



第八章 群

刘世霞

shixia@tsinghua.edu.cn



内容回顾：群的定义

定义8.2.1

封闭么逆

- 设 G 是非空集合， \cdot 是 G 上的二元运算，若代数系统 (G, \cdot) 满足
 1. 适合结合律，即 $\forall a, b, c \in G$, 有 $(ab)c = a(bc)$
 2. 存在单位元 e ，使得 $\forall a \in G, ae = ea = a$
 3. G 中的元素都是可逆元。即 $\forall a \in G$, 都 $\exists a^{-1} \in G$ ，使得 $aa^{-1} = a^{-1}a = e$
- 则称代数系统 (G, \cdot) 是一个群，或记为 (G, \cdot, e) 。
- 为了方便起见，常用 G 表示群 (G, \cdot, e)



内容回顾：群的性质

性质1 设 (G, \cdot) 为群，则 $\forall a \in G$ ， a 的左逆元也是 a 的右逆元.

性质2 设 (G, \cdot) 为群，则 G 的左单位元 e 也是右单位元.

性质3 设 (G, \cdot) 为群，则 $\forall a, b \in G$ ，方程 $a \cdot x = b$ 和 $y \cdot a = b$ 在 G 中的解唯一.



内容回顾：群的性质

性质4 设 (G, \cdot) 为群，则

(1) $\forall a \in G, (a^{-1})^{-1} = a;$

(2) $\forall a, b \in G, (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$

性质5 群 (G, \cdot) 中的乘法满足消去律，即 $\forall a, b, c \in G$ 有

(1) 若 $a \cdot b = a \cdot c$ ，则 $b = c$ (左消去律)

(2) 若 $b \cdot a = c \cdot a$ ，则 $b = c$ (右消去律)



内容回顾：群的性质

性质6 设 G 为群，则 G 中的幂运算满足：

(1) $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbb{Z}$

(2) $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbb{Z}$

(3) 若 G 为交换群，则 $(ab)^n = a^n b^n$.

性质7 G 为群， $a \in G$ 且 $|a| = r$. 设 k 是整数，则

(1) $a^k = e$ 当且仅当 $r \mid k$.

(2) $\langle a^{-1} \rangle = \langle a \rangle$.

内容回顾：群、群的基本性质



定理8.2.6

- H 是 G 的子群的充要条件是：
 1. H 对 G 的乘法运算是封闭的，即 $\forall a, b \in H$ ，都有 $ab \in H$
 2. H 中有单位元 e' ，且 $e' = e$
 3. $\forall a \in H$ ，都有 $a^{-1} \in H$ ，且 a^{-1} 是 a 在 G 中的逆元



内容回顾：满足子群的条件

封闭性、单位元、逆元素

非空的

封闭性

内容回顾：群、群的基本性质



定理8.2.7

- G 的非空子集 H 是 G 的子群的充要条件是 $\forall a, b \in H$, 都有 $ab^{-1} \in H$



内容回顾：循环群定义

- 若群 G 中存在一个元素 a ，使得 G 中的任意元素 g ，都可以表示成 a 的幂的形式，即
$$G = \{a^k | k \in \mathbb{Z}\},$$
- 则称 G 是循环群，记作 $G = \langle a \rangle$ ， a 称为 G 的生成元。

由一个元素生成的群

内容回顾：关于循环群的一个结论



- 所有的循环群都同构于 $(\mathbb{Z}, +)$ 或 $(\mathbb{Z}_n, +)$
- 当 $o(a)=\infty$ 时, $G \cong (\mathbb{Z}, +)$ 无限循环群
- 当 $o(a)=n$ 时, $G \cong (\mathbb{Z}_n, +)$ n 阶循环群

内容回顾：循环群 群的同构



定理8.3.1

- 设 $G = \langle a \rangle$, 则
 - 1. 若 $o\langle a \rangle = \infty$, 则 G 中只有生成元 a 或 a^{-1}
 - 2. 若 $o\langle a \rangle = n$, 则 G 中有 $\varphi(n)$ 个生成元
 - 其中 $\varphi(n)$ 是欧拉函数, 它表示小于 n 且与 n 互素的正整数个数。

循环群中, 若某元素的幂次与 n 互素, 则可以作为另一生成元!



内容回顾：定理8.3.1

定理8.3.1 若 $o\langle a \rangle = n$ ，则 G 中有 $\varphi(n)$ 个生成元

• 证明（续）：

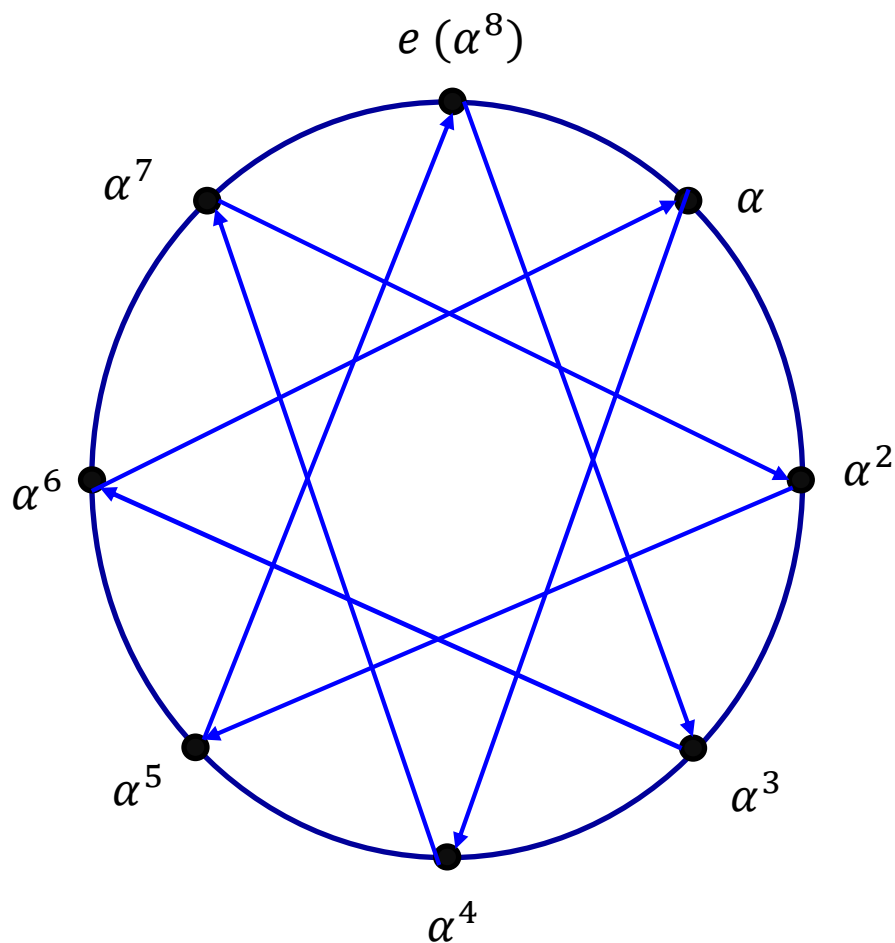
- 当 $o\langle a \rangle = n$ 时，若 $G = \langle a \rangle = \langle a^r \rangle$ ，则存在 p 使 $a = (a^r)^p$ ，即 $a^{rp-1} = e$
- 故存在 q ，使得 $rp - 1 = qn$ 裴蜀定理
- 即 $(r, n) = 1$ 证毕！

裴蜀定理： a, b 互质的充分必要条件是存在整数 x, y 使 $ax + by = 1$

循环群中，若某元素的幂次与 n 互素，则可以作为另一生成元！



内容回顾：举例





关于群的元素阶，下列说法正确的是

- ☒ A 有限群的元素阶都是有限的
- ☐ B 所有元素的阶都是有限的群必为有限群
- ☒ C 存在无限群，其元素的阶都是有限的
- ☐ D 存在无限群，其元素的阶都是无限的



解答

- A: 有限群的元素的阶都是有限的
- B: 所有元素的阶都是有限的群必为有限群
- C: 存在无限群，其元素的阶都是有限的
- D: 存在无限群，其元素的阶都是无限的

解答

- A 正确，否则无限阶元的若干次幂就构成了一个无限集合
- B 错误 C正确，如 $(P(M), \oplus)$ ：除单位元外所有元素阶均为2的群
- D 错误，单位元的阶只能为1



群的同构

定义8.3.2

- 设 (G, \cdot) 和 $(G', *)$ 是两个群,
 $f: G \rightarrow G'$ 是双射, 如果 $\forall a, b \in G$ 都有
$$f(ab) = f(a) * f(b)$$
- 则称 f 是 G 到 G' 的一个同构, 记作 $G \cong G'$

群同构的充分条件: 1. 双射 2. 保持运算!



