74. 定义 G, H 为群，$f: G \longrightarrow H$ 称为群同态

若 $f(a \cdot b) = f(a) \cdot f(b)$. $\forall a, b \in G$.

双射 + 同态 = 同构

① 群同态 自动把 $1 \mapsto 1$.

② $f(a^{-1}) = (f(a))^{-1}$

$\boxed{EX}$ $f: G \longrightarrow H$ 为同态 则 $\operatorname{ord}(f(a)) \mid \operatorname{ord}(a)$.

若 f 是同构 则 $\operatorname{ord}(a) = \operatorname{ord} f(a)$

例 $U\mathbb{Z}_8 \not\cong \mathbb{Z}_4$. (阶表不同)

$\boxed{EX}$ $(\cdot)^{-1}: G \longrightarrow G$ 则 $(\cdot)^{-1}$ 是同态 $\Leftrightarrow$ G Abel.

$g \mapsto g^{-1}$

$\boxed{EX}$ G 的反群 $G^{op} = \{a^{op} \mid a \in G\}$

$a^{op} \cdot b^{op} = (ba)^{op}$.

则 $G^{op} \cong G$.

例. $\det\ GL_n(\mathbb{C}) \longrightarrow \mathbb{C}^{\times}$

$A \longmapsto \det A$.

例 $n \geq 2$. $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} \leq \mathbb{C}^{\times}$

$\cong \Leftarrow \boxed{EX}$

$(\mathbb{Z}_n, +)$

群的直积(笛卡尔积).

$G \times H = \{(g, h) : g \in G, h \in H\}$. 运算是各自运算 $(1_G, 1_H)$ 为幺元

$\boxed{Rmk}$ $G \hookrightarrow G \times H$

$g \mapsto (g, 1_H)$

$G \times H \twoheadrightarrow G$

$(g, h) \mapsto g$

一些典范的同态

$(g, h) = (g, 1_H) \cdot (1_G, h)$

$= (1_G, h) \cdot (g, 1_H)$

$\operatorname{ord}(g, h) = \operatorname{lcm}(\operatorname{ord} g, \operatorname{ord} h)$.

有时有效.

~~不太对~~

$\boxed{\text{Ex}}$ $\mu_2 \times \mu_2 = V_4$

证 $V_4 \simeq U(\mathbb{Z}_8)$.

$X \subseteq G$

记 (X) = 包含X的最小子群 (由X生成的子群).

$= \{ x_1 \cdots x_n \mid x_i \in G \}$.

若 $X = \{a\}$ $\longrightarrow$ 循环群 G 定义为 $\exists\, a \in G;\ (a) = G$

例 μ_n. $(\mathbb{Z}, +)$

命题 循环群 $G \simeq \begin{cases} (\mathbb{Z}, +) \\ (\mathbb{Z}_n, +) \end{cases}$

取 a. $(a) = G$.

Case 1 $\operatorname{ord}(a) = +\infty$. $a^n \neq a^m$

$(\mathbb{Z}, +) \xrightarrow{\sim} G$ 单 满 ✓
$n \longmapsto a^n$

Case 2 $\operatorname{ord}(a) = n$

$(\mathbb{Z}_n, +) \xrightarrow{\sim} G = \{ \underset{\substack{\uparrow \\ 0}}{0}, \underset{\substack{\uparrow \\ 1}}{a}, \cdots, \underset{\substack{\uparrow \\ n-1}}{a^{n-1}} \}$.

Rmk. $\mu_n \simeq \mathbb{Z}_n$

命题 G 循环.

若 $|G| = \infty$

(1) 恰有两个生成元 a, a^{-1} $G \xrightarrow{\sim} (\mathbb{Z}, +)$ $\mathbb{Z}$ 只有两个生成元. 子群已知.

(2) G 的子群 $\{1_G\}$, (a^d). $d \in \mathbb{Z}$.

若 $|G| \overset{=n}{<} \infty$.

(1) G 有 $\varphi(n)$ 个生成元 (a^k) $\gcd(k, n) = 1$

(2) 对 $\forall\, d \mid n$. $\exists !$ d 阶子群 $\underset{H}{(a^{n/d})} \leq G$ 拉到 $\mathbb{Z}_n$ 上.

$\{G$ 的子群$\} \longleftrightarrow \{ d \mid d \mid n \}$. 拉回即可 推荐

76 无限循环群. $\left\{\begin{pmatrix}1 & n\\ & 1\end{pmatrix}\right\} \leq SL_2(\mathbb{R})$ 或 $\mathbb{Z}$

有限循环群 i.n $G=(a)$. $\mathrm{ord}(a^l)=\frac{n}{\gcd(n,l)}$

$$a^{n/d\cdot k}\in\{a\in G \mid \mathrm{ord}(a)=d\}.$$

$d|n$.

$$\Downarrow$$

$$|\cdot|=\phi(d)$$

再次得到 $|G|=\sum_{d|n}\phi(d)$

$\uparrow$ d阶元.

四 $\forall d|n$ $\exists!$ H_d. d阶. $H_d=\{1, a^{n/d},\dots\}=(a^{n/d})\leq G$.

Fact $|G|=n<\infty$. 则 G 循环 $\Leftrightarrow$ G 有 n 阶元. (易证).

Cor 若 p 为素数. $\Rightarrow$ G_p 为循环群. $(G\simeq \mu_p)$.

proof. Lagrange定理.

定理. $|G|=n<\infty$ 则 G 循环 $\Leftrightarrow$ $\forall d|n$, 至多存在一个 d阶子群

($\Rightarrow$) 已知

($\Leftarrow$) $\forall d|n$. $S_d=\{g\in G. \mid \mathrm{ord}(g)=d\}$.

$$G=\bigsqcup_{d|n} S_d$$

Claim $S_n\neq\phi$. $\forall d|n$. 且 $S_d\neq\phi$. $g\in S_d$. d阶.

$H_d=(g)\leq G$.

$\Rightarrow$ $S_d\subseteq H_d$. $\Rightarrow$ $S_d=H_d$ 若非空

$$n=\sum|S_d|\leq\sum|H_d|=\sum\phi(d)=n \qquad \square$$

$\Rightarrow$ $S_n\neq\phi$.

应用. ~~域中~~ 定理 k域 $G\leq k^\times$ G 有限 $\Rightarrow$ G 循环群

If $n=|G|$. 则 G 有n次本原单位根

例 $\mathbb{C}^\times$ μ_n $\mathbb{Q}^\times$ 不可数 当然不是循环群

$\boxed{EX}$ $\mathbb{Q}^\times$ 不是循环群

proof.

$|G|=n$. $\forall d\mid n$. $H\leq G$. $|H|=d$.

$g\in H$ $g^d=1_H=1_K$.

$\therefore H\subseteq Root_K(x^d-1)$. 致唯一! $\square$

Cor E 有限域. 则 $E^\times$ 是循环群. p^n-1.

$(E/\mathbb{F}_p$ 单扩张$)$

正规子群

群同态 $G\xrightarrow{f}H$ $\Rightarrow\begin{cases}\text{满么}\\\text{满逆.}\end{cases}$

$\underline{\mathrm{Im} f\leq H.}$

$a\overset{f}{\sim}b\iff f(ab^{-1})=1_H$ 一般不同.

