第十五周习题课: 第十四周习题讲解, 群简介

郑晓鹏

中国科学院数学与系统科学研究院

本课程中学习群,环,域的目的

希望把 $\mathbb{R}$ 上的线性代数推广到任意的域上, 比如 $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$, p 为素数.

目录

群的定义: 集合 G 和其上的二元运算 $*$ 构成群, 如果

群的定义: 集合 G 和其上的二元运算 $*$ 构成群, 如果

(G1) 对任意 $x, y, z \in G, x * (y * z) = (x * y) * z$; (结合律)

群的定义: 集合 G 和其上的二元运算 $*$ 构成群, 如果

(G1) 对任意 $x, y, z \in G, x * (y * z) = (x * y) * z$; (结合律)

(G2) 存在 $e \in G$ 使得对任意 $g \in G, g * e = e * g = g$; (单位元)

群的定义: 集合 G 和其上的二元运算 $*$ 构成群, 如果

(G1) 对任意 $x, y, z \in G, x*(y*z) = (x*y)*z$; (结合律)

(G2) 存在 $e \in G$ 使得对任意 $g \in G, g*e = e*g = g$; (单位元)

(G3) G 中每个元素都可逆. (逆元)

$\forall g \in G$, $\exists g' \in G$, s.t. $gg' = g'g = e$. 则 $g' = g^{-1}$.

封闭性 $g_1 * g_2 \in G$

群的定义: 集合 G 和其上的二元运算 $*$ 构成群, 如果

(G1) 对任意 $x, y, z \in G, x * (y * z) = (x * y) * z$; (结合律)

(G2) 存在 $e \in G$ 使得对任意 $g \in G, g * e = e * g = g$; (单位元)

(G3) G 中每个元素都可逆. (逆元)

验证 $(G, *, e)$ 是一个群:

1. 直接根据定义;
2. 验证 $(G, *, e)$ 是某个群的子群.

$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$.

习题 1: 设 p 为素数, 验证 $(\mathbb{Z}_p^\times, \cdot, \bar{1})$ 是一个群.

p 为素数.

反证. $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$, 矛盾

证明: 封闭性: 任意 $\bar{a}, \bar{b} \in \mathbb{Z}_p^\times$, 有 $p \nmid a$, $p \nmid b$, 所以 $p \nmid ab$, 即 $\overline{ab} \in \mathbb{Z}_p^\times$.

$\bar{a}, \bar{b} \in \mathbb{Z}_p^\times \Rightarrow \bar{a} \cdot \bar{b} = \overline{ab} \in \mathbb{Z}_p^\times$.

$\overline{ab} \neq \bar{0} \Leftrightarrow p \nmid ab$

习题 1: 设 p 为素数, 验证 $(\mathbb{Z}_p^\times, \cdot, \bar{1})$ 是一个群.

证明: 封闭性: 任意 $\bar{a}, \bar{b} \in \mathbb{Z}_p^\times$, 有 $p \nmid a$, $p \nmid b$, 所以 $p \nmid ab$, 即 $\overline{ab} \in \mathbb{Z}_p^\times$.
结合律: 显然.

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{abc} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$

习题 1: 设 p 为素数, 验证 $(\mathbb{Z}_p^\times, \cdot, \bar{1})$ 是一个群.

证明: 封闭性: 任意 $\bar{a}, \bar{b} \in \mathbb{Z}_p^\times$, 有 $p \nmid a$, $p \nmid b$, 所以 $p \nmid ab$, 即 $\overline{ab} \in \mathbb{Z}_p^\times$.
结合律: 显然.
单位元: 因为任意 $a \in \mathbb{Z}_p^\times$, 有 $\bar{1} \cdot \bar{a} = \bar{a} \cdot \bar{1} = \bar{a}$, 所以 $\bar{1}$ 是单位元.

习题 1: 设 p 为素数, 验证 $(\mathbb{Z}_p^\times, \cdot, \bar{1})$ 是一个群.

