第十三次习题课.

- 群的定义, 单位元与可逆元. 设 G 为一个群, 单位元为 e.
  - 群的定义: 二元运算(乘法), 结合律, 有单位元, 有逆元.
  - 乘法交换的群称为交换群, 或者阿贝尔群. 所含元素个数有限的群称为有限群.
  - 单位元唯一, 逆元唯一。

    证: 以单位元为例, 设 $e, e' \in G$ 为单位元, 则 $ee' = e', ee' = e$, 从而 $e = e'$. $\square$
  - 消去律: 设 $x, y, g \in G$, 且 $xg = yg$, 则 $x = y$. (g 在左侧的情形也一样).

- 子群, 群的生成元, 元素的阶.
  - 子群的定义: 子集且是群.
  - 子群的判别法: 设 H 为 G 的非空子集, 且 $\forall x, y \in H$, $xy^{-1} \in G$, 则 H 成为 G 的子群.
  - Lagrange 定理: 设 G 为有限群, H 为 G 的子群, 则 $\mathrm{card}(H) \,|\, \mathrm{card}(G)$.
  - 设 S 为 G 的非空子集, 定义 $\langle S\rangle := \{x_1^{e_1}x_2^{e_2}\cdots x_m^{e_m} \,|\, m \in \mathbb{N}^+,\ x_1, \cdots, x_m \in S,\ e_1, \cdots, e_m \in \mathbb{Z}\}$, 这是一个 G 的子群, 称为 S 生成的子群. 若 $G = \langle S\rangle$, 则称 S 为 G 的一组生成元.
  - 设 $g \in G$, 定义 g 的阶 $\mathrm{ord}(g) := \min_{m\in\mathbb{N}^+}\{g^m = e\}$.(可以是 ∞)
  - 设 $g^k = e$, 则 $\mathrm{ord}(g) \,|\, k$.
  - $\mathrm{card}(\langle g\rangle) = \mathrm{ord}(g)$.

    证: 设 $m = \mathrm{ord}(g)$, 则 $\langle g\rangle = \{e, g, \cdots, g^{m-1}\}$ $(m < \infty)$ 或 $\{\cdots, g^{-1}, e, g, \cdots, g^n, \cdots\}$ $(m = \infty)$.
  - $g^{\mathrm{card}(\langle g\rangle)} = e$, 或者 $\mathrm{ord}(g) \,|\, \mathrm{card}(\langle g\rangle)$.
  - 设 $k \in \mathbb{N}$, 则 $\mathrm{ord}(g^k) = \dfrac{\mathrm{ord}(g)}{\gcd(k, \mathrm{ord}(g))}$.

- 同态与同构设 G, H 为两个群, 单位元为 e_G, e_H. $\phi: G \to H$ 为映射.
  - 群同态: ϕ 保持乘法, 即 $\phi(ab) = \phi(a)\phi(b)$, $\forall a, b \in G$; 群同构: ϕ 为群同态且为双射.
  - 若 ϕ 为群同态, 则 $\phi(e_G) = e_H$, $\phi(g^{-1}) = (\phi(g))^{-1}$.
  - 若 ϕ 为群同态, 则 $\mathrm{im}(\phi)$ 为 H 的子群.

  循环群.
  - 定义: 由一个元素生成的群称为循环群.
  - 循环群的子群是循环群, 循环群同构于 $\mathbb{Z}$ 或者 Z_n, $\exists\, n \in \mathbb{N}^+$.
  - 素数阶群一定是循环群.

1. 确定 $\mathbb{Z}_{14}$ 中关于乘法的所有可逆元并求它们的逆.

$\mathbb{Z}_{14} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{13}\}$ $\quad a \cdot a^{-1} = \bar{1}$

可逆元： $\bar{1}, \bar{3}, \bar{5}, \bar{9}, \overline{11}, \overline{13}$

对应逆： $\bar{1}, \bar{5}, \bar{3}, \overline{11}, \bar{9}, \overline{13}$

2. 设 G 是实数对 $(a,b), a \neq 0$ 的集合, 在 G 上定义乘法 $\circ$

$$(a,b) \circ (c,d) = (ac, ad+b).$$

证明 $(G, \circ)$ 是群.

