1. 设 p 为素数，记 $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{\bar{0}\}$

(a) 证明：$(\mathbb{Z}_p^\times, \cdot, \bar{1})$ 构成一个群

(b) 设 $p=5$，计算 $\bar{3}$，$\bar{2}$ 关于运算 $\cdot$ 的逆

(c) 列出 $(\mathbb{Z}_5^\times, \cdot, \bar{1})$ 和 $(\mathbb{Z}_5, +, \bar{0})$ 的乘法表

(d) 寻求 $\bar{a} \in \mathbb{Z}_5^\times$，使得 $\{\bar{a}^i \mid i \in \mathbb{Z}\} = \mathbb{Z}_5^\times$.

pf: (a). 封闭性 + 结合律 + 单位元 + 可逆元

$\forall\ a, b \in \mathbb{Z}_p^\times$，$\because p \nmid a$，$p \nmid b$. $\Rightarrow$ $p \nmid ab \Rightarrow ab \in \mathbb{Z}_p^\times$.

故 "$\cdot$" 满足封闭性

显然 "$\cdot$" 满足结合律

$\forall \bar{a} \in \mathbb{Z}_p^\times$，$\bar{1} \cdot \bar{a} = \bar{a} \cdot \bar{1} = \bar{a}$. $\Rightarrow$ $\bar{1}$ 是单位元.

$\forall \bar{a} \in \mathbb{Z}_p^\times$，则 $\gcd(a, p) = 1$

$\Rightarrow \exists\, u, v \in \mathbb{Z}$, s.t. $ua + vp = 1$.

$\Rightarrow \bar{u} \cdot \bar{a} + \bar{v} \cdot \bar{p} = \bar{1}$

$\Rightarrow \bar{u} \cdot \bar{a} = \bar{1}$

$\Rightarrow \bar{u} = \bar{a}^{-1}$

$\Rightarrow \bar{a}$ 存在逆元 $\bar{u}$.

$\Rightarrow (\mathbb{Z}_p^\times, \cdot, \bar{1})$ 构成一个群. 2个条.

(b). $\bar{3} \cdot \bar{2} = \bar{1}$，$\bar{3}^{-1} = \bar{2}$，$\bar{2}^{-1} = \bar{3}$.

(c).

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

(d) $a = 2$，$\bar{2}^1 = \bar{2}$，$\bar{2}^2 = \bar{4}$，$\bar{2}^3 = \bar{4} \cdot \bar{2} = \bar{3}$，$\bar{2}^4 = \bar{1}$.

2. 设 $\phi: S_n \to \{1,-1\}$.

$\sigma \mapsto \epsilon_\sigma$

其中ϵ_σ是置换σ的符号. 验证: ϕ是从置换群S_n到群$(\{-1,1\},\cdot)$的同态

pf: 设 $\sigma_1, \sigma_2 \in S_n$, 则 $\phi(\sigma_1\sigma_2) = \epsilon_{\sigma_1\sigma_2} = \epsilon_{\sigma_1}\epsilon_{\sigma_2} = \phi(\sigma_1)\phi(\sigma_2)$

$\Rightarrow$ ϕ是从置换群S_n到群$(\{-1,1\},\cdot)$的同态.

群元素阶的概念

设$(G,\cdot,e)$是一个群, $g\in G$. 如果不存在$n\in\mathbb{Z}^+$, s.t. $g^n=e$. 则称g是无限阶的. 否则称为有限阶的. 如果k是最小的正整数满足$g^k=e$. 则称k是g的阶. 记为$\mathrm{ord}(g)$.

prop. 如果G是有限群, $\mathrm{ord}(g) \mid \mathrm{card}(G)$.

若$g^m=e$, 则 $\mathrm{ord}(g) \mid m$.

3. $\mathrm{ord}(a)=m$, $\mathrm{ord}(b)=n$. 证明: 如果$ab=ba$, 且$\gcd(m,n)=1$.

$\mathrm{ord}(ab)=mn$.

pf: $(ab)^{mn} = a^{mn}b^{mn}$ $(\because ab=ba)$

$= (a^m)^n (b^n)^m$

$= e^n e^m = e$

$\Rightarrow \mathrm{ord}(ab) \mid mn$.

设 $\mathrm{ord}(ab)=s$.

$(ab)^s = e \Rightarrow (ab)^{sm} = e$. $\qquad \Rightarrow (ab)^{sn} = e$.