$\iff f(b^{-1}a)=1_H$

但 $a^{-1}(ab^{-1})a\overset{\text{"相似"}}{=}ab^{-1}$

Kernel

$N=\ker(f)=\{a\in G\mid f(a)=1\}\leq G.$

$f(a)=f(b)\Rightarrow ab^{-1}\in N\overset{?}{\iff}Na=Nb.$

$\overset{?}{\iff}aN=bN.$

Rmk. Lagrange Thm 右证

Claim $aN=Na$. $b\in aN$ $\iff$ $ba^{-1}\in N$ ($b=ah$, $1=b^{-1}ah$)

$\overset{\star}{\iff}ab^{-1}\in N$

$\iff b\in Na.$

7.8、定义 $N \trianglelefteq G$: $\forall a\in G.\ aN = Na.$ 正规子群
$N \leq G.$

$\forall\ f: G \longrightarrow H$

$\ker G \trianglelefteq H.$

例 (1) G Abel. $\Rightarrow$ 子群正规

(2) $\left\{ \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \right\} \ntrianglelefteq GL_2(\mathbb{F}_2).$

(3) 群的中心 $Z(G) = \{ g\in G \mid g$ 中心元(与任何元交换) $\} \trianglelefteq G.$ EX

Fact. $\forall\ U \leq G.$ $a\in G.$ U 的共轭 $aUa^{-1} = \{ aua^{-1} \mid u\in U \}.$

作为群同构.

Fact $N \trianglelefteq G \Longleftrightarrow \forall a.\ aNa^{-1} = N$
"共轭不变性"

例 $\left\{ \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \right\} \leq GL_2(\mathbb{F}_2)$

$\boxed{EX}$ $N \leq G$ $[G:N] = 2 \Rightarrow N$ 正规.

例. $\det: GL_n(\mathbb{C}) \longrightarrow \mathbb{C}^\times$ 故 $SL_n(\mathbb{C}) \trianglelefteq GL_n(\mathbb{C}).$

$U_n(\mathbb{C}) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix} \right\} \leq GL_n(\mathbb{C})$ 不正规.

设 $N \trianglelefteq G.$ 商群 $G/N = \{ aN \mid a \in G \}$

$\bar{a} = \bar{b} \Longleftrightarrow ab^{-1} \in N$
$b^{-1}a \in N$

$|G/N| = [G:N].$

定义乘法 well-define? $\bar{a} = \bar{a}'$, $\bar{b} = \bar{b}'$ 若 $\overline{ab} \overset{?}{=} \overline{a'b'}$

$\Longleftrightarrow (ab)(a'b')^{-1} \overset{?}{\in} N$

$= a(bb'^{-1})a^{-1} \in N$ ✓, $bb'^{-1} \in N$

Can $\quad G \twoheadrightarrow G/N$

$\ker(\mathrm{Can}) = N.$

群同态基本定理 $\quad f: G \to H$

$\mathrm{Im} f \leq H$

$\ker(f) \trianglelefteq G.$

诱导 $\quad G/\ker f \xrightarrow{\bar f} \mathrm{Im} f$

$\bar a \longmapsto f(a)$

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\mathrm{Can}"'] \arrow[dr, phantom, "\circlearrowright"] & H \\ G/\ker f \arrow[r, "\bar f", "\sim"'] & \mathrm{Im} f \arrow[u, hook] \end{tikzcd}$$

① f 单 $\Leftrightarrow \ker f = 1$

② f 满 $\Leftrightarrow \mathrm{Im} f = H.$

对应定理, $\quad N \trianglelefteq G.$

$\{K \mid N \trianglelefteq K \leq G\} \longleftrightarrow \{G/N$ 的子群$\}.$

$K \longmapsto K/N \leq G/N$

$\trianglelefteq$

此时 $K \trianglelefteq G \Leftrightarrow K/N \trianglelefteq G/N.$

且 $(G/N)/(K/N) \xrightarrow{\sim} G/K.$

证. $\varphi(L) \longrightarrow L \leq G/N.$

$\{\bar a \in L\}$

互逆?

$K \trianglelefteq G \qquad a(K/N)\bar a^{-1} = aKa^{-1}/N = K/N$

$G/N \longrightarrow G/K \qquad \ker = \{aN \mid aK = 1_{G/K}\}$

$aN \longmapsto aK. \qquad = \{aN \mid a \in K\}$

$= K/N.$

80. 设 $N \trianglelefteq G$.

$H \leq G$.

(1) $NH = HN$, $N \leq NH \leq G$.

(2) $(N\cap H) \triangleleft H$ 且 $H/(N\cap H) \xrightarrow{\sim} NH/N$.

$$H \xhookrightarrow{inc} G \xrightarrow{Can} G/N.$$

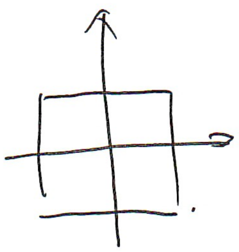
$$h \mapsto h \longmapsto \bar{h}$$ 像. HN/N

核 $\{h\in N\} = H\cap N$.

H 和 N 的顺序?

$\Rightarrow H/H\cap N \cong NH/N$. ($\cancel{HN}$)

$\boxed{EX}$ ...



D_4 V.

$|S(V)| = 4! = 24$.

$S(V)$ (顶点对称群)

$\phi: \Sigma(\square) \longrightarrow S(V)$.

$g \longmapsto (g)_V : V \to V$.

Key Claim. ϕ 单. $\Rightarrow \Sigma(\square) \cong \mathrm{Im}\,\phi$.

$\ker\phi = \{g \mid (g)_V = \mathrm{Id}_V\}$

$= \{g \mid g(OA) = OA, \dots\}$

$= \left\{\begin{pmatrix}1 & \\ & 1\end{pmatrix}\right\}$.

不熟.

例. $x^3-2 \in \mathbb{Q}[x]$. $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^4)$

$= \mathbb{Q}(\sqrt[3]{2}, \omega)$

$E/\mathbb{Q}$ 是分裂的 $|\mathrm{Aut}(E/\mathbb{Q})| = \cancel{\mathrm{Aut}\,E}$ $|\mathrm{Aut}\,E| = \dim_{\mathbb{Q}} E = 6$

$X = \mathrm{Root}_E(x^3-2) = \{a, b, c\}$.

$|S(X)| = 6$. σ 保根

$S(X) = \{\sigma \mid \sigma : X \xrightarrow{\sim} X\}$.

$$\boxed{\phi: \begin{array}{ccc} \mathrm{Aut}\,E & \longrightarrow & S(X) \\ \sigma & \longmapsto & \sigma|_X \end{array}}$$

Key Claim ϕ 是同构

为什么单? $\ker\phi = \{\sigma \mid \sigma|_X = \mathrm{Id}_X\}$ <u>是平凡</u>

但 $\sigma|_{\mathbb{Q}} = \mathrm{Id}$ 恒等.

$= \{\mathrm{Id}\}$.

对称群.

集 X. $S(X) = \{\sigma : X \xrightarrow{\sim} X\}$.

Fact. 若双射 $X \xrightarrow[\sim]{\delta} Y$.

则有同构 $S(X) \xrightarrow{\sim} S(Y)$.

$\sigma \longmapsto \delta \circ \sigma \circ \delta^{-1}$

推论. $|X| = n$, $S(X) \simeq S_n$.

Fact. $|S_n| = n!$

$|S_1| = 1$

$|S_2| = 2$

$|S_3| \leftarrow$ 非交换.

