第13次作业.

1. (柯 P118. 3) M: 乘法幺半群. $t\in M$ 定义运算 $*$: $x*y = xty$

证明 $(M,*)$ 构成半群; $(M,*)$ 构成幺半群 $\Leftrightarrow$ t 可逆, 此时 t^{-1} 为单位元.

Pf. 1) 封闭性 $\forall x,y\in M$ $\because t\in M$ 且 M 对乘法封闭 $\therefore xty\in M \Rightarrow x*y\in M$.

结合律 $\forall x,y,z\in M$. $(x*y)*z = (xty)tz = xt(ytz) = xt(y*z) = x*(y*z)$

$\therefore (M,*)$ 构成半群.

M 幺半群 a 不一定可逆

错误: $\forall a\in M$. $a*\varepsilon = at\varepsilon = a \not\Rightarrow t\varepsilon = 1$

2) $(\Rightarrow)$ 设 e 为乘法单位元, ε 为 $(M,*)$ 的幺元. 则 $e = e*\varepsilon = et\varepsilon = t\varepsilon$

$e = \varepsilon * e = \varepsilon(te) = \varepsilon t \Rightarrow t\cdot\varepsilon = \varepsilon\cdot t = e \Rightarrow t$ 可逆且 $\varepsilon = t^{-1}$.

$(\Leftarrow)$. $\forall x\in M$ $t^{-1}*x = (t^{-1}t)x = ex = x$, $x*t^{-1} = x(tt^{-1}) = x$ $\therefore t^{-1}$ 为 $*$ 单位元.

$\therefore (M,*)$ 构成幺半群.

2. 定义运算 $\circ$: $n\circ m = n+m+mn = (1+n)(1+m)-1$ 证明 $\mathbb{Z}$ 关于 $\circ$ 构成交换幺半群.

并求 $(\mathbb{Z},\circ)$ 的单位元和全部可逆元.

$$\left(\begin{array}{l} (n\circ m)\circ p = ((1+n)(1+m)-1)\circ p \\ \qquad = (1+n)(1+m)(p+1)-1 \\ \quad \| \\ n\circ(m\circ p) = n\circ((1+m)(1+p)-1) = (n+1)(1+m)(1+p)-1 \end{array}\right)$$

Pf. 封闭性: $\forall m,n\in\mathbb{Z}$, $n\circ m\in\mathbb{Z}$.

结合律: $\forall n,m,p\in\mathbb{Z}$. $(n\circ m)\circ p = (n+m+mn)\circ p = n+m+mn+p+(n+m+mn)p$

$= n+m+p+mn+mp+np+mnp$

$= n(p+m+mp)+(p+m+mp)+n$

$= n\circ(p+m+mp) = n\circ(m\circ p)$

单位元: $\forall n\in\mathbb{Z}$ $n\circ 0 = 0\circ n = 1+n-1 = n \Rightarrow 0$ 为 $(\mathbb{Z},\circ)$ 单位元.

交换: $\forall n,m\in\mathbb{Z}$, $n\circ m = (1+n)(1+m)-1 = (1+m)(1+n)-1 = m\circ n$.

可逆元: 设 $n\in\mathbb{Z}$ 可逆 即 $\exists m\in\mathbb{Z}$ s.t. $n\circ m = (1+m)(1+n)-1 = 0 \Rightarrow (1+m)(1+n) = 1$

$\Rightarrow 1+n = 1$ or $1+n = -1 \Rightarrow n = 0$ or $n = -2$ (且 $0^{-1} = 0$, $(-2)^{-1} = -2$)

$\therefore$ 可逆元为 $\{0,-2\}$.

3. 设 G 是群, $1\in G$ 为单位元. 证明 若 $\forall x\in G$, $x^2 = 1$ 则 G 交换.

Pf $\forall x,y\in G$. $(xy)^2 = (xy)(xy) = x(yx)y = 1 = 1\cdot 1 = x^2\cdot y^2 = x(xy)y$

$\Rightarrow x^{-1}(x(yx)y)y^{-1} = x^{-1}(x(xy)y)y^{-1} \Rightarrow yx = xy \Rightarrow G$ 交换 □

5. 找出 $\mathbb{Z}_{30}$ 全部乘法可逆元. 证明全部可逆元构成群.

