



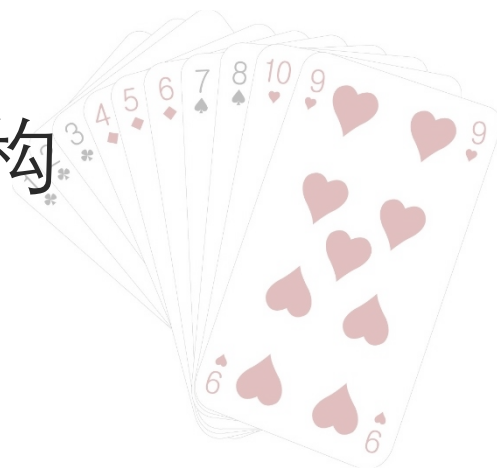
离散数学

Discrete Mathematics

第二十讲：循环群与群同构

吴楠

南京大学计算机学院



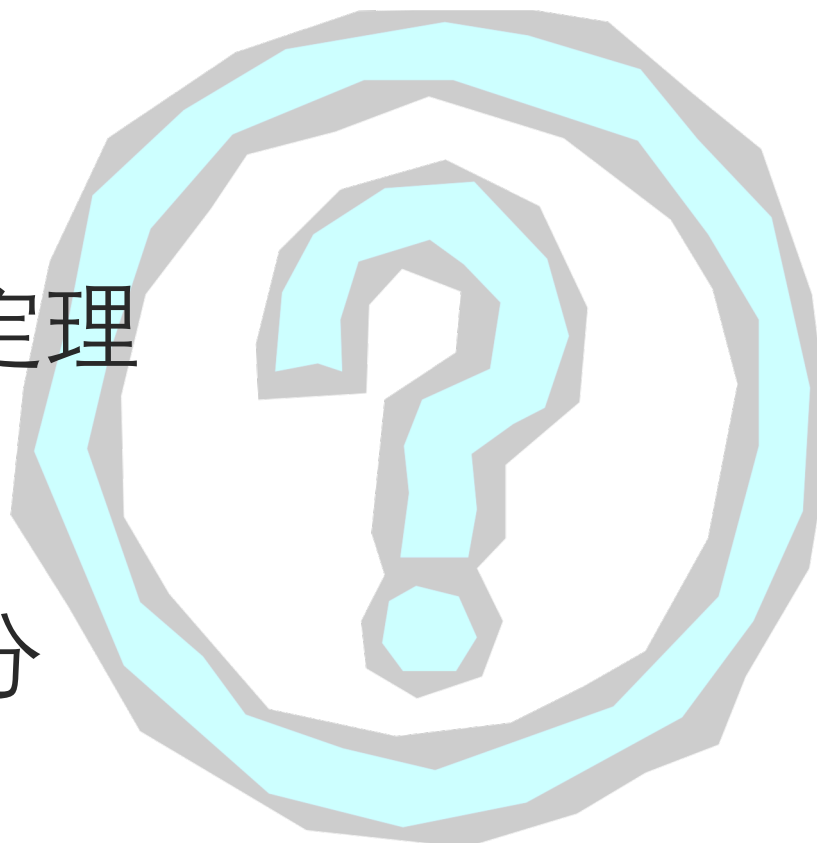
2025 年 5 月 6 日



前情提要



- 子群的定义
- 子群的判定定理
- 有限子群的判定定理
- 群中元素的阶
- 陪集与集合的划分
- Lagrange定理

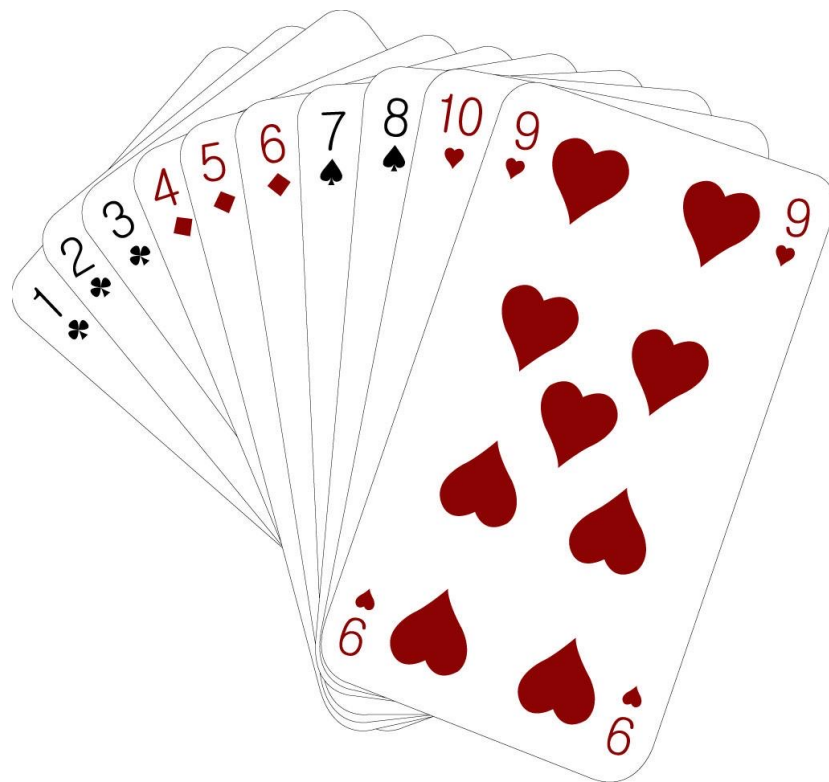




本讲主要内容



- 循环群与生成元
- 循环群的子群
- 群的同构与同态
- 无限循环群的同构群
- 有限循环群的同构群





循环群与生成元

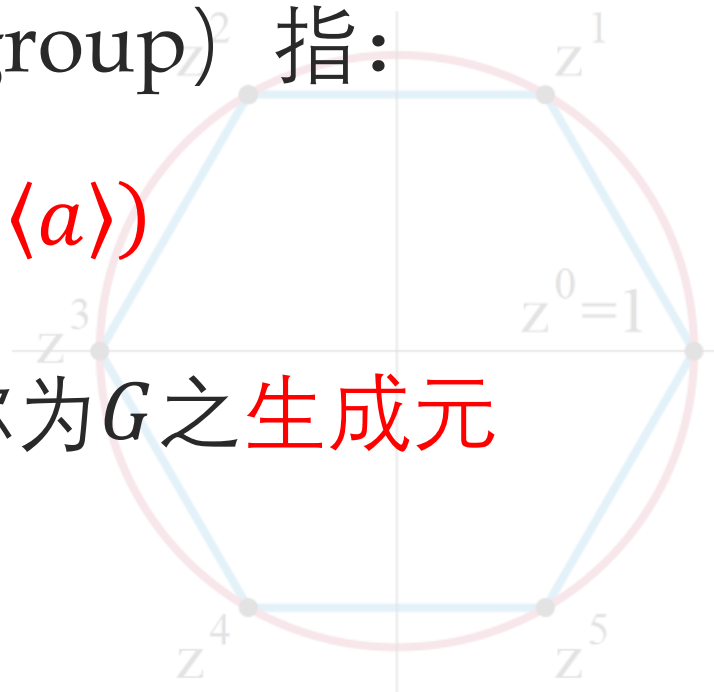


■ 定义（循环群）：

设 $\langle G, * \rangle$ 为循环群 (cyclic group) 指：

$$(\exists a \in G)(G = \langle a \rangle)$$

这里 $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$, a 称为 G 之生成元
(generator)





循环群与生成元 (续)



- **定义 (有限循环群)** : 若循环群 G 的生成元 a 的阶为 n , 则称 G 为有限 (*i.e.* n 阶) 循环群:
 $G = \{a^0, a^1, a^2, \dots, a^{n-1}\}$, 其中 a^0 为单位元
- **定义 (无限循环群)** : 若循环群 G 的生成元 a 为无限阶元, 则称 G 为无限循环群: $G = \{a^0, a^{\pm 1}, a^{\pm 2}, \dots\}$, 其中 a^0 为单位元
- 易见: 循环群的生成元的阶等于群的阶



循环群与生成元 (续)