$\underline{n} = \{1, \cdots, n\}$

$S_n = S(\underline{n})$

$\sigma \in S_n$

即 $\underline{n} \xrightarrow{1:1} \underline{n}$

$1 \mapsto \sigma(1)$

$\vdots$

$n \mapsto \sigma(n)$

82

记号 $\sigma \in S_n$

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \longrightarrow |S_n| = n!$$

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \cdots & \sigma(n) \\ 1 & \cdots & n \end{pmatrix}$$

轮换记法 $c = (i_1 \cdots i_\ell) \in S_n$

$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} \cdots i_{\ell-1} \xrightarrow{\sigma} i_\ell$ 其他不变

$i_\ell \xrightarrow{\sigma} i_1$

$c^{-1} = (i_\ell\, i_{\ell-1} \cdots i_1)$

① $\mathrm{ord}(c) = \ell$

② c^{-1}

③ 2-轮换 对换

S_3 S_4 都是非交换的

$S_3 \longrightarrow$ 轮换之积 / 对

$S_4 \longrightarrow$ 不一定是对换之积

引理 σ, τ 是 S_n 中的两个轮换

① 若 σ, τ 不相交 $\Rightarrow \sigma\tau = \tau\sigma$.

② $\sigma \in S_n$ (不一定轮换)

$$\boxed{\sigma (i_1 \cdots i_\ell) \circ \sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_\ell))}$$

令 $\tau = (i_1 \cdots i_\ell)$ $\boxed{\sigma \circ \tau \circ \sigma^{-1} = \tau}$ $\Downarrow$ V

proof:

$$\boxed{\sigma(i_1) \xmapsto{\sigma^{-1}} i_1 \xmapsto{(i_1 \cdots i_\ell)} i_2 \mapsto \sigma(i_2) \cdots}$$

例 $(12)(23)(12)$

$= (12)(23)(12)^{-1}$

$= (13) \neq (23)$ (不交换)

$(23)(12)(23) = (13)$

$(23)(12)(23)$

$(12)(23)(12) = (23)(12)(23)$

$\sigma\tau\sigma = \tau\sigma\tau$

"弱交换性"

命题 $\forall \sigma \in S_n$ $\exists !$ $\sigma = c_1 \cdots c_l$ c_i 轮换. 不交

$\sigma \in S_n$ σ-轨道 on $\underline{n}$

$\{1, \sigma(1), \sigma^2(1), \cdots\}$ 有限长

例. $\sigma = (4\ 5\ 6)(5\ 6\ 7)(7\ 6\ 1)$

$= (1\ 6)(4\ 5)$

设 σ 的型. λ_i 个 i-轮换

$1^{\lambda_1} \cdots n^{\lambda_n}$

$n = \sum_{i=1}^{n} i\lambda_i$

定理. S_n 中 共轭 $\Longleftrightarrow$ 同型

$(\Rightarrow)$ $\sigma = c_1 \cdots c_l$

$h\sigma h^{-1} = \underbrace{(hc_1h^{-1})}_{\text{同型}} \cdots (hc_lh^{-1})$

$(\Leftarrow)$ 同型, 构造 h. 用之前的共轭算式即可.

$\sigma = (\quad)$ $\downarrow h$

$\tau = (\quad)$

例 S_4 共轭类

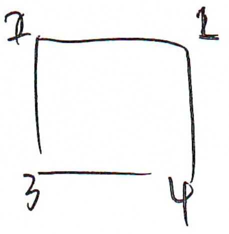
1^4	Id	1
$1^2 2^1$	6个对换	
2^2	3个	
$1^1 3^1$	4×2	8个
4^1	6个	

每个都是 24的因子

$S_3 \hookrightarrow S_4$

非正规

例



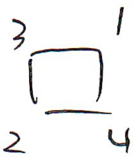
$I(\square) \hookrightarrow S(\underline{4}) = S_4$ 不是正规子群

Id $(1\ 2\ 3\ 4)$ $(1\ 3)(2\ 4)$ $(1\ 4\ 3\ 2)$

$(1\ 4)(2\ 3)$ $(1\ 2)(3\ 4)$ $(1\ 3)$ $(2\ 4)$

84.

$\boxed{Ex}$



H'

等 $H^{\circ} \cap H' \cap H''$

$\boxed{Rx}$

H''

Fact S_n 可由 $(12) \ldots$ ~~$(n-1\ n)$~~ $(n-1, n)$ 生成.

$(ij) = \cancel{(1\ 2)} \cdots$ ~~$(i+1\ i+2) \cdots i$~~

$(i+1\ j)(i\ \ i+1)(i+1\ j)^{-1}$

$(i_1 \cdots i_\ell) = (i_{\ell-1}\ i_\ell) \cdots (i_2\ i_\ell)\ (i_1\ i_\ell)$

$\boxed{Rmk}$ $s_i = (i\ \ i+1)$

(1) $s_i^2 = Id$

(2) $s_i\, s_{i+1}\, s_i = s_{i+1}\, s_i\, s_{i+1}$

(3) $s_i s_j = s_j s_i$ $\quad |j-i| \geq 2$

$S_n \hookrightarrow GL_n(\mathbb{R})$ 置换矩阵 即.换行

可以换成任意一个域

$\sigma \longmapsto P_\sigma$

$(ij) \longmapsto P_{ij} \longmapsto -1$ 这个嵌入是单的

$S_n \xrightarrow{sgn} \{\pm 1\}$ $\quad S_n \hookrightarrow GL_n(\mathbb{R}) \xrightarrow{det} \mathbb{R}.$

A_n {偶置换}.

$|A_n| = \frac{n!}{2}$ $\quad S_n / A_n \simeq \{\pm 1\}$

Fact $\operatorname{sgn}(i_1 \cdots i_m) = (-1)^{m-1}$

since $(i_1 \cdots i_m) = (i_1\, i_m)(i_1\, i_{m-1}) \cdots (i_1\, i_2)$

$A_3 = \{ \mathrm{Id}, (132), (123) \} \trianglelefteq S_3.$

S_3 的子群格

$$\begin{tikzcd}[column sep=small]
 & & S_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[r, dash] & A_3 \arrow[ddl, dash] \\
\{\mathrm{Id}, (12)\} & \{\mathrm{Id}, (23)\} & \{\mathrm{Id}, (13)\} & \\
 & \{\mathrm{Id}\} \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

S_4 (共轭类).

1^4	Id	1.
$1^2 2^1$	(12), (13), (14), (23), (24), (34)	6.
2^2.	(12)(34) (13)(24) (14)(23)	3.
$1 \cdot 3^1$	~~(123)~~	8.
4^1.		6

24.

[illegible] ✓.

S_4 的正规子群分类.

↓

有共轭类封闭性.

$N \trianglelefteq S_4$ ⇒ 共轭类之并.

$12. = 1 + 3 + 8 = \cancel{6+6}$ $\quad A_4.$

$8 = 1 + X.$

$6 = 1 + X$

$4 = 1 + 3 \quad K_4.$

K_4 是 S_4 的正规子群.

$\boxed{\text{EX}}$. $K_4 \cong V_4$

S_4/K_4 按定义要算陪集代表元.

$\parallel$

$\{gK_4\}$

有6个. 是什么呢?

定义 G单群. 若G无非平凡的正规子群.

$\boxed{Ex}$ $|G|<\infty$. G Abel G单 $\Leftrightarrow$ 素阶循环群.

Thm $n\geq 5$. A_n是单群.

$(\because K_4 \trianglelefteq A_4)$

注. $n\geq 5$. S_n非可解

推论 $n\geq 5$. 则 A_n是 S_n的唯一非平凡正规子群

证: $N \ntrianglelefteq S_n$. $N\cap A_n \ntrianglelefteq A_n$.

$$A_n \hookrightarrow S_n \twoheadrightarrow S_n/N.$$

$\Rightarrow$ ① $N\cap A_n = A_n \Rightarrow A_n = N$

② $N\cap A_n = \{\mathrm{Id}\}$.