证明: 封闭性: 任意 $\bar{a}, \bar{b} \in \mathbb{Z}_p^\times$, 有 $p \nmid a$, $p \nmid b$, 所以 $p \nmid ab$, 即 $\overline{ab} \in \mathbb{Z}_p^\times$.
结合律: 显然.
单位元: 因为任意 $a \in \mathbb{Z}_p^\times$, 有 $\bar{1} \cdot \bar{a} = \bar{a} \cdot \bar{1} = \bar{a}$, 所以 $\bar{1}$ 是单位元.
逆元: 任意 $\bar{a} \in \mathbb{Z}_p^\times$, 因为 a 和 p 互素, 所以存在 $u, v \in \mathbb{Z}$, $p \nmid u$, 使得

$$ua + vp = au + pv = 1.$$

则 $\bar{u} = \bar{a}^{-1}$. 于是 $\mathbb{Z}_p^\times$ 的任何元素都存在逆元.

常见的群:

1. $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$;
2. $(\mathbb{Q}^*, \cdot, 1)$.
3. $(\mathbb{Z}_n, +, \bar{0})$
4. $(\mathbb{Z}_p^\times, +, \bar{1})$, p 为素数.
5. $(\mathbb{R}^{m\times n}, +, O)$
6. $(\mathrm{GL}_n(\mathbb{R}), \cdot, E_n)$, $(\mathrm{SL}_n(\mathbb{R}), \cdot, E_n)$

注: $(\mathbb{Z}, \cdot, 1)$ 不是群.

模 n 剩余类环: $(\mathbb{Z}_n, +, 0, \cdot, 1)$

任意 $\bar{a}, \bar{b} \in \mathbb{Z}_n$, 加法: $\bar{a} + \bar{b} = \overline{a+b}$, 乘法: $\bar{a} \cdot \bar{b} = \overline{ab}$.

命题 1.1

设 $\bar{a} \in \mathbb{Z}_n$. 则 $\bar{a}$ 关于乘法可逆当且仅当 a 和 n 互素.

模 n 剩余类环: $(\mathbb{Z}_n, +, 0, \cdot, 1)$

任意 $\bar{a}, \bar{b} \in \mathbb{Z}_n$, 加法: $\bar{a} + \bar{b} = \overline{a+b}$, 乘法: $\bar{a} \cdot \bar{b} = \overline{ab}$.

命题 1.1

设 $\bar{a} \in \mathbb{Z}_n$. 则 $\bar{a}$ 关于乘法可逆当且仅当 a 和 n 互素.

命题 1.2

在 $\mathbb{Z}_n$ 中, $\bar{a}$ 是零因子当且仅当 $1 < \gcd(n, a) < n$.

模 n 剩余类环: $(\mathbb{Z}_n, +, 0, \cdot, 1)$

任意 $\bar{a}, \bar{b} \in \mathbb{Z}_n$, 加法: $\bar{a} + \bar{b} = \overline{a+b}$, 乘法: $\bar{a} \cdot \bar{b} = \overline{ab}$.

命题 1.1

设 $\bar{a} \in \mathbb{Z}_n$. 则 $\bar{a}$ 关于乘法可逆当且仅当 a 和 n 互素.

命题 1.2

在 $\mathbb{Z}_n$ 中, $\bar{a}$ 是零因子当且仅当 $1 < \gcd(n, a) < n$.

推论 1.3

$\mathbb{Z}_n$ 是一个域当且仅当 n 为素数.

注意: $\mathbb{Z}_n$ 中一个元素的表示方式不唯一.

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$.

$\bar{1} = \overline{n+1}$

$\bar{0} = \overline{n}$

习题1. (2) 求 $\overline{2}, \overline{3}, \overline{4}$ 在 $(\mathbb{Z}_5, \cdot, 1)$ 的逆.

u, v.