8.3 循环群 群的同构

- 思考：

循环群 G 的子群 H 是否仍然是循环群？ **YES!**

分析：子群 H 的生成元？

G 的子群 H ，可以写为 $H = \{e, a^{k_1}, a^{k_2}, \dots, a^{k_m}, \dots\}$

不妨设 H 所有元素的幂次中， k_1 是最小值

则对于 H 中其他元素 a^{k_m} 幂次进行分析，一定有 $k_m = l \cdot k_1 + r$ ，其中 $0 \leq r < k_1$ 。

故 $a^{k_m} = a^{r+l \cdot k_1} = a^r a^{l \cdot k_1} \longrightarrow a^r = a^{k_m} (a^{l \cdot k_1})^{-1} \longrightarrow$

$a^r \in H$

$r = 0$

最小次幂是生成元



8.3 循环群 群的同构

- 思考：

G 为循环群时， G 的子群是什么特征？

- 若 G 为无限循环群：

假设子群 H 生成元是 a^k ，则该生成元的阶数一定为 ∞

否则若存在正整数 q ，使得 $(a^k)^q = e$ ，将说明 a 为有限阶元，矛盾！

- 若 G 为无限循环群，则其非平凡子群也为无限循环群！



8.3 循环群 群的同构

- 思考：

G 为循环群时， G 的子群是什么特征？

- 若 G 为 n 阶循环群：

假设子群 H 生成元是 a^{k_1} ，设其阶数为 d

由于 $(a^{k_1})^n = (a^n)^{k_1} = (e)^{k_1} = e$ （定理8.2.5）

则必定有 $d|n$

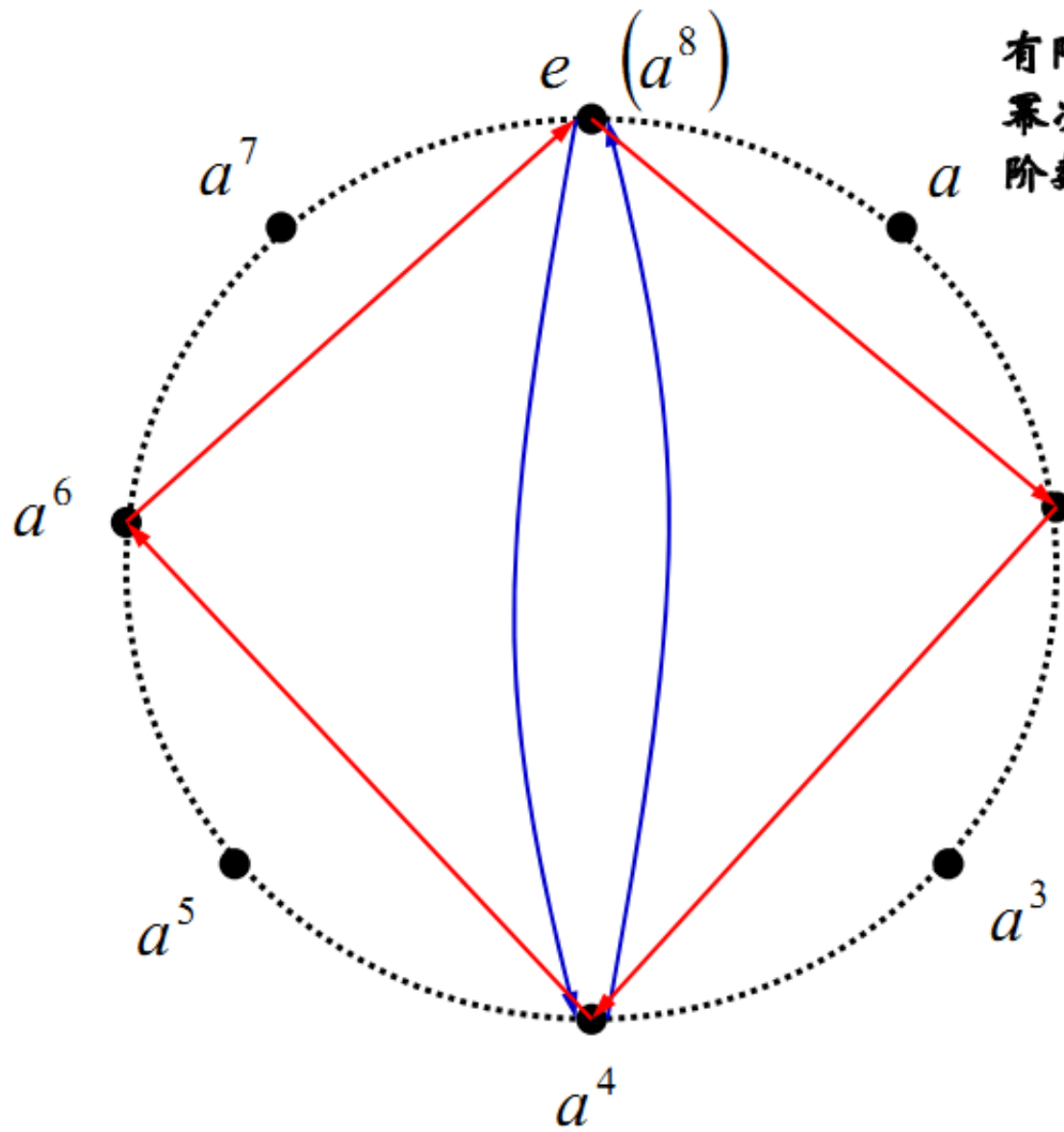
- 若 G 为 n 阶循环群，则其子群生成元阶数为 n 因数！

定理8.2.5 设 a 是群 G 中的一个 r 阶元素， k 是正整数，则

1. $a^k = e$ ，当且仅当 $r|k$



8.3 循环群 群的同构



有限循环群中，
幂次与 n 互质，可做生成元
阶数为 n 因数，可做子群生成元

$$a = (a^r)^p$$

$$a^{rp-1} = e$$

$$rp - 1 = qn$$



8.3 循环群 群的同构

定理8.3.2

- 设 $G = \langle a \rangle$ 是循环群，则
 1. G 的子群 H 都是循环群。
 2. 若 G 是无限群，则子群 $H (H \neq \{e\})$ 也是无限群，
若 G 是有限群时，设 $|G| = n$ ，且 a^k 是 H 中 a 的**最小正幂**，则 $|H| = n/k$ 。



8.3 循环群 群的同构

定理8.3.2

• 证明:

1. G 的子群 H 都是循环群

- H 是 G 子群, 则 H 中的元素可以表示成 a 的方幂的形式
- 设 a^k 是 H 中 a 的最小正幂, 任取 $a^s \in H, s = pk + r (0 \leq r < k)$, 所以 $a^r = a^{s-pk} = a^s a^{-pk} = a^s (a^k)^{-p} \in H$
- a^k 是最小正幂, 故 $r = 0$, 即 $a^s = (a^k)^p$, 故 $H = \langle a^k \rangle$



8.3 循环群 群的同构

定理8.3.2

• 证明:

2. 若 G 是无限群, 则 $H(H \neq \{e\})$ 也是无限循环群

– 反证法

– 设 $a^k (k \neq 0)$ 是 H 的一个生成元, 且 a^k 是 n 阶元

– $(a^k)^n = e$, 即 $a^{kn} = e$, 与 a 是无限阶元矛盾

– a^k 是无限阶元

– H 是无限阶循环群



8.3 循环群 群的同构

定理8.3.2

• 证明:

3. $|G| = n$, 且 a^k 是 H 中的 a 的最小正幂, 则 $|H| = n/k$

- $O\langle a \rangle = n$, 即 $a^n = e$
- a^k 是循环群 H 中 a 的最小正幂 (即 $H = \langle a^k \rangle$)
- 存在最小正整数 m , 使 $(a^k)^m = e = a^n$, 即 $km = n$
- a^k 的阶 $m = n/k$, 即 $|H| = n/k$ 。



8.3 循环群 群的同构

问题：

- n 阶循环群，对于 n 的某个因子，可有几个子群
- 例如：10阶循环群，因子为2、5，则对应生成元阶为2的循环子群有几个？

定理8.3.3: 设 G 是 n 阶循环群, 则对于 n 的每一个正因子 d , G 有且只有一个 d 阶子群



• 证明:

由于 d 为 n 的正因子, 可知 $H = \langle a^{\frac{n}{d}} \rangle$ 是 G 的 d 阶子群。

假设存在 $H_1 = \langle a^m \rangle$ 也是 G 的 d 阶子群, 且 a^m 是 H_1 中最小正幂元。

显然, $a^{md} = (a^m)^d = e$, 则有 $n|md \Rightarrow \frac{n}{d}|m$

令 $m = \frac{n}{d} \cdot t (t \in \mathbb{Z})$ 则有:

$$a^m = a^{\frac{n}{d} \cdot t} = (a^{\frac{n}{d}})^t \in H$$

此时可以看出, a^m 是 H_1 的生成元, 但是却是 H 中的一个元素。因此必然有 $H_1 \subseteq H$ 。但是二者的阶数又相等, 因而 $H_1 = H$ 。



8.3 循环群 群的同构

定理8.3.3

- 设 G 是 n 阶循环群，则对于 n 的每一个正因子 d ， G 有且只有一个 d 阶子群。

n 阶循环群， n 的因子有几个，子群就有几个！



群 $(Z_{14}, +)$ 的子群为

☒ A Z_{14}

☒ B $\langle \overline{2} \rangle$

☒ C $\langle \overline{7} \rangle$

☒ D $\langle \overline{0} \rangle$



实例

- 剩余类加群 $(Z_{14}, +)$ 中14的正因子有1,2,7,14, 因此 Z_{14} 有4个子群: 它自身, 单位元群 $\langle \bar{0} \rangle$, 以及 $\langle \bar{2} \rangle, \langle \bar{7} \rangle$, 其中 $o\langle \bar{2} \rangle = 7, o\langle \bar{7} \rangle = 2$



8.3 循环群 群的同构

定义8.3.2

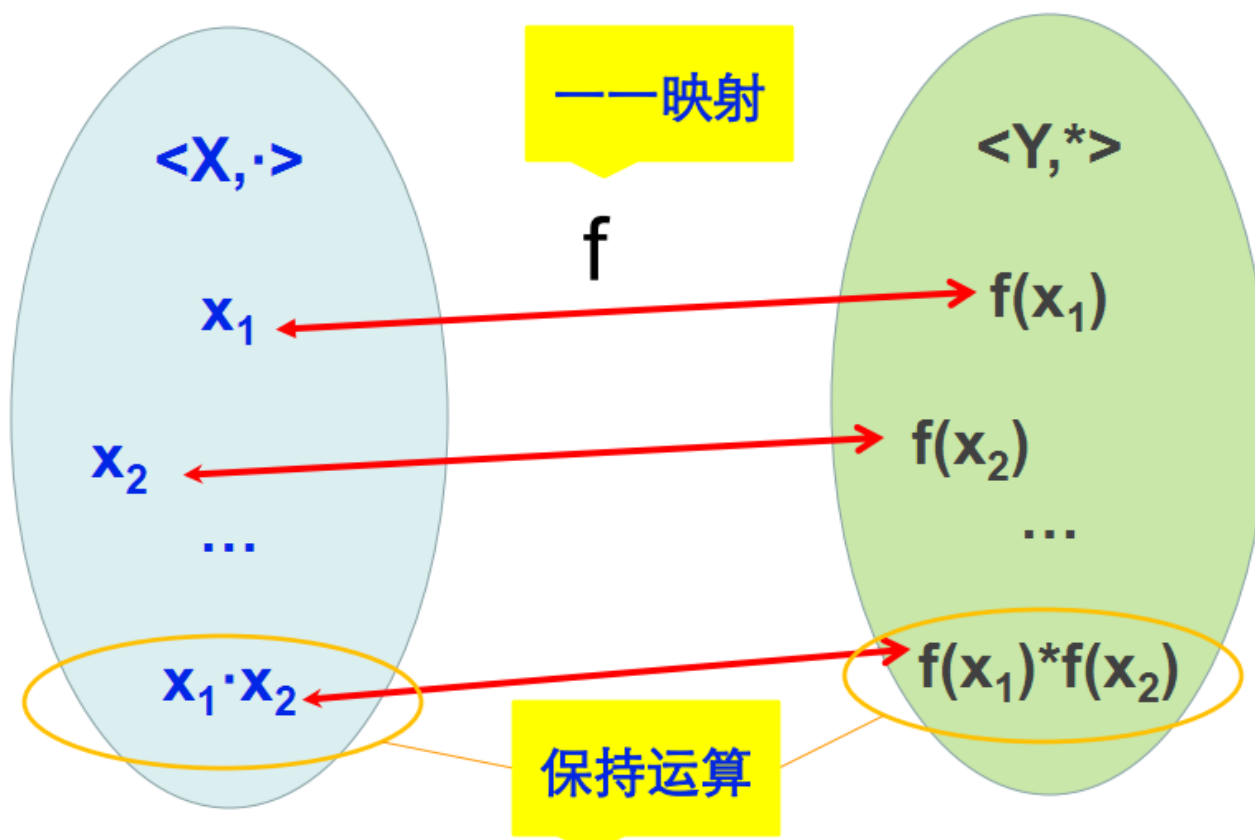
- 设 (G, \cdot) 和 $(G', *)$ 是两个群,
 $f: G \rightarrow G'$ 是双射, 如果 $\forall a, b \in G$ 都有
$$f(ab) = f(a) * f(b)$$
- 则称 f 是 G 到 G' 的一个同构, 记作 $G \cong G'$

群同构的充分条件: 1. 双射 2. 保持运算!



8.3 循环群 群的同构

同构示意图





8.3 循环群 群的同构

例:

- 设 $G = (R^+, \times)$, $G' = (R, +)$, 令 $f: x \rightarrow \ln x$

则 f 是从 G 到 G' 的一个双射, 且 $\forall x, y \in G$

$$f(x \times y) = \ln(xy) = \ln x + \ln y = f(x) + f(y)$$

因此, $G \cong G'$



8.3 循环群 群的同构

定理8.3.4

- 设 G 是循环群, a 为生成元
- 1. 若 $O\langle a \rangle = \infty$, 则 G 与 $(\mathbb{Z}, +)$ 同构
- 2. 若 $O\langle a \rangle = n$, 则 G 与 $(\mathbb{Z}_n, +)$ 同构



8.3 循环群 群的同构

- 证明： 1. 若 $O\langle a \rangle = \infty$ ，则 G 与 $(\mathbb{Z}, +)$ 同构
 - 对于 $O\langle a \rangle = \infty, \forall m, n \in \mathbb{Z}^+ (m \neq n)$ ，一定有 $a^m \neq a^n$
 - 否则若 $a^m = a^n$ ，就有 $a^{(m-n)} = e$
 - 无限循环群中，任何两个不等的元素幂次也不等
 - 构造群 G 到 \mathbb{Z} 的映射关系 $f: a^k \rightarrow k$
 - $\forall x \in G, x = a^k, f(x) = f(a^k) = k \in \mathbb{Z}$ 说明 f 为映射
 - $\forall a^m, a^n \in G (a^m \neq a^n) \quad m \neq n \quad f(a^m) \neq f(a^n)$
 - $\forall k \in \mathbb{Z}$ ，必定 $\exists a^k \in G$ ，使得 $f(a^k) = k$
 - 因此 f 是双射！



8.3 循环群 群的同构

定理8.3.4

- 证明（续）： 1. 若 $O\langle a \rangle = \infty$ ，则 G 与 $(\mathbb{Z}, +)$ 同构
 - 群 G 到 \mathbb{Z} 的映射关系 $f: a^k \rightarrow k$ 为双射
 - 考察 $\forall x, y \in G$, 其中 $x = a^m, y = a^n$
$$\begin{aligned} f(xy) &= f(a^m a^n) = f(a^{m+n}) = m + n \\ &= f(x) + f(y) \end{aligned}$$
 - 因此 f 是 G 到 \mathbb{Z} 的一个同构映射
 - $G \cong \mathbb{Z}$



2. 若 $O\langle a \rangle = n$, 则 G 与 $(Z_n, +)$ 同构

- 证明 由于 $G = O\langle a \rangle$, 故 G 中所有元素为 $e, a^1, a^2, \dots, a^{n-1}$
- Z_n 中所有元素为 $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$
- 易证, 映射 f 是从 G 到 Z_n 的双射!
- 群 G 到 Z_n 的映射关系 $f: a^k \rightarrow \overline{k} (0 \leq k < n)$
- 考察 $\forall x, y \in G$, 其中 $x = a^{m_1}, y = a^{m_2} (0 \leq m_1 \leq m_2 < n)$
- $f(xy) = f(a^{m_1} a^{m_2}) = f(a^{m_1+m_2}) = f(a^{(m_1+m_2) \bmod n}) = (m_1 + m_2) \bmod n = f(x) + f(y)$
- 因此, f 是 G 到 Z_n 的一个同构映射!
- $G \cong Z_n$ 证毕!



