Лекция 5 мая (первая половина)

$\Bbbk < \mathbb{E}$ конечное расширение

$\mathrm{Aut}_{\Bbbk}\mathbb{E}$ – автоморфизмы $\mathbb{E}$ над $\Bbbk$ = тождественно действующие на $\Bbbk$

$$\begin{tikzcd}
\Bbbk \arrow[r, hook, "\varphi"] \arrow[d] & \mathbb{E} \\
\mathbb{E} \arrow[ur, dashed, "\tilde{\varphi}"] &
\end{tikzcd}$$

$|\mathrm{Aut}_{\Bbbk}\mathbb{E}| \leq [\mathbb{E}:\Bbbk]$

и равенство означает:

(1) расширение $\mathbb{E} \supset \Bbbk$ сепарабельно

(2) минимальный многочлен над $\Bbbk$ любого элемента $\theta \in \mathbb{E}$ полностью раскладывается на линейные множители в $\mathbb{E}[x]$

Такие расширения называются расширениями Галуа

Условие (2) наз. Нормальностью поля $\mathbb{E}$ над $\Bbbk$

Нормальность $\Leftrightarrow$ любой неприводимый над $\Bbbk$ многочлен из $\Bbbk[x]$, который имеет корень в $\mathbb{E}$, полностью разложим над $\mathbb{E}$

Примеры:

① $\mathbb{E}$ - любое поле, G - конечная группа его автоморфизмов. $\mathbb{E}^G = \{x \in \mathbb{E} \mid gx = x \ \forall g \in G\}$

поле инвариантов группы G

$\mathbb{E} \supset \mathbb{E}^G$ - это расширение Галуа и

$$\mathrm{Aut}_{\mathbb{E}^G} \mathbb{E} = G$$

все различные

$\swarrow$ α

Док-во: $\forall \theta \in \mathbb{E}$ пусть $\underset{\theta}{\underset{\shortparallel}{\theta_1}}, \dots, \theta_m$ - его G-орбита

$$f_\theta(x) = \prod_{i=1}^{m} (x - \theta_i) \in \mathbb{E}^G[x]$$

неприводим над $\mathbb{E}^G$, т.к. $\forall h \in \mathbb{E}^G[x]$ группа G переставляет корни h, и если $f_\theta = h_1 h_2$, то G не может транзитивно действовать на корнях f_θ

Мораль: каждый элемент θ является корнем сепарабельного мн-на из $\mathbb{E}^G[x]$, полностью разлагающегося на линейные множители в $\mathbb{E}[x]$ и степень этого многочлена делит $|G|$.

$\Downarrow$

$\mathbb{E} \supset \mathbb{E}^G$ нормально, сепарабельно.

$$G < \mathrm{Aut}_{\mathbb{E}^G} \mathbb{E}$$

$$\boxed{G \le |\mathrm{Aut}_{\mathbb{F}^G}\mathbb{F}|}$$

$[\mathbb{F} : \mathbb{F}^G]$ конечно и делит $|G|$

т.к. степени всех эл-тов делят $|G|$

$$\boxed{|\mathrm{Aut}_{\mathbb{F}^G}\mathbb{F}| \le [\mathbb{F} : \mathbb{F}^G] \le |G|}$$

Все неравенства должны быть равенствами

$$G = \mathrm{Aut}_{\mathbb{F}^G}\mathbb{F}$$

Специализация (пример)

$\mathbb{F} = \Bbbk(t) = \Bbbk(\mathbb{P}_1)$ поле рациональных функций

$G = S_3$ действует на $\mathbb{P}_1$, переставляя точки $\infty, 0, 1$.

$$\sigma_1 : \begin{array}{l} 1 \to 1 \\ 0 \to \infty \\ \infty \to 0 \end{array} \quad t \longmapsto \frac{1}{t}$$

$$\tau : 0 \to 1 \to \infty \to 0 \qquad t \longmapsto \frac{1}{1-t}$$

$$\sigma_0 : \begin{array}{l} 0 \to 0 \\ 1 \to \infty \\ \infty \to 1 \end{array} \quad t \longmapsto \frac{t}{t-1}$$

$$\tau^{-1} : 0 \to \infty \to 1 \to 0 \qquad t \longmapsto \frac{t-1}{t}$$

$$\sigma_\infty : \begin{array}{l} \infty \to \infty \\ 0 \to 1 \\ 1 \to 0 \end{array} \quad t \longmapsto 1-t$$

$$\mathrm{Id} : t \to t$$

$\mathbb{F}^G$ - ? $\mathbb{F}^G \subset \mathbb{k}(t)$

$\overset{\shortparallel}{\mathbb{k}(\varphi)}$ для какой-то G-инвар. функции φ.

$[\mathbb{F} : \mathbb{F}^G] = |G| = 6$ $\varphi(t) = \frac{p(t)}{q(t)}$

t явл. корнем мн-на $\underbrace{\varphi q(t) - p(t)}$ $\in \mathbb{F}^G[T]$

Нужно придумать инвариантную функцию φ с $\max(\deg p, \deg q) = 6$. Тогда $\underline{\mathbb{F}^G = \mathbb{k}(\varphi)}$.

В прошлом семестре надо было описать инвариантные однородные многочлены от 2х переменных

($S_3 : \mathbb{C}^2$ инвар. в $S(\mathbb{C}^2)$)

Вернитесь к этой задаче !!!

