# Лекция №5.

Теорема: Основная теорема Теории Галуа

$K:L$ - расширение Галуа, $Gal(K:L) = G$; есть биекция между подполями $L \subset M \subset K$ и подгруппами $H \subset G$

$H \rightsquigarrow M = \varphi(H) = \{x \in K : \sigma x = x \quad \forall \sigma \in H\}$

$M \rightsquigarrow H = \psi(M) = \{\sigma \in G : \sigma x = x \quad \forall x \in M\}$

$\deg(M:L) = \frac{|G|}{|H|}$, $\deg K:M = |H|$.

$M$ нормально $\Leftrightarrow$ $H$ нормально

Лемма: если $x \in K$ инвариантно относительно $\forall g \in G$, то $x \in L$

Д-во теоремы: $H \xrightarrow{\varphi} M = K^H \xrightarrow{\psi} H' = \{\sigma : \sigma x = x \quad \forall x \in M\}$

Надо проверить $H' = H$

Очевидно $H' \supset H$. Пусть $H' \supsetneq H$. Возьмем какой-нибудь примитивный элемент $\theta$

$\theta : K = L(\theta) = M(\theta)$

Многочлен $P(x) = \prod_{h \in H} (x - h(\theta)) \in K[x]$ $\in M[x]$

Коэффициенты $P(x)$ - это симметричные функции корней, т.е. $\{h(\theta)\}$.

Под действием автоморфизмов $h \in H$ все симметричные функции неподвижны $\Rightarrow$

$\Rightarrow$ все коэффициенты $P(x)$ лежат в $M$

Итак, $\theta$ является корнем многочлена $P \in M[x]$

$\deg P = |H| \Rightarrow \deg[K:M] \leq |H|$

Но по предположению $Aut(K:M) = H'$

$\deg[K:M] = |H'|$

Пример: $Gal = S_n$ - симметрическая группа - перестановки $n$ букв.

$L$
$\mathbb{C}(u_1, \ldots, u_n)$ - поле рацион. функций от $n$ переменных.

Рассмотрим уравнение $P(x) = x^n + u_1 x^{n-1} + u_2 x^{n-2} + \ldots + u_n = 0$.

$K:L$ - минимальное поле разложения $P(x)$.

Утв: $Gal(K:L) = S_n$

Если $x_1, \dots, x_n$ - корни $P$, то $Gal$ действует просто всеми перестановками корней.

Д-во: $M = \mathbb{C}(x_1, \dots, x_n)$

формально свободные переменные

на $M$ действует $\mathfrak{S}_n$, перест. $x_i$

$M^{\mathfrak{S}_n} = N = \mathbb{C}(\sigma_1, \dots, \sigma_n)$, где $\sigma_i$ - $i$-я элемент. симметр. функция

$Gal[M:N] = \mathfrak{S}_n$. (например потому, что $\deg[M:N] = n!$)

$$\begin{array}{ccc} M = \mathbb{C}(x_1, \dots, x_n) & \supset & N = \mathbb{C}(\sigma_1, \dots, \sigma_n) \\ \downarrow & & \downarrow \pm \quad \uparrow \pm \\ K = \mathbb{C}(\mathfrak{x}_1, \dots, \mathfrak{x}_n) & \underset{\mathfrak{S}_n}{\supset} & L = \mathbb{C}(u_1, \dots, u_n) \end{array}$$

Утв: Решение уравнений в радикалах.

Пусть $L$ содержит $\sqrt[n]{1}$, $K = L(\sqrt[n]{a})$. Тогда $Gal(K:L)$ циклическая

Д-во: если $\theta = \sqrt[n]{1}$, то $K = L(\theta)$, $\forall g \in G$

определяется $\theta \rightsquigarrow g(\theta) = \theta \sqrt[n]{1}$

Поэтому $Gal(K:L)$ - подгруппа $\{\sqrt[n]{1}\}$, т.е. циклическая

Обратное утверждение: $L \supset \{\sqrt[n]{1}\}$, $K:L$ - расширение с $Gal = \mathbb{Z}/n\mathbb{Z}$

$\xi$ - примитивный, образующая $\sigma$

Тогда $K = L(\sqrt[n]{a})$, $a \in L$

Д-во: $\alpha \in K$ резольвента Лагранжа $\alpha + \xi\sigma\alpha + \dots + \xi^{n-1}\sigma^{n-1}\alpha = R(\alpha)$

$\sigma R(\alpha) = \xi R(\alpha)$

$\sigma R^2(\alpha) = \xi^2 R^2(\alpha)$

$\sigma R^n(\alpha) = R^n(\alpha)$.

