Лекция 5 мая (вторая половина)

Соответствие Галуа

Пусть $\mathbb{k} \subset \mathbb{E}$ - расширение Галуа (нормальное и сепарабельное)

$$[\mathbb{E}:\mathbb{k}] = |\mathrm{Aut}_{\mathbb{k}}\mathbb{E}|$$

В этой ситуации $\mathrm{Aut}_{\mathbb{k}}\mathbb{E}$ называется группой Галуа $\mathbb{E}$ над $\mathbb{k}$, обозначения:

$$\underline{\mathrm{Gal}(\mathbb{E}/\mathbb{k})} \qquad \underline{\mathrm{Gal}_{\mathbb{k}}\mathbb{E}}$$

Теорема: Имеется каноническая биекция между подгруппами $H \subseteq \mathrm{Gal}(\mathbb{E}/\mathbb{k})$ и подполями $\mathbb{L} : \mathbb{k} \subseteq \mathbb{L} \subseteq \mathbb{E}$, которая переводит

$$\mathbb{L} \longmapsto \mathrm{Aut}_{\mathbb{L}}\mathbb{E}$$

$$\mathbb{E}^H = \{x \in \mathbb{E} \mid hx = x \ \forall h\}$$

$$H \subset \mathrm{Gal}(\mathbb{E}/\mathbb{k}) \longmapsto \mathbb{E}^H$$ - поле H-инвариан-

причём расширение $\mathbb{k} < \mathbb{L}$ тов явл. расширением Галуа (т.е. нормально и сепарабельно) $\Longleftrightarrow$ отвечающая ему подгруппа $H = \mathrm{Aut}_{\mathbb{L}}\mathbb{E}$ нормальна в $\mathrm{Gal}(\mathbb{F}/\mathbb{k})$ и в этом случае $\mathrm{Gal}(\mathbb{L}/\mathbb{k}) \cong$

$$\cong \mathrm{Gal}(\mathbb{E}/\mathbb{k})/H.$$

Док-во: $\mathbb{L} \longmapsto H = \mathrm{Aut}_{\mathbb{L}}\mathbb{E}$

мы видели в примере 1:

$\mathbb{E}^H \subset \mathbb{E}$ – конечное расширение Галуа степени $|H|$ и $H = \mathrm{Gal}(\mathbb{F}/\mathbb{E}^H)$

$$\begin{tikzcd} \mathbb{L} \arrow[r] & H \arrow[r] & \mathbb{E}^H \arrow[d, phantom, "\shortparallel\ \cup"] \\ & & \underline{\underline{\mathbb{L}}} \end{tikzcd}$$

$$[\mathbb{E}:\mathbb{E}^H] = |H| = [\mathbb{E}:\mathbb{L}]$$

$$\begin{tikzcd} \text{подполя} \arrow[r] \arrow[rr, bend right] & \text{подгруппы} \arrow[r] & \text{подполя} \end{tikzcd}$$

[конечное множество]

Id.

Утверждение о биекции очевидно из примера 1

Лемма $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \mathbb{F}_2$

(А) $\mathbb{F}_2 \supset \mathbb{F}_0$ сепарабельно $\Leftrightarrow$ оба расширения $\mathbb{F}_0 \subset \mathbb{F}_1$ и $\mathbb{F}_1 \subset \mathbb{F}_2$ сепарабельны

(Б) если $\mathbb{F}_2 \supset \mathbb{F}_0$ нормально, то $\mathbb{F}_2 \supset \mathbb{F}_1$ нормально, а $\mathbb{F}_1 \supset \mathbb{F}_0$ нормально если и только если все вложения $\mathbb{F}_1 \hookrightarrow \mathbb{F}_2$, тождественные на $\mathbb{F}_0$, имеют один и тот же образ.

