РАСШИРЕНИЯ ГАЛУА

Для того, чтобы ввести основные понятия теории Галуа, нам понадобятся некоторые пройденные знания о группах и о расширениях полей.

Если говорить более конкретно, мы будем опираться на два пройденных раньше предложения.

Предложение 1 (повторение). *Любое конечномерное расширение поля K — алгебраическое. Это расширение является цепочкой некоторых простых алгебраических расширений.*

Предложение 2 (повторение). *Пусть $P(\alpha)$ — расширение поля P, полученное присоединением корня α неприводимого многочлена $h \in P[x]$, и φ — гомоморфизм поля P в некоторое поле F.*

Тогда гомоморфизм φ продолжается до гомоморфизма $\psi : P(\alpha) \to F$ ровно столькими способами, сколько различных корней имеет в F многочлен $\varphi(h)$, полученный из h применением к его коэффициентам гомоморфизма φ.

Определение 1. Пусть L — конечномерное расширение поля K, $\dim_K L = n$. Группа автоморфизмов

$$\mathrm{Aut}\,_K L$$

— это автоморфизмы поля L, действующие на K тождественно.

Если

$$G \subset \mathrm{Aut}\,_K L,$$

обозначим через L^G подмножество L, состоящее из всех элементов L, инвариантных относительно G (не сдвигающихся при автоморфизмах из G).

Лемма 1. *Множество L^G является полем.*

Предложение 3. *Имеет место*

$$|\mathrm{Aut}\,_K L| \leqslant n.$$

Если $|G| = n$ (то есть $G = \mathrm{Aut}\,_K L$), то $L^G = K$.

Доказательство. Пусть расширение L поля K есть последовательность l простых расширений $K = L_0 \subset L_1 \dots \subset L_{l-1} \subset L_l = L$, где $\dim L_i/L_{i-1} = m_i$. Тогда $n = m_1 \dots m_l$. При каждом из расширений автоморфизм (уже продолженный на L_i) может продолжиться на L_{i+1} не более чем m_{i+1}

способами. Таким образом, всего способов продолжить тождественный автоморфизм на K на поле L — не более n.

$$|G| \leqslant \dim_{L^G} L \leqslant \dim_K L = n.$$

Если же $|G| = |\operatorname{Aut}_K L| = n$, то поле L является расширением поля $L^G \supset K$, при этом размерность L над L^G не меньше порядка G, т.е. не меньше n. С другой стороны, эта размерность не больше n, так как K содержится в L^G.

Значит,

$$\dim_{L^G} L = \dim_K L,$$

откуда

$$L^G = K.$$

$\square$

Предложение 4. *Если $L^G = K$, то для любых полей P и Q таких, что*

$$K \subset P \subset Q \subset L,$$

всякий гомоморфизм

$$\varphi : P \to L$$

над K продолжается до гомоморфизма

$$\psi : Q \to L$$

ровно $\dim_P Q$ способами.

Доказательство. Пусть $L^G = K$. Для любого элемента $\alpha \in L$ пусть

$$\{\alpha_1, \ldots, \alpha_m\}$$

— его G-орбита.

Тогда

$$f = \prod_{i=1}^{m} (x - \alpha_i) \in L^G[x] = K[x]$$

есть минимальный многочлен элемента α над K.

Действительно, любом автоморфизм $g \in G$ индуцирует перестановку корней этого многочлена, которая не меняет сам многочлен, поэтому коэффициенты многочлена f не меняются ни от одного автоморфизма $g \in G$. Так как $L^G = K$, то $f \in K[x]$.

С другой стороны, если существовал бы многочлен $h(x) \in K[x]$ меньшей степени и содержащий α в качестве корня, то все элементы вида $g\alpha$, $g \in G$ также должны были являться его корнями.

Значит, $f(x)$ — минимальный многочлен элемента α над K.

По построению он разлагается на различные линейные множители в $L[x]$.

Докажем теперь утверждение предложения.

Ясно, что можно доказывать это утверждение для простого расширения от P к Q, $Q = P(\alpha)$.

Пусть h — минимальный многочлен элемента α над P.

Тогда h делит минимальный многочлен f элемента α над K в кольце $P[x]$.

Следовательно, $\varphi(h)|f$ в кольце $\varphi(P[x])$ (так как $\varphi(f) = f$).

Значит, он разлагается на различные линейные множители в $L[x]$.

По предложению 2 гомоморфизм φ продолжается до гомоморфизма $\psi : Q \to L$ ровно $\deg h = \dim_P Q$ способами.

□

Предложение 5. *Если $L^G = K$, то $|\operatorname{Aut}_K L| = n$.*

Доказательство. Применяя предыдущее утверждение к случаю $P = K$, $Q = L$, получим $|\operatorname{Aut}_K L| = n$. □

Далее нам понадобиться следующая вспомогательная лемма.