$(ab)^{sm} = (a^m)^s b^{sm} = b^{sm}$ $\qquad (ab)^{sn} = a^{sn}(b^n)^s = e$

$\Rightarrow n \mid sm$. $\qquad a^{sn} = e$

由于$\gcd(m,n)=1 \Rightarrow n \mid s$, $\qquad \Rightarrow m \mid sn$.

同理 $m \mid s$ $\Rightarrow mn \mid s$ ($\because \gcd(m,n)=1$)

$\Rightarrow \operatorname{ord}(ab)=mn$.

4. 设 H,K 是群 G 的两个子群，证明：HK 是 G 的子群 $\Leftrightarrow HK=KH$.

Pf: "$\Leftarrow$"

回忆：$(G,\cdot,e)$ 是群，H 是 G 的非空子集，则 H 是 G 的子群 $\Leftrightarrow \forall h_1,h_2\in H$, $h_1h_2^{-1}\in H$.

由于 $e\in H,K$, $\Rightarrow e\in HK$ $\Rightarrow$ HK 是非空集合.

设 $a,b\in HK$，则 $\exists h_1,h_2\in H$, $k_1,k_2\in K$, s.t.

$a=h_1k_1$, $b=h_2k_2$.

$ab^{-1}=(h_1k_1)(h_2k_2)^{-1}=h_1\underbrace{k_1k_2^{-1}}_{K}\underbrace{h_2^{-1}}_{H}$

由于 K,H 为子群，故 $k_1k_2^{-1}\in K$, $h_2^{-1}\in H$，则 $k_1k_2^{-1}h_2^{-1}\in KH$

由于 $HK=KH$ $\Rightarrow \exists h'\in H$ $k'\in K$, s.t. $(k_1k_2^{-1})h_2^{-1}=h'k'$

$\Rightarrow ab^{-1}=h_1h'k'\in HK$

$\Rightarrow HK$ 是 G 的子群

"$\Rightarrow$" $\forall hk\in HK$, $\underline{HK\leq G}$ $\Rightarrow (hk)^{-1}\in HK$.

$\Rightarrow (hk)^{-1}=\underline{h'k'}\in G$ $\Rightarrow hk=k'^{-1}h'^{-1}\in KH$.

$\Rightarrow HK\subset KH$.

$\forall kh\in KH$, $(kh)^{-1}=h^{-1}k^{-1}\in HK$.

$HK\leq G$ $\Rightarrow \underbrace{((kh)^{-1})^{-1}}_{kh}\in HK$

$\Rightarrow KH\subseteq HK$.

$\Rightarrow HK=KH$.

5. Pf: $\phi(e_G)=e_H$ $\Rightarrow e_G\in \ker(\phi)$ $\Rightarrow \ker(\phi)$ 非空

$\forall a,b\in\ker(\phi)$, $\phi(ab^{-1})=\phi(a)\phi(b)^{-1}=e_H$ $\Rightarrow ab^{-1}\in\ker(\phi)$

$\Rightarrow \ker(\phi)$ 是 G 的子群

$\Rightarrow$ [illegible]

设 G, H 为两个群，单位元分别为 e_G, e_H. 设 $\phi: G \to H$ 为群同态，记

$$\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}.$$

证明：

(a) $\ker(\phi)$ 为 G 的一个子群

(b) $g\ker(\phi) = \ker(\phi) g$ 对任意 $g \in G$ 成立，其中

$g\ker(\phi) = \{gg' \mid g' \in \ker(\phi)\}$，$\ker(\phi) g = \{g'g \mid g' \in \ker(\phi)\}$

(c) ϕ 是单射 $\Leftrightarrow \ker(\phi) = \{e_G\}$

pf: (b). $\forall a \in g\ker(\phi)$，则 $\exists b \in \ker(\phi)$, s.t $a = gb$.

$\Rightarrow \phi(a) = \phi(g)\phi(b) = \phi(g)$

$\Rightarrow \phi(a)\phi(g)^{-1} = e_H$

$\Rightarrow \phi(ag^{-1}) = e_H$

$\Rightarrow ag^{-1} \in \ker(\phi)$.

$\Rightarrow \exists b' \in \ker(\phi)$, s.t $ag^{-1} = b'$

$\Rightarrow a = b'g \in \ker(\phi) g$

$\Rightarrow g\ker(\phi) \subset \ker(\phi) g$

同理，$g\ker(\phi) \supset g\ker(\phi)$

$\Rightarrow g\ker(\phi) = \ker(\phi) g$.

(c). "$\Rightarrow$" 由单射定义

"$\Leftarrow$" $\forall a, b \in G$, s.t $\phi(a) = \phi(b)$.

