110

Final Ch. Galois Theory

4.1. Galois 扩张

$K/k \rightsquigarrow K$: k-~~线~~线性空间 $\qquad \dim_k K = [K:k]$

K/k 的 Galois 群: $\mathrm{Gal}(K/k) = \mathrm{Aut}(K/k)$

"似乎 k 越大, $\mathrm{Gal}(K/k)$ 越小?"

Lem $\dim_k K < \infty$

则 $|\underbrace{\mathrm{Gal}(K/k)}_{\text{有限群}}| \le \dim_k K < \infty$.

$f(x) \in k[X]$ 可分时 可取等 $\qquad \mathrm{char}\, k = 0$ 中自动

分裂域: 分裂 + 极小 w.r.t. $f(x)$

Key Fact $f(x)$ 可分 $K = \cancel{k(a_1, \dots, a_n)}\ (k, f(x))$

$$\Rightarrow |\mathrm{Gal}(K/k)| = \dim_k K < \infty$$

$G \curvearrowright \mathrm{Aut}\, K \qquad (G \le \mathrm{Aut}\, K).$

$\sigma . v = \sigma(v)$

不动子域 $\underline{K^G}_{\text{K的子域}} = \{ v \in K \mid \sigma(v) = v, \forall \sigma \in G \}$

$\sigma(v^{-1}) = \sigma(v)^{-1} = v^{-1}$

$v \in K^G \quad \sigma(v) = v$

Fact. ① $H \le G$

$K^G \subseteq K^H \subseteq K$. (群越大, 子域越小)

② K/k 且 $G \le \mathrm{Gal}(K/k)$

则 $k \subseteq \cancel{k}\ \underset{\text{中间域}}{K^G} \subseteq K$

③ K/k. $k \subseteq K^{\mathrm{Gal}(K/k)} = \{ v \in K \mid \sigma(v) = v, \forall \sigma \in \mathrm{Gal}(K/k) \} \subseteq K$.

④ $G \le \mathrm{Aut}\,K$.

K/K^G : $\mathrm{Gal}(K/K^G) = \{\sigma \in \mathrm{Aut}\,K \mid \sigma|_{K^G} = \mathrm{Id}\}$.

$\Rightarrow G \le \mathrm{Gal}(K/K^G)$

定理 $G \le \mathrm{Aut}(K)$ 有限子群

(1) $[K:K^G] = |G|$

(2) $G = \mathrm{Gal}(K/K^G)$

证: $n = |G|$　$k = K^G$

Claim $\dim_k K \le n$　　$G = \{\mathrm{Id}, \dots, \sigma_{n-1}\}$

$$n = |G| \le |\mathrm{Gal}(K/k)| \overset{\text{Claim}}{\le} \dim_k K \le n.$$

若 $\{e_1, \dots, e_{n+1}\} \subseteq K$. k-线性无关.

$$A_{n\times(n+1)} = \begin{pmatrix} e_1 & \cdots & e_{n+1} \\ \sigma(e_1) & \cdots & \sigma(e_{n+1}) \\ \vdots & & \vdots \\ \sigma_{n-1}(e_1) & \cdots & \sigma_{n-1}(e_{n+1}) \end{pmatrix} \in M_{n\times(n+1)}(K)$$

解空间 $0 \ne V = \{v \in K^{n+1} \mid Av = 0\} \subseteq K^{n+1}$

K-线性子空间

$G \curvearrowright K^{n+1}$　$\vec{v} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{n+1} \end{pmatrix}$　$\sigma(\vec{v}) = \begin{pmatrix} \sigma(\lambda_1) \\ \vdots \\ \sigma(\lambda_{n+1}) \end{pmatrix}$

key　$\vec{v} \in V$. $\tau \in G$.　$\tau(\vec{v}) \in V$.

$\Downarrow$ $0 = \sum_{i=1}^{n+1} \lambda_i \sigma(e_i)$, in K.

$0 = \sum_{i=1}^{n+1} \tau(\lambda_i)\, \tau\sigma(e_i)$

即 $\forall \delta \in G$.　$0 = \sum_{i=1}^{n+1} \tau(\lambda_i)\, \delta(e_i)$

取 $\vec{v} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{n+1} \end{pmatrix}$　$\vec{v}$ 中 0 个数最多　（个数 $\le n-1$ 否则 $\vec{v} = \begin{pmatrix} \lambda_1 \\ 0 \end{pmatrix}$　$\lambda_1 e_1 = 0$ $\Rightarrow e_1 = 0$）

不妨 $v = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ 0 \end{pmatrix}$　$v' = \lambda_1^{-1} v$

$\exists \tau \in G$　$\tau(\lambda_2) \ne \lambda_2$.　$0 \ne v - \tau(v) \in V$　0 更多了　□

（不懂，也不想懂了）

112. K/k f.d. $G = \mathrm{Gal}(K/k)$

有 $k \subseteq K^G$

$|G| \leq \dim_k K$

定理 TFAE.

① $k = K^G$

② $|G| = \dim_k K$

③ $\forall \alpha \in K$. 则 α 在 k 上的最小多项式在 K 上分裂

④ $K = (k, f(x))$ $f(x)$ 可分.

local

此时 K/k 为有限 Galois 扩张

(似乎要加有限条件)

证. ①$\Leftrightarrow$② $\dim_k K = \dim_k K^G \cdot [K : K^G]$

$\overset{\text{Artin}}{=} \dim_k K^G \cdot |G|$

②$\Rightarrow$③ $\alpha \in K. \rightsquigarrow g(x)$

claim $|\mathrm{Root}_K\, g(x)| = \deg g$

~~若 $\mathrm{Root}_K\, g < \deg g$~~

$\boxed{\text{Ex}}$ $k \xrightarrow[\sim]{\delta} k'$ 则 δ 的延拓个数 $\leq \dim_k K$

K/k K'/k'

③$\Rightarrow$④ $K = k(\alpha_1 \cdots \alpha_n)$

$g_1(x)$ $g_n(x)$

令 $f(x) = g_1(x) \cdots g_n(x)$ 可分

$K = (k, f(x))$

④$\Rightarrow$② ✓

□

"Absolute" Galois bijective

$\forall$ 域 K. 双射

$\{$有限 $G \leq \mathrm{Aut}\,K\} \overset{1:1}{\longleftrightarrow} \{k \subseteq K \mid K/k$ f.d Galois$\}$.

$G \longmapsto K^G$

$\mathrm{Gal}(K/k) \longleftarrow k$.

Artin 等价引理 $\leftarrow$ It's proof.

