## §14. Группы Галуа

**14.1. Построения циркулем и линейкой.** Отождествим евклидову координатную плоскость $\mathbb{R}^2$ с полем $\mathbb{C}$. Традиционный набор школьных задач на построение показывает, что всякая точка $\zeta \in \mathbb{C}$, лежащая в произвольном подполе $\mathbb{L} \subset \mathbb{C}$, к которому ведёт башня квадратичных расширений

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L}, \tag{14-1}$$

где $\mathbb{L}_{i+1} = \mathbb{L}_i\left[\sqrt{a_i}\right]$ для некоторого $a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2$, может быть построена циркулем и линейкой, как только на плоскости $\mathbb{C}$ указаны точки 0 и 1.

Упражнение 14.1. Даны точки 0, 1, $a$, $b \in \mathbb{C}$. Циркулем и линейкой постройте в $\mathbb{C}$ точки $a \pm b$, $a/b$, $ab$ и $\sqrt{a}$.

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 некотором поле $\mathbb{L} \subset \mathbb{C}$, к которому ведёт башня квадратичных расширений вида (14-1), причём все поля $\mathbb{L}_i$ этой башни переходят в себя при комплексном сопряжении $z \mapsto \overline{z}$. В самом деле, построение числа $\zeta$ распадается на элементарные шаги, каждый из которых состоит в отыскании точки пересечения $p$ одного из трёх типов: или прямых $(a, b)$ и $(c, d)$, или прямой $(a, b)$ и окружности с радиусом $[c, d]$, или двух окружностей с радиусами $[a, b]$ и $[c, d]$, в предположении, что точки $a$, $b$, $c$, $d$ уже построены, а искомая точка пересечения на евклидовой плоскости существует. Положим $\mathbb{L}_1 = \mathbb{Q}\left[\sqrt{-1}\right]$ и допустим по индукции, что числа $a$, $b$, $c$, $d$ лежат в уже построенном и переходящем в себя при комплексном сопряжении поле $\mathbb{L}_i$ из башни (14-1). Тогда число $(a, b) \cap (c, d)$ тоже лежит в $\mathbb{L}_i$, а пары чисел, возникающие в пересечении окружности радиуса $[c, d]$ с прямой $(a, b)$ или с окружностью радиуса $[a, b]$ лежат в поле разложения квадратного трёхчлена $f(t)$, полученного подстановкой $z = a+(b-a)\cdot t$ в уравнение окружности $(z-c)(\overline{z}-\overline{c}) = (d-c)(\overline{d}-\overline{c})$: в случае пересечения с прямой этот трёхчлен имеет корни на вещественной прямой, а в случае пересечения с окружностью — на единичной окружности, и подстановка этих корней в $a+(b-a)\cdot t$ вместо $t$ даст искомые точки пересечения $p$. Поскольку поле $\mathbb{L}_i$ инвариантно относительно сопряжения, коэффициенты $f$ вещественны и лежат в $\mathbb{L}_i$. Поэтому корни $f$ лежат либо в $\mathbb{L}_i$, либо в квадратичном расширении $\mathbb{L}_{i+1} \supset \mathbb{L}_i$, базис которого над $\mathbb{L}_i$ образован парой вещественных или комплексно сопряжённых корней квадратного трёхчлена $f$. Поэтому поле $\mathbb{L}_{i+1} \ni p$ также инвариантно относительно комплексного сопряжения, что воспроизводит предположение индукции.

Предложение 14.1
Конечное расширение Галуа $\mathbb{K} \supset \Bbbk$ тогда и только тогда содержится в некотором поле $\mathbb{L} \supset \Bbbk$, к которому ведёт башня квадратичных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L}, \tag{14-2}$$

в которой $\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{a_i}]$ с $a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2$, когда $[\mathbb{K} : \Bbbk] = 2^n$ для некоторого $n \in \mathbb{N}$.

Доказательство. Пусть $\mathbb{K}$ содержится в башне (14-2). Из мультипликативности степени вытекает, что $[\mathbb{L} : \Bbbk] = 2^m$, откуда и $[\mathbb{K} : \Bbbk]$ обязано быть степенью двойки. Наоборот, если $[\mathbb{K} : \Bbbk] = \left|\operatorname{Gal}\mathbb{K}/\Bbbk\right| = 2^n$, то группа Галуа $G = \operatorname{Gal}\mathbb{K}/\Bbbk$ является 2-группой и обладает такой убывающей фильтрацией

$$G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{e\} \tag{14-3}$$

подгруппами $G_{i+1} \lhd G_i$, что $G_i / G_{i+1} \simeq \mathbb{Z}/(2)$ при всех $i$.

Упражнение 14.2. Выведите из это из теоремы Жордана – Гёльдера[1].

Строится такая фильтрация индукцией по $n$. Центр $C \lhd G$ нетривиален и является абелевой нормальной 2-подгруппой.

Упражнение 14.3. Выведите из теоремы о строении конечно порождённых абелевых групп существование фильтрации $C = C_0 \supset C_1 \supset \cdots \supset C_{k-1} \supset C_k = \{e\}$ с факторами $C_i / C_{i+1} \simeq \mathbb{Z}/(2)$.

По индукции, на $G/C$ есть фильтрация $G/C = Q_0 \supset Q_1 \supset \cdots \supset Q_{\ell-1} \supset Q_\ell = \{e\}$ с факторами $Q_i/Q_{i+1} \simeq \mathbb{Z}/(2)$. Из фильтраций на $C$ и $G/C$ составляется фильтрация

$$G = CQ_0 \supset CQ_1 \supset \cdots \supset CQ_{\ell-1} \supset C \supset C_1 \supset \cdots \supset C_{k-1} \supset C_k = \{e\}$$

где $CQ_i \subset G$ суть полные прообразы подгрупп $Q_i \subset G/C$ при факторизации $G \twoheadrightarrow G/C$, так что $CQ_i / CQ_{i+1} \simeq \big(CQ_i/C\big) / \big(CQ_{i+1}/C\big) \simeq Q_{i+1}/Q_i \simeq \mathbb{Z}/(2)$, что и даёт фильтрацию (14-3). Соответствие Галуа[2] сопоставляет ей башню квадратичных расширений $\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{n-1} \subset \mathbb{L}_n = \mathbb{K}$, в которой $\mathbb{L}_i = \mathbb{K}^{G_i}$ и которая ведёт от $\Bbbk$ прямо к полю $\mathbb{K}$. □

Теорема 14.1
Комплексный корень неприводимого многочлена $f(x) \in \mathbb{Q}[x]$ может быть построен циркулем и линейкой исходя из точек $0,\ 1 \in \mathbb{C}$, если и только если степень его поля разложения 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. При $\deg \mathbb{K}/\mathbb{Q} = 2^m$ его по предл. 14.1 можно получить как верхний этаж $\mathbb{L}$ башни (14-1), и значит все числа из поля $\mathbb{K}$ можно построить циркулем и линейкой в силу упр. 14.1. Наоборот, пусть корень $\vartheta$ многочлена $f$ строится циркулем и линейкой. Тогда примитивное расширение $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ содержится в некотором расширении $\mathbb{L}$ вида (14-1). Автоморфизм поля $\mathbb{K}$, переводящий корень $\vartheta$ в другой корень $\vartheta'$ многочлена $f$ переводит подполе $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ в подполе $\mathbb{Q}[\vartheta'] \subset \mathbb{C}$. Получающееся таким образом вложение полей $\psi : \mathbb{Q}[\vartheta] \hookrightarrow \mathbb{C}$,

[1] см. Теорему 13.1 на стр. 208 лекции 13 из второго семестра первого курса (http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/1314/lec-13.pdf)

