

第14章 代数系统



1

代数系统

- 代数系统又称为代数结构。简单说，代数系统就是集合与集合上运算的合成体
- 代数系统对于可计算模型研究、抽象数据结构、形式语言理论、程序设计语言语义分析等都有着深远的影响。

17:09



2

2

主要内容

- ◆ 二元运算
- ◆ 代数系统
- ◆ 特异元



17:09

3

二元运算

➤ **n元代数运算**：设 S, G 是非空集合，映射 $f: S^n \rightarrow G$ 称为从 S 到 G 的 n 元代数运算，简称**n元运算**(n-ary Operation)。

✓ 当 $n = 1$ 时，称为一元运算； Ex. $y = f(x) = 2x$, $x \in S, y \in G$

✓ 当 $n = 2$ 时，称为二元运算； Ex. $z = f(x, y) = x + y$, $x, y \in S, z \in G$

例：设集合 $S = \{a, b, c, d\}$ 。定义从 S 到 S 的一个二元运算“ \cdot ”用表表示为：

$f(a, a) = a, f(a, b) = a, f(a, c) = a, f(a, d) = a$
 $f(b, a) = a, f(b, b) = b, f(b, c) = c, f(b, d) = d$
 $f(c, a) = a, f(c, b) = c, f(c, c) = b, f(c, d) = d$
 $f(d, a) = a, f(d, b) = d, f(d, c) = c, f(d, d) = b$

\cdot	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	b	d
d	a	d	c	b



17:09

4

定义14-1:

- 设 “ \cdot ” 是一个从 S 到 G 的二元运算, 如果
- ① 对任意的 $a, b \in S$, 都有 $a \cdot b \in S$, 即 $G \subseteq S$, 则称 “ \cdot ” 是 S 上的二元运算, 并称 “ \cdot ” 在 S 上是**封闭**的;
 - **进一步**, 设 “ \cdot ” 是 S 上的一个二元运算
 - ② 对任意的 $a, b \in S$, 都有 $a \cdot b = b \cdot a$, 则称 “ \cdot ” 在 S 上是**可交换**的, 或称满足**交换律**。
 - ③ 对任意的 $a, b, c \in S$, 都有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, 则称 “ \cdot ” 在 S 上是**可结合的**, 或称满足**结合律**。
 - ④ 对任意的 $a \in S$, 满足 $a \cdot a = a$, 则称 “ \cdot ” 是**幂等的**, 或称满足**幂等律**。



17:09

5

5

消化二元运算的几个性质: 封闭性, 交换性, 结合性, 幂等性
并完成下表

集合	运算	封闭	交换	结合	幂等
自然数集	+ * -				
整数集	+ * -				
正整数集	+ * - /				
实数集	+ * -				
正实数集	+ * - /				
2^A 幂集	\cup 和 \cap				
命题集合	\wedge 和 \vee				



17:09

6

6

- 定义在**自然数集 N** 上的**加法**和**乘法**运算:
- ✓ 满足**封闭性**、**交换律**和**结合律**, 但不满足**幂等性**
- 定义在**实数集 R** 上的**加法**和**乘法**运算:
- ✓ 满足**封闭性**、**交换律**和**结合律**; 但不满足**幂等性**
- 定义在 **2^A 幂集**上运算 \cup 和 \cap :
- ✓ 满足**封闭性**、**交换律**、**结合律**和**幂等性**
- 定义在**命题集合**上运算 \wedge 和 \vee
- ✓ 满足**封闭性**、**交换律**、**结合率**和**幂等性**



17:09

7

7

定义14-2: 设 “ $*$ ”, “ \cdot ” 是集合 S 上的两个二元运算, 对

$$\forall a, b, c \in S,$$

- ① 若 $a \cdot (b * c) = (a \cdot b) * (a \cdot c)$ 且 $(b * c) \cdot a = (b \cdot a) * (c \cdot a)$, 则称 “ \cdot ” 对 “ $*$ ” 在 S 上满足**分配律**。
- ✓ **乘法对加法**在实数集 R /整数集 Z /自然数集 N 上满足**分配律**
- ② 若 “ $*$ ”、“ \cdot ” 满足交换律, 且 $a \cdot (a * b) = a$ 且 $a * (a \cdot b) = a$, 则称运算 “ $*$ ” 与 “ \cdot ” 满足**吸收律**。
- ✓ 在**幂集 2^A** 上, \cup 和 \cap 是**相互可分配的**, 并且满足**吸收律**
- ✓ 在**命题集合**上, \wedge 和 \vee 是**相互可分配的**, 并且满足**吸收律**