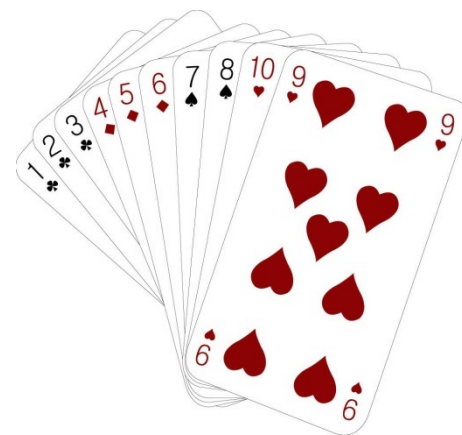


■ 例1: 有限循环群 $\langle \mathbb{Z}_6, \oplus_6 \rangle$

模6剩余加群 $\langle \mathbb{Z}_6, \oplus_6 \rangle$ 是循环群，恰有2个生成元：1和5，如：

$$5^0 = 0, \quad 5^1 = 5, \quad 5^2 = 4,$$

$$5^3 = 3, \quad 5^4 = 2, \quad 5^5 = 1.$$





循环群与生成元 (续)



■ 例2: 无限循环群 $\langle \mathbb{Z}, + \rangle$

$\langle \mathbb{Z}, + \rangle$ 是循环群, 恰有2个生成元: 1和-1

$$\because n \text{ 为 } \mathbb{Z} \text{ 之生成元} \Leftrightarrow \mathbb{Z} = \langle n \rangle \Leftrightarrow (\exists k \in \mathbb{Z}) n^k =$$

$$1 \Leftrightarrow (\exists k \in \mathbb{Z})(k \cdot n = 1) \Leftrightarrow n \in \{1, -1\}$$

\therefore 1和 - 1均是其生成元



循环群与生成元 (续)



■ 例3: 非循环群

Klein四元群 $\langle V, * \rangle$ 不是循环群, 因为对任何

$x \in V$, $\langle x \rangle = \{e, x\}$:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



无限循环群的生成元



- **命题：** 若 a 是无限循环群的生成元，则 a^{-1} 也是该无限循环群的生成元
- **证明：** 设 $G = \langle a \rangle = \{a^k \mid a \in G, k \in \mathbb{Z}\}$, $a^k = (a^{-1})^{-k}$, 令 $p = -k$, 则 $G = \{(a^{-1})^p \mid p \in \mathbb{Z}\}$, 故 $G = \langle a^{-1} \rangle$



无限循环群的生成元 (续)



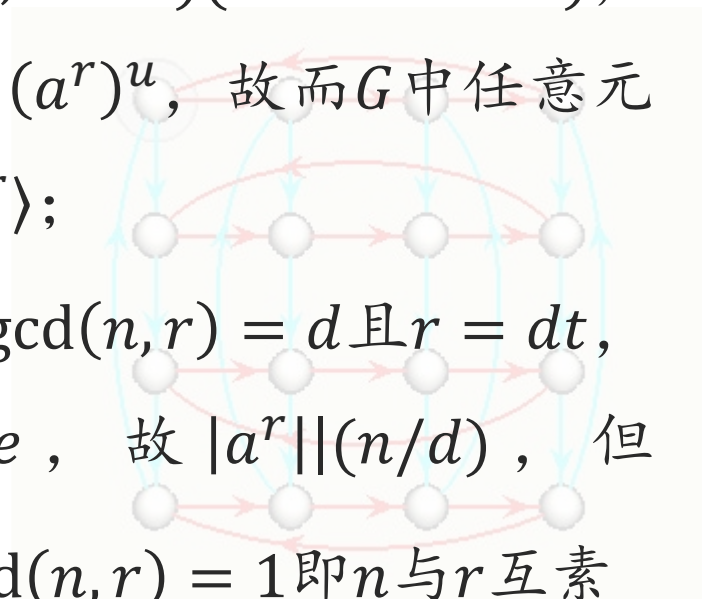
- **命题：** 无限循环群有且只有2个生成元
- **证明：** 设 $G = \langle a \rangle = \{a^k \mid a \in G, k \in \mathbb{Z}\}$, 若 b 亦为 G 的生成元, 则 $(\exists m, t \in \mathbb{Z})(a^m = b \wedge b^t = a)$, 故 $a = b^t = (a^m)^t = a^{mt}$, 由消去律: $a^{mt-1} = e$;
 $\because a$ 是无限阶元, $\therefore mt - 1 = 0 \Rightarrow (m = t = 1) \vee (m = t = -1)$, 故有 $b = a$ 或者 $b = a^{-1}$