8.3 循环群 群的同构

定理8.3.4

- 设 G 是循环群, a 为生成元
- 1. 若 $O\langle a \rangle = \infty$, 则 G 与 $(\mathbb{Z}, +)$ 同构
- 2. 若 $O\langle a \rangle = n$, 则 G 与 $(\mathbb{Z}_n, +)$ 同构

任何两个阶相同的循环群同构!



8.3 循环群 群的同构

定理8.3.5

- 设 G 是一个群, $(G', *)$ 是一个代数系统, 如存在 G 到 G' 的双射 f , 且保持运算, 即 $\forall a, b \in G$, 有

$$f(ab) = f(a) * f(b)$$

则 G' 也是一个群。

依据同构映射, 可以做群的判定!



8.3 循环群 群的同构

- 小结：
 - 循环群的定义
 - 生成元相关定理、性质
 - 子群相关定理、性质
 - 群的同构概念
 - 循环群的同构性质
 - 利用同构做群的判定



第八章 群

8.1 半群

8.2 群、群的基本性质

8.3 循环群 群的同构

8.4 变换群和置换群 Cayley定理

8.5 陪集和群的陪集分解 Lagrange定理

8.6 正规子群与商群

8.7 群的同态、同态基本定理

8.8 群的直积

三维空间中有多少种正多面体



- 我们的证明方式是利用欧拉公式:

$$v + f - e = 2$$

- 假设每个面的边数为 n , 每个顶点发射的边数为 m :

$$\frac{vm}{2} = \frac{fn}{2} = e$$

- 因此带入 $v=2e/m$ 以及 $f=2e/n$, 我们有:

$$\frac{1}{n} + \frac{1}{m} = \frac{1}{2} + \frac{1}{e} > \frac{1}{2}$$

- 其中 $m, n > 2$, 且为正整数

三维空间中有多少种正多面体

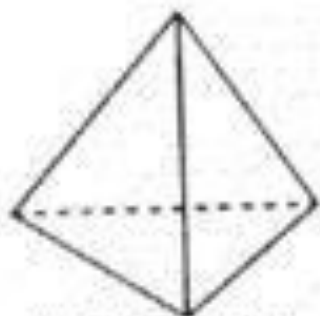


$$\frac{1}{n} + \frac{1}{m} = \frac{1}{2} + \frac{1}{e} > \frac{1}{2}$$

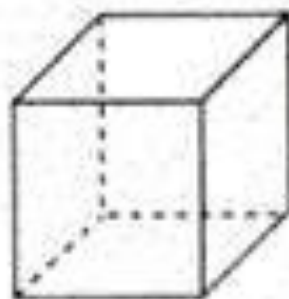
- 该方程解有限: $(3, 3), (3, 4), (4, 3), (3, 5), (5, 3)$
- 因此只有五种正多面体
- 在本节课中, 我们将会学到正多面体的旋转群都是三维旋转群 $SO(3)$ 的子群
- $SO(3)$ 是将三维物体绕一定旋转轴旋转一定角度的变换组成的变换群



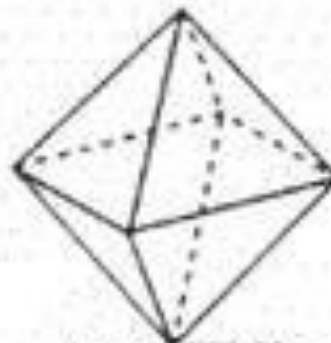
正多面体



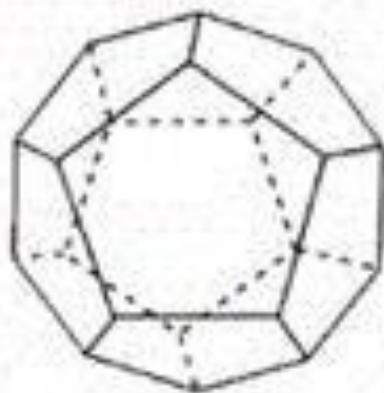
正四面体



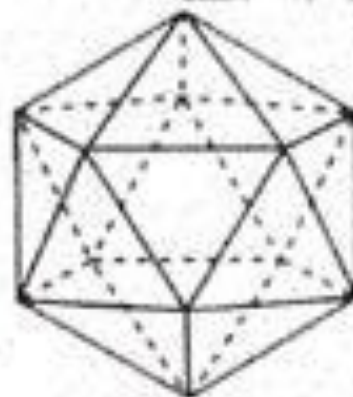
正六面体



正八面体



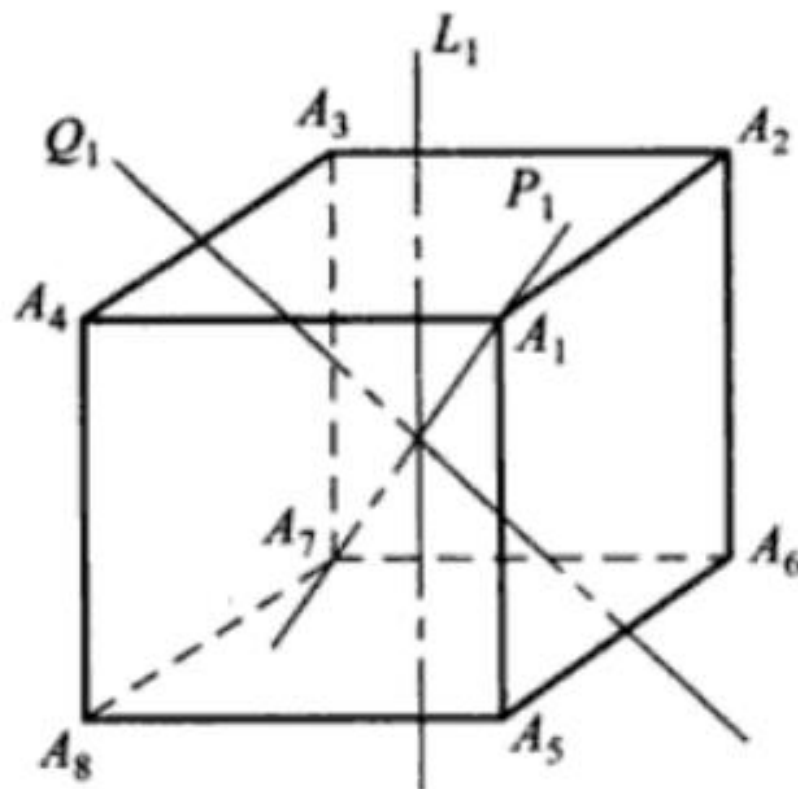
正十二面体



正二十面体



旋转



8.4 变换群和置换群 Cayley定理



定义8.4.0

- 设 $A = \{a_1, a_2, \dots\}$ 是一个非空集合, A 到 A 的一个映射 f 称为 A 的一个变换, 记做

$$f: \begin{bmatrix} a_1 & a_2 & \cdots \\ f(a_1) & f(a_2) & \cdots \end{bmatrix}$$

- 其中, 恒等变换记为 I

8.4 变换群和置换群 Cayley定理



- 思考：

变换有什么特点？

- 定义域和值域为同一个集合
- 如果变换是满射，则一定是单射吗？是双射吗？

有限集合上的变换，如果变换是满射，则一定是单射，也是是双射；无限集合上则不一定

8.4 变换群和置换群 Cayley定理



- 记集合 A 上全部变换的集合为 $M(A)$
 - 若 $|A| = n$, 则 $|M(A)| = n^n$
- 如果变换是双射的话, 我们称之为**一一变换**。

8.4 变换群和置换群 Cayley定理



- 对于 A 中的两个变换 f, g ，定义 A 的另一个变换 gf 为：

$$gf(a) = g(f(a)) \quad \forall a \in A$$

- 称为变换 f 与 g 的乘积（或乘法运算）
- 对于代数系统 $(M(A), \cdot)$ ：
 - 变换乘法运算符符合结合律
 - $fI = If = f$

