Лекция 8 | Алгебра-2 НМУ | Соответствие Галуа

Напомним, что конечное расширение полей $\mathbb{F}/\mathbb{k}$ называется расширением Галуа если выполнено одно из следующих эквивалентных условий:

а) $\mathbb{F}$ — поле разложения сепарабельного мн-на

б) $\mathbb{k} = \mathbb{F}^{Gal(\mathbb{F}/\mathbb{k})}$, где $Gal(\mathbb{F}/\mathbb{k}) := Aut_{\mathbb{k}}(\mathbb{F})$ — группа $\mathbb{k}$-линейных автоморфизмов $\mathbb{F}$.

в) $\exists$ подгруппа $H \subset Aut_{\mathbb{k}}(\mathbb{F})$ т.ч. $\mathbb{k} = \mathbb{F}^H$

г) $\mathbb{F}/\mathbb{k}$ — нормальное сепарабельное расширение

д) $\mathbb{F} \otimes_{\mathbb{k}} \mathbb{F} \simeq \mathbb{F} \oplus \ldots \oplus \mathbb{F}$ (из-зм колец).

Пример 1 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ — поле разложения x^2-2.

Вообще, когда $\mu_\alpha(x)$ — квадратичный без кратных корней, то $\mathbb{k}(\alpha) = \mathbb{k}[x]/\mu_\alpha(x)$ — расширение Галуа.

Группа Галуа $\sqrt{2} \to \pm\sqrt{2}$.

Пример 2 $\mathbb{Q}(\zeta)/\mathbb{Q}$ — поле разложения x^n-1, ζ — примитивный корень n-ой степени из 1.

$[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$

Теор. (Дирихле) (без д-ва) Круговой мн-н $\Phi_n(x) = \prod_{\zeta\text{ — примит.}} (x-\zeta) = \dfrac{x^n-1}{\prod_{d|n,\, d<n} \Phi_d(x)}$ — неприводим $/\mathbb{Q}$.

$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Пример 3 $\mathbb{F}_{q^n}/\mathbb{F}_q$ — поле разложения мн-на $x^{q^n}-x$.

Есть автоморфизм Фробениуса $\phi: a \to a^q$, его инварианты это подполе $\mathbb{F}_q$,

$\phi^n = e$, т.е. $\mathbb{F}_q = (\mathbb{F}_{q^n})^{\phi}$ — инварианты относительно действия циклической подгруппы, порождённой ϕ.

$$\Rightarrow \langle\phi\rangle \simeq \mathbb{Z}/n\mathbb{Z} = Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

эквивалентность опр-ий (б) и (в).

Замечание Если $\mathbb{F}/\mathbb{k}$ — расширение Галуа с группой Галуа G

Тогда $\forall \alpha \in \mathbb{F}$ минимальный мн-н $\mu_\alpha(x) = \prod_{\beta \in G\alpha} (x-\beta)$ ← орбита действие группы G.

Элементы орбиты $G\alpha$ называются сопряжёнными к α над полем $\mathbb{k}$.

Д-во $\forall g \in G$ имеем $g(\mu_\alpha(x)) = \prod\limits_{\beta \in G\alpha} (x - g\beta) = \mu_\alpha(x) \Rightarrow \mu_\alpha(x) \in \mathbb{F}^G[x] = \mathbb{K}[x]$.

Более того, если α корень $\mu_\alpha(x)$, то $g\alpha$ корень $g(\mu_\alpha(x)) = \mu_\alpha(x)$.

$\Rightarrow$ построенный мн-н аннулирующий и делит минимальный. $\square$

Пример. Пусть $a_1, \dots, a_n$ – набор попарно взаимнопростых, свободных от квадратов чисел. Тогда $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})/\mathbb{Q}$ – расширение Галуа степени 2^n с группой Галуа $\mathbb{Z}_2^n$, где i-ая образующая $\hat{\xi}_i$ автоморфизм, который переводит $\sqrt{a_i} \to -\sqrt{a_i}$, $\sqrt{a_j} \to \sqrt{a_j}$ для $j \neq i$.

Д-во: (индукция по n) База очевидна.

(шаг индукции) Пусть $\mathbb{Z}_2^{n-1} = \mathrm{Gal}(\mathbb{Q}(\sqrt{a_1}, \dots \sqrt{a_n})/\mathbb{Q}) =: G$.

Тогда группа Галуа G действует $\mathbb{Q}$-линейными преобразованиями на $\mathbb{Q}$-вект. пр-ве $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_{n-1}})$, т.е. мы имеем пр-ие $/\mathbb{Q}$. Его инвариантные подпространства – это собственные прямые $\mathbb{Q}(\sqrt{a_{i_1} \cdot \ldots \cdot a_{i_s}})$

$\Rightarrow \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_{n-1}}) \simeq \bigoplus\limits_{I \subset \{1, \dots, n-1\}} \mathbb{Q}(\sqrt{a_{i_1} \dots a_{i_s}})$ – это всё неизоморфные одномерные подпр-ия

Из-зм, как G-представлений.

