§5.3 伽罗瓦对应

F为域，$f\in F[X]\setminus F$　K为f在F上的分裂域

$Aut(K/F)=\{\varphi: K\to K \text{ 自同构} \mid \varphi|_F=id\}$

记作 $Aut(K/F)$

BAⅢ P171 推论2 $\Rightarrow |Aut(K/F)|\le [K:F]\le \deg f!$

当f无重根时，$|Aut(K/F)|=[K:F]$.

设$F\subseteq L\subseteq K$为中间域，则 $Aut(K/L)\le Aut(K/F)$为子群

设$H\le Aut(K/F)$为子群 定义：$K^H:=\{\alpha\in K\mid \varphi(\alpha)=\alpha\ \forall \varphi\in H\}$

则 K^H为中间域：$\forall \alpha\in F,\ \varphi\in H,\ \varphi(\alpha)=\alpha \Rightarrow F\le K^H$

$\forall \alpha_1,\alpha_2\in K^H$　$\forall \varphi\in H$，$\varphi(\alpha_1-\alpha_2)=\varphi(\alpha_1)-\varphi(\alpha_2)=\alpha_1-\alpha_2\Rightarrow \alpha_1-\alpha_2\in K^H$

$\varphi(\alpha_1\alpha_2)=\varphi(\alpha_1)\varphi(\alpha_2)=\alpha_1\alpha_2\Rightarrow \alpha_1\alpha_2\in K^H$

$\therefore K^H$为子环（含0,1）.

$\forall \alpha\in K^H$　$\varphi\in H$　$\varphi(\alpha^{-1})=(\varphi(\alpha))^{-1}=\alpha^{-1}\Rightarrow \alpha^{-1}\in K^H$　$\therefore K^H$为域

$K^{\cdot}:\{Aut(K/F)\text{的子群}\}\to\{\text{中间域}\}$，$Aut(K/\cdot):\{\text{中间域}\}\to\{Aut(K/F)\text{的子群}\}$

$H\longrightarrow K^H$　　$L\longrightarrow Aut(K/L)$

伽罗瓦对应：$K^{\cdot}$ 与 $Aut(K/\cdot)$ 均为双射 且互逆.

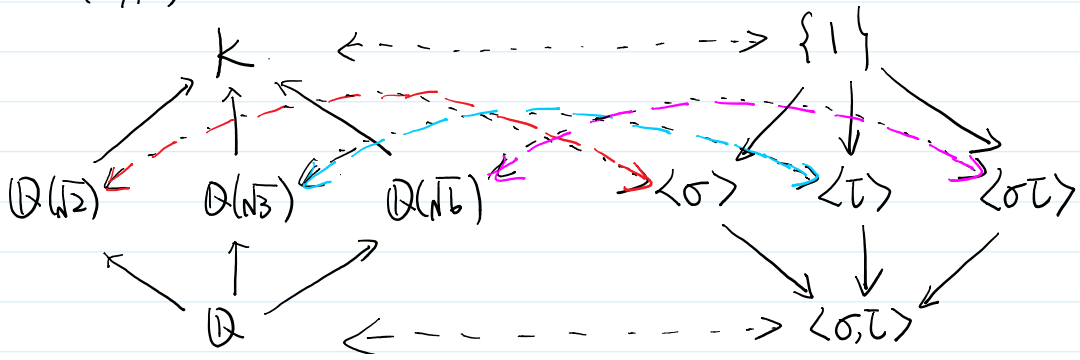
例1：$F=\mathbb{Q}$，$f=(x^2-2)(x^2-3)$　$K=\mathbb{Q}(\sqrt2,\sqrt3)$　$|Gal(K/F)|=4$

$\forall \varphi\in Aut(K/F)$　$\varphi(\sqrt2)=\pm\sqrt2$，$\varphi(\sqrt3)=\pm\sqrt3$

令 $\sigma\in Aut(K/F)$ s.t. $\sigma(\sqrt2)=\sqrt2$，$\sigma(\sqrt3)=-\sqrt3$

$\tau\in Aut(K/F)$ s.t. $\tau(\sqrt2)=-\sqrt2$　$\tau(\sqrt3)=\sqrt3$

则 $Aut(K/F)=\langle\sigma,\tau\rangle$



例2: $F=\mathbb{F}_p(t)$, t为未定元. K为$f=X^p-t$在F上的分裂域

设$\alpha\in K$ s.t $\alpha^p-t=0$. 则 $f=X^p-\alpha^p=(X-\alpha)^p \Rightarrow K=F(\alpha)$

$\forall \varphi\in Aut(K/F)$, $f(\varphi(\alpha))=0 \Rightarrow \varphi(\alpha)=\alpha \Rightarrow \varphi=id \Rightarrow Aut(K/F)=\{id\}$.