$\boxed{EX}$ $K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. 的 Absolute Galois 双射

"Relative" Galois Bijective

K/k f.d. Galois 扩张 则 双射

$\{\mathrm{Gal}(K/k)$ 的子群$\} \overset{1:1}{\longleftrightarrow} \{K/k$ 中间域$\}$

$H \longmapsto K^H$

$\mathrm{Gal}(K/E) \longleftarrow E$

$k \subseteq E \subseteq K$. 则 K/E Galois

不一定 Galois

$\boxed{EX}$ $E = \mathbb{Q}(\sqrt[3]{2})$ $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ $k = \mathbb{Q}$

相对扩张本身的正规

命题 K/k f.d. Galois $k \subseteq E \subseteq K$.

则 E/k Galois $\Leftrightarrow \forall \sigma \in \mathrm{Gal}(K/k)$ $\sigma(E) = E$.

proof

$(\Rightarrow)$ $E = (k, \overset{\in k[x]}{g(x)})$. $\Rightarrow E = k(\beta_1, \cdots \beta_n)$.

$\sigma \in G = \mathrm{Gal}(K/k)$ $\sigma(\beta_1) \overset{?}{\in} E$ $\sigma(g(\beta)) = \sigma(0_E)$

$g(\sigma(E))$ $\quad \| \quad 0_E$

分裂 $\overset{\cap}{E}$

$\Rightarrow \sigma(E) \subseteq E$.

又 $\dim_k \sigma(E) = \dim_k E \Rightarrow \sigma(E) = E$.

(⇐) $\forall \beta \in E$. ⇝ 最小 g 可分. (K/k Galois)

claim g split on E.

$$g = (x-\underline{\beta})(\cdots)(x-\beta_n)$$

$$\begin{tikzcd}
K \arrow[r, dashed, "\exists \sigma"] & K \\
k(\beta) \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\delta_i", "\sim"'] & k(\beta_i) \arrow[u, phantom, "\cup" rotate=90] \\
k \arrow[u, phantom, "\cup" rotate=90] \arrow[r, equal] & k \arrow[u, phantom, "\cup" rotate=90]
\end{tikzcd}$$

$\exists\ \delta_i(\beta) = \beta_i \in E$

$\boxed{\text{Ex}}$ K/k Galois $G = \mathrm{Gal}(K/k)$ $g(x) \in k[x]$ 不可约

$G \circlearrowright \mathrm{Root}_K\, g(x)$ 可迁

例. $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ $K/\mathbb{Q}$ f.d Galois

$G = \mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Aut}\, K$.

$G \circlearrowright \mathrm{Root}_K(x^3-2)$

$\{\overset{a}{\sqrt[3]{2}}, \overset{b}{\sqrt[3]{2}\omega}, \overset{c}{\sqrt[3]{2}\omega^2}\}$

$G \overset{\rho}{\underset{\sim}{\hookrightarrow}} S(\{a, b, c\}) \cong S_3$

⟵ 拉回来看 G.

(ab): $\boxed{\begin{array}{l}\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\end{array}}$

$\Rightarrow$ $\omega \mapsto \omega^2$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega^2$

$\sqrt[3]{2}\omega^2 \in K$ $\quad \underbrace{\mathbb{Q}(\sqrt[3]{2}\omega^2)}_{3维} \subseteq K^{\langle (ab) \rangle}$ $\quad$ 同维度

$3 \mid 6$

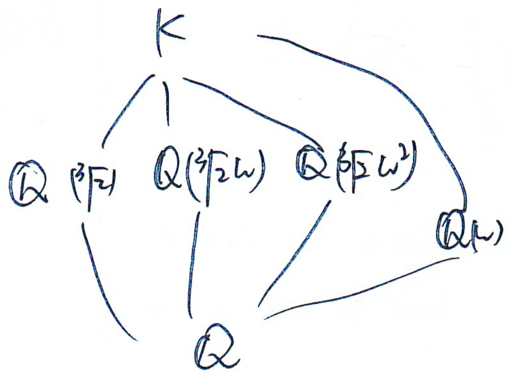
$K^{\langle (ab) \rangle} \overset{?}{=}$

$$\begin{tikzcd}
\mathbb{Q} & & G \arrow[ll] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
& \langle (ab) \rangle \arrow[dr, dash] & \langle (ac) \rangle \arrow[d, dash] & \langle (bc) \rangle \arrow[dl, dash] & \langle (abc) \rangle \arrow[dll, dash] \\
K & & \mathrm{Id} \arrow[ll] & &
\end{tikzcd}$$

$(abc) : K \to K$

$$\boxed{\begin{aligned} \sqrt[3]{2} &\mapsto \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega &\mapsto \sqrt[3]{2}\omega^2 \\ \sqrt[3]{2}\omega^2 &\mapsto \sqrt[3]{2} \end{aligned}}$$

$$\boxed{\omega \mapsto \omega}$$



Galois 对应，以上为全部子域

$\boxed{\text{EX}}$ $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = K$.

$K = (\mathbb{Q}, (x^2-2)(x^2-3))$

$G \curvearrowright \mathrm{Root}_K\ \varphi \cdots = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
$\quad\quad a \quad b \quad c \quad d$

模仿画图.

例. $|K| = p^n$ $\quad K/\mathbb{F}_p$ Galois $\quad K = (\mathbb{F}_p, x^{p^n} - x)$

$\sigma : a \mapsto a^p$

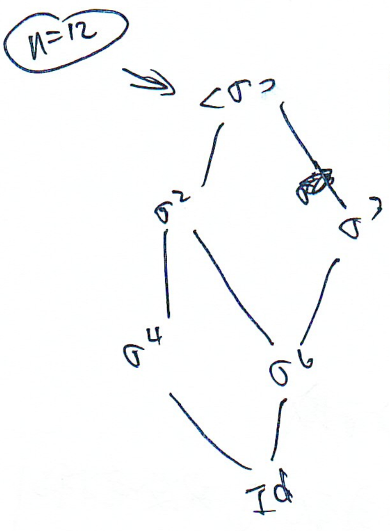
$\mathrm{Gal}(K/\mathbb{F}_p) = \{\mathrm{Id}, \sigma, \cdots \sigma^{n-1}\} = \langle\sigma\rangle$

$\| \quad \{\langle\sigma\rangle \text{的子群}\} \longleftrightarrow \{K \text{的子域}\}$

$\mathrm{Aut}(K)$

$\langle\sigma^d\rangle \longmapsto K^{\langle\sigma^d\rangle}$

$d | n \quad\quad \{x^{p^d} = x\}$



例 任何有限群 $G \leq S_n$

$\sigma \in S_n \curvearrowright k(t_1, \cdots t_n) = \mathrm{Frac}\ k[t_1, \cdots t_n]$.

