§3. Расширения Галуа и группы Галуа

3.1. 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 $\operatorname{Aut}_{\Bbbk} \mathbb{K} \stackrel{\text{def}}{=} \{\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K} \mid \varphi(t) = t \ \ \forall\, t \in \Bbbk \ \}$. Так как каждый автоморфизм поля $\mathbb{K}$ 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 $|\operatorname{Aut}_{\Bbbk} \mathbb{K}| \leqslant \deg \mathbb{K}/\Bbbk$ из предл. 2.2 на стр. 17. Конечные расширения, для которых это неравенство превращается в равенство, называются *расширениями Галуа*. Из предл. 2.2 вытекает, что конечное расширение является расширением Галуа, если и только если оно нормально и сепарабельно. Группа автоморфизмов расширения Галуа $\mathbb{K} \supset \Bbbk$ называется *группой Галуа* и обозначается

$$\operatorname{Gal} \mathbb{K}/\Bbbk \stackrel{\text{def}}{=} \operatorname{Aut}_{\Bbbk} \mathbb{K}\,.$$

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 $\operatorname{char}(\Bbbk) = 0$, или $\mathbb{F}_p = \mathbb{Z}/(p)$, когда $\operatorname{char}(\Bbbk) = p > 0$.

Теорема 3.1
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 $\vartheta_1, \dots, \vartheta_m \in \mathbb{K}$ 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. 2.1 на стр. 15 расширение $\mathbb{K}^G \subset \mathbb{K}$ конечно и $\deg \mathbb{K}/\mathbb{K}^G \leqslant |G|$. С другой стороны, $|G| \leqslant \left|\operatorname{Aut}_{\mathbb{K}^G} \mathbb{K}\right| \leqslant \deg \mathbb{K}/\mathbb{K}^G$. Поэтому все написанные неравенства являются равенствами, и $G = \operatorname{Aut}_{\mathbb{K}^G} \mathbb{K}$. □

Следствие 3.1
Для любого конечного расширения полей $\Bbbk \subset \mathbb{K}$ и любой подгруппы $G \subset \operatorname{Aut}_{\Bbbk} \mathbb{K}$ равенства $\mathbb{K}^G = \Bbbk$ и $|G| = \deg \mathbb{K}/\Bbbk$ эквивалентны друг другу, и в случае их выполнения $G = \operatorname{Aut}_{\Bbbk} \mathbb{K}$, а расширение $\Bbbk \subset \mathbb{K}$ является расширением Галуа.

Доказательство. Это вытекает из установленного в теор. 3.1 равенства $\deg \mathbb{K}/\mathbb{K}^G = |G|$. □

Пример 3.1 (поле инвариантов группы треугольника)
Рассмотрим проективную прямую[1] $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ над произвольным полем $\Bbbk$. Группа треугольника[2] $G = S_3$ действует на ней дробно линейными преобразованиями, переставляющими точки $0 = (0 : 1)$, $1 = (1 : 1)$, $\infty = (1 : 0)$. Тождественное преобразование, циклы $\tau = |0, 1, \infty\rangle$,

[1] См. раздел 16.1 на с. 204 лекций [Гео 1].
[2] См. пример 10.3 на с. 171 лекций [Алг 1].

$\tau^{-1} = |\infty, 1, 0\rangle$ 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:

$$\begin{array}{lll} \mathrm{Id}: t \mapsto t & \tau: t \mapsto 1/(1-t) & \tau^{-1}: t \mapsto (t-1)/t \\ \sigma_0: t \mapsto t/(t-1) & \sigma_1: t \mapsto 1/t & \sigma_\infty: t \mapsto 1-t\,. \end{array} \tag{3-1}$$

Эти шесть замен переменной задают действие группы G на поле $\mathbb{K} = \Bbbk(t)$ 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 (3-1). Согласно теор. 3.1, 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 $\Bbbk(\psi) \subset \mathbb{K}^G$, 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 неравенства делится на $\dim_{\mathbb{K}^G} \mathbb{K} = 6$, мы заключаем, что $\max(\deg p, \deg q) \geqslant 6$, где равенство означает, что $\mathbb{K}^G = \Bbbk(\psi)$. Инвариантную функцию ψ степени 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 (3-1) переводят его в многочлен с тем же множеством нулей, т. е. умножают на константы: $f(g^{-1}t) = \lambda(g) \cdot f(t)$ для всех $g \in G$, где $\lambda: G \to \Bbbk^\times$, $g \mapsto \lambda(g)$, является мультипликативным гомоморфизмом, каковых имеется ровно два: тривиальный и знаковый. Поэтому f либо инвариантен относительно всех постановок (3-1), 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 поворотов[1] — G-инвариантный многочлен $q = t_0^2 - t_0 t_1 + t_1^2$. Минимальный лоранов моном полной степени нуль[2] по $(t_0 : t_1)$, который можно соорудить из p^2 и q, это

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

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

Упражнение 3.1. Убедитесь прямым вычислением, что замены (3-1) не меняют $\psi(t)$.

Теорема 3.2 (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 $G_\mathbb{L} = \mathrm{Aut}_\mathbb{L} \mathbb{K} = \{g \in G \mid g|_\mathbb{L} = \mathrm{Id}_\mathbb{L}\}$, 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 $\mathbb{L} \supseteq \Bbbk$, и в этом случае $\mathrm{Gal}\, \mathbb{L}/\Bbbk \simeq G/H$.

[1] Отметим, что сами эти векторы $((1 \pm \sqrt{-3})/2 : 1)$ могут быть и не определены над полем $\Bbbk$, но инвариантный многочлен, корнями которого они являются (в данном случае совпадающий с характеристическим многочленом матрицы $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ оператора поворота τ), лежит в $\Bbbk[t_0, t_1]$.

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

Доказательство. Для любого поля $\mathbb{L}$, включающегося в башню $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, расширение $\mathbb{L} \subset \mathbb{K}$ нормально по лем. 2.5 на стр. 20 и сепарабельно по сл. 2.2 на стр. 19. Тем самым, оно является расширением Галуа с группой Галуа $G_{\mathbb{L}} = \operatorname{Aut}_{\mathbb{L}} \mathbb{K} = \{g \in G \mid g|_{\mathbb{L}} = \mathrm{Id}_{\mathbb{L}}\}$, причём $|H| = [\mathbb{K} : \mathbb{L}]$. По сл. 3.1 на стр. 23 поле инвариантов $K^{\mathbb{G}_{\mathbb{L}}} = \mathbb{L}$. Наоборот, для любой подгруппы $H \subseteq G$ расширение $\mathbb{K}^H \subseteq \mathbb{K}$ является по теор. 3.1 на стр. 23 расширением Галуа с группой Галуа H. Это доказывает утверждение о биекции. Для доказательства второго утверждения заметим, что для любого промежуточного поля $\mathbb{L}$ расширение $\mathbb{L} \supset \Bbbk$ всегда сепарабельно по сл. 2.2 на стр. 19, а нормально оно в силу лем. 2.5 на стр. 20, если и только если $\varphi(\mathbb{L}) = \mathbb{L}$ для всех тождественных на $\Bbbk$ вложений $\varphi : \mathbb{L} \hookrightarrow \mathbb{K}$. Поскольку $\mathbb{K}$ нормально и сепарабельно над $\mathbb{L}$, любое тождественное на $\Bbbk$ вложение $\varphi : \mathbb{L} \hookrightarrow \mathbb{K}$ продолжается до вложения $g : \mathbb{K} \hookrightarrow \mathbb{K}$, автоматически являющегося автоморфизмом поля $\mathbb{K}$ над $\Bbbk$. Тем самым, $\varphi(\mathbb{L}) = g(\mathbb{L})$ для некоторого $g \in G$, и нормальность $\mathbb{L}$ над $\Bbbk$ равносильна тому, что группа Галуа $G = \operatorname{Gal} \mathbb{K}/\Bbbk$ переводит $\mathbb{L}$ в себя. Если это так, то возникает сюръективный гомоморфизм групп $G \twoheadrightarrow \operatorname{Aut}_{\Bbbk} \mathbb{L} = \operatorname{Gal} \mathbb{L}/\Bbbk$. По уже доказанному, его ядро $\{g \in G \mid g|_{\mathbb{L}} = \mathrm{Id}_{\mathbb{L}}\} = \operatorname{Aut}_{\mathbb{L}} \mathbb{K} = G_{\mathbb{L}}$ соответствует по Галуа полю $\mathbb{L}$, откуда $G_{\mathbb{L}} \lhd G$ и $\operatorname{Gal} \mathbb{L}/\Bbbk = G/G_{\mathbb{L}}$. Если же $g(\mathbb{L}) \neq \mathbb{L}$ для некоторого $g \in G$, то соответствующая полю $g(\mathbb{L})$ по Галуа подгруппа $G_{g(\mathbb{L})} = \operatorname{Aut}_{g(\mathbb{L})} \mathbb{K} = \{h \in G \mid h|_{g(\mathbb{L})} = \mathrm{Id}_{g(\mathbb{L})}\} = gG_{\mathbb{L}}g^{-1}$ по уже доказанному будет отлична от $G_{\mathbb{L}}$, и тем самым подгруппа $G_{\mathbb{L}}$ не нормальна в G. □

