Лекция 28 апреля (вторая половина)

"Единственность" поля разложения

(с точностью до неканонического изоморфизма)

$\mathbb{L}'$ и $\mathbb{L}''$ — два наименьших поля

$$\begin{tikzcd} \mathbb{L}' \arrow[r, hook] \arrow[rr, bend right, "\text{изоморфизм}"'] & \mathbb{L}'' \arrow[r, hook] & \mathbb{L} \arrow[l, bend right] \arrow[ll, bend right, "\text{тоже изоморфизмы}"'] \end{tikzcd}$$

$\exists$ поле разложения!

$f \in \mathbb{k}[x]$ $\quad \mathbb{F} \supset \mathbb{k}$: f полностью раскладывается на линейные множители в $\mathbb{F}[x]$. Пусть $\theta_1, \dots, \theta_m$ — корни f в $\mathbb{F}$.

$$\underset{\mathbb{L}}{\overset{\|}{}} \quad \mathbb{k}[\theta_1, \dots, \theta_m] < \mathbb{F}$$

$\nearrow$ подалгебра, порождённая корнями, "наименьшее поле, содержащее

$\theta_1, \dots \theta_n$

Это и есть поле разложения

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "\varphi"] \arrow[d, phantom, "\cap"] \arrow[d, dashed, bend right] & \mathbb{L}' \\
\mathbb{L} \arrow[ur] &
\end{tikzcd}$$

f полностью раскладывается

$\underline{\underline{\mu_{\theta_i}}}$ делит f

μ_{θ_i} полностью разлагается в $\mathbb{L}'$

Приложение: конечные поля

$\mathbb{K} \supset \mathbb{F}_p$ - простое подполе.

$|\mathbb{K}| = \underbrace{p^n}_{=q}, \quad n = [\mathbb{K} : \mathbb{F}_p]$

$\mathbb{K}^\times$ – конечная мультипликативная группа порядка $q-1$.

$\theta \in \mathbb{K}^\times$ – это корень многочлена $\underline{x^{q-1}-1}$

$\Downarrow$

$\mathbb{K}$ — поле разложения многочлена $x^q - x$

единственно с точностью до изоморфизма

② Алгебраические замыкания

Опр. Поле $\overline{\mathbb{K}}$ наз. алгебраическим замыканием поля $\mathbb{K}$, если $\overline{\mathbb{K}}$ алгебраично над $\mathbb{K}$ и алгебраически замкнуто (любой $f(x) \in \overline{\mathbb{K}}[x]$ полностью разлагается на линейные множители.

Утв. Алг. замыкание $\exists$ и единственно с точностью до (неканонического) изоморфизма.

Единственность: зам

$$\begin{tikzcd} \mathbb{K} \arrow[r, hook, "\varphi"] \arrow[d, "\text{алг.}"'] & \mathbb{L} \\ {} \arrow[ur, dashed] & \end{tikzcd}$$

Лемма Если $\mathbb{K} \subset \mathbb{E}$ алгебраическое расширение, а $\mathbb{L}$ — алг. замк.

$\mathbb{K}$

нутое поле, то любое вложение $k \hookrightarrow L$ продолжается до вложения $F \hookrightarrow L$

Рассмотрим множество объектов:

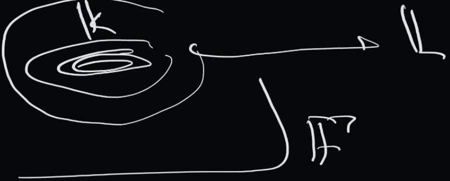
поле $\mathbb{K}$: $k < \mathbb{K} < F$

+ вложение $\mathbb{K} \xhookrightarrow{\psi} F$: $\psi|_{k} = \varphi : k \hookrightarrow L$

Частичный порядок: $(\mathbb{K}_1, \psi_1) \le (\mathbb{K}_2, \psi_2)$

$\Leftrightarrow$

$\mathbb{K}_1 < \mathbb{K}_2$ $\psi_1 = \psi_2|_{\mathbb{K}_1}$



Это полный ЧУМ

$\{\mathbb{K}_\nu\}$: $\mathbb{K}_\nu \le \mathbb{K}_\mu$

$\mathbb{K} = \bigcup \mathbb{K}_\nu$ — верхняя грань семейства $\mathbb{K}_\nu$.