$\sigma(t_i) = t_{\sigma(i)}$

$G \leq S_n \hookrightarrow \mathrm{Aut}(k(t_1, \cdots t_n))$

$G \overset{\text{Artin}}{\simeq} \mathrm{Gal}\left(k(t_1, \cdots t_n) \big/ k(t_1, \cdots t_n)^G\right)$

都是 Galois 群

偏序集 $(L, \leq) = L$ $\neq \phi$

(1) $a \leq a$

(2) $a \leq b \quad b \leq c \Rightarrow a \leq c$

(3) $a \leq b \quad b \leq a \Rightarrow a = b$

同态 $f: (L_1, \leq) \longrightarrow (L_2, \leq)$

- $f: L_1 \to L_2$ 映射
- 保序

G 子群与子群 　 形成的偏序集.

K/k 域与中间域

定义. $(L, \leq)$

(1) a, b 　 $a \vee b \in L$ (最小上界)

$$\left(\begin{array}{l} a \leq (a \vee b) \quad b \leq a \vee b \\ a \leq c \ . \ b \leq c \Rightarrow (a \vee b) \leq c \end{array} \right)$$

存在唯一

(2) $a . b$ 　 $a \wedge b \in L$ 最大下界

$$\left(\begin{array}{l} (a \wedge b) \leq a \quad (a \wedge b) \leq b \\ c \leq a \ . \ c \leq b \Rightarrow c \leq (a \wedge b) \end{array} \right)$$

$(L, \leq)$ 称为格, 若 $a \vee b$, $a \wedge b$ $\exists$,

例. $Sub(G), \subseteq)$ G 的子群格

$H, U \leq G$. 　 $H \wedge U = H \cap U$

$H \vee U = \langle H \cup U \rangle$

例 $Lat(K/k)$ 　 $k \subseteq E$. $F \subseteq K$

$E \wedge F = E \cap F$

$E \vee F =$ 包含 $E \cup F$ 的最小子域

例 $(L, \leq)$ 格 　 $(L^{op}, \leq^{op})$ 反格 　 反过来就行, 如没什么特别

例 $\forall n \geq 1$. $L_n = \{d \mid 1 \leq d \leq n,\ d \mid n\}$.

$a \wedge b = \gcd(a,b)$

$a \vee b = \operatorname{lcm}(a,b)$ $\boxed{EX}$ 格同构保 $\vee, \wedge$

f 双. f, f^{-1} 保序

反例 $n=12$. $(\{1, \cdots 12\}, \leq) \xrightarrow{Id} (L_{12}, \preccurlyeq)$

$\boxed{EX}$ $4 \vee 6 = 6$ $\quad$ $4 \vee 6 = 12$

例 n. $G_n = \langle g \mid g^n = 1 \rangle$

$$\operatorname{sub}(G_n) \overset{\sim}{\longleftrightarrow} (L_n, \preccurlyeq)$$

$$\langle g^{\frac{n}{d}} \rangle \longleftrightarrow d. \quad \text{格同构}$$

用格理论 Galois 对应

Galois 基本定理. K/k f.d Galois

$G = \operatorname{Gal}(K/k)$ $\quad \operatorname{sub} G \xrightarrow{\sim} \operatorname{Lat}(K/k)^{op}$. $\quad H \mapsto K^H$, $\operatorname{Gal}(K/E) \mapsto E$.

推论 ① $H, U \leq G$

$K^H \cap K^U \overset{\text{平凡}}{=\!=} K^{H \vee U}$

$K^H \vee K^U \underset{\text{不平凡}}{=\!=} K^{(H \cap U)}$?

② $k \subseteq E, F \subseteq K$. $\operatorname{Gal}(K/F \vee E) \overset{\text{平凡}}{=\!=} \operatorname{Gal}(K/F) \cap \operatorname{Gal}(K/E)$

$\operatorname{Gal}(K/F \cap E) \underset{\text{不平凡}}{=\!=} \operatorname{Gal}(K/F) \vee \operatorname{Gal}(K/E)$.

注 $H \leq G$. $H = \operatorname{Gal}(K/K^H)$

$|H| = [K : K^H]$ $(= \dim_{K^H} K)$

$|G| = |H| \cdot [G:H]$ $\Rightarrow \dim_k K^H = [G:H]$

$\dim_k K = \dim_{K^H} K \cdot \dim_k K^H$

118.

G-集 $(X, +)$

$G \curvearrowright X \qquad \psi: G \times X \to X$

G-偏序集 · $(L, \leq)$

G-poset · $G \curvearrowright L$

· 相容性

$$\boxed{a \leq b \iff g.a \leq g.b \quad \forall g}$$

$\rho: G \to \mathrm{Aut}(L, \leq)$

例 $G \curvearrowright \mathrm{Sub}(G)$ ~~错~~格

$$g.H = gHg^{-1}$$

$$H \leq U, \quad gHg^{-1} \leq gUg^{-1}$$

例 $G \curvearrowright \mathrm{Lat}(K/k)$

$\sigma \qquad E$

$$\sigma.E = \sigma(E)$$

定理 K/k f.d Galois $G = \mathrm{Gal}(K/k)$

可证 $k \subseteq E \subseteq K$ 有 $\mathrm{Gal}(K/\sigma(E)) = \sigma \mathrm{Gal}(K/E) \sigma^{-1}$

则有 G-poset 同构

$$\mathrm{Sub}(G) \xrightarrow{\sim} \mathrm{Lat}(K/k)^{op}$$

推论 $\mathrm{Sub}(G)^G \xrightarrow{\sim} (\mathrm{Lat}(K/k)^{op})^G$ 不动点

$$k \subseteq E \subseteq K$$

$$\mathrm{Gal}(K/E) \lhd G \iff E/k \text{ Gal}$$

此时 $G/\mathrm{Gal}(K/E) \xrightarrow{\sim} \mathrm{Gal}(E/k)$. 记: $G \to \mathrm{Gal}(E/k)$, $\sigma \mapsto \sigma|_E$.

$\ker = \mathrm{Gal}(K/E)$ ✓ □

记: $H \leq G$. $g \in G$.

$$K^{gHg^{-1}} \overset{?}{\underset{\boxed{EX}}{=}} g(K^H)$$

$H \leq G$ $\qquad G(K^H) = \{g \in H \mid gK^H = K^H\}$

$G_H = \{g \in G \mid gHg^{-1} = H\}$

$\boxed{EX}$ $H \mapsto \cancel{k}^H = E$

$Gal(E/k) = G_H/H$

K/k f.d. Galois. $G = Gal(K/k)$

$G \curvearrowright Sub\,G$ G-枚 $\qquad G \curvearrowright Lat(K/k) = \{中间域\}$.