Упражнение 3.2. Убедитесь, что соответствие Галуа оборачивает включения:

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

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.

Пример 3.2 (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], $\left|\operatorname{Aut}_{\mathbb{F}_p} \mathbb{F}_q\right| = [\mathbb{F}_q : \mathbb{F}_p] = n$. Итерации $F_p^0 = \mathrm{Id}, F_p, F_p^2, \ldots, F_p^{n-1}$ 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 $\operatorname{Aut}_{\mathbb{F}_p} \mathbb{F}_q$ — циклическая группа порядка n, порождённая F_p. Её подгруппы находятся в биекции с натуральными делителями d числа n: для каждого $d|n$ подгруппа $G_d \subset \operatorname{Gal} \mathbb{F}_q/\mathbb{F}_p$ порождается автоморфизмом F_p^d, имеет порядок $|G_d| = n/d$ и индекс $[\operatorname{Gal} \mathbb{F}_q/\mathbb{F}_p : G_d] = d$, а поле её инвариантов $\mathbb{F}_q^{G_d}$ состоит из корней многочлена $x^{p^d} - x$ и тем самым является полем его разложения, изоморфным $\mathbb{F}_{p^d}$. Мы заключаем, что подполя поля $\mathbb{F}_{p^n}$ находятся в биекции с делителями числа n, и подполе, отвечающее делителю d изоморфно $\mathbb{F}_{p^d}$. Иными словами, сопоставление числу $n \in \mathbb{N}$ поля $\mathbb{F}_{p^n}$ задаёт изоморфизм между чумом[2] натуральных чисел с отношением делимости и множеством классов изоморфных конечных полей характеристики p с частичным порядком $\mathbb{F}_1 \leqslant \mathbb{F}_2$, означающим наличие гомоморфного вложения $\mathbb{F}_1 \hookrightarrow \mathbb{F}_2$. Так как поле $\mathbb{F}_{p^d}$ нормально над $\mathbb{F}_p$, все вложения $\mathbb{F}_{p^d} \hookrightarrow \mathbb{F}_{p^n}$ являются изоморфизмами на подполе $\mathbb{F}_q^{G_d}$, всего таких вложений имеется d, и они образуют одну орбиту группы Галуа $\operatorname{Gal} \mathbb{F}_{p^d}/\mathbb{F}_p$.

[1] См. прим. 2.4 на стр. 18.
[2] Т. е. частично упорядоченным множеством, см. раздел 0.7 на с. 17 лекций [Алг 1].

Упражнение 3.3. 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.

Пример 3.3 (подполя кругового поля $\mathbb{Q}[\sqrt[7]{1}]$)
Пусть $\zeta = e^{2\pi i/7} \in \mathbb{C}$. Подалгебра $\mathbb{Q}[\zeta] \subset \mathbb{C}$ является полем разложения кругового многочлена[1] $\Phi_7(x) = x^6 + x^5 + \ldots + x + 1 = (x^7-1)/(x-1)$, неприводимого по критерию Эйзенштейна, применённого к многочлену[2] $\Phi_7(x+1)$. Тем самым, $\mathbb{Q} \subset \mathbb{Q}[\zeta]$ является расширением Галуа степени 6, а его группа Галуа $G = \operatorname{Gal}\mathbb{Q}[\zeta]/\mathbb{Q}$ состоит из 6 элементов и транзитивно действует на примитивных корнях 7-й степени из единицы. Если $g \in G$ переводит ζ в ζ^k, то $g(\zeta^\nu) = g(\zeta)^\nu = \zeta^{k\nu}$ для всех $\nu \in \mathbb{Z}/(7)$, и сопоставление $g \mapsto k$ изоморфно отображает группу G на группу $\operatorname{Aut}_{\mathbb{Z}}(\mathbb{Z}/(7)) = \mathbb{F}_7^\times$ — мультипликативную циклическую группу порядка 6, порождённую первообразным вычетом $[3]_7$ по модулю 7. Мы заключаем, что $G \simeq \mathbb{Z}/(6)$ порождается автоморфизмом $\sigma : \zeta \mapsto \zeta^3$ и имеет ровно две собственные подгруппы: $H_2 \simeq \mathbb{Z}/(3)$ индекса 2, порождённую автоморфизмом σ^2, и $H_3 \simeq \mathbb{Z}/(2)$ индекса 3, порождённую автоморфизмом σ^3, обе нормальные в силу коммутативности группы G. Так как их поля инвариантов $\mathbb{L}_2 = \mathbb{Q}[\zeta]^{H_2}$ и $\mathbb{L}_3 = \mathbb{Q}[\zeta]^{H_3}$ имеют над $\mathbb{Q}$ степени 2 и 3, они выглядят как $\mathbb{Q}[\vartheta_2]$ и $\mathbb{Q}[\vartheta_3]$, где $\vartheta_2, \vartheta_3 \in \mathbb{Q}[\zeta]\smallsetminus\mathbb{Q}$ — какие-нибудь элементы, инвариантные относительно σ^2 и σ^3 соответственно.

В качестве ϑ_2 можно взять сумму $\vartheta_2 = \zeta + \zeta^2 + \zeta^4$ элементов H_2-орбиты числа ζ. Сопряжённым к ϑ_2 относительно действия группы Галуа $\operatorname{Gal}\mathbb{L}_2/\mathbb{Q} \simeq G/H_2 \simeq \mathbb{Z}/(2)$ является

$$\vartheta_2' = \sigma(\vartheta_2) = \zeta^3 + \zeta^6 + \zeta^5 .$$

Поскольку[3] $\vartheta_2 + \vartheta_2' = -1$ и $\vartheta_2\vartheta_2' = 2$, минимальным многочленом элемента ϑ_2 над $\mathbb{Q}$ является $x^2 + x + 2$ с дискриминантом $D = (\vartheta_2 - \vartheta_2')^2 = -7$. Мы заключаем, что $\mathbb{L}_2 = \mathbb{Q}[\sqrt{-7}]$.

