \dots, f_m \in \mathbb{F}$ составляют базис $\mathbb{F}$ над $\mathbb{K}$, а $t_1, t_2, \dots, t_n \in \mathbb{K}$ составляют базис $\mathbb{K}$ над $\Bbbk$. Покажите, что mn попарных произведений $f_i t_j$ составляют базис $\mathbb{F}$ над $\Bbbk$. В частности,

$$\deg \mathbb{F}/\Bbbk = \deg \mathbb{F}/\mathbb{K} \cdot \deg \mathbb{K}/\Bbbk. \tag{13-1}$$

Поскольку целость и алгебраичность элемента над полем означают одно и то же, из доказанных в n° 10.1 на стр. 150 свойств целых элементов вытекает, что всякая коммутативная $\Bbbk$-алгебра A, конечномерная как векторное пространство над $\Bbbk$, алгебраична над $\Bbbk$, и если в A нет делителей нуля, то A является полем. Наоборот, любое поле $\mathbb{K} \supset \Bbbk$, конечно порождённое как $\Bbbk$-алгебра, является конечным расширением поля $\Bbbk$. В частности, любая конечно порождённая $\Bbbk$-подалгебра $\Bbbk[a_1, a_2, \dots, a_m]$ в любом поле $\mathbb{F} \supset \Bbbk$ конечной степени над $\Bbbk$ тоже является полем конечной степени над $\Bbbk$, причём эта степень делит $\deg \mathbb{F}/\Bbbk$ по упр. 13.1.

Упражнение 13.2. Убедитесь, что любое конечное поле $\mathbb{F}$ имеет положительную характеристику $\operatorname{char}(\mathbb{F}) = p > 0$, является конечным расширением своего простого подполя[1] $\mathbb{F}_p = \mathbb{Z}/(p)$ и имеет порядок $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}$.

13.1.1. Примитивные расширения. Пусть многочлен $f \in \Bbbk[x]$ неприводим и $\deg f = n > 1$. Алгебра $\Bbbk[x]/(f)$ не имеет делителей нуля и n-мерна над $\Bbbk$. Поэтому она является полем. Элементы этого поля однозначно записываются в виде

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

где $b_i \in \Bbbk$, а класс $\vartheta = x \bmod (f)$ является корнем многочлена f. Поле $\Bbbk[x]/(f)$ называется *примитивным* расширением поля $\Bbbk$, полученным *присоединением* к полю $\Bbbk$ корня ϑ неприводимого многочлена f. Если понятно, какой многочлен f имеется в виду[2], примитивное расширение $\Bbbk[x]/(f)$ часто обозначают $\Bbbk[\vartheta]$ или $\Bbbk(\vartheta)$. Так, запись $\Bbbk\left[\sqrt[m]{a}\right]$ по определению означает примитивное расширение $\Bbbk[x]/(x^m - a)$, где $a \in \Bbbk$ таков, что многочлен $x^m - a$ неприводим в $\Bbbk[x]$.

Пример 13.1 (кубические расширения)
Пусть $\Bbbk$ — произвольное поле и $f = x^3 + a_1x^2 + a_2x + a_3 \in \Bbbk[x]$ неприводим над $\Bbbk$. Поле $\mathbb{K} = \Bbbk[x]/(f)$ имеет степень 3 над $\Bbbk$ и его элементы однозначно записываются в виде $b_0 + b_1\vartheta + b_2\vartheta^2$, где $b_i \in \Bbbk$, а $\vartheta \in \mathbb{K}$ означает класс $x \bmod (f)$. Такие

[1] напомним, что *простым подполем* поля $\mathbb{F}$ называется наименьшее подполе в $\mathbb{F}$, содержащее единицу

[2] без явного указания многочлена f обозначение $\Bbbk[\vartheta]$ мало осмысленно

записи перемножаются и складываются по стандартным правилам раскрытия скобок с учётом соотношения $f(\vartheta)=0$.

Упражнение 13.3. Пусть $\Bbbk=\mathbb{Q}$ 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

$$q(x)=(x-\vartheta_1)(x-\vartheta_2) \tag{13-2}$$

для некоторых $\vartheta_1,\vartheta_2\in\mathbb{K}$, либо неприводим, и тогда разложение (13-2) пишется лишь над квадратичным расширением $\mathbb{L}=\mathbb{K}[x]/(q)$ поля $\mathbb{K}$, степень которого над исходным полем $\Bbbk$ равна 6. Чтобы выяснить, какой из этих двух случаев имеет место, заметим, что *дискриминант*[1]

$$D(f)=(\vartheta-\vartheta_1)^2(\vartheta-\vartheta_2)^2(\vartheta_1-\vartheta_2)^2=q^2(\vartheta)\cdot D(q)\,, \tag{13-3}$$

будучи симметрическим многочленом от корней, является многочленом от коэффициентов f и лежит в $\Bbbk$.

Упражнение 13.4. 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 (13-3), это эквивалентно тому, что квадратом в $\mathbb{K}$ является $D(f)$. Но если $D(f)$ квадрат в $\mathbb{K}$, то он квадрат и в $\Bbbk$: иначе многочлен $x^2-D(f)$ был неприводим над $\Bbbk$, и квадратичное расширение $\Bbbk[x]/\big(x^2-D(f)\big)$ поля $\Bbbk$ вкладывалось бы в поле $\mathbb{K}$ по правилу $x \bmod \big(x^2-D(f)\big)\mapsto\sqrt{D(f)}\in\mathbb{K}$, что невозможно по упр. 13.1, т. к. $\deg\mathbb{K}/\Bbbk=3$. Итак, неприводимый кубический многочлен $f\in\Bbbk[x]$ тогда и только тогда полностью разлагается на линейные множители над кубическим расширением $\Bbbk[x]/(f)$, когда $D(f)$ квадрат в $\Bbbk$.

Упражнение 13.5. 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 $|c|\leqslant 1$, корнем которого является $x=\cos\big(\frac{1}{3}\arccos(c)\big)$.

[1] напомню, что *дискриминантом* приведённого многочлена $f(x)=\prod(x-\vartheta_i)$ называется произведение $D(f)\overset{\text{def}}{=}\prod\limits_{i<j}(\vartheta_i-\vartheta_j)^2$ квадратов разностей его корней

13.1.2. Сепарабельность. Если в рассмотренном выше прим. 13.1 характеристика исходного поля $\Bbbk$ равна 3, некоторые из корней ϑ, ϑ_1 и ϑ_2 многочлена f могут совпасть, хотя он и *неприводим* над $\Bbbk$. Скажем, над полем $\Bbbk = \mathbb{F}_3(t)$ рациональных функций с коэффициентами в поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ многочлен $f(x) = x^3 - t \in \Bbbk[x]$ неприводим, т. к. не имеет корней в $\Bbbk$, однако над примитивным расширением $\mathbb{K} = \Bbbk\left[\sqrt[3]{t}\right] = \Bbbk[x]/(f)$ он становится полным кубом[1]: $x^3 - t = \left(x - \sqrt[3]{t}\right)^3$.

