§13. Группы Галуа

13.1. 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:

Упражнение 13.1. Даны точки $0,\ 1,\ a,\ b \in \mathbb{C}$. Циркулем и линейкой постройте в $\mathbb{C}$ точки $a \pm b$, a/b, ab и $\sqrt{a}$.

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

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L}, \text{ где } \mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big] \text{ и } a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2, \tag{13-1}$$

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 (13-1), причём все поля $\mathbb{L}_i$ этой башни переводятся в себя комплексным сопряжением $z \mapsto \overline{z}$.

Построение числа ζ распадается на элементарные шаги, каждый из которых добавляет новую точку p, являющуюся пересечением одного из трёх типов: прямых (ab) и (cd), прямой (ab) и проходящей через точку d окружности с центром в c или проходящих через точки b и d окружностей с центрами в точках $a]$ и c соответственно. При этом предполагается, что точки a, b, c, d уже построены, а искомая точка пересечения на евклидовой плоскости существует. Положим $\mathbb{L}_1 = \mathbb{Q}\big[\sqrt{-1}\big]$ и допустим по индукции, что a, b, c, d лежат поле $\mathbb{L}_i$ из башни (13-1), причём это поле переводится комплексным сопряжением в себя. Тогда число $(ab) \cap (cd)$ находится по правилу Крамера и тоже лежит в $\mathbb{L}_i$. Для отыскания пары чисел, возникающих при пересечении проходящей через точку d окружности S с центром в точке c с прямой (ab) или с проходящей через b окружностью с центром в a следует подставить в задающее S уравнение $(z-c)(\overline{z}-\overline{c}) = (d-c)(\overline{d}-\overline{c})$ зависящую от параметра t точку $z = a+(b-a)\,t$, которая пробегает прямую (ab) или проходящую через b окружность с центром в a, когда t пробегает, соответственно, вещественную прямую $\mathbb{R} \subset \mathbb{C}$ или единичную окружность $\mathrm{U}_1 \subset \mathbb{C}$. 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 13.2. Убедитесь в этом, выписав эти уравнения явно 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 $a+(b-a)\cdot t$ прямой или окружности, а значит, лежат в $\mathbb{L}_{i+1}$, что воспроизводит предположение индукции.

Предложение 13.1
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 $\Bbbk$:

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L}, \text{ где } \mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big] \text{ и } a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2, \tag{13-2}$$

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

Доказательство. Пусть $\mathbb{K}$ содержится в башне (13-2). 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 $G_i/G_{i+1} \simeq \mathbb{Z}/(2)$ при всех i. Соответствие Галуа[2] сопоставляет этой башне подгрупп ведущую от $\Bbbk$ к $\mathbb{K}$ башню квадратичных расширений $\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_n = \mathbb{K}$, в которой $\mathbb{L}_i = \mathbb{K}^{G_i}$. □

Теорема 13.1
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. 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. 13.1 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 (13-1). 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 $\psi : \mathbb{Q}[\vartheta] \hookrightarrow \mathbb{C}$, $\vartheta \mapsto \vartheta'$, продолжается до вложения $\overline{\psi} : \mathbb{L} \hookrightarrow \mathbb{C}$, совпадающего с ψ на подполе $\mathbb{Q}[\vartheta] \subset \mathbb{L}$ и переводящего башню (13-1) в башню

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}'_1 \subset \ldots \subset \mathbb{L}'_m = \mathbb{L}'\,, \tag{13-3}$$

в которой $\mathbb{L}'_{i+1} = \mathbb{L}'_i\left[\sqrt{a'_i}\right]$ для некоторого $a'_i = \widetilde{\psi}(a_i) \in \mathbb{L}'_i \smallsetminus \left(\mathbb{L}'_i\right)^2$. 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 $\mathbb{L},\ \mathbb{L}\mathbb{L}'_1,\ \ldots\ ,\ \mathbb{L}\mathbb{L}'_{m-1}$ 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. 13.1 степень $[\mathbb{K} : \mathbb{Q}]$ в этом случае является степенью двойки, что и утверждалось. □

Следствие 13.1
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 ζ, поэтому степень этого расширения над $\mathbb{Q}$ делит степень поля разложения минимального многочлена. □

Пример 13.1 (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 $\cos(\pi/9)$, имеющего над $\mathbb{Q}$ степень 3.