证：① 结合律： $\forall\, a,b,c,d,e,f \in \mathbb{R}$.

$[(a,b)\circ(c,d)]\circ(e,f) = (ac, ad+b)\circ(e,f)$

$= (ace, acf+ad+b)$

$(a,b)\circ[(c,d)\circ(e,f)] = (a,b)\circ(ce, cf+d)$

$= (ace, acf+ad+b)$

$\therefore [(a,b)\circ(c,d)]\circ(e,f) = (a,b)\circ[(c,d)\circ(e,f)]$

$(G,\circ)$ 满足结合律.

② 单位元： $\forall\, (a,b) \in G$

$(a,b)\circ(1,0) = (1,0)\circ(a,b) = (a,b)$

$\Rightarrow (1,0)$ 是 $(G,\circ)$ 单位元.

③ 逆元： $\forall\, (a,b) \in G$.

$(a,b)\circ\left(\frac{1}{a}, -\frac{b}{a}\right) = \left(\frac{1}{a}, -\frac{b}{a}\right)\circ(a,b) = (1,0)$

$\Rightarrow \left(\frac{1}{a}, -\frac{b}{a}\right)$ 是 (a,b) 的逆元.

$\Rightarrow (G,\circ)$ 是群.

3. 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:

(1) $\ker(\phi)$ 为 G 的一个子群;

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

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

(3) ϕ 是单射当且仅当 $\ker(\phi) = \{e_G\}$.

证: (1) ① 需证 $\ker(\phi)$ 非空.

ϕ 同态 $\Rightarrow \phi(e_G) = e_H \Rightarrow e_G \in \ker(\phi)$ 非空.

② 需证 $\forall g_1, g_2 \in \ker(\phi) \Rightarrow g_1 g_2^{-1} \in \ker(\phi)$

$\forall g_1, g_2 \in \ker(\phi)$ $\phi(g_1) = \phi(g_2) = e_H$.

则 $\phi(g_1 g_2^{-1}) = \phi(g_1)\cdot\phi(g_2^{-1}) = \phi(g_1)\cdot\phi(g_2)^{-1} = e_H$.

$\Rightarrow g_1 g_2^{-1} \in \ker(\phi)$.

(2) $\forall x \in g\ker(\phi) \Rightarrow \exists g_1 \in \ker(\phi)$ 使 $\phi(g_1) = e_H$.

由 $x = g g_1 = (g g_1 g^{-1}) g$

且 $\phi(g g_1 g^{-1}) = \phi(g)\phi(g_1)\phi(g)^{-1}$

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

$\Rightarrow g g_1 g^{-1} \in \ker(\phi)$ 即 $x \in \ker(\phi) g$.

反之亦然 则 $g\ker(\phi) = \ker(\phi) g$

(3) ① ϕ 单射 反证. 假设 $\exists g \neq e_G \in G$ $\phi(g) = e_H$

又由 $\phi(e_G) = e_H$ 则与 ϕ 单射矛盾.

② 若 $\ker(\phi) = \{e_G\}$

则设 $\varphi(g_1) = \varphi(g_2) = h$ $g_1, g_2 \in G$, $h \in H$

且 $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = h\cdot h^{-1} = e_H$

$\Rightarrow g_1 \cdot g_2^{-1} = e_G$ 即 $g_1 = g_2$ 则 ϕ 为单射.

4. 设 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.

证：由于 G 有限　H 是 G 的非空子集　$\Rightarrow H$ 有限.

又由于 G 是群，$(G,\cdot)$ 满足结合律　$\Rightarrow (H,\cdot)$ 满足结合律.

下只需证 H 中有单位元，逆元.