证 1) $\bar{n} \in \mathbb{Z}_{30}$ 可逆 $\iff \gcd(n,30)=1$

($\bar{n}$ 可逆 $\iff \exists\, \bar{m} \in \mathbb{Z}_{30}$ s.t. $\bar{n}\cdot\bar{m} = \bar{1} \iff \overline{m\cdot n-1} = \bar{0} \iff m\cdot n - 1 = 30k\ (k\in\mathbb{Z})$

$\iff m\cdot n + (-k)\cdot 30 = 1 \iff \gcd(n,30)=1$)

∴ $\mathbb{Z}_{30}$ 全部可逆元为 $S=\{\bar{1}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}$

2) 封闭性 $\forall\, \bar{m}, \bar{n} \in \mathbb{Z}_{30}$ 可逆. 则 $\exists\, \bar{m}', \bar{n}'$ s.t. $\bar{m}\cdot\bar{m}' = \bar{1} = \bar{n}\cdot\bar{n}'$

$(\bar{m}\cdot\bar{n})\cdot(\bar{n}'\cdot\bar{m}') = \bar{m}\cdot(\bar{n}\cdot\bar{n}')\bar{m}' = 1 \Rightarrow \bar{m}\cdot\bar{n}$ 可逆

结合律自然成立. $\bar{1}$ 自然为 S 的单位元.

$\forall\, \bar{m} \in S$ ∵ $\bar{m}$ 可逆 $\Rightarrow \exists\, \bar{n} \in \mathbb{Z}_{30}$ s.t. $\bar{m}\cdot\bar{n} = \bar{1} \Rightarrow \bar{n}$ 可逆 $\Rightarrow \bar{n} \in S$

∴ S 构成群.

4. $SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid |A| = 1\}$ 则 $SL_n(\mathbb{Z})$ 关于矩阵乘法构成群.

证. 封闭性: $\forall\, A, B \in SL_n(\mathbb{Z})$ $A\cdot B \in M_n(\mathbb{Z})$ 且 $|A\cdot B| = |A|\cdot|B| = 1 \Rightarrow A\cdot B \in SL_n(\mathbb{Z})$

结合律自然成立. E_n 自然为 $SL_n(\mathbb{Z})$ 单位元.

$\forall\, A \in SL_n(\mathbb{Z})$ ∵ $|A|=1$ ∴ A 关于乘法可逆 $\cancel{\Rightarrow \exists B \in M_n}$ 且 $A^{-1} = \dfrac{A^{\vee}}{|A|} = A^{\vee} \in M_n(\mathbb{Z})$

又∵ $|A^{-1}| = |A|^{-1} = 1 \Rightarrow A^{-1} \in SL_n(\mathbb{Z})$ 综上 $SL_n(\mathbb{Z})$ 构成群.

6. 证明 $\varphi: GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$ 为同构.

$\qquad A \longmapsto (A^{-1})^t$

证. 群同态: $\forall\, A, B \in GL_n(\mathbb{R})$ $\varphi(A\cdot B) = ((AB)^{-1})^t = (B^{-1}A^{-1})^t = (A^{-1})^t\cdot(B^{-1})^t = \varphi(A)\cdot\varphi(B)$

单: $(A^{-1})^t = E_n \Rightarrow A^{-1} = E_n \Rightarrow A = E_n \Rightarrow$ 单

(φ 单 $\iff \ker\varphi := \{A \in GL_n(\mathbb{R}) \mid \varphi(A) = E_n\} = \{E_n\}$.

