Лекция 28 апреля (первая половина)

Экзамен — *воскресенье 22 мая*

в 10^{00} на странице курса появятся задачи

строго до 14^{00} надо прислать рукописные решения (сканы или фото бумажных либо написанные от руки на планшете) на gorod@itep.ru

объём каждого письма $\leq$ 5-7 Mb.

$\mathbb{k} \subset \mathbb{F}$ — расширение полей.

$\mathbb{F}$ называется *сепарабельным* расширением, если $\forall \theta \in \mathbb{F}$ минимальный многочлен μ_θ эл-та θ над $\mathbb{k}$ не имеет кратных корней ни в каком расширении поля $\mathbb{k}$.

$\mu_\theta = \mu_\theta(x) \in \mathbb{k}[x]$ $\quad ev_\theta : \mathbb{k}[x] \longrightarrow \mathbb{F}$, $\quad x \longmapsto \theta$

$\ker ev_\theta = (\mu_\theta)$ $\quad f(x) \longmapsto f(\theta)$

$\nearrow$ приведённый многочлен наименьшей степени, корнем которого является θ.

μ_θ неприводим, т.к. $\dfrac{\mathbb{k}[x]}{(\mu_\theta)} = \operatorname{im}(ev_\theta) < \mathbb{F}$ не имеет делителей нуля.

$f(x)$ имеет кратный корень $\Longleftrightarrow$ у f и f' есть общий корень $\Longleftrightarrow$ $\deg \text{НОД}(f, f') \geq 1$.

μ_θ имеет кратный корень $\Longleftrightarrow$ $\mu_\theta' = 0$

$\operatorname{char} \mathbb{k} = 0 \Rightarrow \mu_\theta$ - сепарабелен $\Rightarrow$ любое расширение $\mathbb{F} \supset \mathbb{k}$ сепарабельно.

Пример: $\mathbb{k} = \mathbb{F}_p(t)$ - поле рациональных функций с к-тами из $\mathbb{k}$

$\mu(x) = \underbrace{x^n - t} \in \mathbb{k}[x] \quad t \in \mathbb{k}$

Упражнение: $\boxed{\mu(x) - \text{неприводим}}$

$\boxed{x^n - a}$ приводим $\Leftrightarrow a = \alpha^k$, $\alpha \in K$, $k \mid n$

$\boxed{n = p}$ $(x^p - t)' = p x^{p-1} = 0$ $\boxed{p = 0}$

Положительный пример: любой неприводимый многочлен $f \in \mathbb{F}_p[x]$ сепарабелен.

$f' = 0 \Rightarrow$ все степени делятся на p

$f(x) = a_0 t^{pn_0} + a_1 t^{pn_1} + \dots =$ $a_i \in \mathbb{F}_p$

$= (a_0 t^{n_0} + a_1 t^{n_1} + \dots)^p$

$\alpha \to \alpha^p$ тождественно действует на $\mathbb{F}_p$

несепарабельный многочлен над $\mathbb{F}_p$ это чистая p-тая степень какого-то мн-на.

Теорема о примитивном элементе:

Всякое конечное сепарабельное расширеиле $\mathbb{E} \supset \mathbb{k}$ примитивно, т.е.

$\mathbb{E} = \frac{\mathbb{k}[x]}{(f)}$, где f - приведён, неприводим

$\theta = [x]_f$ наз. примитивным эл-том.