$g.H = gHg^{-1}$ $\qquad g.E = g(E)$

$\leq$

~~then~~ $Sub\,G \simeq Lat(K/k)^{op}$. 格同构

保 $\wedge, \vee$

保 G-作用

$H \longmapsto K^H$

$Gal(K/E) \longleftarrow E$

$\left(K^{gHg^{-1}} = \{v \mid ghg^{-1}(v) = v, \forall H\} = g(K^H)\right.$

$\boxed{\forall 中间域 \; Gal(K/g(E)) = g\,Gal(K/E)\,g^{-1}}$.

$\{g^{-1}v = hg^{-1}v\}$

$g^{-1}v \in K^H$

$v \in g(K^H)$

$\boxed{例}$. $f, g \in k[x]$ 可分.

$K = (k, f(x)g(x))$

$C = (k, g(x))$

$B = (k, f(x))$

设 $B \cap C = k$. $B \vee C = K$

则 $Gal(K/k) \overset{?}{\simeq} Gal(K/B) \times Gal(K/C)$

120 证

$$\begin{array}{ccc} & K & \\ B \subseteq & & \supseteq C \\ & \supseteq k \subseteq & \end{array} \longrightarrow \begin{array}{ccc} & \{Id\} & \\ Gal(K/B) & & Gal(K/C) \\ \triangleleft & G & \triangleleft \end{array}$$

正规 $Gal(K/B)\, Gal(K/C) = G$

$B \cap C = k \longrightarrow Gal(K/B) \vee Gal(K/C) = G$

$B \vee C = K \longrightarrow Gal(K/B) \cap Gal(K/C) = \{Id\}$

用 $\boxed{Ex}$ 和前面的推论

$\boxed{Ex}$ $N_1, N_2 \triangleleft G$. $N_1 \cap N_2 = \{Id\}$, $N_1 \cdot N_2 = G$ 则 $G \simeq (G/N_1) \times (G/N_2)$

例 $K = (\mathbb{Q}, (x^2-2)(x^2-3))$

$B = \mathbb{Q}(\sqrt{2})$

$C = \mathbb{Q}(\sqrt{3})$

$\Rightarrow Gal(K/\mathbb{Q}) \simeq \mu_2 \times \mu_2$

Steinitz K/k. f.d. 则 单 $\Leftrightarrow$ K/k 只有有限中间域

"$\Rightarrow$" $K = k(\alpha) \longrightarrow$ 最小 $f(x) \in k[x]$.

$k \subseteq E \subseteq K$.

α 在 E 上的最小多项式 $g(x) = x^m + c_1 x^{m-1} + \cdots + c_m$

$E \supseteq B = k(c_1, \cdots c_m)$ $\dim_E K = m = \dim_B K$

Claim $E = B$. $\Rightarrow \dim_k E = \dim_k B$ ✓.

$k \subseteq B \subseteq \underbrace{E \subseteq K}_{m}$ B 由 g 决定. 有限

$g \mid f$ in K $\Rightarrow$ 有限 有限

"$\Leftarrow$" 设 $|k| = \infty$ ~~k~~ $K = k(\alpha_1, \cdots \alpha_t)$

$k \subseteq k(\alpha_1, \alpha_2) \subseteq K$

$\forall \lambda \in k$. $E_\lambda = k(\alpha_1 + \lambda\alpha_2)$

$\exists \lambda_1 \neq \lambda_2$. $E_{\lambda_1} = E_{\lambda_2} = A$

$\Rightarrow \alpha_1, \alpha_2 \in A$

$\Rightarrow k(\alpha_1, \alpha_2) = A$

归纳! □

证. K/k f.d. 单 $k \subseteq E \subseteq K$.

$\Rightarrow$ E/k 有限个中间域

$\Rightarrow$ E/k 单.

本原定理. 设 K/k f.d. 是可分扩张 ($\forall \alpha \in K$, 最小多项式可分 e.g. $\operatorname{char} k = 0$)

则 K/k 单

证: $K = k(\alpha_1, \cdots \alpha_t)$

最小 g_1 … g_t

$E = (k, g_1(x) \cdots g_t(x))$. E/k 分裂. E/k Galois.

$\Rightarrow k \subseteq K \subseteq E$.

这个用 Galois 对应得到 有限中间域

① 仅有有限个中间域

$\Downarrow$

单

例 $k = \mathbb{F}_p(t_1, t_2)$

$K = (k, (x^p - t_1)(x^p - t_2))$ $\quad (x^p - t_1)(x^p - t_2) = (x - a_1)^p (x - a_2)^p$

$\operatorname{char} k = p$

$= k(a_1, a_2)$ $\quad \begin{cases} a_1^p - t_1 = 0 \\ a_2^p - t_2 = 0 \end{cases}$

$\boxed{\text{EX}}$. $\dim_k K = p^2$

. $\operatorname{Gal}(K/k) = \{\operatorname{Id}\}$

. $\forall \lambda \in k$,

$E_\lambda = k(a_1 + \lambda a_2)$

. $\dim_k E_\lambda = p$

. $E_\lambda = E_\mu \quad \forall \lambda \neq \mu$

FTA. $\mathbb{C}$ 代数闭,

证: ① $\mathbb{R} \subsetneq K$ 则 $\dim_{\mathbb{R}} K \neq \text{odd}$

$\alpha \in K \setminus \mathbb{R}$. $\deg f \mid \dim_{\mathbb{R}} K$

奇 偶.

② $\mathbb{C} \subseteq K$. $\dim_{\mathbb{C}} K \neq 2$. 否则

$\Rightarrow$ $\mathbb{C}$ 上有二次多项式 不可约 矛. (因为能开根)

12/2 设 $f \in \mathbb{C}[x]$ 不可约 $\deg f \geq 2$

$\mathbb{R} \subseteq \mathbb{C} \subsetneq K = (\mathbb{C}, f(x)\bar{f}(x))$

例 $\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\sqrt{2})}_{\text{Galois}} \subseteq \overbrace{\mathbb{Q}(\sqrt[4]{2})}^{\text{Galois}}$

Claim. $K/\mathbb{R}$ Galois

$K = (\mathbb{R}, f(x)\bar{f}(x)(x^2+1))$.

$G := \mathrm{Gal}(K/\mathbb{R})$ Claim $|G| = 2^r$

否则 $|G| = 2^r \cdot \underset{\text{odd}}{m}$. $\exists$ 2-Sylow P $[G:P] = m$

$\underbrace{\mathbb{R} \subseteq K^P}_{\text{维 odd } m} \subseteq K$ $\dim_{\mathbb{C}} K = 2^{r-1}$

$G' = \mathrm{Gal}(K/\mathbb{C})$

$\boxed{\text{EX}}$ U p-group $\exists V \leq U$. s.t. $[U:V] = p$.