Определение 13.1

Многочлен $f \in \Bbbk[x]$ называется *сепарабельным*, если у него нет кратных корней ни в каком расширении $\mathbb{K} \supset \Bbbk$. Алгебраическое расширение $\mathbb{F} \supset \Bbbk$ (возможно, бесконечное) называется *сепарабельным*, если минимальный над $\Bbbk$ многочлен $\mu_\vartheta \in \Bbbk[x]$ любого элемента $\vartheta \in \mathbb{F} \smallsetminus \Bbbk$ сепарабелен.

Упражнение 13.6. Покажите, что корень $\alpha \in \mathbb{F} \supset \Bbbk$ многочлена $f \in \Bbbk[x]$ является кратным , если и только если $f'(\alpha) = 0$.

Тем самым, многочлен $f \in \Bbbk[x]$ сепарабелен тогда и только тогда, когда

$$\text{нод}(f, f') = 1\,,$$

и это условие проверяемо в самом поле $\Bbbk$ при помощи алгоритма Евклида.

Упражнение 13.7. Убедитесь, что все неприводимые многочлены над любым полем характеристики нуль сепарабельны.

Пример 13.2 (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 $f' \equiv 0$. Над полем $\Bbbk$ характеристики p равенство $f' = 0$ равносильно тому, что показатели всех мономов, входящих в f с ненулевым коэффициентом, делятся на p. Если $\Bbbk = \mathbb{F}_p = \mathbb{Z}/(p)$, так что $a^p = a$ для всех $a \in \Bbbk$, последнее условие означает, что многочлен f является чистой p-той степенью: $f(x) = a_n x^{np} + a_{n-1} x^{(n-1)p} + \dots + a_1 x^p + a_0 = a_n^p x^{np} + a_{n-1}^p x^{(n-1)p} + \dots + a_1^p x^p + a_0^p = \left(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0\right)^p$ и, стало быть, приводим. Тем самым, все неприводимые многочлены над полем $\mathbb{F}_p$ сепарабельны. В частности, каждое конечное поле сепарабельно над своим простым подполем.

Упражнение 13.8. Пусть $\Bbbk = \mathbb{F}_p(t)$. Покажите что многочлен $f(x) = x^p - t \in \Bbbk[x]$ неприводим над $\Bbbk$ и несепарабелен.

[1] напомню, что $(a+b)^3 = a^3 + b^3$ в любом поле характеристики 3

Пример 13.3 (корни из единицы)
Корни уравнения $x^n = 1$ в произвольном поле $\Bbbk$ образуют конечную мультипликативную подгруппу, которая обозначается $\boldsymbol{\mu}_n(\Bbbk)$ и называется *группой корней из единицы* поля $\Bbbk$. Как и всякая конечная мультипликативная подгруппа в поле, группа $\boldsymbol{\mu}_n(\Bbbk)$ циклическая. Если её порядок равен n, то говорят, что поле $\Bbbk$ *содержит все* $\sqrt[n]{1}$, и буде это так, образующие группы $\boldsymbol{\mu}_n(\Bbbk) \simeq \mathbb{Z}/(n)$ называются *первообразными корнями* степени n из единицы. Всего имеется $\varphi(n)$ первообразных корней, и если $\zeta \in \Bbbk$ — один из них, все степени ζ^m с $0 \leqslant m \leqslant n-1$ различны. Поэтому следующие три условия эквивалентны:

- поле $\Bbbk$ допускает расширение, содержащее все $\sqrt[n]{1}$
- многочлен $x^n - 1$ сепарабелен над $\Bbbk$
- $\operatorname{char}(\Bbbk)$ не делит n

Отметим, что при выполнении этих условий любой многочлен $f(x) = x^n - a$ с ненулевым $a \in \Bbbk$ сепарабелен, поскольку $f'(x) = nx^{n-1}$ имеет единственный корень нуль, не являющийся корнем f.

Лемма 13.1
Любое конечное расширение $\mathbb{F} \supset \Bbbk$ можно получить в качестве верхнего этажа башни последовательных примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \tag{13-4}$$

в которых $\mathbb{L}_i = \mathbb{L}_{i-1}[\vartheta_i] \simeq \mathbb{L}_{i-1}[x]/(f_i)$, где $f_i \in \mathbb{L}_{i-1}[x]$ — неприводимый над полем $\mathbb{L}_{i-1}$ многочлен.

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 $\vartheta \in \mathbb{F} \smallsetminus \mathbb{L}_i$ над полем $\mathbb{L}_i$ и вложим примитивное расширение $\mathbb{L}_i[x]/(f)$ в поле $\mathbb{F}$ по правилу $x \bmod (f) \mapsto \vartheta$. 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. □

Лемма 13.2
Для любого многочлена $f \in \Bbbk[x]$ существует конечное расширение $\mathbb{F} \supset \Bbbk$, над которым f полностью раскладывается на линейные множители.

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

Теорема 13.1 (теорема о примитивном элементе)
Всякое конечное сепарабельное расширение $\mathbb{K} \supset \Bbbk$ примитивно, т. е. имеет вид $\mathbb{K} = \Bbbk[x]/(f)$, где $f \in \Bbbk[x]$ — неприводимый многочлен степени $\deg \mathbb{K}/\Bbbk$.