Док-во: если $\mathbb{k}$ - конечно, то $\mathbb{E}$ тоже конечно, мультипликативная группа $\mathbb{E}^\times$ циклическая, т.е. порождается эл-том θ.

$$\mathbb{E} = \mathbb{k}[\theta] = \frac{\mathbb{k}[x]}{(\mu_\theta(x))}$$

Пусть $\mathbb{k}$ - бесконечно.

$$\mathbb{E} \supset \mathbb{k}$$

$$\mathbb{k} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \dots \subset \mathbb{L}_n = \mathbb{E}$$

$\forall i \quad \mathbb{L}_{i+1} = \frac{\mathbb{L}_i[x]}{(f_i)}$ - примитивное расширение

$\mathbb{E}$ имеет базис $e_1, \dots, e_m$ над $\mathbb{k}$

$\mathbb{L}_1 = \frac{\mathbb{k}[x]}{(\mu_{e_1})}$

$\mathbb{E}$ порождается над $\mathbb{L}_1$ меньшим числом эл-тов e_i; процедуру можно продолжить

Можно без ограничения общности считать

что $\mathbb{F} = \Bbbk[\alpha, \beta]$

Будем искать примитивный эл-т в

виде $\theta_t = \alpha + t\beta$ $\quad t \in \Bbbk^\times$ - ненулевая константа.

$\mathbb{F} = \Bbbk[\theta_t] \iff \beta \in \Bbbk[\theta_t]$

$\alpha = \theta_t - t\beta$ тоже будет в $\Bbbk[\theta_t]$

Пусть

$f_\alpha(x)$ $\quad f_\beta(x)$ - это минимальные многочлены α и β.

Главная мысль: β - общий корень

многочлена $\underline{f_\beta(x)}$

$f_\alpha(\alpha) = 0$

$\alpha = \theta_t - t\beta$

β - корень мн-ка

$$\underline{g(x)} = f_\alpha(\theta_t - tx) \in \underline{\underline{\Bbbk[\theta_t]}}$$

Если все остальные корни у f_β и g

в каком-то поле, где они полностью раскладываются на линейные множители, различны, то $(x-\beta) = \text{НОД}(f_\beta, g) \in$

$$\Leftarrow \qquad \in \underline{\underline{\Bbbk[\theta_t][x]}}$$

$$\beta \in \Bbbk[\theta_t]$$

Фиксируем поле $\mathbb{F} \supset \Bbbk$: f_α и f_β (и g) полностью раскладываются на линейные множители, и пусть $\underset{\alpha}{\underset{\shortparallel}{\alpha_1}}, \dots, \alpha_n$ корни f_α

$\overset{\beta}{\overset{\shortparallel}{\beta_1}}, \dots, \beta_n$ корни f_β $\qquad g(x) = f_\alpha(\underbrace{\theta_t - tx}_{\alpha_j})$

$\theta_t - tx = \alpha_i \qquad x = (\theta_t - \alpha_j)/t$ — корни мн-на g

Надо, чтобы $\boxed{\beta_i \neq \frac{\theta_t - \alpha_j}{t}}$ при всех i и j кроме $i = j = 1$

$$\theta_t = \alpha + t\beta \qquad \frac{\theta_t - \alpha_i}{t} = \frac{\alpha_1 + t\beta_1 - \alpha_i}{t} =$$

$$= \frac{\alpha_1 - \alpha_j}{t} + \beta_1 \neq \beta_i$$ (кроме $i = j = 1$)

$j \neq 1$ $\alpha_1 - \alpha_j \neq 0$ (f_α сепарабелен)

$$t \neq \frac{\alpha_1 - \alpha_j}{\beta_i - \beta_1}$$

$\boxed{j = 1}$

$\beta_1 \neq \beta_i$

что так

(f_β сепарабелен)

Следствие: Пусть сепарабельное алгебраическое расширение полей $\mathbb{k} < \mathbb{F}$ таково, что степени минимальных многочленов эл-тов поля $\mathbb{F}$ ограничены. Тогда $\mathbb{F}$ – конечное расширение.

$\mathbb{F} = \mathbb{k}[\theta]$ где $\theta \in \mathbb{F}$ – элемент максимальной степени.