8.4 变换群和置换群 Cayley定理



定义8.4.1

- 非空集合 A 的**所有**一一变换关于变换的乘法所作成的群叫做 A 的**一一变换群**，用 $E(A)$ 表示， $E(A)$ 的**子群**叫做**变换群**

8.4 变换群和置换群 Cayley定理



- 当集合 A 为有限集合时，即 $|A| = n$ 时， A 中的一个一一变换称为一个 n 元置换，由置换构成的群称为置换群。

- 思考：

置换群与变换群的区别？

变换群 一个集合 A 的一一变换所组成的群

置换群 一个有限集合 A 的一一变换所组成的群

8.4 变换群和置换群 Cayley定理



- 对于 n 元置换，可表示为：

$$\sigma: \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

- 显然， $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 就是 $1 \sim n$ 的一个排列。
- 反之， $1 \sim n$ 的一个排列，唯一对应一个 n 元置换，则共有 $n!$ 个 n 元置换。
- 用 S_n 表示这 $n!$ 个 n 元置换的集合



8.4 变换群和置换群 Cayley定理

- 例

- $A = \{1, 2, 3\}$, 则 $S_3 = \{\sigma_1, \sigma_2, \dots, \sigma_6\}$, 其中

$$\begin{aligned}\sigma_1 &= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \sigma_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \\ \sigma_4 &= \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \sigma_5 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \sigma_6 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix},\end{aligned}$$

- 计算置换乘法 $\sigma_2\sigma_4: i \rightarrow \sigma_2(\sigma_4(i))$

- $\sigma_2(\sigma_4(1)) = \sigma_2(2) = 3, \dots$

$$\sigma_2\sigma_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

8.4 变换群和置换群 Cayley定理



定义8.4.2

- S_n 对于置换乘法构成群，称为 n 次对称群。
- S_n 的子群称为 n 元置换群。

8.4 变换群和置换群 Cayley定理



- 对于一个置换 σ ，如果满足
$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_l) = i_1$$
- 则称 (i_1, i_2, \dots, i_l) 是一个长度为 l 的**轮换**
- 当 $l = 1$ 时，称为**恒等置换**
- 当 $l = 2$ 时，称为**对换**

8.4 变换群和置换群 Cayley定理



• 例：

– 置换

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

$$\sigma(1) = 3$$

$$\sigma(3) = 2$$

$$\sigma(2) = 4$$

$$\sigma(4) = 1$$

– 因此，该置换可写为轮换的形式：(1,3,2,4)

(3,2,4,1) (2,4,1,3) (4,1,3,2)



8.4 变换群和置换群 Cayley定理

• 例：

– 置换 $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 7 & 6 & 5 & 2 & 3 \end{bmatrix}$

$$\begin{array}{ll} \left\{ \begin{array}{l} \sigma(1)=4 \\ \sigma(4)=6 \\ \sigma(6)=2 \\ \sigma(2)=1 \end{array} \right. \Rightarrow (4,6,2,1) & \left\{ \begin{array}{l} \sigma(3)=7 \\ \sigma(7)=3 \end{array} \right. \Rightarrow (7,3) \\ & [\sigma(5)=5] \Rightarrow (5) \end{array}$$

- 因此，该置换可写为：(4,6,2,1)(7,3)(5)
- 通常，恒等置换不写入置换的表达式中

$$(4,6,2,1)(7,3)$$

8.4 变换群和置换群 Cayley定理



定义8.4.3

- 设 α, β 是 S_n 中的两个轮换，如果 α 和 β 中的元素都不相同，则称 α 和 β 是**不相交的**。

定理8.4.1

- 设 α, β 是两个不相交的轮换，则 $\alpha\beta = \beta\alpha$ 。

8.4 变换群和置换群 Cayley定理



例

- $\alpha = (1\ 3\ 6), \beta = (2\ 5)$, 不相交
- 对于 $\beta(i) = i, \alpha\beta(i) = \alpha(i), \beta\alpha(i) = \alpha(i)$
- 对于 $\alpha(i) = i, \alpha\beta(i) = \beta(i), \beta\alpha(i) = \beta(i)$
- 对任意 $i, \alpha\beta(i) = \beta\alpha(i), \alpha\beta = \beta\alpha$

8.4 变换群和置换群 Cayley定理



- 思考：

置换群和轮换的关系？

- 轮换是某种特定形式的置换。
- 轮换的乘积，仍然是置换。
- 置换是否一定是轮换的乘积？
如果是，有多少种表现形式？

8.4 变换群和置换群 Cayley定理



定理8.4.2

- S_n 中任意一个 n 元置换，一定可以表示成不相交轮换的乘积的形式，并且表示法是唯一的。即：

$$\forall \sigma \in S_n, \sigma = \sigma_1 \sigma_2 \cdots \sigma_t$$

- 假如 $\sigma = \sigma_1 \sigma_2 \cdots \sigma_t = \tau_1 \tau_2 \cdots \tau_l$
- 则有 $\{\sigma_1, \sigma_2, \cdots, \sigma_t\} = \{\tau_1, \tau_2 \cdots \tau_l\}$
- 事实上，一个置换如果写为可相交的轮换的乘积，表达式将是无穷多个

8.4 变换群和置换群 Cayley定理



例

- S_4 的全部置换可用轮换及其乘积表示为:
- 1. 都不变: $e = (i)$
- 2. 两个元素变: $(1\ 2), (3\ 4), (1\ 3), (2\ 4), (1\ 4), (2\ 3)$
- 3. 三个元素变: $(1\ 2\ 3), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 3),$
 $(1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3)$
- 4. 四个元素变: $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4),$
 $(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$
- 5. 四个元素变: $(12)(34), (13)(24), (14)(23)$

8.4 变换群和置换群 Cayley定理



引理8.4.1

- 设 $\sigma = (i_1, i_2, \dots, i_k)$ 是 S_n 上的 k 阶轮换, $k > 1$, 则

$$\sigma = (i_2 \ i_3)(i_3 \ i_4) \cdots (i_{k-1} \ i_k) (i_1 \ i_k)$$

$$\sigma = (i_1 \ i_k)(i_1 \ i_{k-1}) \cdots (i_1 \ i_3) (i_1 \ i_2)$$

- 比如, 任意一个轮换 σ , 都可以表示为对换的乘积, 且可以无穷多个。例如:

$$\sigma = (1 \ 2 \ 3 \ 4) = (2 \ 3)(3 \ 4)(4 \ 1) = (1 \ 4)(1 \ 3)(1 \ 2)$$

8.4 变换群和置换群 Cayley定理



- 对于一个 n 元置换：
 - 表示成不相交轮换的乘积时，表示法是最唯一的
 - 表示为对换乘积时，表示法并不唯一
 - 对换的个数也不是确定的
- 问题：
 - 一个置换表示为对换乘积时，确定的是什么？

8.4 变换群和置换群 Cayley定理



定义8.4.4

- 设 $i_1 i_2 \cdots i_n$ 是 $1, 2, \dots, n$ 的一个排列, 若 $i_k > i_l$ 且 $k < l$, 则称 $i_k i_l$ 是一个**逆序**
- 排列中逆序的总数称为这个排列的**逆序数**
- 例如: 25431的逆序数?
 - 21, 54, 53, 51, 43, 41, 31共7个
 - 25431的逆序数为7

8.4 变换群和置换群 Cayley定理



引理8.4.2

- 设 $\sigma \in S_n$ 且 $\sigma(j) = i_j, j = 1, 2, \dots, n$, 则在 σ 的对换表示中, 对换个数的奇偶性与排列 $\pi = i_1 i_2 \cdots i_n$ 的逆序数奇偶性相同, 记为 $N(\sigma)$
- 如果 $N(\sigma)$ 为奇数, 则称 σ 为奇置换, 否则称之为偶置换。



下面描述正确的

- ☒ A 任意两个偶置换的乘积仍然是偶置换
- ☒ B 任意两个奇置换的乘积是偶置换
- ☐ C 任意两个奇置换的乘积是奇置换
- ☒ D 一个奇置换和一个偶置换的乘积是奇置换

8.4 变换群和置换群 Cayley定理



定理8.4.3

- n 次对称群 S_n 中所有偶置换的集合，对于 S_n 中的置换乘法构成子群，记为 A_n ，称为交错群，若 $n \geq 2$ ，则 $|A_n| = \frac{1}{2}n!$