Аналогично, в качестве ϑ_3 можно взять сумму $\zeta + \sigma^2(z) = \zeta + \zeta^{-1} = 2\cos(2\pi/7)$. Сопряжёнными к ϑ_3 относительно действия группы Галуа $\operatorname{Gal}\mathbb{L}_3/\mathbb{Q} \simeq G/H_3 \simeq \mathbb{Z}/(3)$ являются $\vartheta_3' = \sigma(\vartheta_3) = \zeta^3 + \zeta^{-3}$ и $\vartheta_3'' = \sigma^2(\vartheta_3) = \zeta^2 + \zeta^{-2}$. Так как[4]

$$\vartheta_3 + \vartheta_3' + \vartheta_3'' = -1\,, \quad \vartheta_3\vartheta_3' + \vartheta_3'\vartheta_3'' + \vartheta_3\vartheta_3'' = -2\,, \quad \vartheta_3\vartheta_3'\vartheta_3'' = 1\,,$$

мы заключаем, что минимальный полином элемента ϑ_3 над $\mathbb{Q}$ равен $f(x) = x^3 + x^2 - 2x - 1$, и поле $\mathbb{L}_3$ является полем разложения многочлена f. Обратите внимание, что поскольку оно имеет степень 3 над $\mathbb{Q}$, дискриминант многочлена f является полным квадратом[5] в $\mathbb{Z}$. Отметим также, что $\cos(2\pi/7) = \vartheta_3/2$ имеет над $\mathbb{Q}$ минимальный многочлен

$$f(2x)/8 = x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{8}\,.$$

3.2. Рабочий пример: построения циркулем и линейкой. Отождествим ориентированную евклидову плоскость с полем $\mathbb{C}$, указав на ней точки 0 и 1. Традиционный набор школьных задач на построение:

[1] См. раздел 2.4.3 на с. 50 лекций [Алг 1].
[2] См. пример 4.11 на с. 80 лекций [Алг 1].
[3] Обязательно проверьте эти равенства, пользуясь соотношением $\Phi_7(\zeta) = 0$.
[4] Обязательно убедитесь в этом!
[5] См. прим. 2.3 на стр. 18.

Упражнение 3.4. Даны точки $0,\ 1,\ a,\ b \in \mathbb{C}$. Циркулем и линейкой постройте в $\mathbb{C}$ точки $a \pm b$, a/b, ab и $\sqrt{a}$.

показывает, что каждая точка ζ любого подполя $\mathbb{L} \subset \mathbb{C}$, которое можно получить последовательными квадратичными расширениями поля $\mathbb{Q}$:

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L}\,,\ \text{где } \mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big] \text{ и } a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2\,, \tag{3-2}$$

может быть построена циркулем и линейкой. Покажем, что верно и обратное: если число $\zeta \in \mathbb{C}$ строится при помощи циркуля и линейки, отправляясь от заданных точек 0 и 1, то оно лежит в таком подполе $\mathbb{L} \subset \mathbb{C}$, к которому ведёт башня квадратичных расширений вида (3-2), причём каждое из полей $\mathbb{L}_i$ этой башни переводятся в себя комплексным сопряжением $z \mapsto \overline{z}$.

Построение числа ζ распадается на элементарные шаги, каждый из которых по уже построенным точкам a, b, c, d строит новую точку p, являющуюся пересечением либо прямых (ab) и (cd), либо прямой (ab) и проходящей через d окружности с центром в c, либо проходящих через b и d окружностей с центрами в a и c соответственно, в ситуации, когда эти точки пересечения существуют. Положим $\mathbb{L}_1 = \mathbb{Q}[\sqrt{-1}]$ и будем по индукции считать, что a, b, c, d лежат в поле $\mathbb{L}_i$ из башни (3-2), причём комплексное сопряжение переводит поле $\mathbb{L}_i$ в себя. Последнее условие гарантирует, что вместе с каждым числом поле $\mathbb{L}_i$ содержит его вещественную и мнимую части. Число $(ab) \cap (cd)$ находится по правилу Крамера и тоже лежит в $\mathbb{L}_i$. Для отыскания пары чисел, возникающих при пересечении проходящей через d окружности S с центром c и прямой (ab) или проходящей через b окружностью с центром a зададим окружность S уравнением $(z-c)(\overline{z}-\overline{c}) = (d-c)(\overline{d}-\overline{c})$ и подставим в него зависящую от параметра t точку $z = a+(b-a)\,t$, которая при t, пробегающем вещественную прямую $\mathbb{R} \subset \mathbb{C}$, движется по прямой (ab), а при t, пробегающем единичную окружность $\mathrm{U}_1 \subset \mathbb{C}$, движется по проходящей через b окружности с центром в a. Так как в первом случае $\overline{t} = t$, а во втором $\overline{t} = t^{-1}$, мы получим на t квадратное уравнение с коэффициентами из $\mathbb{L}_i$ и вещественным дискриминантом $D \in \mathbb{L}_i \cap \mathbb{R}$.

Упражнение 3.5. Убедитесь в этом, явно выписав эти уравнения в обоих случаях.

Корни этого уравнения лежат либо в поле $\mathbb{L}_i$, либо в квадратичном расширении $\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{D}]$, которое переводится комплексным сопряжением в себя. Искомые точки пересечения получаются подстановкой этих корней вместо t в параметрическое представление $a+(b-a)\,t$ прямой или окружности, а значит, лежат в $\mathbb{L}_{i+1}$, что воспроизводит предположение индукции.

Предложение 3.1
Конечное расширение Галуа $\mathbb{K} \supset \Bbbk$ тогда и только тогда содержится в поле $\mathbb{L} \supset \Bbbk$, которое можно получить последовательными квадратичными расширениями поля $\Bbbk$:

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L}\,,\ \text{где } \mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big] \text{ и } a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2\,, \tag{3-3}$$

когда $[\mathbb{K} : \Bbbk] = 2^n$ для некоторого $n \in \mathbb{N}$.

Доказательство. Пусть $\mathbb{K}$ содержится в башне (3-3). Из мультипликативности степени вытекает, что $[\mathbb{L} : \Bbbk] = 2^m$, а значит и $[\mathbb{K} : \Bbbk]$, будучи делителем $[\mathbb{L} : \Bbbk]$, тоже является степенью двойки. Наоборот, если $[\mathbb{K} : \Bbbk] = |\mathrm{Gal}\,\mathbb{K}/\Bbbk| = 2^n$, то группа Галуа $G = \mathrm{Gal}\,\mathbb{K}/\Bbbk$ является 2-группой, и её ряд Жордана–Гёльдера[1] $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$ имеет композиционные факторы

[1] См. раздел 11.2 на с. 190 лекций [Алг 1].

$G_i / G_{i+1} \simeq \mathbb{Z}/(2)$ при всех i. Соответствие Галуа[1] сопоставляет этой башне подгрупп башню квадратичных расширений $\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_n = \mathbb{K}$, где $\mathbb{L}_i = \mathbb{K}^{G_i}$. □

Теорема 3.3
Корень неприводимого многочлена $f \in \mathbb{Q}[x]$ может быть построен в $\mathbb{C}$ циркулем и линейкой исходя из точек $0,\ 1 \in \mathbb{C}$, если и только если степень поля разложения f над $\mathbb{Q}$ является степенью двойки, и в этом случае все корни многочлена f строятся циркулем и линейкой.

