1、设 G 是一个群, $a, b \in G$ 满足 $ab = ba$. 若 a, b 有互素的阶 s, t, 证明: 元素 ab 的阶为 st 且 $\langle a, b\rangle = \langle ab\rangle$.

① 以 $o(a)$ 表示 a 的阶.

设 $o(a)=s$, $o(b)=t$, $(s,t)=1$. 记 $o(ab)=r$

$ab=ba \Rightarrow (ab)^{st} = a^{st}\cdot b^{st} = (a^s)^t\cdot(b^t)^s = e$.

$\Rightarrow r \mid st$.

$(ab)^r=e \Rightarrow a^r=b^{-r} \Rightarrow a^{rt}=b^{-rt}=e$

$\Rightarrow s \mid rt$ $(s,t)=1 \Rightarrow s \mid r$

同理 $t \mid r$, $(s,t)=1 \Rightarrow s\cdot t \mid r$

$\Rightarrow r=s\cdot t$.

② $\langle ab\rangle \subset \langle a,b\rangle$ $ab=ba$

$\Rightarrow \forall g\in\langle a,b\rangle$ $g=a^i\cdot b^j$

$\Rightarrow \#\langle a,b\rangle \leq s\cdot t$

又 $o(ab)=st \Rightarrow \#\langle a,b\rangle \geq \#\langle ab\rangle = st$

$\Rightarrow \langle a,b\rangle = \langle b,a\rangle$

2、设 G 是一个幺半群, 使得任取 $a, b \in G$, 方程 $ax = b, ya = b$ 有唯一解, 证明: G 是一个群.

我们有更强命题：若 G 是一个半群, $\forall$ $a\cdot b\in G$, 方程 $ax=b$ 与 $ya=b$ 均有解, 则 G 是一个群.

① 任取 $b\in G$, 则 $yb=b$ 有解. 记为 e.

则 $\forall$ $a\in G$, 考虑方程 $bx=a$, 其有解 c

则有 $ea=e\cdot(bc)=(e\cdot b)\cdot c=b\cdot c=a$.

$\Rightarrow G$ 有左逆元 e.

② $\forall a\in G$, $y\cdot a=e$ 有解. 记为 a'

$a'\cdot a=e$.

$\Rightarrow \forall a\in G$, a有左逆元.

③ $\forall a\in G$, $\exists a'\in G$ s.t. $a'\cdot a=e$.

② $\Rightarrow \exists a''$ s.t. $a''\cdot a'=e$.

于是 $a\cdot a'=e(a\cdot a')=(a''\cdot a')\cdot(a\cdot a')$

$=a''(a'\cdot a)\cdot a'$

$=a''\cdot(e)\cdot a'$

$=e$.

且 $a\cdot e=a\cdot a'\cdot a=(a\cdot a')\cdot a=e\cdot a=a$

$\Rightarrow e$为单位元. 任意元素a有逆 a'.

3、 证明:

i) 所有的四阶群都是阿贝尔群, 精确到同构只有置换群 $U=\langle(1234)\rangle$ 和克莱因四元群 V_4 两种.

ii) 所有阶数小于等于 5 的群都是阿贝尔群.

iii) 存在 6 阶非阿贝尔群.

i) $|G|=4$, 若$\exists g\in G$, s.t. $o(g)=4$ 则 $G\cong \mathbb{Z}_4\cong U$

若$\forall g\in G$, $o(g)<4$ Lagrange thm $\Rightarrow$ $o(g)=2$ or 1.

任取 $g_1, g\in G$, $g_1\neq e$, $g_2\neq e$, $g_1\neq g_2$. 则 $o(g_1)=o(g_2)=2$

考虑元素 $g_1\cdot g_2$, 则 $g_1\cdot g_2\neq g_1$

$\neq g_2$

$\neq e$.