($\Leftarrow$): $\boxed{(\text{若 } (A_1^{-1})^t = (A_2^{-1})^t \Rightarrow A_1^{-1} = A_2^{-1} \Rightarrow A_1 = A_2 \Rightarrow \text{则 } \varphi \text{ 单})}$ ($\Rightarrow$) 显然

~~若 $\varphi(A_1) = \varphi(A_2) \Rightarrow \varphi(A_1)/\varphi(A_2) = \varphi(A_1/A_2) = E \Rightarrow A_1/A_2$~~

$A_1 = A_2$ $\Uparrow$

若 $\varphi(A_1) = \varphi(A_2) \Rightarrow \varphi(A_1)\cdot(\varphi(A_2^{-1})) = \varphi(A_2\cdot A_2^{-1}) = E = \varphi(A_1A_2^{-1}) \Rightarrow A_1A_2^{-1} = E$

满: $\forall\, A \in GL_n(\mathbb{R})$ ∵ $|A| \neq 0$ ∴ A 可逆 令 $B = (A^t)^{-1}$ 则 $\varphi(B) = (((A^t)^{-1})^{-1})^t = (A^t)^t = A$

群

Def 子群

设 $(G,\cdot,e)$ 为群. $H\subseteq G$. 若 H 关于 $\cdot$ 封闭 且, $e\in H$ 且 $\forall h\in H\ \exists h^{-1}\in H$ 则称 H 为 G 子群 记 $H\leq G$.
(即子群是子集＋群结构)

判定: $H\leq G \iff \forall a,b\in H.\ a\cdot b^{-1}\in H$.

eg1. 设 $\varphi:(G,\cdot,e)\longrightarrow(G',*,e')$ 为群同态.

则 $\ker\varphi := \{g\in G \mid \varphi(g)=e'\}\leq G$

$\operatorname{im}\varphi := \varphi(G)=\{g'\in G' \mid \exists g\in G \text{ s.t. } g'=\varphi(g)\}\leq G'$

另外 $\ker\varphi=\{e\}\iff\varphi$ 单.

Pf $\forall a,b\in\ker\varphi$ $\varphi(a\cdot b^{-1})=\varphi(a)*(\varphi(b))^{-1}=e'*(e')^{-1}=e'\Rightarrow a\cdot b^{-1}\in\ker\varphi$

$\forall a',b'\in\operatorname{im}\varphi.$ $\exists a,b\in G$ s.t. $a'=\varphi(a),\ b'=\varphi(b)$ 则 $a'*b'^{-1}=\varphi(a\cdot b^{-1})\in\operatorname{im}\varphi$.

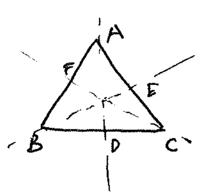
$(\Rightarrow)$ 若 $\varphi(a)=\varphi(b)\Rightarrow\varphi(a)*(\varphi(b))^{-1}=e'=\varphi(a\cdot b^{-1})\Rightarrow a\cdot b^{-1}\in\ker\varphi=\{e\}$

$\therefore a\cdot b^{-1}=e\Rightarrow a=b\Rightarrow\varphi$ 单

$(\Leftarrow)$ $\because\varphi$ 同态 $\therefore e\in\ker\varphi$ 又$\because\varphi$ 单 $\therefore\{e\}=\ker\varphi$.

eg2 (略讲) 所有将等边三角形变为自身の变换构成的群 且与 S_3 同构.

Pf. $G=\{\varphi:\{A,B,C\}\longrightarrow\{A,B,C\}\mid\varphi$ 为一一映射$\}$



G 对关于变换の复合 显然 满足 封闭性 和 结合律.

单位元: id φ 逆元 即为 φ^{-1} ($\because\varphi$ 为双射,就是变回来).

