抽象代数学

设 $\mathbb{E}/\mathbb{F}$ 是域的扩张，令 $Gal(\mathbb{E}/\mathbb{F}) = Aut_{\mathbb{F}}\mathbb{E}$，即

$$Aut_{\mathbb{F}}\mathbb{E} = \{\sigma: \mathbb{E} \to \mathbb{E} \text{ 域自同构} \mid \sigma(x) = x,\ \forall x \in \mathbb{F}\}$$

给定 $G \leq Aut(\mathbb{E})$，定义

$$Inv(G) = \{x \in \mathbb{E} \mid \sigma(x) = x,\ \forall \sigma \in G\}$$

这诱导了两个映射

$$Inv: \{Aut(\mathbb{E}) \text{ 的子群}\} \longrightarrow \{\mathbb{E} \text{ 的子域}\}$$

$$G \longmapsto Inv(G)$$

$$Gal(\mathbb{E}/\ ): \{\mathbb{E} \text{ 的子域}\} \longrightarrow \{Aut(\mathbb{E}) \text{ 的子群}\}$$

$$\mathbb{L} \longmapsto Gal(\mathbb{E}/\mathbb{L})$$

若我们关心是 $\mathbb{F}$ 和 $\mathbb{E}$ 之间的中间域，则有

$$Inv: \{Aut_{\mathbb{F}}(\mathbb{E}) \text{ 的子群}\} \longrightarrow \{\mathbb{L} \text{ 域} \mid \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}\}$$

$$Gal(\mathbb{E}/\ ): \{\mathbb{L} \text{ 域} \mid \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}\} \longrightarrow \{Aut_{\mathbb{F}}(\mathbb{E}) \text{ 的子群}\}$$

引理1 设 $\mathbb{E}$ 为域，$G, G_1, G_2 \leq Aut(\mathbb{E})$，$\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}$ 是 $\mathbb{E}$ 的子域

(1) $G_1 \subseteq G_2 \Rightarrow Inv(G_1) \supseteq Inv(G_2)$

(2) $\mathbb{F}_1 \subseteq \mathbb{F}_2 \Rightarrow Gal(\mathbb{E}/\mathbb{F}_1) \supseteq Gal(\mathbb{E}/\mathbb{F}_2)$

(3) $\mathrm{Inv}\circ \mathrm{Gal}(\mathbb{E}/\ )(\mathbb{F}) = \mathrm{Inv}(\mathrm{Gal}(\mathbb{E}/\mathbb{F})) \supseteq \mathbb{F}$

(4) $\mathrm{Gal}(\mathbb{E}/\ )\circ \mathrm{Inv}(G) = \mathrm{Gal}(\mathbb{E}/_{\mathrm{Inv}G}) \supseteq G$

(5) $\mathrm{Gal}(\mathbb{E}/\ )\circ \mathrm{Inv}\circ \mathrm{Gal}(\mathbb{E}/\ )(\mathbb{F}) = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$

(6) $\mathrm{Inv}\circ \mathrm{Gal}(\mathbb{E}/\ )\circ \mathrm{Inv}(G) = \mathrm{Inv}(G)$.

注：(5),(6) 意味着 Inv 和 $\mathrm{Gal}(\mathbb{E}/\ )$ 限制在像上互逆映射

$$\begin{tikzcd} \mathrm{Im}(\mathrm{Inv}) \arrow[r, bend left, "\mathrm{Gal}(\mathbb{E}/\ )"] & \mathrm{Im}(\mathrm{Gal}(\mathbb{E}/\ )) \arrow[l, bend left, "\mathrm{Inv}"] \end{tikzcd}$$

我们关心何种条件下，(3),(4) 变为等式 $\begin{cases} 若\ \mathbb{F} = \mathrm{Inv}\,G \\ 若\ G = \cancel{\mathrm{Inv}}\,\mathrm{Gal}(\mathbb{E}/\mathbb{F}). \end{cases}$

若限制到 $\mathbb{F}$ 和 $\mathbb{E}$ 之间中间域，引理展示

$$\begin{tikzcd} \mathbb{F} \arrow[r, "\mathrm{Gal}(\mathbb{E}/\ )"] & \mathrm{Gal}(\mathbb{E}/\mathbb{F})\ \cancel{\{id\}} \\ \cap\!\!\mid & \vee\!\!/ \\ L' & \mathrm{Gal}(\mathbb{E}/L') \\ \cap\!\!\mid & \vee\!\!/ \\ L & \mathrm{Gal}(\mathbb{E}/L) \\ \cap\!\!\mid & \vee\!\!/ \\ \mathbb{E} & \{id\} \arrow[l, bend left, "\mathrm{Inv}"] \end{tikzcd}$$

