## Лекция №4

### 1. Нормальные расширение полей $K:L$. Определение:

Если какой-нибудь многочлен (неприводим) $P(x) \in L[x]$ имеет корень в $K$ (т.е. линейный множитель), то он имеет все корни в $K$ (т.е. разлагается на линейные множители)

Контрпример: $L = \mathbb{Q}$, $K = \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[t]/_{t^3-2}$ (остальные комплексные корни здесь не лежат)

Пример: $L = \mathbb{R}$, $K = \mathbb{C}$

$\forall$ квадратное расширение будет нормальным

Пример: $L = \mathbb{Q}(\sqrt[3]{1})$, $K = L(\sqrt[3]{2})$

Пример: Неприводимый над $\mathbb{Q}$, но имеющий 3 корня:

$$x(x+1)(x+2) \approx x^3 + 3x^2 + 2x + \frac{17}{8} = p$$

$\mathbb{Q}[x]/p(x)$ - нормальное расширение $\mathbb{Q}$

### Теория Галуа

Теорема: Если $K$ - минимальное поле разложения какого-то многочлена $P(x) \in L[x]$, то $K$ - нормально.

Д-во: Возьмем многочлен $f(x) \in L[x]$, который в $K$ имеет корень $\alpha_1$, но не имеет корня $\alpha_2$.

От противного

Пусть $\beta_1, \dots, \beta_n$ - все корни $P(x)$ в $K$.

Тогда $L(\alpha_1) \overset{iso}{\cong} L(\alpha_2)$

$\wr\wr$ $L[x]/(f)$

$\longrightarrow$ продолжим до изоморфизма $L(\alpha_1, \beta_1, \dots \beta_n) \simeq L(\alpha_2, \beta_1, \dots \beta_n)$, $K \wedge$

т.к. это минимальные поля разложения $P(x)$ над $L(\alpha_1) \simeq L(\alpha_2)$

(по Лемме: минимальные поля разложения $P(x)$ изоморфны)

Получили, что $K \cong$ (чему-то что $> K$)

$\Downarrow$

Противоречие

$\boxtimes$

... Определение:

Элемент $\theta \in K:L$ называется сепарабельным (отделимым), если его минимальный многочлен над $L$ не имеет кратных корней

$\underbrace{1, \theta, \dots, \theta^n}_{\text{все линейно независимы}}; \Rightarrow \theta^n + a_{n-1}\theta^{n-1} + \dots$ – минимальный

а $\theta^{n+1} = b_1\theta^n + \dots$ -лин. зависим

Контрпример: $L = \mathbb{F}_p(t) = \left\{\frac{P(t)}{Q(t)}\right\}$ $K = L(\sqrt[p]{t})$, $\theta = \sqrt[p]{t}$,

Минимальный многочлен: $x^p - t$

$\theta^p - t = 0$ $\Rightarrow$ $\theta$ не сепарабельно

$\frac{\partial}{\partial x}(x^p - t) = 0$ – все корни кратные

Пример: $\operatorname{char} L = 0 \Rightarrow \forall \theta$ сепарабельное

$\# K < \infty \Rightarrow \forall \theta$ сепарабельный

Определение $K:L$ сепарабельное расширение, если $\forall \theta \in K$ сепарабельный.

Теорема: пусть $K:L$ - сепарабельное расширение (конечное); тогда $\exists \theta \in K$, т.что $K = L(\theta)$. Т.е. если $P(x)$ - минимальный многочлен $\theta$, то $K = L[x]/(P)$ (Теорема о примитивном элементе $\rightsquigarrow \theta$)

Д-во: 1) $L$ конечно $\simeq \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$ - все известно и хорошо

2) $L$ - бесконечно ; $K = L(\alpha_1, \dots, \alpha_n)$ по индукции достаточно рассмотреть случай $\alpha_1, \alpha_2$

$\alpha, \beta$ : $K = L(\alpha, \beta)$.

Будем искать $\theta$ в виде $\alpha + c\beta$, где $c \in L$.