8.4 变换群和置换群 Cayley定理



定理8.4.3

- 证明:

- S_n 是有限群, 任意两个偶置换的乘积仍然是偶置换
- 由定理8.2.7得 S_n 中所有偶置换构成 S_n 的一个子群
- 偶置换数 n_1 , 奇置换数 n_2
- 某奇置换去乘不同偶置换, 得到互异奇置换, $n_1 \leq n_2$
- 某奇置换去乘不同奇置换, 得到互异偶置换, $n_1 \geq n_2$
- $n_1 = n_2, A_n = \frac{1}{2}n!$

定理8.2.7: G 的非空子集 H 是 G 的子群的充要条件是

$\forall a, b \in H$, 都有 $ab^{-1} \in H$



8.4 变换群和置换群 Cayley定理

定理8.4.4 (Cayley定理)

- 任意群 G 与一个变换群同构。
- 证明：首先构造一个变换群：
 - 任取 $a \in G$ 定义 G 上的一个变换 $f_a: x \rightarrow ax, \forall x \in G$
 - 定义 $\bar{G} = \{f_a | a \in G\}$ ，想办法证明其为变换群
 - 再想办法证明 $(G, \cdot) \cong (\bar{G}, \circ)$ —— 变换？

非空集合 A 的所有一一变换关于变换的乘法所作成的群叫做 A 的一一变换群，用 $E(A)$ 表示， $E(A)$ 的子群叫做变换群



8.4 变换群和置换群 Cayley定理

定理8.4.4 (Cayley定理)

- 证明 (续) : 证 $f_a: x \rightarrow ax$ 是双射

考察 $\forall b \in G$, 是否存在 $x \in G$, 使得 $f_a(x) = b$

实际上, 群 G 中方程 $ax = b$ 有唯一解

因此 f_a 是满射 (有解)、单射 (唯一解) $\longrightarrow f_a$ 是双射。

– 以下证明 $\overline{G} = \{f_a | a \in G\}$ 关于变换乘法成群



8.4 变换群和置换群 Cayley定理

定理8.4.4 (Cayley定理)

• 证明 (续) : 证 $\overline{G} = \{f_a | a \in G\}$ 关于变换乘法成群

– $\forall f_a, f_b \in \overline{G}, (f_a f_b)(x) = f_a(f_b(x)) = f_a(bx) = abx = f_{ab}(x)$

封闭性

– $\forall f_a, f_b \in \overline{G} \iff a, b \in G \implies ab \in G \implies f_{ab} \in \overline{G}$

结合律

– $f_e: x \rightarrow ex$, 是变换中的单位元

单位元

– 由于 f_a 是一一变换, 因此必定存在逆元素

逆元素

$$f_a^{-1}: x \rightarrow a^{-1}x \quad f_a^{-1} = f_{a^{-1}}$$

因此 \overline{G} 关于变换乘法成群, 即它是一个变换群!

8.4 变换群和置换群 Cayley定理



定理8.4.4 (Cayley定理)

• 证明（续）：证 G 和 \overline{G} 同构

– 构造映射关系 $\varphi: a \rightarrow f_a$

单射 – $\forall a, b, x \in G, a \neq b \Rightarrow ax \neq bx \Rightarrow f_a \neq f_b \Rightarrow \varphi(a) \neq \varphi(b)$

满射 – $\forall f_a \in \overline{G}$, 一定存在 $a \in G$, 使得 $\varphi(a) = f_a$

保持运算 – $\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\varphi(b)$

– 因此, $G \cong \overline{G}$

证毕!

8.4 变换群和置换群 Cayley定理



定理8.4.4 (Cayley定理) 任意群 G 与一个变换群同构

- 任何一个群 G ，都与一个变换群同构

推论：

- 设 G 是 n 阶有限群，则 G 与 S_n 的一个子群同构。
- 任何一个有限群 G ，都与一个置换群同构

S_n 表示这 $n!$ 个 n 元置换的集合

8.4 变换群和置换群 Cayley定理



- 小结：
 - 变换、一一变换
 - 一一变换群、变换群、对称群、置换群
 - 置换：轮换、对换、恒等变换
 - 逆序、逆序数、置换的逆序数性质
 - Cayley定理



第八章 群

8.1 半群

8.2 群、群的基本性质

8.3 循环群 群的同构

8.4 变换群和置换群 Cayley定理

8.5 陪集和群的陪集分解 Lagrange定理

8.6 正规子群与商群

8.7 群的同态、同态基本定理

8.8 群的直积



8.5 陪集和群的陪集分解 Lagrange定理

- 群内的子群反映了群的结构和性质，因此我们需要进一步研究有关群内子群的性质
- G 是一个群， H 是 G 的一个子群，利用 H 可以在 G 的元素之间确定一个二元关系 R

$$a R b \text{ 当且仅当 } ab^{-1} \in H$$

R 是 G 中的一个二元关系，是等价关系

因此由等价关系就可以确定 G 的一个划分，其划分块就是子群 H 的陪集



8.5 陪集和群的陪集分解 Lagrange定理

定义8.5.1

- 设 H 是群 G 的一个子群，对任意的 $a \in G$ ，集合

$$aH = \{ah | h \in H\}$$

- 称为子群 H 在 G 中的一个左陪集。同理， H 在 G 中的一个右陪集是

$$Ha = \{ha | h \in H\}$$

思考：左陪集和右陪集是否相等？



判断题：左陪集和右陪集是否相等

- ☐ A 相等
- ☐ B 不相等
- ☒ C 不一定
- ☐ D 不确定



实例

设 $G = S_3$, $H = \{e, (1\ 2)\}$, 取 a 为 e , $(1\ 3)$ 和 $(2\ 3)$ 时,

$$eH = H = \{e, (1\ 2)\},$$

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\},$$

$$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\},$$

$$He = H,$$

$$H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\},$$

$$H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\},$$

$$G = eH \cup (1\ 3)H \cup (2\ 3)H$$

显然一般情况下

$$aH \neq Ha$$



轮换计算的一个小技巧

$\forall i, j$, 当 $a_i \neq b_j$ 时

$$(a_1, \dots, a_n, c)(c, b_1, \dots, b_m) = (a_1, \dots, a_n, c, b_1, \dots, b_m)$$

• 例, 计算 $(132)(13)(24)$

$$\begin{aligned}(132)(13)(24) &= (213)(13)(24) = (21)(13)(13)(24) \\ &= (21)(24) = (12)(24) = (124)\end{aligned}$$



实例

$G = (\mathbb{Z}, +)$, $H = \{km \mid k \in \mathbb{Z}\}$, H 是 G 的子群, 因为 G 是交换群, H 的左、右陪集相等, 它们是

$$0+H = H+0 = \{km \mid k \in \mathbb{Z}\},$$

$$1+H = H+1 = \{1+km \mid k \in \mathbb{Z}\},$$

$$2+H = H+2 = \{2+km \mid k \in \mathbb{Z}\},$$

...

$$m-1+H = H+m-1 = \{m-1+km \mid k \in \mathbb{Z}\},$$

每个陪集正好与一个同余类对应



8.5 陪集和群的陪集分解 Lagrange定理

定理8.5.1

• 设 H 是 G 的子群，则 H 的左陪集具有下述性质

1. $H = eH, a \in aH$ 。

2. $|aH| = |H|$ 。

因 H 为 G 的子群，故消去律成立。则
 $\forall h_1, h_2 \in H$ ，若 $h_1 \neq h_2$ ，则 $\forall a \in G$ 必定有 $ah_1 \neq ah_2$ ，故 aH 中没有共同元素，故 $|aH| = |H|$

H 的任意一个左陪集，其元素个数与 H 相同

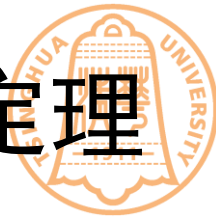
3. $a \in H \Leftrightarrow aH = H$ 。

\Rightarrow : 因为 $a \in H$ ，所以 $aH = \{ah | h \in H\} \subseteq H$

$\forall h \in H, h = (aa^{-1})h = a(a^{-1}h) \in aH$ 故 $H \subseteq aH$ ，故 $aH = H$