Доказательство. Поле разложения $\mathbb{K}$ многочлена f над $\mathbb{Q}$ является расширением Галуа. Если $\deg \mathbb{K}/\mathbb{Q} = 2^m$, то поле $\mathbb{K}$ можно получить из $\mathbb{Q}$ последовательными квадратичными расширениями, как мы видели в доказательстве предл. 3.1 выше. Поэтому все числа из поля $\mathbb{K}$ можно построить циркулем и линейкой. Наоборот, пусть у многочлена f имеется корень $\vartheta \in \mathbb{C}$, который можно построить циркулем и линейкой. Тогда примитивное расширение $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ содержится в некотором расширении $\mathbb{L}$ вида (3-2). Автоморфизм поля $\mathbb{K}$, переводящий корень ϑ в другой корень ϑ' многочлена f переводит подполе $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ в подполе $\mathbb{Q}[\vartheta'] \subset \mathbb{C}$. Получающееся таким образом вложение полей $\psi\colon \mathbb{Q}[\vartheta] \hookrightarrow \mathbb{C}$, $\vartheta \mapsto \vartheta'$, продолжается до вложения $\widetilde{\psi}\colon \mathbb{L} \hookrightarrow \mathbb{C}$, совпадающего с ψ на подполе $\mathbb{Q}[\vartheta] \subset \mathbb{L}$ и переводящего башню (3-2) в башню

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}'_1 \subset \ldots \subset \mathbb{L}'_m = \mathbb{L}'\,, \tag{3-4}$$

в которой $\mathbb{L}'_{i+1} = \mathbb{L}'_i\big[\sqrt{a'_i}\big]$, где $a'_i = \widetilde{\psi}(a_i) \in \mathbb{L}'_i \smallsetminus \big(\mathbb{L}'_i\big)^2$. Так как $\vartheta' \in \mathbb{L}'$, корень ϑ' тоже строится циркулем и линейкой. Композит $\mathbb{L}\mathbb{L}'$ содержит оба корня ϑ, ϑ' и также является башней квадратичных расширений, поскольку получается последовательным присоединением к $\mathbb{L}$ чисел $a'_1, \ldots, a'_m$, степени которых над соответствующими подполями $\mathbb{L}$, $\mathbb{L}\mathbb{L}'_1$, … , $\mathbb{L}\mathbb{L}'_{m-1}$ не превышают двойки. Продолжая по индукции, мы построим башню квадратичных раширений, содержащую все корни многочлена f, а значит и его поле разложения $\mathbb{K}$. По предл. 3.1 степень $[\mathbb{K} : \mathbb{Q}]$ в этом случае является степенью двойки, что и утверждалось. □

Следствие 3.2
Если число $\zeta \in \mathbb{C}$ строится циркулем и линейкой по данным точкам 0 и 1, то оно алгебраично над $\mathbb{Q}$ и его степень над $\mathbb{Q}$ является степенью двойки.

Доказательство. Примитивное расширение $\mathbb{Q}[\zeta]$ содержится в поле разложения минимального многочлена числа ζ, поэтому степень этого расширения над $\mathbb{Q}$ делит степень поля разложения минимального многочлена. □

Пример 3.4 (трисекция угла, удвоение куба и правильный семиугольник)
Угол $\pi/3$ нельзя разделить на три равные части циркулем и линейкой, поскольку такая возможность влечёт возможность построения циркулем и линейкой числа $\cos(\pi/9)$, имеющего над $\mathbb{Q}$ степень 3.

Упражнение 3.6. Убедитесь, что $\cos(\pi/9)$ является корнем неприводимого над $\mathbb{Q}$ многочлена $8x^3 - 6x - 1$.

По той же причине циркулем и линейкой нельзя построить сторону куба, объём которого вдвое больше объёма единичного куба: это равносильно построению корня неприводимого над $\mathbb{Q}$ многочлена $x^3 - 2$. Правильный семиугольник тоже нельзя построить циркулем и линейкой:

[1] См. теор. 3.2 на стр. 24.

такое построение позволяло бы построить первообразный корень $\sqrt[7]{1} = e^{2\pi i/7}$, минимальный многочлен которого[1] $\Phi_7(x) = (x^7 - 1)/(x - 1)$ имеет степень 6.

3.2.1. Влияние побочных иррациональностей. Задачу о построении циркулем и линейкой можно расширить, считая что в начале построения даны не только точки 0, 1, но и некоторые другие точки $\zeta_1, \dots, \zeta_n \in \mathbb{C}$. Поскольку все точки порождённого этими числами поля $\mathbb{F} = \mathbb{Q}(\zeta_1, \dots, \zeta_n) \subset \mathbb{C}$ строятся циркулем и линейкой, можно считать, что дополнительно заданные точки образуют подполе[2] $\mathbb{F} \subset \mathbb{C}$, элементы которого принято называть *побочными иррациональностями*. Всё сказанное выше сохраняет силу после замены поля $\mathbb{Q}$ полем $\mathbb{F}$. А именно, если даны все точки поля $\mathbb{F}$, то число $\zeta \in \mathbb{C}$ строится циркулем и линейкой, если и только если оно содержится в конечной башне последовательных квадратичных расширений поля $\mathbb{F}$, и это равносильно тому, что ζ алгебраично над $\mathbb{F}$ и степень поля разложения его минимального многочлена над $\mathbb{F}$ является степенью двойки. В частности, для этого необходимо, чтобы степень самого минимального многочлена тоже была степенью двойки.

Упражнение 3.7. Докажите все эти утверждения.

В самом общем виде взятие композита с произвольным полем побочных иррациональностей действует на расширение Галуа следующим образом.

Предложение 3.2 (теорема о побочных иррациональностях)
Пусть поля $\mathbb{F}, \mathbb{K} \supset \Bbbk$ содержатся в некотором общем алгебраически замкнутом поле $\mathbb{L}$ и расширение $\mathbb{K} \supset \Bbbk$ является конечным расширением Галуа. Тогда $\mathbb{FK} \supset \mathbb{F}$ также является конечным расширением Галуа, и его группа Галуа изоморфна подгруппе $H_{\mathbb{F}\cap\mathbb{K}} \subset \operatorname{Gal} \mathbb{K}/\Bbbk$, отвечающей при соответствии Галуа промежуточному подполю $\Bbbk \subset \mathbb{F} \cap \mathbb{K} \subset \mathbb{K}$.

Доказательство. По предл. 2.3 на стр. 21 поле $\mathbb{K}$ является полем разложения некого сепарабельного многочлена $f \in \Bbbk[x]$ и порождается как $\Bbbk$-алгебра его корнями $\vartheta_1, \dots, \vartheta_n \in \mathbb{L}$. Они же порождают $\mathbb{FK}$ как алгебру над $\mathbb{F}$. По предл. 2.4 расширение $\mathbb{FK} \supset \mathbb{F}$ нормально и сепарабельно, т. е. является конечным расширением Галуа. Тем самым, $\mathbb{FK}$ является полем разложения f над $\mathbb{F}$. Автоморфизмы $\mathbb{K}$ над $\Bbbk$ и $\mathbb{FK}$ над $\mathbb{F}$ оставляют многочлен f на месте и переводят множество его корней в себя, причём каждый автоморфизм однозначно определяется своим действием на корни. Это позволяет рассматривать обе группы $\operatorname{Gal} \mathbb{K}/\Bbbk$ и $\operatorname{Gal} \mathbb{FK}/\mathbb{F}$ как подгруппы в S_n: группа $\operatorname{Gal} \mathbb{K}/\Bbbk$ состоит из всех перестановок корней $\vartheta_1, \dots, \vartheta_n$, которые продолжаются до автоморфизма порождённой ими $\Bbbk$-алгебры $\mathbb{K} = \Bbbk[\vartheta_1, \dots, \vartheta_n]$, а группа $\operatorname{Gal} \mathbb{FK}/\mathbb{F}$ — из перестановок, продолжающихся до автоморфизма $\mathbb{F}$-алгебры $\mathbb{FK} = \mathbb{F}[\vartheta_1, \dots, \vartheta_n]$. Так как $\Bbbk \subset \mathbb{F}$, вторая группа содержится в первой и состоит в точности из всех $\mathbb{F}$-линейных преобразований $g : \Bbbk[\vartheta_1, \dots, \vartheta_n] \to \Bbbk[\vartheta_1, \dots, \vartheta_n]$ из группы $\operatorname{Gal} \mathbb{K}/\Bbbk$. Но $\mathbb{F}$-линейность оператора g в точности и означает, что g оставляет на месте подполе $\mathbb{F} \cap \mathbb{K}$. □