引理2 (1) 设 $\mathbb{E}/\mathbb{F}$ 有限扩张，则 $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| \leq [\mathbb{E}:\mathbb{F}]$

(2) (Artin) 设 $\mathbb{E}$ 是域，$G \leq \mathrm{Aut}(\mathbb{E})$，且 $|G| < \infty$，$\mathbb{F} = \mathrm{Inv}(G)$

则 $[\mathbb{E}:\mathbb{F}] \leq |G|$

证明：(1) $|Gal(\mathbb{E}/\mathbb{F})| = |Aut_{\mathbb{F}}(\mathbb{E})| \leq |Hom_{\mathbb{F}}(\mathbb{E},\mathbb{F})| \leq [\mathbb{E}:\mathbb{F}]$

(上一讲义)

(2) 设 $|G| = n$，因为 $[\mathbb{E}:\mathbb{F}] \geq |Gal(\mathbb{E}/\mathbb{F})| \geq |G|$

只需证 $\forall x_1, \cdots, x_{n+1} \in \mathbb{E}$，它们是 $\mathbb{F}$-线性相关的。即

$\sum c_j x_j = 0$，$c_j \in \mathbb{F}$ 不全为 0. 令 $c = (c_1, \cdots, c_{n+1})^T$

设 $G = \{g_1, \cdots, g_n\}$ 令 $A = (g_i(x_j))_{i,j} \in M_{n\times(n+1)}(\mathbb{E})$

$Ac = 0$ 有非零解. $Ac = 0 \Leftrightarrow \sum_j g_i(x_j) c_j = 0 \quad (*)$ $i=1,\cdots,n$

设 $b = \begin{pmatrix} b_1 \\ \vdots \\ b_{n+1} \end{pmatrix}$ 是一个非零解，在所有非零解中有最少的

非零分量，不妨设 $b_1, \cdots, b_r \neq 0$，$b_{r+1} = \cdots = b_{n+1} = 0$，且 $b_1 = 1$

应用 $g \in G$ 到 $(*)$ 得到（将 c 换成 b）且 $g(b_2) \neq b_2$. $\exists g \in G$. 若 $b_2 \notin \mathbb{F}$

$$0 = \sum g g_i(x_j) g(b_j)$$

$\{g_1, \cdots, g_n\} = \{gg_1, \cdots, gg_n\} \Rightarrow Ac = 0$ 有解 $\begin{pmatrix} g(b_1)=1 \\ \vdots \\ g(b_{n+1}) \end{pmatrix} = d$

$b - d$ 有更少非零分量，矛盾！$\Rightarrow b_i \in \mathbb{F}$ $i = 1, \cdots, n+1$

$\Rightarrow |G| \leq [\mathbb{E}:\mathbb{F}] \Rightarrow |G| = |E:F|$

注：证明(2)中，矩阵 $A = (g_i(x_j))_{\substack{i=1,\cdots,n \\ j=1,\cdots,n+1}}$ 诱导了 $\mathbb{F} = Inv G$.

中元素. 设 A_j 是将 A 中第 j 列删去得到的 矩阵行列

式，则 $\sum_{j=1}^{n+1} A_j x_j = 0$，选择合适 $\{x_i\}$ 使得 $\mathrm{rank} A = n$，

不妨设 $A_1 \neq 0$，则令 $c_i = \frac{A_i}{A_1}$，$\sum c_j x_j = 0$.

$g \in G$ 作用在 A_i 上… $\Rightarrow$ A_i 乘上 ± 1 $\Rightarrow$ $c_i \in \mathrm{Inv}(G)$.

定义 $\mathbb{E}/\mathbb{F}$ 域扩张，称为Galois扩张，如果它是正规可分扩张.