$\Rightarrow \phi(a)\phi(b)^{-1} = e_H$

$\Rightarrow \phi(ab^{-1}) = e_H$

$\ker(\phi) = e_G \Rightarrow ab^{-1} = e_G \Rightarrow a = b \Rightarrow \phi$ 是单射.

[illegible] 为素数，证明：任意 $g \in G \setminus \{1\}$，有 $\langle g \rangle = G$

6. 设 $(G,\cdot,1)$ 是个群且 $card(G)=p$，p 为素数，证明：G 为循环群。

pf: $\forall g\in G$，$ord(g) \mid \underset{p}{\underline{card(G)}}$。

p 是个素数，则 $ord(g)=1$ or p

$g\neq 1 \Rightarrow ord(g)\neq 1$

$\Rightarrow ord(g)=p$

$\Rightarrow G=\{g^0, g^1, \cdots, g^{p-1}\} = \langle g\rangle$。

换句话说，素数阶有限群是循环群。

同态与同构：

prop: 设 $\varphi:(G,\cdot,e)\to(G',*,e')$ 为群同态，若 $ord(a)<\infty$，则 $ord(\varphi(a)) \mid ord(a)$。

pf: 设 $ord(a)=n$，则 $a^n=e_G$

$\Rightarrow \underset{\varphi(a)^n}{\varphi(a^n)} = \varphi(e_G)=e_{G'}$

$\Rightarrow ord(\varphi(a)) \mid ord(a)$

若 φ 是同构，则 φ^{-1} 也是群同态。

$\Rightarrow \underset{ord(a)}{ord(\varphi^{-1}(\varphi(a)))} \mid ord(\varphi(a))$

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

例 $GL_n(\mathbb{R})=\{A \mid A\in M_n(\mathbb{R})\}$ 可逆，证明：$\varphi: GL_n(\mathbb{R})\to GL_n(\mathbb{R})$，$A\mapsto (A^{-1})^t$ 为同构

pf: $\forall A,B\in GL_n(\mathbb{R})$，$\varphi(AB)=((AB)^{-1})^t = (B^{-1}A^{-1})^t = (A^{-1})^t(B^{-1})^t$

$=\varphi(A)\varphi(B)$。

单：φ 是单射 $\Leftrightarrow \ker(\varphi)=E_n$。

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

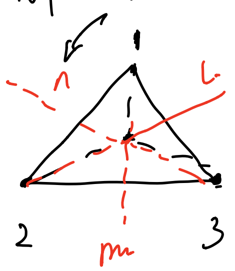
满：$\forall A\in GL_n(\mathbb{R})$ 令 $B=(A^t)^{-1}$

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

$\Rightarrow \varphi(B) \ni [(H^0)^{\cdot}]$

$\Rightarrow \varphi$ 是满射.

例. 所有将等边三角形变为自身的变换构成群 记为 G, 则 $G \simeq S_3$.



逆时针旋转
$$\begin{cases} 0^\circ, & id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\ 120^\circ, & \varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \\ 240^\circ, & \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) \end{cases}$$

轴对称
$$\begin{cases} l: & \varphi_3 = (1\,3) \\ m: & \varphi_4 = (2\,3) \\ n: & \varphi_5 = (1\,2) \end{cases}$$

$\Rightarrow \quad G \simeq S_3$.

循环群

Def 设 G 是群, 如果存在 $g \in G$. s.t $G = \langle g \rangle$, 则称 G 为循环群

prop: 设 $(G, \cdot, e)$ 是循环群且 $card(G) > 1$

① $card(G) = n$, 则 $G \simeq (\mathbb{Z}_n, +, \bar{0})$.

② $card(G) = \infty$, 则 $G \simeq (\mathbb{Z}, +, 0)$

prop. 循环群的子群是循环群.

证明 设 $(G, \cdot, e)$ 是循环群且 $card(G) = \infty$, 设 H 是 G 的子群且 $H \neq \{e\}$. 证明 $H \simeq G$.

Pf: 设 $G = \langle g \rangle$. 则 $\exists\, s \in \mathbb{Z}^+$. s.t $H = \langle g^s \rangle$. 于是 $ord(g^s) = \infty$

假设 $ord(g) < \infty \Rightarrow card(G) < \infty \rightarrow \Leftarrow$.

$\Rightarrow H \simeq (\mathbb{Z}, +, 0)$

$\rightarrow G \simeq H$.

作业题3的一个证明.