$\Rightarrow g_1 \cdot g_2$ 为第4个元素．同理 $g_2 g_1 \neq g_1$
$\neq g_2$
$\neq e$

则 $g_1 g_2 = g_2 g_1$．故而 G 为交换群．

考虑映射 $\varphi: G \longrightarrow V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{aligned} e &\longmapsto (0,0) \\ g_1 &\longmapsto (\bar{1},0) \\ g_2 &\longmapsto (0,\bar{1}) \\ g_1 \cdot g_2 &\longmapsto (\bar{1},\bar{1}) \end{aligned}$$

则此为一同构映射．

ii) ~~素数阶群均为循环群~~ 若 $|G| = 1,2,3,5$，其为循环群．
若 $|G| = 4$，i) $\Rightarrow G$ 交换．

iii) S_3．$|S_3| = 3! = 6$

$(12)(123) = (32)$
$(123)(12) = (13)$

4、 写出正有理数乘法群 $(\mathbb{Q}_+, \cdot)$ 的一个生成元集．在 $(\mathbb{Q}_+, \cdot)$ 中是否存在有限生成元集?

$\{p \in \mathbb{Z} \mid p$ 素数$\}$ 构成 $(\mathbb{Q}_+, \cdot)$ 的一个生成元集．

由算术基本定理：$\forall$ 整数 $a = p_1^{i_1} \cdots p_n^{i_n}$．$i_1, \cdots, i_n \in \mathbb{N}$

故而 $\forall q \in \mathbb{Q}_+$，$q = p_1^{i_1} \cdots p_n^{i_n}$　$i_1, \cdots, i_n \in \mathbb{Z}$．

不存在有限生成元集：若存在，设其为 $q_1, \cdots, q_m$
则 $\exists$ 有限素数 $\{p_1, \cdots, p_n\}$ s.t.
$q_1, \cdots, q_m \in \langle p_1, \cdots, p_n \rangle$
则 $\langle q_1, \cdots, q_m \rangle \subseteq \langle p_1, \cdots, p_m \rangle$
$\Rightarrow (\mathbb{Q}_+, \cdot) \subseteq \langle p_1, \cdots, p_m \rangle$
矛盾，因为存在素数不在 $p_1, \cdots, p_m$ 中．

5、设群 G 是一个有限 (乘法) 群, H 是 G 的一个非空子集, 如果 H 关于 G 的乘法封闭, 证明: H 是一个子群.

事实上，仅需G是一个群，不一定有限，H有限即可。

任取 $h_0\in H$，由于 H关于乘法封闭，

考虑映射 $\varphi_{h_0}: H \longrightarrow H$, $h \longmapsto h\cdot h_0$.

由于G是一个群，φ_{h_0} 为单射，

H有限，任取 $h\in H$，考虑序列

$hh_0, h^2h_0, \ldots, h^nh_0, \ldots$

则必有 $n_1<n_2\in \mathbb{N}_+$ s.t. $h^{n_1}h_0=h^{n_2}h_0$

$\Rightarrow h^{n_2-n_1}=e\in H$

$\forall h\in H$，考虑映射 $\varphi_h: H\longrightarrow H$, $h'\longmapsto h'\cdot h$

φ_h 为单射，H有限 $\Rightarrow \varphi_h$ 为双射。

$\Rightarrow \exists h'\in H$ s.t. $\varphi_h(h')=h'\cdot h=e$.

$\Rightarrow$ H为子群。

Rem：若用①中更一般命题，可简化证明。

6、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.

i) $g,g'\in G$, 定义 $g\sim g'$ 当且仅当 $gg'^{-1}\in\ker\phi$. 证明:$\sim$ 是一个等价关系.

ii) 在 i) 的等价关系下, 证明 $(G/\sim,\cdot)$ 是一个群, 其中 $\bar g\cdot\bar{g'}=\overline{g\cdot g'}$

iii) 证明: $\bar\phi:(G/\sim,\cdot)\to H$, $\bar\phi(\bar g)=\phi(g)$ 是一个群同态.