回到引理2 (1)：

定理1 $\mathbb{E}/\mathbb{F}$ 有限扩张，则 $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E}:\mathbb{F}]$（$|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = |\mathrm{Gal}(\mathbb{E}/\mathbb{F})|$）

$\Leftrightarrow$ $\mathbb{E}/\mathbb{F}$ 是 Galois扩张

证明：$\mathrm{Aut}_{\mathbb{F}}\mathbb{E} \xrightarrow{T} \mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \overline{\mathbb{F}})$

$\sigma \longmapsto T(\sigma): x \longmapsto \sigma(x) \in \mathbb{E} \subseteq \overline{\mathbb{F}}$

T 是单射，T 是满射 $\Leftrightarrow$ $\forall \tau: \mathbb{E} \to \overline{\mathbb{F}}$，$\tau|_{\mathbb{F}} = id$，$\tau(\mathbb{E}) = \mathbb{E}$

$\Leftrightarrow$ $\mathbb{E}/\mathbb{F}$ 是正规扩张. $|\mathrm{Aut}_{\mathbb{F}}\mathbb{E}| = |\mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \overline{\mathbb{F}})|$

$|\mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \overline{\mathbb{F}})| = [\mathbb{E}:\mathbb{F}]$ $\Leftrightarrow$ $\mathbb{E}/\mathbb{F}$ 是可分扩张.

定理2. 设 $\mathbb{E}/\mathbb{F}$ 有限扩张，$\mathbb{E}/\mathbb{F}$ 是Galois扩张 $\Leftrightarrow$ 存在可分多项式 $f(x) \in \mathbb{F}[x]$，$\mathbb{E}$ 是 $f(x)$ 在 $\mathbb{F}$ 上分裂域.

证明："$\Rightarrow$" $\mathbb{E}/\mathbb{F}$ 有限可分，则它是单扩张，$\mathbb{E} = \mathbb{F}(\theta)$.

设θ的极小多项式为$f(x)$. 因为θ是可分元，$f(x)$是可分多项式. 因为$\mathbb{E}/\mathbb{F}$正规，$f(x)$所有根属于$\mathbb{E}$. 从而$\mathbb{E}$是$f(x)$在$\mathbb{F}$上分裂域.

"$\Leftarrow$" 设$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$ $c,\alpha_1,\cdots,\alpha_n\in\mathbb{E}$

则$\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_n)$ 因为$f(x)$可分$\Rightarrow\alpha_1,\cdots,\alpha_n$是$\mathbb{F}$上可分元，则$\mathbb{E}$是$\mathbb{F}$的有限可分扩张. 从而是Galois扩张.

注：这个定理展示从基域$\mathbb{F}$如何生成所有的有限Galois扩张.

定理3. 设$\mathbb{E}/\mathbb{F}$有限扩张，$\mathbb{E}/\mathbb{F}$是Galois扩张$\Leftrightarrow$存在$\mathrm{Aut}(\mathbb{E})$的有限子群G, $\mathbb{F}=\mathrm{Inv}(G)$, $(G=\mathrm{Gal}(\mathbb{E}/\mathbb{F}))$

证明："$\Rightarrow$"令$G=\mathrm{Aut}_{\mathbb{F}}(\mathbb{E})=\mathrm{Gal}(\mathbb{E}/\mathbb{F})$，因为$|\mathrm{Gal}(\mathbb{E}/\mathbb{F})|=[\mathbb{E}:\mathbb{F}]$ ($\mathbb{E}$是$\mathbb{F}$上有限可分扩张)，则$\mathrm{Gal}(\mathbb{E}/\mathbb{F})$有限子群，令$\mathbb{F}'=\mathrm{Inv}(G)$, $\mathbb{F}\subseteq\mathbb{F}'\subseteq\mathbb{E}$，因为$\mathbb{E}$是$\mathbb{F}$的可分扩张，它也是$\mathbb{F}'$的可分扩张$\Rightarrow|\mathrm{Gal}(\mathbb{E}/\mathbb{F}')|=[\mathbb{E}:\mathbb{F}']$

由Artin引理，$[\mathbb{E}:\mathbb{F}']=|G|=[\mathbb{E}:\mathbb{F}]\Rightarrow\mathbb{F}=\mathbb{F}'$

"$\Leftarrow$" 设$\alpha\in\mathbb{E}$，在G作用下轨道为$G.\alpha$, $|G.\alpha|=m$.

$\{\sigma_1\alpha=\alpha, \sigma_2\alpha, \cdots, \sigma_m\alpha\}$是$G.\alpha$中全部互异元素 $\sigma_i\in G$.

$\forall\tau\in G$, $\{\tau\sigma_1\alpha, \cdots, \tau\sigma_m\alpha\}$是$\{\sigma_1\alpha, \cdots, \sigma_m\alpha\}$的重排.

令 $f_\alpha(x)=(x-\sigma_1\alpha)(x-\sigma_2\alpha)\cdots(x-\sigma_m\alpha)\in\mathbb{E}[x]$.