17:09

8

8

例：设运算“ \vee ”、“ \wedge ”分别是实数集 R 上的最大值和最小值二元运算，即对任意的 $a, b \in R$, $a \vee b = \max(a, b)$, $a \wedge b = \min(a, b)$, 试判断运算“ \vee ”与“ \wedge ”是否满足分配律和吸收律。

分配率：需判断 对任意的 $a, b, c \in R$

$$a \vee (b \wedge c) \stackrel{?}{=} (a \vee b) \wedge (a \vee c)$$

$$(b \wedge c) \vee a \stackrel{?}{=} (b \vee a) \wedge (c \vee a)$$

$$a \wedge (b \vee c) \stackrel{?}{=} (a \wedge b) \vee (a \wedge c)$$

$$(b \vee c) \wedge a \stackrel{?}{=} (b \wedge a) \vee (c \wedge a)$$

6 种情况

$$a > b > c, a > c > b$$

$$b > a > c, b > c > a$$

$$c > a > b, c > b > a$$

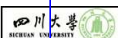
吸收率需判断：对任意的 $a, b \in R$

$$a \vee (a \wedge b) \stackrel{?}{=} a; a \wedge (a \vee b) \stackrel{?}{=} a$$

2 种情况

$$a > b$$

$$b > a$$



17:09

9

9

➤ 定义14-3: 设 S 是一个非空集合, f_1, f_2, \dots, f_m 分别是定义在 S 上的封闭二元运算, 称集合 S 和运算 f_1, f_2, \dots, f_m 所组成的系统为一个二元代数系统, 简称代数, 记为 $\langle S, f_1, f_2, \dots, f_m \rangle$ 。

➤ 判断集合 S 及某些二元运算是否可组成二元代数系统, 关键是判断两点:

① 集合 S 是否非空;

② 二元运算关于 S 是否满足封闭性。



17:09

10

10

定义14-4: 设 $\langle S, * \rangle$ 是个二元代数系统

1) 若 $\exists e \in S$, 使得对 $\forall a \in S$, 都有: $a * e = e * a = a$,

则称 e 为二元代数系统 $\langle S, * \rangle$ 的单位元或幺元;

✓ 0 为 $\langle R, + \rangle$ 的单位元; 1 为 $\langle R, \times \rangle$ 的单位元

2) 若 $\exists 0 \in S$, 使得对 $\forall a \in S$, 都有: $a * 0 = 0 * a = 0$,

则称 0 为二元代数系统 $\langle S, * \rangle$ 的零元;

✓ 0 为 $\langle R, \times \rangle$ 的零元

3) 若 $\exists a \in S$, 有 $a * a = a$, 则称 a 是二元代数系统 $\langle S, * \rangle$ 的幂等元。

✓ 0, 1 为 $\langle R, \times \rangle$ 的幂等元

✓ 0 为 $\langle R, - \rangle, \langle R, + \rangle$ 的幂等元



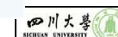
17:09

11

11

自学 幺元, 零元, 幂等元的定义, 并完成下表

代数系统	幺元/单位元	零元	幂等元
$\langle N, + \rangle$			
$\langle Z, * \rangle$			
$\langle Z, - \rangle$			
$\langle R, + \rangle$			
$\langle R - \{0\}, / \rangle$			
$\langle R, - \rangle$			
$\langle 2^A, \cup \rangle$			
$\langle 2^A, \cap \rangle$			
$\langle \{0, 1\}, \vee \rangle$			
$\langle \{0, 1\}, \wedge \rangle$			



17:09

12

设二元代数系统 $\langle A, * \rangle$, 其中 $A = \{a, b, c, d\}$, 二元运算 $*$ 结果见下表

问:

1. “ $*$ ” 满足交换律, 结合律, 幂等律吗?
2. 幺元是 a ;
3. 零元是 无 ;
4. 幂等元是 a, b, d .

