

# 第五部分 代数结构

## 第15章 半群与群

---

计算机（软件）学院

林 兰

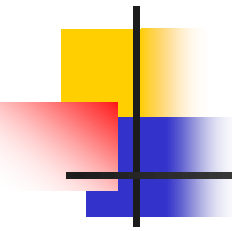
[linlan@scu.edu.cn](mailto:linlan@scu.edu.cn)



# 主要内容

---

- 15.1 半群
- 15.2 群和子群
- 15.3 交换群和循环群

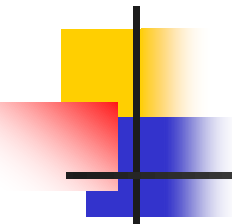


## 15.1 半群

---

### 1. 半群

**定义** 设 $\langle S, * \rangle$ 是一个二元代数（广群），若运算“\*”可结合，则称 $\langle S, * \rangle$ 为一个半群；进一步，若运算“\*”可交换，则称 $\langle S, * \rangle$ 为可换半群。



## 15.1 半群

### 2. 元素的方幂

**定义** 设 $\langle S, \cdot \rangle$ 是半群,  $a \in S$ ,  $n$ 是正整数, 约定:  $n$ 个 $a$ 在运算“ $\cdot$ ”下的结果表示为 $a^n$ 。可以递归定义如下:

①  $a^1 = a$

②  $a^{n+1} = a^n \cdot a$

✓ 幂运算有以下性质:

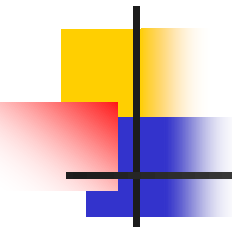
设 $\langle S, \cdot \rangle$ 是半群,  $a \in S$ ,  $m$ 和 $n$ 是正整数, 则

①  $a^m \cdot a^n = a^{m+n}$

②  $(a^m)^n = a^{mn}$

**说明:** 进一步, 当 $\langle S, \cdot \rangle$ 是含么半群或群时, 上述结论对任意非负整数 $m$ 和 $n$ 都成立, 有 $a^0 = e$ 。

当 $\langle S, \cdot \rangle$ 是群,  $a^{-n} = (a^{-1})^n$



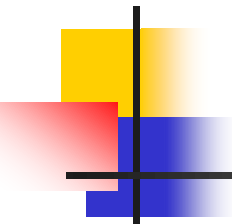
## 15.1 半群

证明 ①式：设 $m$ 为固定的任意正整数，对 $n$ 归纳证明  
当 $n=1$ 时，由前递归定义知， $a^m \cdot a = a^{m+1}$ ，结论成立。  
假设 $n=k$ 时，结论成立，即等式 $a^m \cdot a^k = a^{m+k}$ 成立。  
现证当 $n=k+1$ 时：

$$\begin{aligned} a^m \cdot a^{k+1} &= a^m \cdot (a^k \cdot a) && \text{(由定义)} \\ &= (a^m \cdot a^k) \cdot a && \text{(具有结合律)} \\ &= (a^{m+k}) \cdot a && \text{(归纳假设)} \\ &= a^{m+(k+1)} && \text{(由定义)} \end{aligned}$$

$\therefore$ 结论对任意 $n$ 成立。

②式的证明方法同①



## 15.1 半群

**定理** 设 $\langle S, * \rangle$ 是半群, 如果 $S$ 是有限集, 则必有 $a \in S$ , 使得  $a^2 = a$ 。

**证明:** 因为 $\langle S, * \rangle$ 是半群,  $S$ 是有限集,

对 $\forall b \in S$ , 则元素 $b^1, b^2, b^3, \dots$ 中必有重复的,

设 $b^i = b^j$ , 其中 $j > i$ 。

由 $b^i = b^{j-i} * b^i$ ,  $b^{i+1} = b^{j-i} * b^{i+1}$ ,  $\dots b^{i+x} = b^{j-i} * b^{i+x}$  ( $x \geq 0$ )