Максимальный элемент $\psi : \mathbb{K} \hookrightarrow L$

имеет $\underline{\underline{\mathbb{K} = \mathbb{F}}}$

$\exists \theta \in \mathbb{F} \setminus \mathbb{K} \Rightarrow \varphi$ можно продолжить на $\mathbb{K}[\theta]$

$\mu_\theta : \mu_\theta^\varphi \in \mathbb{L}[x]$

$\nwarrow$ имеет корни

$\theta \to$ корень

$$\begin{tikzcd} & \mathbb{K} \arrow[dl, hook] \arrow[dr, hook] & \\ \overline{\mathbb{K}} \arrow[rr, hook, shift left] & & \overline{\mathbb{K}}' \arrow[ll, hook, shift left] \end{tikzcd}$$

$\overline{\mathbb{K}} \to \overline{\mathbb{K}}$ тождественно на $\mathbb{K}$

$\Leftarrow$ изоморфизм.

$\exists$ алгебраическое замыкание:

Шаг 1 Пусть есть алгебраически замкнутое поле $\mathbb{L} \supset \mathbb{K}$.

множество целых над $\mathbb{K}$ (= алгебраичных над $\mathbb{k}$) элементов из $\mathbb{L}$ = целое замыкание $\mathbb{K}$ в $\mathbb{L}$ — это поле $\overline{\mathbb{K}}$

оно алгебраически замкнуто.

$f \in \overline{\mathbb{K}}[x]$ то его корни (в каком-то расширении) алгебраичны над $\overline{\mathbb{K}}$ $\Rightarrow$ алгебраичны над $\mathbb{K}$

$\Leftarrow$ они лежат в $\overline{\mathbb{K}}$

Шаг 2 первый шаг в построении $\mathbb{L}$.

Построим поле $\mathbb{E}_1 \supset \mathbb{K}$: все многочлены из $\mathbb{K}[x]$ полностью раскладываются на линейные множители в $\mathbb{E}_1[x]$.

Рассмотрим множество, объектами которого являются такие наборы данных: (1) линейно упорядоченное семейство L многочленов из $\Bbbk[x]$

(2) $\forall f \in L$ должно быть указано поле $\mathbb{L}_f(L)$ (зависящее от семейства L и конкретного $f \in L$)

Имеем что f полностью разложим в $\mathbb{L}_f(L)[x]$

(3) $\forall f \le g$ из L

$$\mathbb{L}_f(L) \subset \mathbb{L}_g(L)$$

Это полный? непустой? ЧУМ

Частичный порядок? : $L_1 \le L_2$

$\Leftrightarrow$

$L_1 \subset L_2$ с сохранением порядка

$\forall f \in L_1 \quad \mathbb{L}_f(L_1) = \mathbb{L}_f(L_2)$

$L = \{f\}$ поле разложения $\mathbb{L}_f$

$\{L_\nu\} \qquad L = \bigcup L_\nu$

$\exists$ максимальное семейство

Даже нет $L = \Bbbk[x]$

если $\exists f \notin L$ $\quad$ $\mathbb{L}_f$ - поле разложения f над $\bigcup\limits_{g \in L} \mathbb{L}_g$

$L' = L \cup \{f\}$

считаем, что $f > L$

$\exists \mathbb{F}_1 \supset \mathbb{k} : \forall f \in \mathbb{k}[x]$ разложим в $\mathbb{F}_1[x]$

Шаг 3: итерируем эту процедуру:

$\mathbb{k} < \mathbb{F}_1 < \mathbb{F}_2 < \mathbb{F}_3 < \ldots$

$\forall f\ \mathbb{F}_i[x]$ полностью разложим в $\mathbb{F}_{i+1}[x]$

$\mathbb{L} = \bigcup\limits_{i \geq 1} \mathbb{F}_i$ — алгебраически замкнутое поле.

$f \in \mathbb{L}[x] \Rightarrow f \in \mathbb{F}_i[x] \Rightarrow f$ разложим над $\mathbb{F}_{i+1}$

$\swarrow$

f разложим над $\mathbb{L}$

$\boxed{\mathbb{k}} \subset \underset{\circlearrowleft}{\mathbb{F}}$ $\quad$ $|\mathrm{Aut}_{\mathbb{k}} \mathbb{F}| = [\mathbb{F} : \mathbb{k}]$

максимальная группа симм.
