# 离散数学

杨桐
yangt@nankai.edu.cn

机器人与信息自动化研究所
Institute of Robotics & Automatic Information System
IRAIS

南開大學
Nankai University

# 第8章 代数系统

机器人与信息自动化研究所
Institute of Robotics & Automatic Information System
IRAIS
南開大學
Nankai University

# 主要内容

- **第8章 代数系统**
  - 8.1 二元运算及其性质
  - 8.2 代数系统
  - 8.3 几个典型的代数系统

# 8.1 二元运算及其性质

- 二元运算及一元运算的定义
- 二元运算的性质
  - 交换律、结合律、幂等律、消去律
  - 分配律、吸收律
- 二元运算的特异元素
  - 单位元
  - 零元
  - 可逆元素及其逆元

# 8.1.1 二元运算及一元运算的定义

- **二元运算的定义及其实例**

**定义** **设 $S$ 为集合,函数 $f$: $S\times S\to S$ 称为 $S$ 上的二元运算,简称为二元运算. 也称 $S$ 对 $f$ 封闭.**

封闭

设 $*$ 是定义在集合 $A$ 上的二元运算, 如果对任意 $x, y \in A$, 都有 $x * y \in A$, 则称运算 $*$ 在 $A$ 上封闭.

☞ 通俗地讲, 封闭就是和谐、不自相矛盾.

理论、系统都具有这个特点: 基本要求是能自成一体.

# 8.1.1 二元运算及一元运算的定义

## ➢ 二元运算的定义及其实例

**定义** 设 $S$ 为集合,函数 $f$: $S\times S\to S$ 称为 $S$ 上的二元运算,简称为**二元运算**. 也称 $S$ 对 $f$ **封闭**.

对集合 $A$，一个从 $A^n$ 到 $B$ 的映射, 称为集合 $A$ 上的一个 $n$ 元运算 (n-nary operation). 如果 $\boxed{B \subseteq A,}$ 则称该运算是封闭的.

例如 $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}, f(\langle x,y\rangle)=x+y$ (这里 $+$ 表示普通的加法运算) 就是自然数集合 $\mathbb{N}$ 上封闭的二元运算.

- 而普通的减法不是自然数集合 $\mathbb{N}$ 上封闭的二元运算. 因为两个自然数相减可能得负数, 而负数不是自然数. 这时称集合 $\mathbb{N}$ 对减法运算不封闭.

- 实数集合上的加法和乘法是可交换的, 但减法不可交换.
- 幂集 $\mathscr{P}(A)$ 上的 $\cup, \cap, \oplus$ (对称差) 都是可交换的, 但是相对补运算 (差运算) 不可交换.

# 8.1.1 二元运算及一元运算的定义

- **二元运算的定义及其实例**

**定义** 设 $S$ 为集合,函数 $f$: $S\times S\to S$ 称为 $S$ 上的二元运算,简称为**二元运算**. 也称 $S$ 对 $f$ **封闭**.

例1

(1) N 上的二元运算：加法、乘法.

(2) Z 上的二元运算：加法、减法、乘法.

(3) 非零实数集 R* 上的二元运算: 乘法、除法.

(4) 设 $S = \{ a_1, a_2, \ldots , a_n\}$, $a_i \circ a_j = a_i$

$\circ$为 S 上二元运算

# 8. 1. 1 二元运算及一元运算的定义

(5) 设 $M_n(\mathrm{R})$ 表示所有 $n$ 阶 ($n\geq 2$) 实矩阵的集合，即

$$M_n(\mathbf{R})=\left\{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \middle| \; a_{ij}\in\mathbf{R},\ i,j=1,2,\ldots,n\right\}$$

矩阵加法和乘法都是 $M_n(\mathrm{R})$ 上的二元运算.

(6) 幂集 $P(S)$ 上的二元运算：$\cup,\cap,-,\oplus$.

(7) $S^S$ 为 $S$ 上的所有函数的集合：合成运算$\circ$.

# 8. 1. 1 二元运算及一元运算的定义

- ***n*元运算**

定义 设 $S$ 为集合，$n$为正整数，函数

$$f:\underbrace{S\times S\times\ldots\times S}_{n\text{个}}\to S$$

称为 $S$ 上的 $n$ 元运算，简称为 $n$元运算.