iv) 证明: $\bar\phi$ 是一个单射, $\mathrm{im}(\phi)=\mathrm{im}(\bar\phi)$, 有 $(G/\sim,\cdot)\cong\mathrm{im}(\phi)$.

i) • $\forall g\in G$. $g\cdot g^{-1}=e\in\ker\varphi$. $\Rightarrow g\sim g$

• $\forall g,g'\in G$ 若 $g\sim g'$ $g\cdot g'^{-1}\in\ker\varphi\Rightarrow g'\cdot g^{-1}=(g\cdot g'^{-1})^{-1}\in G$

$\Rightarrow g'\sim g$

• 若 $g\sim g'$, $g'\sim g''$ 则 $g\cdot g'^{-1}\in\ker\varphi$ $g'\cdot g''^{-1}\in\ker\varphi$

$\Rightarrow g\cdot g''^{-1}=g\cdot g'^{-1}\cdot g'\cdot g''^{-1}\in\ker\varphi$.

$\Rightarrow g\sim g''$

ii)

• 群运算良定义

若 $\bar{g}=\bar{g'}$, $\bar{h}=\bar{h'}$, 要证 $\overline{gh}=\overline{g'h'}$.

i.e. $gh\cdot(g'h')^{-1}=gh\cdot h'^{-1}\cdot g'^{-1}\in\ker\varphi$.

$h\cdot h'^{-1}\in\ker\varphi$, $g\cdot g'^{-1}\in\ker\varphi$

$\Rightarrow \varphi(ghh'^{-1}g'^{-1})=\varphi(g)\cdot\varphi(h\cdot h'^{-1})\cdot\varphi(g'^{-1})$

$=\varphi(g\cdot g'^{-1})=e$.

• $\forall\bar{g},\bar{g'},\bar{g''}\in G/\sim$,

$(\bar{g}\cdot\bar{g'})\cdot\bar{g''}=\overline{g\cdot g'}\cdot\bar{g''}=\overline{g\cdot g'\cdot g''}=\bar{g}\cdot\overline{g'\cdot g''}=\bar{g}\cdot(\bar{g'}\cdot\bar{g''})$

$\forall\bar{g}\in G/\sim$ $\bar{e}\cdot\bar{g}=\overline{eg}=\bar{g}$

$\forall\bar{g}\in G/\sim$ $\overline{g^{-1}}\cdot\bar{g}=\overline{g^{-1}g}=\bar{e}=\overline{g\cdot g^{-1}}=\bar{g}\cdot\bar{g}^{-1}$

$\Rightarrow (G/\sim,\cdot)$ 为一个群.

iii) • $\bar{\varphi}$ 良好定义.

若 $\bar{g}=\bar{g'}$，则 $g\cdot g'^{-1}\in \ker\varphi$

$\Rightarrow \varphi(g\cdot g'^{-1})=e$

$\Rightarrow \varphi(g)=\varphi(g')$

则 $\bar{\varphi}(\bar{g})=\varphi(g)=\varphi(g')=\bar{\varphi}(\bar{g'})$

• $\bar{\varphi}$ 为同态.

$\forall\, \bar{g},\bar{g}'\in G/\sim$

$\bar{\varphi}(\bar{g}\cdot\bar{g}')=\bar{\varphi}(\overline{g\cdot g'})=\varphi(g\cdot g')=\varphi(g)\cdot\varphi(g')$
$=\bar{\varphi}(\bar{g})\cdot\bar{\varphi}(\bar{g}')$

iv) $\mathrm{Im}\,\bar{\varphi}=\{\bar{\varphi}(\bar{g})\mid \bar{g}\in G/\sim\}=\{\varphi(g)\mid g\in G\}=\mathrm{Im}\,\varphi$

若 $\bar{g}\in\ker\bar{\varphi}$，则 $\bar{\varphi}(\bar{g})=\varphi(g)\in\ker\varphi$

$\Rightarrow g\in\ker\varphi \Rightarrow \bar{g}=\bar{e}$.

