Лекция 5 | Поле разложения и алгебраическое замыкание поля.

Главный пример расширения с прошлого раза:

$$\mathbb{K} \subset \mathbb{K}(\alpha) \subset \mathbb{F}, \quad \alpha \text{ - алгебраическое}$$

и тогда $\mathbb{K}(\alpha) \simeq \mathbb{K}[x]/(\mu_\alpha(x))$

↑ неприводимый мн-н.

Пусть теперь наоборот мы имеем мн-н $f(x) \in \mathbb{K}[x]$ и хотим построить поле $\mathbb{F}$, в котором $f(x)$ раскладывается на линейные мн-ны.

<u>Пример 1</u> $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ $\quad f(x) = x^2 - 2$

$\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ $\quad f(x) = x^3 - 2$

<u>Пример 2</u> $\mathbb{F}_p$, $x^p - x - a$ или не имеет корень
или α- корень $\Rightarrow$ $\alpha+1$ -корень, $\alpha+2, \dots, \alpha+p-1$ — всё корни.

<u>Опр.</u> $\mathbb{F}/\mathbb{K}$ наз-ся полем разложения мн-на $f(x) \in \mathbb{K}[x]$,
если $f(x) = \prod_{i=1}^{\deg f}(x - \alpha_i)$ и $\mathbb{F} = \mathbb{K}(\alpha_1, \dots, \alpha_{\deg f})$ - миним. подполе, порожд. корнями.

<u>Теор.</u> Поле разложения существует.

<u>Д-во</u> Последовательно присоединяем корни

$$\mathbb{K} \subset \mathbb{K}(\alpha_1) \subset \mathbb{K}(\alpha_1, \alpha_2) \subset \dots$$

каждое присоединение это операция $\mathbb{L} \rightsquigarrow \mathbb{L}[x]/\mu_\alpha(x)$

где $\mu_\alpha(x)$ -неприводимый сомножитель $f(x)$ в $\mathbb{L}$, содержащий $(x-\alpha)$. □

Теперь попытаемся объяснить, что поле разложения единственно, с точностью до из-зма. Для этого надо подробнее проследить за процедурой присоединения корня.

<u>Лемма</u>

$$\begin{tikzcd} \mathbb{F} = \mathbb{K}[x]/\mu_\alpha(x) \arrow[r, dotted, "?"] & \mathbb{L} \\ \mathbb{K} \arrow[u, hook] \arrow[ur] & \end{tikzcd}$$

имеет место биекция мн-в:

$\{\mathbb{K}$-линейных гомоморфизмов $\psi: \mathbb{K}[x]/\mu_\alpha(x) \longrightarrow \mathbb{L}\}$

$\updownarrow$

$\{$Мн-во корней мн-на $\mu_\alpha(x)\}$.

В частности их не больше, чем $\deg \mu_\alpha(x)$.

Пусть теперь $\mathbb{L}$ – поле, в котором $f(x)$ раскл. на линейные мн-мн,

$$\begin{tikzcd} \mathbb{F} = \mathbb{K}(\alpha_1,\dots,\alpha_n) \arrow[drrrr, "\varphi_n"] & \supset \mathbb{K}(\alpha_1,\dots,\alpha_{n-1}) \supset \dots & & \supset \mathbb{K}(\alpha_1) \arrow[dr, "\varphi_1"] & \supset \mathbb{K} \arrow[d, "\varphi_0"] \\ & & & & \mathbb{L} \end{tikzcd}$$

Поле разложения мн-на $f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$.

Каждое из φ_i существует и его можно выбрать не более, чем $n!$ способами.

<u>Сл-ие</u> Поле разложения единственно:

$$\begin{tikzcd} \mathbb{F}_1 \arrow[r, shift right, "\psi"'] & \mathbb{F}_2 \arrow[l, shift right, "\varphi"'] \\ \mathbb{K} \arrow[u] \arrow[ur] \end{tikzcd}$$

$[\mathbb{F}_1 : \mathbb{K}]$, $[\mathbb{F}_2 : \mathbb{K}] < \infty$.

φ, ψ – вложения, т.к. это 2-змы полей.

$\Rightarrow \varphi, \psi$ – из-змы, т.к. $\mathbb{F}_1/_{\mathbb{K}}$, $\mathbb{F}_2/_{\mathbb{K}}$ – конечномерны.

<u>Сл-ие</u> Группа $Gal(\mathbb{F}/_{\mathbb{K}}) := Aut_{\mathbb{K}}(\mathbb{F})$.

и её порядок не превосходит степень расширения $[\mathbb{F} : \mathbb{K}]$.

Если совпадает, то расширение наз-ся расширением Галуа.

<u>Пример.</u> $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ $\quad f(x) = x^2 - 2$, $\sqrt{2} \to \pm\sqrt{2}$

$\mathbb{C} \simeq \mathbb{R}(i)/_{\mathbb{R}} \simeq \mathbb{R}[x]/(x^2+1)$. $\quad \lambda \to \overline{\lambda}$.

$\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q}(\omega) \supset \mathbb{Q}$. $\quad \omega \to \omega, \overline{\omega}$; $\sqrt[3]{2} \to \omega\sqrt[3]{2}, \overline{\omega}\sqrt[3]{2}, \sqrt[3]{2}$.