$A_n \hookrightarrow S/N \xrightarrow[\text{共轭不封闭}]{|N|=2}$ 乙.

~~proof of thm~~: ① A_n由3-轮换生成 $n\geq 3$.

② 3-轮换在A_n中共轭. $n\geq 5$.

③ $N \trianglelefteq A_n$. 则N有3-轮换.

定理 $|G|<\infty$. $C\subseteq G$ 共轭类. $|C| \mid |G|$.

例 $|A_4|=12$.

Id

~~(12)(34)~~ ··· 在 S_4 中共轭. A_4 中呢 $8\nmid 12$.

要分类!

$\boxed{\text{问 } \exists ? \quad \sigma\in A_4}$

$\sigma(12)(34)\sigma^{-1} = (13)(24)$

$\|$

$(\sigma(1)\ \sigma(2))(\sigma(3)\ \sigma(4))$

A_4.

① $\begin{cases}\sigma(1)\sigma(2) = (1\ \ 3)\\ \sigma(3)\sigma(4) = (2\ \ 4)\end{cases}$

(1.1) $\sigma(1)=1$ $\sigma(2)=3$ $\sigma(3)=2$ $\sigma(4)=4$ X.

(1.2) $\sigma(1)=3$ $\sigma(2)=1$ $\sigma(3)=4$. $\sigma(4)=2$.

⋮

~~假设 σ~~ ···

问题 (123) (132) 在 A_4 不共轭?

$(\sigma(1)\ \sigma(2)\ \sigma(3)) = (1\ \ 3\ \ 2)$ 找 σ $\longrightarrow$ 找不到.

Check!

例 $|A_4| = 12 = 1+3+4+4$

$\boxed{\text{EX}}$ A_4 没有 6 阶子群

群作用. 群 G 左作用于集 X. $G \curvearrowright X$

(置换表示) 映射 $G\times X \xrightarrow{\varphi} X$ 满足 ① $1_G.x=x$ $\forall x$

$(g,x)\longmapsto g.x$. ② $h.(g.x)=(hg).x$ $\forall x, h, g$.

此时 X 为左 G-集

$S(X) \curvearrowright X$. [$S_n \curvearrowright \underline{n}$]

$S(X) \times X \xrightarrow{\rho} X$

$(\sigma, x) \longmapsto \sigma(x)$

$X = (X, \rho)$ 为左 $S(X)$ 集.

例. K/k. $\mathrm{Aut}(K/k) \curvearrowright K$.

$\mathrm{Aut}(K/k) \times K \xrightarrow{\rho} K$.

$(\sigma, a) \longmapsto \sigma(a)$

例 $GL(V) \curvearrowright V$, V线性空间

Fact. 左G集 (G, ψ).

有 $\rho : G \longrightarrow S(X)$

$g \longmapsto \rho(g)$. 把群元变为置换.

其中 $\rho(g) : X \longrightarrow X$. 问 $\rho(g)$ 是否双射?

$x \qquad gx$. $\cancel{\rho^{-1}}$ $g^{-1}g(x) = x$.

单位性.

check. ρ为群同态.

$\rho(gh)$

$gh(x) = g(hx) = \rho(g)\rho(h)x$

i.e. 左G集 $\Rightarrow$ 群同态.

Fact 反之. 从群同态 $G \xrightarrow{\rho} S(Y)$ $G \curvearrowright Y$

$\boxed{\text{Ex}}$ $g.y = \rho(g)(y)$ 为作用

注 右作用 $X \circlearrowleft G$.

给定 $G \curvearrowright X$.

① X 的 G-轨道.

$$x \in O_x = \{ g.x \mid g \in G \}$$

② orbit $\longrightarrow$ 等价类

$$X = \coprod_{x \in X} O_x \quad \text{轨道分解}$$

定义 $G \curvearrowright X$ 可迁, 若 仅有一个轨道.

Fact $G \curvearrowright X$

则 $G \curvearrowright O_x$ 可迁.

$G \curvearrowright X$ 中 x 是 G 的稳定化子

$$G_x = \{ g \mid gx = x \} \leq G.$$

引理. $x = hy$ $h \in G$. $(O_x = O_y)$

则 $G_x = hG_yh^{-1}$ ($\Rightarrow$ G_x G_y 同构)

自己证.

例. $H \leq G$. $G/H = \{ aH \mid a \in G \}$

则 $G \curvearrowright G/H$.

$g(aH) = \cancel{(ga)}\, gaH$ 可迁的.

左陪集作用. $\boxed{EX}$ $G_{aH} = aHa^{-1}$ $G \curvearrowright G/1_G$ 左正则作用.

$g.x = gx$

例 $S_n \curvearrowright \underline{n}$ 可迁.

$\forall i \in \underline{n}$ 稳定化子 $\cong S_{n-1}$

例 $\forall \sigma \in S_n$. $(\sigma) \leqslant S_n$ 则 $G = (\sigma) \curvearrowright \underline{n}$ 的轨道?

例 K/k.

$\mathrm{Aut}\, K/k \curvearrowright K$.

$\sigma . a = \sigma(a)$.

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

$\mathrm{Root}_K f \overset{<\infty}{=} \{a \in K \mid f(a) = 0_K\}$.

key Fact. $\underset{\sigma}{\mathrm{Aut}\, K/k} \curvearrowright \underset{a}{\mathrm{Root}_K f}$

$\underline{(\sigma(a) \in \mathrm{Root}_K f)}$.

更进一步. K/k 为 $f(x) \in k[x]$ 的分裂域. 则

$\mathrm{Gal}_k(f) = \mathrm{Aut}(K/k) \curvearrowright \mathrm{Root}_K(f)$.

$$\mathrm{Aut}\, K/k \xrightarrow{\ \rho\ } S(\mathrm{Root}_K(f)).$$

$$\sigma \longmapsto \sigma|_{\mathrm{Root}_K(f)}.$$

① 是单射. $\sigma|_{\mathrm{Root}_K f} = \mathrm{Id}$ 则 $\sigma = \mathrm{Id}$

② $f(x)$ k上不可约. $\Leftrightarrow$ 可迁! $\exists \sigma$ $\underset{\text{直证}}{\ }$ $\sigma(a) = b$

$$\begin{tikzcd} K \arrow[r, "\exists\sigma"] & K \\ k(a) \arrow[u, phantom, "\cup"] \arrow[r, dashed] & k(b) \arrow[u, phantom, "\cup"] \\ k \arrow[u, bend left] \arrow[r] & k \arrow[u, bend right] \end{tikzcd}$$

例 $GL_2(\mathbb{F}_2)$

$G = GL_2(\mathbb{F}_2) \curvearrowright (\mathbb{F}_2)^2 = V$.

两轨道 $\begin{pmatrix}0\\0\end{pmatrix}$

$\begin{pmatrix}1\\0\end{pmatrix} \begin{pmatrix}0\\1\end{pmatrix} \begin{pmatrix}1\\1\end{pmatrix} = X$

$G \curvearrowright X$ 可迁.

$\therefore \exists\ \rho : G \longrightarrow S(X) \simeq S_3$.

$\boxed{\text{EX}}$ ρ 是同构.