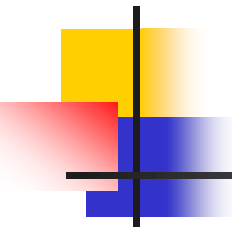
令 $t = i + x$ , 则 $t \geq i$ 的任意正整数, 得到  $b^t = b^{j-i} * b^t$ ,

利用上式反复迭代, 则对任何正整数 $k \geq 1$ , 有

$$b^t = b^{k(j-i)} * b^t, \quad (t \geq i)$$

特别, 取 $k$ 使得 $k(j-i) \geq i$ , 同时令 $t = k(j-i)$ , 则得到幂等元。

✓ 这是一种构造性的证明方法。



## 15.1 半群

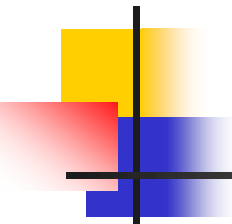
### 3. 子半群

① 如果 $\langle S, * \rangle$ 是半群， $T$ 是 $S$ 的非空子集，且 $T$ 对运算 $*$ 是封闭的，则称 $\langle T, * \rangle$ 是半群 $\langle S, * \rangle$ 的子半群；

（同一般代数系统，仅验证 $T$ 的非空性和“ $*$ ”关于 $T$ 的封闭性，结合律自然继承。）

② 如果 $\langle S, *, e \rangle$ 是含幺半群， $T$ 是 $S$ 的非空子集，且 $e \in T$ ， $T$ 对运算 $*$ 是封闭的，则称 $\langle T, *, e \rangle$ 是含幺半群 $\langle S, *, e \rangle$ 的含幺子半群。

例如 半群 $\langle \mathbb{R}, \times \rangle$ 的子代数 $\langle [0, 1], \times \rangle$ ， $\langle \mathbb{Z}, \times \rangle$ ， $\langle \mathbb{R}^+, \times \rangle$ 都是 $\langle \mathbb{R}, \times \rangle$ 的子半群。



## 15.1 半群

**例1** 设 $\langle S, * \rangle$ 是一个可换的含幺半群， $M$ 是它的所有幂等元构成的集合，则 $\langle M, * \rangle$ 是 $\langle S, * \rangle$ 的一个含幺子半群。

**证明：**(1) 显然， $M \subseteq S$ ；

$\langle S, * \rangle$ 是含幺半群，所以幺元 $e$ 存在，又 $e * e = e$ ，则 $e$ 是一个幂等元，即有 $e \in M$ ，所以 $M$ 是非空的；

(2)  $e \in M$ ，幺元；

(3) 对任意 $a, b \in M$ ，有

$$\begin{aligned} (a * b) * (a * b) &= a * (b * a) * b = a * (a * b) * b \\ &= (a * a) * (b * b) = a * b, \end{aligned}$$

即运算“ $*$ ”关于集合 $M$ 是封闭的运算。

由(1)、(2)、(3)知： $\langle M, * \rangle$ 是 $\langle S, * \rangle$ 的一个含幺子半群。





作业

---

✓ 习题十五

4



# 主要内容

---

- 15.1 半群
- 15.2 群和子群
- 15.3 交换群和循环群



## 15.2 群和子群

### 1. 群

设 $\langle G, * \rangle$ 是一个二元代数，且满足：

- ① 运算 $*$ 在 $G$ 上满足结合律；
- ② 在 $G$ 上关于运算“ $*$ ”的幺元存在；
- ③ 对 $\forall a \in G$ ，有 $a^{-1} \in G$ 存在。

则称 $\langle G, * \rangle$ 是一个群。

进一步，若运算“ $*$ ”又满足交换律，则称此群为交换群（Abel群）。群中元素的数目 $|G|$ 称为群的阶。若 $|G|$ 有限，则称为有限群；若 $|G|$ 无限，则称为无限群。