$\# Aut(\ ) = 6$. $\Rightarrow Aut(\ ) = S_3$.

группа не абелева и транзитивно действует на корнях.

<u>Пример</u> Если $\operatorname{char} \mathbb{K} = p$, то имеем

$f(x) = x^p - x - a$, если α - корень, то $\mathbb{F}_p(\alpha) = \mathbb{F}_p[x]/_{x^p - x - a}$

↑ неприводим $\qquad \alpha \to \alpha+1, \alpha+2, \vdots$ $\qquad$ ↑ Тоже расширение Галуа

<u>Пример.</u> $\mathbb{K} = \mathbb{F}_p(t)$ $\quad f(x) = x^p - t$ - не имеет корней

$\cap$

$\mathbb{F}_p(\sqrt[p]{t})$, но $x^p - t = (x - \sqrt[p]{t})^p$. Корень 1, но с большой кратностью.

Поле $\overline{\mathbb{K}}$ называется алгебраическим замыканием поля $\mathbb{K}$, если $\overline{\mathbb{K}}$ - алгебраично над $\mathbb{K}$ и алгебраически замкнуто, т.е. любой мн-н $f(x) \in \overline{\mathbb{K}}[x]$ имеет корень в $\overline{\mathbb{K}}$.

Пример. $\mathbb{C}$ — алгебраически замкнуто.

Теор. Если $\mathbb{L} \supset \mathbb{K}$, $\mathbb{L}$ — алгебраически замкнуто, то мн-во $\mathbb{F} \subset \mathbb{L}$ алгебраичных над $\mathbb{K}$ эл-ов — является алгебр. замыканием $\mathbb{K}$.

Д-во: Заметим, что $\mathbb{F}$ — подполе, т.к. сумма, умнож. алгебр. эл-ов алгебраично (взятие обратного для поля).

Пусть $f(x) \in \mathbb{F}[x]$, его коэф. алгебраичны над $\mathbb{K}$.

$\exists$ конечное расширение $\mathbb{F}_0/\mathbb{K}$, т.ч. $f \in \mathbb{F}_0[x]$

тогда $\exists$ корень $\alpha \in \tilde{\mathbb{F}}/\mathbb{F}_0$ — конечное расширение подполя $\mathbb{F}_0$.

$\Rightarrow$ α — алгебраичен над $\mathbb{K}$, т.к. $\alpha \in \mathbb{K}(a_0, a_1, \ldots, a_n; \alpha) \subset \mathbb{L}$

Переформулировка

Если $\mathbb{F}/\mathbb{K}$ — алгебраично и $\forall f(x) \in \mathbb{K}[x]$ раскладывается на линейные мн-ли в $\mathbb{F}[x]$ $\Rightarrow$ $\mathbb{F} = \overline{\mathbb{K}}$

Теор. $\forall$ поля $\mathbb{K}$ $\exists$ алгебр. замыкание $\overline{\mathbb{K}}/\mathbb{K}$.

Д-во: Рассмотрим все (неприводимые) мн-ны $f(x) \in \mathbb{K}[x]$, обозначим соотв. мн-во за Ω.

Рассмотрим кольцо $A := \mathbb{K}[x_f \mid f \in \Omega]$ — кольцо перем. от бесконечного числа образующих.

Рассмотрим идеал I, порождённый $\{f(x_f) \mid f \in \Omega\}$.

Лемма $I \subsetneq A$.

Д-во: если $I = A \Rightarrow 1 = \sum_{k=1}^{N} g_k f_k(x_{f_k})$ ← сумма конечная. $g_k \in A$.

$\Rightarrow I_0 \subset A_0 = \mathbb{K}[x_{f_k} \mid k = 1, \ldots N]$

Р-м мн-н $g(x) := \prod_{f \in \Sigma_0} f(x)$ и поле разложения $\mathbb{L}$ мн-на $g(x)$.

Тогда имеем г-зм $\mathbb{K}$-алгебр $A_0 \xrightarrow{\pi} \mathbb{L}$

$x_f \longrightarrow a_f$ — корень мн-на $g(x)$ в $\mathbb{L}$.

$I_0 \subset \ker \pi \Rightarrow A_0/I_0 \xrightarrow{\pi} \mathbb{L}$, однако справа поле $\Rightarrow 1 \neq 0$.

$\Rightarrow 1 \notin I_0 \subset A_0$.

$\square$.

Рассмотрим максимальный идеал $\underset{I}{\underset{\cup}{J}} \subset A$.

Имеем $\mathbb{K}_i := A/J$ — алгебраич. расширение поля $\mathbb{K}$.

Также построим $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \dots$

и назовём $\overline{\mathbb{K}} := \bigcup_s \mathbb{K}_s$.

<u>Замечание</u> $\mathbb{K}_i / \mathbb{K}$ — алгебраичн, т.к. композиция алгебр. расширений — алгебраич.

Кроме того, любой неприв. мн-н $f(x) \in \mathbb{K}[x]$ расклад. на лин. мн-ны уже в $\mathbb{K}_{\deg f}$.