*	a	b	c	d
a	a	b	c	d
b	b	b	a	d
c	c	a	b	a
d	d	d	a	d



17:11

13

13

二元代数系统的特异元 --逆元

定义14-5: 设 $\langle S, * \rangle$ 是一个二元代数系统, e 是 $\langle S, * \rangle$ 的幺元, 若对 $a \in S$, $\exists b \in S$, 使得: $a * b = b * a = e$, 则称 b 是 a 的**逆元**, 记为 $b = a^{-1}$, 也称 a 为**可逆元** (同样, a 也称为 b 的**逆元**, 记为 $a = b^{-1}$, 也称 b 为**可逆的**)

幺元的逆元是它本身

例: $\langle S = \{a, b, c, d\}, * \rangle$ 的可逆元有 ;
a, b, c, d

*	a	b	c	d
a	a	b	c	d
b	b	b	a	d
c	c	a	b	a
d	d	d	a	d

在一个代数系统中, **并不是每个元都是可逆的**.

如 $\langle R, * \rangle$ 的 0



17:13

14

14

请思考

在一个代数系统 $\langle S, * \rangle$ 中

1. 如果存在幺元, 幺元是否唯一?
2. 如果存在零元, 零元是否唯一?
2. 若存在可逆元, 其逆元是否唯一?



17:09

15

15

二元代数系统的特异元

定理14-1 设 $\langle S, * \rangle$ 是一个二元代数系统:

- 1) 若 $\langle S, * \rangle$ 存在**幺元**, 则该幺元**唯一**;
- 2) 若 $\langle S, * \rangle$ 存在**零元**, 则该零元**唯一**;
- 3) 若 “ $*$ ” 满足**结合律** 且 $\langle S, * \rangle$ 存在幺元, 则对 $\forall a \in S$, 若 a 存在逆元, 则逆元**唯一**.

用来判断不满足结合律

证明: (反证法)

- 1) 设 $\langle S, * \rangle$ 含有幺元 e_1, e_2 , 根据定义 $e_1 = e_1 * e_2 = e_2$, 因此, 幺元唯一.
- 2) 设 S 中有两个零元 θ_1 和 θ_2 , 由定义有 $\theta_1 = \theta_1 * \theta_2 = \theta_2$, 故 零元唯一.
- 3) 设 e 是 $\langle S, * \rangle$ 的幺元, 且元素 a 有两个逆元 b_1, b_2 , 则有
 $b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$, 因此, 逆元唯一.



17:09

16

16

定义14-6: 设 $\langle S, \cdot \rangle$ 是一个二元代数系统, 其么元为 e .

对 $a \in S$, 若存在 $b \in S$, 使 $b \cdot a = e$, 则称 b 是 a 的**左逆元**; 若存在 $c \in S$, 使 $a \cdot c = e$, 则称 c 是 a 的**右逆元**.

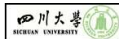
例: $\langle S = \{a, b, c, d\}, * \rangle$ 中, b 的左逆元为 无, 右逆元为 c , c 的左逆元为 b , 右逆元为 d .

若“ \cdot ”满足结合律, 且一个元既有左逆元又有右逆元, 则其左右逆元必相等且等于其逆元

也可用来判断不满足结合律

该代数系统满足结合律吗?