性质: 1) $H_1\subseteq H_2\subseteq Aut(K/F)$为子群 $\Rightarrow K^{H_2}\subseteq K^{H_1}$

2) $F\subseteq L_1\subseteq L_2\subseteq K$为中间域 $\Rightarrow Aut(K/L_2)\subseteq Aut(K/L_1)$

3) 设E为中间域 则 $E\subseteq K^{Aut(K/E)}$

4) 设$H\subseteq Aut(K/F)$为子群. 则 $H\subseteq Aut(K/K^H)$.

定义: 代数扩张K/F称为正规扩张, 若对$\forall$不可约$f\in F[X]\setminus F$. 如果f在K中有根

则f的所有根都在K中, 即 $f=\lambda(X-\alpha_1)\cdots(X-\alpha_m)$. $\lambda\in F$, $\alpha_1,\cdots\alpha_m\in K$, $m=\deg f$

或 K中含f在F上的分裂域

命题0: 设K/F为域扩张. 则 K/F为$f\in F[X]\setminus F$在F上的分裂域 $\Leftrightarrow$ K/F为有限正规扩张.

称可分正规扩张为伽罗瓦扩张.

设K/F为伽罗瓦扩张, 记 $Gal(K/F):=Aut(K/F)$称为K/F的伽罗瓦群.

进一步, 若K为f在F上的分裂域 也记 $Aut(K/F)$为$Gal(f)$

引理1 (Artin): 设K为域, $H\subseteq Aut(K)$为有限子群, $F=K^H$.

则 $[K:F]\leq |H|$.

证: 令 $n=|H|$. 设$\alpha_1,\cdots\alpha_m\in K$, $m>n$. 我们将证$\alpha_1,\cdots\alpha_m$在F上线性相关. 设 $H=\{\varphi_1,\cdots\varphi_n\}$. 考虑方程:

$$(*)\quad \sum_{j=1}^{m}\varphi_i(\alpha_j)X_j=0 \qquad i=1,\cdots,n.$$

$\because m>n$ $\therefore$ $(*)$有非零解.

在$(*)$的解空间中取非零解$(b_1,\cdots b_m)$ s.t. 其非0分量个数最小.

不妨设$b_1\neq 0$. 除以b_1后得$(1,\tilde{b_2},\cdots\tilde{b_m})$为$(*)$的非0解且非0分量个数依然最小.

下证 $\forall \tilde{b_i}\in F$. ($1=\tilde{b_1}$)

(反证) 设$\exists \tilde{b_{i_0}}\notin F$. 则$\exists\varphi\in H$ s.t. $\varphi(\tilde{b_{i_0}})\neq\tilde{b_{i_0}}$.

$\varphi\left(\sum_{j=1}^{m}\varphi_i(\alpha_j)\widetilde{b_j}\right)=0 \Rightarrow \varphi\varphi_i(\alpha_1)+\sum_{j=2}^{m}\varphi\varphi_i(\alpha_j)\varphi(\widetilde{b_j})=0$. $\forall 1\le i\le n$.

$\because \{\varphi\varphi_i \mid 1\le i\le n\}=H$ $\therefore$ 有 $\varphi_i(\alpha_1)+\sum_{j=2}^{m}\varphi_i(\alpha_j)\varphi(\widetilde{b_j})=0$

$\varphi_i(\alpha_1)+\sum_{j=2}^{m}\varphi_i(\alpha_j)\widetilde{b_j}=0$

$\Rightarrow \sum_{j=2}^{m}\varphi_i(\alpha_j)(\widetilde{b_j}-\varphi(\widetilde{b_j}))=0 \quad \forall 1\le i\le n$.

$\therefore (0,\widetilde{b_2}-\varphi(\widetilde{b_2}),\cdots\widetilde{b_{i_0}}-\varphi(\widetilde{b_{i_0}}),\cdots\widetilde{b_m}-\varphi(\widetilde{b_m}))$ 为 $(*)$ 的非0解

且其非0分量个数 $<(b_1,\cdots b_m)$ 的非0分量个数. 矛盾.

取 $\varphi_i=1$, 则 $\sum_{j=1}^{n}\alpha_j\widetilde{b_j}=0 \Rightarrow \alpha_1,\cdots\alpha_m$ F-线性相关

$\therefore [K:F]\le n=|H|$. □

定理: 设 K/F 为域扩张.