\Leftarrow : $a = ae \in aH = H$

子群中任意一个元素和子群自身作用，得到的左陪集仍为子群自身



8.5 陪集和群的陪集分解 Lagrange定理

4. $\forall x \in aH$, 都有 $xH = aH$, 并叫 a 是 aH 的一个陪集代表

- 证明: 左陪集中任意一个元素和子群 H 作用, 得到的左陪集不变

$\forall x \in aH$, 必定有 $x = ah_1$, 其中 $h_1 \in H$

$\forall xh \in xH$, 有 $xh = (ah_1)h = a(h_1h) = ah'$, 其中 $h' \in H$

因此 $ah' \in aH$ 即 $\forall xh \in xH$, 有 $xh \in aH$ 即 $xH \subseteq aH$

$\forall ah' \in aH, \because x = ah_1, \therefore a = xh_1^{-1}$

故 $ah' = (xh_1^{-1})h' = x(h_1^{-1}h') \in xH$ 即 $aH \subseteq xH$



8.5 陪集和群的陪集分解 Lagrange定理

$$\begin{aligned} 5. aH = bH &\Leftrightarrow a \in bH \text{ 或 } b \in aH \\ &\Leftrightarrow b^{-1}a \in H \text{ 或 } a^{-1}b \in H \end{aligned}$$

- 证明:

- 充分性: 由性质1可知, $a \in aH = bH$
- 故 $\exists h' \in H$, 使得 $a = bh'$ 即 $b^{-1}a = h' \in H$
- 必要性: 因 $b^{-1}a \in H$ 所以 $\exists h_1 \in H$ 使得 $b^{-1}a = h_1$
- 即 $a = bh_1$, 即 $a \in bH$ 。 由性质4, $bH = aH$
- 性质的另一半, 显然!

思考: 说明了什么?

左陪集中任意一个元素和子群 H 作用, 得到的左陪集不变



8.5 陪集和群的陪集分解 Lagrange定理

6. $\forall a, b \in G$, 若非 $aH = bH$, 必有 $aH \cap bH = \emptyset$

• 证明:

- 假如 $aH \cap bH \neq \emptyset$, 则必定 $\exists x \in aH \cap bH$
- 也就是 $x \in aH$, 同时 $x \in bH$
- 则根据性质4, 一定有 $xH = aH = bH$

同一子群的两个左陪集要么相等、要么交集为空!

思考: 该性质意味着什么?

$$G = \bigcup_{a \in G} aH$$

aH 是 G 的一个划分



8.5 陪集和群的陪集分解 Lagrange定理

定理8.5.1

• 设 H 是 G 的子群，则 H 的左陪集具有下述性质

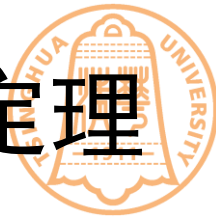
1. $H = eH, a \in aH$ 。 2. $|aH| = |H|$ 。 H的任意一个左陪集，其元素个数与H相同

3. $a \in H \Leftrightarrow aH = H$ 。 子群中任意一个元素和子群自身作用，得到的左陪集仍为子群自身

4. $\forall x \in aH$ ，都有 $xH = aH$ ，并叫 a 是 aH 的一个陪集代表 左陪集中任意一个元素和子群H作用，得到的左陪集不变

5. $aH = bH \Leftrightarrow a \in bH$ 或 $b \in aH$ 同一子群的两个左陪集要么相等、要么交集为空！
 $\Leftrightarrow b^{-1}a \in H$ 或 $a^{-1}b \in H$

6. $\forall a, b \in G$ ，若非 $aH = bH$ ，必有 $aH \cap bH = \emptyset$



8.5 陪集和群的陪集分解 Lagrange定理

定理8.5.2

- 设 G 是有限群, H 是 G 的子群, 则存在一个正整数 k , 满足

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

- 其中 $a_iH \cap a_jH = \emptyset, i \neq j, i, j = 1, 2, \dots, k$
- 思考:
 - 单位元 e 在哪个陪集中?



8.5 陪集和群的陪集分解 Lagrange定理

定义8.5.2

- 群 G 关于其子群 H 的左陪集的个数，称为 H 在 G 中的**指数**，记作 $[G:H]$ 。
- 观察 G 的子群 $H = \{e\}$:
 - H 的左陪集个数为 $|G|$
 - $[G:H] = [G:1] = |G|$



8.5 陪集和群的陪集分解 Lagrange定理

Lagrange定理

- 设 G 是有限群， H 是 G 的子群，则

$$[G:1] = [G:H][H:1]$$

$$G = a_1H \cup a_2H \cup \cdots \cup a_mH$$

$$|G| = m|H| = [G:H]|H|$$

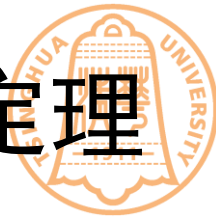
有限群中，子群的阶只能是群的阶的因子！



8.5 陪集和群的陪集分解 Lagrange定理

推论1

- 设有限群 G 的阶为 n ，则 G 中任意元素的阶都是 n 的因子，且适合 $x^n = e$ 。
- 证明：
 - $\forall a \in G$ ，可以得到 G 的循环子群 $H = \langle a \rangle$
 - 则根据Lagrange定理， $p|H| = |G| = n$
 - 又有 $a^{|H|} = e \implies a^n = a^{p|H|} = (a^{|H|})^p = e^p = e$



8.5 陪集和群的陪集分解 Lagrange定理

推论2

- 阶为素数 p 的群 G 是循环群。
- 证明：
 - 取 G 中一非单位元 a ，可以得到 G 的循环子群 $H = \langle a \rangle$
 - 根据推论1， a 的阶为 p 的因子，因此只能为 p ，所以 $O\langle a \rangle = p$
 - 所以 $G = \langle a \rangle$



8.5 陪集和群的陪集分解 Lagrange定理

推论3

- 设 A, B 是群 G 的两个有限子群, 则

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

其中 $AB = \{ab | a \in A, b \in B\} = \bigcup_{a \in A} aB$ 。



8.5 陪集和群的陪集分解 Lagrange定理

推论3

- 证明:

- 因为 B 是 G 的子群, 所以 aB 是 B 的左陪集
- 令 $S_1 = \{aB | a \in A\} = \{a_1B, a_2B, \dots, a_mB\}$, $D = A \cap B$
- 故 $A = \bigcup aD$, 令 $S_2 = \{aD | a \in A\} = \{a_1D, a_2D, \dots, a_mD\}$
- 构造 S_1 与 S_2 的一一映射关系 $\sigma: a_iB \rightarrow a_iD$
- $\forall a_i, a_j \in A$, 若 $a_iB = a_jB$, 必有 $a_i^{-1}a_j \in B$ (定理8.5.1)
- 且 $a_i^{-1}a_j \in A$, 故 $a_i^{-1}a_j \in A \cap B = D \iff a_iD = a_jD$
- 故 σ 是映射, 且是单射, 也是满射



8.5 陪集和群的陪集分解 Lagrange定理

推论3

- 证明（续）：

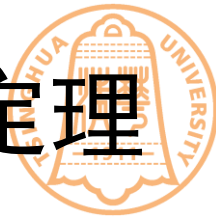
$$S_1 = \{a_1B, a_2B, \dots, a_mB\} \quad S_2 = \{a_1D, a_2D, \dots, a_mD\}$$

– $\sigma: a_iB \rightarrow a_iD$ 为双射。

– 显然 $|S_1| = |S_2| = k = [A:D] = |A|/|D|$

– 因此 $|AB| = |\bigcup_{a \in A} aB| = |S_1||B| = k|B|$,

– 两式合并，即得 $|AB| = \frac{|A||B|}{|A \cap B|}$ 证毕！



8.5 陪集和群的陪集分解 Lagrange定理

- 推论1 设有限群 G 的阶为 n ，则 G 中任意元素的阶都是 n 的因子，且适合 $x^n = e$ 。
- 推论2 阶为素数 p 的群 G 是循环群。
- 推论3 设 A, B 是群 G 的两个有限子群，则

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

利用Lagrange定理可以确定一个群内的可能存在的子群、元素的阶等，从而搞清一个群的结构
根据 $|G|$ 的因子来确定可能存在子群的阶数或元素的阶数

8.5 陪集和群的陪集分解 Lagrange定理



- 小结：
 - 左陪集
 - 左陪集6个性质
 - 群的陪集分解
 - Lagrange定理
 - 几个重要推论



第八章 群

8.1 半群

8.2 群、群的基本性质

8.3 循环群 群的同构

8.4 变换群和置换群 Cayley定理

8.5 陪集和群的陪集分解 Lagrange定理

8.6 正规子群与商群

8.7 群的同态、同态基本定理



8.6 正规子群与商群

- 如果存在群 G 的一个子群 H ，根据它的左陪集可以完成群的分解。
- 事实上，子群 H 的右陪集，也有对称的性质
- 但是，在许多情况下，群 G 的子群的左右陪集并不相等
- 思考：
 - 任意给定一个群 G ，它是否存在子群 H ，使得其左右陪集相等？
 - 子群 $\{e\}$ ，子群 G