Лемма 2. *Конечномерное векторное пространство над бесконечным полем не может быть покрыто конечным числом собственных подпространств.*

Доказательство. Пусть утверждение неверно, и некоторое конечномерное векторное пространство над бесконечным полем покрыто конечным числом подпространств, отличных от самого этого пространства.

Сначала последовательно ислючим все подпространства, которые содержатся в объединении остальных. Таким образом, у нас останется конечное число собственных подпространств, в каждом из которых есть вектор, не содержащийся ни в одном из остальных.

Далее выберем по вектору v_i в каждом пространстве, который не лежит в остальных.

Рассмотрим линейные комбинации

$$\alpha v_1 + v_2.$$

Какие-то две из них лежат в одном и том же подпространстве, так как поле бесконечно.

Это не может быть никакое подпространство, кроме первого, так как в ином случае вектор v_1 (как разность двух таких векторов, умноженная на число) содержался бы в каком-то пространстве, отличном от первого.

Но первое тоже не может быть — тогда с нем лежит второй вектор.

Получаем противоречие. $\square$

Теорема 1. *Пусть G — подгруппа группы $\operatorname{Aut}_K L$, $n = \dim_K L$.*

При этих условиях $L^G = K$ тогда и только тогда, когда $|G| = n$ (то есть $G = \operatorname{Aut}_K L$).

Кроме того, если это условие выполнено, то для любых полей P и Q таких, что

$$K \subset P \subset Q \subset L,$$

всякий гомоморфизм

$$\varphi : P \to L$$

над K продолжается до гомоморфизма

$$\psi : Q \to L$$

ровно $\dim_P Q$ способами.

Доказательство. В предложении 3 было доказано, что если $|G| = n$, то $L^G = K$.

В предложении 5 было доказано, что если $L^G = K$, то $|\operatorname{Aut}_K L| = n$.

Получается, что нам достаточно доказать, что если $L^G = K$, то $G = \operatorname{Aut}_K L$.

Пусть $\varphi \in \operatorname{Aut}_K L$.

Тогда для любого $\alpha \in L$ элемент $\varphi(\alpha)$, как и α, является корнем многочлена

$$f = \prod_{i=1}^{m} (x - \alpha_i) \in L^G[x] = K[x]$$

т. е. существует такой элемент $g = g_\alpha \in G$ (быть может, зависящий от α), что $\varphi(a) = ga$.

Если поле L конечно, то в качестве α возьмем элемент, порождающий группу L^* (которая, как мы знаем, является циклической), и тогда мы получим, что

$$\varphi = g \in G.$$

Если же L (и, стало быть, K) бесконечно, то для каждого $g \in G$ положим

$$L_g = \{\alpha \in L : \varphi(\alpha) = g\alpha\} \subset L.$$

Очевидно, что L_g — подпространство над K (и даже подполе в L). Из доказанного следует, что

$$L = \bigcup_{g \in G} L_g.$$

Отсюда мы получаем, что на самом деле $L = L_g$ для некоторого $g \in G$.

$\square$

Определение 2. Если $\dim_K L = |\operatorname{Aut}_K L|$, то L называется *расширением Галуа поля* K, группа $\operatorname{Aut}_K L$ в этом случае называется *группой Галуа* $\operatorname{Gal} L/K$.

Предложение 6. *Пусть L — расширение Галуа поля K, $K \subset P \subset L$.*

Тогда L — расширение Галуа поля P.

Доказательство. Если L — расширение Галуа поля K.

Тогда по теореме 1 для поля P такого, что

$$K \subset P \subset L$$

(полагаем в этой теореме $Q = L$), всякий гомоморфизм

$$\varphi : P \to L$$

над K продолжается до гомоморфизма

$$\psi : L \to L$$

ровно $\dim_P L$ способами.

В том числе, тождественный автоморфизм $P \to P$ продолжается $\dim_P L$ способами до эндоморфизма $L \to L$, тождественного на P. Так как иделов в поле нет, то ядро каждого такого эндоморфизма должно быть нулевым, то есть он является автоморфизмом.

Значит, мы получили не менее $\dim_P L$ различных автоморфизмов поля L, тождественных на P, что означает, что L — расширение Галуа поля P.

□

СЕПАРАБЕЛЬНЫЕ МНОГОЧЛЕНЫ

Определение 3. Многочлен $f \in K[x]$ называется *сепарабельным*, если он не имеет кратных корней ни в одном расширении поля K.

Лемма 3. *Многочлен $f \in K[x]$ сепарабелен тогда и только тогда, когда $(f, f') = 1$.*

Доказательство. Если многочлен f имеет кратный корень α в каком-то расширении поля K, то и он, и его (формальная) производная делятся на $x - \alpha$.