3.3. Группы Галуа многочленов. Согласно предл. 2.3 на стр. 21, поле разложения $\mathbb{L}_f$ любого сепарабельного многочлена $f \in \Bbbk[x]$ является расширением Галуа поля $\Bbbk$. Его группа Галуа над $\Bbbk$ обозначается через $\operatorname{Gal} f/\Bbbk$ и называется *группой Галуа многочлена* f над $\Bbbk$. Так как коэффициенты f инвариантны относительно действия группы Галуа, возникает каноническое действие группы $\operatorname{Gal} f/\Bbbk$ на корнях $\vartheta_1, \dots, \vartheta_n$ многочлена f, и поскольку поле $\mathbb{L}_f$ как алгебра над $\Bbbk$ порождается этими корнями, каждый автоморфизм из группы Галуа однозначно определяется

[1] Ср. с прим. 3.3 на стр. 26.
[2] Не обязательно алгебраическое над $\mathbb{Q}$.

своим действием на корнях, т. е. группа Галуа *канонически вложена* в группу перестановок корней. Перестановка корней лежит в группе Галуа тогда и только тогда, когда она сохраняет все полиномиальные соотношения между корнями. Формализуется это следующим образом.

Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$. Поле разложения $\mathbb{L}_f \subset \overline{\Bbbk}$ является образом гомоморфизма вычисления

$$\mathrm{ev}_{\vartheta_1,\dots,\vartheta_n} : \Bbbk[t_1,\dots,t_n] \to \overline{\Bbbk}, \quad \psi \mapsto \psi(\vartheta_1,\dots,\vartheta_n), \tag{3-5}$$

ядро которого $I_\Bbbk(\vartheta) \stackrel{\text{def}}{=} \ker \mathrm{ev}_{\vartheta_1,\dots,\vartheta_n}$ является идеалом, состоящим из всех полиномиальных соотношений между корнями многочлена f, т. е. из всех многочленов $\psi \in \Bbbk[t_1,\dots,t_n]$, равных нулю в точке $\vartheta = (\vartheta_1,\dots,\vartheta_n) \in \mathbb{A}^n\big(\overline{\Bbbk}\big)$. Перестановка переменных $g : t_i \mapsto t_{g(i)}$ корректно факторизуется до эндоморфизма алгебры $\mathbb{L}_f = \Bbbk[t_1,\dots,t_n]/I_\Bbbk(\vartheta)$, если и только если она переводит идеал $I_\Bbbk(\vartheta)$ себя, т. е. когда для любого $\psi \in I_\Bbbk(\vartheta)$ многочлен $\psi^g(t_1,\dots,t_n) \stackrel{\text{def}}{=} \psi(t_{\sigma(1)},\dots,t_{\sigma(n)})$ тоже лежит в $I_\Bbbk(\vartheta)$. Тем самым, группа Галуа многочлена f имеет вид

$$\mathrm{Gal}\, f/\Bbbk \simeq \{g \in S_n \mid \forall \psi \in I_\Bbbk(\vartheta)\ \psi^g \in I_\Bbbk(\vartheta)\} \tag{3-6}$$

Именно так изначально и определял группу многочлена сам Галуа.

Замечание 3.1. Задаваемое формулой (3-6) вложение группы Галуа $\mathrm{Gal}\, f$ в стандартную симметрическую группу $S_n = \mathrm{Aut}\{1,\dots,n\}$ не является каноническим и *зависит* от выбора нумерации корней ϑ_i многочлена f.

Предложение 3.3
Множество нулей идеала $I_\Bbbk(\vartheta)$ в аффинном пространстве $\mathbb{A}^n(\overline{\Bbbk})$:

$$V(I_\Bbbk(\vartheta)) = \{p \in \mathbb{A}^n(\overline{\Bbbk}) \mid f(p) = 0\ \forall f \in I_\Bbbk(\vartheta)\}$$

представляет собой набор из $m = [\mathbb{L}_f : \Bbbk] = |\mathrm{Gal}\, f/\Bbbk|$ различных точек $\vartheta_g = (\vartheta_{g(1)},\dots,\vartheta_{g(n)})$, где $g \in \mathrm{Gal}\, f/\Bbbk$, составляющих одну орбиту действия группы $\mathrm{Gal}\, f/\Bbbk \subset S_n$ на пространстве $\mathbb{A}^n$ перестановками координат.

Доказательство. Пусть $f = x^n + a_1 x^{n-1} + \dots + a_n$. По теореме Виета

$$e_i(\vartheta_1,\dots,\vartheta_n) = (-1)^i a_i,$$

где $e_i \in \Bbbk[t_1,\dots,t_n]$ — элементарный симметрический многочлен. Тем самым, для каждого i

$$e_i(t_1,\dots,t_n) - (-1)^i a_i \in I_\Bbbk(\vartheta).$$

Если точка $a = (\alpha_1,\dots,\alpha_n) \in V\left(I_\Bbbk(\vartheta)\right)$, то $e_i(\alpha_1,\dots,\alpha_n) = (-1)^i a_i$, откуда

$$(x-\alpha_1)\dots(x-\alpha_n) = f(x) = (x-\vartheta_1)\dots(x-\vartheta_n),$$

т. е. $(\alpha_1,\dots,\alpha_n) = (\vartheta_{g(1)},\dots,\vartheta_{g(n)})$ для некоторой перестановки $g \in S_n$. Если g не лежит в группе $\mathrm{Gal}\, f/\Bbbk$, то найдётся такой многочлен $\psi \in I_\Bbbk(\vartheta)$, что $\psi^g \notin I_\Bbbk(\vartheta)$, и тогда

$$\psi(\alpha_1,\dots,\alpha_n) = \psi(\vartheta_{g(1)},\dots,\vartheta_{g(n)}) = \psi^g(\vartheta_1,\dots,\vartheta_n) \neq 0,$$

что невозможно для точки $a \in V\left(I_{\Bbbk}(\vartheta)\right)$. Мы заключаем, что координаты каждой точки $a \in \in V\left(I_{\Bbbk}(\vartheta)\right)$ получаются из координат точки ϑ перестановкой из группы Галуа многочлена f. Наоборот, для любой перестановки $g \in \operatorname{Gal} f/\Bbbk$ и всех $\psi \in I_{\Bbbk}(\vartheta)$

$$\psi(\vartheta_{g(1)}, \dots, \vartheta_{g(n)}) = \psi^g(\vartheta_1, \dots, \vartheta_n) = 0\,,$$

так как $\psi^g \in I_{\Bbbk}(\vartheta)$. Поэтому все точки из $\operatorname{Gal} f/\Bbbk$-орбиты точки ϑ лежат в $V(I_{\Bbbk}(\vartheta))$. □

Упражнение 3.8. Покажите, что сепарабельный многочлен $f \in \Bbbk[x]$ неприводим если и только если группа $\operatorname{Gal} f/\Bbbk$ транзитивно действует на его корнях.