8.6 正规子群与商群

定义8.6.1

- 设 H 是 G 的一个子群，如果对任意的 $a \in G$ ，都有 $aH = Ha$ ，则称 H 是 G 的一个正规子群（亦称不变子群），用符号 $H \triangleleft G$ 表示。
- 因此，对正规子群 H 就不必区分其左右陪集，而简称为 H 的陪集



8.6 正规子群与商群

定理8.6.1

• 设 H 是 G 的子群，则以下几个条件等价：

1. $H \triangleleft G$

2. $\forall g \in G, gHg^{-1} = H$

3. $\forall g \in G, gHg^{-1} \subseteq H$

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



8.6 正规子群与商群

证明：1. $H \triangleleft G \longrightarrow$ 2. $\forall g \in G, gHg^{-1} = H$

- 因为 H 为正规子群，因此 $\forall g \in G, gH = Hg$
- 因此

$$\begin{aligned} gHg^{-1} &= (gH)g^{-1} = (Hg)g^{-1} = \\ &H(gg^{-1}) = He = H \end{aligned}$$



8.6 正规子群与商群

证明: 2. $\forall g \in G, gHg^{-1} = H \implies$

$$3. \forall g \in G, gHg^{-1} \subseteq H$$

- $\forall g \in G, gHg^{-1} = H$



- $\forall g \in G, gHg^{-1} \subseteq H$



8.6 正规子群与商群

证明：3. $\forall g \in G, gHg^{-1} \subseteq H \implies$

$$4. \forall g \in G, h \in H, ghg^{-1} \in H$$

- $gHg^{-1} \subseteq H$



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



8.6 正规子群与商群

证明：4. $\forall g \in G, h \in H, ghg^{-1} \in H \longrightarrow 1. H \triangleleft G$

- 求证 $\forall g \in G, gH = Hg$
- 据已知条件, $\forall g \in G, \forall h \in H$, 都有 $ghg^{-1} = h_1 \in H$
- 即 $gh = h_1g \in Hg$ 。因此 $\forall g \in G, gH \subseteq Hg$
- 反之, 易证 $\forall g \in G, Hg \subseteq gH$
- 因此 $\forall g \in G, gH = Hg$



8.6 正规子群与商群

定理8.6.1

• 设 H 是 G 的子群，则以下几个条件等价：

1. $H \triangleleft G$

2. $\forall g \in G, gHg^{-1} = H$

3. $\forall g \in G, gHg^{-1} \subseteq H$

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



8.6 正规子群与商群

定理8.6.2

- 设 A, B 是 G 的两个子群
 1. 若 $A \triangleleft G, B \triangleleft G$, 则 $A \cap B \triangleleft G, AB \triangleleft G$
 2. 若 $A \triangleleft G, B \leq G$, 则 $A \cap B \triangleleft B, AB \leq G$



8.6 正规子群与商群

证明: 1. 若 $A \triangleleft G, B \triangleleft G$, 则 $A \cap B \triangleleft G, AB \triangleleft G$

- $\forall h \in A \cap B \implies h \in A, h \in B$
 - $\forall g \in G, ghg^{-1} \in A, ghg^{-1} \in B$
 - $\forall g \in G, \forall h \in A \cap B, ghg^{-1} \in A \cap B \implies A \cap B \triangleleft G$
 - 首先证明 AB 是 G 的子群
 - $\forall h \in AB \implies h = ab, a \in A, b \in B$
 - $\forall g \in G, ghg^{-1} = gabg^{-1} = gag^{-1}gbg^{-1} = a'b' \in AB$
 - $AB \triangleleft G$
4. $\forall g \in G, h \in H, ghg^{-1} \in H$



8.6 正规子群与商群

证明: 2. 若 $A \triangleleft G, B \leq G$, 则 $A \cap B \triangleleft B, AB \leq G$

- $\forall h \in A \cap B \longrightarrow h \in A, h \in B$
- $\forall g \in B \longrightarrow ghg^{-1} \in A$ ($A \triangleleft G$ 且 $B \leq G$, 性质4),
 $ghg^{-1} \in B$
- $\forall g \in B, \forall h \in A \cap B, ghg^{-1} \in A \cap B \longrightarrow A \cap B \triangleleft B$

$$4. \forall g \in G, h \in H, ghg^{-1} \in H$$



8.6 正规子群与商群

证明：2. 若 $A \triangleleft G, B \leq G$ ，则 $A \cap B \triangleleft B, AB \leq G$

- $e \in A, e \in B \Rightarrow e \in AB$ 单位元! 结合律!
- $\forall ab, a_1b_1 \in AB$
- $(ab)(a_1b_1) = a(ba_1)b_1 = a(a_1'b)b_1 = (aa_1')(bb_1) \in AB$ 封闭性!
- $\forall ab \in AB, (ab)^{-1} = b^{-1}a^{-1} = (a^{-1})'b^{-1} \in AB$ 逆元素!
- $AB \leq G$ 证毕!



8.6 正规子群与商群

定理8.6.2

• 设 A, B 是 G 的两个子群

1. 若 $A \triangleleft G, B \triangleleft G$, 则 $A \cap B \triangleleft G, AB \triangleleft G$

2. 若 $A \triangleleft G, B \leq G$, 则 $A \cap B \triangleleft B, AB \leq G$

正规子群的乘积仍然是正规子群！

正规子群的交集仍然是正规子群！

正规子群与普通子群的乘积是普通子群！

正规子群与普通子群的交集是普通子群的正规子群！



8.6 正规子群与商群

定理8.6.3

- 设 H 是 G 的一个正规子群， G/H 表示 H 的所有陪集构成的集合，即

$$G/H = \{gH | g \in G\}$$

- 则 G/H 关于陪集乘法作成群。称之为 G 关于 H 的商群



8.6 正规子群与商群

证明:

陪集乘法对于 G/H 是一个二元运算

- $\forall aH, bH \in G/H, aHbH = \{ah_1bh_2 | h_1, h_2 \in H\}$
- $bH = Hb \xrightarrow{\text{blue arrow}} ah_1bh_2 = a(h_1b)h_2 = a(bh_1')h_2 = (ab)(h_1'h_2) \in abH$
- 故 $aHbH \subseteq abH$
- 又 $\forall h \in H, (ab)h \in abH, (ab)h = (ae)(bh) \in aHbH$
- 故 $abH \subseteq aHbH$
- 因此 $\forall aH, bH \in G/H, aHbH = abH = G/H$

二元运算!

关于乘法是封闭的



8.6 正规子群与商群

证明（续）：

G/H 对陪集乘法成群

- $\forall aH, bH, cH \in G/H$ 结合律！
$$(aHbH)cH = (abH)cH = (ab)cH = a(bc)H$$
$$= aH(bc)H = aH(bHcH)$$
- $eHaH = eaH = aH, aHeH = aeH = aH \Rightarrow eH =$
 H 是单位元 单位元！
- $a^{-1}HaH = aHa^{-1}H = eH$, 因此 aH 的逆元为 $a^{-1}H$
逆元素！

证毕！



8.6 正规子群与商群

定理8.6.3

- 设 H 是 G 的一个正规子群, G/H 表示 H 的所有陪集构成的集合, 即

$$G/H = \{gH | g \in G\}$$

- 则 G/H 关于陪集乘法作成群。称之为 G 关于 H 的商群。



8.6 正规子群与商群

小结

- 正规子群
- 正规子群的等价性质
- 正规子群与子群的交、乘积性质
- 商群



谢谢

shixia@tsinghua.edu.cn



清華大學

Tsinghua University

第十五周 作业

刘世霞

shixia@tsinghua.edu.cn



Homework

《离散数学2》

- 习题八
 - 21
 - 27
 - 30
 - 33



教学组成员

教 师： 刘世霞 shixia@tsinghua.edu.cn

助 教： 袁隽 thss15_yuanj@163.com 18612600388

肖冬 xiaodong14ry@163.com 15201152906

所在单位：清华大学软件学院