$\mathbb{F} \neq \mathbb{k}[\theta]$ $\exists\, \alpha \in \mathbb{F} \setminus \mathbb{k}[\theta]$

$$\mathbb{k}[\alpha, \theta] \supsetneq \mathbb{k}[\theta]$$

$$\overset{\mathbb{k}[\alpha,\theta]}{\|} \quad \Rightarrow \deg \beta > \deg \theta$$

$\mathbb{k}[\beta]$

Продолжение гомоморфизмов

$$\begin{tikzcd}
\mathbb{k} \arrow[r, hook, "\varphi"] \arrow[d, phantom, "\cap"] & \mathbb{E} \\
\mathbb{L} \arrow[ur, hook, dashed, "\varphi'"']
\end{tikzcd}$$

когда существуют продолжения и сколько их

Пусть $\mathbb{k} < \frac{\mathbb{k}[x]}{(\mu)}$ – примитивное расширение

$\mu(x) \in \mathbb{k}[x]$ $\qquad \mu^\varphi(x) \in \mathbb{E}[x]$

$\overset{\parallel}{\sum a_i x^i}$ $\qquad \mu^\varphi := \sum \varphi(a_i) x^i$

различных продолжений φ до вложения $\tilde{\varphi} : \frac{\mathbb{k}[x]}{(\mu)} \longrightarrow \mathbb{E}$ существует ровно столько, сколько различных корней есть у многочлена μ^φ в поле $\mathbb{E}$

Док-во: $\psi : \frac{\mathbb{k}[x]}{(\mu)} \longrightarrow \mathbb{E}$

$\theta = [x]_\mu \longmapsto$ корень мн-на $\mu^\varphi(x)$

$[0] = [\mu(x)] \longmapsto \mu^\varphi(\psi(\theta))$

$$\sum a_i \theta^i \longmapsto \overset{\parallel}{\sum \underset{\varphi(a_i)}{\underset{\parallel}{\psi(a_i)}}\, \psi(\theta)^i}$$

$\forall$ корня α мн-на $\mu^{\varphi}(x)$

$$\begin{tikzcd}
\mathbb{k}[x] \arrow[r] & \mathbb{F} \\
x \arrow[r, mapsto] & \alpha \\
f(x) \arrow[r, mapsto] & f(\alpha)
\end{tikzcd}$$

факторизуется до гом-ма

$$\frac{\mathbb{k}[x]}{(\mu)} \longrightarrow \mathbb{F}$$

если и только если $\mu^{\varphi}(\alpha)=0$

Следствие: $\mathbb{k} \subset \mathbb{L}$ - любое конечное расширение, $\mathbb{k} \xhookrightarrow{\varphi} \mathbb{F}$ - вложение.

Различных продолжений $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$: $\psi|_{\mathbb{k}} = \varphi$ имеется не более $[\mathbb{L}:\mathbb{k}]$

и их имеется ровно столько если $\forall \theta \in \mathbb{L}$ мин. многочлен $\mu_{\theta} \in \mathbb{k}[x]$ сепарабелен и μ^{φ} полностью раскладывается на линейные множители в $\mathbb{F}$.

Док-во:

$$\begin{tikzcd}
\mathbb{K} = \mathbb{L}_0 \arrow[r, phantom, "\subset"] \arrow[drr, "\varphi"'] & \mathbb{L}_1 \arrow[r, phantom, "\subset"] \arrow[dr] & \mathbb{L}_2 \arrow[r, phantom, "\subset \dots \subset"] \arrow[d] & \mathbb{L}_m = \mathbb{L} \arrow[dl, "\varphi"] \\
 & & \mathbb{E} &
\end{tikzcd}$$

$$\boxed{\mathbb{L}_{i+1} = \frac{\mathbb{L}_i[x]}{(f_i)}}$$

примитивное расширение $\forall i$

продолжений вложения $\mathbb{L}_i \hookrightarrow \mathbb{E}$ до вложения $\mathbb{L}_{i+1} \to \mathbb{E}$ столько, сколько разных корней имеет многочлен f_i в поле $\mathbb{E}$ таких корней

$$\le \deg f_i = [\mathbb{L}_{i+1} : \mathbb{L}_i]$$

и их ровно столько $\Leftrightarrow$ f_i полностью раскладывается в $\mathbb{E}[x]$ на различные линейные множители