Пример 3.5 (дискриминант)
Пусть приведённый многочлен $f \in \Bbbk[x]$ степени n имеет корни $\vartheta_1, \dots, \vartheta_n$ в своём поле разложения $\mathbb{E}_f \subset \Bbbk$. Положим

$$\delta_f = \prod_{i<j}(\vartheta_i - \vartheta_j)\,, \quad D(f) = \delta_f^2 = \prod_{i<j}(\vartheta_i - \vartheta_j)^2\,.$$

Число $\delta_f \in \mathbb{E}_f$ зависит от выбора нумерации корней и меняет знак при их нечётной перестановке. Его квадрат $D(f)$, будучи симметрическим многочленом от корней, является полиномом от коэффициентов многочлена f и лежит в $\Bbbk$. Он называется *дискриминантом*[1] многочлена f.

Упражнение 3.9. Убедитесь, что дискриминант кубического многочлена $x^3 + ax^2 + bx + c$ равен $-4ca^3 + b^2a^2 + 18cba - (4b^3 + 27c^2)$.

Обращение дискриминанта в нуль равносильна несепарабельности многочлена f. Если f сепарабелен и неприводим, то $D(f)$ является квадратом в $\Bbbk$, если и только если числа $\pm\delta_f$ лежат в $\Bbbk$ и тем самым инвариантны относительно группы Галуа $\operatorname{Gal} f/\Bbbk = \operatorname{Gal} \mathbb{E}_f/\Bbbk$. В этом случае группа Галуа осуществляет только чётные перестановки корней и таким образом содержится в A_n. Если же пересечение $A_n \cap \operatorname{Gal} f/\Bbbk$ является собственной подгруппой группы Галуа, то эта подгруппа имеет индекс 2, и квадратичное над $\Bbbk$ подполе в $\mathbb{E}_f$, соответствующее ей по Галуа, имеет вид $\Bbbk[\delta_f] = \Bbbk[\sqrt{D(f)}]$.

Пример 3.6 (многочлены степени 3, продолжение прим. 2.1)
Группа Галуа $G_f = \operatorname{Gal} f/\Bbbk$ неприводимого сепарабельного кубического многочлена $f \in \Bbbk[x]$ транзитивно действует на его корнях. Поэтому она либо совпадает со всей симметрической группой S_3, либо является группой чётных перестановок $A_3 \simeq \mathbb{Z}/(3)$ и осуществляет лишь циклические перестановки корней. Как мы видели в прим. 3.5 выше, последнее равносильно тому, что дискриминант $D(f)$ является квадратом в $\Bbbk$. Это согласуется с прим. 2.1 на стр. 13, где мы установили, что степень поля разложения многочлена f над $\Bbbk$ равна 3 или 6 в в соответствии с тем, квадрат $D(f)$ в $\Bbbk$ или нет.

Пример 3.7 (многочлены степени 4)
Обозначим через $\alpha, \beta, \gamma, \delta$ корни неприводимого сепарабельного многочлена

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \in \Bbbk[x] \tag{3-7}$$

[1] Ср. с примером 5.18 на с. 100 лекций [Алг 1].

в поле его разложения. Перестановки корней $\alpha, \beta, \gamma, \delta$ действуют на тройке ассоциированных с этими корнями чисел[1]

$$\xi = \alpha\beta + \gamma\delta\,, \quad \eta = \alpha\gamma + \beta\delta\,, \quad \zeta = \alpha\delta + \beta\gamma\,, \tag{3-8}$$

что задаёт эпиморфизм $S_4 \twoheadrightarrow S_3$, ядром которого является подгруппа Клейна $V_4 \subset S_4$, состоящая из тождественной перестановки и трёх пар независимых транспозиций[2]. Стабилизаторами элементов ξ, η, ζ в группе S_4 являются три её силовские 2-подгруппы[3] порядка 8, изоморфные диэдральной группе D_4 и пересекающиеся по подгруппе Клейна V_4. Поскольку группа Галуа $G_f = \mathrm{Gal}\, f/\Bbbk$ транзитивно действует на корнях, она может быть изоморфна либо S_4, либо A_4, либо D_4, либо V_4, либо циклической подгруппе $C_4 \subset D_4$. Этим возможностям отвечают следующие значения порядков $|G_f \cap V_4|$ и $|G_f/(G_f \cap V_4)|$:

G_f	S_4	A_4	D_4	V_4	C_4
$\lvert G_f \cap V_4\rvert$	4	4	4	4	2
$\lvert G_f/(G_f \cap V_4)\rvert$	6	3	2	1	2

Поскольку нормальной подгруппе $G_f \cap V_4 \lhd G_f$ соответствует расширение Галуа $\Bbbk \subset \Bbbk[\xi, \eta, \zeta]$ с группой Галуа $G_f/(G_f \cap V_4)$, порядок $|G_f/(G_f \cap V_4)|$ равен степени поля разложения многочлена

$$g(x) = (x - \xi)(x - \eta)(x - \zeta) = x^3 - bx^2 + (ac - 4d)x - a^2d + 4bd - c^2\,,$$

который называется *кубической резольвентой* многочлена f из формулы (3-7) и имеет тот же дискриминант, что f.

Упражнение 3.10. Убедитесь в этом, а также в том, что многочлен g имеет именно такие коэффициенты, как написано.

Мы заключаем, что если g неприводим над $\Bbbk$, то $G_f = S_4$, когда $D(f)$ не квадрат в $\Bbbk$, и $G_f = A_4$, когда $D(f)$ квадрат, а если g полностью раскладывается над $\Bbbk$ на линейные множители, то $G_f = V_4$. Если же g является в $\Bbbk[x]$ произведением неприводимого квадратного трёхчлена и линейного двучлена, то $G_f \simeq D_4$, когда f остаётся неприводимым над полем $\Bbbk[\xi, \eta, \zeta]$, и $G_f \simeq C_4$, когда он становится приводимым, ибо порядок $|G_f \cap V_4|$ равен степени поля разложения $\mathbb{E}_f$ многочлена f над подполем $\Bbbk[\xi, \eta, \zeta] \subset \mathbb{E}_f$.

Упражнение 3.11. Вычислите группы Галуа над $\mathbb{Q}$ у следующих многочленов: а) $x^4 - 4x + 2$ б) $x^4 + 4x^2 + 2$ в) $x^4 - 10x^2 + 4$ г) $x^4 - 2$.

3.4. Резольвента Галуа и редукция коэффициентов. Обозначим через $\mathbb{L}_f \supset \Bbbk$ поле разложения многочлена $f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \Bbbk[x]$, а через $\vartheta_1, \ldots, \vartheta_n$ — его корни в $\mathbb{L}_f$, и рассмотрим однородную линейную форму

$$\psi = \vartheta_1 t_1 + \ldots + \vartheta_n t_n \in \mathbb{L}_f[t_1, \ldots, t_n]\,. \tag{3-9}$$

[1] Обратите внимание, что в силу сепарабельности многочлена f эти числа различны:

$$\xi - \eta = (\alpha - \delta)(\beta - \gamma)\,, \quad \xi - \zeta = (\alpha - \gamma)(\beta - \delta)\,, \quad \eta - \zeta = (\alpha - \beta)(\gamma - \delta)\,.$$

[2] Ср. с примерами 10.9 и 10.10 на с. 176-177 лекций [Алг 1].

[3] См. определение 11.1 на с. 197 лекций [Алг 1].