[2] см. теор. 13.6 на стр. 211

$\vartheta \mapsto \vartheta'$, продолжается до вложения $\overline{\psi} : \mathbb{L} \hookrightarrow \mathbb{C}$, совпадающего с $\psi$ на подполе $\mathbb{Q}[\vartheta] \subset \mathbb{L}$ и переводящего башню (14-1) в башню

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}'_1 \subset \mathbb{L}'_2 \subset \cdots \subset \mathbb{L}'_{m-1} \subset \mathbb{L}'_m = \mathbb{L}', \tag{14-4}$$

в которой $\mathbb{L}'_{i+1} = \mathbb{L}'_i\bigl[\sqrt{a'_i}\bigr]$ для некоторого $a'_i = \widetilde{\psi}(a_i) \in \mathbb{L}'_i \smallsetminus \bigl(\mathbb{L}'_i\bigr)^2$. Так как $\vartheta' \in \mathbb{L}'$, корень $\vartheta'$ тоже строится циркулем и линейкой. Композит $\mathbb{L}\mathbb{L}'$ содержит оба корня $\vartheta$, $\vartheta'$ и также является башней квадратичных расширений, поскольку получается последовательным присоединением к $\mathbb{L}$ чисел $a'_1, a'_2, \ldots, a'_m$, 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 расширений, содержащую все корни многочлена $f$, а значит и его поле разложения $\mathbb{K}$. По предл. 14.1 степень $[\mathbb{K} : \mathbb{Q}]$ в этом случае является степенью двойки, что и утверждалось. □

Следствие 14.1
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 $\zeta$, поэтому его степень над $\mathbb{Q}$ делит степень поля разложения минимального многочлена. □

Пример 14.1 (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 $\cos(\pi/9)$ — корня многочлена[1] $4x^3 - 3x - 1/2$, не имеющего рациональных корней и, тем самым, неприводимого над $\mathbb{Q}$, а значит, являющегося минимальным многочленом числа $\cos(\pi/9)$. 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 7-угольник тоже нельзя построить циркулем и линейкой: такое построение позволяло бы построить первообразный корень 7-й степени $e^{\frac{2\pi i}{7}}$, минимальный многочлен которого[2] $\Phi_7(x) = (x^7 - 1)/(x - 1)$ имеет степень 6.

Упражнение 14.4* (построение Гаусса). Постройте циркулем и линейкой правильный 17-угольник.

[1] он получается из соотношения $\cos(3\varphi) = 4\cos\varphi - 3\cos^2\varphi$ при $\varphi = \pi/9$

[2] напомню, что круговой многочлен $\Phi_p(x)$ при простом $p$ неприводим по критерию Эйзенштейна

**14.1.1. 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 $\zeta_1, \zeta_2, \dots, \zeta_n \in \mathbb{C}$. Поскольку все точки порождённого ими поля $\mathbb{F} = \mathbb{Q}(\zeta_1, \zeta_2, \dots, \zeta_n) \subset \mathbb{C}$ строятся циркулем и линейкой, всегда можно считать, что данные точки образуют произвольное[1] подполе $\mathbb{F} \subset \mathbb{C}$. Элементы поля $\mathbb{F}$ называются в этой ситуации *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 квадратичных расширений поля $\mathbb{F}$, что происходит тогда и только тогда, когда $\zeta$ алгебраичен над $\mathbb{F}$ и степень поля разложения минимального многочлена числа $\zeta$ над $\mathbb{F}$ является степенью двойки. В частности, что для этого необходимо, чтобы степень самого′ минимального многочлена была степенью двойки.

Упражнение 14.5. Докажите все эти утверждения.

В наиболее общем виде влияние на расширение Галуа взятия его композита с произвольным полем побочных иррациональностей описывается так:

Предложение 14.2 (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 $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ 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. 13.3 поле $\mathbb{K}$ является полем разложения некого сепарабельного многочлена $f \in \Bbbk[x]$ и порождается как $\Bbbk$-алгебра его корнями $\vartheta_1, \vartheta_2, \dots, \vartheta_n \in \mathbb{L}$. Они же порождают $\mathbb{F}\mathbb{K}$ как алгебру над $\Bbbk$, и т. к. по предл. 13.4 расширение $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ нормально и сепарабельно, оно является конечным расширением Галуа. Автоморфизмы $\mathbb{K}$ над $\Bbbk$ и $\mathbb{F}\mathbb{K}$ над $\mathbb{F}$ оставляют многочлен $f$ на месте и переводят множество его корней в себя, причём каждый автоморфизм однозначно определяется осуществляемой им перестановкой корней. Группа $\operatorname{Gal}\mathbb{K}/\Bbbk$ изоморфна подгруппе в $S_n$, состоящей из всех таких перестановок корней $\vartheta_1, \vartheta_2, \dots, \vartheta_n$, которые продолжаются до автоморфизма алгебры $\mathbb{K} = \Bbbk[\vartheta_1, \vartheta_2, \dots, \vartheta_n]$. Такой автоморфизм продолжается до автоморфизма большей алгебры $\mathbb{F}[\vartheta_1, \vartheta_2, \dots, \vartheta_n] \supset \Bbbk[\vartheta_1, \vartheta_2, \dots, \vartheta_n]$, если и только если он $\mathbb{F}$-линеен, т. е. оставляет на месте подполе $\mathbb{F} \cap \mathbb{K}$. □

**14.2. Группы многочленов.** Согласно предл. 13.3, 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

[1] возможно, что и не алгебраическое над $\mathbb{Q}$

корнях $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ многочлена $f$, и поскольку поле $\mathbb{L}_f$ как алгебра над $\Bbbk$ порождается этими корнями, каждый автоморфизм из группы Галуа однозначно определяется 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

$$\mathrm{ev}_{\vartheta_1,\vartheta_2,\dots,\vartheta_n} : \Bbbk[t_1, t_2, \dots, t_n] \to \overline{\Bbbk}, \quad \psi \mapsto \psi(\vartheta_1, \vartheta_2, \dots, \vartheta_n), \tag{14-5}$$

ядро которого $I_\Bbbk(\vartheta) \stackrel{\text{def}}{=} \ker \mathrm{ev}_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$ является идеалом всех полиномиальных соотношений между корнями многочлена $f$, т. е. состоит из всех многочленов $\psi \in \Bbbk[t_1, t_2, \dots, t_n]$, равных нулю в точке $\vartheta = (\vartheta_1, \vartheta_2, \dots, \vartheta_n) \in \mathbb{A}^n\big(\overline{\Bbbk}\big)$. Перестановка переменных $g : t_i \mapsto t_{g(i)}$ тогда и только тогда корректно факторизуется до эндоморфизма алгебры $\mathbb{L}_f = \Bbbk[t_1, t_2, \dots, t_n]/I_\Bbbk(\vartheta)$, когда она переводит идеал $I_\Bbbk(\vartheta)$ себя, т. е. для любого $\psi \in I_\Bbbk(\vartheta)$ многочлен

$$\psi^g(t_1, t_2, \dots, t_n) \stackrel{\text{def}}{=} \psi\left(t_{\sigma(1)}, t_{\sigma(2)}, \dots, t_{\sigma(n)}\right)$$

тоже лежит в $I_\Bbbk(\vartheta)$. Тем самым, группа Галуа многочлена $f$ имеет вид

$$\mathrm{Gal}\, f/\Bbbk \simeq \{g \in S_n \mid \forall \psi \in I_\Bbbk(\vartheta)\, \psi^g \in I_\Bbbk(\vartheta)\} \tag{14-6}$$

Именно так изначально и определял группу многочлена сам Галуа.