Предположим, что эл-нт $\sqrt{a_n} \in \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_{n-1}})/\mathbb{Q}$, минимальный мн-н $\sqrt{a_n}/\mathbb{Q}$ равен $x^2 - a_n = (x - \sqrt{a_n})(x + \sqrt{a_n})$

$\Rightarrow$ Мн-во эл-ов сопряжённых с $\sqrt{a_n}$ это только $\pm\sqrt{a_n}$.

$\Rightarrow \mathbb{Q}(\sqrt{a_n})$ – инвариантная прямая для G.

$\Rightarrow \sqrt{a_n}$ пропорционален одному из $\sqrt{a_{i_1} \dots a_{i_s}}$, что не верно в силу взаимной простоты.

Упр. (насколько сильно можно ослабить условие взаимной простоты a_s).

Сформулируем центральный результат теории Галуа, док-во которого у нас уже практически имеется.

Теор (Соответствие Галуа) Пусть $\mathbb{F}/\mathbb{K}$ – конечное расширение Галуа.

Тогда имеет место биекция (взаимнообр. отображения)

$$\left\{ \begin{matrix} \text{Мн-во подгрупп} \\ H \subset Gal(\mathbb{F}/\mathbb{K}) \end{matrix} \right\} \quad \begin{matrix} H \longmapsto \mathbb{F}^H \\ \underset{\mathbb{L}}{Aut(\mathbb{F})} \longleftarrow \mathbb{L} \end{matrix} \quad \left\{ \begin{matrix} \text{Мн-во промежуточных} \\ \text{подполей:} \\ \mathbb{K} \subset \mathbb{L} \subset \mathbb{F} \end{matrix} \right\}$$

Д-во: покажем, что отображение взаимнообратны:

$\Leftarrow$ Пусть $H \subset Gal(\mathbb{F}/\mathbb{K})$, тогда $\mathbb{F}/\mathbb{F}^H$ – расширение Галуа по Опр (в)

и $Gal(\mathbb{F}/\mathbb{F}^H) = H$ по Опр (б).

$\Rightarrow$ Пусть $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$, $\mathbb{F}/\mathbb{K}$ – расширение Галуа $\Leftrightarrow$ $\mathbb{F}$ – поле разложения сепарабельного мн-на $f(x) \in \mathbb{K}[x] \subset \mathbb{L}[x]$, тогда $\mathbb{F}$ можно воспринимать, как поле разложения того же самого мн-на $f(x)$, рассматриваемого, как мн-н с коэф из $\mathbb{L}[x]$. $\Rightarrow$ $\mathbb{F}/\mathbb{L}$ – расширение Галуа.

$\Rightarrow \mathbb{L} = \mathbb{F}^{Gal(\mathbb{F}/\mathbb{L})}$. $\square$

Св-ва соответствия.

Соответствие Галуа это больше, чем биекция, оно согласовано с вложениями и действием группы G; а именно

1) $H_1 \subset H_2 \iff \mathbb{F}^{H_1} \supset \mathbb{F}^{H_2}$

и индекс подгруппы: $(H_2 : H_1)$ $=$ степени расширения $[\mathbb{F}^{H_1} : \mathbb{F}^{H_2}]$.

2) $G \curvearrowright$ подгруппах сопряжениями $\longleftrightarrow$ $G \curvearrowright$ подполях.

т.е. $\forall g \in G \quad \mathbb{F}^{gHg^{-1}} = g(\mathbb{F}^H) \iff Gal(\mathbb{F}/g(\mathbb{L})) = g\, Gal(\mathbb{F}/\mathbb{L})\, g^{-1}$

3) $H \subset G$ – нормальная $\iff$ $\mathbb{F}^H/\mathbb{K}$ – нормальное $\Rightarrow$ расширение Галуа.

Д-во: (1) следует из того, что $[\mathbb{F} : \mathbb{F}^H] = \# H$.

(2) выводится из равносильности: $h\alpha = \alpha \iff (ghg^{-1})g\alpha = g\alpha$.

(3) Если $H \lhd G$, то $\forall g \in G$ $\; gHg^{-1} = H \iff g(\mathbb{F}^H) = \mathbb{F}^H$.

$\Rightarrow$ имеется действие группы G автоморфизмами $\mathbb{F}^H$.

Ядро этого действия сама группа H. $\Rightarrow \mathbb{K} = \mathbb{F}^G = (\mathbb{F}^H)^{G/H}$.

$\Rightarrow \mathrm{Gal}(\mathbb{F}^H/\mathbb{K}) = G/H$.

Наоборот, если $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$ и $\mathbb{L}/\mathbb{K}$ – нормально, то

$\forall \alpha \in \mathbb{L}$ $\; \mu_\alpha(x) \in \mathbb{K}[x]$ раскладывается на лин. мн-ли в $\mathbb{L}$.

$\Rightarrow$ сопряжённые к α принадлежат $\mathbb{L} \Rightarrow \forall g \in G \; g\mathbb{L} \subset \mathbb{L}$.