$2 \cdot u + 5 \cdot v = 1$

$\overline{u} = \overline{2}^{-1}$

$\overline{2} \cdot ? = \overline{1}$

$\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$. $\overline{2}^{-1} = \overline{3}$

$\overline{3} \cdot \overline{2} = \overline{1}$ $\cdot\ \overline{3}^{-1} = \overline{2}$

$\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$, $\overline{4}^{-1} = \overline{4}$

习题1. (2) 求 $\overline{2}, \overline{3}, \overline{4}$ 在 $(\mathbb{Z}_5, \cdot, 1)$ 的逆.
(3) 写出 $(\mathbb{Z}_5^\times, \cdot, 0)$ 和 $(\mathbb{Z}_5, +, 0)$

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

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

$\mathbb{Z}_p^\times = \langle a \rangle$

定理 1.4

当 p 为素数时, $\mathbb{Z}_p^\times$ 是一个循环群. (不好证)

习题1. (4) 取 $\bar{a} = \bar{2}$ 或 $\bar{3}$.

$\bar{a} \in \mathbb{Z}_5^\times$, $\mathbb{Z}_5^\times = \langle \bar{a} \rangle$.

$= \{\bar{a}^i \mid i \in \mathbb{Z}\}$.

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

$= \{\bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{3}, \bar{2}^4 = \bar{1}\}$

目录

命题 2.1

设 $(G, \cdot, e)$ 是群, H 是 G 的非空子集. 则 H 是 G 的子群当且仅当对任意 $h_1, h_2 \in H, h_1 h_2^{-1} \in H$.

命题 2.1

设 $(G, \cdot, e)$ 是群, H 是 G 的非空子集. 则 H 是 G 的子群当且仅当对任意 $h_1, h_2 \in H, h_1 h_2^{-1} \in H$.

命题 2.2

设 $(G, \cdot, e)$ 是群, H 是 G 的非空子集. 则 H 是 G 的子群当且仅当对任意 $h_1, h_2 \in H, h_1 h_2 \in H$ 且 $h_1^{-1} \in H$.

习题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 $AB = \{ab \mid a \in A, b \in B\}$.)

易错点: $HK = KH$

$\not\Rightarrow$ $\forall h \in H, k \in K$, 有 $hk = kh$. ✗

$HK = \{hk \mid h \in H, k \in K\}$ ≠

$KH = \{h'k' \mid k' \in K, h' \in H\}$

$\Leftarrow$ $HK = KH$, $\Rightarrow$ HK是G的子群, (显然, HK是非空)

因为K是G的子群, 所以 $k_1 k_2^{-1} \in K$, 同理, $h_2^{-1} \in H$

设 $a, b \in HK$, $\Rightarrow$ $ab^{-1} \in HK$? ≤ 目标.

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

$ab^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 (k_1 k_2^{-1} h_2^{-1}) \in KH$

因为 $HK = KH$, 所以由 $(k_1 k_2^{-1}) h_2^{-1} \in KH = HK$, 即 $(k_1 k_2^{-1}) h_2^{-1} \in HK$.

存在 $h' \in H$, $k' \in K$, 使得 $(k_1 k_2^{-1}) h_2^{-1} = h'k'$, 代入得

$ab^{-1} = h_1 h' k' \in HK$.

则 $ab^{-1} \in HK$ 得 HK为G的子群.

习题3. 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 $AB = \{ab \mid a \in A, b \in B\}$.)

易错点:

证明: $\Rightarrow$. $HK \subset KH$? $KH \subset HK$? ✓

设 $a \in HK$, 因为 HK 是 G 的子群, 所以 $a^{-1} \in HK$, 则 $\exists h' \in H, k' \in K$, s.t.

$a^{-1} = h'k'$

则 $(a^{-1})^{-1} = (h'k')^{-1} = (k')^{-1}(h')^{-1}$,

因为 $(k')^{-1} \in K$, $(h')^{-1} \in H$, 所以 $(k')^{-1}(h')^{-1} \in KH$.