Замечание 14.1. Задаваемое формулой (14-6) вложение группы Галуа $\mathrm{Gal}\, f$ в стандартную симметрическую группу $S_n = \mathrm{Aut}\{1, 2, \dots, n\}$ не является каноническим и *зависит* от выбора нумерации корней $\vartheta_i$ многочлена $f$.

Предложение 14.3
Аффинное алгебраическое многообразие $V(I_\Bbbk(\vartheta)) \subset \mathbb{A}^n\big(\overline{\Bbbk}\big)$ представляет собою набор из $m = [\mathbb{L}_f : \Bbbk] = |\mathrm{Gal}\, f/\Bbbk|$ различных точек $\left(\vartheta_{g(1)}, \vartheta_{g(2)}, \dots, \vartheta_{g(n)}\right)$, $g \in \mathrm{Gal}\, f/\Bbbk$, образующих одну орбиту действия группы $\mathrm{Gal}\, f/\Bbbk \subset S_n$ на $\mathbb{A}^n$ перестановками координат.

Доказательство. Обозначим через $e_i(t_1, t_2, \dots, t_n)$ элементарные симметрические многочлены, и пусть $f = x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n$. Многочлены $e_i(t_1, t_2, \dots, t_n) - (-1)^i a_i \in I_\Bbbk(\vartheta)$, т. к. $e_i(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = (-1)^i a_i$ по теореме Виета. Если точка $a = (\alpha_1, \alpha_2, \dots, \alpha_n) \in V(I_\Bbbk(\vartheta))$, то $e_i(\alpha_1, \alpha_2, \dots, \alpha_n) = (-1)^i a_i$, откуда

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = f(x) = (x - \vartheta_1)(x - \vartheta_2) \cdots (x - \vartheta_n).$$

Следовательно, $(\alpha_1, \alpha_2, \dots, \alpha_n) = \left(\vartheta_{g(1)}, \vartheta_{g(2)}, \dots, \vartheta_{g(n)}\right)$ для некоторой перестановки $g \in S_n$. Если $g$ не лежит в группе Галуа $\operatorname{Gal} f$, то найдётся такой многочлен $\psi \in I_{\Bbbk}(\vartheta)$, что $\psi^g \notin I_{\Bbbk}(\vartheta)$, и тогда $\psi(\alpha_1, \dots, \alpha_n)) = \psi\left(\vartheta_{g(1)}, \dots, \vartheta_{g(n)}\right) = \psi^g\left(\vartheta_1, \dots, \vartheta_n\right) \neq 0$, что невозможно, ибо $a \in V(I_{\Bbbk}(\vartheta))$. Таким образом, координаты точки $a$ получаются из координат точки $\vartheta$ перестановкой из группы Галуа многочлена $f$. Наоборот, для любой перестановки $g \in \operatorname{Gal} f / \Bbbk$ и всех $\psi \in I_{\Bbbk}(\vartheta)$ значение $\psi\left(\vartheta_{g(1)}, \vartheta_{g(2)}, \dots, \vartheta_{g(n)}\right) = \psi^g(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = 0$, т. к. $\psi^g \in I_{\Bbbk}(\vartheta)$. Поэтому все точки, получающиеся из $\vartheta$ перестановками координат из группы Галуа, лежат в $V(I_{\Bbbk}(\vartheta))$. □

Упражнение 14.6. Покажите, что сепарабельный многочлен $f \in \Bbbk[x]$ неприводим, если и только если группа $\operatorname{Gal} f / \Bbbk$ транзитивно действует на его корнях.

**14.2.1. Резольвента Галуа.** Рассмотрим однородную линейную форму

$$\psi = \vartheta_1 t_1 + \vartheta_2 t_2 + \dots + \vartheta_n t_n \in \mathbb{L}_f[t_1, t_2, \dots, t_n], \tag{14-7}$$

где $\mathbb{L}_f \supset \Bbbk$ — поле разложения многочлена $f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n$ с коэффициентами $a_i \in \Bbbk$, а $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ — корни $f$ в $\mathbb{L}_f$. Многочлен

$$F\left(t_1, \dots, t_n\right) = \prod_{\sigma \in S_n} \psi^\sigma\left(t_1, \dots, t_n\right) = \prod_{\sigma \in S_n} \left(\vartheta_1 t_{\sigma(1)} + \dots + \vartheta_n t_{\sigma(n)}\right) \tag{14-8}$$

степени $n!$ называется *резольвентой Галуа* многочлена $f$. Группируя вместе сомножители, отвечающие перестановкам $\sigma$ из одного смежного класса $hG$ группы Галуа $G = \operatorname{Gal} f / \Bbbk \subset S_n$, перепишем (14-8) в виде

$$F\left(t_1, \dots, t_n\right) = \prod_{h \in S_n/G} F_h\left(t_1, \dots, t_n\right), \quad \text{где} \tag{14-9}$$

$$\begin{aligned} F_h\left(t_1, \dots, t_n\right) &= \prod_{g \in G} \left(\vartheta_1 t_{hg(1)} + \dots + \vartheta_n t_{hg(n)}\right) = \\ &= \prod_{g \in G} \left(\vartheta_{g^{-1}(1)} t_{h(1)} + \dots + \vartheta_{g^{-1}(n)} t_{h(n)}\right) = \prod_{g \in G} g\left(\psi^h\right) \end{aligned} \tag{14-10}$$

и $g\left(\psi^h\right)$ означает результат применения к *коэффициентам* линейной формы[1] $\psi^h \in \mathbb{L}_f[t_1, t_2, \dots, t_n]$ 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 (14-10) различны и составляют одну орбиту группы Галуа, каждый многочлен $F_h$ имеет коэффициенты в поле $\Bbbk$ и неприводим над $\Bbbk$. Поэтому $F \in \Bbbk[t_1, t_2, \dots, t_n]$, и формула (14-9) даёт разложение $F$ на неприводимые множители в кольце $\Bbbk[t_1, t_2, \dots, t_n]$. Эти неприводимые множители образуют одну орбиту действия симметрической группы $S_n$ на кольце $\Bbbk[t_1, t_2, \dots, t_n]$ перестановками координат, а группа Галуа $G = \operatorname{Gal} f$ изоморфна стабилизатору в $S_n$ многочлена $F_e$ и сопряжена стабилизаторам всех остальных многочленов $F_h$. Суммируем сказанное как

[1] полученной из формы (14-7) перестановкой $h$ переменных $t_1, \dots, t_n$

Предложение 14.4
Перестановки переменных $t_1, t_2, \dots, t_n$, оставляющие неизменным какой-либо множитель $F_h$ из разложения резольвенты Галуа на неприводимые множители в кольце $\Bbbk[t_1, t_2, \dots, t_n]$, образуют в $S_n$ подгруппу, изоморфную $\operatorname{Gal} f/\Bbbk$. □

**14.2.2. Редукция коэффициентов.** Пусть теперь поле $\Bbbk = \mathbb{Q}$ и многочлен

$$f = x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x].$$

Обозначим через $\overline{f} = x^n + \overline{a}_1 x^{n-1} + \dots + \overline{a}_{n-1}x + \overline{a}_n \in \mathbb{F}_p[x]$, где $\overline{a}_i = a_i \bmod(p)$, редукцию $f$ по простому модулю $p \in \mathbb{N}$.