Упражнение 13.3. Убедитесь, что $\cos(\pi/9)$ является корнем неприводимого над $\mathbb{Q}$ многочлена $8x^3 - 6x - 1$.

[1] См. Теорему 12.1 на стр. 179 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_12.pdf.

[2] См. теор. 12.6 на стр. 181.

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

Упражнение 13.4* (построение Гаусса). Постройте правильный 17-угольник циркулем и линейкой.

13.1.1. 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 $\zeta_1, \dots, \zeta_n \in \mathbb{C}$. Поскольку все точки поля $\mathbb{F} = \mathbb{Q}(\zeta_1, \dots, \zeta_n) \subset \mathbb{C}$, порождённого этими числами, строятся циркулем и линейкой, можно считать, что изначально заданные точки образуют произвольное[2] 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 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 этого минимального многочлена тоже была степенью двойки.

Упражнение 13.5. Докажите все эти утверждения.

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

Предложение 13.2 (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. 12.3 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 $\mathbb{F}\mathbb{K}$ как алгебру над $\mathbb{F}$. По предл. 12.4 расширение $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ нормально и сепарабельно, т. е. является конечным расширением Галуа. Тем самым, $\mathbb{F}\mathbb{K}$ является полем разложения f над $\mathbb{F}$. 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 своим действием на корни. Это позволяет рассматривать обе группы $\operatorname{Gal} \mathbb{K}/\Bbbk$ и $\operatorname{Gal} \mathbb{F}\mathbb{K}/\mathbb{F}$ 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 $\operatorname{Gal} \mathbb{F}\mathbb{K}/\mathbb{F}$ — из перестановок, продолжающихся до автоморфизма $\mathbb{F}$-алгебры $\mathbb{F}\mathbb{K} = \mathbb{F}[\vartheta_1, \dots, \vartheta_n]$. 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 $\mathbb{F} \cap \mathbb{K}$. □

[1] Напомню, что круговой многочлен $\Phi_p(x)$ при простом p неприводим по критерию Эйзенштейна.
[2] Не обязательно алгебраическое над $\mathbb{Q}$.

13.2. Группы многочленов. Согласно предл. 12.3, 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 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 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

$$\operatorname{ev}_{\vartheta_1,\dots,\vartheta_n} : \Bbbk[t_1, \dots, t_n] \to \overline{\Bbbk}, \quad \psi \mapsto \psi(\vartheta_1, \dots, \vartheta_n), \tag{13-4}$$

ядро которого $I_\Bbbk(\vartheta) \stackrel{\text{def}}{=} \ker \operatorname{ev}_{\vartheta_1,\dots,\vartheta_n}$ является идеалом всех полиномиальных соотношений между корнями многочлена f, т. е. состоит из всех многочленов $\psi \in \Bbbk[t_1, \dots, t_n]$, равных нулю в точке $\vartheta = (\vartheta_1, \dots, \vartheta_n) \in \mathbb{A}^n(\overline{\Bbbk})$. 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. 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

$$\operatorname{Gal} f/\Bbbk \simeq \{g \in S_n \mid \forall \psi \in I_\Bbbk(\vartheta)\ \psi^g \in I_\Bbbk(\vartheta)\} \tag{13-5}$$

Именно так изначально и определял группу многочлена сам Галуа.

Замечание 13.1. Задаваемое формулой (13-5) вложение группы Галуа $\operatorname{Gal} f$ в стандартную симметрическую группу $S_n = \operatorname{Aut}\{1, \dots, n\}$ не является каноническим и *зависит* от выбора нумерации корней ϑ_i многочлена f.

Предложение 13.3
Аффинное алгебраическое многообразие $V(I_\Bbbk(\vartheta)) \subset \mathbb{A}^n(\overline{\Bbbk})$ представляет собою набор из $m = [\mathbb{L}_f : \Bbbk] = |\operatorname{Gal} f/\Bbbk|$ различных точек $(\vartheta_{g(1)}, \dots, \vartheta_{g(n)})$, где $g \in \operatorname{Gal} f/\Bbbk$, образующих одну орбиту действия группы $\operatorname{Gal} f/\Bbbk \subset S_n$ на пространстве $\mathbb{A}^n$ перестановками координат.