$\iff g\,\mathrm{Gal}(\mathbb{L}/\mathbb{K})\,g^{-1} = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

□

Примеры $\quad f(x) = x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})\cdot(x - \bar{\omega}\sqrt[3]{2})$.

Имеем $\mathbb{Q}_f = \mathbb{Q}(\omega, \sqrt[3]{2})$ и $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Имеем $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \hookrightarrow S_3$

$\Rightarrow$ это вложение из-зм.

Опишем биекцию:

$$\begin{tikzcd}
 & \mathbb{Q}(\omega, \sqrt[3]{2}) & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[ur] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[u] & \mathbb{Q}(\bar{\omega}\sqrt[3]{2}) \arrow[ul] \\
 & \mathbb{Q}(\omega) \arrow[uu, bend left] & \\
 & \mathbb{Q} \arrow[uul] \arrow[u] \arrow[uu, bend right] \arrow[uur] &
\end{tikzcd}
\longleftrightarrow
\begin{tikzcd}
 & e \arrow[dl] \arrow[d] \arrow[dr] \arrow[dd, bend left] & \\
(23) \arrow[ddr] & (13) \arrow[dd] & (12) \arrow[ddl] \\
 & A_3 \arrow[d] & \\
 & S_3 &
\end{tikzcd}$$

Замечание если $\deg f = n$, $\mathbb{K}_f$ - поле разложения сепарабельного мн-на f, то имеет место вложение

$\mathrm{Gal}(\mathbb{K}_f/\mathbb{K}) \hookrightarrow S_n$

А именно группа Галуа действует на мн-ве корней мн-на.

$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$

Имеем $\mathbb{K}_f = \mathbb{K}(\alpha_1, \dots, \alpha_n)$,

поэтому любой автоморфизм однозначно определён образами $\alpha_1, \dots, \alpha_n$.

Пример. $\quad f(x) = x^7 - 1 \qquad \mathbb{Q}_f = \mathbb{Q}(\zeta)$, где $\zeta = e^{\frac{2\pi i}{7}}$ – примитивный корень.

Имеем $\mathrm{Aut}(\mathbb{Q}_f/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z}$

Образующая мультипликативной группы $\sigma : \zeta \to \zeta^3$.

$\langle \sigma^3 \rangle$ – подгруппа порядка 2, $\langle \sigma^2 \rangle$ – подгруппа пор-ка 3

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta) & \\
\mathbb{Q}(\zeta + \zeta^2 + \zeta^4) \arrow[ur] & & \mathbb{Q}(\zeta + \bar{\zeta}) \arrow[ul] \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & e \arrow[dl] \arrow[dr] & \\
\mathbb{Z}_3 = \langle \sigma^2 \rangle \arrow[dr] & & \langle \sigma^3 \rangle \simeq \mathbb{Z}_2 \arrow[dl] \\
 & \langle \sigma \rangle = \mathbb{Z}_6 &
\end{tikzcd}$$

Сегодня не упомянули никакой связи с определением через полупростое разложение $\mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} = \mathbb{F}\oplus\ldots\oplus\mathbb{F}$.

<u>Лемма</u> Пусть $\mathbb{F}/\mathbb{k}$ – расширение Галуа.
Тогда существует естественная биекция между следующими мн-вами
(а) Группа Галуа $Gal(\mathbb{F}/\mathbb{k})$
(б) Простые идеалы в $\mathbb{F}\otimes_{\mathbb{k}}\mathbb{F}$.
(в) Гомоморфизмы $\varphi: \mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} \to \mathbb{F}$, тождественные на $\mathbb{F}\otimes 1 \hookrightarrow \mathbb{F}\otimes\mathbb{F} \twoheadrightarrow \mathbb{F}$

$$\begin{array}{c} \mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} \\ \uparrow {\scriptstyle Id\otimes 1} \\ \mathbb{F} \end{array}$$

<u>Д-во:</u> (б) $\Leftrightarrow$ (в) очевидно, т.к. сопоставляем простому идеалу проекцию $\mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} \to \mathbb{F}\oplus\ldots\oplus\mathbb{F} \twoheadrightarrow \mathbb{F}$.

(а) $\Rightarrow$ (в) $g\in Aut(\mathbb{F}/\mathbb{k})$ имеем $\mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} \to \mathbb{F}$

$a\otimes b \to a\,g^{-1}(b)$.

(в) $\Rightarrow$ (а) Пусть e – идемпотент в $\mathbb{F}\otimes_{\mathbb{k}}\mathbb{F}$, тогда есть два отображения

$L_e: \mathbb{F} \Rightarrow \mathbb{F}\otimes 1 \subset \mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} \xrightarrow{\pi_e} \mathbb{F}_e$

$R_e: \mathbb{F} = 1\otimes\mathbb{F} \subset \mathbb{F}\otimes_{\mathbb{k}}\mathbb{F} \xrightarrow{\pi} \mathbb{F}_e$.

В качестве автоморфизма следует взять $L_e R_e^{-1}: \mathbb{F}\to\mathbb{F}$.

<u>Упр.</u> Показать, что это биекция.