1) K 为某个可分多项式 f 在 F 上的分裂域

2) $F=K^{Aut(K/F)}$ 且 $|Aut(K/F)|<+\infty$

3) K/F 为有限伽罗瓦扩张.

进而当(3)成立时有 $[K:F]=|Gal(K/F)|$.

证: 1) $\Rightarrow$ 2). 记 $f=f_1^{m_1}\cdots f_s^{m_s}$ f_i 为互异的不可约因子. 令 $\underline{f}=f_1\cdots f_s$.

则 K 为 $\underline{f}$ 在 F 上的分裂域且 $\underline{f}$ 可分.

令 $\widetilde{F}=K^{Aut(K/F)}$ 则 $F\subseteq\widetilde{F}$. 且 $Aut(K/F)\subseteq Aut(K/\widetilde{F})\subseteq Aut(K/F)$

$\therefore Aut(K/F)=Aut(K/\widetilde{F})$

$\because \underline{f}$ 可分 $\therefore \underline{f}$ 无重根 由§5.1推论2知:

$[K:F]=|Aut(K/F)|=|Aut(K/\widetilde{F})|=[K:\widetilde{F}]$

$\Rightarrow F=\widetilde{F}=K^{Aut(K/F)}$ 且 $|Aut(K/F)|<+\infty$

2) $\Rightarrow$ 3) 由引理1 $\Rightarrow [K:F]\le|Aut(K/F)|<+\infty \Rightarrow K/F$ 为有限扩张.

设 $g\in F[X]\setminus F$ 不可约且 g 在 K 中有根 α.

记 $\{\varphi(\alpha) \mid \varphi \in Aut(K/F)\} = \{\alpha_1 = \alpha, \alpha_2, \cdots \alpha_m\}$.

令 $g = (X-\alpha_1)\cdots(X-\alpha_m) = X^m + \sum_{i=0}^{m-1} c_i X^i$, $c_i \in K$.

$\forall \psi \in H$, $\because \{\psi(\alpha_i) \mid 1 \le i \le m\} = \{\alpha_1, \cdots \alpha_m\}$

$\therefore \psi(g) = X^m + \sum_{i=0}^{m-1} \psi(c_i) X^i = \prod_{i=1}^{m} (X - \psi(\alpha_i)) = \prod_{i=1}^{m} (X-\alpha_i) = g$

$\Rightarrow \forall \psi \in H$, $\forall 0 \le i \le m-1$, $\psi(c_i) = c_i \Rightarrow c_i \in F$ $\forall 0 \le i \le m-1$

$\therefore g \in F[X]$ $\therefore g \mid g \Rightarrow g$ 所有根在 K 中且无重根.

$\therefore K/F$ 是正规扩张.

$\forall \alpha \in K$, 则 α 在 F 上的极小多项式 f_α 不可约且在 K 中有根

$\therefore f_\alpha$ 在 K 中无重根 $\Rightarrow \alpha$ 在 F 上可分 $\Rightarrow K/F$ 为可分扩张.

3) $\Rightarrow$ 1) $[K:F] < +\infty \Rightarrow K = F(\alpha_1, \cdots \alpha_m)$ α_i 在 F 上代数且可分.

记 f_{α_i} 为 α_i 在 F 上的极小多项式, 则 f_{α_i} 的所有根在 K 中.

令 $f = \prod_{i=1}^{m} f_{\alpha_i}$. 则 f 可分且 f 的所有根在 K 中.

由定义知: K 为 f 在 F 上的分裂域 □

注: 定理1中的 2) 可替换为 2)': $\exists H \le Aut(K)$ 有限子群 s.t. $F = K^H$.

引理2: 设 K/F 为伽罗瓦扩张, $F \subseteq E \subseteq K$ 为中间域. 则 K/E 为伽罗瓦扩张.

证: 由定理1知 □

定义: 设 $F \subseteq K \subseteq L$ 为域扩张, $\varphi \in Aut(L/F)$. 称 $\varphi(K) = \{\varphi(\alpha) \mid \alpha \in K\}$ 为 K 的一个共轭域.

例: $F = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\varphi \in Aut(L/F)$ s.t. $\varphi(\sqrt{2}) = \sqrt{2}$, $\varphi(\sqrt{3}) = -\sqrt{3}$. 则 $\varphi(K) = \mathbb{Q}(\sqrt{2}-\sqrt{3})$ 与 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 共轭.