Доказательство. Если поле $\Bbbk$ конечно, поле $\mathbb{K}$ тоже конечно, и его ненулевые элементы образуют циклическую мультипликативную группу. Если $\vartheta \in \mathbb{K}$ — образующая этой группы[1], то $\mathbb{K} = \Bbbk[\vartheta]$. Поэтому далее мы будем считать, поле $\Bbbk$ бесконечным. Индукция по длине башни из лем. 13.1 сводит теорему к случаю, когда поле $\mathbb{K} = \Bbbk[\alpha,\beta] \supset \Bbbk[\alpha] \supset \Bbbk$ является башней двух примитивных расширений и как $\Bbbk$-алгебра порождается двумя сепарабельными алгебраическими элементами α, β. Мы собираемся подобрать $t \in \Bbbk^*$ так, чтобы порождённая над $\Bbbk$ элементом $\vartheta = \alpha + t\beta$ подалгебра $\Bbbk[\vartheta] \subset \mathbb{K}$ совпадала со всем полем $\mathbb{K}$. Так как ϑ алгебраичен над $\Bbbk$, алгебра $\Bbbk[\vartheta]$ всегда будет полем. Достаточно добиться, чтобы оно содержало 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 $\Bbbk$. Элемент β является общим корнем многочлена $f_\beta(x) \in \Bbbk[x]$ и многочлена $g(x) = f_\alpha(\vartheta - tx)$, коэффициенты которого лежат в зависящем от параметра t поле $\Bbbk[\vartheta]$. Рассмотрим любое поле $\mathbb{F} \supset \mathbb{K}$, над которым f_α, f_β, а с ними и g, полностью разлагаются на линейные множители. Если мы подберём t так, чтобы β был *единственным* общим корнем многочленов f_β и g в поле $\mathbb{F}$, то выразив $(x-\beta) = \text{нод}\left(f_\beta(x), g(x)\right)$ через многочлены f_β и g по алгоритму Евклида, мы получим искомое представление β в виде рациональной функции от их коэффициентов, лежащих в поле $\Bbbk[\vartheta]$. Пусть $\deg f_\alpha = m$, $\deg f_\beta = \deg g = k$. Обозначим через $\alpha_1, \alpha_2, \dots, \alpha_m$ и $\beta_1, \beta_2, \dots, \beta_k$ корни многочленов f_α и f_β в $\mathbb{F}$, считая, что $\alpha = \alpha_1$ и $\beta = \beta_1$. Тогда корни g суть $(\vartheta - \alpha_i)/t = \beta_1 + (\alpha_1 - \alpha_i)/t$, где $1 \leqslant i \leqslant m$. Мы хотим, чтобы $\beta_j \neq \beta_1 + (\alpha_1 - \alpha_i)/t$ для всех i, j кроме $i = j = 1$. В силу сепарабельности α при $i \neq 1$ разности $\alpha_1 - \alpha_i \neq 0$, поэтому каждое из неравенств с $i \neq 1$ запрещает ровно одно значение t. При $i = 1$ запреты выражаются неравенствами $\beta_1 \neq \beta_j$ для всех $j \neq 1$, и автоматически соблюдаются в силу сепарабельности β. Таким образом, нам не подходит всего лишь конечное множество значений t, что и доказывает теорему в случае, когда поле $\Bbbk$ бесконечно. □

Следствие 13.1
Если поле $\mathbb{K}$ является сепарабельным алгебраическим расширением поля $\Bbbk$ и степени всех его элементов[2] ограничены, то $\mathbb{K}$ конечно над $\Bbbk$, и $\deg \mathbb{K}/\Bbbk = \max\limits_{\vartheta \in \mathbb{K}} \deg_{\Bbbk} \vartheta$.

[1]это рассуждение показывает, что любое конечное поле как алгебра над любым своим подполем всегда порождается одним элементом — образующей своей мультипликативной группы, и хотя сепарабельность не используется при этом явно, в прим. 13.2 мы видели, что все конечные поля сепарабельны над своими простыми подполями

[2]напомним, что *степенью* алгебраического элемента называется степень минимального многочлена этого элемента

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

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

Лемма 13.3

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

Доказательство. Каждый элемент $\alpha \in \mathbb{F}$ задаёт гомоморфизм

$$\varphi_\alpha : \Bbbk[x] \to \mathbb{F}, \quad g(x) \mapsto g^{\varphi}(\alpha).$$

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 $\widetilde{\varphi}_\alpha : \Bbbk[x]\,/\,(f) \hookrightarrow \mathbb{F}$, переводящего примитивный элемент $\vartheta = x \bmod (f)$ поля $\mathbb{K}$ в $\alpha \in \mathbb{F}$. При этом разные корни $\alpha \neq \beta$ задают разные вложения $\widetilde{\varphi}_\alpha \neq \widetilde{\varphi}_\beta$. С другой стороны, любое вложение $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, совпадающее с φ на подполе $\Bbbk \subset \mathbb{K}$, переводит ϑ в некоторый корень многочлена f^{φ}, т. к. $f^{\varphi}\left(\widetilde{\varphi}(\vartheta)\right) = \widetilde{\varphi}\left(f(\vartheta)\right) = \varphi(0) = 0$. Поэтому $\widetilde{\varphi}$ совпадает с одним из $\widetilde{\varphi}_\alpha$. □

Лемма 13.4

Пусть алгебраическое расширение[1] $\mathbb{K} \supset \Bbbk$ и вложение $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ таковы, что для любого элемента $\vartheta \in \mathbb{K}$ с минимальным над $\Bbbk$ многочленом $\mu_\vartheta \in \Bbbk[x]$ 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 $\Bbbk$ вложение $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, что $\widetilde{\varphi}(\vartheta) = \xi$.

Доказательство. По лем. 13.3 вложение $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ продолжается до вложения $\varphi_\xi : \Bbbk[\vartheta] \hookrightarrow \mathbb{F}$, переводящего ϑ в ξ. Множество всех продолжений $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$

[1] не обязательно конечное

отображения φ_ξ на всевозможные подполя $\Bbbk[\vartheta] \subseteq \mathbb{L} \subseteq \mathbb{K}$ непусто, ибо содержит φ_ξ, и частично упорядочено отношением $(\mathbb{L}'', \psi'') \geqslant (\mathbb{L}', \psi')$ когда $\mathbb{L}'' \supseteq \mathbb{L}'$ и $\psi''|_{\mathbb{L}'} = \psi'$.

Упражнение 13.9. 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 $\vartheta \in \mathbb{K} \smallsetminus \mathbb{L}$, то его минимальный многочлен $\mu_\vartheta \in \Bbbk[x]$ над полем $\Bbbk$ 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. 13.3, и вложение ψ продолжается на строго большее подполе $\mathbb{L}[\vartheta] = \mathbb{L}[x]/(\mu_{\vartheta,\mathbb{L}})$. □

Предложение 13.1

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

Доказательство. Разложим $\mathbb{K}$ в башню (13-4) примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \tag{13-5}$$

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 $\vartheta_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_{i-1}$. 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. 13.3 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 больше, чем $\prod_i [\mathbb{L}_i : \mathbb{L}_{i-1}] = [\mathbb{K} : \Bbbk]$, и их ровно столько, если и только если каждый многочлен f_i^φ имеет $\deg f_i$ различных корней в поле $\mathbb{F}$. Поскольку башню (13-5) можно начать присоединением любого элемента $\vartheta = \vartheta_1 \in \mathbb{K}$, из наличия $[\mathbb{K} : \Bbbk]$ продолжений вытекает, что образ μ_ϑ^φ минимального многочлена $\mu_f = f_1$ любого элемента $\vartheta \in \mathbb{K}$ раскладывается над $\mathbb{F}$ в произведение $\deg \mu_\vartheta$ различных линейных множителей. В частности, μ_f 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 (13-5) 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 $\mathbb{F}[x]$ в произведение попарно различных линейных множителей. Поэтому вложение $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ будет продолжаться вдоль такой цепочки ровно $[\mathbb{K} : \Bbbk]$ способами. □

Упражнение 13.10. Пусть в условиях предл. 13.1 поле $\mathbb{K}$ как алгебра над $\Bbbk$ порождается элементами $\xi_1, \xi_2, \dots, \xi_m$. Покажите, что наличие ровно $[\mathbb{K} : \Bbbk]$ продолжений равносильно тому, что каждый элемент ξ_ν сепарабелен и его минимальный многочлен полностью раскладывается в $\mathbb{F}[x]$ на линейные множители.