用$\boxed{\text{EX}}$. $\exists H \leq G'$ $\underbrace{\mathbb{C} \subseteq K^H}_{2\text{维}} \subseteq K$

矛盾. $\square$

根式可解

定义. • E/k 是根式扩张. $E = k(\alpha)$, $\alpha^m = a \in k$. $\exists m$

• 根式扩张塔 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m$

E_k/E_{k-1} 是根式扩张

定义 $f(x) \in k[x]$ 根式可解. 若 $\exists$ 根式扩张塔 $k = E_0 \subseteq E_1 \subseteq \cdots E_n$.

s.t. $(k, f(x)) \subseteq E_n$.

例 x^2+bx+c

$k_0 \subseteq k(\sqrt{b^2-4c}) = k(\alpha)$

$\alpha^2 = b^2 - 4c$.

Fact. $E = k(\alpha)$ $\alpha^m = a \in k$.

① 若 k 包含 m 次本原单位根 ω

则 $x^m - a = \prod_{i=0}^{m-1}(x - \alpha\omega^i)$

$\Rightarrow E = (k, x^m - a) = $ Galois　　　　用方程给出 Gal 结构

$\mathrm{Gal}(E/k) \hookrightarrow (\mathbb{Z}, +)$

$\sigma(\alpha) = \omega^i \alpha \mapsto i$

② $\mathrm{char}\, k = 0$　　　　　　本原

$E' = (E, x^m - 1) = E(\omega)$　　　　单嵌入

$k \subseteq E \subseteq E'$
$\subseteq k(\omega) \subseteq$
$\| $
k'

$\Rightarrow \mathrm{Gal}(E'/k') \hookrightarrow (\mathbb{Z}_m, +)$

$\mathrm{Gal}(k'/k) \hookrightarrow U(\mathbb{Z}_m)$　　Check.

Abel　　　　　　　　乘法

k'/k Galois

$\mathrm{Gal}\, E'/k' \lhd \mathrm{Gal}\, E'/k$.

商 $\simeq \mathrm{Gal}\, k'/k$

Abel

换言之正合列：

$1 \longrightarrow \mathrm{Gal}(E'/k') \xhookrightarrow{\lhd} \mathrm{Gal}(E'/k) \twoheadrightarrow \mathrm{Gal}(k'/k) \to 1$

Abel　　　　　　　　　　　　Abel

例 $A_3 \hookrightarrow S_3 \twoheadrightarrow C_2$

推广 $\mathrm{Gal}(E/k) \simeq \mathrm{Gal}(E'/E) \,/\, \mathrm{Gal}(E'/E)$　　"子商"

$\| \mathrm{Gal}(E'/k)$ 若 E/k Galois

若 E/k 不 Galois

12.4.

根式扩张塔.

$k=E_0\subseteq E_1\subseteq\cdots\subseteq E_n$ $\quad E_i/E_{i-1}$ 根式扩张

Fact. $\mathrm{char}\, k=0$

则 $\forall$ 塔 可扩张 Galois 扩张

i.e. $k=E_0\subseteq\cdots\subseteq E_n\subseteq E_{n+1}\cdots\subseteq E_m$

E_m/k Galois

证: E_n/k 单 $\longrightarrow E_n=k(\beta)$ $\quad f(x)$ 最小

$K=(E_n, f(x))$ 故 $k\subseteq E_n\subseteq K$.

$\quad\;\; \| $

$\quad (k, f(x))$ $\Rightarrow$ K/k Galois ☒

局部看不清了.

$\mathrm{Gal}(K/k)=\{\underset{Id}{\sigma_0},\cdots,\sigma_l\}$

用 σ_i 把之前的列平移

$k\underset{塔}{\subseteq}E_n\subseteq E_n\vee\sigma_1(E_n)\subseteq E_n\vee\sigma_1(E_n)\vee\sigma_2(E_n)\cdots$

$\subseteq E_n\vee\sigma_l(E_n)\vee\cdots$

$=K.$ □.

$\Rightarrow$ $\boxed{Ex}$ 证明

Fact. 可设 $k=E_0\subseteq\cdots\subseteq E_n$ 根式. E_n/k Galois

设 k 有充分多的单位根.

$\Rightarrow$ 局部也能 Galois $\begin{cases} E_i/E_{i-1} & \text{Galois} \\ \mathrm{Gal}(E_i/E_{i-1}) & \text{Abel}\end{cases}$

$$\mathrm{Gal}(E_n/k) \trianglerighteq \mathrm{Gal}(E_n/E_1) \trianglerighteq \cdots \trianglerighteq \mathrm{Gal}(E_n/E_{n-1}) \trianglerighteq \{\mathrm{Id}\}$$

$\uparrow$ E_1/k Galois

"同构"商 $\downarrow$

$\mathrm{Gal}(E_1/k)$ Abel

$\mathrm{Gal}(E_2/E_1)$ Abel

对 E_n/E_1 用Galois理论

但 E_2/E_1 Galois

Fact. In general Char $k=0$.

$k = E_0 \underset{m_1}{\subseteq} E_1 \subseteq \cdots \subseteq E_n$ $\quad E_n/k$ Galois

$M = \mathrm{lcm}(m_1, \cdots)$

$E_n' = (E_n, x^M - 1) = E_n(w)$

$k \subseteq E_n \subseteq E_n'$

$\subseteq k'(w) \subseteq$

$$1 \to \mathrm{Gal}(E_n'/k') \xrightarrow{\triangleleft} \mathrm{Gal}(E_n'/k) \to \mathrm{Gal}(k'/k) \text{ Abel} \to 1$$

$\mathrm{Gal}(E_n'/k) \to \mathrm{Gal}(E_n/k)$

Recall. $f(x) \in k[x]$.

$\mathrm{Gal}_k(f) = \mathrm{Gal}\left(\overset{L}{\overset{\|}{k.f(x)}}/k\right)$

若 f 根式可解, 即, 存在 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$.

f 在 E_n 上 split.

$\mathrm{Gal}_k f = \mathrm{Gal}(L/k) \twoheadleftarrow \mathrm{Gal}\, E_n/k$

的

$k \overset{\mathrm{Gal}}{—} L \trianglelefteq E_n$

$E_n/k \big/ E_n/L \quad G \simeq L/G.$

定义. 称群 G 称为可解群 (solvable)

若 ∃ 子群 降链.