引理3: 设 K/F 为伽罗瓦扩张, $G = Gal(K/F)$, $E \in \Sigma$. 则

$Gal(K/E) \subseteq G$ 为正规子群 $\Leftrightarrow \forall \varphi \in G$, $\varphi(E) = E$ $\Leftrightarrow E/F$ 为正规扩张.

① ② ③

证: 由引理1, K/E 为有限伽罗瓦扩张 $\overset{\text{定理1}}{\Longrightarrow}$

设 $\varphi \in G$.

$\forall \psi \in Gal(K/E)$, $\varphi^{-1}\psi\varphi \in Gal(K/E) \Leftrightarrow \forall \psi \in Gal(K/E), \alpha \in E$ $\varphi^{-1}\psi\varphi(\alpha)=\alpha$

$\Leftrightarrow \forall \psi \in Gal(K/E), \alpha \in E$, $\psi(\varphi(\alpha))=\varphi(\alpha)$

$\Leftrightarrow \forall \alpha \in E$, $\varphi(\alpha) \in E$

$\Leftrightarrow \varphi(E)=E$

$\therefore$ ① $\Leftrightarrow$ ②

② $\Rightarrow$ ③: $\varphi(E)=E \Rightarrow \varphi|_E \in Aut(E/F)$

$\therefore F=K^G \supseteq E^{\{\varphi|_E \mid \varphi \in G\}} \supseteq E^{Aut(E/F)} \supseteq F \Rightarrow F=E^{Aut(E/F)}$

$\therefore E/F$ 为正规扩张

③ $\Rightarrow$ ② E/F 为正规 $\Rightarrow E/F$ 为伽罗瓦扩张 $\Rightarrow E$ 为可分 $f \in F[X]$ 在 F 上分裂域

即 $E=F(\alpha_1, \cdots \alpha_m)$, $\alpha_1, \cdots \alpha_m \in E$ 为 f 的所有根

$\forall \varphi \in G$, $f(\varphi(\alpha_i))=\varphi(f(\alpha_i))=0 \Rightarrow \varphi(\alpha_i) \in E$ $\forall 1 \le i \le m$

$\therefore \varphi(E)=E$ □

定理2 (伽罗瓦对应) 设 K/F 为有限伽罗瓦扩张, $\Gamma=\{Gal(K/F)$ 的子群$\}$

$\Sigma=\{$中间域 $E: F \subseteq E \subseteq K\}$. 则

1) $K: \Gamma \to \Sigma$, $H \to K^H$; $Gal(K/\cdot): \Sigma \to \Gamma$, $E \to Gal(K/E)$ 为互逆的双射.

2) $\forall H_1, H_2 \in \Gamma$, $H_1 \subseteq H_2 \Leftrightarrow K^{H_2} \subseteq K^{H_1}$

3) $\forall H \in \Gamma$, $|H|=[K:K^H]$, $[Gal(K/F):H]=[K^H:F]$

4) 设 $H \in \Gamma$, $H \subseteq Gal(K/F)$ 为正规子群 $\Leftrightarrow K^H/F$ 是正规的.

此时有: $Gal(K^H/F) \cong Gal(K/F)/H$.

证: 3) $\forall H \in \Gamma$, K/K^H 为有限伽罗瓦扩张 $\overset{定理1}{\Rightarrow} |Gal(K/K^H)|=[K:K^H]$

引理1 $\Rightarrow [K:K^H] \le |H| \le |Gal(K/K^H)|=[K:K^H]$

$\therefore |H|=[K:K^H]=|Gal(K/K^H)|$

特别地: $|Gal(K/F)|=[K:F] \Rightarrow [Gal(K/F):H]|H|=[K:K^H][K^H:F]$

$\Rightarrow [Gal(K/F):H] = [K^H:F]$

1) $\forall E \in \Sigma$, K/E 为有限伽罗瓦扩张 $\Rightarrow E = K^{Gal(K/E)}$

即 $K^{\cdot} \circ Gal(K/\cdot) = id_\Sigma$

$\forall H \in \Gamma$, $H \subseteq Gal(K/K^H)$, $|H| = |Gal(K/K^H)|$ $\Rightarrow H = Gal(K/K^H)$

即 $Gal(K/\cdot) \circ K^{\cdot} = id_\Gamma$

2) $\forall H_1, H_2$, $K^{H_1} \supseteq K^{H_2} \Rightarrow H_1 = Gal(K/K^{H_1}) \subseteq Gal(K/K^{H_2}) = H_2$

4) $\forall H \in \Gamma$, $K^H \in \Sigma$ 且 $H = Gal(K/K^H)$

由引理3知：H 正规 $\Leftrightarrow K^H/F$ 为正规扩张.