Доказательство. Пусть $f = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. По теореме Виета $e_i(\vartheta_1, \dots, \vartheta_n) = (-1)^i a_i$, где $e_i(t_1, \dots, t_n) \in \Bbbk[t_1, \dots, t_n]$ — элементарный симметрический многочлен. Тем самым, $e_i(t_1, \dots, t_n) - (-1)^i a_i \in I_\Bbbk(\vartheta)$ для каждого i. 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 $(x - \alpha_1)\cdots(x - \alpha_n) = f(x) = (x - \vartheta_1)\cdots(x - \vartheta_n)$, 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 $\operatorname{Gal} f/\Bbbk$, 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 $a \in V\left(I_\Bbbk(\vartheta)\right)$ получаются из координат точки ϑ перестановкой из группы Галуа многочлена f. Наоборот, для любой перестановки $g \in \operatorname{Gal} f/\Bbbk$ и всех $\psi \in I_\Bbbk(\vartheta)$ значение $\psi(\vartheta_{g(1)}, \dots, \vartheta_{g(n)}) = \psi^g(\vartheta_1, \dots, \vartheta_n) = 0$, поскольку $\psi^g \in I_\Bbbk(\vartheta)$. Следовательно все точки из $\operatorname{Gal} f/\Bbbk$-орбиты точки ϑ лежат в $V(I_\Bbbk(\vartheta))$. □

Упражнение 13.6. Покажите, что сепарабельный многочлен $f \in \Bbbk[x]$ неприводим если и только если группа $\operatorname{Gal} f/\Bbbk$ транзитивно действует на его корнях.

13.2.1. Резольвента Галуа. Обозначим через $\mathbb{L}_f \supset \Bbbk$ поле разложения многочлена

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \Bbbk[x]\,,$$

а через $\vartheta_1, \ldots, \vartheta_n$ — корни f в $\mathbb{L}_f$, и рассмотрим однородную линейную форму

$$\psi = \vartheta_1 t_1 + \cdots + \vartheta_n t_n \in \mathbb{L}_f[t_1, \ldots, t_n]\,. \tag{13-6}$$

Однородный многочлен $F(t_1, \ldots, t_n) = \prod_{\sigma\in S_n} \psi^\sigma = \prod_{\sigma\in S_n} (\vartheta_1 t_{\sigma(1)} + \cdots + \vartheta_n t_{\sigma(n)})$ степени $n!$ 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

$$F\left(t_1, \ldots, t_n\right) = \prod_{h\in S_n/G} F_h\left(t_1, \ldots, t_n\right)\,, \tag{13-7}$$

где

$$\begin{aligned} F_h\left(t_1, \ldots, t_n\right) &= \prod_{g\in G} \left(\vartheta_1 t_{hg(1)} + \cdots + \vartheta_n t_{hg(n)}\right) = \\ &= \prod_{g\in G} \left(\vartheta_{g^{-1}(1)} t_{h(1)} + \cdots + \vartheta_{g^{-1}(n)} t_{h(n)}\right) = \prod_{g\in G} g\left(\psi^h\right)\,. \end{aligned} \tag{13-8}$$

В последнем произведении $\psi^h \in \mathbb{L}_f[t_1, \ldots, t_n]$ означает линейную форму, полученную из формы ψ перестановкой $h \in S_n$ переменных $t_1, \ldots, t_n$, 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 (13-8) различны и составляют одну орбиту группы Галуа, каждый многочлен F_h имеет коэффициенты в поле $\Bbbk$ и неприводим над $\Bbbk$. Мы заключаем, что $F \in \Bbbk[t_1, \ldots, t_n]$, и формула (13-7) представляет собою разложение многочлена F на неприводимые множители в $\Bbbk[t_1, \ldots, t_n]$. Неприводимые многочлены F_h образуют орбиту многочлена F_e при действии симметрической группы S_n на кольце $\Bbbk[t_1, \ldots, t_n]$ 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 13.4
Перестановки переменных $t_1, \ldots, t_n$, переводящие в себя какой-нибудь неприводимый делитель резольвенты Галуа многочлена f в кольце $\Bbbk[t_1, \ldots, t_n]$, образуют в S_n подгруппу, изоморфную $\operatorname{Gal} f/\Bbbk$. □