Предложение 13.2
Если поле $\mathbb{K} \supset \Bbbk$ алгебраично[1] над $\Bbbk$, то любое вложение $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$, тождественное на подполе $\Bbbk$, является автоморфизмом поля $\mathbb{K}$.

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

13.3. Поле разложения и алгебраическое замыкание. В этом разделе мы установим существование у любого поля $\Bbbk$ некоторых специальных расширений, единственных с точностью до неканонического изоморфизма, тождественно действующего на $\Bbbk$.

Определение 13.2 (поле разложения)
Поле $\mathbb{L}_f \supset \Bbbk$ называется *полем разложения* многочлена $f \in \Bbbk[x]$, если f полностью раскладывается в $\mathbb{L}_f[x]$ на линейные множители, и для любого расширения $\mathbb{F} \supset \Bbbk$, в котором f полностью раскладывается на линейные множители, существует вложение $\mathbb{L}_f \hookrightarrow \mathbb{F}$, тождественное на подполе $\Bbbk$.

Пример 13.4 (поле разложения кубического многочлена)
В прим. 13.1 на стр. 196 мы видели, что полем разложения неприводимого кубического многочлена $f \in \Bbbk[x]$, дискриминант $D(f)$ которого является квадратом в $\Bbbk$, служит примитивное кубическое расширение $\mathbb{K} = \Bbbk[x]/(f)$, а если $D(f)$ не квадрат в $\Bbbk$, 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 $\Bbbk$ степень 6.

Теорема 13.2
У любого многочлена $f \in \Bbbk[x]$ есть поле разложения $\mathbb{L}_f$, и между любыми двумя полями разложения многочлена f имеется тождественный на подполе $\Bbbk$ (но *не* канонический) изоморфизм.

Доказательство. Рассмотрим любое конечное над $\Bbbk$ поле $\mathbb{F} \supset \Bbbk$, над которым f полностью раскладывается на линейные множители[2] и обозначим через $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{F}$ корни f, а через $\mathbb{L}_f$ — наименьшее подполе в $\mathbb{F}$, содержащее $\Bbbk$ и все эти корни. Поле $\mathbb{L}_f$ раскладывается в башню (13-4) примитивных

[1] но не обязательно конечно
[2] см. лем. 13.2 на стр. 199

расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \tag{13-6}$$

на каждом этаже которой присоединяется элемент[1] $\vartheta \in \{\alpha_1, \alpha_2, \dots, \alpha_m\}$. Если поле $\mathbb{F} \subset \Bbbk$ таково, что f полностью раскладывается над ним на линейные множители, включение $\Bbbk \subset \mathbb{F}$ продолжается вдоль башни (13-6) до тождественного на $\Bbbk$ вложения $\mathbb{L}_f \hookrightarrow \mathbb{F}$ по лем. 13.4: минимальный многочлен каждого присоединяемого элемента ϑ, будучи делителем многочлена f, полностью раскладываются над $\mathbb{F}$ 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 $\varphi' : \mathbb{L}'_f \hookrightarrow \mathbb{L}_f$. Поскольку композиции $\varphi \circ \varphi'$ и $\varphi' \circ \varphi$ биективны по предл. 13.2, каждое из вложений сюрьективно, т. е. является изоморфизмом. □

Пример 13.5 (классификация конечных полей)
Согласно упр. 13.2 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 $\mathbb{L}$ 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 $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, сепарабельного, поскольку $f' = 1$. Таким образом, поле $\mathbb{F}$ является полем разложения многочлена f и единственно с точностью до (неканонического) изоморфизма.

Определение 13.3 (алгебраическое замыкание)
Алгебраическое над $\Bbbk$ алгебраически замкнутое поле $\overline{\Bbbk} \supset \Bbbk$ называется *алгебраическим замыканием* поля $\Bbbk$.

> Упражнение 13.11. Покажите, что любое конечное расширение $\mathbb{K} \supset \Bbbk$ допускает тождественное на $\Bbbk$ вложение в любое алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$.

Теорема 13.3
У каждого поля $\Bbbk$ есть алгебраическое замыкание, и между любыми двумя алгебраическими замыканиями поля $\Bbbk$ имеется тождественный на $\Bbbk$ (но *не* канонический) изоморфизм.

Доказательство. Для любых двух алгебраических замыканий $\mathbb{L}'$, $\mathbb{L}''$ поля $\Bbbk$ включение $\Bbbk \subset \mathbb{L}'$ продолжается до тождественного на $\Bbbk$ вложения $\varphi' : \mathbb{L}' \hookrightarrow \mathbb{L}''$. Симметричным образом имеется тождественное на $\Bbbk$ вложение $\varphi'' : \mathbb{L}'' \hookrightarrow \mathbb{L}'$. По предл. 13.2 композиции $\varphi' \circ \varphi''$ и $\varphi'' \circ \varphi'$ биективны. Поэтому φ' и φ'' тоже биективны, и $\mathbb{L}' \simeq \mathbb{L}''$.

[1]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

Существование алгебраического замыкания устанавливается в несколько итераций. Для начала допустим, что поле $\Bbbk$ содержится в алгебраически замкнутом поле $\mathbb{F}$. Тогда множество $\overline{\Bbbk}$ алгебраичных над $\Bbbk$ элементов поля $\mathbb{F}$ является полем по предл. 10.2 на стр. 152. Любой многочлен из $\overline{\Bbbk}[x] \subset \mathbb{F}[x]$ имеет корень ϑ в $\mathbb{F}$. Поскольку ϑ алгебраичен над $\overline{\Bbbk}$, он алгебраичен и над $\Bbbk$, а значит, лежит в $\overline{\Bbbk}$. Тем самым, поле $\overline{\Bbbk}$ алгебраически замкнуто и является алгебраическим замыканием поля $\Bbbk$. Остаётся убедиться в наличии какого-нибудь алгебраически замкнутого поля $\mathbb{F} \supset \Bbbk$. Сначала установим существование поля $\mathbb{F}_1 \supset \Bbbk$, над которым каждый многочлен $f \in \Bbbk[x]$ полностью разлагается на линейные множители. Это делается при помощи трансфинитной индукции. Введём на множестве $\Bbbk[x]$ такой линейный порядок, при котором у любого подмножества имеется минимальный элемент[1]. Тогда для каждого $f \in \Bbbk[x]$ имеется поле $\mathbb{K}_f$ над которым f полностью разлагается на линейные множители и которое содержит аналогичные поля $\mathbb{K}_g$ для всех $g < f$, а также поле $\Bbbk$: для наименьшего $f \in \Bbbk[x]$ таковым полем является поле разложения f над $\Bbbk$, и буде h наименьшим многочленом, для которого такого поля нет, возьмём в качестве $\mathbb{K}_h$ поле разложения h над полем $\bigcup_{f<h} \mathbb{K}_f$. Теперь можно положить $\mathbb{F}_1 = \bigcup_{f\in\Bbbk[x]} \mathbb{K}_f$. Повторяя процедуру, строим бесконечную цепочку вложенных полей $\mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \cdots$, в которой каждый многочлен из $\mathbb{F}_i[x]$ полностью разлагается на множители над $\mathbb{F}_{i+1}$. Поле $\mathbb{L} = \bigcup_{i\in\mathbb{N}} \mathbb{F}_i$ алгебраически замкнуто и содержит $\Bbbk$. □