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1_G\}$$

满足 $G_i \trianglerighteq G_{i+1}$ $\quad G_i/G_{i+1}$ Abel

例 $n=1$.

$G = G_0 \triangleright 1_G \quad \Rightarrow G$ Abel 可解

$n=2$.

$G = G_0 \triangleright G_1 \triangleright G_2 = \{1_G\}$

$\quad\quad\quad\quad\quad\quad\quad$ Abel

$\Rightarrow \quad G_0/G_1$ Abel $\quad G_1$ Abel

即 正合列 $\quad 1 \to G_1 \to G_0 \to G_0/G_1 \to 1$

$1 \to A_3 \to \boxed{S_3} \to C_2 \to 0$

可解

$n=3 \quad G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 = \{e\}$

$\quad\quad\quad\quad\quad$ Abel

3个 循环群 拼合.

$1 \to K_4 \to S_4 \to S_3 \to 1$

$1 \to A_3 \to S_3 \to C_2 \to 1$

or $\quad S_4 \triangleright A_4 \triangleright K_4 \triangleright \{1_d\}$

可解群 要有 充分多正规子群 $\Rightarrow$ 非Abel 单群不可解

Fact G 可解, $H \leq G$. $\to$ H 可解

$N \trianglelefteq G \Rightarrow G/N$ 可解

证 设 $G \triangleright G_1 \triangleright \cdots$

$\boxed{\text{EX}} \Rightarrow H \triangleright G_1 \cap H \triangleright \cdots$

$\Rightarrow G/N \triangleright \overline{G_1 N}/N \triangleright \cdots$

$\overset{\|}{\overline{G}}$ 这里记号可能有误. $\square$.

Fact. $N \trianglelefteq G$. N, G/N 可解 $\Rightarrow$ G 可解

证: $N \triangleright N_1 \triangleright \cdots$

$G/N \triangleright G_1/N \triangleright \cdots$

$G_1 \supseteq N$.

$\Rightarrow G \triangleright G_1 \triangleright \cdots$

例. S_n, $n \geq 5$. 不可解

p 群可解 $\quad P/Z(P)$

对 ⊙ 阶归纳

$1 \to Z(P) \to P \to$ 小 p 群 可解

"群的世界观"

单群 : v.s. 可解群 (Abel, p群)

Galois 大定理. $\text{char}\, k = 0$ $f(x) \in k[x]$.

则 $f(x)$ 根式可解 $\Leftrightarrow$ $\text{Gal}_k(f)$ 可解.

128

证: "$\Rightarrow$" $k=E_0\subseteq\cdots\subseteq E_n$ 塔

$L=(k,f(x))$ $L\subseteq E_n$

$k \subseteq E_n$, E_n/k Galois

$\mathrm{Gal}_k f \twoheadleftarrow \mathrm{Gal}(E_n/k) \twoheadleftarrow \mathrm{Gal}(E_n'/k)$

可解

"$\Leftarrow$" 下课想想.

由 lem. k_1/k 根式 of type p.

$\mathrm{Gal}(K/k_1)\simeq H$ 可解

$\underbrace{G \trianglerighteq H}_{C_p} \underbrace{\trianglerighteq U}_{C_p'} \trianglerighteq\cdots \Rightarrow$ 塔

(此情况, k 有单位根).

(Case 2) In general

$k\subseteq K\subseteq K'=(k,x^{|G|}-1)$

$=K(\omega)$.

$|G|$ 次本原

lem K/k f.d. Galois $\mathrm{Gal}(K/k)=\langle\sigma\rangle$,

$\sigma^p=\mathrm{Id}$ p prime

k 有 p 次本原单位根.

则 K/k 根式 of p type

Claim $\mathrm{Gal}(K'/k')\hookrightarrow G$

可解

$\Rightarrow k\subseteq \overset{k'}{\overset{\parallel}{k(\omega)}} \underset{塔}{\subseteq} K'=(k(\omega),f(x))$

根式

Claim 证明: $\mathrm{Gal}(K'/k')\longrightarrow G$.

$\sigma\longmapsto\sigma|_K$.

核 $\sigma|_K=\mathrm{Id}_K$

$\sigma=\mathrm{Id}_{K'}$ $\sigma|_{k'}=\mathrm{Id}_{k'}$, $K\vee k'=K'$

证: $\sigma: K\longrightarrow K$ k-linear

σ 有特征值 ω. $\omega^p=1$, $\omega\neq1$

$\det(\sigma-\omega\,\mathrm{Id}_k)=0$

$\sigma(\beta)=\omega\beta\neq\beta\in K$.

特征向量. $\notin k$.

$\sigma(\beta^p)=\beta^p\Rightarrow\beta^p\in k$.

但 $k\subsetneq k(\beta)\subseteq K$

$\Rightarrow k(\beta)=K$ (算维数) $\square$

$K=(k,f(x))$ $G=\mathrm{Gal}(K/k)$ 可解.

Case k 有 $|G|$ 次本原单位根

EX G 可解, $\exists H\triangleleft G$. $G/H\simeq C_p$ p 素.

用 **EX** $k\subseteq k_1=K^H\subseteq K$

- k_1/k Galois $\mathrm{Gal}(k_1/k)=G/H\simeq C_p$.
-

近世代数梳理

Galois 理论 $|Gal(K/k)| \le \dim_k K$ 对有限域扩张，也成立

不变子域 $G \le Aut K$.

$K^G := \{a \in G \mid \sigma(a) = a \ \forall \sigma \in G\}$.

G是约束方程 $\Rightarrow$ $H \le G$,

$\Rightarrow K^G \subseteq K^H$

K/k $G \le Gal(K/k) \Rightarrow k \subseteq K^G \subseteq K$.

$\boxed{Gal(K/K^G) \ge G}$.

最重要的是有限情况.

Artin 引理. $G \le \cancel{Aut(K)}$. $\dim_{K^G} K \le n$ $G \le Aut(K)$ finite

$\cancel{\Rightarrow G = Gal(K/K^G)}$ ($K^G = k$.)

$G = \{Id, \sigma_2, \cdots \sigma_n\}$. ($Id = \sigma_1$)

If not 有 k-线性无关 $\{e_1, \cdots e_{n+1}\}$

$$\begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_{n+1}) \\ \vdots & & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_{n+1}) \end{pmatrix}_{n\times n+1} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{n+1} \end{pmatrix} = 0$$

由线性 必有解 由于 G 都是子群 V 在 G 下不变 $\downarrow$ $G \curvearrowright V$ 不变

对某个 $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{n+1} \end{pmatrix}$ (至少2个非零) 0最多

$\Rightarrow \begin{pmatrix} 1 \\ \lambda_2 \\ \vdots \\ \lambda_{n+1} \end{pmatrix} \notin K^G \Rightarrow \tau(\lambda_2) \ne \lambda_2$ $v - \tau v$ 0更少.