例2 (1) Z, Q 和 R 上的一元运算: 求相反数

(2) 非零有理数集 Q*和实数集 R*的一元运算: 倒数

(3) 复数集合 C 上的一元运算: 求共轭复数

(4) 幂集 $P(S)$ 上, 全集为 $S$: 求绝对补运算~

(5) $A$ 为 $S$ 上所有双射函数的集合，$A\subseteq S^S$: 求反函数

(6) 在 $M_n(\mathrm{R})$ ( $n\geq 2$ )上，求转置矩阵

# 8.1.1 二元运算及一元运算的定义

- **运算的表示**

算符：$\circ, *, \cdot, \oplus, \otimes$ 等符号

表示 $n$ 元运算

$$\circ(a_1, a_2, \ldots, a_n)=b.$$

对二元运算 $\circ$，如果 $x$ 与 $y$ 运算得到 $z$，记做

$$x \circ y = z;$$

对一元运算 $\circ$，$x$ 的运算结果记作 $\circ x$

注意：在同一问题中不同的运算使用不同的算符

# 8.1.1 二元运算及一元运算的定义

- 二元与一元运算的表示

**公式表示**

例3 设 R 为实数集合，如下定义 R 上的二元运算 $*$:

$$\forall x, y \in \mathrm{R},\ x * y = x.$$

那么 $3 * 4 = 3$

$0.5 * (-3) = 0.5$

# 8.1.1 二元运算及一元运算的定义

- **运算表**（表示有穷集上的一元和二元运算）

| $\circ$ | $a_1$ | $a_2$ | … | $a_n$ |
|---|---|---|---|---|
| $a_1$ | $a_1\circ a_1$ | $a_1\circ a_2$ | … | $a_1\circ a_n$ |
| $a_2$ | $a_2\circ a_1$ | $a_2\circ a_2$ | … | $a_2\circ a_n$ |
| . | | . . . | | |
| . | | . . . | | |
| . | | . . . | | |
| $a_n$ | $a_n\circ a_1$ | $a_n\circ a_2$ | … | $a_n\circ a_n$ |

| | $\circ a_i$ |
|---|---|
| $a_1$ | $\circ a_1$ |
| $a_2$ | $\circ a_2$ |
| . | . |
| . | . |
| . | . |
| $a_n$ | $\circ a_n$ |

# 8. 1. 1 二元运算及一元运算的定义

例4 $A = P(\{a, b\})$, $\oplus$, ~分别为对称差和绝对补运算

($\{a,b\}$为全集)

$\oplus$ 的运算表

| $\oplus$ | $\varnothing$ | $\{a\}$ | $\{b\}$ | $\{a,b\}$ |
|---|---|---|---|---|
| $\varnothing$ | $\varnothing$ | $\{a\}$ | $\{b\}$ | $\{a,b\}$ |
| $\{a\}$ | $\{a\}$ | $\varnothing$ | $\{a.b\}$ | $\{b\}$ |
| $\{b\}$ | $\{b\}$ | $\{a,b\}$ | $\varnothing$ | $\{a\}$ |
| $\{a,b\}$ | $\{a,b\}$ | $\{b\}$ | $\{a\}$ | $\varnothing$ |

~ 的运算表

| $X$ | $\sim X$ |
|---|---|
| $\varnothing$ | $\{a,b\}$ |
| $\{a\}$ | $\{b\}$ |
| $\{b\}$ | $\{a\}$ |
| $\{a,b\}$ | $\varnothing$ |

# 8. 1. 1 二元运算及一元运算的定义

**例5 $Z_5 = \{0, 1, 2, 3, 4\}$, ⊗, ⊕分别为模 5 加法与乘法**

**⊗ 的运算表**

| ⊗ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

*Example* 4. 设 $S = \{1, 2, 3, 4\}$, 定义 $S$ 上的二元运算 $\circ$ 如下:

$$x \circ y = (xy) \pmod 5, \quad \forall x, y \in S$$

则 $\langle S, \circ \rangle$ 构成一个代数系统.

这里, 运算 $\circ$ 还可用表格的形式来定义, 称为运算表:

| $\circ$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

从表中可以看出, 运算 $\circ$ 在 $S$ 上是封闭的.