又因为 $(a^{-1})^{-1} = a$, 所以 $a = (k')^{-1}(h')^{-1} \in KH$; 于是 $HK \subset KH$.

反之, $b \in KH$, 则 $\exists k \in K, h \in H$, s.t. $b = kh$. 则

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

又因为 HK 是 G 的子群. 所以

$(b^{-1})^{-1} \in HK$, 即 $b \in HK$. 于是 $KH \subset HK$.

$b \in HK$. ✓

习题3. 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 $AB = \{ab \mid a \in A, b \in B\}$.)

易错点:

证明: 充分性. 显然 HK 非空. 设 $a, b \in HK$, 则存在 $h_1, h_2 \in H$, $k_1, k_2 \in K$, 使得 $a = h_1k_1$, $b = h_2k_2$. 则

$$ab^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}.$$

因为 K, H 为子群, 所以 $k_1k_2^{-1} \in K, h_2^{-1} \in H$, 则 $(k_1k_2^{-1})h_2^{-1} \in KH$. 又因为 $HK = KH$, 所以存在 $h' \in H, k' \in K$, 使得 $(k_1k_2^{-1})h_2^{-1} = h'k'$. 代入可得

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

所以 HK 是 G 的子群.

必要性.

必要性. 设 $hk \in HK$, 因为 HK 是 G 的子群, 所以 $(hk)^{-1} \in HK$. 于是存在 $h' \in H$, $k' \in K$, 使得 $(hk)^{-1} = h'k'$. 两边取逆得 $hk = (k')^{-1}(h')^{-1} \in KH$. 所以 $HK \subset KH$. 反之, 设 $kh \in KH$, 则 $(kh)^{-1} = h^{-1}k^{-1} \in HK$, 因为 HK 为 G 的子群, 所以 $((kh)^{-1})^{-1} \in HK$, 即 $kh \in HK$. 则 $KH \subset HK$. 综上, $HK = KH$.

定理 1 (Lagrange)

设 G 是有限群, H 是 G 的子群. 则

$$\mathrm{card}(H) \mid \mathrm{card}(G).$$

注: $[G : H] = \mathrm{card}(G)/\mathrm{card}(H)$ 称为子群 H 关于 G 的指标(index).

习题6. 设$(G,\cdot,1)$是一个群且$\mathrm{card}(G)=p$, p 为素数. 证明: 任意 $g\in G\setminus\{1\}$, 有$\langle g\rangle = G$.

证明: 设 $H=\langle g\rangle$, 则 H 是 G 的子群. 所以由拉格朗日定理得

$\mathrm{card}(H) \mid \mathrm{card}(G)$.

又因 $\mathrm{card}(G)=p$ 为素数. 所以

$\mathrm{card}(H)=1$ 或 p.

又因为 $H\neq\{1\}$, 所以 $\mathrm{card}(H)=p$, 又因为

$H\subseteq G$,

则 $H=G \Rightarrow \langle g\rangle = G$ □

$H=\{g^{-1}\}$ $g\neq 1$

$\mathrm{card}(H)=1$

$\Rightarrow H=\{1\}$

习题6. 设$(G,\cdot,1)$是一个群且$\mathrm{card}(G)=p$, p 为素数. 证明: 任意 $g\in G\setminus\{1\}$, 有$\langle g\rangle=G$.
证明: 根据拉格朗日公式以及 p 为素数可得.

目录

定义 2

设 $(G, *, e)$ 和 $(H, \star, \epsilon)$ 是两个群. 则映射 $\phi: G \longrightarrow H$ 称为同态 (映射) (homomorphism), 如果对于任意 $x, y \in G$,

$$\phi(x * y) = \phi(x) \star \phi(y).$$

(保持乘法)

(映射)

当同态 ϕ 是双射时, ϕ 称为同构 (isomorphism). 此时我们称群 G 和 H 是同构的(isomorphic), 记为 $G \simeq H$ (即 G 和 H 同构当且仅当 G 和 H 之间存在同构映射).