## 15.2 群和子群

---

例如  $\langle \mathbf{Z}, + \rangle$  , 整数加群

$\langle \mathbf{R}, + \rangle$  , 实数加群

$\langle \mathbf{Z}, \times \rangle$  , 含么半群, 不是群 (一般无乘法逆元)

$\langle \mathbf{R}, \times \rangle$  , 含么半群, 不是群 ( “0” 无逆元)

$\langle \mathbf{R} - \{0\}, \times \rangle$  , 实数乘群



## 15.2 群和子群

例2 设 $Z_k$ 表示整数集 $Z$ 上的模 $k$ 剩余类集合，即

$$Z_k = \{[0], [1], [2], \dots, [k-1]\}$$

在 $Z_k$ 上定义运算 $\oplus$ 和 $\otimes$ 如下：

$$[i] \oplus [j] = [t] \Leftrightarrow (i+j) \equiv t \pmod{k}$$

$$[i] \otimes [j] = [t] \Leftrightarrow ij \equiv t \pmod{k}$$

➤  $\langle Z_k, \oplus \rangle$ 是群（剩余类加群）。

$[0]$ 是 $\oplus$ 的幺元，每元 $[i]$ 的 $\oplus$ 逆元是 $[k-i]$ 。

➤  $\langle Z_k, \otimes \rangle$ 不是群，因为虽然它满足封闭性和可结合性，且 $[1]$ 是它的幺元，但是 $[0]$ 无 $\otimes$ 逆元，所以它仅仅是一个含幺半群。

## 15.2 群和子群

➤  $\langle \mathbb{Z}_k - \{[0]\}, \otimes \rangle$  是不是群呢？ 不一定！

例如：  $\mathbb{Z}_4 - \{[0]\} = \{[1], [2], [3]\}$ ，

而  $[2] \otimes [2] = [0] \notin \mathbb{Z}_4 - \{[0]\}$

$\therefore \langle \mathbb{Z}_4 - \{[0]\}, \otimes \rangle$  不是群。

而  $\mathbb{Z}_5 - \{[0]\} = \{[1], [2], [3], [4]\}$

其运算表如右图，

运算是封闭的，可结合的；

$[1]$  是幺元， $[1]$ 、 $[4]$  的逆元是自身， $[2]$ 、 $[3]$  互为逆元；

因此  $\langle \mathbb{Z}_5 - \{[0]\}, \otimes \rangle$  是群。

可以证明：当  $k$  是素数时，  
 $\langle \mathbb{Z}_k - \{[0]\}, \otimes \rangle$  一定是群。

| $\otimes$ | [1] | [2] | [3] | [4] |
|-----------|-----|-----|-----|-----|
| [1]       | [1] | [2] | [3] | [4] |
| [2]       | [2] | [4] | [1] | [3] |
| [3]       | [3] | [1] | [4] | [2] |
| [4]       | [4] | [3] | [2] | [1] |

## 15.2 群和子群

该定理是群的另一  
种等价定义形式。

**定理** 如果 $\langle G, * \rangle$ 是半群, 并且对 $\forall a, b \in G$ , 都存在 $x, y \in G$  使 $x*a=b, a*y=b$ , 则 $\langle G, * \rangle$ 是群。

**证明:** 设  $a \in G$ , 方程  $x*a=a$  的解为 $e_1$ ,  
对 $\forall t \in G$ , 方程  $a*y=t$  有解 $y_0$ ,  $\left. \vphantom{\begin{matrix} \text{设 } a \in G, \text{ 方程 } x*a=a \text{ 的解为 } e_1, \\ \text{对 } \forall t \in G, \text{ 方程 } a*y=t \text{ 有解 } y_0, \end{matrix}} \right\} \Rightarrow$