продолжений не больше, чем

$$[\mathbb{L}_1 : \mathbb{L}_0][\mathbb{L}_2 : \mathbb{L}_1] \dots [\mathbb{L}_m : \mathbb{L}_{m-1}]$$

$$[\mathbb{L} : \mathbb{K}] = \prod [\mathbb{L}_{i+1} : \mathbb{L}_i]$$

в силу мультипликативности степени

$[\mathbb{L}_2 : \mathbb{k}] =$ $\Leftarrow \mathbb{k} < \mathbb{L}_1 \subset \mathbb{L}_2$

$= [\mathbb{L}_1 : \mathbb{k}] \cdot [\mathbb{L}_2 : \mathbb{L}_1]$

$e_1 \dots e_n$ $\mathbb{L}_1$ над $\mathbb{k}$ (как векторного пр-ва)

$\xi_1 \dots \xi_m$ $\mathbb{L}_2$ над $\mathbb{L}_1$ (" — ")

$e_i \xi_j$ – базис $\mathbb{L}_2$ над $\mathbb{k}$ как векторного пр-ва.

в качестве $\mathbb{L}_1$ можно взять $\mathbb{k}[\theta]$ с любым $\theta \in \mathbb{L}$

Специальные расширения

① Поле разложения многочлена

$\mathbb{k}[x] \ni f$.

$\exists$ поле $\mathbb{L} \supset \mathbb{k}$: (1) $f(x)$ полностью раскладывается в $\mathbb{L}[x]$ на линейные множители. & (2) $\forall$ поле $\mathbb{L}'$:

в $\mathbb{L}'[x]$ на линейные

$f(x)$ раскладывается в

множители $\exists$ вложения $\mathbb{L} \overset{}{\underset{\text{тождеств. на } \mathbb{k}}{\hookrightarrow}} \mathbb{L}'$

Зам.: Любые два поля $\mathbb{L}$ изоморфны.

$$\begin{tikzcd}
\mathbb{L} \arrow[r, hook] \arrow[rr, bend right, "\text{тожд. на } \mathbb{k}"'] & \mathbb{F} \arrow[r, hook] & \mathbb{L}
\end{tikzcd}$$

Лемма: Если $\mathbb{L}$ алгебраично над $\mathbb{k}$ и $\mathbb{L} \overset{\varphi}{\hookrightarrow} \mathbb{L}$ вложение, тождественное на $\mathbb{k}$, то φ – автоморфизм поля $\mathbb{L}$ (т.е. это биекция).

Док.-во: Надо проверить сюръективность

$\alpha \in \mathbb{L}$ у него есть минимальный многочлен $\mu_\alpha(x) \in \mathbb{k}[x] \Rightarrow \varphi$ переводит корни μ_α у $\mathbb{L}$ в корни μ_α у $\mathbb{L}$

$$\mu_\alpha(\xi) = 0 \qquad \varphi(\underset{\overset{\|}{0}}{\mu_\alpha(\xi)}) = \mu_\alpha(\varphi(\xi)) = 0$$

$\{\varphi(\alpha)\ \varphi^2(\alpha)\ \varphi^3(\alpha)\ldots\}$ — это конечное множество

$\cap$

корней μ_α в $\mathbb{L}$

$\varphi^k(\alpha)=\varphi^m(\alpha)$ для какого-то $m>k$

$$\boxed{\varphi^{m-k}}\left(\varphi^k(\alpha)-\alpha\right)=0$$

φ инъективен $\Rightarrow \boxed{\varphi^k(\alpha)=\alpha}$ $\boxed{\alpha\in \operatorname{im}\varphi}$