G:
- 旋转(逆时针)
  - 0° $id=\begin{pmatrix}A&B&C\\A&B&C\end{pmatrix}\longleftrightarrow(1)$
  - 120° $\varphi_1=\begin{pmatrix}A&B&C\\C&A&B\end{pmatrix}\longleftrightarrow(1\,3\,2)$
  - 240° $\varphi_2=\begin{pmatrix}A&B&C\\B&C&A\end{pmatrix}\longleftrightarrow(1\,2\,3)$
- 翻转(对称)
  - 沿AD $\psi_1=\begin{pmatrix}A&B&C\\A&C&B\end{pmatrix}\longleftrightarrow(2\,3)$
  - 沿BE $\psi_2=\begin{pmatrix}A&B&C\\C&B&A\end{pmatrix}\longleftrightarrow(1\,3)$
  - 沿CF $\psi_3=\begin{pmatrix}A&B&C\\B&A&C\end{pmatrix}\longleftrightarrow(1\,2)$

自己验证 $G\cong S_3$

eg3. 设 $(G,\cdot,e)$ 为有限群. $H\subseteq G$ 是非空子集

若 H 关于 $\cdot$ 封闭 则 $H\leqslant G$.

Pf. ∵ $H\neq\phi$ 则 $\exists\ a\in H$. ∵ G 为有限群 则 $d=ord(a)<+\infty$ 且 $a^d=e$

∵ H 关于 $\cdot$ 封闭 ∴ $a^d\in H \Rightarrow e\in H$

且 $a\cdot a^{d-1}=a^{d-1}\cdot a=e \Rightarrow a^{-1}=a^{d-1}\in H$ $\Big\}\Rightarrow H\leqslant G$.

回顾: Lagrange 定理: 设 G 为有限群, $H\leqslant G$ 则 $|H|\,\big|\,|G|$

Cor1 设 G 为有限群 $\forall\ a\in G$ $ord(a)\,\big|\,|G|$

Cor2 设 G 为有限群 $\forall\ a\in G$ $a^{|G|}=e$

注: 一般 Lagrange 定理的逆命题不成立 即对 $|G|$ 的一个因子 d 不一定有一个子群 H s.t. $|H|=d$.

但如果 G 是循环群且有限 则逆命题成立 即 $\forall\ d\,\big|\,|G|$. $\exists!\ H\leqslant G$ s.t. $|H|=d$.

eg4. 给出 $(\mathbb{Z}_{12},+,\bar{0})$ 的所有子群, 求 $\bar{5}$, $\bar{8}$ 的阶.

解. 设 $H\leqslant\mathbb{Z}_{12}=\langle\bar{1}\rangle$ 则 $|H|\,\big|\,12 \Rightarrow |H|$ 可能等于 1, 2, 3, 4, 6, 12

若 $|H|=1$ 则 $H=\{\bar{0}\}$.

若 $|H|=2$ 则 $H=\langle\bar{6}\rangle$

若 $|H|=3$ 则 $H=\langle\bar{4}\rangle$

若 $|H|=4$ 则 $H=\langle\bar{3}\rangle$

若 $|H|=6$ 则 $H=\langle\bar{2}\rangle$

若 $|H|=12$ 则 $H=\langle\bar{1}\rangle=\mathbb{Z}_{12}$

设 $ord(\bar{5})=d_1$ 则 $d_1\cdot\bar{5}=\overline{d_1\cdot 5}=\bar{0} \Rightarrow 12\,|\,d_1\cdot 5 \Rightarrow 12\,|\,d_1$ 且 $d_1|12$ $\Rightarrow ord(\bar{5})=12$.

设 $ord(\bar{8})=d_2$ 则 $d_2\cdot\bar{8}=\overline{d_2\cdot 8}=\bar{0} \Rightarrow 12\,|\,d_2\cdot 8 \Rightarrow 3\,|\,2\cdot d_2 \Rightarrow d_2=3$ □

eg5. 设 $\varphi:(G,\cdot,e)\longrightarrow(G',*,e')$ 为群同态 若 $a^n=e\ (n\in\mathbb{Z})$ ~~$a\in G$ 的阶为 n~~ 则 $ord(\varphi(a))\,|\,n$.