由 H 对乘法封闭 $\Rightarrow \forall\, h\in H$，则 $\forall\, n\in\mathbb{Z}^+$，$h^n\in H$.

① 由于 H 有限，$\exists\, s,t\in\mathbb{Z}^+$，$h^s=h^t$　$\Rightarrow h^{t-s}=e_H$
（$s<t$）

② 由于 $h\cdot h^{t-s-1}=h^{t-s-1}\cdot h=e_H$　$\Rightarrow h$ 有逆元

5. 设 A,B 分别是群 G 的两个子群，证明：

(1) $A\cup B$ 是 G 的子群当且仅当 A 是 B 的子群或者 B 是 A 的子群；

(2) 群 G 不能表示成两个真子群的并.

证：(1) "$\Rightarrow$"　若 $A\cup B$ 是 G 的子群，假设 $A\not\subseteq B$ 且 $B\not\subseteq A$

则 $\exists\, x\in A$ 且 $x\notin B$　$y\in B$ 且 $y\notin A$.

$\Rightarrow z=x\cdot y\in A\cup B$

$\Rightarrow z\in A$ 或 $z\in B$.

① $z\in A$　$\Rightarrow y=x^{-1}z\in A$　与条件矛盾.

② $z\in B$　$\Rightarrow x=z\cdot y^{-1}\in B$　与条件矛盾.

则假设不成立　$A\subseteq B$ 或 $B\subseteq A$ 成立.

"$\Leftarrow$"　显然成立.

(2) 设 $G=C\cup D$，$C\subsetneq G$，$D\subsetneq G$

由 G 自身是 G 的子群，由(1)可知　$C\subseteq D$ 或 $D\subseteq C$.

不妨设 $C\subseteq D$，则 $C\cup D=D=G$　那与 D 是真子群矛盾.

则原假设不成立　G 不能写成两个真子群的并.

6. 设 $(G,\cdot,e)$ 是有限群. 证明: $\mathrm{card}(G)$ 为偶数当且仅当 G 中包含有元素 g 满足 $g\neq e$ 和 $g^2=e$.

证: "⇒"

card(G)为偶数. 设 $g\neq e$ 且 $g^2\neq e$

则 $g\neq g^{-1}$ ⇒ $G\setminus\{e\}$ 有偶数个元素 即 card(G) 为奇数. 矛盾.

"⇐"

若 $\forall g\neq e,\ g^2=e$ ⇒ $\mathrm{card}(g)=2$

由 Lagrange 定理 $\mathrm{card}(g)\mid\mathrm{card}(G)$ ⇒ card(G)为偶数

补充:

4. 设 H, K 是群 G 的两个子群, 证明 HK 是 G 的子群当且仅当 $HK=KH$.
(注: 设 A,B 是 G 的两个非空子集, 定义 $AB=\{ab\mid a\in A,b\in B\}$.)

证: "⇒"

$HK<G$

$\Rightarrow\forall hk\in HK\quad (hk)^{-1}\in HK$

又: $(hk)^{-1}=k^{-1}h^{-1}\in KH$

$\therefore HK\subseteq KH$ 同理 $KH\subseteq HK$

"⇐" 显然 HK 非空且 $HK\subseteq G$.

$H<G,\ K<G$ ⇒ $\forall h_1,h_2\in H\quad k_1,k_2\in K$

$h_1h_2^{-1}\in H\quad k_1k_2^{-1}\in K$

$\therefore\forall x=h_1k_1,\ y=h_2k_2\in HK$

$x\cdot y^{-1}=h_1k_1(h_2k_2)^{-1}=h_1k_1k_2^{-1}h_2^{-1}$

$\because k_1k_2^{-1}\in K\quad h_2^{-1}\in H\quad \therefore\exists h'\in H\ k'\in K$

$\therefore k_1k_2^{-1}h_2^{-1}\in KH=HK\quad k_1k_2^{-1}h_2^{-1}=h'k'$

$\Rightarrow xy^{-1}=h_1h'k'\in HK$. 即 $HK<G$.