有限循环群的生成元



- **命题：** 设有限群 $G = \langle a \rangle$ ，且 $|a| = n$ ，则对任意不大于 n 的正整数 r ， $G = \langle a^r \rangle \Leftrightarrow \gcd(n, r) = 1$
- “ \Leftarrow ”：设 $\gcd(n, r) = 1$ ，则 $(\exists u, v \in \mathbb{Z})(ur + vn = 1)$ ，因此 $a = a^{ur+vn} = (a^r)^u (a^n)^v = (a^r)^u$ ，故而 G 中任意元素 a^k 可表为 $(a^r)^{uk}$ ，故有 $G = \langle a^r \rangle$ ；
 - “ \Rightarrow ”：设 a^r 是 G 的生成元，令 $\gcd(n, r) = d$ 且 $r = dt$ ，则 $(a^n)^t = (a^n)^{r/d} = (a^r)^{n/d} = e$ ，故 $|a^r| \mid (n/d)$ ，但 $|a^r| = n$ 故 $n \mid \frac{n}{d} \Rightarrow d = 1$ ，故有 $\gcd(n, r) = 1$ 即 n 与 r 互素



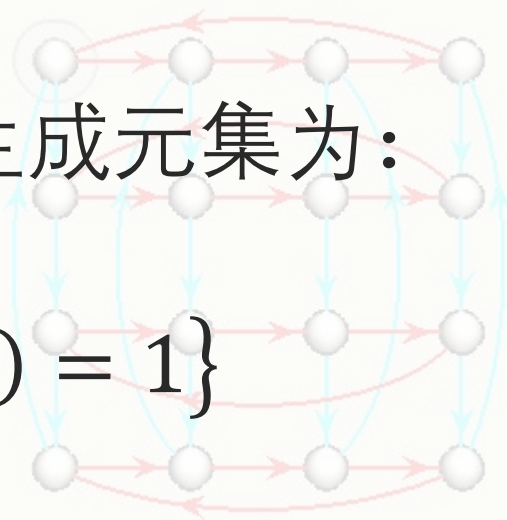


有限循环群的生成元 (续)



- 推论： n 阶循环群 $G = \langle a \rangle$ 的生成元的个数恰为不大于 n 且与 n 互素的正整数的个数，即等于 Euler 函数 $\varphi(n)$ ，因此 G 的生成元集为：

$$\{a^i \mid 0 < i \leq n \wedge \gcd(i, n) = 1\}$$





有限循环群的生成元 (续)



例 (1) 设 $G=\{e,a,\dots,a^{11}\}$ 是 12 阶循环群, 则 $\varphi(12)=4$. 小于或等于 12 且与 12 互素的数是 1, 5, 7, 11, 由定理 11.19 可知 a, a^5, a^7 和 a^{11} 是 G 的生成元.

(2) 设 $G=\langle \mathbb{Z}_9, \oplus \rangle$ 是模 9 的整数加群, 则 $\varphi(9)=6$. 小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理 11.19, G 的生成元是 1, 2, 4, 5, 7 和 8.

(3) 设 $G=3\mathbb{Z}=\{3z \mid z \in \mathbb{Z}\}$, G 上的运算是普通加法. 那么 G 只有两个生成元: 3 和 -3.



循环群的子群



■ 命题：设 $G = \langle a \rangle$ 为循环群，则：

(1) G 的子群亦为循环群

(2) 若 $|a| = \infty$ ，则 G 的子群除 $\{e\}$ 外皆为无限循环群
证：

(1) 令 $\langle H, * \rangle \leq \langle G, * \rangle$ ，从而 $H \subseteq \langle a \rangle$ ，若 $H = \{e\}$ 自然成立

否则取 a^m 为 H 中最小正幂元。下证 $H = \langle a^m \rangle$ ：只需证 $H \subseteq \langle a^m \rangle$ ，任取 $h \in H \subseteq \langle a \rangle$ ，故 $h = a^n$ 。（注：由于子群 H 的运算封闭性， $\langle a^m \rangle \subseteq H$ 易见：若 $\exists (a^m)^k \notin H$ 则 H 不能构成子群）

令 $n = qm + r$ ， $0 \leq \underline{r} < m$ ，从而 $h = a^n = a^{qm+r} = (a^m)^q a^r$ ，从而 $a^r = h(a^m)^{-q} \in H$ ，故由 m 的最小性得 $r = 0$ ，从而 $h = (a^m)^q \in \langle a^m \rangle$ ，因此 H 为循环群。