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

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

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

Теорема 13.2
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 $\vartheta_1, \ldots, \vartheta_n$ многочлена f в его поле разложения $\mathbb{L}_f$ целы над $\mathbb{Z}$. Поэтому коэффициенты формы $\psi = \vartheta_1 t_1 + \cdots + \vartheta_n t_n$ из (13-6), а с ними и коэффициенты всех многочленов F_h из разложения (13-7), 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 (13-7) имеет место в $\mathbb{Z}[t_1,\dots,t_n]$. Приводя его по модулю p, получаем в $\mathbb{F}_p[t_1,\dots,t_n]$ равенство

$$\overline{F}(t_1,\dots,t_n)=\prod_{h\in S_n/G}\overline{F}_h(t_1,\dots,t_n) \tag{13-9}$$

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 13.7. 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. 13.4 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 $\overline{F}_h$. Следовательно $\operatorname{Gal}\overline{f}/\mathbb{F}_p\subset\operatorname{Gal}f/\mathbb{Q}$. □

Следствие 13.2
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 λ.

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 группы $\operatorname{Gal}\overline{f}/\mathbb{F}_p$ осуществляет перестановку корней многочлена $\overline{f}$ циклового типа λ. По теор. 13.2 эта перестановка содержится и в $\operatorname{Gal}f/\mathbb{Q}$. □

Пример 13.2 (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 неприводимых множителей $\leqslant 2$, и произведение всех неприводимых приведённых многочленов степеней 1 и 2 в $\mathbb{F}_p[x]$ равно[2] $x^{p^2}-x$. 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. 13.2 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

[1] См. прим. 12.7 на стр. 181.
[2] См. упр. 12.16 на стр. 181.

всю симметрическую группу, $\operatorname{Gal} f/\mathbb{Q} \simeq S_5$. Из теор. 13.5, которую мы докажем на стр. 192 ниже, вытекает, что корни многочлена $x^5 - x - 1$ не выражаются через рациональные числа при помощи четырёх арифметических операций и извлечения корней произвольных степеней.

13.3. 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*[1] 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 ζ_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 $\mathbb{Z}/(n)$. Это задаёт гомоморфное вложение группы Галуа кругового поля в мультипликативную группу обратимых элементов кольца вычетов:

$$\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q} \hookrightarrow \big(\mathbb{Z}/(n)\big)^*, \quad \sigma \mapsto m(\sigma). \tag{13-10}$$

Поскольку множество $R_n \stackrel{\text{def}}{=} \{\zeta_n^m \mid \text{нод}(n,m) = 1\} \subset \boldsymbol{\mu}_n$ всех первообразных корней степени n из единицы 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 Φ_n и $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q} = \operatorname{Gal}\Phi_n/\mathbb{Q}$.

13.3.1. Элементы Фробениуса. При простом $p \nmid n$ многочлен $x^n - 1$ сепарабелен над $\mathbb{F}_p$. Редукция $\overline{\Phi}_n$ многочлена Φ_n по модулю p тоже сепарабельна над $\mathbb{F}_p$, т. к. $\overline{\Phi}_n$ делит $x^n - 1$. Поэтому сопоставление $\xi \mapsto \overline{\xi} = \xi \pmod p \in \mathcal{O}/(p)$ задаёт биекцию между множеством $R_n \subset \mathcal{O} \subset \mathbb{Q}[\zeta_n] \subset \mathbb{C}$ комплексных первообразных корней и множеством корней многочлена $\overline{\Phi}_n$ в его поле разложения над $\mathbb{F}_p$, которое порождается этими корнями как алгебра над $\mathbb{F}_p$ и является конечным расширением Галуа поля $\mathbb{F}_p$ с циклической группой Галуа, порождённой автоморфизмом Фробениуса[2] $\overline{\xi} \mapsto \overline{\xi}^p$. По теор. 13.2 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

$$F_p : \boldsymbol{\mu}_n \xrightarrow{\sim} \boldsymbol{\mu}_n, \quad \xi \mapsto \xi^p, \tag{13-11}$$

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 $\operatorname{Gal}\overline{\Phi}_n/\mathbb{F}_p$ *канонически* вложены в группу $\operatorname{Gal}\Phi_n/\mathbb{Q}$.

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 ζ_n^m для некоторого $m = p_1^{m_1} \cdots p_k^{m_k}$, взаимно простого с n, и равен $F_{p_1}^{m_1} \cdots F_{p_k}^{m_k} \zeta_n$. Мы заключаем, что группа Галуа кругового многочлена транзитивно действует на его корнях.