定理 $G \curvearrowright X \quad x \in X$

则 $\exists$ 双 $\quad G/G_x \xleftrightarrow{1:1} O_x$

G-集间的同构 $\quad aG_x \longmapsto ax$

注 G-集之映射

$(X, \psi) \xrightarrow{f} (Y, \varphi)$

(1) $X \xrightarrow{f} Y$

(2) 相容 $f(g.x) = g.f(x) \quad \forall g \in G$.

proof: 良定性. $aG_x = bG_x \quad \exists\ h \in G_x \quad a = bh$

$a.x = (bh).x$
$= b.(hx)$
$= b.x$.

若 $ax = bx$

$\Rightarrow aG_x = bG_x$ 单

$\Rightarrow$ 同构

Cor 轨道-稳定化子公式. $|G| \overset{<\infty}{=} |G_x||O_x|$

9.2

定义 $G \curvearrowright X$ 忠实的. $\forall 1 \neq g \in G$

$\exists x \in X$ s.t. $g.x \neq x$

$\Longleftrightarrow$ $\rho: G \hookrightarrow S(X)$ $\ker = 0$

Rmk $\boxed{\ker\rho = \bigcap_{x\in X} G_x}$ Ex

例. $G \curvearrowright X$ 左正则. $g.a = ga$ 忠实的

Cayley 定理

定义 $G \curvearrowright X$ 自由. 若 $G_x = \{1_G\}$ $\forall x \in X$

稳定 $\Longrightarrow$ $|Gx| = |G|$

轨道分解 $\Longrightarrow$ $|G| \mid |X|$

例 $H \leq G$ 则 $H \curvearrowright G$

$h.a = ha$

$\Longrightarrow |H| \mid |G|$ 再次证明 L 定理.

定义 $G \curvearrowright X$ 平凡

若 $g.x = x$ $\forall g, x$.

此时 $\rho: G \to S(X)$
$\forall g \mapsto Id_X$

共轭作用 $G \curvearrowright X = G$
$g.x = gxg^{-1}$

(1) 作用平凡 $\Longleftrightarrow$ G Abel

(2) $x \in G$ 的轨道.
$Gx = \{gxg^{-1} \mid g \in G\}$ 共轭类.

$\Rightarrow$ 轨道公式 $\underline{|Gx| \mid |G|}$ 是之前的定理.

例 $Gx = \{x\} \Leftrightarrow x =$ 中心元 $Z(X)$

同. x 的 stabilizer

$x \in Z(x) = \{g \mid gx = xg\}$

中心化子.

~~共轭群同一类~~

$|G| = |Gx||Z(x)|$.

<u>类公式</u> $|G| = |Z(G)| + \sum_{|Gx|>1} |Gx|$ (分类罢了)

例. $A_4 \ni (123)$

$|G(123)| = ?$

$12 = |A_4| = \underline{|Z(123)|}_{\mathbb{Z}_3} |G(123)|_{\leq 4}$

---

p-群 $|G| = p^n$, p prime.

注 $|G| = p \Rightarrow G \simeq \mathbb{Z}_p$

例 p-群有非平凡中心.

$|Z(G)| = p^r$

若 $|Z(G)| = 1 \Rightarrow |G| = 1 + \sum_{|Gx|>1} \underset{p^s}{\underset{\shortparallel}{|Gx|}}$ X.

9.14 命题 p^2 阶群是 Abel 群 同构于 $(\mathbb{Z}_{p^2},+)$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

$Z(G)$ 不平凡

$1 \neq g \in$

(1) $\mathrm{ord}(g) = p^2$ ✓

(2) $\mathrm{ord}\, g = p$ $H = \{1, g, \cdots g^{p-1}\} \leq G$.

$g' \notin H$

$\Rightarrow \langle g, g' \rangle = G$.

$$\begin{matrix} 1 & g & \cdots & g^{p-1} \\ g' & gg' & \cdots & g^{p-1}g' \\ \vdots & & & \end{matrix} = \underset{H}{\langle g \rangle} \times \underset{K}{\langle g' \rangle}.$$

(可证明)

$\boxed{EX}$ $H \times K \xrightarrow{\Phi} G$ 是同态
$(h, k) \longmapsto hk$.

例 $S_4 \curvearrowright X = \{(12)(34)\ (13)(24)\ (14)(23)\}$

$S_4 \xrightarrow{\rho} S(X) \simeq S_3$

$\boxed{EX}$ $\ker \rho$.

例 $H \leq G$. $G \curvearrowright X_H = \{H' \leq G \mid H' 与 H 共轭\}$

$g \cdot H' = gH'g^{-1}$

H 的 stabilizer

$H \subseteq N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

H 而正规化 $N_G(H) = G$.

$H \trianglelefteq G \Longleftrightarrow X_H = 1$

有 $|G| = |X_H|\,|N_G(H)|$

Sylow子群. $|G| = p^r m$. $p \nmid m$

子群 $P \le G$ 称 Sylow p-子群

若 $|P| = p^r$, $[G:P] = m$.

Thm (Sylow) $|G| = p^r \cdot m$ $p \nmid m$. 则

(1) 总有 Sylow p-子群.

(2) Sylow p 子群间相互共轭.

(3) Sylow p-子群个数 是m的因子, 且形如 $kp+1$.

(4) $\forall$ p 子群 $B \le G$. 总存在 ~~Sylow~~ P 子群 P s.t. $B \subseteq P$.

例 $|S_4| = 3^1 \cdot 2^3$.

Sylow 3 子群 = 3阶子群.

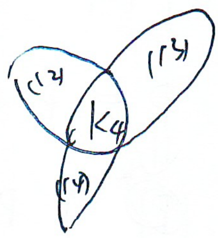
$(3+1) \mid 8$ 4个

Sylow 2 子群

② 8阶子群. 不正规.

$\overset{\|}{2k+1} \mid 3$.

恰有 3个.



命题. 108 阶群非单群

$|G| = 2^2 \cdot 3^3$

取 $P \le G$. $|P| = 27$

$G \curvearrowright G/P$. 非平凡.

$\rho : G \longrightarrow S(G/P) \cong S_4$

$\ker \rho \ne G$

$\{1\} \ne \ker \rho \lhd G$.

例 $|G|=35$. $|G|$循环

$|G| = 5\times 7$

$|5阶个数| = \dfrac{5k+1}{k=0.} \mid 7$

1个.

$\Rightarrow \exists P \trianglelefteq G.$ $+$ $P\cap Q=\{1\}$

$\exists Q \trianglelefteq G$ $|Q|=7$ $\Downarrow$ $\boxed{EX}$

$P\times Q \simeq G$

~~$\Rightarrow \exists!$ Sylow P 子群~~

例 $|G| = p_1^{k_1}\cdots p_t^{k_t}$

G Abel

$\Rightarrow \exists!$ Sylow p_i 子群 P_i $\boxed{EX}$

$P_1\times\cdots P_t \xrightarrow{\sim} G$

Thm (Cauchy). $p\mid |G| \Rightarrow$ G有p阶元

记 取 P = p-子群

$\Downarrow$

$|P|$ 阶 p^k. $g^{p^a}=1$

令 $g^{p^{a-1}}$

$\boxed{EX}$ P40 2, 4, 7, 8, 13

例. $|G|=56$ 则 G 非单

$56=7\times 2^3$

7阶 P. $7k+1 \mid 8$ $k=1$? $\dfrac{k=0?}{正规}$. ~~幂零群~~

$H_1\cdots H_8$

$H_i\cap H_j=\{1\}$

$\left|\bigcup^8 H_i\right| = 49$ $\Rightarrow$ 中心有一个

正规. 不可能

Proof of Sylow. thm

$|G| = p^r \cdot m \quad p \nmid m$

Claim $\exists P \leq G.\ |P| = p^r$

$X = \{ U \subseteq G \mid |U| = p^r \} \subseteq \mathcal{P}(G)$

群作用 → 轨道 → 稳定化.