Если $(f, f') \neq 1$, то какой-то неприводимый множитель $h(x)$ многочлена f над K делит f'.

Это означает

$$f(x) = h(x)g_1(x), \quad f'(x) = h(x)g_2(x),$$

при этом

$$f'(x) = (h(x)g_1(x))' = h(x)g_1'(x) + h'(x)g_1(x) = h(x)g_2(x).$$

Таким образом, произведение $h'(x)g_1(x)$ делится на неприводимый многочлен $h(x)$. Значит, либо $g_1(x)$ делится на $h(x)$, либо $h'(x) = 0$,

В первом случае f имеет кратный корень в каком-то расширении поля K.

Второй случай имеет место, только если $\operatorname{char} K = p > 0$ и многочлен h имеет вид

$$h = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_mx^{mp} \quad (a_0, a_1, \ldots, a_m \in K).$$

Пусть L — расширение поля K, содержащее такие элементы $b_0, \ldots, b_m$, что $b_k^p = a_k$. Тогда в $L[x]$

$$h = (b_0 + b_1x + b_2x^2 + \cdots + b_nx^m)^p.$$

Следовательно,в некотором расширении поля L многочлен h имеет кратный корень. □

Следствие 1. *Если* $\operatorname{char} K = 0$*, то всякий неприводимый многочлен над полем* K *сепарабелен.*

Доказательство. Производная многочлена (отличного от константы) над полем нулевой характеристики не бывает нулевой. Если у многочлена есть кратный корень в каком-то расширении, то $(f, f') = d \neq 1$. При этом f не может делить свою производную, откуда следует, что кратных корней нет. □

Следствие 2. *Если* $\operatorname{char} K \nmid \deg f$*, то всякий неприводимый многочлен над полем* K *сепарабелен.*

Доказательство. То же самое, что и в предыдущем следствии, так как производная не будет нулевой. □

Следствие 3. *Если поле* K *конечно, то всякий неприводимый многочлен над полем* K *сепарабелен.*

Доказательство. Пусть h — несепарабельный неприводимый многочлен над конечным полем K. Тогда он имеет вид вид

$$h = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_m x^{mp} \quad (a_0, a_1, \ldots, a_m \in K).$$

Так как $K^p = K$, то существуют такие элементы $b_0, \ldots, b_m$, что $b_k^p = a_k$. Тогда в $K[x]$

$$h = (b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^m)^p.$$

Это противоречит неприводимости. □

Упражнение 1. Приведите пример несепарабельного неприводимого многочлена.

Доказательство.

$$x^p - t = (x - \sqrt[p]{t})^p$$

над полем $\mathbb{Z}_p(t)$. □

Теорема 2. *Пусть* $f \in K[x]$ *— многочлен, все неприводимые множители которого сепарабельны.*

Тогда его поле разложения над K *является расширением Галуа.*

Доказательство. Вспомним, как мы доказывали теорему о единственности поля разложения многочлена. Данная теорема доказывается похожим образом.

Именно, пусть поле разложение L многочлена f построено как последовательность простых расширений

$$K = K_0 \subset K_1 \subset K_2 \subset \dots$$

Пусть при переходе от поля K_{i-1} к его расширению K_i мы присоединяем корень неприводимого многочлена f_i.

Пусть у нас имеется некоторый гомоморфизм $\varphi_{i-1} : K_{i-1} \to L$. Тогда, как мы знаем, мы можем продложить его до гомоморфизма

$$\varphi_i : K_i \to L$$

столькими способами, сколько различных корней в поле L есть у многочлена f_i.

Однако у этого многочлена в поле L есть ровно $\deg f_i$ корней, так как он является делителем исходного многочлена f, а L — поле разложения этого многочлена. Значит, на каждому шаге мы можем продолжать гомоморфизм, полученный из предыдущего шага, ровно $\deg f_i$ способами.

Начинаем мы с тождественного гомоморфизма $K \to L$.

Таким образом, всего гомоморфизмом (которые, конечно, будут являться и автоморфизмами) можно постороить ровно

$$\deg f_1 \deg f_2 \dots \deg f_m$$

штук, что равно

$$\dim_K L.$$

Значит, L — раширение Галуа поля K. $\square$

ГРУППА ГАЛУА

Определение 4. Пусть $f(x) \in K[x]$, L — поле разложения f, причем L — расширение Галуа K.

Будем говорить, что группа

$$\operatorname{Gal} L/K = \operatorname{Gal} f$$

— *группа Галуа многочлена* $f(x)$.

Определение 5. Пусть теперь L — расширение Галуа поля K.