若 φ 是同构 则 $ord(\varphi(a))=ord(a)$

Pf. 若 $n\in\mathbb{N}$ $\underbrace{a\cdot a\cdots a}_{n}=e \Rightarrow \varphi(a^n)=\varphi(e)=e'$ ∵ φ 是同态 $\varphi(a^n)=\varphi(a)^n=\underbrace{\varphi(a)*\cdots*\varphi(a)}_{n个}$

$\Rightarrow ord(\varphi(a))\,|\,n$ 若 $n\in\mathbb{Z}^-$ 则 $\underbrace{a^{-1}\cdots a^{-1}}_{-n个}=e$ $\varphi((a^{-1})^{-n})=(\varphi(a^{-1}))^{-n}=(\varphi(a))^{-1\cdot(-n)}=(\varphi(a))^n=e'$

若 φ 是同构 则 φ^{-1} 也是群同构. 则 $\underbrace{ord(\varphi^{-1}(\varphi(a)))}_{=ord(a)}\,\big|\,ord(\varphi(a))\,\big|\,ord(a)$

$\Rightarrow ord(\varphi(a))=ord(a)=n$.

eg6. 设置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in S_n$ 定义 $E_\sigma = (\vec{e}^{(i_1)} \cdots \vec{e}^{(i_n)})$ 其中 $\vec{e}^{(j)} = \begin{array}{c} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{array} \begin{array}{l} \\ \\ \\ \leftarrow j \\ \\ \\ \\ \end{array}$

例如 $n=3$ 时 $E_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $E_{(123)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ $E_{(132)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

令 $G_n = \{ E_\sigma \mid \sigma \in S_n \}$ 则 G_n 为 $GL_n(\mathbb{R})$ 的子群 且 $G_n \cong S_n$.

Pf. $\forall E_\sigma \in G_n$ 由行列式定义 $\det(E_\sigma) = (-1)^{\operatorname{sgn}\sigma} \neq 0 \Rightarrow E_\sigma \in GL_n(\mathbb{R})$ $\therefore G_n \subseteq GL_n(\mathbb{R})$.

断言: $\forall \sigma, \tau \in S_n$ $E_\sigma \cdot E_\tau = E_{\sigma\tau}$

Pf. $\tau = id$ 恒同置换时 $E_\tau = E_n$ 单位矩阵 则 $E_\sigma \cdot E_n = E_\sigma = E_{\sigma \cdot id}$ 自然成立.

设 τ 为 m个对换之积, 且 $m \geq 1$ 对 m 归纳.

$m=1$ 时 设 $\tau = (p\ q)$ 不妨设 $p<q$. $\sigma = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \in S_n$.

则 $E_\sigma \cdot E_\tau = (\vec{e}^{(i_1)} \cdots \vec{e}^{(i_n)}) \cdot E_{(p,q)}$ 右乘 $E_{(pq)}$ 相当于 对换 p, q 两列

$= (\vec{e}^{(i_1)} \cdots \vec{e}^{(i_q)} \cdots \vec{e}^{(i_p)} \cdots \vec{e}^{(i_n)})$

$$\sigma \cdot \tau = \begin{pmatrix} 1 & \cdots & p & \cdots & q & \cdots & n \\ i_1 & \cdots & i_p & \cdots & i_q & \cdots & i_n \end{pmatrix} \cdot \begin{pmatrix} 1 & \cdots & p & \cdots & q & \cdots & n \\ 1 & \cdots & q & \cdots & p & \cdots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \cdots & p & \cdots & q & \cdots & n \\ i_1 & \cdots & i_q & \cdots & i_p & \cdots & i_n \end{pmatrix} \quad \therefore E_{\sigma\tau} = (\vec{e}^{(i_1)} \cdots \vec{e}^{(i_q)} \cdots \vec{e}^{(i_p)} \cdots \vec{e}^{(i_n)})$$

$\therefore E_\sigma \cdot E_\tau = E_{\sigma\tau}$

假设 $m-1$ 时成立 则 $\tau = \pi_1 \cdots \pi_m$ 时 (π_k 为对换)

$$E_\sigma \cdot E_\tau = E_\sigma \cdot E_{(\pi_1 \cdots \pi_{m-1}) \cdot \pi_m} \xlongequal{\text{归纳}\cancel{\text{假设}}\text{基础}} (E_\sigma \cdot E_{\pi_1 \cdots \pi_{m-1}}) \cdot E_{\pi_m} \xlongequal{\text{归纳假设}} E_{\sigma \cdot \pi_1 \cdots \pi_{m-1}} \cdot E_{\pi_m}$$