$G \curvearrowright X$

$|X| = \binom{p^r m}{p^r} = \dfrac{n \cdots (n - p^r + 1)}{p^r \cdots 1}$ $p \nmid |X|$

$X = \dot{\bigsqcup} O_u$

$\exists u.\ p \nmid |O_u|$

$G_u = \{ g \in G \mid gu = u \} \leq G.$

$|G| = |G_u| \cdot |O_u| \qquad |G_u| = p^r \cdot m' \quad m' \mid m$

注. $G_u \overset{\text{free}}{\curvearrowright} U \qquad g.x = gx \in U$

$g \in G_u$, $x \in U$

$|G_u| \mid |U|$ $\square$

另一证明 $n \gg 1$

$G \hookrightarrow GL_n(\mathbb{F}_p) \qquad G \hookrightarrow S(G) \hookrightarrow \cdots$

$\boxed{EX}$ $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

$= p^{\frac{n(n-1)}{2}} q$

GL_n 有天然的 Sylow 子群 $\left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$

$\boxed{EX}$ $H \leq K$. finite P 是 K 的 Sylow p-子群

则 $\exists g \in K$. s.t. $H \cap gPg^{-1}$ 为 H 的 Sylow 子群

Hint. $H \curvearrowright K/P$?

98 群表现 representation　　表示 representation

Aim　$G = F/N$　F free　$N \triangleleft F$

free group.　$X \neq \phi$　$X^{-1} := \{x^{-1} \mid x \in X\}$

$X \sqcup X^{-1}$ = 字母

<u>Def</u>　Word　$w = x_1 \cdots x_s$　$x_i \in X \sqcup X^{-1}$

reduced　if $\nexists\, i$　$x_i = x_{i+1}^{-1}$

<u>Fact</u>　$\forall$ word 可被约化为唯一的既约字

对字长归纳

EX

空字 = 1　约定 空字也是既约的

<u>Def</u>　X生成的自由群 $F(X) := \{$所有的以 $X \sqcup X^{-1}$ 为字母的既约字全体$\}$.

乘法，字的连接 + 约化

接头可约

结合律．$w_1(w_2 w_3) = (w_1 w_2) w_3 \Longleftarrow$ $w_1 w_2 w_3$ 的约化

本质上是既约的唯一性．

若 $|X| < \infty$．$F(X)$ 为有限生成自由群

例 $X = \{a\}$　$F(X) \cong (\mathbb{Z}, +)$

$X = \{x, y\}$　$F(X)$ 太大了

<u>Prop</u>　泛性质　$f: \underset{\text{Set}}{X} \longrightarrow \underset{\text{group}}{G}$　f 可唯一延拓为群同态

$\hat{f}: F(X) \longrightarrow G$

$\hat{f}|_X = f$

$$\begin{tikzcd} F(X) \arrow[dr, dashed, "\tilde{f}"] & \\ X \arrow[u] \arrow[r, "f"'] & G \end{tikzcd}$$

Cor $\forall G$ 都是自由群的商群.

$X \subseteq G$ 生成元集 (e.g $X = G$)

$inc : X \hookrightarrow G$.

$\widetilde{inc}: F(X) \twoheadrightarrow G$ □

定义. 群的有限表现 指

$G = \langle x_1, \cdots x_n \mid r_1, \cdots r_n \rangle$

$r_i \in F(x_1, \cdots x_n)$

$$\| \quad F(x_1, \cdots x_n) / N(r_1, \cdots r_n)$$

包含 $r_1, \cdots r_n$ 的最小正规子群

$\boxed{Ex}$ $N(r_1, \cdots r_n) = \{ w r_j w^{-1} \mid w \in F(x_1, \cdots x_n) \}$ $1 \le j \le n$

命题. $G = \langle x_1, \cdots x_n \mid r_1, \cdots r_n \rangle$.

$f: X \to H$ 同态

则 $\hat{f}: G \to H \iff f(x_1) \cdots f(x_n)$ 在 H 中满足关系.

例 $G = \langle x, y \mid x^2, y^2, (xy)^3 \rangle \cong S_3$.

$x \mapsto (12)$ $\quad f: \{x, y\} \to S_3$

$y \mapsto (13)$ $\quad (12)(13) = (132)$ $\quad N \subseteq \ker \tilde{f}$

可延拓 $\hat{f}: G \twoheadrightarrow S_3$

100 Claim $G = \{x, y, xy, yx, xyx, 1\}$

claim $w \in$ RHS $\quad x^2=y^2=1,\ (xy)^3 = 1 \Rightarrow xyx = yxy$

$w = xyxy\cdots = \cancel{x}xy\,\cancel{x}xy\cdots$

或 $= yxyx\cdots =$

长度 / 8降

例 $D_6 = \{g \in O_2 \mid g(⬡) = ⬡\}$

6个旋转 6个对称

$a \in D_6 \quad a^6 = 1$

$b \in D_6 \quad \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \quad b^2 = 1 \qquad b, ba, \ldots, ba^5$ 是对称

$(ba)^2 = 1$

定义 $G = \langle a, b \mid a^6 = b^2 = (ab)^2 = 1 \rangle$

证: $G \cong D_6 \qquad G \twoheadrightarrow D_6$

Claim $G = \{x^i y^j \mid 0 \le i \le 5,\ 0 \le j \le 1\} \Rightarrow |G| = 12.$

$|G| \le 12$

$xyxy = 1$

$yx = x^5 y$

$\boxed{EX}$ $\langle s, t \mid s^2, t^2, (st)^6 \rangle \cong D_6.$

例 Q_8 四元数 $\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k = \mathbb{H} \qquad ij = k \quad jk = i \quad ki = j$

非交换环，可除环

$Q_8 \le \mathbb{H}^* = \mathbb{H} \setminus \{0\}$

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ 非Abel.

in Q_8 $(ij)^4 =$

令 $G = \langle x, y \mid x^4 = 1, x^2 = y^2, yx = x^3 y \rangle$.

与 $\Sigma(\square)$ 不同构.（表现不同）.

有限生成Abel群

加法群的直和 $A \oplus B := A \times B$

$\mathbb{Z}^n_{col} = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right\}$

Fact $\mathbb{Z}^n$ 由 $\vec{e}_1, \cdots \vec{e}_n$ 生成 —— 整线性组合

$\boxed{\text{定义}}$ 加法群 $S \subseteq A$ 为 A 的有限基.
$|S| < \infty$

(1) $\forall a \in A.\ a = \sum_i n_i s_i \quad s_i \in S$. （$S$生成$A$）

(2) S 是$\mathbb{Z}$线性无关

有限 Abel 群 没有基. 如 $\mathbb{Z}_n$. $na = 0$ 一个元素都不线性无关

$\boxed{\text{命题}}$ A Abel 有有限基 $\Longleftrightarrow A \simeq \mathbb{Z}^n$

秩 n 的自由Abel群

证明 平凡, 略

$\boxed{\text{Ex}}$ $\mathbb{Z}^n \simeq \langle x_1 \cdots x_n \mid x_i x_j = x_j x_i \ \forall i,j \rangle$.

Aim：分类 有限生成 Abel群（同构意义下分类）

$\exists |S| < \infty \quad S$生成$A$
$S \subseteq A$

由于無挠, 需要更精细处理.