Следствие 13.2

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 этажа башни $\mathbb{L}_1 \subset \mathbb{L}_2 \subset \mathbb{L}_3$ сепарабельны, то согласно предл. 13.1 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. 13.1 означает сепарабельность расширения $\mathbb{L}_1 \subset \mathbb{L}_3$. □

[1] существование такого порядка на любом множестве составляет утверждение *теоремы Цермело*, которая равносильна лемме Цорна и аксиоме выбора, см. *Ван Дер Варден*. «Алгебра» (М., «Мир», 1976, стр. 246 – 249) или *П. С. Александров*. «Введение в теорию множеств и общую топологию» (М., «Наука», 1977, стр. 80 – 83.)

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

Упражнение 13.12. Покажите, что неприводимый над $\Bbbk$ приведённый многочлен $f \in \Bbbk[x]$, имеющий корень ϑ в алгебраическом расширении $\mathbb{K} \supset \Bbbk$, является минимальным многочленом элемента ϑ над $\Bbbk$.

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

Упражнение 13.13. Убедитесь, что любое квадратичное расширение нормально.

Лемма 13.5
Фиксируем произвольное алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$. Алгебраическое расширение $\Bbbk \subset \mathbb{K}$ нормально тогда и только тогда, когда образы всех тождественных на $\Bbbk$ вложений $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ совпадают друг с другом.

Доказательство. Отождествим $\mathbb{K}$ с подполем $\varphi(\mathbb{K}) \subset \overline{\Bbbk}$ при помощи одного из вложений[1] $\varphi : \mathbb{K} \hookrightarrow \overline{\Bbbk}$ и будем далее считать, что $\Bbbk \subset \mathbb{K} \subset \overline{\Bbbk}$. Любое тождественное на $\Bbbk$ вложение $\psi : \mathbb{K} \hookrightarrow \overline{\Bbbk}$ переводит каждый элемент $\vartheta \in \mathbb{K}$ в один из корней его минимального над полем $\Bbbk$ многочлена $\mu_\vartheta \in \Bbbk[x]$, и если для каждого $\vartheta \in \mathbb{K}$ все корни μ_ϑ лежат в $\mathbb{K}$, то и $\psi(\mathbb{K}) \subset \mathbb{K}$. Наоборот, по лем. 13.4 для каждого корня ξ минимального многочлена $\mu_\vartheta \in \Bbbk[x]$ каждого элемента $\vartheta \in \mathbb{K}$ имеется вложение $\psi_{\vartheta,\xi} : \mathbb{K} \hookrightarrow \overline{\Bbbk}$ с $\psi_{\vartheta,\xi}(\vartheta) = \xi$, и если образы всех вложений $\psi_{\vartheta,\xi}$ лежат в $\mathbb{K}$, то и все корни всех минимальных многочленов всех элементов поля $\mathbb{K}$ лежат в $\mathbb{K}$. □

Лемма 13.6
Пусть в башне алгебраических расширений $\Bbbk \subset \mathbb{L} \subset \mathbb{K}$ поле $\mathbb{K}$ нормально над $\Bbbk$. Тогда $\mathbb{K}$ нормально и над $\mathbb{L}$, а вот $\mathbb{L}$ нормально над $\Bbbk$, если и только если образ любого тождественного на $\Bbbk$ 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 $\Bbbk$, 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. 13.5: фиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \mathbb{K} \supset \mathbb{L} \supset \Bbbk$ и заметим, что образы всех вложений $\mathbb{L} \hookrightarrow \overline{\Bbbk}$ лежат в $\mathbb{K}$, поскольку каждое такое вложение продолжается до вложения $\mathbb{K} \hookrightarrow \overline{\Bbbk}$, образ которого совпадает с $\mathbb{K}$. □

Предостережение 13.1. Башня $\mathbb{F} \supset \mathbb{L} \supset \Bbbk$ нормальных расширений $\mathbb{F} \supset \mathbb{L}$ и $\mathbb{L} \supset \Bbbk$ может не быть нормальным расширением. Например, расширение

[1] существующих по лем. 13.4 на стр. 201

$\mathbb{Q}\left[\sqrt[4]{2}\right] \supset \mathbb{Q}$ представляется башней из двух нормальных по упр. 13.13 квадратичных расширений, не является нормальным: четыре его вложения в алгебраическое замыкание $\overline{\mathbb{Q}} \subset \mathbb{C}$, переводят примитивный элемент $x \bmod (x^4 - 2)$ поля $\mathbb{Q}\left[\sqrt[4]{2}\right] = \mathbb{Q}[x]/(x^4 - 2)$ в четыре разных комплексных корня из 2, и образы этих вложений суть *три* разных подполя в $\mathbb{C}$.

Предложение 13.3
Конечное расширение $\mathbb{K} \supset \Bbbk$ нормально тогда и только тогда, когда $\mathbb{K}$ является полем разложения некоторого многочлена[1] $f \in \Bbbk[x]$.

Доказательство. Пусть нормальное над $\Bbbk$ поле $\mathbb{K} \supset \Bbbk$ порождается как алгебра над $\Bbbk$ элементами $\alpha_1, \alpha_2, \dots, \alpha_k$, и пусть $f_i \in \Bbbk[x]$ — минимальный многочлен элемента α_i над полем $\Bbbk$. Тогда многочлен $f = \prod f_i$ полностью раскладывается над $\mathbb{K}$ на линейные множители, и по упр. 13.10 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 $\mathbb{K} \supset \Bbbk$ является полем разложения некоторого многочлена $f \in \Bbbk[x]$, то любое тождественное на подполе $\Bbbk$ вложение $\mathbb{K}$ в фиксированное алгебраическое замыкание $\overline{\Bbbk}$ является изоморфизмом $\mathbb{K}$ на подполе $\Bbbk[\alpha_1, \alpha_2, \dots, \alpha_k] \subset \overline{\Bbbk}$, порождённое всеми корнями $\alpha_1, \alpha_2, \dots, \alpha_k$ многочлена f в $\overline{\Bbbk}$. Поэтому $\mathbb{K}$ нормально по лем. 13.5. □

13.4.1. Композиты. Зафиксируем алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$. Для любого набора содержащих $\Bbbk$ и содержащихся в $\overline{\Bbbk}$ полей $\mathbb{K}_1, \mathbb{K}_2, \dots, \mathbb{K}_m$ наименьшее подполе в $\overline{\Bbbk}$, которое содержит все поля $\mathbb{K}_\nu$, называется *композитом* этих полей и обозначается $\mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_m$. Иначе композит можно описать как пересечение всех подполей в $\overline{\Bbbk}$, содержащих каждое из полей $\mathbb{K}_i$, или как $\Bbbk$-линейную оболочку всевозможных произведений $\vartheta_1\vartheta_2 \dots \vartheta_m$, где $\vartheta_i \in \mathbb{K}_i$ для каждого i.