Тк Лемма $R^n(\alpha) \in L$

$a = R^n(\alpha)$, $\sqrt[n]{a} = R(\alpha)$.

Надо только проследить чтобы $R(\alpha) \neq 0$

Лемма: $\exists \alpha : R(\alpha) \neq 0$ о линейной независимости мультипликативных гомоморфизмов.

какая-нибудь группа $H$ $(= K^*)$

гомоморфизмы $H \xrightarrow{\varphi_i} K^*$

$\gamma_0 = Id,\ \gamma_1 = \sigma,\ \gamma_2 = \sigma^2, \dots \gamma_{n-1} = \sigma^{n-1}$

Тогда $\gamma_i$ линейно независимы, т.е. если $c_0\gamma_0 + c_1\gamma_1 + \dots + c_n\gamma_n = 0$, на группе $H$, то $c_i \equiv 0$ $\in k$

Д-во: индукция по $n$: $n = 1$.

шаг: $c_0\gamma_0(h) + \dots + c_{n-1}\gamma_{n-1}(h) = 0 \quad h \rightsquigarrow h \circ f$

$c_0\gamma_0(hf) + \dots + c_{n-1}\gamma_{n-1}(hf) \equiv 0$

$c_0\gamma_0(h)\gamma_0(f) + \dots + c_{n-1}\gamma_{n-1}(h)\gamma_{n-1}(f) \equiv 0$

$c_0\gamma_0(f)\gamma_0(h) + \dots + c_{n-1}\gamma_{n-1}(f)\gamma_{n-1}(h)$

старая $\cdot \gamma_0(f)$ - новая =

$= \boxed{c_1\gamma_0(f) - c_1\gamma_1(f)}\gamma_1(h)$

$+ \dots$

$+ \boxed{c_{n-1}\gamma_0(f) - c_{n-1}\gamma_{n-1}(f)}\gamma_{n-1}(h) = 0.$

По предположению индукции $c_i(\gamma_0(f) - \gamma_i(f)) \equiv 0$

т.к. $\gamma_0 \not\equiv \gamma_i$, $c_i \equiv 0$.

Вывод для решений уравнений в радикалах

Пусть $L \supset \{\sqrt[n]{1}\}$ $\quad K \supset L$

1) $K$ получается последовательным присоединением $\sqrt[n]{a}$

$K = L[x]/p(x)$

$P$ - разрешимо в радикалах, $K$ - радикально

$L \rightsquigarrow L(\sqrt[n]{a}) = K_1 \rightsquigarrow K_1(\sqrt[m]{b}) = K_2 \rightsquigarrow \dots K_\ell = K$

2) $Gal(K:L)$ имеет цепочку подгрупп разрешима

31/56??

$G \supset G_1 \supset G_2 \supset G_3 \supset \dots$

т.что $G_{i+1}$ нормальна в $G_i$ и $G_i / G_{i+1}$ циклическая

Пример: $S_7 \supset A_7$ - знакопеременная

$A_7$ неразрешима

Д-во: если $A_7$ - разрешима, то $\exists$ гомоморфизм $A_7 \to \mathbb{Z}/k\mathbb{Z}$

$A_7 \ni (123) = a$

$\ni (14567) = b$

$ab = (4315672)$

$a^3 = 1$

$b^5 = 1$

$(ab)^7 = 1$

Образы $a, b, ab,$

$\mathbb{Z}/k\mathbb{Z}$ , $\bar{a}, \bar{b}, \overline{ab}$

$3\bar{a} = 0 \Rightarrow 5\bar{b} = 7\bar{a} + 7\bar{b}$; $\bar{a} = \bar{b} = 0$.

Если бы у $A_7$ была такая башня, то у её подгруппы $H = \langle a, b \rangle$ тоже такая башня

$H \to \mathbb{Z}/k\mathbb{Z}$

$a, b \quad \bar{a}, \bar{b}$