*	a	b	c	d
a	a	b	c	d
b	b	b	a	d
c	c	c	b	a
d	d	d	c	d



1. 代数系统 $\langle S, * \rangle$
集合 S 与其上运算 $*$ 的结合体
2. 二元运算的4个性质
封闭性, 结合律, 交换律, 幂等律
3. 四种特异元
 1. 么元, 若有, 一定唯一
 2. 零元, 若有, 一定唯一
 3. 幂等元,
 4. 可逆元, 若“ $*$ ”满足结合律, 有唯一逆元



第15章 半群与群



1

主要内容

- ◆ 广群、半群、含么半群及群
- ◆ 半群与子半群
- ◆ 群与子群
- ◆ 元素的周期与循环群
- ◆ 交换群 (Abel群)
- ◆ 同态与同构



2

广群、半群、含么半群及群

定义14-7:

- ✓ 广群: 含一个二元运算的代数系统 $\langle S, * \rangle$ 称为广群; (闭)
- ✓ 半群: 若 $\langle S, * \rangle$ 为广群, 且“*”在S上满足结合率, 则称 $\langle S, * \rangle$ 为半群; (闭、结)
- ✓ 含么半群: 若 $\langle S, * \rangle$ 是半群, 且存在么元 e , 则称 $\langle S, * \rangle$ 是含么半群, 常记为 $\langle S, *, e \rangle$; (闭、结、么)
- ✓ 群: 如果 $\langle S, * \rangle$ 是含么半群, 且每个元素都有逆元, 则称 $\langle S, * \rangle$ 为群。 (闭、结、么、逆)

群 \subset 含么半群 \subset 半群 \subset 广群



3

广群、半群、含么半群及群

例: 设 $k \in \mathbb{Z}$, 令集合 $S_k = \{x | (x \in \mathbb{Z}) \wedge (x \geq k)\}$, “+”是一个普通的加法运算, 试判断 $\langle S_k, + \rangle$ 是否是一个广群, 半群, 含么半群, 群?

1. 判断封闭性

- ① 若 $k < 0$, 运算“+”在 S_k 上不封闭;
- ② 若 $k \geq 0$, 运算“+”在 S_k 上是封闭的。
故 $k \geq 0$ 时, $\langle S_k, + \rangle$ 是广群。

2. 判断结合性:

$k \geq 0$ 时, “+”在 S_k 上满足结合律, 故 $k \geq 0$ 时, $\langle S_k, + \rangle$ 是半群。

3. 判断是否有么元:

$k = 0$ 时, 有么元 $e = 0$, 故 $k = 0$ 时, $\langle S_k, + \rangle$ 是含么半群。

4. 判断是否每个元可逆:

$k = 0$ 时, 除了0, 其他元均不可逆, 故 $k = 0$ 时, $\langle S_k, + \rangle$ 不是群。



4

广群、半群、含么半群及群

- 含 $+$, \times 的广群 (封) 通常为半群 (封, 结)
 - $\langle \mathbb{R}, \times \rangle$, $\langle \mathbb{Q}, \times \rangle$, $\langle \mathbb{N}, + \rangle$ 等;
- 含 $-$, \div 的广群 不是半群
 - ✓ $\langle \mathbb{Q} \setminus \{0\}, \div \rangle$, $\langle \mathbb{Z}, - \rangle$, $\langle \mathbb{Q}, - \rangle$ 等是广群, 但不是半群;



5

一些典型的(含么)半群

- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{Q}, + \rangle$ 是含么半群;
 - ✓ 0 是么元, 也是唯一的幂等元, 无零元; 满足结合律和交换律
- $\langle \mathbb{Z}, \times \rangle$, $\langle \mathbb{N}, \times \rangle$, $\langle \mathbb{R}, \times \rangle$, $\langle \mathbb{Q}, \times \rangle$ 是含么半群;
 - ✓ 1 是么元, 0 是零元, 1 和 0 都是幂等元; 满足结合律和交换律
- $\langle \mathbb{Z}^+, + \rangle$, $\langle \mathbb{Q}^+, + \rangle$, $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$ 等是半群, 但不是含么半群;
 - ✓ 无么元, 无幂等元, 无零元; 满足结合律和交换律
- $\langle \mathbb{Q}^+, \times \rangle$, $\langle \mathbb{Z}^+, \times \rangle$ 等是含么半群,
 - ✓ 么元为 1, 无零元, 1 是幂等元; 满足结合律和交换律