Предложение 13.4
Пусть поля $\mathbb{F}$ и $\mathbb{K}$ содержат $\Bbbk$ и содержатся в $\overline{\Bbbk}$. Если поле $\mathbb{K}$ нормально (соотв. сепарабельно) над $\Bbbk$, то композит $\mathbb{K}\mathbb{F}$ нормален (соотв. сепарабелен) над $\mathbb{F}$.

Доказательство. Тождественные на подполе $\mathbb{F} \subset \mathbb{K}\mathbb{F}$ вложения композита $\mathbb{K}\mathbb{F}$ в алгебраическое замыкание $\overline{\mathbb{F}} = \overline{\Bbbk}$ биективно соответствуют тождественным на подполе $\Bbbk \subset \mathbb{K}$ вложениям $\mathbb{K}$ в $\overline{\Bbbk}$: любое вложение $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ по $\mathbb{F}$-линейности продолжается до вложения $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$, и наоборот, каждое $\mathbb{F}$-линейное вложение $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$ ограничивается на подполе $\mathbb{K} \subset \mathbb{K}\mathbb{F}$. Поэтому утверждения непосредственно следуют из лем. 13.5 и предл. 13.1. □

[1] не исключено, что приводимого над $\Bbbk$

Теорема 13.4 (нормальное замыкание)
Для любого конечного сепарабельного расширения $\mathbb{F} \supset \Bbbk$ существует нормальное и сепарабельное над $\Bbbk$ поле $\mathbb{K} \supset \mathbb{F}$, которое вкладывается над $\mathbb{F}$ в любое другое нормальное и сепарабельное над $\Bbbk$ поле $\mathbb{K}' \supset \mathbb{F}$. Все такие поля[1] конечны над $\Bbbk$ и между любыми двумя из них имеется тождественный на подполе $\mathbb{F}$ (но *не* канонический) изоморфизм.

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

13.5. Автоморфизмы полей и соответствие Галуа. Автоморфизмы поля $\mathbb{K}$, тождественно действующие на его подполе $\Bbbk \subset \mathbb{K}$, называются *автоморфизмами* $\mathbb{K}$ *над* $\Bbbk$. Все такие автоморфизмы образуют группу

$$\operatorname{Aut}_{\Bbbk} \mathbb{K} \overset{\text{def}}{=} \{\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K} \mid \varphi(t) = t \ \forall t \in \Bbbk\}.$$

Поскольку каждый автоморфизм $\mathbb{K}$ над $\Bbbk$ является продолжением включения $\Bbbk \subset \mathbb{K}$ на расширение $\mathbb{K} \supset \Bbbk$, порядок группы автоморфизмов конечного расширения $\mathbb{K} \supset \Bbbk$ удовлетворяет неравенству из предл. 13.1 на стр. 202:

$$|\operatorname{Aut}_{\Bbbk} \mathbb{K}| \leqslant \deg \mathbb{K}/\Bbbk .$$

Конечные расширения, для которых это неравенство превращается в равенство, называются *расширениями Галуа*. Из предл. 13.1 вытекает, что конечное расширение является расширением Галуа , если и только если оно нормально и сепарабельно.

Для любой группы G автоморфизмов поля $\mathbb{K}$ элементы $t \in \mathbb{K}$, неподвижные относительно всех преобразований из G, образуют в $\mathbb{K}$ подполе

$$\mathbb{K}^G \overset{\text{def}}{=} \{t \in \mathbb{K} \mid \forall \varphi \in G \ \varphi(t) = t\},$$

которое называется *полем инвариантов группы* G. Отметим, что $\mathbb{K}^G$ содержит простое подполе поля $\mathbb{K}$, изоморфное $\mathbb{Q}$, когда $\operatorname{char}(\Bbbk) = 0$, или $\mathbb{F}_p = \mathbb{Z}/(p)$, когда $\operatorname{char}(\Bbbk) = p > 0$.

Теорема 13.5
Для любой конечной группы G автоморфизмов произвольного поля $\mathbb{K}$ расширение $\mathbb{K} \supset \mathbb{K}^G$ является расширением Галуа степени $|G|$, и $\operatorname{Aut}_{\mathbb{K}^G} \mathbb{K} = G$.

Доказательство. Пусть элементы $\vartheta_1, \vartheta_2, \dots, \vartheta_m \in \mathbb{K}$ попарно различны и составляют G-орбиту элемента $\vartheta = \vartheta_1 \in \mathbb{K}$. Многочлен

$$f_\vartheta(x) = (x - \vartheta_1)(x - \vartheta_2) \cdots (x - \vartheta_m) \tag{13-7}$$

[1] они называются *нормальными замыканиями* сепарабельного расширения $\mathbb{F} \supset \Bbbk$

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 в $\mathbb{K}[x]$ в произведение попарно различных линейных множителей, расширение $\mathbb{K}^G \subset \mathbb{K}$ алгебраично, нормально и сепарабельно, и степень над $\mathbb{K}^G$ любого элемента $\vartheta \in \mathbb{K}$ не выше $|G|$. По сл. 13.1 расширение $\mathbb{K}^G \subset \mathbb{K}$ конечно и $\deg \mathbb{K} / \mathbb{K}^G \leqslant |G|$. С другой стороны, $|G| \leqslant \left|\mathrm{Aut}_{\mathbb{K}^G} \mathbb{K}\right| \leqslant \deg \mathbb{K} / \mathbb{K}^G$. Поэтому все написанные неравенства являются равенствами, и $G = \mathrm{Aut}_{\mathbb{K}^G} \mathbb{K}$. □

Следствие 13.3
Для любых конечного расширения полей $\Bbbk \subset \mathbb{K}$ и подгруппы $G \subset \mathrm{Aut}_\Bbbk \mathbb{K}$ равенства $\mathbb{K}^G = \Bbbk$ и $|G| = \deg \mathbb{K}/\Bbbk$ эквивалентны друг другу, и в случае их выполнения $G = \mathrm{Aut}_\Bbbk \mathbb{K}$.