[1] Или *циклотомическим*.

[2] См. прим. 12.7 на стр. 181 и доказательство сл. 13.2 на стр. 188.

Предложение 13.5
Многочлен Φ_n неприводим над $\mathbb{Q}$ и является минимальным многочленом первообразного корня ζ_n над $\mathbb{Q}$, а вложение (13-10) является изоморфизмом групп, т. е. $\operatorname{Gal}\Phi_n \simeq (\mathbb{Z}/(n))^*$. В частности, $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$, где φ — функция Эйлера.

Доказательство. Если бы многочлен Φ_n был приводим над $\mathbb{Q}$, его группа Галуа переводила бы множество корней каждого неприводимого множителя в себя и не могла бы транзитивно действовать на корнях многочлена Φ_n. Из транзитивности действия группы $\operatorname{Gal}\Phi_n$ на корнях вытекает неравенство $|\operatorname{Gal}\Phi_n| \geqslant \deg\Phi_n = \varphi(n) = |(\mathbb{Z}/(n))^*|$, гарантирующее сюръективность вложения (13-10). □

Пример 13.3 (Гауссова сумма)
При простом $p > 2$ любая мультипликативная подгруппа $H \subset \mathbb{F}_p^*$ индекса 2 содержит все ненулевые квадраты поля $\mathbb{F}_p$, поскольку в $\mathbb{F}_p^*/H \simeq \mathbb{Z}/(2)$ выполняется равенство $\xi^2 H = \xi H \cdot \xi H = H$. Это означает, что мультипликативная подгруппа индекса индекса 2 в $\mathbb{F}_p^*$ единственна и совпадает с группой ненулевых квадратов. Мы заключаем, что группа Галуа кругового поля $\mathbb{Q}[\zeta_p]$, порождённого корнем $\zeta_p = e^{2\pi i/p}$, тоже содержит ровно одну подгруппу индекса 2, и изоморфизм $m: \operatorname{Gal}\Phi_p \xrightarrow{\sim} \mathbb{F}_p^*$ из форм. (13-10) на стр. 189 отождествляет эту подгруппу с группой ненулевых квадратов в $\mathbb{F}_p^*$. Согласно соответствию Галуа, круговое поле $\mathbb{Q}[\zeta_p]$ содержит ровно одно квадратичное расширение $\mathbb{K} \supset \mathbb{Q}$, и оно порождается над $\mathbb{Q}$ числом[1]

$$\vartheta = \sum_{\substack{\sigma\in\operatorname{Gal}\Phi_p:\\ m(\sigma)\in\mathbb{F}_p^{*\,2}}} \sigma(\zeta_p) - \sum_{\substack{\sigma\in\operatorname{Gal}\Phi_p:\\ m(\sigma)\notin\mathbb{F}_p^{*\,2}}} \sigma(\zeta_p) = \sum_{m=1}^{p-1} \left[\frac{m}{p}\right]\cdot\zeta_p^m\,, \tag{13-12}$$

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

Упражнение 13.8. Покажите, что $\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{Q}[\zeta_p]$ для всех простых $p > 2$, и явно выразите этот квадратный корень через корни p-той степени из единицы. Правая часть (13-12) называется *Гауссовой суммой*.

13.4. Циклические расширения. Элемент ζ произвольного поля $\Bbbk$ называется *примитивным* или *первообразным* 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 ζ, то циклическая мультипликативная группа корней уравнения $x^m = 1$ в поле $\Bbbk$ имеет порядок m и порождается элементом ζ, 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 $\operatorname{char}(\Bbbk)$, 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 $\Bbbk$.

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

Теорема 13.3
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 $f = g_1 \dots g_k$ с $g_i(x) = x^n - b_i$, где $b_i \in \Bbbk^*$ и $n = m/k$. Такое разложение возникает если и только если группа $\operatorname{Gal} f/\Bbbk$ циклическая порядка n, и в этом случае $a \in \Bbbk^{*k}$. В частности, неприводимость f равносильна равенству $|\operatorname{Gal} f/\Bbbk| = m$, а также тому, что $\Bbbk$-алгебра $\Bbbk[x]/(f)$ является полем разложения многочлена 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 ξ пробегает $\boldsymbol{\mu}_m$. Если $g \in \operatorname{Gal} f/\Bbbk$ переводит α в $g(\alpha) = \zeta_g\alpha$, то g действует и на остальные корни f умножением на ζ_g, ибо $g(\xi\alpha) = \xi g(\alpha) = \xi\zeta_g\alpha = \zeta_g\xi\alpha$. Поэтому отображение

$$\operatorname{Gal} f/\Bbbk \hookrightarrow \boldsymbol{\mu}_m\,, \quad g \mapsto \zeta_g = g(\alpha)/\alpha\,, \tag{13-13}$$