Док-во: (А) $\underline{\mathbb{F}_0 \subset \mathbb{F}_1} \subset \underline{\mathbb{F}_2} \subset \overline{\mathbb{F}_0}$

$\mathbb{F}_2 \supset \mathbb{F}_0$ сепарабельно $\Leftrightarrow$ имеется $[\mathbb{F}_2 : \mathbb{F}_0]$ вложений $\mathbb{F}_2 \hookrightarrow \overline{\mathbb{F}_0}$, тождеств. над $\mathbb{F}_0$

$\mathbb{F}_1 \supset \mathbb{F}_0$ " — " $\Leftrightarrow$ $[\mathbb{F}_1 : \mathbb{F}_0]$ вложений $\mathbb{F}_1 \hookrightarrow \overline{\mathbb{F}_0}$

$\mathbb{E}_2 \supset \mathbb{E}_1$ " — " $\Leftrightarrow$ $[F_2 : F_1]$ вложений

$$\mathbb{E}_2 \hookrightarrow \overline{\mathbb{E}_1} = \overline{\mathbb{E}_0}$$

$[F_2 : F_0] = [F_1 : F_0] \cdot [F_2 : \mathbb{E}_1]$ А доделали

(Б) $\mathbb{E}_2 \supset \mathbb{E}_0$ нормально, то минимальный многочлен любого $\theta \in \mathbb{E}_2$ над $\mathbb{E}_0$ полностью разложим в $\mathbb{E}_2[x]$.

минимальный многочлен θ над $\mathbb{E}_1$ делит мин. многочлен θ над $\mathbb{E}_0$ $\Rightarrow$ тоже полностью разложим в $\mathbb{E}_2[x]$

$$\Downarrow \qquad \mathbb{E}_0 \subset \mathbb{E}_1 \subset \underset{\theta}{\mathbb{E}_2}$$

$\mathbb{E}_2 \supset \mathbb{E}_1$ нормально.

$$\left[\begin{tikzcd}
\mathbb{E}_0 \arrow[r, hook, "\text{нормально}"] \arrow[d, phantom, "\cap"] & \mathbb{E}_2 \arrow[r, hook] & \overline{\mathbb{E}_0} \\
\mathbb{E}_1 & &
\end{tikzcd}\right.$$

все вложения $\mathbb{E}_2$ в $\overline{\mathbb{E}_0}$ над $\mathbb{E}_0$ имеют один и тот же образ $\mathbb{E}_2 \subseteq \overline{\mathbb{E}_0}$

(мы считаем, что $\mathbb{E}_0 < \mathbb{E}_1 < \mathbb{E}_2 < \overline{\mathbb{E}_0}$)

всякое вложение $\mathbb{E}_1 \hookrightarrow \overline{\mathbb{E}_0}$ над $\mathbb{E}_0$ имеет образ в $\mathbb{E}_2$

$\Downarrow$

нормальность $\mathbb{E}_1$ над $\mathbb{E}_0$ (т.е. одинаковость образов всех вложений $\mathbb{E}_1 \hookrightarrow \overline{\mathbb{E}_0}$) равносильна одинаковости образов всех вложений $\mathbb{E}_1 \hookrightarrow \mathbb{E}_2$ над $\mathbb{E}_0$

Лемма доказана.

Предупреждение башня нормальных расширений реально может не быть нормальной.

Пример: $$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{2}] = \underset{\substack{\shortparallel \\ \mathbb{F}}}{\frac{\mathbb{Q}[x]}{(x^4-2)}}$$

$$\varphi : \mathbb{F} \hookrightarrow \overline{\mathbb{Q}} \subset \mathbb{C}$$

задаётся образом $\underset{\shortparallel}{\varphi(\theta)}$ $\theta = [x]_{x^4-2}$

одному из корней x^4-2 в $\mathbb{C}$

$\sqrt[4]{2} \in \mathbb{R}$ $\qquad i\sqrt[4]{2} \in \mathbb{C} \setminus \mathbb{R}$

$-\sqrt[4]{2} \in \mathbb{R}$ $\quad -i\sqrt[4]{2} \in \mathbb{C} \setminus \underline{\mathbb{R}}$

есть 4 вложения $\mathbb{Q}[\sqrt[4]{2}]$ в $\overline{\mathbb{Q}} \subset \mathbb{C}$

2 разных образа! $\mathbb{Q}[\sqrt[4]{2}] \subset \mathbb{R}$

$\mathbb{Q}[i\sqrt[4]{2}] \subset \mathbb{C}$

Это расширение НЕ нормально

$$\begin{array}{ccccc} \mathbb{Q} & \subset & \mathbb{Q}[\sqrt{2}] & \subset & \mathbb{Q}[\sqrt[4]{2}] \\ & & \parallel & & \parallel \\ & & \dfrac{\mathbb{Q}[x]}{x^2-2} & & \mathbb{Q}[\sqrt{2}][\sqrt{\theta}] \\ & & \Downarrow & & \\ & & \theta = [x]_{x^2-2} & & \end{array}$$