□

这个证明很重要 $n \ge [K : K^G] \ge |Gal(K/K^G)| \ge |G| = n$

$\Rightarrow \underline{Gal(K/K^G) = G}$

绝对双射　Artin lem

finite $\boxed{G \leq \mathrm{Aut}\,K} \longleftrightarrow \{k \subseteq K \quad K/k \text{ 有 f.d}\}$

$G \longrightarrow K^G$

$\mathrm{Gal}\,K/k \qquad k$

相对

$\mathrm{Gal}\,K/k$

$H \longrightarrow K^H$

$\mathrm{Gal}(K/E) \longleftarrow E$

$\checkmark$

$$\overbrace{k \subseteq E}^{\text{Galois}} \Downarrow \subseteq K$$

$\underbrace{k \subseteq}\ \underbrace{E \subseteq}_{\text{Galois}}$

$\Updownarrow$

E/k Galois $\Longleftrightarrow \forall \sigma \in \mathrm{Gal}(K/k),\ \sigma(E) = E.$

$(\Longrightarrow)$ $E = (k, g(x))$　$E = k(\beta_1, \cdots \beta_n)$

σ 保持根集 $\Rightarrow \sigma(E) = E$　然后看维数.

$(\Longleftarrow)$ $\forall \beta \in E$　g 可分. 需要 g split

上面是Galois

$$\begin{tikzcd} K \arrow[r, "\exists\sigma"] & K \\ k(\beta) \arrow[u] \arrow[r, "s"] & k(\beta') \arrow[u] \\ k \arrow[u] \arrow[r, equal] & k \arrow[u] \end{tikzcd}$$

$g(x) = (x - \beta_1) \cdots (x - \beta_n)$

$\Rightarrow g$ 在 E 上 split. $\square$

用lattice写Galois理论　$\mathrm{Sub}\,G = \mathrm{Gal}(K/k) \xrightarrow{\sim} \mathrm{Lat}(K/k).$

$\mathrm{Gal}(K/K^E)$

$H, U \leq G.$　$K^H \cap K^G = K^H \wedge K^G \longrightarrow H \vee G \longrightarrow K^{H \vee G}$

$K^H \vee K^U \longrightarrow H \wedge U = H \cap H \longrightarrow K^{H \cap U}$

②

$$\mathrm{Gal}(K/F\vee E) \longrightarrow K^{\mathrm{Gal}(K/F\vee E)} = F\vee E \longrightarrow \mathrm{Gal}(K/F) \wedge \mathrm{Gal}(K/E)$$
$$= \mathrm{Gal}(K/F) \cap \mathrm{Gal}(K/E).$$

$\wedge$

$\mathrm{Gal}\, K/k$

$$\mathrm{Gal}(K/F\cap E) \longrightarrow F\cap E = F\wedge E \longrightarrow \mathrm{Gal}(K/F) \vee \mathrm{Gal}(K/E).$$

$H \le G$.

$|H| = [K : K^H]$

$|G| = |H| \cdot [G : H]$

$\|$ $\quad \Rightarrow [K^H : k] = [G : H]$

$[K : k]$

设 $K^{gHg^{-1}} = g(K^H)$.

$\mathrm{Gal}(K/\sigma(E))$

$$\mathrm{Gal}(K/\sigma(E)) = \{ g \in \mathrm{Aut}(K) : g(v) = v \text{ for } \forall v \in \sigma(E) \}.$$

$v = \sigma(w)$, $w \in E$

$\Downarrow$

$g\sigma(w) = \sigma w$

$\sigma^{-1} g \sigma w = w$

$$= \{ g \in \mathrm{Aut}\, K : \sigma^{-1} g \sigma (w) = w \text{ for } \forall w \in E \}.$$

$$= \sigma^{-1} \mathrm{Gal}(K/E)\, \sigma \quad \times.$$

$$\mathrm{Gal}(K/\sigma(E)) = \sigma\, \mathrm{Gal}(K/E)\, \sigma^{-1}$$

proof $\forall \rho \in \mathrm{Gal}(K/\sigma(E)) \Rightarrow \forall v \in \sigma(E) \quad v = \sigma(w)$

$\rho(v) = v$

固定 E $\quad \rho\sigma w = \sigma w$

$\tau = \sigma^{-1}\rho\sigma$

$\rho = \sigma\tau\sigma^{-1} \in \sigma\, \mathrm{Gal}(K/E)\, \sigma^{-1}$

$\forall \rho \in \sigma\, \mathrm{Gal}(K/E)\, \sigma^{-1}$

$\rho(v)$, $v \in \sigma(E)$: $\quad \sigma\tau\sigma^{-1} \cdot \sigma(w) = \sigma(w) = v.$ $\quad \square$

因此 $k - E - K$

$\Rightarrow$ "$\mathrm{Gal}(K/E) \triangleleft \mathrm{Gal}(K/k) \Leftrightarrow \sigma(E)=E$"

$\Leftrightarrow E/k$ Galois

$\dfrac{\mathrm{Gal}(K/k)}{\mathrm{Gal}(K/E)}$

$\mathrm{Gal}(K/k) \xrightarrow{\phi} \mathrm{Gal}(E/k)$

$\sigma \longmapsto \sigma|_E$

$\ker\phi = \mathrm{Gal}(K/E)$.

$K^{gHg^{-1}} = g(K^H)$.

Steinitz. $\Rightarrow$ Galois $\overset{f.d.}{:}$ 可分扩张是单扩张

根式扩张

1. k 单位根多 $\Rightarrow$ $E=k(\alpha)/k$ 是 Galois 的

$\Rightarrow \mathrm{Gal}(E/k)$ Abel

嵌入还是同构到加法群中.

