ЛЕКЦИЯ 22

СЕПАРАБЕЛЬНЫЕ МНОГОЧЛЕНЫ

ГРУППА ГАЛУА

ВЫРАЗИМОСТЬ В РАДИКАЛАХ

НЕРАЗРЕШИМЫЕ ЗАДАЧИ НА ПОСТРОЕНИЕ

СЕПАРАБЕЛЬНЫЕ МНОГОЧЛЕНЫ

Определение 1. Многочлен $f \in K[x]$ называется *сепарабельным*, если он не имеет кратных корней ни в одном расширении поля K.

Лемма 1. *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. $\square$

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 1. *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. □

ГРУППА ГАЛУА

Определение 2. 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 3. 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 2 (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 4. 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 1. *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 2. *Пусть даны отрезки длин $\alpha_1, \alpha_2, \ldots, \alpha_n$, требуется построить циркулем и линейкой отрезок длины α.*

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

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 3 (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 4 (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 5 (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. □