6

一些典型的(含么)半群

设 $M_n(\mathbb{R})$ 为 $n \times n$ 实数矩阵集合, $+$ 和 \cdot 分别是矩阵的加法和乘法运算, 则

- $\langle M_n(\mathbb{R}), + \rangle$ 是含么半群,
 - ✓ 么元为零矩阵; 也是唯一的幂等元; 无零元;
 - ✓ 满足结合律和交换律
- $\langle M_n(\mathbb{R}), \cdot \rangle$ 是含么半群,
 - ✓ 么元为单位矩阵, 零元为零矩阵, 单位矩阵和零矩阵都是幂等元。
 - ✓ 满足结合律和交换律



7

一些典型的(含么)半群

设 A 为任意集合, 则 $\langle 2^A, \cap \rangle$ 和 $\langle 2^A, \cup \rangle$ 都是含么半群,

- $\langle 2^A, \cup \rangle$ 的么元为 Φ ; 零元为 A 。
- $\langle 2^A, \cap \rangle$ 的么元为 A ; 零元为 Φ 。
- 满足结合律, 交换律和幂等律



8

一些典型的(含幺)半群

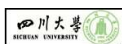
例：设 $A = \{a, b, c, \dots, z\}$ ，由 A 中有限个元素组成的序列称为 A 上的字符串，不包含任何字符的字符串称为空串，用 ε 表示，

令 $A^* = \{x \mid x \text{ 是 } A \text{ 上的字符串}\}$

$$A^+ = A^* - \varepsilon$$

设二元运算“ \circ ”为： $\alpha\beta$ 为两个字符串的连接，即对任意两个字符串 α, β ， $\alpha\beta$ 为将字符串 α 写在字符串 β 的左边而得到的字符串。

问： $\langle A^*, \circ \rangle, \langle A^+, \circ \rangle$ 是否是含幺半群，若是，求其幺元。



9

幂运算

➤ 设 $\langle S, * \rangle$ 是一个半群，由于 $*$ 满足结合律，故可定义幂运算，即对 $\forall x \in S$ ，定义：

$$x^1 = x,$$

$$x^2 = x * x,$$

$$x^3 = x * x^2 = x^2 * x = x * x * x,$$

.....

$$x^n = x^{n-1} * x = x * x^{n-1}$$

➤ 若进一步， $\langle S, * \rangle$ 是含幺半群，设其单位元为 e ，可定义：

$$x^0 = e$$



10

幂运算

➤ 定理14-2 设 $\langle S, * \rangle$ 是半群， $a \in S$ ， m 和 n 是正整数，则

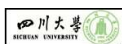
$$\textcircled{1} a^m * a^n = a^{m+n}$$

$$\textcircled{2} (a^m)^n = a^{mn}$$

➤ 当 $\langle S, * \rangle$ 是含幺半群时，上述结论对任意非负整数 m 和 n 都成立。

$$\textcircled{1} a^m * a^n = a^{m+n}$$

$$\textcircled{2} (a^m)^n = a^{mn}$$



11

幂运算

定理14-3 设 $\langle S, * \rangle$ 是半群，如果 S 是有限集，则 $\langle S, * \rangle$ 必有幂等元，即必有 $a \in S$ ，满足 $a^2 = a$ 。

注意：如果 S 不是有限集，则不一定有幂等元。

如： $\langle \mathbb{Z}^+, + \rangle$ 是半群，但 \mathbb{Z}^+ 不是有限集，没有幂等元

$\langle \mathbb{Z}, + \rangle$ 是半群，但 \mathbb{Z} 不是有限集，有幂等元 0

含幺半群至少有一个幂等元——幺元

含幺半群至少有一个可逆元——幺元



12

(含幺)子半群

定义14-8

- ①如果 $\langle S, * \rangle$ 是半群, T 是 S 的**非空子集**, 且“ $*$ ”在 T 上是**封闭的**, 则 $\langle T, * \rangle$ 是半群, 并称 $\langle T, * \rangle$ 是半群 $\langle S, * \rangle$ 的**子半群**;
- ②如果 $\langle S, *, e \rangle$ 是**含幺半群**, $T \subseteq S$, $e \in T$, 且“ $*$ ”在 T 上是**封闭的**, 则 $\langle T, * \rangle$ 是含幺半群, 称 $\langle T, *, e \rangle$ 是 $\langle S, *, e \rangle$ 的**含幺子半群**。