$$e_1*t = e_1*(a*y_0) = (e_1*a)*y_0 = a*y_0 = t$$

即对 $\forall t \in G$ , 必有 $e_1*t=t$ ,  $e_1$ 是 $G$ 中的左幺元。

也可以证明 $G$ 中有右幺元 $e_2$ , 所以 $G$ 中有幺元 $e=e_1=e_2$ 。

同理, 对 $\forall b \in G$ , 方程 $x*b=e$ 有解 $x_0$ , 则 $x_0$ 是 $b$ 的左逆元,  
方程 $b*y=e$ 的解是 $b$ 的右逆元, 且左右逆元相等, 从而 $b$ 有逆元。

此定理说明: 在群的定义中幺元及逆元的条件可用方程有解来代替。  
另外, 群的定义中的幺元条件可用存在左幺元 (右幺元) 的条件代替, 逆元的条件可用存在左逆元 (右逆元) 的条件代替。



## 15.2 群和子群

---

### ✓ 几条结论

- 1)  $G$  为群，则  $G$  中每个元素都是可消去元，即如果  $a*b=a*c$ ，或  $b*a=c*a$ ，则必有  $b=c$ 。（消去律成立）
- 2) 群  $G$  中除幺元  $e$  外无其它幂等元；
- 3) 阶大于1的群无零元；
- 4) 群  $G$  的运算表中任意一行（列）都没有两个相同的元素（重复元素）；





## 15.2 群和子群

证明:

- (1) 由于群 $G$ 中每个元素都有逆元 $a^{-1}$ ,  
由 $a*b=a*c \Rightarrow a^{-1}*a*b=a^{-1}*a*c$ , 即 $b=c$ .  
( $a$ 为 $G$ 上关于运算“ $*$ ”的左可消去元)  
同理, 可证右可消去元.
- (2) (反证法) 假设 $a$ 是群 $G$ 中非幺元的幂等元, 即 $a*a=a$ , 且  
 $a \neq e$ . 因此 $a*a=a*e$ ,  
由消去律知 $a=e$ , 矛盾.
- (4) (反证法) 假设群 $G$ 的运算表中某一行有两个相同的元素, 设为 $a$ , 并设它们所在的行表头元素为 $b$ , 列表头元素分别为 $c_1, c_2$ , 这时显然有 $c_1 \neq c_2$ . 而 $a=bc_1=bc_2$ ,  
由消去律得 $c_1=c_2$ , 矛盾。(同理可证, 任意一列都没有两个相同的元素)



## 15.2 群和子群

### 2. 群中元素的方幂

**定义** 设 $\langle G, \cdot \rangle$ 是群,  $a \in G$ ,  $n \in \mathbb{Z}$ , 则 $a$ 的 $n$ 次幂定义如下:

$$a^0 = e;$$

$$a^n = a^{n-1} \cdot a;$$

$$a^{-m} = (a^{-1})^m = (a^m)^{-1}。$$

**例如** 求 $\langle \mathbb{Z}, + \rangle$  中有 $3^{-5}$ :

$$3^{-5} = (3^{-1})^5 = (-3)^5$$

$$= (-3) + (-3) + (-3) + (-3) + (-3) = -15$$



## 15.2 群和子群

**定理** 设 $\langle G, \cdot \rangle$ 是群,  $\forall a, b \in G, m, n \in \mathbb{Z}$ ,  $G$ 中的幂运算满足:

①  $(a^{-1})^{-1} = a$

②  $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

③  $a^m \cdot a^n = a^{m+n}$

④  $(a^m)^n = a^{mn}$

⑤ 若 $G$ 为交换群 (Abel群), 则 $(a \cdot b)^n = (a)^n \cdot (b)^n$



## 15.2 群和子群

### 3. 元素的周期

设 $\langle G, \cdot \rangle$ 是一个群, 对 $\forall a \in G$ , 若有 $a^n = e$ , (其中:  
 $n \in \mathbb{Z}^+$ , 且 $n$ 是使得 $a^n=e$ 成立的最小的正整数), 则称 $n$ 为元素 $a$ 的周期或为元素 $a$ 的阶数; 记作 $|a| = n$ , 也称 $a$ 为 $n$ 阶元。若对 $a \in G$ , 不存在这样的 $n$ , 则称元素 $a$ 的周期为 $\infty$ 。

例如: 在剩余类加群 $\langle \mathbb{Z}_6, \oplus \rangle$ 中, 元素的周期分别为多少?