$G \simeq H$

$$\begin{cases} x \xmapsto{\phi} x' = \phi(x) \\ y \longmapsto y' = \phi(y) \\ x*y \longmapsto x'*y' \end{cases}$$

$$\phi(x*y) = x'*y' = \phi(x) * \phi(y)$$

定义 2

设 $(G, *, e)$ 和 $(H, \star, \epsilon)$ 是两个群. 则映射 ϕ: $G \longrightarrow H$ 称为同态 (homomorphism), 如果对于任意 $x, y \in G$,

$$\phi(x * y) = \phi(x) \star \phi(y).$$

当同态 ϕ 是双射时, ϕ 称为同构 (isomorphism). 此时我们称群 G 和 H 是同构的(isomorphic), 记为 $G \simeq H$ (即 G 和 H 同构当且仅当 G 和 H 之间存在同构映射).

群论基本问题. 对群按同构分类, 即找出 $\mathcal{G}/\cong$ 中所有的等价类, 并在每一类中找出一个典型的代表元.

$G_1 = \langle g_1 \rangle$, $\mathrm{card}(G_1) = n$

$G_2 = \langle g_2 \rangle$, $\mathrm{card}(G_2) = n$

$\phi: G_1 \longrightarrow G_2$

$g_1^i \longmapsto g_2^i$, $i = 1, 2, \cdots, n$.

$g_1 \longmapsto g_2$

- 两个 n 阶的循环群同构, 比如 $(\mathbb{Z}_4, +, \bar{0})$ 和 $(\mathbb{Z}_5^\times, \cdot, \bar{1})$ 同构.
- 当 p 为素数时, 两个 p 阶的群同构.

素数阶的群都是循环群.

$(\mathbb{Z}_4, +, \bar{0}) = (\langle \bar{1} \rangle, +, \bar{0})$

$(\mathbb{Z}_5^\times, \cdot, \bar{1}) = (\langle \bar{2} \rangle, \cdot, \bar{0})$

$\bar{4} = \bar{2}^2$, $\bar{3} = \bar{2}^3$, $\bar{1} = \bar{2}^4$

$\phi: \mathbb{Z}_4 = \{\bar{1}, 2\cdot\bar{1}, 3\cdot\bar{1}, 4\cdot\bar{1} = 0\} \longrightarrow \mathbb{Z}_5^\times = \{\bar{2}, \bar{2}^2, \bar{2}^3, \bar{2}^4\}$

$\bar{1} \longmapsto \bar{2}$

$n\cdot\bar{1} \longmapsto (\bar{2})^n$

$\bar{1} \longmapsto \bar{2}$

$\bar{2} \longmapsto \bar{4}$

$\bar{3} \longmapsto \bar{3}$

$\bar{0} \longmapsto \bar{1}$

阶数	交换群	非交换群
1	$\{e\}$	
2	$(\mathbb{Z}_2, +, \bar{0})$	
3	$(\mathbb{Z}_3, +, \bar{0})$	
4	$\mathbb{Z}_4, (\mathbb{Z}_2 \times \mathbb{Z}_2, +, (0,0))$	
5	$(\mathbb{Z}_5, +, \bar{0})$	
6	$\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$	S_3
7	$\mathbb{Z}_7$	

如何证明 $\mathbb{Z}_4$ 和 $\mathbb{Z}_2 \times \mathbb{Z}_2$.

假设同构，存在同构映射(双射) $\rightarrow$

保持乘法，

习题2. 设

$$\phi : S_n \to \{1, -1\}$$
$$\sigma \mapsto \epsilon_\sigma$$

$\epsilon_{\sigma_1\sigma_2} = \epsilon_{\sigma_1} \cdot \epsilon_{\sigma_2}$

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

证明:

$\sigma_1, \sigma_2 \in S_n$

$\phi(\sigma_1\sigma_2) = \phi(\sigma_1) \cdot \phi(\sigma_2)$?

