ЛЕКЦИЯ 23

КРИТЕРИЙ РАЗРЕШИМОСТИ В РАДИКАЛАХ

НЕРАЗРЕШИМЫЕ УРАВНЕНИЯ

КРИТЕРИЙ РАЗРЕШИМОСТИ В РАДИКАЛАХ

Лемма 1. *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. □

Лемма 2. *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 $g^k\alpha$:

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

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

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

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. □

Теорема 1. *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:

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

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

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

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

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

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.

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

□

Следствие 1. *Любое уравнение вида*

$$f(x) = 0,$$

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

Лемма 4. *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. □

Лемма 5. *Пусть $f(x)$ — неприводимый многочлен простой степени p над $\mathbb{Q}$, причем ровно два его корня невещественны.*

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

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. □

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

Предложение 1 (лемма Гаусса). *Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.*

Предложение 2 (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 2. *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

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

— 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

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

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 $k - 2, k - 1, k$:

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

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. □

Упражнение 1 **. Пусть $f(x) = \sum_{m=0}^{m=n} x^m/m!$. Докажите, что

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