$\xlongequal{\text{归纳基础}} E_{\sigma \cdot \pi_1 \cdots \pi_m} = E_{\sigma \cdot \tau}$ 综上 $E_\sigma \cdot E_\tau = E_{\sigma \cdot \tau}$

由断言, G_n 关于矩阵乘法封闭. 再且 $\forall \sigma \in S_n$ $E_\sigma \cdot E_{\sigma^{-1}} = E_{\sigma \cdot \sigma^{-1}} = E_n$

$\Rightarrow \forall E_\sigma \in G_n$ 有逆元 $E_{\sigma^{-1}}$ (乘法结合律和单位元 E_n 自然成立)

$\therefore G_n \leq GL_n(\mathbb{R})$

构造映射 $\varphi: S_n \longrightarrow G_n$, $\sigma \longmapsto E_\sigma$ 显然是双射 (单: $\varphi(\sigma) = E_n = (\vec{e}^{(1)} \cdots \vec{e}^{(n)}) \Rightarrow \sigma = id$
满 和良定义均由 E_σ 定义可知)

由断言 $\varphi(\sigma \cdot \tau) = E_{\sigma\tau} = E_\sigma \cdot E_\tau = \varphi(\sigma) \cdot \varphi(\tau) \Rightarrow \varphi$ 为群同构.

Cor (柯 P82.6) $A = E_{\overset{\sigma}{(12 \cdots n)}}$ $\because \operatorname{ord}(\sigma) = n$ 即 $\sigma^n = id \Rightarrow \varphi(\sigma^n) = \varphi(id) = E_n$

$\Rightarrow (\varphi(\sigma))^n = E_n \Rightarrow A^n = E_n$ □.

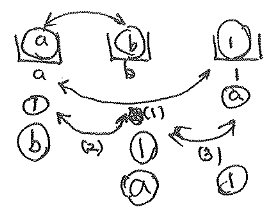
<u>Lemma</u> 设 $(i_1 i_2 \cdots i_r) \in S_n$ 为循环. 则 $\forall\, \sigma \in S_n$ $\sigma(i_1 \cdots i_r)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_r))$ (习题课4 P_1)

<u>柯 P_{128}. 9</u> 求证 $S_n = \langle (12), (13), \cdots (1n) \rangle$

<u>Pf.</u> 已知 $\forall\, \sigma \in S_n$ σ可拆成若干对换之积. $\therefore$ 只需证 $\forall$ 对换 $\overset{(a\,b)}{\cancel{(a\,b)}} \in \langle (12), \cdots (1n) \rangle$

由 Lemma $(a\,b) = (1a)(1b)(1a)$ 则 $S_n \subseteq \langle (12), \cdots (1n) \rangle$ 得证

注：也可以这么看



<u>柯 P_{128}.10</u> 求证 $S_n = \langle (12)\ (12 \cdots n) \rangle \overset{G}{=}$

<u>Pf</u> 先证 $S_n = \langle (12), (23) \cdots (n-1\ n) \rangle \overset{H}{=}$ 只需证 $(1\,i) \in H$ 即可 $(\cancel{i=1,2}\ 2,3 \cdots n)$

归纳法 $(12) \in H$ 假设 $(1\,i) \in H$ 则 $(1\ i{+}1) = (1\,i)(i\ i{+}1)(1\,i)^{-1} \in H$ 得证.

再证 所有 $(i\ i{+}1) \in G$ $(i = 1, 2 \cdots n-1)$

归纳法 $(12) \in G$ 假设 $(i{-}1\ i) \in G$ 则 $(i\ i{+}1) = (12 \cdots n)(i{-}1\ i)(12 \cdots n)^{-1} \in G$

$\therefore \forall\, i = 1, 2 \cdots n-1$ $(i\ i{+}1) \in G$ $\therefore$ $S_n = G$.