$\forall\tau\in G$, $(\tau f_\alpha)(x)=f_\alpha(x)$ 即$f_\alpha(x)$是τ-不变的.

即$f_\alpha(x)$的系数是τ-不变的, $\Rightarrow f_\alpha(x)\in\mathbb{F}[x]$且无重根

$\Rightarrow\alpha$在$\mathbb{F}$上极小多项式$P_\alpha(x)$是可分的$(P_\alpha(x)\mid f_\alpha(x))$.

$\Rightarrow\alpha$是$\mathbb{F}$上可分元 $\Rightarrow\mathbb{E}$是$\mathbb{F}$的有限可分扩张.

$P_\alpha(x)$在$\mathbb{E}$中分裂 $\Rightarrow\mathbb{E}$是$\mathbb{F}$的正规扩张.

注: 这个定理从任一域$\mathbb{E}$构造子域$\mathbb{F}$, 使得$\mathbb{E}/\mathbb{F}$是Galois扩张. 设$\mathbb{E}/M/\mathbb{F}$域扩张, $\mathbb{E}/\mathbb{F}$有限Galois扩张 $\Rightarrow M/\mathbb{F}$有限Galois扩张

Galois理论基本定理

定理 设$\mathbb{E}/\mathbb{F}$有限Galois扩张, $G=\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, 则有如下一一对应

$$\Gamma=\{G\text{的子群}\}\ \underset{\mathrm{Gal}(\mathbb{E}/\ )}{\overset{\mathrm{Inv}}{\rightleftarrows}}\ \{\mathbb{F}\subseteq\mathbb{E}\text{的中间域}\ \mathbb{L}\}=\Sigma$$

满足: (1) Inv, $\mathrm{Gal}(\mathbb{E}/\ )$互逆

(2) $G_1\subseteq G_2$, $G_1,G_2\in\Gamma\iff\mathrm{Inv}\,G_1\supseteq\mathrm{Inv}\,G_2\in\Sigma$

(3) $\mathrm{Inv}(G_1\cup G_2)=\mathrm{Inv}(G_1)\cap\mathrm{Inv}(G_2)$

$\mathrm{Inv}(G_1\cap G_2)=(\mathrm{Inv}(G_1))\cdot(\mathrm{Inv}(G_2))$

其中 $G_1\cup G_2$ 是 G_1, G_2 生成的 G 的子群.

(4) $G_1 \lhd G \Leftrightarrow \mathrm{Inv}G_1/\mathbb{F}$ 是有限Galois扩张，此时

$$G/G_1 \cong \mathrm{Gal}(\mathrm{Inv}G_1/\mathbb{F}).$$

证明：(1) 若 $\mathbb{E}/\mathbb{F}$ 有限Galois扩张，由定理3，$G=\mathrm{Gal}(\mathbb{E}/\mathbb{F})$

$\mathbb{F}=\mathrm{Inv}G$. 反之，给定 $G \overset{\text{有限}}{\le} \mathrm{Aut}(\mathbb{E})$，$\mathrm{Inv}(G)=\mathbb{F}$

由定理3，$\mathbb{E}/\mathbb{F}$ 有限Galois扩张，$\mathrm{Gal}(\mathbb{E}/\mathbb{F})=G$.

因此，$\mathrm{Gal}(\mathbb{E}/\ )$ 和 Inv 在 Γ 和 Σ 之间互逆（$\mathbb{E}/M/\mathbb{F}$，$\mathbb{E}/\mathbb{F}$ Galois $\Rightarrow$ $\mathbb{E}/M$ Galois）.

(3) 由(2)可得

(4) $G_1 \lhd G \Leftrightarrow \forall g\in G,\ g^{-1}G_1 g = G_1 \quad \forall \sigma\in G$

$\Updownarrow$

$\mathrm{Inv}G_1 \qquad \sigma(\mathrm{Inv}G_1)=\mathrm{Inv}G_1 \quad \forall\sigma\in G.$

这里 $\sigma(\mathrm{Inv}G_1)=\mathrm{Inv}(\sigma G_1\sigma^{-1})$.