Пусть $\alpha = \alpha_1, \alpha_2, \dots \alpha_n$ - все корни минимального многочлена $\alpha$ $(f(\alpha) = 0)$

$\beta = \beta_1, \beta_2, \dots \beta_s$ - все корни минимального $\beta$ $(g(\beta) = 0)$

Т.к. $L$ - бесконечно, можно выбрать $c$ т. что $\alpha_i + c\beta_i \neq \alpha_1 + c\beta_1 = \alpha + c\beta = \theta$

$f(\alpha) = 0 = g(\beta)$;

$f(\alpha) = f(\theta - c\beta)$

Рассмотрим уравнение $f(\theta - c\beta) - f(\alpha) = 0 = g(\beta)$; $L(\theta)[x] \ni g(x)$ и $f(\theta - cx) \to$

↳ имеют общий корень $\beta$ и не имеют других общих корней

$$\Downarrow$$

$$\text{НОД}\big(f(x - c\beta),\ g(x)\big) = x - \beta$$

$\Rightarrow$ коэффициент $(x-\beta)$ выражается через $L(\theta) \Rightarrow$

$\Rightarrow \beta \in L(\theta) \Rightarrow \alpha \in L(\theta)$ ▨

3 **Определение** $K:L$ – конечное, нормальное, сепарабельное расширение называется расширением Галуа (Galois)

**Утверждение:** $\#\mathrm{Aut}(K:L) = \deg[K:L]$

$\sigma: K \circlearrowleft \qquad \sigma(x+y) = \sigma(x) + \sigma(y)$

$\qquad\qquad\quad \sigma(xy) = \sigma(x)\sigma(y)$

Д-во: возьмем примитивной $\theta$: $K = L(\theta) = L[x]/P(x)$

Тогда $\sigma(\theta)$ обязан быть корнем $P \Rightarrow$

$\#\mathrm{Aut} \le \deg P$

$\sigma \to \sigma(\theta)$

$K$ - минимальное поле разложения $P$

$L(\theta) \simeq L(\theta)$

## Основная теорема теории Галуа

Пусть $K:L$ - расширение Галуа с группой Галуа $G$

Тогда имея подполе $L \subset M \subset K$, можно сопоставить ему подгруппу $H \subset G \qquad H = \{g \in G : gm = m, \forall m \in M\}$

И наоборот, имея подгруппу $H \subset G$, можно сопоставить ей подполе $L \subset M \subset K$, $M = \{x \in K,$ т.ч. $hx = x \ \forall h \in H\} = K^H$ - поле инвариантов

тогда

$M \xrightarrow{\Psi} H$

$H \xrightarrow{\varphi} M$

1) $\Psi$ и $\varphi$ - взаимнообратные биекции

2) $\deg[M:L] = \dfrac{\#G}{\#H}$

$\deg [K : M] = \# H$

3) $M : L$ нормально $\Leftrightarrow$ $H$ нормально в $G$.

{ Пример: $\mathbb{Q}(\sqrt[17]{1}) \supset K_8 \supset K_4 \supset K_2 \supset \mathbb{Q}$

$Gal(\mathbb{Q}(\sqrt[17]{1})) \simeq \mathbb{Z}/16\mathbb{Z}$

$\mathbb{Z}_2 \subset \mathbb{Z}_4 \subset \mathbb{Z}_8 \subset \mathbb{Z}_{16}$

<u>Д-во теоремы</u>: надо проверить, что $H \xrightarrow{\varphi} M \xrightarrow{\psi} H'$ $\psi\varphi = id$

Могло бы быть $H' \supsetneq H$

<u>Лемма</u>: $K^G = L$, $\alpha \in K$, : $\sigma\alpha = \alpha$, $\forall \sigma : K \circlearrowleft$

иначе возьмем минимальный многочлен $\alpha$, $P(\alpha) = 0$. Пусть $\beta$ - другой корень

$L(\alpha) \simeq L(\beta)$ - этот изоморфизм продолжается до изоморфизма

$\cap$ $\cap$ $K$ - нормально

$K \simeq^{m.к.} K$

минимального поля разложения многочлена $Q(\theta) = 0$

$Q \in L(\alpha)[x]$, $Q \in L(\beta)[x]$.

Т.е. мы построили автоморфизм поля $K$, который $\alpha \longrightarrow \beta \neq \alpha$ - противоречие $\blacksquare$

Пусть $H' \supsetneq H$