Доказательство. По теор. 13.5 в башне $\Bbbk \subset \mathbb{K}^G \subset \mathbb{K}$ 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. 13.1, данной при доказательстве теор. 13.5.

Итак, пусть $|G| = \deg \mathbb{K}/\Bbbk$. Из неравенств $|G| \leqslant \deg \mathbb{K}/\mathbb{K}^G \leqslant \deg \mathbb{K}/\Bbbk$ вытекает, что $\deg \mathbb{K} / \mathbb{K}^G = \deg \mathbb{K} / \Bbbk = \deg \mathbb{K} / \mathbb{K}^G \cdot \deg \mathbb{K}^G / \Bbbk$, откуда $\deg \mathbb{K}^G / \Bbbk = 1$ и $\mathbb{K}^G = \Bbbk$. Наоборот, пусть $\mathbb{K}^G = \Bbbk$. Те же рассуждения, что и в теор. 13.5 показывают, что расширение $\mathbb{K} \supset \Bbbk$ нормально и сепарабельно. Поэтому тождественное вложение $\Bbbk \hookrightarrow \mathbb{K}$ продолжается до автоморфизма поля $\mathbb{K}$ над $\Bbbk$ ровно $\deg \mathbb{K} / \Bbbk$ способами, и $\left|\mathrm{Aut}_\Bbbk \mathbb{K}\right| = \deg \mathbb{K}/\Bbbk$. Остаётся показать, что $\mathrm{Aut}_\Bbbk \mathbb{K} = G$. Поскольку коэффициенты минимального многочлена f_ϑ любого элемента $\vartheta \in \mathbb{K}$ инвариантны относительно $\mathrm{Aut}_\Bbbk \mathbb{K}$, каждый автоморфизм $\varphi \in \mathrm{Aut}_\Bbbk \mathbb{K}$ переводит ϑ в один из корней многочлена f_ϑ. Согласно (13-7) эти корни составляют орбиту группы G. Таким образом, для каждого $\vartheta \in \mathbb{K}$ и каждого $\varphi \in \mathrm{Aut}_\Bbbk \mathbb{K}$ существует такой элемент $g \in G$, что $g(\vartheta) = \varphi(\vartheta)$. Поэтому для каждого $\varphi \in \mathrm{Aut}_\Bbbk \mathbb{K}$ поле $\mathbb{K}$ является объединением по всем $g \in G$ конечного числа подмножеств $V_g = \{\vartheta \in \mathbb{K} \mid g(\vartheta) = \psi(\vartheta)\}$, каждое из которых является подпространством конечномерного векторного пространства $\mathbb{K}$ над полем $\Bbbk$. Если поле $\Bbbk$ бесконечно, то конечномерное пространство над ним не представимо в виде объединения конечного числа собственных подпространств[1], и значит, одно из подпространств V_g совпадает с $\mathbb{K}$, откуда[2] $\varphi = g$. Если поле $\Bbbk$ конечно, то $\mathbb{K}$ тоже конечно и порождается над $\Bbbk$ образующей ϑ циклической мультипликативной группы ненулевых элементов поля $\mathbb{K}$. В этом случае $\varphi = g$ для такого $g \in G$, что $\varphi(\vartheta) = g(\vartheta)$. □

[1] см. упр. 11.13 на стр. 170

[2] полезно сопоставить это рассуждение с тем, что использовалось в теор. 13.1 на стр. 200

Пример 13.6 (поле инвариантов группы треугольника)
Рассмотрим проективную прямую $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ над произвольным полем $\Bbbk$. Группа треугольника $G = S_3$ действует на ней дробно линейными преобразованиями, переставляющими точки $0 = (0 : 1)$, $1 = (1 : 1)$, $\infty = (1 : 0)$. Тождественное преобразование, циклы $\tau : 0 \mapsto 1 \mapsto \infty \mapsto 0$, $\tau^{-1} : \infty \mapsto 1 \mapsto 0 \mapsto \infty$ и отражения σ_0, σ_1, σ_∞, оставляющие на месте точки 0, 1, ∞ соответственно, преобразуют аффинную координату $t = t_0/t_1$ по формулам:

$$\begin{array}{lll} \mathrm{Id} : t \mapsto t & \tau : t \mapsto 1/(1-t) & \tau^{-1} : t \mapsto (t-1)/t \\ \sigma_0 : t \mapsto t/(t-1) & \sigma_1 : t \mapsto 1/t & \sigma_\infty : t \mapsto 1-t \end{array} \tag{13-8}$$

которые определяют действие G на поле рациональных функций $\mathbb{K} = \Bbbk(t)$ по правилу $g : \varphi(t) \mapsto \varphi\left(g^{-1}(t)\right)$. Поле инвариантов $\mathbb{K}^G$ этого действия состоит из таких функций $\varphi(t)$, которые не меняются при подстановках (13-8). Согласно теор. 13.5, 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 G-инвариантна и любая рациональная функция от ψ. Такие функции образуют подполе $\Bbbk(\psi) \subset \mathbb{K}^G$, и функция $t \in \mathbb{K}$ является корнем многочлена $\psi \cdot q(x) - p(x)$ с коэффициентами в этом подполе. Поэтому $\dim_{\Bbbk(\psi)} \mathbb{K} \leqslant \max(\deg p, \deg q)$. Так как левая часть этого неравенства делится на $\dim_{\mathbb{K}^G} \mathbb{K} = 6$, мы заключаем, что $\max(\deg p, \deg q)$ не меньше 6, и если он равен 6, то $\mathbb{K}^G = \Bbbk(\psi)$. 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 (13-8) переводят его в многочлен с тем же множеством нулей, т. е. умножают на константы: $f(g^{-1}t) = \lambda(g) \cdot f(t)$, где $\lambda : G \to \Bbbk^*$, $g \mapsto \lambda(g)$, — мультипликативный гомоморфизм, или — что то же самое — 1-мерный характер группы G, коих имеется ровно два: тривиальный и знаковый. Стало быть, f либо инвариантен относительно всех постановок (13-8), либо сохраняется поворотами и меняет знак при отражениях. Из трёхточечной орбиты $\{0, 1, \infty\}$ таким образом получается знакопеременный многочлен $p = t_0t_1(t_0-t_1)$, квадрат которого p^2 G-инвариантен, а из двухточечной, образованной собственными векторами поворотов[1], — G-инвариантный многочлен $q = t_0^2 - t_0t_1 + t_1^2$. Минимальный лоранов моном полной степени нуль[2] по $(t_0 : t_1)$, который можно соорудить из p^2 и q, это

$$\psi(t) = \frac{p^2}{q^3} = \frac{t_0^2t_1^2\left(t_0 - t_1\right)^2}{\left(t_0^2 - t_0t_1 + t_1^2\right)^3} = \frac{t^2(t-1)^2}{(t^2 - t + 1)^3}$$

т. к. это отношение многочленов степени $\leqslant 6$, поле инвариантов $\mathbb{K}^G = \Bbbk(\psi)$.