元素 $[1]$ 、 $[5]$ 的周期是6;

元素 $[2]$ 、 $[4]$ 的周期是3;

元素 $[3]$ 的周期是2; 元素 $[0]$ 的周期是1。



## 15.2 群和子群

---

### 定理

设 $\langle G, * \rangle$ 是一个群, 对 $\forall a \in G$ , 若 $a$ 的周期为 $n$ , 则

- ①  $a^m = e$  当且仅当  $n \mid m$ ;
- ②  $a^i = a^j$  当且仅当  $n \mid (i - j)$ ;
- ③  $a^0, a^1, a^2, \dots, a^{n-1}$  互不相同。



## 15.2 群和子群

证明：① “ $\Rightarrow$ ” (反证法) 设  $a^m=e$ 。

若  $n \nmid m$  不成立，则  $\exists q \in \mathbb{Z}$ ，使得

$$m=nq+r \ (1 \leq r \leq n-1),$$

由  $a$  的周期为  $n$ ，且  $a^m=e$ ，有：

$$a^m=a^{nq+r}=a^{nq} * a^r=(a^n)^q * a^r=e^q * a^r=a^r=e$$

由于  $1 \leq r \leq n-1$ ，这就与  $a$  的周期为  $n$  矛盾，

所以有  $n \mid m$ 。

“ $\Leftarrow$ ” 设  $n \mid m$ 。

则  $\exists k \in \mathbb{Z}$ ，使得  $m=nk$ ，于是有：

$$a^m=a^{nk}=(a^n)^k=e^k=e$$

所以有  $a^m=e$ 。证毕。



## 15.2 群和子群

### 4. 子群

**定义** 设 $\langle G, * \rangle$ 是一个群， $e$ 是 $G$ 中的幺元， $S$ 是 $G$ 的一个非空子集，若 $S$ 对运算“ $*$ ”也构成群，则称 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群。

例如：  $\langle \mathbf{Z}, + \rangle$  是  $\langle \mathbf{Q}, + \rangle$  的子群；  
 $\langle \mathbf{Q}, + \rangle$  是  $\langle \mathbf{R}, + \rangle$  的子群。

群 $\langle G, * \rangle$ ，至少有两个子群 $\langle \{e\}, * \rangle$ ， $\langle G, * \rangle$ ，此两个子群称为平凡子群；若有子群 $\langle S, * \rangle$ 且 $S \subset G$ 和 $S \neq \{e\}$ ，则称 $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的非平凡真子群。



## 15.2 群和子群

**定理（子群的性质）** 设 $\langle G, * \rangle$ 是一个群,  $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群, 则:

- 1) 子群 $\langle S, * \rangle$ 的幺元 $e_S$ 也是群 $\langle G, * \rangle$ 的幺元 $e_G$ ;
- 2) 对 $\forall a \in S$ ,  $a$ 在 $S$ 中的逆元 $a_S^{-1}$ 就是 $a$ 在 $G$ 中的逆元 $a_G^{-1}$ 。

**证明:** 1) 对 $\forall a \in S$ , 由于 $e_S$ 是 $S$ 的幺元,

$$\text{所以有: } e_S * a = a * e_S = a \quad \text{①}$$

又 $S \subseteq G$ , 所以 $a \in G$ , 由 $e_G$ 是 $G$ 的幺元, 所以有:

$$e_G * a = a * e_G = a \quad \text{②}$$

由①、②有:  $e_S * a = a * e_S = a = e_G * a = a * e_G$ ,

由于 $G$ 满足消去律, 所以有:  $e_S = e_G$ 。

2) 对 $\forall a \in S$ , 由于 $S \subseteq G$ , 所以 $a \in G$ , 即 $a$ 在 $S$ 中的逆元就是 $a$ 在 $G$ 中的逆元。