习题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 $(\{1, -1\}, \cdot, 1)$ 的同态.

证明: 设 $\sigma, \sigma' \in S_n$, 则

$$\phi(\sigma\sigma') = \epsilon_{\sigma\sigma'} = \epsilon_\sigma \epsilon_{\sigma'} = \phi(\sigma)\phi(\sigma').$$

则 ϕ 为同态.

命题 3.1

设 $(G, *, e)$ 和 $(H, \star, \epsilon)$ 是两个群.
(i) 如果 $\phi : G \longrightarrow H$ 是同态, 则对任意的 $x \in G$, $\phi(e) = \epsilon$ 和 $\phi\left(x^{-1}\right) = \phi(x)^{-1}$. *(保持单位元和求逆)*

环同态

命题 3.1

设 $(G, *, e)$ 和 $(H, \star, \epsilon)$ 是两个群.

(i) 如果 $\phi : G \longrightarrow H$ 是同态, 则对任意的 $x \in G$, $\phi(e) = \epsilon$ 和 $\phi\left(x^{-1}\right) = \phi(x)^{-1}$. *(保持单位元和求逆)*

(ii) 如果 $\phi : G \longrightarrow H$ 是同构, 则 ϕ^{-1} 也是同构. *(同构的逆还是同构)*

$\phi(ab) = \phi(a)\phi(b)$

双射

命题 3.1

设 $(G, *, e)$ 和 $(H, \star, \epsilon)$ 是两个群.
(i) 如果 $\phi : G \longrightarrow H$ 是同态, 则对任意的 $x \in G$, $\phi(e) = \epsilon$ 和 $\phi\left(x^{-1}\right) = \phi(x)^{-1}$. *(保持单位元和求逆)*
(ii) 如果 $\phi : G \longrightarrow H$ 是同构, 则 ϕ^{-1} 也是同构. *(同构的逆还是同构)*
(iii) 再设 $(M, \diamond, \theta)$ 是群. 如果 $\phi : G \to H$ 和 $\psi : H \to M$ 是同态*(构)*. 则 $\psi \circ \phi$ 也是同态*(构)*. *(同态的复合还是同态)*

$G_1 \simeq G_2$
$G_2 \simeq G_3$
$\Rightarrow G_2 \simeq G_1$
$\Rightarrow G_1 \simeq G_3$

命题 3.1

设 $(G, *, e)$ 和 $(H, \star, \epsilon)$ 是两个群.
(i) 如果 $\phi : G \longrightarrow H$ 是同态, 则对任意的 $x \in G$, $\phi(e) = \epsilon$ 和 $\phi\left(x^{-1}\right) = \phi(x)^{-1}$. *(保持单位元和求逆)*
(ii) 如果 $\phi : G \longrightarrow H$ 是同构, 则 ϕ^{-1} 也是同构. *(同构的逆还是同构)*
(iii) 再设 $(M, \diamond, \theta)$ 是群. 如果 $\phi : G \to H$ 和 $\psi : H \to M$ 是同态*(构)*. 则 $\psi \circ \phi$ 也是同态*(构)*. *(同态的复合还是同态)*

命题 3.2

设 G, H 是两个群, $\phi : G \longrightarrow H$ 是群同态. 则 $\mathrm{im}(\phi)$ 是 H 的子群.

$\mathrm{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$.

习题5. 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 $\ker(\phi) = \{e_G\}$.

证明: (1) 显然 $e_G \in \ker(\phi)$, 所以 $\ker\phi$ 非空

$\forall a, b \in \ker\phi$, 有 $ab^{-1} \in \ker\phi$ ✓

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

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

所以 $ab^{-1} \in \ker\phi$, 则 $\ker\phi$ 是 G 的子群.

习题5. 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

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

3. ϕ 是单射当且仅当 $\ker(\phi) = \{e_G\}$.