Теорема 14.2
Если многочлен $\overline{f} \in \mathbb{F}_p[x]$ сепарабелен, то имеется вложение групп

$$\operatorname{Gal} \overline{f}/\mathbb{F}_p \hookrightarrow \operatorname{Gal} f/\mathbb{Q}.$$

Доказательство. Корни $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ многочлена $f$ в его поле разложения $\mathbb{L}_f$ целы над $\mathbb{Z}$. Поэтому коэффициенты формы $\psi = \vartheta_1 t_1 + \vartheta_2 t_2 + \dots + \vartheta_n t_n$ из (14-7), а с ними и коэффициенты всех многочленов $F_h$ из разложения (14-9), лежат в кольце целых $\mathcal{O} \subset \mathbb{L}_f$. Так как коэффициенты каждого многочлена $F_h$ инвариантны относительно группы Галуа $\operatorname{Gal} \mathbb{L}_f/\Bbbk$, они лежат в $\mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$, и разложение (14-9) имеет место в кольце $\mathbb{Z}[t_1, t_2, \dots, t_n]$. Приводя его по модулю $p$, получаем в кольце $\mathbb{F}_p[t_1, t_2, \dots, t_n]$ равенство

$$\overline{F}(t_1, t_2, \dots, t_n) = \prod_{h \in S_n/G} \overline{F}_h(t_1, t_2, \dots, t_n) \tag{14-11}$$

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

Упражнение 14.7. Убедитесь, что $\mathbb{F}_p$-подалгебра в $A$, порождённая корнями многочлена $\overline{f}$ является его полем разложения над $\mathbb{F}_p$.

Стало быть, многочлен $\overline{F} \in \mathbb{F}_p[t_1, t_2, \dots, t_n]$ является резольвентой Галуа (14-8) для многочлена $\overline{f} \in \mathbb{F}_p[x]$ над $\mathbb{F}_p$, и по предл. 14.4 группа Галуа $\operatorname{Gal} \overline{f}/\mathbb{F}_p$ изоморфна группе перестановок переменных $t_i$, сохраняющих один из неприводимых множителей, назовём его $P$, многочлена $\overline{F}$ в $\mathbb{F}_p[t_1, t_2, \dots, t_n]$. Множитель $P$ приходит из разложения на неприводимые множители над полем $\mathbb{F}_p$ редукции $\overline{F}_h$ одного из сомножителей $F_h$ произведения (14-9) в кольце $\mathbb{Z}[t_1, t_2, \dots, t_n]$. Отождествим группу Галуа $\operatorname{Gal} f/\mathbb{Q}$ с группой перестановок из $S_n$, переводящих $F_h$ в себя. Перестановки, не лежащие в $\operatorname{Gal} f/\mathbb{Q}$ переводят $F_h$ в множители $F_{h'} \neq F_h$. Поскольку каждая перестановка из $\operatorname{Gal} \overline{f}/\mathbb{F}_p$ оставляет на месте множитель $P$ многочлена $\overline{F}_h$, она не может переводить $F_h$ ни в какой многочлен $F_{h'} \neq F_h$, и значит, лежит в $\operatorname{Gal} f/\mathbb{Q}$. □

Следствие 14.2
Пусть при редукции по простому модулю $p$ неприводимый приведённый многочлен $f \in \mathbb{Z}[x]$ распадается в $\mathbb{F}_p[x]$ в произведение $\overline{f} = q_1 q_2 \dots q_m$ неприводимых над $\mathbb{F}_p$ многочленов $q_1, q_2, \dots, q_m$ степеней $\lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_m$. Тогда группа Галуа $\operatorname{Gal} f/\mathbb{Q}$ содержит перестановку его корней циклового типа $\lambda$.

Доказательство. Поле разложения многочлена $\overline{f}$ над $\mathbb{F}_p$ конечно, и его группа Галуа над $\mathbb{F}_p$ циклическая[1]. Так как она транзитивно действует на корнях каждого из неприводимых многочленов $q_i$, образующий элемент осуществляет перестановку корней многочлена $\overline{f}$ циклового типа $\lambda$. По теор. 14.2 эта перестановка лежит в $\operatorname{Gal} f/\mathbb{Q}$. □

Пример 14.2 (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 множителей $\leqslant 2$, и по упр. 13.15 произведение всех неприводимых приведённых многочленов степени $\leqslant 2$ в $\mathbb{F}_p[x]$ равно $x^{p^2} - x$. При помощи алгоритма Евклида убеждаемся, что над полем $\mathbb{F}_2$

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

и разложение на неприводимые имеет вид $\overline{f} = (x^2+x+1)\cdot(x^3+x^2+1)$, а над полем $\mathbb{F}_3$ $\text{нод}\left(x^5 - x - 1,\, x^9 - x\right) = 1$, и значит $\overline{f}$ неприводим. По сл. 14.2 группа Галуа $\operatorname{Gal} f/\mathbb{Q}$ содержит цикл длины 5 и перестановку циклового типа $(3, 2)$, куб которой — транспозиция. Так как цикл максимальной длины и транспозиция порождают всю симметрическую группу, $\operatorname{Gal} f/\mathbb{Q} \simeq S_5$. Из теор. 14.5, которую мы докажем на стр. 225 ниже, вытекает, что корни многочлена $x^5 - x - 1$ не выражаются через рациональные числа при помощи четырёх арифметических операций и извлечения корней произвольных степеней.

**14.3. Группы круговых полей.** Расширение $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$, порождённое как алгебра над $\mathbb{Q}$ примитивным корнем $n$-той степени из единицы

$$\zeta_n \stackrel{\text{def}}{=} e^{2\pi i/n} \in \mathbb{C},$$

называется $n$-тым *круговым*[2] полем. Это поле содержит циклическую мультипликативную группу $\boldsymbol{\mu}_n \subset \mathbb{Q}[\zeta_n]$ корней $n$-той степени из единицы и является полем разложения сепарабельного многочлена $x^n - 1$. Поэтому круговое поле является расширением Галуа поля $\mathbb{Q}$, а каждый автоморфизм $\sigma \in \operatorname{Gal} \mathbb{Q}[\zeta_n]/\mathbb{Q}$ переводит образующую $\zeta_n$ группы $\boldsymbol{\mu}_n$ в образующую группы $\boldsymbol{\mu}_n$, т. е. действует по правилу $\sigma : \zeta_n \mapsto \zeta_n^{m(\sigma)}$, где $m(\sigma) \in (\mathbb{Z}/(n))^*$ обратим в кольце вычетов $\mathbb{Z}/(n)$.

[1] см. прим. 13.7 на стр. 211
[2] или *циклотомическим*

Это задаёт гомоморфное вложение группы Галуа кругового поля в мультипликативную группу обратимых элементов кольца вычетов:

$$\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q} \hookrightarrow \big(\mathbb{Z}/(n)\big)^*, \quad \sigma \mapsto m(\sigma). \tag{14-12}$$

Поскольку множество всех первообразных корней степени $n$ из единицы

$$R_n \stackrel{\text{def}}{=} \{\zeta_n^m \mid \text{нод}(n,m)=1\} \subset \boldsymbol{\mu}_n$$

переводится группой $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q}$ в себя, *n-тый круговой многочлен*

$$\Phi_n(x) \stackrel{\text{def}}{=} \prod_{\xi\in R_n}(x-\xi)$$

инвариантен относительно группы Галуа, и значит, лежит в $\mathbb{Q}[x]$. Будучи полиномами от корней многочлена $x^n-1$, все коэффициенты многочлена $\Phi_n(x)$ целы над $\mathbb{Z}$, и тем самым $\Phi_n(x)\in\mathbb{Z}[x]$. Так, $\Phi_2(x)=x+1$, $\Phi_3(x)=(x-\omega)(x-\omega^2)=$ $=x^2+x+1$, $\Phi_4(x)=(x-i)(x+i)=x^2+1$, $\Phi_5(x)=(x^5-1)/(x-1)=x^4+x^3+x^2+x+1$, $\Phi_6(x)=(z-\zeta_6)(x-\zeta_6^{-1})=x^2-x+1$ и т. д. Круговое поле $\mathbb{Q}[\zeta_n]$ является полем разложения кругового многочлена $\Phi_n$ и $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q}=\operatorname{Gal}\Phi_n$.