## 15.2 群和子群

### 定理（子群判定定理）

设 $\langle G, * \rangle$ 是一个群， $S$ 是 $G$ 的一个非空子集，则 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群的充要条件是：

对 $\forall a, b \in S$ ，有 $a * b^{-1} \in S$ 。

**证明 “ $\Rightarrow$ ”** 设 $S$ 是 $G$ 的子群，对 $\forall a, b \in S$ ，由群的定义知， $b^{-1} \in S$ ，即有 $a * b^{-1} \in S$ 。所以必要性成立；

**“ $\Leftarrow$ ”** 由子群的定义知，需证明如下四点：

1)  $S$ 是非空的子集；

2) **么元存在**：由于 $S \neq \emptyset$ ，对 $\forall a, b \in S$ ，有 $a * b^{-1} \in S$ ，取 $a = b$ ，有 $e = b * b^{-1} \in S$ ， $S$ 有么元；



## 15.2 群和子群

- 3) 逆元存在：对 $\forall a, b \in S$ ，有 $a * b^{-1} \in S$ ，  
对 $\forall b \in S$ ，由 $e \in S$ ，取 $a = e$ ，有 $e * b^{-1} = b^{-1} \in S$ ；
- 4) 封闭性：对 $\forall a, b \in S$ ，由3)知： $b^{-1} \in S$ ，  
由条件知： $a * (b^{-1})^{-1} \in S$ ，即 $a * b \in S$ 。  
由1)、2)、3)、4)知： $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群。

推论：设 $\langle G, * \rangle$ 是一个群， $S$ 是 $G$ 的非空有限子集，则  
 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群当且仅当对 $\forall a, b \in S$ ，有 $a * b \in S$ 。  
(即只需判断在 $S$ 中运算是否封闭即可)

## 15.2 群和子群

例4 设 $\langle G, * \rangle$ 是一个群，令：

$$C = \{a \mid a \in G \text{ 且对 } \forall x \in G, \text{ 有: } a*x = x*a\}$$

证明 $\langle C, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群。（称为 $G$ 的中心）

证明：（下面利用子群判定定理证明）

1) 对 $\forall x \in G$ ，有 $e*x = x*e = x$ ，即 $e \in C$ ，所以 $C$ 是非空的；

2) 设 $\forall a, b \in C$ ，为证明 $a*b^{-1} \in C$ ，只需证明 $a*b^{-1}$ 与 $G$ 中所有元素都可交换。

对 $\forall x \in G$ ， $b*x = x*b$ ，也必有 $b^{-1}*x = x*b^{-1}$

则有  $a*b^{-1}*x = a*x*b^{-1}$

$$\Rightarrow (a*b^{-1}) * x = a*x*b^{-1} = x * (a*b^{-1})$$

即 $a*b^{-1} \in C$ 。

$\langle C, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群。



## 15.2 群和子群

### ✓ 生成子群

**例5** 设 $\langle G, * \rangle$ 是一个群, 对任意的 $a \in G$ , 令 $S = \{a^n \mid n \in \mathbb{Z}, \mathbb{Z} \text{ 是整数}\}$ , 则 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群。称为由 $a$ 生成的子群, 记作 $\langle a \rangle$ 。

证明: ①因为 $a \in S$ , 所以显然 $S$ 是 $G$ 的非空子集。

②对任意的 $a^n, a^m \in S$ , 则 $a^n * a^m = a^{n+m}$ ,

由 $n, m \in \mathbb{Z}$ , 有 $n+m \in \mathbb{Z}$ , 所以 $a^{n+m} \in S$ , 即运算是封闭的;