(2) 设 $H \leq G$ ，由 (1) 得 $H = \langle a^m \rangle$ ，若 $H \neq \{e\}$ 则 $m \neq 0$ ，从而若 $|H|$ 有穷则 $|a^m|$ 有穷与 $|a|$ 无穷矛盾。



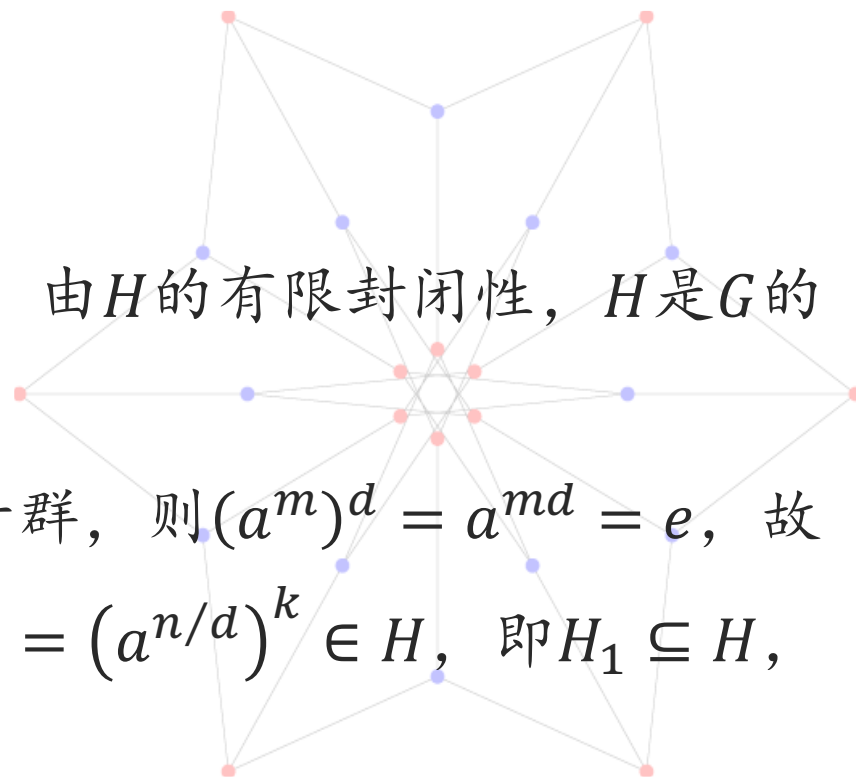
循环群的子群 (续)



■ **命题：**对 n 的每个因子 d ， n 阶循环群 G 中恰有一个 d 阶子群

■ **证明：**

- 设 $G = \langle a \rangle$ ，令 $H = \langle a^{n/d} \rangle$ ，由 H 的有限封闭性， H 是 G 的 d 阶子群
- 令 $H_1 = \langle a^m \rangle$ 亦为 G 的 d 阶子群，则 $(a^m)^d = a^{md} = e$ ，故有 $n|md$ ，即 $\frac{n}{d}|m$ ，因此 $a^m = (a^{n/d})^k \in H$ ，即 $H_1 \subseteq H$ ，但 $H_1 \approx H$ ，故有 $H_1 = H$





循环群的子群 (续)



$G=Z_{12}$ 是 12 阶循环群. 12 的正因子是 1,2,3,4,6 和 12, 因此 G 的子群是:

1 阶子群	$\langle 12 \rangle = \langle 0 \rangle = \{0\}$
2 阶子群	$\langle 6 \rangle = \{0, 6\}$
3 阶子群	$\langle 4 \rangle = \{0, 4, 8\}$
4 阶子群	$\langle 3 \rangle = \{0, 3, 6, 9\}$
6 阶子群	$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$
12 阶子群	$\langle 1 \rangle = Z_{12}$