является инъективным гомоморфизмом групп. Обозначим через $G \subset \boldsymbol{\mu}_m$ его образ. Так как группа $\boldsymbol{\mu}_m$ циклическая, $G \simeq \operatorname{Gal} f/\Bbbk$ является циклической группой порядка $n|m$ и порождается некоторым примитивным корнем ζ 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 13.9. Покажите, что $f_\xi(x) = x^n - \xi^n\alpha^n$.

Так как $f_\xi \in \Bbbk[x]$, все элементы $b_\xi = \xi^n\alpha^n$ и, в частности, $c = \alpha^n$ лежат в $\Bbbk$. Таким образом, 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 свободный член $a = \alpha^m = c^k \in \Bbbk^{*k}$, где $k = m/n$. Неприводимость f означает равенство $n = m$, и в этом случае вложение (13-13) является изоморфизмом, а алгебра $\Bbbk[x]/(f)$ — полем, содержащим вместе с $\alpha = x \pmod f$ и все остальные m корней $\xi\alpha$ двучлена f. □

Упражнение 13.10. В условиях теор. 13.3 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 13.1
Расширение Галуа $\mathbb{K} \supset \Bbbk$ называется *циклическим степени* m, если $\operatorname{Gal}\mathbb{K}/\Bbbk$ является циклической группой m-того порядка.

Теорема 13.4
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 $\mathbb{K} \supset \Bbbk$ 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 $\sigma^0 = \mathrm{Id}$, σ, σ^2, … , σ^{m-1} являются различными мультипликативными характерами[1] абелевой группы $\mathbb{K}^*$ над полем $\mathbb{K}$, они линейно независимы в пространстве функций[2] $\mathbb{K}^* \to \mathbb{K}$. Поэтому эндоморфизм $L_{\zeta,\sigma}$ ненулевой.

Упражнение 13.11. 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 σ с собственным значением ζ^{-1}. Тем самым, в $\mathbb{K}$ имеется такое ненулевое α, что $\sigma(\alpha) = \zeta^{-1}\alpha$. Галуа-орбита числа α 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 $\Bbbk$, так как 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 13.12* (изоморфизм Куммера). Для каждого элемента $a \in \Bbbk^*/\Bbbk^{*m}$ зафиксируем некоторый корень $\alpha = \sqrt[m]{a} \in \overline{\Bbbk}$ и сопоставим каждому автоморфизму $\sigma \in \mathrm{Gal}\,\overline{\Bbbk}/\Bbbk$ корень из единицы $\zeta_\sigma = \sigma(\alpha)/\alpha \in \boldsymbol{\mu}_m$. Покажите, что таким образом корректно задаётся изоморфизм групп $\Bbbk^*/\Bbbk^{*m} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}\,\overline{\Bbbk}/\Bbbk, \boldsymbol{\mu}_m)$.

13.5. Разрешимые расширения. Конечная группа G называется *разрешимой*, если все её композиционные факторы Жордана – Гёльдера[3] суть простые циклические группы. Расширение Галуа $\mathbb{K} \supset \Bbbk$ поля $\Bbbk$ характеристики нуль называется *разрешимым*, если разрешима его группа Галуа $\mathrm{Gal}\,\mathbb{K}/\Bbbk$. Из установленных во втором семестре первого курса свойств композиционных рядов вытекает, что разрешимость группы G равносильна существованию убывающей фильтрации $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ подгруппами $G_{i+1} \lhd G_i$ с абелевыми факторами G_i/G_{i+1}.