**14.3.1. Элементы Фробениуса.** При простом $p\nmid n$ многочлен $x^n-1$ сепарабелен над $\mathbb{F}_p$. Редукция $\overline{\Phi}_n$ многочлена $\Phi_n$ по модулю $p$ тоже сепарабельна над $\mathbb{F}_p$, т. к. $\overline{\Phi}_n$ делит $x^n-1$. Поэтому сопоставление $\xi\mapsto\overline{\xi}=\xi \bmod(p)$ задаёт биекцию между множеством комплексных первообразных корней

$$R_n \subset \mathcal{O} \subset \mathbb{Q}[\zeta_n] \subset \mathbb{C}$$

и корнями многочлена $\overline{\Phi}_n$ в его поле разложения над $\mathbb{F}_p$, которое порождается как алгебра над $\mathbb{F}_p$ классами $\overline{\xi}\in\mathcal{O}/(p)$ комплексных коней $\xi$ в фактор алгебре кольца целых $\mathcal{O}$ кругового поля $\mathbb{Q}[\zeta_n]$ по главному идеалу $(p)$ и является конечным расширением Галуа поля $\mathbb{F}_p$ с циклической группой Галуа, порождённой автоморфизмом Фробениуса[1] $\overline{\xi}\mapsto\overline{\xi}^p$. По теор. 14.2 в группе Галуа $\operatorname{Gal}\Phi_n/\mathbb{Q}$ имеется такая перестановка комплексных первообразных корней $\sigma\in\operatorname{Aut}R_n$, что $\overline{\sigma(\xi)}=\overline{\xi}^p$. Мы заключаем, что автоморфизм мультипликативной группы $\boldsymbol{\mu}_n\subset\mathbb{Q}[\zeta_n]$, заданный правилом

$$F_p : \boldsymbol{\mu}_n \xrightarrow{\sim} \boldsymbol{\mu}_n, \quad \xi\mapsto\xi^p, \tag{14-13}$$

продолжается до автоморфизма кругового поля $\mathbb{Q}[\zeta_n]$ над $\mathbb{Q}$. Он называется *p-элементом Фробениуса* в группе Галуа кругового поля. Таким образом, для всех простых $p\nmid n$ автоморфизмы Фробениуса из групп Галуа $\operatorname{Gal}\overline{\Phi}_n/\mathbb{F}_p$ *канонически* вложены в группу Галуа $\operatorname{Gal}\Phi_n/\mathbb{Q}$ кругового поля.

[1] см. прим. 13.7 на стр. 211 и доказательство сл. 14.2 на стр. 220

Применяя к корню $\zeta_n \in R_n$ автоморфизмы $F_p$ со всевозможными простыми $p \nmid n$, а также их итерации, можно получить все первообразные корни: любой из них имеет вид $\zeta_n^m$ для некоторого $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, взаимно простого с $n$, и равен $F_{p_1}^{m_1} F_{p_2}^{m_2} \cdots F_{p_k}^{m_k} \zeta_n$ . Следовательно, группа Галуа кругового многочлена транзитивно действует на его корнях.

Предложение 14.5
Вложение (14-12) является изоморфизмом групп, т. е. $\operatorname{Gal} \Phi_n \simeq (\mathbb{Z}/(n))^*$. В частности, $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$, где $\varphi$ — функция Эйлера.

Доказательство. Поскольку группа $\operatorname{Gal} \Phi_n$ транзитивно действует на корнях, $\left|\operatorname{Gal} \Phi_n\right| \geqslant \deg \Phi_n = \varphi(n) = \left|(\mathbb{Z}/(n))^*\right|$. □

Предложение 14.6
Многочлен $\Phi_n$ неприводим над $\mathbb{Q}$ и является минимальным многочленом первообразного корня $\zeta_n$ над $\mathbb{Q}$.

Доказательство. Если бы $\Phi_n$ был приводим, группа Галуа переводила бы множество корней каждого неприводимого множителя в себя и не могла бы транзитивно действовать на корнях $\Phi_n$. □

Пример 14.3 (Гауссова сумма)
При простом $p > 2$ всякая подгруппа $H \subset \mathbb{F}_p^*$ индекса 2 содержит все ненулевые квадраты поля $\mathbb{F}_p$, поскольку $\xi^2 H = \xi H \cdot \xi H = H$ в $\mathbb{F}_p^* / H \simeq \mathbb{Z}/(2)$. Поэтому такая подгруппа единственна и равна группе ненулевых квадратов. В частности, группа Галуа кругового поля содержит ровно одну подгуппу индекса 2, и она переводится изоморфизмом $m : \operatorname{Gal} \Phi_n \xrightarrow{\sim} \mathbb{F}_p^*$ из форм. (14-12) на стр. 221 в подгруппу ненулевых квадратов в $\mathbb{F}_p^*$. Согласно соответствию Галуа это означает, что круговое поле $\mathbb{Q}[\zeta_p]$ содержит ровно одно квадратичное расширение $\mathbb{K} \supset \mathbb{Q}$, и оно порождается над $\mathbb{Q}$ числом[1]

$$\vartheta = \sum_{\substack{\sigma \in \operatorname{Gal} \Phi_n : \\ m(\sigma) \in \mathbb{F}_p^{*\,2}}} \sigma(\zeta_p) - \sum_{\substack{\sigma \in \operatorname{Gal} \Phi_n : \\ m(\sigma) \notin \mathbb{F}_p^{*\,2}}} \sigma(\zeta_p) = \sum_{m=1}^{p-1} \left[\frac{m}{p}\right] \cdot \zeta_p^m , \tag{14-14}$$

которое инвариантно относительно подгруппы $\mathbb{F}_p^{*\,2} \subset \operatorname{Gal} \Phi_n$ и меняет знак под действием всех остальных автоморфизмов кругового поля.

Упражнение 14.8. Покажите, что $\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}[\vartheta]$ для всех простых $p > 2$, и явно выразите этот квадратный корень через корни $p$-той степени из единицы.

[1] напомню, что *символ Лежандра – Якоби* $\left[\frac{m}{p}\right] \stackrel{\text{def}}{=} \begin{cases} 0 & \text{если } m \bmod(p) = 0 \\ 1 & \text{если } m \bmod(p) \in \mathbb{F}_p^2 \smallsetminus 0 \\ -1 & \text{если } m \bmod(p) \notin \mathbb{F}_p^2 \end{cases}$

**14.4. Циклические расширения.** Элемент $\zeta$ произвольного поля $\Bbbk$ называется *примитивным*[1] корнем степени $m$ из единицы, если $\zeta^m = 1$ и $\zeta^i \neq 1$ при всех $0 < i < m$. Если поле $\Bbbk$ содержит такой корень $\zeta$, то циклическая мультипликативная группа корней уравнения $x^m = 1$ в поле $\Bbbk$ имеет порядок $m$ и порождается элементом $\zeta$, а множество образующих этой группы есть множество всех примитивных корней из единицы степени $m$. В частности, многочлен $x^m - 1$ в этом случае сепарабелен. Поэтому $m$ не делится на $\mathrm{char}(\Bbbk)$, и все многочлены $x^d - a \in \Bbbk[x]$ степени $d|m$ тоже сепарабельны. Мы продолжим обозначать циклическую мультипликативную группу корней $m$-той степени из единицы через $\boldsymbol{\mu}_m \subset \Bbbk^*$, и обозначим через $\Bbbk^{*s}$ мультипликативную группу $s$-тых степеней ненулевых элементов поля $\Bbbk$.