~~柯 P_{128} 11. 求证 $A_n = \langle (123), (124), \cdots (12n) \rangle$ $(n \geqslant 3)$ 其中 A_n 为偶置换群(交错群)~~

~~Pf. 首先 $A_n \leqslant S_n$ $\because$ 偶置换相乘仍为偶置换 且 单位(恒同置换)为偶置换.~~

~~对 $\forall\, a, b, c, d \in \{1, 2 \cdots n\}$ 且 $a \neq b \neq c \neq d$ $(ab)(cd) = (abc)(abd)$~~

柯 P_{128}.11. 求证 $A_n = \langle (123), (124), \cdots (12n) \rangle \overset{G}{=}$ $(n \geqslant 3)$ 其中 A_n 是偶置换群(交错群).

Pf 首先 $A_n \leqslant S_n$ 为子群 对 $\forall$ 偶置换 可拆成偶数个对换之积.

$A_n \subseteq B$ 而3循环是偶置换.

$$\left.\begin{array}{l} (ab)(ac) = (acb) \quad (a \neq b,\ a \neq c,\ b \neq c) \qquad (ab)(ab) = e \end{array}\right\} \Rightarrow \therefore A_n \text{ 可由所有3循环生成的群} B$$

$(ab)(cd) = (acb)(acd)$ (a, b, c, d 两两不同)

$\forall\, \sigma \in A_n \subseteq S_n$ ~~则 $\sigma = (1\,i)$~~ $\because S_n = \langle (12), \cdots (1n) \rangle$ $\therefore \sigma = (1\,i_1) \cdots (1\,i_{2k})$

技巧: $\sigma = (1\,i_1)(1\,i_2) \cdots (1\,i_{2k-1})(1\,i_{2k}) = (1\,i_1)(12)(12)(1\,i_2) \cdots (1\,i_{2k-1})(12)(12)(1\,i_{2k})$

$= (12\,i_1)(1\,i_2\,2) \cdots (12\,i_{2k-1})(1\,i_k\,2)$ (结合律) $\because (1\,j\,2) = (12j)(12j)$

$= (12\,i_1)(12\,i_2)^2 \cdots (12\,i_{2k-1})(12\,i_k)^2 \in G$

$\because (12j) = (1j)(12) \in A_n \Rightarrow G \subseteq A_n$ $\therefore A_n = G$ $\square$.

循环群

群论基本问题 $\begin{cases} \text{给出一类群，找出所有不同构的群} & \checkmark \text{(循环群)} \\ \text{研究子群结构} & \checkmark \end{cases}$

<u>Thm1</u>（不同构的循环群）

设 $G=\langle a\rangle$ 为循环群 则 $\begin{cases} \text{若 } |G| = ord(a) = +\infty \text{ 则 } G \cong (\mathbb{Z}, +, 0) \\ \text{若 } |G| = ord(a) = n < +\infty \text{ 则 } G \cong (\mathbb{Z}_n, +, 0) \end{cases}$

子群结构

<u>Lemma1</u> $H \leq G = \langle a \rangle$ 则 $\exists\, k \in \mathbb{Z}$ s.t. $H = \langle a^k \rangle$

<u>Pf</u>. 若 $H=\{e\}$ 则 $H = \langle a^0 \rangle$

对 $\forall\, x \in H$ 且 $x \neq e$ 则 $\exists\, m \in \mathbb{Z}\setminus\{0\}$ s.t. $x = a^m$

不妨设 $a^k \in H$ 且 k 为最小正整数 显然 $\langle a^k \rangle \subseteq H$

另一方面，$\forall\, a^m \in H$ 考虑带余除法 $m = q\cdot k + r$ $(0 \leq r < k)$

$\because a^m, a^k \in H$ 则 $a^r = a^m \cdot (a^k)^{-q} \in H$ 由 k 极小性 $\Rightarrow r=0$

$\therefore a^m = (a^k)^q \in \langle a^k \rangle$ $\therefore \langle a^k \rangle = H$ □