Идея поиска p и q:

θ_1
θ_6

орбита S_3

$\theta_i = (\theta_{i_0} : \theta_{i_1})$

$\prod^{6} \det\begin{pmatrix} t_0 & \theta_{i0} \\ t_1 & \theta_{i1} \end{pmatrix}$ S_3 переводит в себя его корни $\Rightarrow$

$i=1$

$t=(t_0:t_1)$ $\qquad gf=\lambda(g)f$ будет пропорционален f

$\boxed{\lambda: S_3 \to \Bbbk}$ мультипликативный характер

есть ровно 2 характера $\underline{\underline{\mathrm{sgn}}}$ и Id.

есть 3 точечная орбита $\underline{0=(0:1)}$ $\underline{1=(1:1)}$ $\underline{\infty=(1:0)}$

$t_0 t_1 (t_0-t_1)$ зануляется на орбите $0\,1\,\infty$

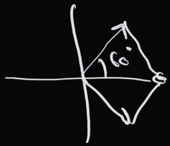
инвариант $\underline{p=t_0^2 t_1^2 (t_0-t_1)^2}$

$\sigma_1: 0 \leftrightarrow \infty$
$t_0 \leftrightarrow t_1$

есть ещё 2-точечная орбита

$$t=\frac{1}{1-t} \qquad t=\frac{t-1}{t}$$

умножение, инвар. отн. поворота — у него 2х точечная орбита



$$\underline{\underline{t^2-t+1}}=\frac{t^3+1}{t+1}$$

$\omega=(1+\sqrt{3}i:2)$
$\bar{\omega}=(1-\sqrt{3}i:2)$

могут не лежать в $\Bbbk$

$q(t)=t^2-t+1$ всё равно инвар.

$q=t_0^2-t_0t_1+t_1^2$ $\qquad \deg 2$

$p = t_0^2 t_1^2 (t_0 - t_1)^2$ deg 6

$$\psi(t) = \frac{p}{q^3} = \frac{t^2(t-1)^2}{(t^2-t+1)^3}$$ степень 6.

S_3-инварианты и $\mathbb{K}(t)^{S_3} = \mathbb{K}(\psi)$

Пример 2: Конечные поля

$q = p^n$ $\quad \mathbb{F}_q \supset \mathbb{F}_p$ — нормальное сепарабельное расширение

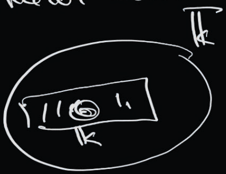
- все конечные расширения $\mathbb{F}_p$ сепарабельны
- нормальное, т.к. это поле разложения многочлена $x^q - x$

Замечание: Конечное расширение $\mathbb{F} \supset \mathbb{K}$ нормально, если выполняется любое из 2х эквивалентных условий:

(1) $\mathbb{F}$ — поле разложения некоторого многочлена из $\mathbb{K}[x]$ (возможно при-

водимого)

(2) Все вложения $\mathbb{E} \hookrightarrow \overline{\mathbb{k}}$, тождественные на подполе $\mathbb{k}$, имеют один и тот же образ.



Док-во: (2) можно считать, что $\mathbb{k} < \mathbb{E} \subset \overline{\mathbb{k}}$

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

$\theta \in \mathbb{E}$

$\theta \to$ один из корней минимального мн-на $\mu_\theta(x)$ эл-та θ над $\mathbb{k}$.

если $\mathbb{E}$ нормально, то все корни μ_θ лежат в $\mathbb{E}$

$\varphi(\mathbb{E}) \subset \mathbb{E}$

если $\forall \varphi$ $\underline{\varphi(\mathbb{E})} \subset \mathbb{E}$ $\Rightarrow$ все корни μ_θ лежат в $\mathbb{E}$ $\forall \theta \in \mathbb{E}$

(2) тавтологически равносильно нормальности.

---

(1) если $\mathbb{E}$ — поле разложения мн-на $f(x)$ из $\underline{\mathbb{k}}[x]$ пусть $\alpha_1, \dots, \alpha_m$ — это корни f в $\overline{\mathbb{k}}$. Подалгебра $\mathbb{k}[\alpha_1, \dots, \alpha_m]$ — это поле, изоморфное полю разложения.

$\varphi: \mathbb{F} \longrightarrow \Bbbk$

$\mathrm{im}(\mathbb{F}) \underset{=}{\subset} \Bbbk[\alpha_1, \dots, \alpha_m]$

образы всех вложений одинаковы $\Rightarrow$ расширение нормально по (2).

если есть конечное нормальное расширение $\mathbb{E} \supset \Bbbk$, пусть $\underline{\mathbb{F} = \Bbbk[\theta_1, \dots, \theta_m]}$,

$\mu_i = \mu_{\theta_i} \in k[x]$ — минимальный многочл. для θ_i над $\Bbbk$. μ_i полностью разлагается на линейные множители в $\mathbb{F}$ $\Longrightarrow$

$\mathbb{F}$ поле разложения $\prod \mu_i$

Возвращаемся к примеру:

$\mathbb{F}_{p^n} \supset \mathbb{F}_p$ нормально и сепарабельно, т.е. является расширением Галуа

$|\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^n}| = n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$

Имеется Фробениус: $F: x \longrightarrow x^p$

тождественный на $\mathbb{F}_p$.

$$\mathrm{Id} = F^0, F^1, \ldots, F^{n-1}$$

Это разные автоморфизмы $F^k \quad x \longmapsto x^{p^k}$

$\boxed{x^{p^k} \equiv x^{p^m}}$ где $0 \le k, m \le n-1$

невозможно тождественно в $\underline{\mathbb{F}_{p^n}}$

многочлен степени $< p^n$ не может иметь p^n корней.

$\Downarrow$

$\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^n}$ = циклическая группа порядка n, порождённая Фробениусом.