Теорема 14.3
Если в поле $\Bbbk$ есть примитивный корень степени $m$ из единицы и $a \in \Bbbk^*$, то разложение двучлена $f(x) = x^m - a$ на неприводимые множители в $\Bbbk[x]$ всегда имеет вид $f = g_1 g_2 \ldots g_k$, где $g_i(x) = x^n - b_i$ и $kn = m$, при этом группа $\mathrm{Gal}\, f/\Bbbk$ циклическая порядка $n$, а свободный член $a$ двучлена $f$ лежит в $\Bbbk^{*k}$. В частности, $f$ неприводим $\Longleftrightarrow n = m \Longleftrightarrow$ $\Bbbk$-алгебра $\Bbbk[x]/(f)$ является полем разложения $f$.

Доказательство. Фиксируем алгебраическое замыкание $\overline{\Bbbk}$ и какой-нибудь корень $\alpha \in \overline{\Bbbk}$ двучлена $f$. Корни $f$ в $\overline{\Bbbk}$ находится в биекции с корнями из единицы и имеют вид $\xi\alpha$, где $\xi$ пробегает $\boldsymbol{\mu}_m$. Если перестановка $g \in \mathrm{Gal}\, f/\Bbbk$ переводит $\alpha$ в $g(\alpha) = \zeta_g \cdot \alpha$, то она действует на остальные корни $f$ умножением на $\zeta_g$: $g(\xi\alpha) = \xi g(\alpha) = \xi\zeta_g\alpha = \zeta_g\xi\alpha$. Тем самым, отображение

$$\mathrm{Gal}\, f/\Bbbk \hookrightarrow \boldsymbol{\mu}_m, \quad g \mapsto \zeta_g = g(\alpha)/\alpha, \tag{14-15}$$

является инъективным гомоморфизмом групп. Так как группа $\boldsymbol{\mu}_m$ циклическая, образ $G \subset \boldsymbol{\mu}_m$ гомоморфизма (14-15) является циклической группой порядка $n|m$ и порождается некоторым примитивным корнем $\zeta$ степени $n$ из единицы. Смежные классы $G\xi \subset \boldsymbol{\mu}_m$ подгруппы $G$ биективно соответствуют орбитам действия группы Галуа на корнях $f$, и каждой такой орбите отвечает неприводимый множитель $f_\xi(x) \stackrel{\text{def}}{=} \prod_{\nu=0}^{n-1} \left(x - \zeta^\nu \xi\alpha\right)$ двучлена $f$ в $\Bbbk[x]$.

Упражнение 14.9. Покажите, что $f_\xi(x) = x^n - \xi^n\alpha^n$.

Так как $f_\xi \in \Bbbk[x]$, элементы $b_\xi = \xi^n\alpha^n$, а с ними и $c = \alpha^n$, лежат в $\Bbbk$, и разложение $f$ на неприводимые множители в $\Bbbk[x]$ имеет вид $x^m - a = \prod_{\xi\in\boldsymbol{\mu}_m/G} \left(x^n - b_\xi\right)$, а $a = \alpha^m = c^k \in \Bbbk^{*k}$, где $k = m/n$. В частности, $f$ неприводим, если и только если $n = m$, и в этом случае вложение (14-15) является изоморфизмом, а алгебра $\Bbbk[x]/(f)$ — полем, причём вместе с корнем $\alpha = x \bmod(f)$ она содержит и все остальные $m$ корней $\xi\alpha$ двучлена $f$. □

[1] или *первообразным*

Упражнение 14.10. В условиях теор. 14.3 покажите, что совпадение в $\overline{\Bbbk}$ полей разложения двучленов $x^m - a$ и $x^m - b$ равносильно равенству $a = b^r c^m$ для неких $c \in \Bbbk$ и целого $r$, взаимно простого с $m$.

Определение 14.1
Расширение Галуа $\mathbb{K} \supset \Bbbk$ называется *циклическим степени* $m$, если $\operatorname{Gal} \mathbb{K}/\Bbbk$ является циклической группой $m$-того порядка.

Теорема 14.4
Всякое циклическое расширение степени $m$ любого поля $\Bbbk$, содержащего первообразный корень $m$-той степени из единицы, является полем разложения неприводимого двучлена $x^m - a$ с $a \in \Bbbk$.

Доказательство. Пусть группа Галуа $G = \operatorname{Gal} \mathbb{K}/\Bbbk$ циклического расширения $\mathbb{K} \subset \Bbbk$ порождена автоморфизмом $\sigma \in \operatorname{Aut}_{\Bbbk} \mathbb{K}$ порядка $m$. Фиксируем какой-нибудь первообразный корень $m$-той степени из единицы $\zeta \in \Bbbk$ и рассмотрим $\Bbbk$-линейный эндоморфизм поля $\mathbb{K}$

$$L_{\zeta,\sigma} \stackrel{\text{def}}{=} \sum_{i=0}^{p-1} \zeta^i \sigma^i \,:\, \vartheta \mapsto \sum_{i=0}^{p-1} \zeta^i \sigma^i(\vartheta).$$

Поскольку автоморфизмы $\sigma^0 = \mathrm{Id}$, $\sigma$, $\sigma^2$, … , $\sigma^{m-1}$ являются различными мультипликативными характерами[1] абелевой группы $\mathbb{K}^*$ над полем $\mathbb{K}$, они линейно независимы в пространстве функций[2] $\mathbb{K}^* \to \mathbb{K}$, и значит, эндоморфизм $L_{\zeta,\sigma}$ ненулевой.

Упражнение 14.11. Убедитесь, что $\sigma L_{\zeta,\sigma} = \zeta^{-1} L_{\zeta,\sigma}$.

Равенство $\left(\sigma - \zeta^{-1}\right) L_{\zeta,\sigma} = 0$ означает, что образ оператора $L_{\zeta,\sigma}$ состоит из собственных векторов оператора $\sigma$ с собственным значением $\zeta^{-1}$. Тем самым, в $\mathbb{K}$ имеется такое ненулевое $\alpha$, что $\sigma(\alpha) = \zeta^{-1}\alpha$. Галуа-орбита числа $\alpha$ состоит из $m$ различных чисел $\sigma^i(\alpha) = \zeta^{-i}\alpha$, $0 \leqslant i \leqslant m-1$, являющихся корнями двучлена $f(x) = x^m - \alpha^m$, свободный член которого $a = \alpha^m$ лежит в $\Bbbk$, ибо он инвариантен относительно группы Галуа: $\sigma(\alpha^m) = \sigma(\alpha)^m = \zeta^{-m}\alpha^m = \alpha^m$. Поскольку корни $f$ образуют одну орбиту группы Галуа, двучлен $f$ неприводим, а так как все корни лежат в $\Bbbk[\alpha]$, примитивное расширение $\Bbbk[\alpha]$ является полем разложения $f$. Поскольку $\Bbbk[\alpha] \subset \mathbb{K}$ и степень обоих полей над $\Bbbk$ равна $m$, они совпадают друг с другом. □

Упражнение 14.12* (изоморфизм Куммера). Для каждого элемента $a \in \Bbbk^*/\Bbbk^{*m}$ зафиксируем некоторый корень $\alpha = \sqrt[m]{a} \in \overline{\Bbbk}$ и сопоставим каждому автоморфизму $\sigma \in \operatorname{Gal} \overline{\Bbbk}/\Bbbk$ корень из единицы $\zeta_\sigma = \sigma(\alpha)/\alpha \in \boldsymbol{\mu}_m$. Покажите, что таким образом корректно задаётся изоморфизм групп $\Bbbk^*/\Bbbk^{*m} \xrightarrow{\sim} \operatorname{Hom}\left(\operatorname{Gal} \overline{\Bbbk}/\Bbbk, \boldsymbol{\mu}_m\right)$.