<u>Lemma2</u> 设 G 为群（不一定是循环群）若 $a \in G$ 满足 $ord(a) = n$

则对 $\forall\, k \in \mathbb{Z}$ $a^k \in G$ 且 $ord(a^k) = \dfrac{n}{\gcd(n,k)}$

<u>Pf</u>. 令 $d = \gcd(n,k)$ 且 $n = \tilde{n}\cdot d$ $k = \tilde{k}\cdot d$ 则 $\gcd(\tilde{n}, \tilde{k}) = 1$

$(a^k)^{\tilde{n}} = a^{\tilde{k}\cdot d\cdot \tilde{n}} = a^{\tilde{k}\cdot n} = (a^n)^{\tilde{k}} = e^{\tilde{k}} = e \Rightarrow ord(a^k) \mid \tilde{n}$

对 $\forall\, l \in \mathbb{Z}$ s.t. $(a^k)^l = e$ 则 $n \mid kl \Rightarrow \tilde{n} \mid \tilde{k} l \Rightarrow \tilde{n} \mid l$ $(\because \gcd(\tilde{n}, \tilde{k}) = 1)$.

$\therefore ord(a^k) = \tilde{n} = \dfrac{n}{\gcd(n,k)}$ □

<u>Cor</u> 群 G. 若 $a \in G$ 且 $ord(a) = n$, $\gcd(n,k) = 1 \Rightarrow ord(a^k) = n$.

Thm 设 $G=\langle a\rangle$ 为循环群 则

i) 若 $|G|=n$ 则对 $\forall\, k\in\mathbb{N}$ 且 $k\mid n$，$\exists!\, H\leqslant G$ s.t. ~~ord~~ $|H|=k$ 且 $H=\langle a^{\frac{n}{k}}\rangle$

ii) 若 $|G|=+\infty$ 则 G 有无穷多子群.

Pf i) $|G|=n$ 设 $k\mid n$ 且 $n=l\cdot k$ 由 Lemma 2 $\operatorname{ord}(a^{l})=\frac{n}{\gcd(l,n)}=\frac{n}{l}=k$

$\Rightarrow \langle a^{\frac{n}{k}}\rangle\leqslant G$ 为 k 阶子群.

设 $H\leqslant G$ 且 $|H|=k$ 由 Lemma 1 $\exists\, m\in\mathbb{N}$ s.t. $H=\langle a^m\rangle$

显然 $|H|=|a^m|=k=\frac{n}{\gcd(m,n)} \Rightarrow \gcd(m,n)=\frac{n}{k}$

由扩展 Euclidean 算法（Bezout's 关系）$\exists\, l_1,l_2\in\mathbb{Z}$ s.t. $ml_1+nl_2=\frac{n}{k}$

$\therefore\ a^{\frac{n}{k}}=(a^m)^{l_1}\cdot(\cancel{a^n}^{\,e})^{l_2}=(a^m)^{l_1}\in\langle a^m\rangle \quad \therefore \langle a^{\frac{n}{k}}\rangle\subseteq H$

且 $|\langle a^{\frac{n}{k}}\rangle|=|H|=k \quad \therefore \langle a^{\frac{n}{k}}\rangle=H \Rightarrow$ 唯一性.

ii) $|G|=+\infty$ $\{e\},\langle a\rangle,\langle a^2\rangle\cdots$ 是 G 的不同子群 且 $\langle a^k\rangle\cong(\mathbb{Z},+,0)$ $(k\geqslant1)$

$(\because \operatorname{ord}(a^k)=+\infty$ 否则 $\operatorname{ord}(a^k)=d \Rightarrow \operatorname{ord}(a)\mid kd \to\Leftarrow)$

Cor 设 G 为 n 阶循环群 则 若 $n=1$ 则 G 仅有唯一子群 G.

若 $n>1$ 且 $n=p_1^{k_1}\cdots p_s^{k_s}$ 为标准素分解 则 G 有 $T(n)=\prod_{i=1}^{s}(k_i+1)$ 个子群.