因为 $\mathbb{E}/\mathbb{F}$ 正规扩张，$G=\mathrm{Gal}(\mathbb{E}/\mathbb{F})=\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})$ $\forall \tau\in$ $\mathrm{Hom}_{\mathbb{F}}(\mathrm{Inv}G_1,\overline{\mathbb{F}})$，$\tau$ 可扩充为某一个 $\sigma:\mathbb{E}\to\overline{\mathbb{F}}$，$\sigma|_{\mathbb{F}}=id$

$$\begin{tikzcd}
\mathrm{Inv}G_1 \arrow[r, "\tau"] \arrow[d, phantom, "\subseteq" rotate=-90] & \overline{\mathbb{F}} \\
\mathbb{E} \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

$\tau(\mathrm{Inv}\,G_1) = \sigma(\mathrm{Inv}\,G_1) = \mathrm{Inv}\,G_1$

即 $\mathrm{Inv}\,G_1$ 保持 $\mathbb{F}$-共轭元 $\Rightarrow$ $\mathrm{Inv}(G_1)$ 是 $\mathbb{F}$ 的正规扩张

$\mathbb{E}/\mathbb{F}$ 可分 $\Rightarrow$ $\mathrm{Inv}(G_1)/\mathbb{F}$ 可分. $\Rightarrow$ $\mathrm{Inv}(G_1)/\mathbb{F}$ 有限Galois扩张

反之，若 $\mathbb{L} \subseteq \mathbb{E}$，$\mathbb{L}$ 是 $\mathbb{F}$ 的有限Galois扩张.

$\forall \tau \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{L}, \overline{\mathbb{F}})$，$\tau(\mathbb{L}) = \mathbb{L}$ 　特别地，给定 $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$

$\mathrm{Hom}_{\mathbb{F}}(\mathbb{L}, \overline{\mathbb{F}}) = \mathrm{Aut}_{\mathbb{F}}\mathbb{L}$

$\sigma|_{\mathbb{L}} \in \mathrm{Aut}_{\mathbb{F}}\mathbb{L}$

$\mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \overline{\mathbb{F}})$. $\mathrm{Hom}_{\mathbb{F}}(\mathbb{L}, \overline{\mathbb{F}})$

即 $\mathrm{Aut}_{\mathbb{F}}\mathbb{E} \xrightarrow{\varphi} \mathrm{Aut}_{\mathbb{F}}\mathbb{L}$.

$\sigma \longmapsto \sigma|_{\mathbb{L}}$

$\mathrm{Ker}\,\varphi = \{\sigma \mid \sigma|_{\mathbb{L}} = id\} = \mathrm{Aut}_{\mathbb{L}}(\mathbb{E}) \lhd \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$

$$\Rightarrow \frac{\mathrm{Aut}_{\mathbb{F}}\mathbb{E}}{\mathrm{Aut}_{\mathbb{L}}\mathbb{E}} \xrightarrow{\sim} \mathrm{Aut}_{\mathbb{F}}\mathbb{L}$$

注：$\mathbb{E}/\mathbb{F}$ 是有限Galois扩张 $\Rightarrow$ $\mathbb{E}/\mathbb{L}$ 是有限Galois扩张

$\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$ 　　$\mathbb{L}/\mathbb{F}$ 可分扩张

例1. 设 $\mathbb{E}$ 是 $\mathbb{Q}$ 上 x^5-2 的分裂域 $\mathbb{E} = \mathbb{Q}(\sqrt[5]{2}, \xi)$ $\xi = e^{\frac{2\pi i}{5}}$

$[\mathbb{E}:\mathbb{Q}] = 20$，$\mathrm{char}\,\mathbb{Q} = 0$ $\Rightarrow$ $\mathbb{E}$ 是 $\mathbb{Q}$ 的Galois扩张.

$\forall \sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$，$\sigma(\sqrt[5]{2})$ 仍是 $x^5-2=0$ 的根

$\sigma(\xi)$ 仍是 $x^4+x^3+x^2+x+1=0$ 的根

$\alpha_1 = \sqrt[5]{2}$，$\alpha_2 = \sqrt[5]{2}\xi$，$\cdots$，$\alpha_5 = \sqrt[5]{2}\xi^4$：$x^5-2=0$ 的5个根

令 $r: \sqrt[5]{2} \longmapsto \sqrt[5]{2}\xi$ $\quad$ $s: \sqrt[5]{2} \longmapsto \sqrt[5]{2}$

$\xi \longmapsto \xi$ $\quad$ $\xi \longmapsto \xi^2$

我们得到 $\underbrace{Gal(\mathbb{E}/\mathbb{Q})}_{=G}$ 的三个子群：$\langle r\rangle = G_1$，$\langle s\rangle = G_2$，$\langle s^2\rangle = G_3$