③由 $S$ 是 $G$ 的子集可得结合律也成立;

④由于  $e = a^0 \in S$ , 所以 $S$ 中有幺元;

⑤又 $\because a^n \in S$ 有逆元 $a^{-n}$ 使 $a^n * a^{-n} = e$

$\therefore$ 综上所述,  $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群。



## 15.2 群和子群

**定理** 元素 $a$ 的周期为 $n$ ，则由 $a$ 生成的子群恰有 $n$ 个元素，  
即 $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ 。

**例如** (1) 在整数加群 $\langle \mathbb{Z}, + \rangle$ 中，2的生成子群是由全体偶数关于加法构成的群，可记为 $\langle 2 \rangle$ 。

由1生成的子群正好是 $\mathbb{Z}$ 本身，记为 $\langle 1 \rangle$ 。

(2) 在 $\langle \mathbb{Z}_6, \oplus \rangle$  **剩余类加群**中， $|\langle 2 \rangle| = 3$ ，则 $\langle 2 \rangle$ 的生成子群为 $\langle 2 \rangle = \{[0], [2], [4]\}$ 。



## 15.2 群和子群

**例6** 设 $n$ 个元素的集合 $A$ 上的全体置换构成集合 $S_n$ ，证明 $\langle S_n, \circ \rangle$ 构成群。（ $n$ 次对称群）

**证明：** 1)  $S_n$ 中两个置换的复合仍然是 $A$ 上的一个置换，所以运算是封闭的；

2) 由于函数的复合是可结合的，所以置换的复合也是可结合的；

3)  $S_n$ 中存在幺置换(单位置换)  $\pi = (1)$ ，

使对  $\forall \sigma \in S_n$ ，  $\pi \circ \sigma = \sigma \circ \pi = \sigma$

所以 $\pi = (1)$ 是幺元；

4) 每个置换将 $x$ 变成 $y$ ，而逆置换是将 $y$ 变成 $x$ ，所以，每个置换都有逆。



## 15.2 群和子群

---

**定义** 设 $A$ 是一个非空集合,  $|A| = n$ ,  $A$ 上所有置换构成的群称为 $n$ 次对称群, 记为 $\langle S_n, \circ \rangle$ ; 它的任何子群都叫做置换群。

✓习题十五

6、9、10





# 主要内容

---

- 15.1 半群
- 15.2 群和子群
- 15.3 交换群和循环群



## 15.3 交换群和循环群

### 1. 交换群

**定义** 若群 $\langle G, * \rangle$ 中的运算“ $*$ ”是可交换的运算，则称该群 $\langle G, * \rangle$ 是一个**交换群**（或**阿贝尔/Abel群**）。

例如

整数加群 $\langle \mathbb{Z}, + \rangle$ ，实数加群 $\langle \mathbb{R}, + \rangle$ ，有理数加群 $\langle \mathbb{Q}, + \rangle$ ，剩余类乘群 $\langle \mathbb{Z}_n - \{[0]\}, \otimes \rangle$ 、实数乘群 $\langle \mathbb{R} - \{0\}, \times \rangle$ 都是交换群。

而 $n$ 阶非奇异矩阵乘群 $\langle M_n, \times \rangle$ 、 $n$ 次对称群 $\langle S_n, \circ \rangle$ 等都不是交换群。



## 15.3 交换群和循环群

**定理** 设 $\langle G, * \rangle$ 是一个群，则 $\langle G, * \rangle$ 为交换群的充分必要条件是：对 $\forall a, b \in G$ ，有 $(a*b)^2 = a^2 * b^2$ 。

**证明：**“ $\Rightarrow$ ” 对 $\forall a, b \in G$ ，由于运算“ $*$ ”是可交换的，所以有：

$$\begin{aligned}(a*b)^2 &= (a*b) * (a*b) = a * (b*a) * b \\ &= a * (a*b) * b = (a*a) * (b*b) = a^2 * b^2.\end{aligned}$$