$\boxed{\text{Fact}}$ A f.g $\Rightarrow A \simeq \mathbb{Z}^n / K.\ K \leq \mathbb{Z}^n$

Proof：$\mathbb{Z}^n \twoheadrightarrow A$ $\square$

$\mathbb{Z}^n$ 的子群是什么？ 这不是平凡的

$\boxed{\text{Fact}}$ 设 $K \leq \mathbb{Z}^n$ 则 K f.g.

$n=1 \quad n\mathbb{Z} \leq \mathbb{Z}^n$

$n=2 \quad K \leq \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$

$\underbrace{(K \cap \mathbb{Z}e_1)}_{f.g.} \leq \mathbb{Z}e_1 \leq \mathbb{Z} \oplus \mathbb{Z}$

102

$\underbrace{K/K\cap \mathbb{Z}e_1}_{f.g.} \simeq K+\mathbb{Z}e_1/\mathbb{Z}e_1 \le \mathbb{Z}^2/\mathbb{Z}e_1 \simeq \mathbb{Z}$. (Abel总正规)

$\boxed{\text{EX}}$ $N \triangleleft G$. N f.g. G/N f.g $\Rightarrow$ G f.g

由$\boxed{\text{EX}}$. K f.g. $n=2$ ✓ n一般是一样的

矩阵

$A \in Mat_{n\times m}(\mathbb{Z})$

$\phi_A : \mathbb{Z}^m_{col} \longrightarrow \mathbb{Z}^n_{col}$ Abel群同态

$\vec{v} \longmapsto A\vec{v}$ $\mathbb{Z}$线性映射

$e_i \longmapsto A$的第i列

$\boxed{\text{Fact}}$ 任何一个同态 从 $\mathbb{Z}^m \longrightarrow \mathbb{Z}^n$. 都形如$\phi_A$

记 $A = \begin{pmatrix}\theta(e_1) & \cdots & \theta(e_m)\end{pmatrix}$ 这些还都取

复合 $\longrightarrow$ 矩阵乘法

$\phi_B \circ \phi_A = \phi_{BA}$

$\boxed{\text{命题}}$ $\mathbb{Z}^m \simeq \mathbb{Z}^n \Rightarrow m=n$ 秩是良定的

若同构$\Leftrightarrow$ 矩阵可逆 $\Rightarrow m=n$

$\boxed{\text{定义}}$ $A \in Mat_{n\times m}(\mathbb{Z})$ $\phi_A : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$

$\mathrm{Im}(\phi_A) \le \mathbb{Z}^n$

ϕ_A的余核 $\mathrm{coker}\,\phi_A = \mathbb{Z}^n/\mathrm{Im}\,\phi_A$

由A的列生成

$\boxed{\text{key Fact}}$ f.g. Abel G 均同构于某个 $\mathrm{coker}\,\phi_A$

$G \simeq \mathbb{Z}^n/K$

K f.g $=$ Span $(v_1 \cdots v_m)$

令 $A = (v_1 \cdots v_m)_{n\times m}$ $\boxed{\mathrm{Im}\,\phi_A = K}$ $\Rightarrow G \simeq \mathrm{Coker}\,\phi_A$ □

$\phi_A : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$

$e_i \mapsto v_i$

问题驱动 线性代数 —— Coker 的分类

关键一招是 Smith 标准型保持 coker

$\underline{GL_n(\mathbb{Z})} \Rightarrow \{A \mid \det A = \pm 1\}$ (幺模阵)

用 A^* 看看就知道

$\boxed{EX}$ $A \in M_n(\mathbb{Z})$

$A \in GL_n(\mathbb{Z}) \iff \phi_A : \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^n$

$GL_n(\mathbb{Z}) \simeq Aut(\mathbb{Z}^n)$

$\boxed{定义}$. $A, B \in M_{n\times m}(\mathbb{Z})$

称 A B 相抵 当 $\exists P \in GL_n$ $Q \in GL_m$ $A = PBQ$.

$\boxed{Key Fact}$ $A \sim B \Rightarrow Coker(\phi_A) \simeq Coker(\phi_B)$

相抵 $\Downarrow$ 交换

$AB = P^{-1}AQ$

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{\phi_A} & \mathbb{Z}^n & \xrightarrow{can} & Coker\ \phi_A \ni \phi_P(\bar{v}) \\ \uparrow \phi_Q \wr & \circlearrowleft & \uparrow \wr \phi_P & & \uparrow \\ \mathbb{Z}^m & \xrightarrow{\phi_B} & \mathbb{Z}^n & \xrightarrow{can} & coker\ \phi_B \ni \bar{v} \end{array}$$

$\bar{v} = \bar{v}'$

$v - v' \in Im\ \phi_B$

$\phi_P(v - v') \in Im\ \phi_A$

$\boxed{EX}$ $\bar{\phi}_B$ 是群同构

$\boxed{定理}$ $A \in Mat_{n\times m}\mathbb{Z}$

$$A \text{ - } \mathbb{Z}\text{相抵于} \begin{pmatrix} \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix} & 0 \\ 0 & 0 \end{pmatrix}$$

$1 \le d_1 \mid d_2 \mid \cdots d_r$

$r = rank\ A$.

例子 $\begin{pmatrix} 2 & 4 \\ 6 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & \\ & 14 \end{pmatrix}$

$\mathbb{Z}^2 /) = \underline{14个}$

104 $G_1 \cdots G_n$ 群

Ex $N_i \lhd G_i$

(1) $(N_1 \times \cdots N_n) \lhd (G_1 \times \cdots G_n)$

(2) $\frac{G_1 \times \cdots \times G_n}{N_1 \times \cdots N_n} \cong \prod_1^n G_i/N_i$

三) 有限 Abel 群的结构定理

G f.g Abel

$\Rightarrow G \cong (\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s$

$s \geq 0$

$1 \leq d_1 \mid d_2 \cdots \mid d_r$

特别地 若 $|G| < \infty$

$G \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$

算 $\underline{\underline{\text{Coker} A}} \sim \text{Coker } S$ □

Fact $A \in \text{Mat}_n \mathbb{Z}$

$\det A \neq 0 \Rightarrow |\text{Coker } \varphi_A| < \infty$

$\| $

$|\det A|$

$G \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ ✓

$A \sim \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix} \Rightarrow$

Fact. $K \leq \mathbb{Z}^n$ ($\Rightarrow K$. f.g)

则 $\exists \mathbb{Z}^n$ 基 $\vec{e}_1 \cdots \vec{e}_n$

和 $1 \leq d_1 \mid \cdots \mid d_r$

s.t K 中的 $d_1\vec{e}_1 \cdots d_r\vec{e}_r$ 为基

$\Rightarrow K$ f.g. 自由 $\text{rank}(K) = r \leq n$

证. K f.g $\exists A$ s.t $K = \mathrm{Im}\,\phi_A$

取 $A \sim$ Smith $\Rightarrow K < d_1 e_1, \cdots d_n e_n >$.

K的生成元为 $\xi_1 \cdots \xi_m$ $\quad A = (\xi_1 \cdots \xi_m)_{n\times m}$

$A_{n\times m}$ $\quad$ ~~$\mathbb{Z}^m \to \mathbb{Z}^m$~~ $\quad \mathbb{Z}^m \to \mathbb{Z}^n$

~~$e_i \mapsto \xi_i$~~

扭子群 $\quad g \in G$ 有限阶 $\Leftrightarrow ng = 0_G$.