Сопоставим подгруппе H группы Галуа $\operatorname{Gal} L/K$ поле L^H:

$$H \mapsto L^H = \{l \in L \mid h(l) = l, \forall h \in H\};$$

и, наоборот, пусть P — поле, $K \subset P \subset L$:

$$P \mapsto G_P = \{g \in \operatorname{Gal} L/K \mid g(p) = p, \forall p \in P\}.$$

Теорема 3 (основная теорема теории Галуа). *Отображения*

$$P \mapsto G_P$$

и

$$H \mapsto L_H$$

взаимно обратны, т. е. имеет место взаимно-однозначное соответствие подполей L, содержащих K, и подгрупп группы Галуа.

Нормальным подгруппам соответствуют подполя, являющиеся расширениями Галуа поля K, и наоборот.

Доказательство. Так как L — расширение Галуа поля K, то L является расширением Галуа любого своего подполя, содержащего K (доказывали в прошлой лекции).

Отсюда следует

$$|G_P| = \dim_P L,$$
$$\dim_{L^H} L = |H|.$$

Очевидно, что

$$L^{G_P} \supseteq P.$$

В то же время из выписанных выше соотношений следует, что

$$\dim_{L^{G_P}} L = |G_P| = \dim_P L.$$

Следовательно,

$$L^{G_P} = P.$$

Аналогично доказывается, что

$$G_{L^H} = H.$$

Поле P является расширением Галуа поля K тогда и только тогда, когда существует ровно

$$\dim_K P$$

автоморфизмов P над K.

Однако любой такой автоморфизм можно продолжить до автоморфизма поля L, причем $\dim_P L$ способами.

Всего у нас получается

$$\dim_K P \cdot \dim_P L = \dim_K L$$

автоморфизмов поля L, действующих на K тождественно и переводящих P в себя.

Но таким образом мы перечислили все автоморфизмы L над K, поэтому P — расширение Галуа тогда и только тогда, когда все преобразования из группы G переводят его в себя.

Так как $P = L^H$, где $H = G_P$, то если

$$gP = P,$$

то

$$H = G_{gP}$$

откуда

$$\begin{aligned} H = \{h \in G \mid \forall x \in gP\ hx = x\} = \\ = \{h \in G \mid \forall y \in P\ h(gy) = gy\} = \\ = \{h \in G \mid \forall y \in P\ g^{-1}hgy = y\} = gHg^{-1}. \end{aligned}$$

Следовательно, подполе P инвариантно относительно всех преобразований из G тогда и только тогда, когда подгруппа H нормальна. $\square$

ВЫРАЗИМОСТЬ В РАДИКАЛАХ

Определение 6. Будем говорить, что элемент α некоторого расширения поля K *выражается в радикалах над* K, если он выражается через элементы поля K при помощи арифметических операций и извлечения корней. Другими словами, если есть цепочка расширений

$$K = K_0 \subset K_1 \subset \ldots \subset K_s,$$

в которой
$$K_i = K_{i-1}(\alpha_i),$$
где $\alpha_i^{n_i} \in K_{i-1}$, и $\alpha \in K_s$.

Будем говорить, что α *разрешим в квадратных радикалах*, если все расширения K_i получаются присоединением квадратного корня из некоторого элемента α_i, то есть все n_i равны 2.

Предложение 7. *Пусть $f(x)$ — неприводимый многочлен над полем K, L — его поле разложения.*

Уравнение $f(x) = 0$ разрешимо в квадратных радикалах тогда и только тогда, когда $\dim_K L = 2^n$.

Доказательство. 1) Пусть уравнение $f(x) = 0$ разрешимо в квадратных радикалах. Тогда сущесвует такая цепочка квадратичных расширений
$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_s,$$
что $L \subset K_s$. Имеем
$$\dim_K L | \dim_K K_s = 2^s.$$

Значит,
$$\dim_K L = 2^l,$$
что и требовалось доказать.

2) Обратно, пусть $\dim_K L = 2^n$. Тогда группа $G = \operatorname{Gal} L/K$ есть 2-группа и, следовательно, разрешима. Рассмотрим какой-либо ее композиционный ряд
$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{e\}.$$
Можно так уплотнить этот ряд, чтобы все его факторы имели порядок два (по индукции и с помощью факторизации по элементам центра). Положим $K_i = L^{G_i}$, получим цепочку квадратичных расширений, доказывающую разрешимость уравнения $f(x) = 0$ в квадратичных радикалах. □

Предложение 8. *Пусть даны отрезки длин $\alpha_1, \alpha_2, \dots, \alpha_n$, требуется построить циркулем и линейкой отрезок длины α.*

Это возможно тогда и только тогда, когда α разрешимо в квадратных радикалах над $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$.