$\Rightarrow \ker\bar{\varphi}=\{\bar{e}\} \Rightarrow \bar{\varphi}$ 为单射.

故而我们有 $\bar{\varphi}: G/\sim \longrightarrow \mathrm{im}\,\bar{\varphi}$ 为同态且为双射

$\Rightarrow G/\sim\ \simeq \mathrm{im}\,\bar{\varphi}=\mathrm{im}\,\varphi$.

Rem: 此题结论称为群第一同构定理.

如何从旧群构造新群?

① 取子群

② 作直积: 若 G_1, G_2 为群, 则 $G_1\times G_2$ 有一个自然的群结构

$(g_1, g_2), (g_1', g_2') \in G_1\times G_2$ 定义: $(g_1, g_2)\cdot(g_1', g_2') := (g_1 g_1', g_2\cdot g_2')$

更一般地 设 Λ 为一个集合, G_λ, $\lambda\in\Lambda$ 为一族群

$\prod_{\lambda\in\Lambda} G_\lambda$ 上有一自然的群结构

$(g_\lambda), (g_\lambda') \in \prod G_\lambda$ $g_\lambda, g_\lambda' \in G_\lambda$ $(g_\lambda)\cdot(g_\lambda') = (g_\lambda g_\lambda')$.

③ 作直和: 课上已给出.

④ 作商:

- $\forall H < G$ 为一子群, 则我们可以定义等价关系 $\sim_H$

  $g\sim_H g' \Leftrightarrow g\cdot g'^{-1}\in H$.

- 若在 $G/\sim_H$ 上定义运算 $\bar{g}\cdot\bar{g'} = \overline{g\cdot g'}$.

  这个运算良好定义?

  若已知此运算良好定义, 则类似于6题, $G/\sim_H$ 为一个群.
  此时常记为 G/H, 称为 G 关于 H 的商群.

- 什么时候这个运算良好定义?

  运算良定义 $\Leftrightarrow \forall\ \bar{g_1} = \bar{g_1'}, \bar{g_2} = \bar{g_2'}, \overline{g_1 g_2} = \overline{g_1'\cdot g_2'}$

  $\Leftrightarrow \forall\ g_1, g_1', g_2, g_2'$ 若 $g_1 g_1'^{-1}\in H$, $g_2 g_2'^{-1}\in H$
  则 $g_1\cdot g_2\cdot g_2'^{-1}\cdot g_1'^{-1}\in H$

a) 若为良定义, 任取 $g_2\in H$, $g_1' = g_1$, 则有 $g_1\cdot g_2\cdot g_1^{-1}\in H$.

$\Rightarrow \forall\ h\in H, g\in G$, 有 $ghg^{-1}\in H$.

b) 若 $\forall h\in H, g\in G$，有 $ghg^{-1}\in H$.

$$g_1\cdot g_2\cdot g_2'^{-1}\cdot g_1'^{-1}=\left[g_1\cdot(g_2\cdot g_2'^{-1})\cdot g_1^{-1}\right]\cdot(g_1\cdot g_1'^{-1})\in H$$

$\Rightarrow$ 前述运算良定.

- 上述讨论可知，若 H 满足 $\forall g\in G, h\in H$，$ghg^{-1}\in H$，则有商群 G/H.

  满足此条件的子群称为正规子群，记为 $H\trianglelefteq G$

- 可以证明：正规子群有如下等价定义：

  ① $H\trianglelefteq G$，

  ② $\forall g\in H$，$gHg^{-1}=H$，

  ③ $\forall g\in H$，$gH=Hg$.

- Eg：考虑 $\mathbb{Z}$，则 $n\mathbb{Z}\subset\mathbb{Z}$ 为正规子群.

  $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$.

- 若 G 为交换群，$\forall$ 子群 $H\leq G$，则 H 为 G 的正规子群.

- A_3 为 S_3 的正规子群，A_n 为 S_n 的正规子群.