$G \leqslant S_5$（$x^5-2=0$ 的5个根置换）

① $G_1 = \langle(12345)\rangle$ $\quad$ $[\mathrm{Inv}G_1 : \mathbb{Q}] = Gal(\mathrm{Inv}G_1/\mathbb{Q}) \cong G/G_1$

$\Rightarrow [\mathrm{Inv}G_1 : \mathbb{Q}] = 4$. 显然 $\mathbb{Q}(\xi) \subseteq \mathrm{Inv}\,G_1$

$\Rightarrow \mathrm{Inv}G_1 = \mathbb{Q}(\xi)$

② $G_2 = \langle(2354)\rangle$ $\quad$ $[\mathrm{Inv}G_2 : \mathbb{Q}] = G/G_2 = 5$，$\mathbb{Q}(\sqrt[5]{2}) \subseteq \mathrm{Inv}G_2$

$\Rightarrow \mathrm{Inv}\,G_2 = \mathbb{Q}(\sqrt[5]{2})$

③ $G_3 = \langle(25)(34)\rangle$ $\quad$ $[\mathrm{Inv}G_3 : \mathbb{Q}] = G/G_3 = 10$

显然 $\mathrm{Inv}\,G_2 \subseteq \mathrm{Inv}\,G_3$ $\quad$ $\mathrm{Inv}G_3 = \mathbb{Q}(\sqrt[5]{2}, x_0)$ 求 $x_0=$?

$x_0 \notin \mathbb{Q}(\sqrt[5]{2})$，且 $[\mathbb{Q}(x_0):\mathbb{Q}]=2$. x_0 满足一个 $\mathbb{Q}$ 上2次多项式

因为 $(25)(34)$ 固定了 $\alpha_2+\alpha_5$ 和 α_1 因此 $x_0 = \dfrac{\alpha_2+\alpha_5}{\alpha_1}$

$= \xi+\xi^4$ 它是 $x^2+x-1=0$ 的根 $\Rightarrow \mathrm{Inv}(G_3) = \mathbb{Q}(\sqrt[5]{2}, \xi+\xi^4)$

注：$G = Gal(\mathbb{E}/\mathbb{Q})$ 的全部元素

$G_{(a,b)}: \sqrt[5]{2} \longmapsto \sqrt[5]{2}\xi^a$, $\xi \longmapsto \xi^b$ $\quad$ $a=0,1,\cdots,4$
$b=1,2,\cdots,4$

$G = \langle r\rangle \rtimes \langle s\rangle$ 半直积 $\quad$ $\langle r\rangle \lhd G$,

一般地，设 p 素数，$x^p-2\in\mathbb{Q}[x]$，它的根是 $\sqrt[p]{2}\xi^i$，$i=0,1,\cdots,p-1$. 设 $\mathbb{E}$ 是 x^p-2 在 $\mathbb{Q}$ 上分裂域. 令 $G=Gal(\mathbb{E}/\mathbb{Q})$

$\forall\sigma\in G$，$\mathbb{E}\longrightarrow\mathbb{E}=\mathbb{Q}(\sqrt[p]{2},\xi)$　$\sigma(\sqrt[p]{2}\xi^i)$ 仍是 x^p-2 的根

σ 是根的重排. $G\subseteq S_p$，$\alpha_1=\sqrt[p]{2}$，$\alpha_2=\sqrt[p]{2}\xi$，$\cdots$，$\alpha_p=\sqrt[p]{2}\xi^{p-1}$

σ 完全由 $\sqrt[p]{2}$ 和 ξ 的像决定，$\sigma(\xi)$ 仍是 x^p-1 的根.

$\Rightarrow$ G 中元素：$\sigma_{(a,b)}:\sqrt[p]{2}\longmapsto\sqrt[p]{2}\xi^a$，$\xi\longmapsto\xi^b$，$a\in\mathbb{Z}_p$，

$b\in\mathbb{Z}_p^*$，$|G|=p(p-1)$. $\sigma_{(a,b)}\circ\sigma_{(c,d)}(\xi)=\xi^{bd}$

$\sigma_{(a,b)}\circ\sigma_{(c,d)}(\sqrt[p]{2})=\sqrt[p]{2}\xi^{\cancel{k+lm}\,a+bc}$

$\Rightarrow\sigma_{(a,b)}\circ\sigma_{(c,d)}=\cancel{\sigma_{k+lm,\,ln}}\ \sigma_{a+bc,bd}$

定义 $G\xrightarrow{\Phi}\left\{\begin{pmatrix}x&y\\0&1\end{pmatrix}\middle|\ x,y\in\mathbb{Z}_p,\ x\neq\bar{0}\right\}$

$$\sigma_{(a,b)}\longmapsto\begin{pmatrix}b&a\\0&1\end{pmatrix}$$

$\begin{pmatrix}b&a\\0&1\end{pmatrix}\cdot\begin{pmatrix}d&c\\0&1\end{pmatrix}=\begin{pmatrix}bd&a+bc\\0&1\end{pmatrix}$　即 Φ 是群同构.