[1] отметим, что сами точки могут быть и не определены над полем $\Bbbk$, но *инвариантный* многочлен, корнями которого они являются, лежит в $\Bbbk[t_0, t_1]$

[2] а именно они являются рациональными функциями от $t = t_0/t_1$

Упражнение 13.14. Проверьте прямым вычислением, что $\psi(t)$ не меняется при подстановках (13-8).

Пример 13.7 (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 сепарабельно[1], $\left|\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q\right| = [\mathbb{F}_q : \mathbb{F}_p] = n$. Итерации $F_p^0 = \mathrm{Id}$, F_p, F_p^2, … , F_p^{n-1} автоморфизма Фробениуса $F_p : \vartheta \mapsto \vartheta^p$ различны, т. к. равенство $F_p^k = F_p^m$ означает, что все p^n элементов поля $\mathbb{F}_q$ корни многочлена $x^{p^k} - x^{p^m}$, что невозможно при $k, m < n$. Поэтому $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q$ — циклическая группа порядка n, порождённая F_p. Для каждого $k|n$ подгруппа $G_k \subset \mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q$, порождённая автоморфизмом F_p^k, имеет порядок n/k, а её неподвижные точки это 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 $G_k \simeq \mathrm{Aut}_{\mathbb{F}_{p^k}} \mathbb{F}_{p^n}$. 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 $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^k}$.

Упражнение 13.15. 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 13.6 (соответствие Галуа)
Для любого конечного расширения Галуа $\Bbbk \subset \mathbb{K}$ с группой Галуа $G = \mathrm{Aut}_{\Bbbk} \mathbb{K}$ отображение, сопоставляющее подгруппе $H \subseteq G$ её поле инвариантов $\mathbb{K}^H \subseteq \mathbb{K}$, и отображение, сопоставляющее содержащему $\Bbbk$ подполю $\mathbb{L} \subseteq \mathbb{K}$ подгруппу $\mathrm{Aut}_{\mathbb{L}} \mathbb{K} \subseteq G$, являются взаимно обратными биекциями между множеством подгрупп $H \subseteq G$ и множеством таких полей $\mathbb{L}$, что $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$. При этом нормальные подгруппы $H \trianglelefteq G$ взаимно однозначно соответствуют содержащимся в $\mathbb{K}$ расширениям Галуа $\mathbb{L} \supset \Bbbk$, и в этом случае $\mathrm{Gal}\, \mathbb{L}/\Bbbk \simeq G/H$.

Доказательство. Для любого такого поля $\mathbb{L}$, что $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, расширение $\mathbb{L} \subset \mathbb{K}$ нормально по лем. 13.6 и сепарабельно по сл. 13.2. Тем самым, оно является расширением Галуа с группой Галуа $H = \mathrm{Aut}_{\mathbb{L}} \mathbb{K}$, причём $|H| = \deg \mathbb{K}/\mathbb{L}$. Очевидно, что H является подгруппой в G. По сл. 13.3 $K^H = \mathbb{L}$. Отсюда сразу следует утверждение о биекции[2]. Для доказательства второго утверждения рассмотрим действие группы $G = \mathrm{Gal}\, \mathbb{K}/\Bbbk$ на содержащихся в $\mathbb{K}$ подполях $\mathbb{L} \supset \Bbbk$. По уже доказанному, централизатор $C_{\mathbb{L}} \stackrel{\text{def}}{=} \{g \in G \mid g|_{\mathbb{L}} = \mathrm{Id}_{\mathbb{L}}\} = \mathrm{Aut}_{\mathbb{L}} \mathbb{K}$ каждого такого поля $\mathbb{L}$ совпадает с подгруппой $H \subseteq G$, соответствующей по Галуа полю $\mathbb{L}$. Поскольку расширение $\mathbb{K} \supset \Bbbk$ нормально и сепарабельно, любое вложение

$$\varphi : \mathbb{L} \hookrightarrow \mathbb{K} \quad (\text{над } \Bbbk) \tag{13-9}$$

[1] см. прим. 13.5 на стр. 204

[2] вместо сл. 13.3 для доказательства биективности соответствия Галуа можно было бы воспользоваться теор. 13.5, из которой вытекает, что для любой подгруппы $H \subseteq G$ расширение $\mathbb{K}^H \subseteq \mathbb{K}$ является расширением Галуа с группой Галуа H

продолжается до автоморфизма $g : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ над $\Bbbk$, т. е. образ $\varphi(\mathbb{L}) = g(\mathbb{L})$ для некоторого $g \in G$, а его централизатор в G сопряжён подгруппе H:

$$\mathrm{Aut}_{\varphi(\mathbb{L})}\,\mathbb{K} = C_{\varphi(\mathbb{L})} = C_{g(\mathbb{L})} = gC_{\mathbb{L}}g^{-1} = gHg^{-1}\,.$$

Согласно лем. 13.6 и сл. 13.2 расширение $\mathbb{L} \supset \Bbbk$ всегда сепарабельно, а нормально тогда и только тогда, когда $\varphi(\mathbb{L}) = \mathbb{L}$ для всех вложений (13-9). Последнее равносильно тому, что все подгруппы, сопряжённые с H, совпадают с H, т. е. нормальности H. В этом случае группа $\mathrm{Gal}\,\mathbb{K}/\Bbbk$ переводит $\mathbb{L}$ в себя, и возникает сюрьективный гомоморфизм $\mathrm{Gal}\,\mathbb{K}/\Bbbk \twoheadrightarrow \mathrm{Gal}\,\mathbb{L}/\Bbbk$ с ядром $\mathrm{Gal}\,\mathbb{K}/\mathbb{L}$. Таким образом, $\mathrm{Gal}\,\mathbb{L}/\Bbbk = \big(\mathrm{Gal}\,\mathbb{K}/\Bbbk\big)/\big(\mathrm{Gal}\,\mathbb{K}/\mathbb{L}\big)$. □

Упражнение 13.16. Убедитесь, что соответствие Галуа оборачивает включения:

$$H \subset K \subset \mathrm{Gal}\,\mathbb{K}/\Bbbk \iff \mathbb{K}^H \supset \mathbb{K}^K \supset \Bbbk$$

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. 13.2. В силу конечности $\mathbb{F}$ гомоморфизм колец $\mathbb{Z} \to \mathbb{F}$, 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. 13.6. 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. 13.7. Поскольку $\deg f \geqslant 2$, 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. 13.11. Это вытекает из лем. 13.4.

Упр. 13.15. Корни многочлена $x^{p^n} - x$ распадаются на орбиты группы $G = \operatorname{Aut} \mathbb{F}_{p^n} \simeq \mathbb{Z}/(n)$. Длина m каждой орбиты $\alpha_1, \alpha_2, \dots, \alpha_m$ 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 $m|n$.