Упражнение 13.13. 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 13.5
Пусть[4] $\mathrm{char}(\Bbbk) = 0$ 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 $\mathrm{Gal}\, f/\Bbbk$ 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

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L} \tag{13-14}$$

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 $\mathrm{Gal}\,\mathbb{L}'/\Bbbk$. Тогда

[1] См. n° 5.4.1 на стр. 72.
[2] См. цитированный выше n° 5.4.1 на стр. 72, в частности упр. 5.21.
[3] См. n° 12.2 на стр. 178 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_12.pdf.
[4] Требование $\mathrm{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\mathrm{char}(\Bbbk)$ не делила ни один из показателей радикалов, участвующих в формуле для вычисления корня. Приводимое доказательство в этом случае тоже работает.

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 башню (13-14) до башни $\Bbbk \subset \mathbb{L}'_0 \subset \mathbb{L}'_1 \subset \ldots \subset \mathbb{L}'_m = \mathbb{L}'$, в которой $\mathbb{L}_i \subset \mathbb{L}'_i$ и все $\mathbb{L}'_i$ являются расширениями 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 α. Далее действуем по индукции: если $\mathbb{L}'_i$ уже построено, то в качестве $\mathbb{L}'_{i+1}$ возьмём поле разложения многочлена $\prod_{\sigma\in\operatorname{Gal}\mathbb{L}'_i/\Bbbk}(x^{k_i} - \sigma(a_i))$ над полем $\mathbb{L}'_i$. 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 $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$. 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. 13.3 все такие переходы являются расширениями Галуа с циклическими группами Галуа. Согласно предл. 13.5 и предл. 12.4 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 13.4 (общее уравнение степени n и теорема Абеля)
Зафиксируем произвольное поле $\mathbb{F}$. Многочлен

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}(a_1, \ldots, a_n)[x], \tag{13-15}$$

рассматриваемый над полем $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$ рациональных функций от n алгебраически независимых переменных $a_1, \ldots, a_n$ 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 (13-15) через элементы поля $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$ в радикалах[1], то она позволяет единообразно решить в радикалах все уравнения n-той степени с коэффициентами из $\mathbb{F}$. Из прим. 13.2 на стр. 188 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 $t_1, \ldots, t_n$ корни f в его поле разложения $\mathbb{K} \supset \Bbbk$. Поскольку $\mathbb{K}$ алгебраично над $\Bbbk$, его базис трансцендентности над $\mathbb{F}$ согласно сл. 9.6 можно выбрать из элементов $t_1, \ldots, t_n$, порождающих $\mathbb{K}$ как $\mathbb{F}$-алгебру[2]. Так как $\operatorname{tr deg}_{\mathbb{F}}\mathbb{K} \geqslant n$, базисом трансцендентности $\mathbb{K}$ над $\mathbb{F}$ является весь набор $t_1, \ldots, t_n$. В частности, $t_1, \ldots, t_n$ алгебраически независимы над $\mathbb{F}$ и различны, многочлен f сепарабелен, а $\mathbb{K} = \mathbb{F}(t_1, \ldots, t_n)$ является расширением Галуа поля $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$. Поскольку любая перестановка независимых переменных продолжается до автоморфизма поля рациональных функций, группа $\operatorname{Gal}\mathbb{K}/\Bbbk = S_n$, степень $[\mathbb{K} : \Bbbk] = n!$ и поле инвариантов $\mathbb{F}(t_1, \ldots, t_n)^{S_n} = \mathbb{F}(a_1, \ldots, a_n)$. Так как подгруппа $A_n \lhd S_n$ проста, группа S_n не разрешима, а значит, общее уравнение степени $n \geqslant 5$ не разрешимо в радикалах ни над каким полем $\mathbb{F}$. Этот результат известен как *теорема Абеля*[3].

Упражнение 13.14. Покажите, что поле инвариантов $\mathbb{K}^{A_n}$ подгруппы $A_n \lhd S_n$ является квадратичным расширением поля $\Bbbk$ элементом $\sqrt{D(f)} = \prod_{1\leqslant i<j\leqslant n}(t_i - t_j)$.

[1] Как это делает, например, школьная формула $x_\pm = (p \pm \sqrt{p^2 - 4q})/2$ 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 $\mathbb{F} = \mathbb{C}$ с привлечением комплексного анализа.