设 H 正规，则 $\forall \varphi \in Gal(K/F)$, $\varphi(K^H) = K^H$ (引理3)

定义：$\Psi: Gal(K/F) \longrightarrow Gal(K^H/F)$

$\varphi \longrightarrow \varphi|_{K^H}$

$\ker\Psi = \{\varphi \in Gal(K/F) \mid \varphi|_{K^H} = id\} = \{\varphi \in Gal(K/K^H)\} = Gal(K/K^H) = H$.

另外：$[Gal(K/F):H] = [K^H:F] = |Gal(K^H/F)|$

$\therefore |Gal(K/F)/H| = |Gal(K/F)| \Rightarrow Gal(K/F)/H \cong Gal(K^H/F)$. □

应用：分圆域 $\mathbb{Q}(\zeta)$ 之伽罗瓦群 (先假设 x^n 不可约)

设 ζ 为 n 次本原根，则 $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z})$

$\forall \varphi \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) = G$, $\varphi(\zeta) = \zeta^{m_\varphi}$ ∵ $x^n(\varphi(\zeta)) = 0 \Rightarrow \zeta^{m_\varphi}$ 为 n 次本原根.

$\Leftrightarrow \exists\, 0 < l < n$ s.t. $\zeta^{m_\varphi l} = \zeta$

$\Leftrightarrow l m_\varphi \equiv 1 \mod n$.

$\Leftrightarrow m_\varphi + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$

$\therefore \Psi: G \longrightarrow U(\mathbb{Z}/n\mathbb{Z})$

$\varphi \longrightarrow m_\varphi + n\mathbb{Z}$

$\varphi_1\varphi_2(\zeta) = \varphi_1(\zeta^{m_{\varphi_2}}) = \zeta^{m_{\varphi_1}m_{\varphi_2}} \Rightarrow \psi(\varphi_1\varphi_2) = \psi(\varphi_1)\psi(\varphi_2)$

$\therefore \psi$ 为群同态　　若 $m_\varphi + n\mathbb{Z} = 1 + n\mathbb{Z} \Rightarrow \varphi(\zeta) = \zeta \Rightarrow \varphi = id$

$\therefore \psi$ 为单射　　$\because [\mathbb{Q}(\zeta):\mathbb{Q}] = \deg \Phi_n = \varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$

$\therefore \psi$ 为双射.

尺规作图：

直尺（无刻度），圆规

C1：从 P 与 Q 两点，画过 P, Q 的直线

C2：从 P 与 Q，O 出发，画以 O 为圆心，|PQ| 为半径的圆.

P1：由 C1 所画的两条不同直线的交点.

P2：由 C1, C2 所画直线与圆的交点.

P3：由 C2 所画的两个不同圆的交点.

可构造点：从已有点出发利用 C1, C2 所画图形的交点（P1, P2 或 P3）.

初始设置：(0,0), (0,1)

$\mathbb{C} \longleftrightarrow \mathbb{R}^2$　　$\alpha = a + b\sqrt{r}$ 为可构造数 若 (a, b) 为可构造点.

$a + b\sqrt{r} \longrightarrow (a, b)$.

$\mathcal{C} := \{\alpha \in \mathbb{C} \mid \alpha$ 为可构造数$\}$.

命题：$\mathcal{C}$ 为 $\mathbb{C}$ 子域 且有 1) $\alpha + \beta\sqrt{r} \in \mathcal{C} \Leftrightarrow \alpha, \beta \in \mathcal{C}$

2) $\alpha \in \mathcal{C} \Rightarrow \sqrt{\alpha} \in \mathcal{C}$

定理：设 $\alpha \in \mathbb{C}$ 在 $\mathbb{Q}$ 上代数，f_α 为极小多项式/$\mathbb{Q}$，K 为 f_α 在 $\mathbb{Q}$ 上的分裂域

则 $\alpha \in \mathcal{C} \Leftrightarrow [K:\mathbb{Q}] = 2^s$, $s \geq 0$.

1) 正 n 边形 $\Leftrightarrow$ n 次本原根 $\zeta \in \mathcal{C} \Leftrightarrow [\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n) = 2^s$

$n = 17$, $\varphi(17) = 16 = 2^4$　　(Gauss 1796)