“ $\Leftarrow$ ” 对 $\forall a, b \in G$ ，若有 $(a*b)^2 = a^2 * b^2$ ，则等式为：

$$(a*b) * (a*b) = (a*a) * (b*b),$$

$$\text{则有 } a * (b*a) * b = a * (a*b) * b,$$

由**消去律**知： $b*a = a*b$ ，

所以，运算“ $*$ ”满足交换律，即群 $\langle G, * \rangle$ 是交换群。



## 15.3 交换群和循环群

### 2. 循环群

**定义** 设 $\langle G, * \rangle$ 是一个群，若 $G$ 中存在元素 $a$ ，使得对 $\forall x \in G$ ，都有：

$$x = a^i \ (i \in I)$$

则称 $\langle G, * \rangle$ 是由 $a$ 所生成的**循环群**，记为 $G = \langle a \rangle$ ， $a$ 称为 $G$ 的一个**生成元**，群 $G$ 中的一切生成元的集合叫做该群 $G$ 的**生成集**。

循环群 $G = \langle a \rangle$ ，根据生成元 $a$ 的阶（周期）可以分成两类： $n$ 阶循环群和无限循环群。



## 15.3 交换群和循环群

设 $G = \langle a \rangle$ 是循环群，若 $a$ 是 $n$ 阶元，则

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

那么 $|G| = n$ ，称 $G$ 为 $n$ 阶循环群。

若 $a$ 是无限阶元，则

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

称 $G$ 为无限循环群。

例如

1) 整数加群 $\langle \mathbb{Z}, + \rangle$ 是一个无限循环群，1和-1都是生成元，而除此以外别无其它生成元。

2) 剩余类加群 $\langle \mathbb{Z}_k, \oplus \rangle$ 是一个 $k$ 阶有限循环群，只要 $[a]$ 满足 $\gcd(a, k) = 1$ ，则 $\mathbb{Z}_k = ([a])$ ，即 $[a]$ 是 $\mathbb{Z}_k$ 的一个生成元。



## 15.3 交换群和循环群

对于循环群 $G=(a)$ ，它的生成元可能不止一个，怎样求得所有生成元？有以下结论：

设 $G=(a)$ 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 ( $n \in \mathbb{Z}^+$ )，则对任何小于 $n$ 且与 $n$ 互素的正整数 $r$ ， $a^r$ 是 $G$ 的生成元。 $G$ 含有 $\varphi(n)$ 个生成元。（ $\varphi(n)$ 为欧拉函数）



## 15.3 交换群和循环群

- 例7 (1) 设 $\langle \mathbb{Z}_9, \oplus \rangle$ 是模9的整数加群，求群的生产元？  
(2) 设 $G = 3\mathbb{Z} = \{3z | z \in \mathbb{Z}\}$ ， $G$ 上的二元运算是普通加法， $G$ 有哪些生产元？

解：(1)  $\langle \mathbb{Z}_9, \oplus \rangle$ 是循环群， $\varphi(9) = 6$   
小于9且与9互素的正整数是1, 2, 4, 5, 7, 8。  
因此， $\mathbb{Z}_9$ 生产元是 $[1], [2], [4], [5], [7], [8]$ 。  
(2)  $G=3\mathbb{Z}$ 是无限循环群，则 $G$ 只有两个生成元，  
即3和 $3^{-1}$ 。



## 15.3 交换群和循环群

---

### 定理

- (1) 设 $G = \langle a \rangle$ 是循环群， $G$ 的子群仍是循环群。
- (2) 若 $G$ 是无限循环群，则 $G$ 的子群除 $\{e\}$ 以外，都是无限循环群。
- (3) 循环群一定是可换群。

证明：(1) 留作课后练习。



✓习题十五

16、17、18