Однородный многочлен степени $n!$

$$F(t_1, \dots, t_n) = \prod_{\sigma \in S_n} \psi^\sigma = \prod_{\sigma \in S_n} (\vartheta_1 t_{\sigma(1)} + \dots + \vartheta_n t_{\sigma(n)})$$

называется *резольвентой Галуа* многочлена f. Группируя вместе сомножители, отвечающие перестановкам σ из одного смежного класса подгруппы $G = \operatorname{Gal} f / \Bbbk \subset S_n$, перепишем F в виде

$$F\left(t_1, \dots, t_n\right) = \prod_{h \in S_n/G} F_h\left(t_1, \dots, t_n\right), \tag{3-10}$$

где

$$\begin{aligned} F_h\left(t_1, \dots, t_n\right) &= \prod_{g \in G} \left(\vartheta_1 t_{hg(1)} + \dots + \vartheta_n t_{hg(n)}\right) = \\ &= \prod_{g \in G} \left(\vartheta_{g^{-1}(1)} t_{h(1)} + \dots + \vartheta_{g^{-1}(n)} t_{h(n)}\right) = \prod_{g \in G} g\left(\psi^h\right). \end{aligned} \tag{3-11}$$

В последнем произведении $\psi^h \in \mathbb{L}_f[t_1, \dots, t_n]$ означает линейную форму, полученную из формы ψ перестановкой $h \in S_n$ переменных $t_1, \dots, t_n$, а $g(\psi^h)$ означает результат применения к *коэффициентам* этой формы автоморфизма $g : \mathbb{L}_f \xrightarrow{\sim} \mathbb{L}_f$ из группы Галуа $G = \operatorname{Aut}_{\Bbbk} \mathbb{L}_f$. Так как все линейные формы $g\left(\psi^h\right)$ в произведении (3-11) различны и составляют одну орбиту группы Галуа, каждый многочлен F_h имеет коэффициенты в поле $\Bbbk$ и неприводим над $\Bbbk$. Мы заключаем, что $F \in \Bbbk[t_1, \dots, t_n]$, и формула (3-10) доставляет разложение многочлена F на неприводимые множители в $\Bbbk[t_1, \dots, t_n]$. Неприводимые многочлены F_h образуют орбиту многочлена F_e при действии симметрической группы S_n на кольце $\Bbbk[t_1, \dots, t_n]$ перестановками переменных, и группа Галуа $G = \operatorname{Gal} f / \Bbbk$ изоморфна стабилизатору многочлена F_e и сопряжена стабилизатору любого из многочленов F_h. Суммируем сказанное так:

Предложение 3.4
Перестановки переменных $t_1, \dots, t_n$, переводящие в себя какой-нибудь неприводимый делитель резольвенты Галуа многочлена f в кольце $\Bbbk[t_1, \dots, t_n]$, образуют в S_n подгруппу, изоморфную $\operatorname{Gal} f / \Bbbk$. □

Пусть теперь $\Bbbk = \mathbb{Q}$ и $f = x^n + a_1 x^{n-1} + \dots + a_n \in \mathbb{Z}[x]$. Обозначим через

$$\overline{f} = x^n + \overline{a}_1 x^{n-1} + \dots + \overline{a}_n \in \mathbb{F}_p[x], \text{ где } \overline{a}_i = a_i \,(\mathrm{mod}\ p),$$

редукцию многочлена f по простому модулю $p \in \mathbb{N}$.

Теорема 3.4
Если многочлен $\overline{f} \in \mathbb{F}_p[x]$ сепарабелен, то $\operatorname{Gal} \overline{f} / \mathbb{F}_p$ гомоморфно вкладывается в $\operatorname{Gal} f / \mathbb{Q}$.

Доказательство. Корни $\vartheta_1, \dots, \vartheta_n$ многочлена f в его поле разложения $\mathbb{L}_f$ целы над $\mathbb{Z}$. Поэтому коэффициенты формы $\psi = \vartheta_1 t_1 + \dots + \vartheta_n t_n$ из формулы (3-9), а с ними и коэффициенты всех многочленов F_h из разложения (3-10), лежат в кольце целых $\mathcal{O} \subset \mathbb{L}_f$. Так как коэффициенты каждого многочлена F_h инвариантны относительно $\operatorname{Gal} \mathbb{L}_f / \mathbb{Q}$, они лежат в $\mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$, т. е. разложение (3-10) имеет место в кольце $\mathbb{Z}[t_1, \dots, t_n]$. Приводя его по модулю p, получаем в $\mathbb{F}_p[t_1, \dots, t_n]$ равенство

$$\overline{F}(t_1, \dots, t_n) = \prod_{h \in S_n/G} \overline{F}_h(t_1, \dots, t_n) \tag{3-12}$$

Обозначим через $\overline{\vartheta}_i = \vartheta_i \pmod p$ классы корней ϑ_i в $\mathbb{F}_p$-алгебре $A \stackrel{\text{def}}{=} \mathcal{O}/(p)$. В $A[t]$ многочлен $\overline{f}(x) = \prod(x - \overline{\vartheta}_i)$ полностью раскладывается на линейные множители, и все они различны в силу сепарабельности $\overline{f}$ над $\mathbb{F}_p$.

Упражнение 3.12. Убедитесь, что $\mathbb{F}_p$-подалгебра в A, порождённая $\overline{\vartheta}_1, \dots, \overline{\vartheta}_n$, является полем разложения многочлена $\overline{f}$ над $\mathbb{F}_p$.

Стало быть, многочлен $\overline{F} \in \mathbb{F}_p[t_1, \dots, t_n]$ является резольвентой Галуа многочлена $\overline{f} \in \mathbb{F}_p[x]$ над $\mathbb{F}_p$. По предл. 3.4 группу Галуа $\operatorname{Gal}\overline{f}/\mathbb{F}_p$ можно вложить в группу перестановок переменных t_i как стабилизатор какого-нибудь неприводимого делителя многочлена $\overline{F}$ в $\mathbb{F}_p[t_1, \dots, t_n]$. Зафиксируем такой делитель P, и пусть он приходит из разложения на неприводимые множители над полем $\mathbb{F}_p$ редукции $\overline{F}_h$ неприводимого делителя F_h многочлена F в кольце $\mathbb{Z}[t_1, \dots, t_n]$. Отождествим $\operatorname{Gal} f/\mathbb{Q}$ с группой перестановок переменных, переводящих F_h в себя. Поскольку каждая не лежащая в $\operatorname{Gal} f/\mathbb{Q}$ перестановка из S_n переводит F_h в другой неприводимый множитель $F_{h'} \neq F_h$ многочлена F, она не может оставлять на месте многочлен P, являющийся делителем многочлена $\overline{F}_h$. Следовательно $\operatorname{Gal}\overline{f}/\mathbb{F}_p \subset \operatorname{Gal} f/\mathbb{Q}$. □

Следствие 3.3
Пусть редукция по модулю p неприводимого приведённого многочлена $f \in \mathbb{Z}[x]$ распадается в произведение неприводимых над $\mathbb{F}_p$ многочленов $q_1, \dots, q_m$ степеней $\lambda_1 \geqslant \dots \geqslant \lambda_m$. Тогда группа Галуа $\operatorname{Gal} f/\mathbb{Q}$ содержит перестановку циклового типа[1] λ.