2. Char=0

$E'=(E, x^m-1)$

根式: $k - E$

$k \xrightarrow{\text{Galois}} E'$

$k - k(\omega) - E'$

分圆多项式 构造 Galois

$k'=k(\omega)$ 单位

Galois 嵌入 Abel

Gal

$\mathrm{Gal}(E'/k') \hookrightarrow \mathbb{Z}_m$ 不是 m 是因为 $x^m=\alpha$ 没有要求最小性

$x^m-\alpha$

$\mathrm{Gal}(k'/k) \hookrightarrow \mathbb{Z}_m$

例1. $f(x)=x^5-4x+2$

$$\mathrm{Gal}_{\mathbb{Q}} f=\mathrm{Gal}(E/\mathbb{Q}) \quad E=\mathbb{Q}(z_1,\cdots z_5)$$

(1) f 不可约　画图知两个实根(介值定理)

设 $z_3,\cdots z_5\in\mathbb{R}$

$z_1, z_2\notin\mathbb{R}$

$$|\mathrm{Gal}_{\mathbb{Q}} f|=\dim_{\mathbb{Q}} E$$

$G\curvearrowright\{z_1,\cdots z_5\}=X$

$G\xhookrightarrow{\rho} S(X)\cong S_5 \longrightarrow \boxed{G\leq S_5}$　S_5 子群 很多

$\mathbb{Q}\subseteq\underbrace{\mathbb{Q}(z_1)}_{f\ 5\text{维}}\subseteq E$

$\Rightarrow 5\mid |G| \xRightarrow{\text{Cauchy定}} G$有 5阶元 $\Rightarrow$ 有一个 5-cycle

$\tau: E\longrightarrow E$
$z\longmapsto\bar{z}$
$\Rightarrow \tau\in G$ 2阶元

$\tau\mapsto(12)$.

> Fact (12), 任何一个 5-cycle 可生成 S_5
> 移动
> (12, abc)

$\Rightarrow G\cong\rho(G)=S_5$ □

例2. $F=k(t_1,\cdots t_n)$　一般方程 $f(x)=x^n-t_1x^{n-1}+t_2x^{n-2}+\cdots(-1)^nt_n\in F[x]$

则 $\boxed{\mathrm{Gal}_F(f(x))\cong S_n}$ (If char $k=0\Rightarrow$ char $F=0$, $n\geq5$ 则 f 不根式可解)

Idea $k[y_1,\cdots y_n]\hookrightarrow k(y_1,\cdots y_n)$

$S_n\curvearrowright k(y_1,\cdots y_n)$　$y_i\longrightarrow y_{\sigma(i)}\Rightarrow S_n\hookrightarrow\mathrm{Aut}(k(y_1,\cdots y_n))$

130 算 $k[y_1,\cdots y_n]^{S_n}$

$$\mathrm{Gal}\left(k(y_1,\cdots y_n)\Big/ k(y_1,\cdots y_n)^{S_n}\right) \simeq S_n$$

这里就要 $F \simeq k(y_1,\cdots y_n)^{S_n}$

$F \hookrightarrow k(y_1,\cdots y_n)$

$$k[y_1,\cdots y_n]^{S_n} = \{ \underset{\text{对称多项式}}{\underset{\uparrow}{g(y_1,\cdots y_n)}} \mid \sigma(g) = g \quad \forall \sigma \in S_n \}$$

Fact: $k[t_1,\cdots t_n] \xrightarrow{\simeq} k[y_1,\cdots y_n]^{S_n}$

$t_1 \longmapsto y_1+\cdots+y_n$ 没讲啥证

$\vdots$

$t_n \longmapsto y_1\cdots y_n$

$\Rightarrow k(t_1,\cdots t_n) \xrightarrow{\simeq} k(y_1,\cdots y_n)^{S_n}$

$f(x) = (x-y_1)\cdots(x-y_n)$

群的合成列

$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \{1\}$

G_i/G_{i+1} 单群

G 可由 因子 G_i/G_{i+1} 构成.

引理. $|G| < \infty$ 有合成列.

证: (1) G 单 ✓

(2) G 不单. 取 $H \trianglelefteq G$, H 极大 $\quad G \trianglerighteq H \Rightarrow G/H$ 单 (有对应定理)

□

例3. $(\mathbb{Q},+)$ 无极大子群 不能无限.

反证 $H \subsetneq \mathbb{Q} \Rightarrow \mathbb{Q}/H$ Abel 单群 $\simeq C_p$

$\Rightarrow \mathbb{Q} \twoheadrightarrow C_p$ ↯

$n \longmapsto \bar{1}$

$p^{-1}n \longmapsto \bar{a}$ ×

例4. $D_8 = \langle x, y \mid x^4 = 1 = x^2,\ yxy^{-1} = x^3 \rangle$

$D_8 \trianglerighteq \langle x \rangle \trianglerighteq \langle x^2 \rangle \trianglerighteq \{1\}$

$D_8 \trianglerighteq \langle x^2, y \rangle \trianglerighteq \langle y \rangle \trianglerighteq \{1\}$

例5. $C_6 = \langle g \mid g^6 = 1 \rangle$　　合成列不唯一.

$C_6 \trianglerighteq \langle g^2 \rangle \trianglerighteq \{1\}$

$C_6 \trianglerighteq \langle g^3 \rangle \trianglerighteq \{1\}$

Jordan-Hölder

设G有两个合成列

$G_0 \trianglerighteq G_1 \cdots G_n$

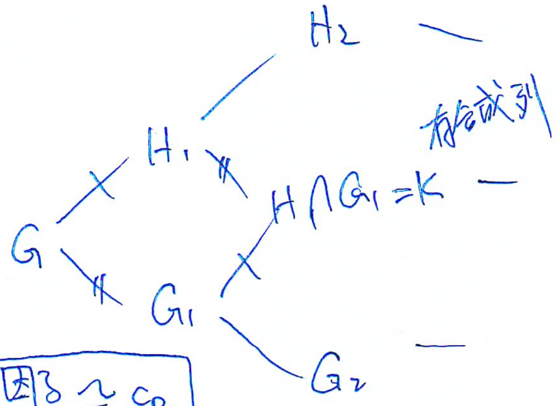
$G_0 \trianglerighteq H_1 \cdots H_m$

$\boxed{\text{则 } n=m\text{, 因子一样}}$

对 $\min(n,m)$ 归纳

$H_1 = G_1$ ✓

$H_1 \neq G_1$　　$G = H_1 G_1$



□

$\boxed{|G| < \infty \text{ 则 } G \text{可解} \iff G\text{的合成因子} \cong C_p.}$

没有真正的因子

Burnside: $|G| = p^a q^b$　G可解

换位子　G群　$g, h \in G$

$[g,h] = ghg^{-1}h^{-1}$　　$[g,h] = 1 \iff gh = hg$

$[G,G]$ = 由换位子生成的子群

Fact (1) $[G,G] \trianglelefteq G$

(2) $G/[G,G] = G^{ab}$

(3) $N \triangleleft G$　$G/N \iff N \supseteq [G,G]$.

132. $G = \langle x_1, \cdots x_n \mid r_1, \cdots r_m \rangle$

$G^{ab} = \langle x_1, \cdots x_n \mid r_1, \cdots r_m, \; x_i x_j x_i^{-1} x_j^{-1} \rangle$