

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 $\mathbb{K}(\alpha) \cong \mathbb{K}[x] / (\mu_\alpha(x))$
 ↑ неприводимый ми-и.

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

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

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

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

Опр. \mathbb{F}/\mathbb{K} наз-ся полем разложения ми-и 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. поле, порожд. корнями.

Теор. Поле разложения существует.

До-во Последовательно присоединяем корни

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

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

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

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

корней. имеет место биекция ми-и-в:

$$\mathbb{F} = \mathbb{K}[x] / \mu_\alpha(x) \xrightarrow{?} \mathbb{L}$$

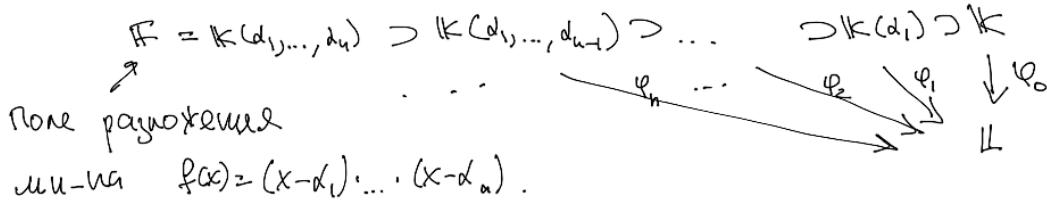
$$\{ \text{K-линейных гомоморфизмов } \psi: \mathbb{K}[x] / \mu_\alpha(x) \rightarrow \mathbb{L} \}$$

$\{ \text{ми-и-в корней ми-и } \mu_\alpha(x) \}$.

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

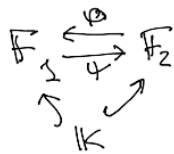
Лемма

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



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

Сл-ие Поле разложения существует:



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

φ, ψ - вложения, т.к. 2-зми поля.

$\Rightarrow \varphi, \psi$ - м-зми, т.к. $\mathbb{F}_1/\mathbb{K}, \mathbb{F}_2/\mathbb{K}$ - конечны.

Кл-ие Группа $\text{Gal}(\mathbb{F}/\mathbb{K}) := \text{Aut}_{\mathbb{K}}(\mathbb{F})$.

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

Если совпадает, то расширение наз-ся расширением Галуа.

Пример. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ $f(x) = x^2 - 2$, $\sqrt{2} \rightarrow \pm\sqrt{2}$

$\mathbb{C} \simeq \mathbb{R}(i)/\mathbb{R} \simeq \mathbb{R}[x]/(x^2+1)$. $\lambda \rightarrow \bar{\lambda}$.

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

$\omega \rightarrow \omega, \bar{\omega}$
 $\sqrt[3]{2} \rightarrow \omega\sqrt[3]{2}, \bar{\omega}\sqrt[3]{2}, \sqrt[3]{2}$.

$\# \text{Aut}(\) = 6 \Rightarrow \text{Aut}(\) = S_3$.

группа не абелева и транзитивно действует на корнях.

Пример Если $\text{char } \mathbb{K} = p$, то имеем

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

\uparrow неприводим

$a \rightarrow a+1, a+2, \dots$

\uparrow тоже расширение Галуа

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

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

Поле $\bar{\mathbb{K}}$ называется алгебраическим замыканием поля \mathbb{K} ,

если $\bar{\mathbb{K}}$ - алгебраично над \mathbb{K} и алгебраически замкнуто, т.е. любой мн-и $f(x) \in \bar{\mathbb{K}}[x]$ имеет корень в $\bar{\mathbb{K}}$.

Пример. \mathbb{C} - алгебраически замкнуто.

Теор. Если $\mathbb{L} \supset \mathbb{K}$, \mathbb{L} - алгебраически замкнуто,

то мн-во $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ алгебраических над \mathbb{K} эл-ов - является алгебр. замыканием \mathbb{K} .

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

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

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

тогда \exists корень $d \in \mathbb{F}/\mathbb{F}_0$ - конечное расширение. подполе \mathbb{F}_0 .

$\Rightarrow d$ - алгебраичен над \mathbb{K} , т.к. $d \in \mathbb{K}(a_0, a_1, \dots, a_n; d) \subset \mathbb{L}$

Переформулировка

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

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

Д-во: Рассмотрим все мн-ли $f(x) \in \mathbb{K}[x]$. 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 , порожденный $\{f(x_f) \mid f \in \Omega\}$.

Лемма $I \neq A$.

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

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

P -н мн-ли $g(x) := \prod_{f \in \Omega_0} f(x)$ и поле разложения \mathbb{L} мн-ли $g(x)$.

Тогда имеет 2-ю \mathbb{K} -алгебр $A_0 \xrightarrow{\pi} \mathbb{L}$
 $x_f \rightarrow a_f$ - корень мн-ли $g(x)$ в \mathbb{L} .

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

□.

Рассмотрим максимальный идеал $\mathfrak{J} \subset A$.

Имеет $K_i := A/\mathfrak{J}$ — алгебраич. расширение поля K .

Также построим $K \subset K_1 \subset K_2 \subset \dots$

и назовём $\bar{K} := \bigcup_s K_s$.

Замечание K_i/K — алгебраичит, т.к. всевозможные алгебр. расширения — алгебр.

Кроме того, любой центр. мн-н $f(x) \in K[x]$ расклад. на прим. мн-н уже в K^{alg} .