设 G 是一个群, $a, b \in G$. 满足 $ab = ba$, $ord(a) = s$, $ord(b) = t$. 若 $\gcd(s, t) = 1$, 则 G 中有一个 (st) 阶的循环群, $\langle a, b \rangle = \langle a \cdot b \rangle$

作业3.

pf: $\mathrm{ord}(a\cdot b)=st$.

先证 $\langle a,b\rangle=\langle a\cdot b\rangle$.

$\langle a\cdot b\rangle\subseteq\langle a,b\rangle$

$\because \gcd(s,t)=1 \Rightarrow \exists u,v\in\mathbb{Z},\ s.t\ us+vt=1$

$$\Rightarrow \boxed{a=a^{su+tv}=(a^s)^u\cdot a^{tv}=a^{tv}\cdot e=a^{tv}\cdot b^{tv}=(ab)^{tv}}$$

$\Rightarrow a\in\langle a\cdot b\rangle$.

同理 $b\in\langle a\cdot b\rangle$

$\Rightarrow \langle a,b\rangle\subseteq\langle a\cdot b\rangle$

$\Rightarrow \langle ab\rangle=\langle a\cdot b\rangle$.

例 群中两元素的阶是有限的，但是这两元素乘积的阶可能是无限的。

$SL_2(\mathbb{Z})$ 含元素 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$. 阶分别为4,3.

证明：$\langle AB\rangle$是无限循环群。

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

pf: $A^4=E_2$, $B^3=E_2$.

$$AB=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}=\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}$$

$$(AB)^n=\left(-\begin{pmatrix}1&1\\0&1\end{pmatrix}\right)^n=(-1)^n\begin{pmatrix}1&1\\0&1\end{pmatrix}^n=(-1)^n\Big(\underbrace{\begin{pmatrix}1&0\\0&1\end{pmatrix}}_{E_2}+\begin{pmatrix}0&1\\0&0\end{pmatrix}\Big)^n$$

$$=(-1)^n\sum_{i=0}^{n}\binom{n}{i}\begin{pmatrix}0&1\\0&0\end{pmatrix}^i$$

$$=(-1)^n\left[\binom{n}{0}\begin{pmatrix}1&0\\0&1\end{pmatrix}+\binom{n}{1}\begin{pmatrix}0&1\\0&0\end{pmatrix}\right]$$

$$=(-1)^n\begin{pmatrix}1&n\\0&1\end{pmatrix}\neq E_2,\quad\forall n\in\mathbb{Z}^+$$

$\Rightarrow \mathrm{ord}(AB)=\infty$

上述结论在Abel群不成立，两个有限阶元素乘积的阶是有限的。

交换群。

证明：① 所有四阶群都是交换群。

pf: 设群 G 为 4阶群，则 $\forall a \in G$. $ord(a) = 1, 2, 4$.

① 若 $\exists a \in G$, s.t $ord(a) = 4$, 则 G 为循环群，可交换. $a^i a^j = a^{i+j} = a^j \cdot a^i$.

② 若 G 中无4阶元，则 $\forall a \in G$, $a^2 = e$.

claim: 若 G 是群，若 $\forall x \in G$, $x^2 = e$, 则 G 交换.

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

$x^2 = e$. $y^2 = e$. $\Rightarrow x^2 \cdot y^2 = x(xy)\cdot y = e\cdot e = e$.

$\Rightarrow x(yx)\cdot y = x(xy)\cdot y$

$\Rightarrow x^{-1}x(yx)yy^{-1} = x^{-1}x(xy)yy^{-1}$

$\Rightarrow yx = xy$.

$\Rightarrow G$ 交换。

② 对4阶群 G，要么 $G \cong U = \langle(1234)\rangle$. 要么 $G \cong$

$U_4 = \{e, (12)(34), (14)(23), (13)(24)\}$.

Klein群.

若 G 中有4阶元，$G \cong (\mathbb{Z}_4, +, \bar{0}) \cong U$.

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4$

$\varphi: \mathbb{Z}_4 \to U$

$\bar{1} \mapsto (1234)$

$ord(\bar{1}) = 4$.

若 G 中无4阶元，则设 $G = \{e, a, b, c\}$.

$a^2 = b^2 = c^2 = e$, $ab = c$, $ac = b$, $bc = a$.

若 $ab = a \Rightarrow b = e \rightarrow\leftarrow$.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

构造 $\varphi: G \longrightarrow U_4$

$e \mapsto e$

$a \mapsto (12)(34)$

$b \mapsto (13)(24)$

$c \mapsto (14)(23)$

验证 $\varphi(ab) = \varphi(a)\varphi(b)$.