常用结论

1. (Generalized Main extension lemma)

设K/M是代数扩张，$L=\overline{M}$是M的代数闭包，则对于$\forall \sigma: M \to L$域同态，存在$\sigma': K \to L$使得$\sigma'|_M=\sigma$

如下图：

$$\begin{tikzcd}
M \arrow[r, "\subseteq"] \arrow[dr, "\sigma"'] & K \arrow[d, dashed, "\exists \sigma'"] \\
 & L=\overline{M}
\end{tikzcd}$$

证明：设$\Omega=\{(\mathbb{E},\varphi) \mid M\subseteq \mathbb{E}\subseteq K,\ \varphi: \mathbb{E}\to L$ 满足 $\varphi|_M=\sigma\}$

定义偏序 $(\mathbb{E},\varphi)\leq(\mathbb{E}',\varphi') \Leftrightarrow \mathbb{E}\subseteq\mathbb{E}',\ \varphi'|_{\mathbb{E}}=\varphi$.

$\Omega\neq\phi$ 因为$(M,\sigma)\in\Omega$. 任意一个链$\{(\mathbb{E}_i,\varphi_i)\in\Omega \mid (\mathbb{E}_i,\varphi_i)\leq(\mathbb{E}_{i+1},\varphi_{i+1})\}$有上界$(\bigcup \mathbb{E}_i,\varphi)$ φ定义为：

$\forall \alpha\in\bigcup\mathbb{E}_i$ $\exists i$, $\alpha\in\mathbb{E}_i$, $\varphi(\alpha)=\varphi_i(\alpha)$, 由Zorn引理，$\Omega$有极大元$(\mathbb{E},\sigma')$，若$\mathbb{E}\neq K$，则存在$\beta\notin\mathbb{E}$, $\beta\in K$, $\mathbb{E}\xrightarrow{\sigma'}L$ 可扩充为$\mathbb{E}(\beta)\xrightarrow{\tilde{\sigma}'}L$，则$(\mathbb{E},\sigma)\lneq(\mathbb{E}(\beta),\tilde{\sigma}')$ 与极大性矛盾！因此$\mathbb{E}=K$，且$K\xrightarrow{\sigma'}L$ $\sigma'|_M=\sigma$.

注：(1) 我们通常只处理K/M是有限扩张，可以不用Zorn引理.

(2) $Hom(K,L)\longrightarrow Hom(M,L)$是一个满射

2. $K/\mathbb{F}$ 代数扩张，则 $\overline{K}=\overline{\mathbb{F}}$.（代数闭包）

3. 由1. 设 $K/\mathbb{F}$ 代数扩张，$\mathbb{E}/\mathbb{F}$ 代数扩张，$\mathbb{F}\subseteq K\subseteq\mathbb{E}$

则有 $\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})\xrightarrow{\Phi}\mathrm{Hom}_{\mathbb{F}}(K,\overline{\mathbb{F}})$ 是满射

$\sigma\longmapsto\sigma|_K$

$\forall\,\tau_1,\tau_2\in\mathrm{Hom}_{\mathbb{F}}(K,\overline{\mathbb{F}})$，$\Phi^{-1}(\tau_1)$ 和 $\Phi^{-1}(\tau_2)$ 一一对应.