Всякое расширение степени 2 нормально

$[\mathbb{E} : \mathbb{k}] = 2$ $\quad \mu_\theta$ имеет степень 2 $\forall \theta$

если имеет корень в $\mathbb{E}$, то и полностью раскладывается,

---

Окончание доказательства теоремы

$$\mathbb{k} \subset \mathbb{E}$$

$$\mathbb{k} \subset \mathbb{L} \subset \mathbb{E}$$

$$\Downarrow$$

$$H = \mathrm{Aut}(\mathbb{E}/\mathbb{L})$$

расширение $\mathbb{L} \subset \mathbb{E}$ всегда расширение Галуа и $\mathrm{Gal}(\mathbb{E}/\mathbb{L}) = H$.

$\mathbb{L} \supset \mathbb{k}$ – расширение Галуа $\Longleftrightarrow$ у всех вложений $\mathbb{L} \hookrightarrow \mathbb{E}$ над $\mathbb{k}$ один и тот же образ.

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

$\overline{\varphi} \in \mathrm{Aut}_{\mathbb{k}} \mathbb{E} \in \mathrm{Gal}(\mathbb{E}/\mathbb{k})$

$\forall \varphi : \mathbb{L} \to \mathbb{E}$ образ $\varphi(\mathbb{L})$ имеет вид $g\mathbb{L}$ для некоторого эл-та $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{k})$

$H = \mathrm{Aut}\, \mathbb{E}/\mathbb{L} =$ централизатор $\mathbb{L}$
(поточечный стабилизатор)
в $\mathrm{Gal}(\mathbb{E}/\mathbb{k})$

сопряжён поточечному стабилизатору

поля $\varphi(\mathbb{L}) = g\mathbb{L}$

$$\mathrm{Aut}\, \mathbb{E}/\varphi(\mathbb{L}) = gHg^{-1}$$

$\psi(\mathbb{L}) = \mathbb{L} \iff gHg^{-1} = H \quad \forall g \in G.$

$\mathbb{L} \supset \mathbb{k}$ нормально $\iff H \triangleleft \mathrm{Gal}(\mathbb{F}/\mathbb{k})$

Соответствие Галуа оборачивает включения!

$$H_1 \subset H_2 \Rightarrow \mathbb{F}^{H_1} \supset \mathbb{F}^{H_2}$$

$$\mathrm{Aut}_{\mathbb{L}_1} \mathbb{F} \supset \mathrm{Aut}_{\mathbb{L}_2} \mathbb{F} \Leftarrow \mathbb{L}_1 \subset \mathbb{L}_2$$

$H_1 \cap H_2$ – наибольшая подгруппа, лежащая и в H_1 и в H_2

$\updownarrow$

наименьшее подполе, содержащее $\mathbb{L}_1 = \mathbb{F}^{H_1}$ и $\mathbb{L}_2 = \mathbb{F}^{H_2}$

$\mathbb{L}_1\mathbb{L}_2$ – композит.

$\mathbb{LK}$ – наим. подполе, содержащее $\mathbb{L}$ и $\mathbb{K}$ = линейная

$$\mathbb{k} \subset \mathbb{L} \subset \mathbb{F}$$
$$\mathbb{k} \subset \mathbb{K} \subset \mathbb{F}$$

алгебраично над $\mathbb{L}$ и над $\mathbb{k}$

оболочки всевозможных
произведений $\underline{\underline{xy}}$ $x \in \mathbb{L}$, $y \in \mathbb{K}$,

(эта подалгебра, целая над $\mathbb{K}$ и без делителей нуля $\Longrightarrow$ это поле).

пересечение подгрупп $\longleftrightarrow$ композит полей

пересечение полей $\longleftrightarrow$ $\boxed{\text{группу, порождённую } H_1 \text{ и } H_2}$

$\mathbb{L}_1 \cap \mathbb{L}_2$ - наибольшее поле лежащее в $\mathbb{L}_1$ и в $\mathbb{L}_2$ $\longleftrightarrow$ наименьшую подгруппу, содержащую H_1 и H_2