[1] см. n° 5.4.1 на стр. 76

[2] см. уже цитированный n° 5.4.1 на стр. 76, в частности упр. 5.13

**14.5. Разрешимые расширения.** Группа $G$ называется *разрешимой*, если все её композиционные факторы Жордана – Гёльдера[1] суть простые циклические группы. Расширение Галуа $\mathbb{K} \supset \Bbbk$ поля $\Bbbk$ характеристики нуль называется *разрешимым*, если разрешима его группа Галуа $\operatorname{Gal} \mathbb{K}/\Bbbk$. Из установленных во втором семестре первого курса свойств композиционных рядов вытекает, что разрешимость группы $G$ равносильна существованию убывающей фильтрации $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{e\}$ подгруппами $G_{i+1} \lhd G_i$ с абелевыми факторами $G_i / G_{i+1}$.

Упражнение 14.13. Убедитесь, что любая подгруппа и любая фактор группа разрешимой группы $G$ разрешимы, и наоборот, разрешимость нормальной подгруппы $H \lhd G$ и фактора $G/H$ влекут разрешимость $G$.

Теорема 14.5
Пусть[2] $\operatorname{char}(\Bbbk) = 0$ и один из корней неприводимого многочлена $f \in \Bbbk[x]$ выражается через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечений корней произвольных степеней. Тогда группа $\operatorname{Gal} f/\Bbbk$ разрешима, и все корни $f$ выражаются в радикалах через элементы поля $\Bbbk$.

Доказательство. Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$. Если корень $\alpha \in \overline{\Bbbk}$ многочлена $f$ выражается в радикалах, то он лежит в подполе $\mathbb{L} \subset \overline{\Bbbk}$, к которому ведёт башня примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_m = \mathbb{L} \tag{14-16}$$

вида $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$, где $a_i \in \mathbb{L}_i$. Для доказательства теоремы достаточно вложить поле $\mathbb{L}$ в поле $\mathbb{L}' \supset \Bbbk$, являющееся расширением Галуа с разрешимой группой $\operatorname{Gal} \mathbb{L}'/\Bbbk$. Тогда поле разложения $\mathbb{K}$ многочлена $f$ будет нормальным над $\Bbbk$ подполем в $\mathbb{L}'$, и его группа Галуа $\operatorname{Gal} \mathbb{K}/\Bbbk = (\operatorname{Gal} \mathbb{L}'/\Bbbk)\,/\,(\operatorname{Gal} \mathbb{L}'/\mathbb{K})$, будучи фактором разрешимой группы, тоже будет разрешима. Для построения $\mathbb{L}'$ расширим по индукции башню (14-16) до башни

$$\Bbbk \subset \mathbb{L}'_0 \subset \mathbb{L}'_1 \subset \mathbb{L}'_2 \subset \cdots \subset \mathbb{L}'_m = \mathbb{L}', \tag{14-17}$$

в которой $\mathbb{L}_i \subset \mathbb{L}'_i$ и каждое $\mathbb{L}'_i$ является расширением Галуа поля $\Bbbk$. В качестве $\mathbb{L}'_0$ возьмём поле разложения многочлена $x^N - 1$ с таким $N$, чтобы в $\mathbb{L}'_0$ содержались первообразные корни из единицы всех степеней $k_i$, являющихся показателями радикалов в формуле для $\alpha$. Если $\mathbb{L}'_i$ уже построено, то в качестве $\mathbb{L}'_{i+1}$ возьмём поле разложения многочлена $\prod\limits_{\sigma \in \operatorname{Gal} \mathbb{L}'_i/\Bbbk} \bigl(x^{k_i} - \sigma(a_i)\bigr)$ над полем $\mathbb{L}'_i$.

[1] см. раздел 13.2 из лекции 13, прочитанной во втором семестре на первом курсе (http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/1314/lec-13.pdf)

[2] требование $\operatorname{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\operatorname{char}(\Bbbk)$ не делила ни один из показателей радикалов, участвующих в формуле для вычисления корня — приводимое ниже доказательство в этом случае тоже работает

Так как коэффициенты этого многочлена инвариантны относительно группы $\operatorname{Gal}\mathbb{L}'_i/\Bbbk$, они лежат в $\Bbbk$, и $\mathbb{L}'_{i+1} \supset \Bbbk$ является расширением Галуа, содержащим поле $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$. Отметим, что поле $\mathbb{L}'_{i+1}$ получается из поля $\mathbb{L}'_i$ цепочкой последовательных переходов к полям разложения двучленов вида $x^n - a$ с $a \in \mathbb{L}'_i$. По теор. 14.3 все такие переходы являются расширениями Галуа с циклическими группами Галуа. Согласно предл. 14.5 и предл. 13.4 первый шаг нашего построения — переход от $\Bbbk$ к $\mathbb{L}'_0$ — также является расширением Галуа с абелевой группой Галуа. Таким образом, поле $\mathbb{L}'$ можно получить из $\Bbbk$ последовательными абелевым расширением Галуа, и его группа $\operatorname{Gal}\mathbb{L}'/\Bbbk$ разрешима. □

Пример 14.4 (общее уравнение степени $n$ и теорема Абеля)
Зафиксируем произвольное поле $\mathbb{F}$. Многочлен

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}(a_1, a_2, \ldots, a_n)[x], \tag{14-18}$$

рассматриваемый над полем $\Bbbk = \mathbb{F}(a_1, a_2, \ldots, a_n)$ рациональных функций от $n$ алгебраически независимых переменных $a_1, a_2, \ldots, a_n$ с коэффициентами в $\mathbb{F}$, называется *общим*, поскольку придавая его коэффициентам конкретные значения из поля $\mathbb{F}$, можно получить любой «конкретный» многочлен $f \in \mathbb{F}[x]$. В частности, если имеется формула, выражающая корни общего многочлена (14-18) через элементы поля $\Bbbk = \mathbb{F}(a_1, a_2, \ldots, a_n)$ в радикалах[1], то она позволяет единообразно решить в радикалах все уравнения $n$-той степени с коэффициентами из $\mathbb{F}$. Из прим. 14.2 на стр. 220 следует, что над полем $\mathbb{F} = \mathbb{Q}$ такой формулы нет. Чтобы проанализировать наличие такой формулы над произвольным полем $\mathbb{F}$, вычислим группу $\operatorname{Gal} f/\Bbbk$. Обозначим через $t_1, t_2, \ldots, t_n$ корни $f$ в его поле разложения $\mathbb{K} \supset \Bbbk$. Поскольку $\mathbb{K}$ алгебраично над $\Bbbk$, его базис трансцендентности над $\mathbb{F}$ согласно сл. 10.4 можно выбрать из элементов $t_1, t_2, \ldots, t_n$, порождающих $\mathbb{K}$ как $\mathbb{F}$-алгебру[2], а т. к. $\operatorname{tr\,deg}_{\mathbb{F}}\mathbb{K} \geqslant n$, весь набор $t_1, t_2, \ldots, t_n$ и является таким базисом. Поэтому $t_1, t_2, \ldots, t_n$ алгебраически независимы над $\mathbb{F}$ и, в частности, различны. Значит, многочлен $f$ сепарабелен, а $\mathbb{K} = \mathbb{F}(t_1, t_2, \ldots, t_n)$ является расширением Галуа поля $\Bbbk = \mathbb{F}(a_1, a_2, \ldots, a_n)$. Поскольку любая перестановка независимых переменных продолжается до автоморфизма поля рациональных функций, $\operatorname{Gal}\mathbb{K}/\Bbbk = S_n$, $[\mathbb{K} : \Bbbk] = n!$ и $\mathbb{F}(t_1, t_2, \ldots, t_n)^{S_n} = \mathbb{F}(a_1, a_2, \ldots, a_n)$. Так как подгруппа $A_n \lhd S_n$ проста, группа $S_n$ не разрешима, а значит, общее уравнение степени $n \geqslant 5$ неразрешимо в радикалах ни над каким полем $\mathbb{F}$ нулевой характеристики. Этот результат известен как *теорема Абеля*[3].