的确，设 $\tau_1=id_K$（即 $K\subseteq\overline{\mathbb{F}}$），$\tau_2=\tau$，设 $\sigma\in\Phi^{-1}(\tau)$

若 $\sigma'\in\Phi^{-1}(\tau)$，则 $\sigma'\sigma^{-1}|_K=id\Rightarrow\sigma'\sigma^{-1}\in\Phi^{-1}(\tau_1)$

$$\Phi^{-1}(\tau_1)\longrightarrow\Phi^{-1}(\tau_2)$$

$$f\longmapsto\sigma\circ f$$

$\Phi^{-1}(\tau_1)=\Phi^{-1}(id_K)=\{\sigma:\mathbb{E}\to\overline{\mathbb{F}}\mid\sigma|_K=id_K\}=\mathrm{Hom}_K(\mathbb{E},\overline{\mathbb{F}})$

特别地，若 $\mathbb{F}\subseteq K\subseteq\mathbb{E}$ 均是有限扩张.

$$|\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|=|\mathrm{Hom}_K(\mathbb{E},\overline{\mathbb{F}})|\cdot|\mathrm{Hom}_{\mathbb{F}}(K,\overline{\mathbb{F}})|.\quad(*)$$

4. 使用3中 $(*)$，关于阶数归纳，得：若 $\mathbb{E}/\mathbb{F}$ 有限扩张，

$|\mathrm{Hom}_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|\leq[\mathbb{E}:\mathbb{F}]$ 等号成立 $\Leftrightarrow$ $\mathbb{E}/\mathbb{F}$ 可分扩张.

特别地 $|\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}(\alpha),\overline{\mathbb{F}})|\leq\deg P_\alpha(x)$ ← α 在 $\mathbb{F}[x]$ 中极小多项式

5. 设 $\mathbb{F}\subseteq\mathbb{L}\subseteq\mathbb{E}$ 代数扩张，则 $\mathbb{E}/\mathbb{F}$ 可分扩张 $\Leftrightarrow$ $\mathbb{L}/\mathbb{F}$，$\mathbb{E}/\mathbb{L}$ 均可分扩张.

"⇒" 容易验证.

"⇐" $\forall \alpha\in\mathbb{E}$, α在$\mathbb{L}$上极小多项式为 $P_{\mathbb{L}}(x)=P_nx^n+\cdots+P_1x+P_0$

令 $\mathbb{L}'=\mathbb{F}(P_0,P_1,\cdots,P_n)$, 则有 $\mathbb{F}\subseteq\mathbb{L}'\subseteq\mathbb{L}'(\alpha)$ 均有限扩张

$\mathbb{E}/\mathbb{L}$ 可分 $\Rightarrow$ $\mathbb{L}'(\alpha)/\mathbb{L}'$ 可分, $\mathbb{L}/\mathbb{F}$ 可分 $\Rightarrow$ $\mathbb{L}'/\mathbb{F}$ 可分

$[\mathbb{L}'(\alpha):\mathbb{F}]=[\mathbb{L}'(\alpha):\mathbb{L}'][\mathbb{L}':\mathbb{F}]=|Hom_{\mathbb{L}'}(\mathbb{L}'(\alpha),\overline{\mathbb{F}})|\cdot|Hom_{\mathbb{F}}(\mathbb{L}',\overline{\mathbb{F}})|$

由~~4~~3. 右边 $=|Hom_{\mathbb{F}}(\mathbb{L}'(\alpha),\overline{\mathbb{F}})|$ 再由4, $\mathbb{L}'(\alpha)/\mathbb{F}$ 可分扩张.

6. $\mathbb{E}/\mathbb{F}$ 代数扩张, $\mathbb{E}$是$\mathbb{F}$上正规扩张 $\Leftrightarrow$ $\forall\sigma\in Hom_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})$

$\sigma(\mathbb{E})=\mathbb{E}$.

"⇒" $\forall\alpha\in\mathbb{E}$, α在$\mathbb{F}$上极小多项式为$p(x)$, 则$p(x)$所有根落在$\mathbb{E}$中, $\sigma(\alpha)$是$\sigma(p(x))=p(x)$的根 $\Rightarrow\sigma(\alpha)\in\mathbb{E}\Rightarrow\sigma(\mathbb{E})\subseteq\mathbb{E}$.

又$\mathbb{E}$是分裂域 $\Rightarrow\mathbb{E}\subseteq\sigma(\mathbb{E})$

"⇐" 设α,β是$p(x)\in\mathbb{F}[x]$(不可约)的两根, $\alpha\in\mathbb{E}$, 存在$\sigma\in Hom_{\mathbb{F}}(\mathbb{F}(\alpha),\overline{\mathbb{F}})$

$\sigma(\alpha)=\beta$, 由1. σ可扩展为$\tilde{\sigma}\in Hom(\mathbb{E},\overline{\mathbb{F}})$. $\tilde{\sigma}(\alpha)=\beta$

但$\tilde{\sigma}(\mathbb{E})=\mathbb{E}\Rightarrow\beta\in\mathbb{E}$.