Доказательство. Так как единственное, что мы можем делать, — это строить отрезки длин α_i, проводить прямые, а также окружности радиуса α_i (и последующих полученных длин), то на каждом новом шаге у нас возникает пересечение двух отрезков, либо двух окружностей, либо отрезка и окружности, что всегда выражается не более чем квадратичным расширением поля, порожденного элементами $\alpha_1, \alpha_2, \ldots, \alpha_n$.

В обратную сторону, нам нужно научиться строить сумму, разность, произведение, частное двух отрезков (имея при этом эталонный отрезок длины один, а также строить отрезок длины, равной корню квадратному длины данного отрезка.

Сумма и разность двух отрезков строится очевидным образом.

Произведение и частное отрезков длин a и b строится с помощью пропорции:

$$\frac{a}{b} = \frac{x}{1} \text{ или } \frac{x}{b} = \frac{a}{1}.$$

Корень из отрезка длины a извлекается с помощью пропорции

$$\frac{a}{x} = \frac{x}{1},$$

которую можно построить, взяв отрезок длины a (назовем его AB), отметив в нем точку на расстоянии 1 от вершины A (назовем ее D), далее проведя окружность с центром в середине отрезка AB и радиуса $|AB|/2$ и восстановив перпендикуляр к отрезку AB из точки D. Пересечение окружности и перпендикуляра обозначим через C. Треугольник ABC — прямоугольный с гипотенузой длины a и высотой, делящей гипотенузу на отрезки 1 и $a - 1$.

Тогда катет AC и будет иметь искомую длину. □

Теорема 4 (квадратура круга). *Невозможно построить циркулем и линейкой квадрат, равный по площади данному кругу.*

Доказательство. Если получится построить квадрат, равный по площади кругу радиуса один, то это означает, что получилось построить циркулем и линейкой отрезок длины $\sqrt{\pi}$. Тогда число π должно лежать в каком-то квадратичном расширении рациональных чисел, что неверно, так как π трансцендентно. □

Теорема 5 (удвоение куба). *Невозможно построить циркулем и линейкой куб, объем которого в два раза больше объема данного куба.*

Доказательство. Удвоение куба сводится к построению отрезка длины $\sqrt[3]{2}$. Так как многочлен $x^3 - 2$ неприводим над $\mathbb{Q}$ и его степень не есть степень двойки, то эта задача неразрешима. □

Теорема 6 (трисекция угла). *Нельзя циркулем и линейкой разделить любой угол на три равные части. Например, это невозможно для угла $\pi/3$.*

Доказательство. Трисекция угла, равного φ, сводится к построению отрезка длины $\cos\frac{\varphi}{3}$ по отрезку длины $\cos\varphi$. По известной формуле

$$\cos\varphi = 4\cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3},$$

так что число $\alpha = \cos(\varphi/3)$ является корнем многочлена

$$f = 4x^3 - 3x - \cos\varphi \in K[x],$$

где $K = \mathbb{Q}(\cos\varphi)$.

Если речь идет об универсальном методы трисекции угла, не зависящем от величины угла φ, то мы должны рассматривать $\cos\varphi$ как независимую переменную. Тогда многочлен f неприводим над K, и задача неразрешима по той же причине, что и в предыдущая.

Для конкретных углов (например, для прямого) задача, конечно, может быть разрешима. Критерием разрешимости является наличие у многочлена f корней в поле K.

Если, например, $\varphi = \pi/3$, то $K = \mathbb{Q}$,

$$f = 4x^3 - 3x - 1/2$$

не имеет корней в $\mathbb{Q}$, так что задача неразрешима. □

КРИТЕРИЙ РАЗРЕШИМОСТИ В РАДИКАЛАХ

Лемма 4. *Пусть L — расширение Галуа поля K такое, что группа $G = \operatorname{Gal} L/K$ — циклическая.*

Тогда расширение L над K является простым и порождается одним элементом.

Доказательство. Если группа G циклическая, то у нее есть образующий элемент $g \in G$. Это такой автоморфизм, что все остальные автоморфизмы L над K являются его степенями.

Так как в случае расширения Галуа $L^G = K$, то множество элементов, которые не сдвигаются под действием элемента g, совпадает с полем K.

Если поле L конечно, то L^* порождена некоторым элементом α.

В этом случае ясно, что L над K — простое расширение, получающееся из K присоединением корня α минимального многочлена для α.

Если поле L (а значит, и поле K) бесконечно, то рассмотрим подполя

$$L_1\ (= K), L_2, \ldots, L_{n-1},$$

где

$$L_i = \{x \in L \mid g^i x = x\}.$$

Ни одно из этих подполей не совпадает с L, так как в этом случае автоморфизм g^i, $i = 1, \ldots, n-1$, был бы тождественным.