例: 代数系统 $\langle [0, 1], \times \rangle$, $\langle \mathbb{Z}, \times \rangle$, $\langle \mathbb{R}^+, \times \rangle$ 都是 $\langle \mathbb{R}, \times \rangle$ 的子半群。
 $\langle [10, 20], \times \rangle$ **不是**半群, 故**不是** $\langle \mathbb{R}, \times \rangle$ 的子半群,



13

(含幺)子半群

例 设 $\langle S, * \rangle$ 是一个**可交换的含幺半群**, M 是它的所有的等幂元构成的集合, 则 $\langle M, * \rangle$ 是 $\langle S, * \rangle$ 的一个含幺子半群。

证明:

- (1) **子集:** 显然, $M \subseteq S$;
- (2) $\langle M, * \rangle$ **封闭:** 设任意 $a, b \in M$,
- $$a * b = (a * a) * (b * b) = a * a * b * b$$
- $$= (a * b) * (a * b)$$

所以 $a * b \in M$, 即运算“ $*$ ”关于集合 M 是封闭的。

- (3) **M含幺:** $\langle S, * \rangle$ 是含幺半群, 所以幺元 e 是等幂元, 即有 $e \in M$;

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



14

群

如果 $\langle G, * \rangle$ 是含幺半群, 且每个元素都是可逆元, 则称 $\langle G, * \rangle$ 为**群**。(闭、结、幺、逆), $|G|$ 称为群的阶

- $\langle \mathbb{Z}, + \rangle$ 是**含幺半群**; 因每个整数 a 都有逆元 $-a$, 故 $\langle \mathbb{Z}, + \rangle$ 是群, 通常称为**整数加群**
- $\langle \mathbb{R}, + \rangle$: **实数加群**
- $\langle \mathbb{Q}, + \rangle$: **有理数加群**;
- $\langle \mathbb{R} - \{0\}, \times \rangle$ 是**实数乘群**;

为什么要去掉0?



15

Your turn

1. 已知代数系统 $\langle A, \$ \rangle$ 是群, 定义二元运算 $\#$ 为:

$$x \# y = x \$ a \$ y, \quad a \in A$$

1) 试判断运算 $\#$ 在 A 上是否满足封闭性, 结合律, 是否有幺元(若有, 请表达出来), 是否每元可逆(若可逆, 写出逆元的表达式)

- 2) $\langle A, \# \rangle$ 是否为群?



16

例：设 $S = \{1, 3, 4, 5, 9\}$ ，在 S 上定义运算 $\#$ ， $\$$ 为：

$$\forall x, y \in S, \quad x \# y = ((x \% 11) * (y \% 11)) \% 11 = (x * y) \% 11$$

$$\forall x, y \in S, \quad x \$ y = ((x \% 11) + (y \% 11)) \% 11 = (x + y) \% 11$$

这里 $+$ ， $*$ 为普通加和普通乘， $\%$ 为求模运算

问： $\langle S, \# \rangle$ ， $\langle S, \$ \rangle$ 是否为群？

$S = \{1, 2, 3, 5, 10\}$ 呢？

$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ 呢？



17

➤ 剩余类加群

设 Z_k 表示整数集 Z 上的模 k 剩余类（模 k 同余等价类）集合，即

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

在 Z_k 上定义运算 \oplus 和 \otimes 如下：

$$[i] \oplus [j] = [(i+j) \% k], \quad i, j \in \{0, 1, \dots, k-1\}$$

$$[i] \otimes [j] = [(ij) \% k]$$

则 $\langle Z_k, \oplus \rangle$ 是群，常被称为**剩余类加群**。 $[0]$ 是 \oplus 的幺元，每元 $[i]$ 的逆元是 $[k-i]$ 。