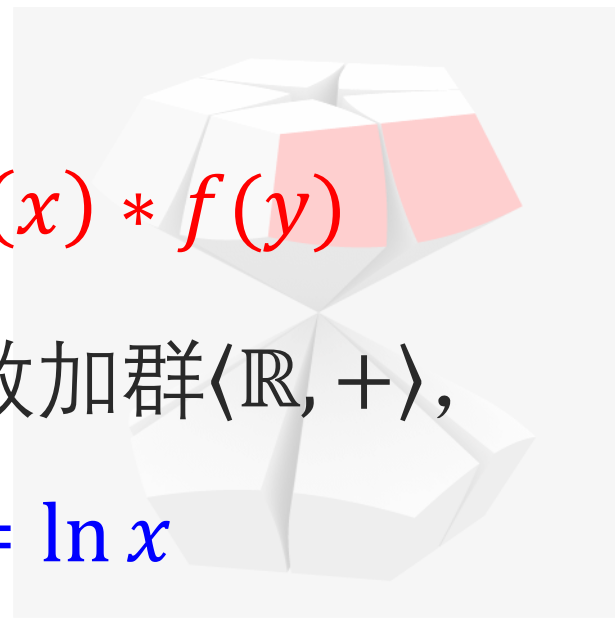
群同构与同构映射



- **定义 (群同构)** : 群 $\langle G_1, \circ \rangle$ 与 $\langle G_2, * \rangle$ 同构 ($G_1 \cong G_2$) 当且仅当存在双射函数 $f: G_1 \rightarrow G_2$, 满足:

$$\forall x, y \in G_1, f(x \circ y) = f(x) * f(y)$$

- **例**: 正实数乘群 $\langle \mathbb{R}^+, \times \rangle$ 和实数加群 $\langle \mathbb{R}, + \rangle$, 同构映射 $f: \mathbb{R}^+ \rightarrow \mathbb{R}, f(x) = \ln x$





群同构关系是等价关系



- **自反性**: 对任意群 $\langle G, \circ \rangle$, $G \cong G$
 - 此时同构映射为恒同映射 $f(x) = x$
- **对称性**: 对任意群 G_1, G_2 , 若 $G_1 \cong G_2$ 则 $G_2 \cong G_1$
 - 后者的同构映射为前者同构映射的逆函数
- **传递性**: 对任意群 G_1, G_2, G_3 , 若 $G_1 \cong G_2$ 且 $G_2 \cong G_3$ 则 $G_1 \cong G_3$
 - 设前二者同构映射分别为 $f: G_1 \rightarrow G_2$, $g: G_2 \rightarrow G_3$, 则
$$g \circ f: G_1 \rightarrow G_3$$



群同构与同构映射（续）



- 回忆第18讲中提到的四阶群以下的同构性：
 - 任意两个三阶群同构

$1 \rightarrow a \quad 2 \rightarrow b \quad 3 \rightarrow c$

\circ	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

$*$	a	b	c
a	a	b	c
b	b	?	a
c	c	a	b



群同构与同构映射 (续)



- 回忆第18讲中提到的四阶群以下的同构性：
 - 不同构的四阶群

	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

四元循环群

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Klein四元群



同态与同态映射



- 群同态对映射的要求远低于群同构，只需找到符合条件的函数即可

- **定义（群同态）**：群 $\langle G_1, \circ \rangle$ 与 $\langle G_2, * \rangle$ 同态($G_1 \sim G_2$)当且仅当存在函数 $f: G_1 \rightarrow G_2$ ，满足：

$$\forall x, y \in G_1, f(x \circ y) = f(x) * f(y)$$

- 如果上述映射是满射，则称为**满同态**；如映射是单射，则称为**单同态**；若 $G_1 = G_2$ ，则称 φ 为**自同态***



同态与同态映射 (续)



■ **命题：** 设 f 为从群 $\langle G, \circ \rangle$ 到群 $\langle H, * \rangle$ 的同态，则

$$(1) f(e_G) = e_H;$$

$$(2) f(a^{-1}) = (f(a))^{-1}, \quad \forall a \in G$$

■ **证明：**

$$(1) \because f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$$

$$\therefore f(e_G) = f(e_G) * (f(e_G))^{-1} = e_H$$

$$(2) \because f(a^{-1}) * f(a) = f(a^{-1} \circ a) = f(e_G) = e_H$$

$$f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e_G) = e_H$$

$$\therefore f(a^{-1}) = (f(a))^{-1}$$



同态与同态映射 (续)



- **例：** 整数加系统 $\langle \mathbb{Z}, + \rangle$ 与模3剩余加系统 $\langle \mathbb{Z}_3, \oplus_3 \rangle$ 同态，同态映射为

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_3, f(3k + r) = r, k \in \mathbb{Z}$$

此同态为满同态

- **趣味问题：** 由 $1, 2, \dots, 2024$ 所有这些自然数按照任意的组合进行加减，能否得到2025？



同态与同态映射 (续)