Значит, существует $\alpha \in L$, не переводящийся в себе ни одной ненулевой степенью автоморфизма g.

Таким образом, аннулирующим многочленом элемента α является многочлен

$$\prod_{i=0}^{n-1}(x - g^i\alpha),$$

имеющий степень ровно n (совпадающую с порядком группы Галуа, то есть со степенью расширения). Значит, L — простое расширение с помощью элемента α. $\square$

Лемма 5. *Пусть поле K содержит n различных корней степени n из 1, и пусть L — расширение Галуа поля K такое, что группа $\operatorname{Gal} L/K$ циклическая.*

Тогда $L = K(\alpha)$, где $\alpha^n \in K$.

Доказательство. Раз группа Галуа расширения — циклическая, то расширение является простым и порождается одним элементом α. Пусть группа порождается элементом g. Тогда все корни минимального многочлена элемента α имеют вид $g^k\alpha$:

$$f(x) = (x - \alpha)(x - g\alpha)\ldots(x - g^{n-1}\alpha) \in K[x].$$

Рассмотрим элемент

$$\alpha_\varepsilon := \alpha + \varepsilon^{-1} g\alpha + \dots + \varepsilon^{1-n} g^{n-1}\alpha.$$

Заметим, что $g(\alpha_\varepsilon) = \varepsilon\alpha_\varepsilon$. Если этот элемент не оказался равным нулю, то он — искомый, так как

$$\begin{aligned}\alpha_\varepsilon^n = (1 \cdot \varepsilon \cdot \varepsilon^2 \cdot \dots \cdot \varepsilon^{n-1})\alpha_\varepsilon^n = \\ = \alpha \cdot \varepsilon\alpha \cdot \dots \cdot \varepsilon^{n-1}\alpha = \alpha \cdot g\alpha \cdot g^2\alpha \cdot \dots \cdot g^{n-1}\alpha \in K[x].\end{aligned}$$

Мало того, если элемент ${\alpha^k}_\varepsilon$, построенный по нкоторой степени элемента α, окажется не равным нулю, то он тоже является искомым.

Пусть теперь все

$$\alpha_\varepsilon, \alpha_\varepsilon^2, \dots$$

оказались равными нулю.

Это означает существование нулевого вектора

$$(\gamma_1, \dots, \gamma_k) = (1, \varepsilon^{-1}, \dots, \varepsilon^{1-k})$$

такого, что

$$\begin{cases} \gamma_1\alpha + \gamma_2 g\alpha + \dots + \gamma_k g^{k-1}\alpha & = 0, \\ \gamma_1\alpha^2 + \gamma_2 g\alpha^2 + \dots + \gamma_k g^{k-1}\alpha^2 & = 0, \\ \dots\dots\dots \\ \gamma_1\alpha^k + \gamma_2 g\alpha^k + \dots + \gamma_k g^{k-1}\alpha^k & = 0, \end{cases}$$

что бывает (благодаря определителю Вандермонда) только при некоторых совпадающих $g^l\alpha$ и $g^m\alpha$, $l \neq m$, $0 \leqslant l, m < k$.

Однако в нашем случае (благодаря выбору α) таких совпадающих элементов нет, что доказывает лемму. $\square$

Теорема 7. *Пусть f — неприводимый многочлен над полем K нулевой характеристики.*

Тогда уравнение $f(x) = 0$ разрешимо в радикалах тогда и только тогда, когда группа $\operatorname{Gal} f$ разрешима.

Доказательство. Если уравнение $f(x)$ разрешимо в радикалах, то для поля L разложения многочлена $f(x)$ существует такая цепочка последовательных расширений, где каждое новое расширение получается из предыдущего добавлением корня какой-то степени из элемента предыдущего расширения.

Пусть мы начинаем с поля K, а заканчиваем полем L, проходя последовательно расширения

$$K = L_0, L_1, \ldots, L_m = L.$$

При каждом расширении от поля L_{i-1} к полю L_i мы добавляем к полю L_{i-1} новый элемент α_i — корень n_i-й степени из $a_i \in L_{i-1}$.

На каждом расширении количество автоморфизмов не превосходит n_i, т.е. равно n_i (так как в результате мы получаем расширение Галуа), т.е. каждое расширение над предыдущим — это расширение Галуа.

Получается, что мы имеем цепочку вложенных полей

$$K = L_0 \subset L_1 \subset \cdots \subset L_m = L,$$

где каждое следующее поля является расширением Галуа над предыдущим полем.

В группе Галуа это соответствует цепочке вложенных подгрупп группы G, где каждая подгруппа нормальна в той, которая следует за ней, и при этом фактор каждой следующей подгруппы по предыдущей — циклический.