Доказательство. Поле разложения многочлена $\overline{f}$ над $\mathbb{F}_p$ конечно, и его группа Галуа над $\mathbb{F}_p$ циклическая[2]. Так как она транзитивно действует на корнях каждого из неприводимых многочленов q_i, образующий элемент группы $\operatorname{Gal}\overline{f}/\mathbb{F}_p$ осуществляет перестановку корней многочлена $\overline{f}$ циклового типа λ. По теор. 3.4 эта перестановка содержится и в $\operatorname{Gal} f/\mathbb{Q}$. □

Пример 3.8 (многочлен с группой S_5)
Вычислим группу Галуа многочлена $f(x) = x^5 - x - 1$ над $\mathbb{Q}$. Для этого разложим его на неприводимые множители над $\mathbb{F}_2$ и над $\mathbb{F}_3$. В нетривиальном разложении степень одного из неприводимых множителей $\leqslant 2$, и произведение всех неприводимых приведённых многочленов степеней 1 и 2 в $\mathbb{F}_p[x]$ равно[3] $x^{p^2} - x$. При помощи алгоритма Евклида убеждаемся, что над $\mathbb{F}_2$

$$\text{нод}(x^5 - x - 1,\ x^4 - x) = x^2 + x + 1$$

и разложение на неприводимые имеет вид $\overline{f} = (x^2 + x + 1)(x^3 + x^2 + 1)$, тогда как над полем $\mathbb{F}_3$ $\text{нод}(x^5 - x - 1,\ x^9 - x) = 1$, и значит, $\overline{f}$ неприводим. По сл. 3.3 группа $\operatorname{Gal} f/\mathbb{Q}$ содержит цикл длины 5 и перестановку циклового типа $(3, 2)$. Возводя последнюю в куб, заключаем, что группа Галуа содержит транспозицию. Так как цикл максимальной длины и транспозиция порождают группу[4] S_5, мы заключаем, что $\operatorname{Gal} f/\mathbb{Q} \simeq S_5$.

[1] См. определение 10.1 на с. 170 лекций [Алг 1].
[2] См. прим. 3.2 на стр. 25.
[3] См. упр. 3.3 на стр. 26.
[4] Убедитесь в этом. Будьте внимательны: цикл $|1, 2, 3, 4\rangle$ и транспозиция $|1, 3\rangle$ *не* порождают всю группу S_4 точно также, как S_6 *не* порождается циклом $|1, 2, 3, 4, 5, 6\rangle$ и транспозицией $|1, 4\rangle$.

Ответы и указания к некоторым упражнениям

Упр. 3.1. Достаточно проверить, что $\psi(t)$ не меняется при отражениях $\sigma_1 : t \mapsto 1/t$ и $\sigma_\infty : t \mapsto 1-t$.

Упр. 3.3. Корни многочлена $x^{p^n} - x$ распадаются на орбиты группы Галуа $G = \mathrm{Gal}\,\mathbb{F}_{p^n}/\mathbb{F}_p \simeq \mathbb{Z}/(n)$. Длина m каждой орбиты $\alpha_1, \ldots, \alpha_m$ 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, мы заключаем, что получающееся таким образом разложение многочлена $x^{p^n} - x$ на простые множители в $\mathbb{F}_p[x]$ имеет вид произведения попарно различных приведённых неприводимых многочленов, степени которых делят n. С другой стороны, каждый неприводимый приведённый многочлен $g \in \mathbb{F}_p[x]$ степени $m \mid n$ имеет корень в простом расширении $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_{p^m}$, которое вкладывается в поле $\mathbb{F}_{p^n}$, состоящее из корней многочлена $x^{p^n} - x$. Тем самым, у этого многочлена имеется общий корень с g, откуда $\mathrm{нод}(g, x^{p^n} - x) \neq 1$, и поскольку g неприводим в $\mathbb{F}_p[x]$, $x^{p^n} - x$ делится на g.

Упр. 3.4. Поскольку четыре арифметических действия над комплексными числами и извлечение из них квадратных корней полностью сводятся к этим пяти операциям над вещественными и мнимыми частями, можно предполагать числа a и b вещественными. В этом случае $a \pm b$ строятся непосредственно, a/b и ab — при помощи подобия или теоремы Фалеса (для этого и требуется отрезок длины 1), а $\sqrt{a} = \sqrt{1 \cdot a}$ — при помощи теоремы о среднем геометрическом в прямоугольном треугольнике (для этого и также требуется отрезок длины 1).

Упр. 3.5. При пересечении окружности и прямой получается вещественный трёхчлен

$$(b-a)(\overline{b}-\overline{a})\,t^2 + \big((b-a)(\overline{a}-\overline{c}) + (a-c)(\overline{b}-\overline{a})\big)\,t + (b-a)(\overline{b}-\overline{a}) - (d-c)(\overline{d}-\overline{c})\,,$$

при пересечении двух окружностей — трёхчлен $\alpha t^2 + \beta t + \overline{\alpha} = 0$, у которого $\alpha = (b-a)(\overline{a}-\overline{c})$, а $\beta = (b-a)(\overline{b}-\overline{a}) + (a-c)(\overline{a}-\overline{c}) - (d-c)(\overline{d}-\overline{c}) \in \mathbb{R}$.

Упр. 3.6. Воспользуйтесь равенством $\cos(3\varphi) = 4\cos\varphi - 3\cos^2\varphi$ при $\varphi = \pi/9$ и убедитесь, что у многочлена $8x^3 - 6x - 1$ нет рациональных корней.

Упр. 3.8. Пусть корни $\{\vartheta_1, \ldots, \vartheta_k\} \subset \{\vartheta_1, \ldots, \vartheta_n\}$ образуют орбиту группы Галуа. Тогда коэффициенты многочлена $g(x) = (x-\vartheta_1)\ldots(x-\vartheta_k)$ инвариантны относительно действия группы Галуа, и значит, $g \in \Bbbk[x]$. Таким образом, многочлен f является произведением многочленов g, отвечающих орбитам действия группы Галуа $\mathrm{Gal}\,f/\Bbbk$ на корнях f. С другой стороны, группа Галуа переводит в себя множество корней любого многочлена с коэффициентами из $\Bbbk$ и, тем самым, не может транзитивно действовать на корнях приводимого в $\Bbbk[x]$ многочлена f.

Упр. 3.11. Убедитесь, что все четыре многочлена неприводимы над $\mathbb{Z}$ и тем самым над $\mathbb{Q}$, а их кубические резольвенты имеют вид $x^3 - 8x + 16$ в (а), $x^3 - 4x^2 - 8x + 16 = (x-4)(x^2-8)$ в (б), $x^3 + 10x^2 - 16x - 160 = (x-4)(x+4)(x+10)$ в (в) и $x^3 + 8x$ в (г). Так как в (а) резольвента неприводима и имеет дискриминант -4864, многочлен из (а) имеет группу S_4. В (б) поле разложения кубической резольвенты изоморфно $\mathbb{Q}[\sqrt{2}]$, и исходный многочлен разлагается над ним как $(x^2+2-\sqrt{2})(x^2+2+\sqrt{2})$. Поэтому его группа Галуа циклическая порядка 4. В (в) исходный многочлен имеет группу Галуа V_4. В (г) поле разложения кубической резольвенты изоморфно $\mathbb{Q}[\sqrt{-2}]$, и исходный многочлен неприводим над ним. Поэтому его группа Галуа изоморфна D_4.

Упр. 3.12. Поле разложения $\mathbb{L}_{\overline{f}}$ многочлена $\overline{f}$ над $\mathbb{F}_p$ является башней примитивных расширений $\mathbb{F}_p = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L}_{\overline{f}}$, на каждом этаже которой происходит присоединение одного из корней ϑ многочлена $\overline{f}$. Так как $\overline{f}$ полностью распадается в $A[t]$ в произведение различных

линейных множителей, тавтологическое вложение $\mathbb{F}_p \hookrightarrow A$ продолжается вдоль башни до гомоморфизма $\mathbb{F}_p$-алгебр $\mathbb{L}_{\overline{f}} \to A$, который инъективен, ибо $\mathbb{L}_{\overline{f}}$ — поле, и имеет образом $\mathbb{F}_p$-подалгебру, порождённую корнями многочлена $\overline{f}$ в A.