Замечание 13.2. 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 13.6
Пусть[1] $\operatorname{char}(\Bbbk) = 0$ и $f \in \Bbbk[x]$ приведён и неприводим. Если группа $\operatorname{Gal} f / \Bbbk$ разрешима, то все корни многочлена 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 степени $n = |\operatorname{Gal} \mathbb{K}/\Bbbk|$ из единицы. Все элементы поля $\mathbb{L}$ выражаются в радикалах через элементы поля $\Bbbk$. По предл. 13.2 расширение $\mathbb{LK} \supset \mathbb{L}$ является расширением Галуа, и его группа Галуа G является подгруппой разрешимой группы $\operatorname{Gal} \mathbb{K} / \Bbbk$. Поэтому G тоже разрешима и имеет фильтрацию $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ с простыми циклическими факторами $G_i / G_{i+1} \simeq \mathbb{Z} / (p_i)$. Тем самым, поле $\mathbb{LK}$ получается из $\mathbb{L}$ последовательными циклическими расширениями Галуа. По теор. 13.4 каждое такое расширение получается присоединением радикала. Следовательно, все элементы поля $\mathbb{LK}$ 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 доказательство в этом случае тоже работает.

Ответы и указания к некоторым упражнениям

Упр. 13.1. 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 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. 13.2. 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. 13.3. 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. 13.6. 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 $\operatorname{Gal} f/\Bbbk$ 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. 13.7. 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.

Упр. 13.8. Подставляя $t = 1$ в $1 + t + \ldots + t^{p-1} = \Phi_p(t) = \prod_{k=1}^{p-1}(t - \zeta^k)$, где $\zeta = e^{2\pi i/p}$, получаем

$$p = \prod_{k=1}^{(p-1)/2} (1-\zeta^k)(1-\zeta^{-k}) = \prod_{k=1}^{(p-1)/2} (-\zeta^{-k})\cdot(1-\zeta^k)^2 = (-1)^{(p-1)/2}\alpha^2\beta^2\,,$$

где $\beta = \prod_{k=1}^{(p-1)/2}(1-\zeta^k)$, а $\alpha = \zeta^m$ с $2m \equiv -\sum_{k=1}^{(p-1)/2} k = (1-p^2)/8 \pmod p$.

Упр. 13.9. Поскольку $\prod_{\nu=0}^{n-1}\left(x - \zeta^\nu\right) = x^n - 1$, значения элементарных симметрических многочленов $e_i(\zeta^0, \zeta^1, \ldots, \zeta^{n-1}) = 0$ при $1 \leqslant i \leqslant n-1$. Поэтому все коэффициенты многочлена f_ξ, кроме старшего, равного 1, и свободного члена, равного $-\xi^n\alpha^n$, нулевые: $e_i(\zeta^0\xi\alpha, \zeta^1\xi\alpha, \ldots, \zeta^{n-1}\xi\alpha) = \xi^i\alpha^i e_i(\zeta^0, \zeta^1, \ldots, \zeta^{n-1}) = 0$.

Упр. 13.13. Пересекая с подгруппой $H \subset G$ цепочку $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$, в которой $G_{i+1} \lhd G_i$ и факторы G_i/G_{i+1} абелевы, получим цепочку $H = G_0 \cap H \supseteq G_1 \cap H \supseteq \ldots \supseteq G_m \cap H = H$ с факторами $(G_i \cap H)/(G_{i+1} \cap H) \simeq ((G_i \cap H)\,G_{i+1})/G_{i+1} \subset G_i/G_{i+1}$. Будучи подгруппами абелевых факторов G_{i+1}/G_i, они тоже абелевы. Умножая цепочку $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ на подгруппу $N \lhd G$ получаем цепочку $G = G_0N \supset G_1N \supset \ldots \supset G_mN = N$, факторы которой

по N дают ведущую от G/N к $e = N/N$ цепочку подгрупп с факторами $(G_iN/N)/(G_{i+1}N/N) \simeq$ $\simeq G_i/(G_{i+1}(N \cap G_i)) \simeq (G_i/G_{i+1})/((G_i \cap N)/G_{i+1})$. Будучи факторами абелевых групп G_i/G_{i+1}, они абелевы. Цепочки $H = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$ и $G/H = Q_0 \supset Q_1 \supset \ldots \supset Q_k = \{e\}$ для $H \lhd G$ и G/H собираются в $G = Q_0' \supset Q_1' \supset \ldots \supset Q_k' = H \supset H_1 \supset \ldots \supset H_m = \{e\}$, где Q_i' обозначают полные прообразы подгрупп $Q_i \subset G/H$ при гомоморфизме факторизации $G \twoheadrightarrow G/H$.