



代数结构

Algebra Structures



内容提要

1. 运算及其性质
2. 代数系统
3. 群与子群
4. 阿贝尔群和循环群
5. 环与域
6. 格与布尔代数

内容提要

1. 运算及其性质
2. 代数系统
3. 群与子群
4. 阿贝尔群和循环群
5. 环与域
6. 格与布尔代数

4、阿贝尔群和循环群

概念：

阿贝尔群(交换群)，循环群, 生成元

阿贝尔 (Abel) 群

若群 G 中的运算是可交换的，则称 G 为交换群或阿贝尔群。

例：（1） $\langle \mathbb{Z}, + \rangle$ 和 $\langle \mathbb{R}, + \rangle$ ， $\langle \mathbb{Z}_n, \oplus \rangle$ 、Klein四元群均是阿贝尔群。

（2） n 阶($n \geq 2$)实可逆矩阵集合关于矩阵乘法构成的群 不是 阿贝尔群。

循环群 (Cyclic group)

设 G 是群, 若存在 $a \in G$ 使得

$$G = \{a^k \mid k \in \mathbb{Z}\}$$

则称 G 是循环群, 记作 $G = \langle a \rangle$, 称 a 为 G 的生成元.

循环群的分类

(1) n 阶循环群: 设 $G = \langle a \rangle$ 是循环群, a 是 n 阶元, 则

$$G = \{a^0=e, a^1, a^2, \dots, a^{n-1}\} \quad (\text{注意 } |G| = |a| = n)$$

(2) 无限循环群: a 是无限阶元, 则

$$G = \{a^0=e, a^{\pm 1}, a^{\pm 2}, \dots\}$$

循环群的生成元

设 $G=\langle a \rangle$ 是循环群。

- (1) 若 G 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1} 。
- (2) 若 G 是 n 阶循环群，则对于任何小于 n 且与 n 互质的数 $r \in \{0, 1, \dots, n-1\}$ ， a^r 是 G 的生成元。这样的 r 共有 $\phi(n)$ 个，因而 G 共有 $\phi(n)$ 个生成元。

证明（思路）：

- (1) 容易说明 a^{-1} 也是生成元。设 b 也是生成元。
则有 $a = b^t, b = a^m$, 因而 $a = b^t = (a^m)^t = a^{mt}$, 从而 $a^{mt-1} = e$
因为 G 是无限循环群，必有 $mt-1=0$ ，从而 $m=t=1$ 或 $m=t=-1$ 。
- (2) 利用以下性质： 若 r 与 n 互素，则存在整数 u, v , 满足 $ur + vn = 1$ 。

实例

- (1) 设 $G = \{e, a, \dots, a^{11}\}$ 是12阶循环群，小于12且与12互素的数是1, 5, 7, 11 ($\phi(12)=4$)。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，小于9且与9互素的数是 1, 2, 4, 5, 7, 8 ($\phi(9)=6$)。可知 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

设 $G=\langle a \rangle$ 是循环群。

- (1) 设 $G=\langle a \rangle$ 是循环群，则 G 的子群仍是循环群；
- (2) 若 $G=\langle a \rangle$ 是无限循环群，则 G 的子群除 $\{e\}$ 以外都是无限循环群；
- (3) 若 $G=\langle a \rangle$ 是 n 阶循环群，则对 n 的每个正因子 d ， G 恰好含有一个 d 阶子群。

实例

- (1) $G=\langle \mathbb{Z}, + \rangle$ 是无限循环群，其生成元为1和-1. 对于自然数 $m \in \mathbb{N}$ ，1的 m 次幂是 m ， m 生成的子群是 $m\mathbb{Z}$ ， $m \in \mathbb{N}$ 。即

$$\langle 0 \rangle = \{0\} = 0\mathbb{Z}$$

$$\langle m \rangle = \{mz \mid z \in \mathbb{Z}\} = m\mathbb{Z}, \quad m > 0$$

- (2) $G=\mathbb{Z}_{12}$ 是12阶循环群。12正因子是1,2,3,4,6和12， G 的子群:

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 $\langle 1 \rangle = \mathbb{Z}_{12}$