Отсюда, конечно, следует, что группа Галуа $G = \operatorname{Gal} f$ разрешима.

Докажем обратное утверждение.

Если группа Галуа $G = \operatorname{Gal} f$ разрешима. Тогда ее коммутант $G' = G^{(1)}$ строго вложен в группу G, а любая подгруппа H, содержащая G' и содержащаяся в G, нормальна в G:

$$\begin{aligned}\forall g \in G \forall h \in H \quad ghg^{-1} = ghg^{-1}h^{-1}h = \\ = [g,h]h \in G'H = H.\end{aligned}$$

Факторгруппа G/G' является конечной абелевой группой, которую мы можем разложить в сумму циклических подгрупп:

$$G/G' = U_1 \oplus \cdots \oplus U_m.$$

Если

$$\pi : G \to G/G'$$

— гомоморфизм факторизации, то группы

$$
\begin{aligned}
G_0 = \pi^{-1}(\{e\}) = G', \quad G_1 = \pi^{-1}(U_1),\\
G_2 = \pi^{-1}(U_1 \oplus U_2), \quad \ldots, G_{m-1} = \pi^{-1}(U_1 \oplus U_2 \oplus \cdots \oplus U_{m-1}),\\
G_m = \pi^{-1}(U_1 \oplus \cdots \oplus U_m) = G
\end{aligned}
$$

образуют вложенную цепь подгрупп, содержащих G' и содержащихся в G, т.е. нормальных в группе G, с циклическими факторами между соседними подгруппами.

Аналогично можно вставить цепочки нормальных друг в друге подгрупп и между коммутантом G' и его коммутантом G'', и т.д.

Таким образом, все группа Галуа G может быть прелставлена как цепочка вложенных подгрупп, где каждая предыдущая подгруппа нормальна в следующей, а соответствующие факторы — циклические.

Следовательно, по основной теореме теории Галуа мы имеем цепочку расширений поля K:

$$K = L_0 \subset L_1 \subset \cdots \subset L_M = L,$$

где каждое L_i — расширение Галуа поля L_{i-1} (степени n_i), при этом группа Галуа L_i над L_{i-1} — циклическая.

Добавим к полю K все корни из единицы всех степеней $n_1, n_2, \ldots, n_M$. Тогда по предыдущей лемме каждое из расширений L_i получается из предыдущего добавлением корня некоторой степени из некоторого элемента L_{i-1}.

Таким образом, все корни многочлена $f(x)$ выражаются в радикалах над K. □

ПОСТРОЕНИЕ НЕРАЗРЕШИМОГО УРАВНЕНИЯ

Лемма 6. *Пусть $f(x)$ — неприводимый многочлен степени n над полем K нулевой характеристики. Тогда*

$$\operatorname{Gal} f \subset \mathbf{S}_n.$$

Доказательство. Поле разложения многочлена f порождается корнями этого многочлена, которых у многочлена f в поле разложения ровно n штук.

При этом каждый автоморфизм поля разложения над K индуцирует перестановку корней (разные автоморфизмы индуцируют разные перестановки).

Значит, каждому автоморфизму из $\mathrm{Gal}\, f$ сответствует некоторая подстановка из $\mathbf{S}_n$, т.е.

$$\mathrm{Gal}\, f \subset \mathbf{S}_n.$$

$\square$

Следствие 4. *Любое уравнение вида*

$$f(x) = 0,$$

где $f(x)$ — многочлен степени, меньшей пяти, разрешимо в радикалах.

Лемма 7. *Пусть p — простое число, G — подгруппа в $\mathbf{S}_p$, причем в группе G есть транспозиция и элемент порядка p. Тогда $G = S_p$.*

Доказательство. Пусть цикл — это

$$(i_1\, i_2\, \ldots i_p),$$

транспозиция —

$$(i_1\, i_l).$$

Если $l = 2$ или $l = p - 1$, то доказательство следует из того, что подстановки

$$(1\,2) \text{ и } (1\,2\, \ldots\, n-1\, n)$$

порождают всю группу $\mathbf{S}_n$.

Если i_l находится на расстоянии от i_1, большем одного (в ту или другую сторону по циклу), то нужно возвести цикл $(i_1\, i_2\, \ldots i_p)$, в подходящую степень, чтобы в этой степени i_1 и i_l оказались рядом. Понятно, что это возможно из-за простоты p. $\square$

Лемма 8. *Пусть $f(x)$ — неприводимый многочлен простой степени p над $\mathbb{Q}$, причем ровно два его корня невещественны.*

Тогда $\mathrm{Gal}\, f = \mathbf{S}_p$.

Как следствие, уравнение $f(x) = 0$ неразрешимо в радикалах при $p \geqslant 5$.