- 趣味问题：由 $1, 2, \dots, 2024$ 这些自然数按照任意的组合进行加减，能否得到2025？

- 定义系统（奇偶加群）： $\langle \{e, o\}, * \rangle$ ，运算表如下：

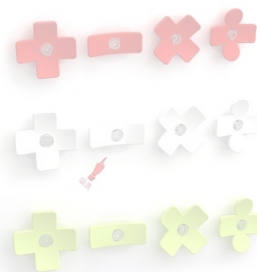
则 $f: \mathbb{Z} \rightarrow \{e, o\}$

$*$	e	o
e	e	o
o	o	e

$$f(x) = \begin{cases} e & x \text{ 是偶数} \\ o & x \text{ 是奇数} \end{cases}$$

是从 $\langle \mathbb{Z}, + \rangle$ 到 $\langle \{e, o\}, * \rangle$

的满同态映射





无限循环群的同构群



■ **定理：** 设 $\langle G, * \rangle$ 为无限循环群，则 $\langle G, * \rangle \cong \langle \mathbb{Z}, + \rangle$

■ **证明：** $|a| = \infty$ ，令 $f: \mathbb{Z} \rightarrow G$ 如下： $f(x) = a^x$ ，

$\because f(n + m) = a^{n+m} = a^n * a^m = f(n) * f(m) \therefore f$ 为

同态；又 $\because f(n) = f(m) \Rightarrow a^n = a^m \Rightarrow a^{|n-m|} =$

$e \Rightarrow |n - m| = 0 \Rightarrow n = m$ ， $\therefore f$ 为 1-1，由循环群

的定义易见 f 亦为满射，从而 $\langle G, * \rangle \cong \langle \mathbb{Z}, + \rangle$



有限循环群的同构群



- **定理：** 设 $\langle G, * \rangle$ 为有限循环群，则 $\langle G, * \rangle \cong \langle \mathbb{Z}_n, \oplus_n \rangle$
- **证明：** 设的 G 生成元为 a ， $|a| = n > 0$ 从而 $G = \{a^0, a^1, \dots, a^{n-1}\}$ ， $f: \mathbb{Z}_n \rightarrow G$ 定义为： $f(x) = a^x (x = 0, 1, \dots, n-1)$ ，由于在 G 中 $a^{i+j} = a^{i \oplus_n j}$ ，所以 $f(i \oplus_n j) = a^{i \oplus_n j} = a^i * a^j = f(i) * f(j)$ ， f 为同态；又由于 $\forall i, j \in \mathbb{Z}_n$ ， $f(i) = f(j) \Rightarrow a^i = a^j \Rightarrow a^{|i-j|} = e \Rightarrow n \mid |i-j| \Rightarrow i \equiv j \pmod{n} \Rightarrow i = j$ ，故 f 为单射；由循环群的定义易见 f 亦为满射，因此 $\langle G, * \rangle \cong \langle \mathbb{Z}_n, \oplus_n \rangle$



循环群的同构群



- 定理：设 $\langle G, * \rangle$ 为无限循环群，则 $\langle G, * \rangle \cong \langle \mathbb{Z}, + \rangle$
- 定理：设 $\langle G, * \rangle$ 为有限循环群，则 $\langle G, * \rangle \cong \langle \mathbb{Z}_n, \oplus_n \rangle$

推论：循环群皆为阿贝尔群



本次课后作业



- 教材内容：[屈婉玲] 10.3节
- 课后习题：
 - Problem Set 20
- 提交时间：5月13日 10:00 前



Joseph Louis Lagrange (1736–1813)



- “拉格朗日是数学科学界高耸的金字塔。” —— 拿破伦·波那巴
- “在短得令人难以置信的时间内，他就完全靠自学掌握了他那个时代的现代分析。十六岁时（可能不太准确），拉格朗日成了在都灵的皇家炮兵学院的数学教授。然后开始了数学史上最光辉的经历之一。”
- “他的杰作《分析力学》是他作为一个十九岁的少年在都灵设想出来的。”
- 这位十八世纪最伟大，最谦虚的数学家的最著名的语录是：“我不知道。” —— E.T.贝尔《数学精英》
- 法国伟大的数学传统 —— “4L”
 - Lagrange(1736–1813); Laplace(1749–1827); Legendre(1752–1833); Lebesgue(1875–1941)
(拉格朗日、拉普拉斯、勒让德、勒贝格)