扭元

定义. $(G,+)$ 的扭子群

$t(G) = \{ g \in G \mid g \text{ 有限阶} \}$.

定义. G torsion free 若 $t(G) = \{0_G\}$

称 G 扭群. 若 $G = t(G)$

例 $\mathbb{Q}/\mathbb{Z}$

$\boxed{\text{Ex}}$ f.g. 扭群 = finite

定理 G f.g. Abel群

则 $\exists$ 内直和

$G = t(G) \oplus F$

s.t F f.g 自由 Abel

Rmk. F 同构唯一.

$$G \simeq \underbrace{(\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r})}_{t(G)} \oplus \underbrace{\mathbb{Z}^s}_{F}$$

$$G \xrightarrow[\sim]{\theta} \underbrace{(\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s}_{= R}$$

$$t(G) \xrightarrow{\sim} t(R) = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus (0\,\mathbb{Z})^s$$

$$\underset{内}{R} = t(R) \oplus \underbrace{F'}_{\cong \mathbb{Z}^s}$$

作用 θ^{-1} $\quad G = t(G) \oplus \underbrace{\theta^{-1}(F')}_{= F}$

Fact $\quad F \cong G/t(G)$ $\quad \square$

例 $G = \mathbb{Z}_2 \times \mathbb{Z}$

$F_1 = \{0 \times n\}$

$F_2 = \{\bar{n} \times n\}$

$\boxed{\text{EX}}$ 写作为的 G 的 F ~~只有两个~~ 只有两个.

Hint：看生成元

$\boxed{\text{Cor}}$ G torsion free 且 f.g.

$\Rightarrow G$ 自由 Abel

定义 G. f.g Abel

rank G = rank F

Fact $\quad G\ H$. f.g Abel

$$G \cong H \iff \begin{cases} t(G) \cong t(H) \\ \text{rank } G = \text{rank } H \end{cases}$$

G f.g. Abel

$G \simeq \mathbb{Z}_{d_1} \times \cdots \mathbb{Z}_{d_r}$

$d_i = p_1^{s_{i1}} \cdots p_l^{s_{il}}$ ⟶ 不变因子.

$\begin{cases} s_{11} \le \cdots \le s_{r1} \\ \vdots \\ s_{1l} \le \cdots \quad s_{rl} \end{cases}$

$\mathbb{Z}_{d_i} \simeq \mathbb{Z}_{p_1^{s_{i1}}} \times \cdots \mathbb{Z}_{p_l^{s_{il}}}$ 类比 模的空间

$G = B_{p_1} \times \cdots \times B_{p_l}$ Sylow

$B_{p_1} = \mathbb{Z}_{p_1^{s_{11}}} \times \cdots \mathbb{Z}_{p_1^{s_{r1}}}$ 初等因子

Fact. B Abel p群

$B \simeq \mathbb{Z}_{p^{s_1}} \cdots \mathbb{Z}_{p^{s_l}}$ $\Rightarrow l = r \quad s_1 = t_1 \cdots$

$\simeq \mathbb{Z}_{p^{t_1}} \cdots \mathbb{Z}_{p^{t_r}}$

证. $B \supseteq pB \supseteq \cdots p^m B = 0$

$p^k B / p^{k+1} B$ $\mathbb{F}_p$ 线性. 算维数 $\dim\left(p^k B / p^{k+1} B\right)$ 对分量计算

$\#$

$\sim$

$s_1 \cdots s_l$ $\ge k$ 的个数

$p^k \mathbb{Z}_{p^s} / p^{k+1} \mathbb{Z}_{p^s} = \begin{matrix} 1 \\ 0 \end{matrix}$

$\Rightarrow$ 初等因子由 B 确定 (循环分解)

定理. $G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ $d_1 | \cdots | d_r$

则 $d_1 \cdots d_r$ 由 G 唯一决定.

上面的过程, 不写了.

试证 Jordan标准形

例. 1500阶 Abel 分类. $\underbrace{2^2}_{\mathbb{Z}_4 \text{ or } \mathbb{Z}_2 \oplus \mathbb{Z}_2} \times \underbrace{3^1}_{\mathbb{Z}_3} \times \underbrace{5^3}_{\mathbb{Z}_{125}}$ $\mathbb{Z}_5 \oplus \mathbb{Z}_{25}$ or $(\mathbb{Z}_5)^3$

108

例. $D_\infty = \langle s,t \mid s^2, t^2 \rangle$ 无限阶
st

$(st)^n = 1 \Rightarrow (st)^n \in N(s^2, t^2)$

$D_{2n} = \langle x, y \mid x^{n}=1, y^2=1, (xy)^n = 1 \rangle$

$D_\infty \longrightarrow \boxed{D_{2(n+1)}}$ 有限. $|D_{2n}| = 2n$

$t \longmapsto y$

$st \longmapsto x$ 可有? Check

$s \longmapsto xy$

感觉是 對不同

H 群 N 群 $H \xrightarrow{\rho} \mathrm{Aut}\, N$

称 H 作用 N

Fact $(N, \rho) \Longleftrightarrow H \times N \xrightarrow{\phi} N$

$(h, n) \longmapsto h.n = \phi(h, n)$

s.t. $\begin{cases} g'.(g.n) = (g'g).h \\ 1_G.h = h \\ g.(nn') = (g.n)\circ(g.n') \end{cases}$

例. G. $N \trianglelefteq G$. $H \leq G$.

则 H 作用于 N.

$h.n = hnh^{-1}$
$\in N$

定义. H 作用于 N. 由 ρ

半直积 $N \rtimes_\rho H = N \rtimes H$

$$(n,h)(n',h') = (n\cdot(h\cdot n'),\ hh') = (n\,\rho(h)(n'),\ hh')$$

$$\rho(h) \in \mathrm{Aut}\ N.$$

构造群（代数专题）

定理 $\begin{cases} N \lhd G.\ H \leq G. \\ N\cap H = \{1_G\} \\ G = NH \end{cases}$

$\rho: H \longrightarrow \mathrm{Aut}(N)$ 共轭

则 $N \rtimes_\rho H \xrightarrow{\sim} G$

$(n,h) \longmapsto nh.$

例 $A_3 \lhd S_3.$

$H = \{\mathrm{Id}, (12)\}$

$H \xrightarrow{\rho} \mathrm{Aut}(A_3)$

C_2 $\quad \mathrm{Id} \longmapsto \mathrm{Id}$ $\quad \Rightarrow \boxed{C_2 \rtimes_\rho C_3 \simeq S_3.}$

$(12) \longmapsto$ 取逆.

例 $A_4 \supseteq K_4 = \{\mathrm{Id},\ \underset{a}{(12)(34)}\ \underset{c}{(14)(23)}\ \underset{b}{(13)(24)}\}.$

$H = \{\mathrm{Id}\ (123),\ (132)\}$

$K_4 \lhd A_4$

$H \xrightarrow{\rho} \mathrm{Aut}\ K_4$

~~$(123) \longmapsto$~~ $\quad \Rightarrow K_4 \rtimes_\rho H \simeq A_4$

排序上：H是K_4的补.

例 $D_8 = \langle s, t \mid s^4, t^2, (st)^2 \rangle.$

$N_1 = \langle a \rangle.\ H = \langle b \rangle.$ $\quad N_2 = \langle a^2, b \rangle\ H_2 = \langle ab \rangle$

$\rho_1: H \longrightarrow \mathrm{Aut}(N_1)$ $\quad$ 并 $\rho_2: H_2 \longrightarrow \mathrm{Aut}(N_2)$