Доказательство. Мы знаем, что $|\operatorname{Gal} f|$ делится на p (так как степень расширения делится на p, а p — простое число). Значит, в $\operatorname{Gal} f$ содержится длинный цикл (как единственный элемент порядка p в группе $\mathbf{S}_p$).

Транспозиция там также содержится, так как комплексное сопряжение является автоморфизмом, сохраняющим этот многочлен, а при этом меняющим местами ровно два (невещественных) корня.

Оставшееся доказательство следует из предыдущей леммы. $\square$

Два следующих предложения доказывались еще на первом курсе. Мы напомним только формулировки, не повторяя доказательства.

Предложение 9 (лемма Гаусса). *Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.*

Предложение 10 (критерий Эйзенштейна). *Пусть $f(x) \in \mathbb{Z}[x]$ — многочлен со старшим коэффициентом 1, все остальные его коэффициенты делятся на p, причем свободный член не делится на p^2.*

Тогда $f(x)$ неприводим над $\mathbb{Z}$.

Теорема 8. *Пусть $m; n_1, \ldots, n_{k-2}$ — различные целые четные числа, причем*

$$m > 0, \quad n_1 < n_2 < \ldots < n_{k-2}, \quad k > 3 \text{ — нечетно.}$$

Определим

$$f(x) = (x^2 + m)(x - n_1) \cdot \ldots \cdot (x - n_{k-2}) - 2.$$

Тогда $f(x)$ неприводим над $\mathbb{Q}$, и можно подобрать m так, чтобы он имел ровно 2 невещественных корня.

Таким образом, для любого простого $p \geqslant 5$ существует многочлен с рациональными коэффициентами, неразрешимый в радикалах над $\mathbb{Q}$.

Доказательство. Неприводимость любого такого многочлена следует из критерия Эйзенштейна (все коэффициенты четны, а последний точно не кратен четырем).

Нам осталось подобрать m так, чтобы у $f(x)$ было ровно два невещественных корня.

Докажем сначала, что у данного многочлена (независимо от m) есть по крайней мере $m - 2$ вещественных корня.

Действительно, рассмотрим интервалы

$$(n_1, n_1+1); \quad (n_2-1; n_2); \quad (n_3; n_3+1); \quad (n_4-1; n_4); \ldots$$

Мы знаем, что

$$f(n_1) = f(n_2) = \cdots = f(n_{k-2}) = -2 < 0.$$

При этом

$$f(n_1+1) = f(m_1) = (m_1^2+m)\cdot 1\cdot (m_1-n_2)\ldots(m_1-n_{k-2}) - 2$$

— произведение четного числа отрицательных целых чисел (из которых все отличны от нуля и все, кроме одного, по модулю строго больше двух) и числа m_1^2+m, строго большего двух, из которого вычитается двойка.

Таким образом, ясно, что

$$f(n_1+1) > 0.$$

Точно так же показывается, что

$$f(n_2-1) > 0; \quad f(n_3+1) > 0; \ldots$$

Значит, на каждом из рассматриваемых $k-2$ интервалах в концах интервалов значения имеют разные знаки.

Следовательно, у многочлена $f(x)$ не менее $k-2$ различных корней.

Теперь нам надо показать, что m можно подобрать таким образом, чтобы у $f(x)$ не было k различных корней, либо $k-2$ различных и одного кратного корня.

Заметим, что из наличия у многочлена $f(x)$ степени k либо k различных корней, либо $k-2$ различных корней и одного кратного следует, что у его производной (степени $k-1$) ровно $k-1$ различных действительных корней. Соответственно, у его $k-2$-й производной (по индукции) должно быть ровно два различных корня. Значит, если у $k-2$-й производной нет корней, то многочлен $f(x)$ является для нас искомым.

При этом $k-2$-я производная многочлена $f(x)$ зависит только от коэффициентах при его степенях $k-2, k-1, k$:

$$f(x)^{(k-2)} = \\ = (x^k - (n_1+n_2+\cdots+n_{k-2})x^{k-1} + (m + \sum_{i\neq j} n_i n_j)x^{k-2})^{(k-2)} = \\ = ax^2 + bx + mc + d,$$

где a, b, c, d — фиксированные целые числа (их легко вычислить), не зависящие от m, $a, c > 0$.

Ясно, что можно легко подобрать положительное число m так, чтобы у данного квадартного трехчлена не было корней.

Теорема доказана. $\square$

Упражнение 2 **. Пусть $f(x) = \sum\limits_{m=0}^{m=n} x^m/m!$. Докажите, что

$$\operatorname{Gal} f = \begin{cases} A_n, & n \equiv 0 \pmod 4, \\ S_n, & \text{иначе.} \end{cases}$$