剩余类
乘半群

$\langle Z_k, \otimes \rangle$ 只是含幺半群， $[1]$ 是它的幺元，但不是群，因 $[0]$ 无逆元，



18

已有证明：当 k 是素数时， $\langle Z_k - \{[0]\}, \otimes \rangle$ 是群。

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

➤ 如， $Z_4 - \{[0]\} = \{[1], [2], [3]\}$ ，

$$[2] \otimes [2] = [0] \notin Z_4 - \{[0]\}, \quad \text{不封闭}$$

$\therefore \langle Z_4 - \{[0]\}, \otimes \rangle$ **不是群**。

➤ 又如， $Z_5 - \{[0]\} = \{[1], [2], [3], [4]\}$

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] 和 [3] 互为逆元**；

因此 $\langle Z_5 - \{[0]\}, \otimes \rangle$ **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]



19

➤ n 次对称群/ n 阶置换群

设基数为 n 的集合 A 上的全体置换构成集合 S_n ，“ \circ ” 是复合运算，则 $\langle S_n, \circ \rangle$ 是群，常称为 **n 次对称群/ n 阶置换群**

证明：

- 1) **封闭**： 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) **结合律**： 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) **含幺**： S_n 中存在幺置换(单位置换) $e = (1)$ ，使对 $\forall \sigma \in S_n$ ， $e \circ \sigma = \sigma \circ e = \sigma$ ，所以 $e = (1)$ 是**幺元**；
- 4) **每元可逆**： 每个置换 σ 都有逆 σ^{-1} 。 $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = (1)$



20

① 若 $\langle G, * \rangle$ 是群, 则运算 $*$ 满足消去律;

➤ 即 $a*b = a*c \Leftrightarrow b=c$; $b*a = c*a \Leftrightarrow b=c$

② 群的运算表中同一行(列)没有相同的值;

③ 群 $\langle G, * \rangle$ 中除幺元 e 外无其它幂等元;

反证法: 设 $a \neq e$, $a*a = a$

$a*a = a \Rightarrow a*a = a*e \Rightarrow a = e$, 与假定 $a \neq e$ 矛盾

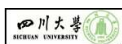
④ 阶大于1的群 $\langle G, * \rangle$ 没有零元; (用反证法)

证: 假设有零元 z , 任取 $a \neq b$, 则有 $a*z = b*z = z \Rightarrow a=b$, 与 $a \neq b$ 矛盾

⑤ $\langle G, * \rangle$ 中的任意两个元素 a, b , 都有 $(a*b)^{-1} = b^{-1}*a^{-1}$.

证: $(a*b)*(a*b)^{-1} = e \Rightarrow a^{-1}* (a*b)*(a*b)^{-1} = a^{-1} \Rightarrow b^{-1}*b*(a*b)^{-1} = b^{-1}*a^{-1}$

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



21

➤ 定义15.1 设 $\langle G, * \rangle$ 是一个群, S 是 G 的一个非空子集, 若 $\langle S, * \rangle$ 也是群, 则称 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群。

➤ 对任意的群 $\langle G, * \rangle$, 都有两个子群

① 幺元子群 $\langle \{e\}, * \rangle$

② 群自身 $\langle G, * \rangle$

平凡子群

➤ 若 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群, 且非平凡子群, 则称 $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的真子群。



22

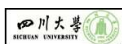
➤ 定理15-3 设 $\langle S, * \rangle$ 是群 $\langle G, * \rangle$ 的子群, 则:

(1) 子群 $\langle S, * \rangle$ 的幺元 e_S 与群 $\langle G, * \rangle$ 的幺元 e_G 相同;

(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} 。

定理15-4 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 $a*b^{-1} \in S$



23

1 设 $\langle G, * \rangle$ 是群, 其中 $G = \{0, 1, 2, 3, 4, 5, \dots, 999\}$ “*” 为模

1000 加运算, $H = \{0, 2, 4, 6, \dots, 996, 998\}$,

试证明 $\langle H, * \rangle$ 是 $\langle G, * \rangle$ 的子群。

2. 已知 $\langle G, * \rangle$ 是群, $\langle S_1, * \rangle, \langle S_2, * \rangle$ 均为 $\langle G, * \rangle$ 的子群, $S = S_1 \cap S_2$, 试证明 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群。



24