证明: (1) 因为 $\phi(e_G) = e_H$, 所以 $\ker\phi$ 非空. 设 $a, b \in \ker\phi$, 则 $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e_H$, 所以 $\ker\phi$ 是 G 的子群.

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

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

证明: $g\ker(\phi) \subset \ker(\phi)g$?

设 $a \in g\ker\phi$, 则 $\exists b \in \ker\phi$, s.t. $a = gb$, 所以

$$\phi(a) = \phi(gb) = \phi(g)\phi(b) = \phi(g)\cdot e_H = \phi(g)$$

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

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

所以存在 $b' \in \ker\phi$, s.t.

$$ag^{-1} = b', \text{ 即 } a = b'g \in \ker\phi \cdot g$$

于是 $g\ker(\phi) \subset \ker(\phi)g$. 同理可证 $g\ker\phi \supset \ker(\phi)g$.

综上 $g\ker\phi = \ker\phi g$.

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

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

证明: 设 $a \in g\ker(\phi)$, 则 $a = gb, b \in \ker(\phi)$, 则
$\phi(a) = \phi(g)\phi(b) = \phi(g)$. 于是 $\phi(a)\phi(g)^{-1} = e_H$, 即 $\phi(ag^{-1}) = e_H$, 于是
有 $ag^{-1} \in \ker(\phi)$. 所以存在 $b' \in \ker(\phi)$, 使得 $ag^{-1} = b'$, 得到
$a = b'g \in \ker(\phi)g$. 所以

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

同理可得 $g\ker(\phi) \supset \ker(\phi)g$. 所以 $g\ker(\phi) = \ker(\phi)g$.

$H \ni$

显然 $\Rightarrow$

(3) ϕ 是单射当且仅当 $\ker(\phi) = \{e_G\}$.

e_G

$\Rightarrow$ 因为 $\phi(e_G) = e_H$，所以 $e_G \in \ker(\phi)$，若 $g \in \ker\phi$，即

$\phi(g) = e_H = \phi(e_G)$

和单射的定义矛盾.

$\Leftarrow$ 设 $a, b \in G$，且 $\phi(a) = \phi(b)$，则

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

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

因为 $\ker\phi = \{e_G\}$，即 $ab^{-1} = e_G$，$\Rightarrow a = b$，则 ϕ 为单射.

□

(3) ϕ 是单射当且仅当 $\ker(\phi) = \{e_G\}$.
证明: 必要性显然. 充分性. 设 $\phi(a) = \phi(b)$, 则 $\phi(ab^{-1}) = e_H$. 由 $\ker(\phi) = \{e_G\}$ 得 $ab^{-1} = e_G$, 即 $a = b$.

目录

定义 3

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

$g^k = e$ 最小的 k 为 g 的阶

命题 4.1

设 $(G, \cdot, e)$ 是群且 $g \in G$.

1. 如果 $\mathrm{ord}(g) = \infty$, 则对任意 $i, j \in \mathbb{Z}, g^i = g^j$ 当且仅当 $i = j$;
2. 如果 $\mathrm{ord}(g) = k < \infty$, 则对任意 $i, j \in \mathbb{Z}, g^i = g^j$ 当且仅当 $k \mid (i - j)$; 特别地, $g^m = e \Longleftrightarrow k \mid m$.

$g^m = e \Rightarrow \mathrm{ord}(g) \mid m$.

命题 4.1

设 $(G, \cdot, e)$ 是群且 $g \in G$.

1. 如果 $\mathrm{ord}(g) = \infty$, 则对任意 $i, j \in \mathbb{Z}, g^i = g^j$ 当且仅当 $i = j$;
2. 如果 $\mathrm{ord}(g) = k < \infty$, 则对任意 $i, j \in \mathbb{Z}, g^i = g^j$ 当且仅当 $k \mid (i - j)$; 特别地, $g^m = e \Longleftrightarrow k \mid m$.