[1] как это делает, например, школьная формула $x_\pm = \left(p \pm \sqrt{p^2 - 4q}\right)/2$ для решения «общего» квадратного уравнения $x^2 + px + q = 0$

[2] по теореме Виета $a_i$ являются полиномами от $t_i$

[3] сам Абель доказал эту теорему для поля $\mathbb{F} = \mathbb{C}$

Упражнение 14.14. Покажите, что поле инвариантов $\mathbb{K}^{A_n}$ подгруппы $A_n \lhd S_n$ является квадратичным расширением поля $\Bbbk$ элементом $\sqrt{D(f)} = \prod\limits_{1 \leqslant i < j \leqslant n} (t_i - t_j)$.

Замечание 14.2. Отсутствие «общей» формулы для решения в радикалах полиномиального уравнения $n$-той степени не запрещает существования специальных «конкетных» уравнений, корни которых можно выразить в радикалах через коэффициенты уравнения.

Теорема 14.6
Пусть[1] $\operatorname{char}(\Bbbk) = 0$ и $f \in \Bbbk[x]$ приведён и неприводим. Если группа $\operatorname{Gal} f / \Bbbk$ разрешима, то все корни $f$ выражаются через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечения корней.

Доказательство. Обозначим через $\mathbb{K} \supset \Bbbk$ поле разложения многочлена $f$, а через $\mathbb{L} \supset \Bbbk$ результат присоединения к $\Bbbk$ первообразного корня из единицы степени $n = |\operatorname{Gal} \mathbb{K}/\Bbbk|$. Все элементы поля $\mathbb{L}$ выражаются в радикалах через элементы поля $\Bbbk$. По условию, группа Галуа $\mathbb{K}$ над $\Bbbk$ разрешима. По предл. 13.4 расширение $\mathbb{LK} \supset \mathbb{L}$ является расширением Галуа, и его группа Галуа $G$ по теор. 13.4 является подгруппой в $\operatorname{Gal} \mathbb{K}/\Bbbk$, а значит, тоже разрешима и допускает фильтрацию $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{e\}$ подгруппами $G_{i+1} \lhd G_i$ с простыми циклическими факторами $G_i / G_{i+1} \simeq \mathbb{Z}/(p_i)$. Поэтому поле $\mathbb{LK}$ получается из поля $\mathbb{L}$ последовательностью циклических расширений Галуа. По теор. 14.4 каждое такое расширение является присоединением радикала. Следовательно, все элементы поля $\mathbb{LK} \supset \mathbb{K}$ выражаются в радикалах через элементы поля $\Bbbk$. □

[1] требование $\operatorname{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\operatorname{char}(\Bbbk)$ не совпадала с порядком никакого композиционного фактора Жордана – Гёльдера группы Галуа многочлена $f$ — приводимое ниже доказательство в этом случае тоже работает

## Ответы и указания к некоторым упражнениям

Упр. 14.1. 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 и/или теоремы Виета (для этого и требуется отрезок длины 1), а $\sqrt{a} = \sqrt{1 \cdot a}$ — при помощи теоремы о среднем геометрическом в прямоугольном треугольнике.

Упр. 14.2. Композиционные факторы 2-группы являются простыми 2-группами. Так как каждая 2-группа имеет нетривиальный центр, простая 2-группа абелева, а значит, изоморфна $\mathbb{Z}/(2)$.

Упр. 14.6. Пусть корни $\{\vartheta_1, \vartheta_2, \dots, \vartheta_k\} \subset \{\vartheta_1, \vartheta_2, \dots, \vartheta_n\}$ образуют орбиту группы Галуа. Тогда коэффициенты многочлена $g(x) = (x - \vartheta_1)(x - \vartheta_2) \cdots (x - \vartheta_k)$ инвариантны относительно действия группы Галуа, и значит, $g \in \Bbbk[x]$. Таким образом, многочлен $f$ является произведением многочленов $g$, отвечающих орбитам действия группы Галуа $\operatorname{Gal} f/\Bbbk$ 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. 14.7. Поле разложения $\mathbb{L}_{\overline{f}}$ многочлена $\overline{f}$ над $\mathbb{F}_p$ раскладывается в башню примитивных расширений $\mathbb{F}_p = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L}_{\overline{f}}$ на каждом этаже которой происходит присоединение одного из корней $\vartheta$ многочлена $\overline{f}$. Поскольку $\overline{f}$ 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, т. к. $\mathbb{L}_{\overline{f}}$ поле, и имеет образом $\mathbb{F}_p$-подалгебру, порождённую корнями многочлена $\overline{f}$ в $A$.

Упр. 14.9. Поскольку $x^n - 1 = \prod\limits_{\nu=0}^{n-1} \left(x - \zeta^\nu\right)$, элементарные симметрические полиномы $e_i\left(\zeta^0, \zeta^1, \dots, \zeta^{n-1}\right) = 0$ при $1 \leqslant i \leqslant n-1$. Поэтому все коэффициенты многочлена $f_\xi$, кроме старшего, равного 1, и свободного члена, равного $-\xi^n \alpha^n$, нулевые:

$$e_i\left(\zeta^0 \xi\alpha, \zeta^1 \xi\alpha, \dots, \zeta^{n-1} \xi\alpha\right) = \xi^i \alpha^i e_i\left(\zeta^0, \zeta^1, \dots, \zeta^{n-1}\right) = 0\,.$$

Упр. 14.13. Пересекая с подгруппой $H \subset G$ цепочку

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{e\} \tag{14-19}$$

в которой $G_{i+1} \lhd G_i$ и факторы $G_i / G_{i+1}$ абелевы, получим цепочку

$$H = G_0 \cap H \supset G_1 \cap H \supset G_2 \cap H \supset \cdots \supset G_{m-1} \cap H \supset G_m \cap H = H$$

с факторами $\big(G_i \cap H\big)/\big(G_{i+1} \cap H\big) \simeq \big((G_i \cap H) \cdot G_{i+1}\big)/G_{i+1} \subset G_i/G_{i+1}$. Будучи подгруппами абелевых факторов $G_{i+1}/G_i$ из цепочки (14-19), они тоже абелевы. Умножая элементы цепочки (14-19) на нормальную подгруппу $N \lhd G$ получаем цепочку $G = G_0 N \supset G_1 N \supset$

$G_2N \supset \cdots \supset G_{m-1}N \supset G_mN = N$, факторы которой по нормальной подгруппе $N$ дают цепочку подгрупп, ведущую от $G/N$ к $e = N/N$ с

$$\frac{G_iN/N}{G_{i+1}N/N} \simeq \frac{G_i}{G_{i+1}(N \cap G_i)} \simeq \frac{G_i/G_{i+1}}{(G_i \cap N)/G_{i+1}}\,.$$

Будучи факторами абелевых групп $G_i/G_{i+1}$ из цепочки (14-19), они тоже абелевы. Из двух цепочек $H = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{m-1} \supset H_m = \{e\}$ и $G/H = Q_0 \supset Q_1 \supset Q_2 \supset \cdots \supset Q_{k-1} \supset Q_k = \{e\}$ для нормальной подгруппы $H \lhd G$ и фактор группы $G/H$ собирается цепочка $G = Q_0H \subset Q_1H \supset Q_2H \supset \cdots \supset Q_kH = H_0 \supset H_1 \supset \cdots \supset H_m = \{e\}$, в которой $Q_iH$ суть полные прообразы подгрупп $Q_i \supset G/H$ относительно гомоморфизма факторизации $G \twoheadrightarrow G/H$.