已知 g 的阶, 求 g^k 的阶

推论 4.2

设 G 是群, $g \in G$ 且 $m = \mathrm{ord}(g) < \infty$. 再设 $k \in \mathbb{Z}^+$. 则

$$\mathrm{ord}\left(g^k\right) = \frac{m}{\gcd(m, k)} = \frac{\mathrm{lcm}(m, k)}{k}.$$

↑循环群证明中用到

带余除法. $m = qg + r,\ 0 \le r < g$

习题3. 设群中元素 a 的阶是 m, 元素 b 的阶是 n, 证明: 当 $ab = ba$ 且 m, n 互素时, 有 ab 的阶为 mn.

易错点: $(ab)^p = a^p b^p = e \not\Rightarrow a^p = e,\ b^p = e$

$xy = e \not\Rightarrow x = e$ 且 $y = e$.

$\approx$

$\checkmark$

证明: $(ab)^{mn} = a^{mn} b^{mn} = e^n \cdot e^m = e$

$\checkmark$

$mn \mid ord(ab)$?

于是 $ord(ab) \mid mn$.

设 $ord(ab) = s$, $(ab)^s = e$.

$e = (ab)^{sm} = a^{sm} b^{sm} = (a^m)^s b^{sm} = e^s b^{sm} = b^{sm}$

于是 $b^{sm} = e$, 所以 $n \mid sm$, 又因为 n, m 互素, 所以 $n \mid s$.

同理. 考虑 $(ab)^{sn} = e$, 可得 $m \mid s$. 因为 n, m 互素, 所以 $nm \mid s$.

$\Rightarrow nm = ord(ab)$

习题3. 设群中元素 a 的阶是 m, 元素 b 的阶是 n, 证明: 当 $ab = ba$ 且 m, n 互素时, 有 ab 的阶为 mn.

易错点:

证明.

习题3. 设群中元素 a 的阶是 m, 元素 b 的阶是 n, 证明: 当 $ab = ba$ 且 m, n 互素时, 有 ab 的阶为 mn.

易错点:

证明. 交换性得, $(ab)^{mn} = (a^m)^n(b^n)^m = e$, 所以 $ord(ab) \mid mn$. 反之, 设 $ord(ab) = s$, 则 $e = (ab)^{sm} = (a^m)^s b^{sm} = b^{sm}$, 所以 $n \mid sm$, 又因为 n, m 互素, 所以 $n \mid s$. 同理 $m \mid s$, 在由 n, m 互素, 得 $mn \mid s$. 即 $mn \mid ord(ab)$. 于是有 $ord(ab) = mn$.

目录

定义 4

设 G 是群, S 是 G 中的非空子集.由 S 生成的子群是指

$$\langle S\rangle = \left\{x_1^{e_1}\cdots x_m^{e_m} \mid m\in\mathbb{Z}^+, x_1,\ldots,x_m\in S, e_1,\ldots,e_m\in\mathbb{Z}\right\}.$$

如果 $G=\langle S\rangle$, 则称 S 中的元素是 G 的一组生成元.

注: S 可能是有限集也可能是无限集. 特别地, 当H 由一个元素生成时, 我们称 H 为循环群.

如果群 G 中的运算是以加法表示的. 则

$$\langle S\rangle = \left\{e_1x_1+\cdots+e_mx_m \mid m\in\mathbb{Z}^+, e_1,\ldots,e_m\in\mathbb{Z}, x_1,\ldots,x_m\in S\right\}$$

命题 5.1

设 G 是群, $g \in G$ 且 $\mathrm{ord}(g) < \infty$. 则

$$\mathrm{card}(\langle g \rangle) = \mathrm{ord}(g)$$

命题 5.1

设 G 是群, $g \in G$ 且 $\mathrm{ord}(g) < \infty$. 则

$$\mathrm{card}(\langle g \rangle) = \mathrm{ord}(g)$$

定理 5

设 G 是有限群, $g \in G$. 则 $g^{\mathrm{card}(G)} = e$, 即 $\mathrm{ord}(g) \mid \mathrm{card}(G)$.

谢谢！