# 8. 1. 1 二元运算及一元运算的定义

例5 $Z_5 = \{ 0, 1, 2, 3, 4 \}$, $\otimes$ , $\oplus$分别为模 5 加法与乘法

$\oplus$ 的运算表

| $\oplus$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

# 8.1.2 二元运算的性质

**定义** 设 $\circ$ 为 $S$ 上的二元运算,

(1) 如果对于任意的 $x, y \in S$ 有

$$x \circ y = y \circ x,$$

则称运算在 $S$ 上满足**交换律**.

(2) 如果对于任意的 $x, y, z \in S$ 有

$$(x \circ y) \circ z = x \circ (y \circ z),$$

则称运算在 $S$ 上满足**结合律**.

(3) 如果对于任意的 $x \in S$ 有

$$x \circ x = x,$$

则称运算在 $S$ 上满足**幂等律**.

# 8. 1. 2 二元运算的性质

- Z, Q, R分别为整数、有理数、实数集；$M_n$(R)为 $n$ 阶实矩阵集合, $n\geq 2$；$P(B)$为幂集；$A^A$ 为 $A$上$A$，$|A|\geq 2$.

| 集合 | 运算 | 交换律 | 结合律 | 幂等律 |
|---|---|---|---|---|
| Z, Q, R | 普通加法+ | 有 | 有 | 无 |
| | 普通乘法× | 有 | 有 | 无 |
| $M_n$(R) | 矩阵加法+ | 有 | 有 | 无 |
| | 矩阵乘法× | 无 | 有 | 无 |
| $P(B)$ | 并∪ | 有 | 有 | 有 |
| | 交∩ | 有 | 有 | 有 |
| | 相对补– | 无 | 无 | 无 |
| | 对称差⊕ | 有 | 有 | 无 |
| $A^A$ | 函数符号 o | 无 | 有 | 无 |

# 8.1.2 二元运算的性质

**定义** 设 $\circ$ 和 $*$ 为 $S$ 上两个不同的二元运算,

(1) 如果 $\forall x, y, z \in S$ 有

$$(x * y) \circ z = (x \circ z) * (y \circ z)$$

$$z \circ (x * y) = (z \circ x) * (z \circ y)$$

则称 $\circ$ 运算对 $*$ 运算满足**分配律**.

(2) 如果 $\circ$ 和 $*$ 都可交换, 并且 $\forall x, y \in S$ 有

$$x \circ (x * y) = x$$

$$x * (x \circ y) = x$$

则称 $\circ$ 和 $*$ 运算满足**吸收律**.

# 8. 1. 2 二元运算的性质

- Z, Q, R分别为整数、有理数、实数集；$M_n$(R) 为 $n$ 阶实矩阵集合, $n\geq 2$；$P(B)$为幂集；$A^A$为 $A$上$A$，$|A|\geq 2$.

| 集合 | 运算 | 分配律 | 吸收律 |
|---|---|---|---|
| Z,Q,R | 普通加法 + 与乘法 × | × 对 + 可分配 | 无 |
| | | + 对 × 不分配 | |
| $M_n$(R) | 矩阵加法 + 与乘法 × | × 对 + 可分配 | 无 |
| | | + 对 × 不分配 | |
| $P(B)$ | 并 ∪ 与交 ∩ | ∪ 对 ∩ 可分配 | 有 |
| | | ∩ 对 ∪ 可分配 | |
| | 交 ∩ 与对称差 ⊕ | ∩ 对 ⊕ 可分配 | 无 |
| | | ⊕ 对 ∩ 不分配 | |

# 8. 1. 2 二元运算的性质

例如幂集 $\mathscr{P}(S)$ 上的 $\cup$ 和 $\cap$ 运算 满足幂等律 任意 $A \in \mathscr{P}(S)$, 有

$$A \cup A = A, \quad A \cap A = A.$$

例如幂集 $\mathscr{P}(S)$ 上的 $\cup$ 和 $\cap$ 运算满足吸收律: 任意 $A, B \in \mathscr{P}(S)$,

$$A \cup (A \cap B) = A,$$
$$A \cap (A \cup B) = A.$$

*Example* 9. 设 $A = \{a, b, c, d\}$, 由表

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $d$ | $a$ | $c$ |
| $c$ | $c$ | $a$ | $b$ | $dd$ |
| $d$ | $d$ | $c$ | $aa$ | $b$ |

所给的代数运算是否满足交换律?

解: 注意到 $d * c = a$, 而 $c * d = d$, 所以该运算不满足交换律.

☞ 可见满足交换律的运算, 其运算表是对称的.

*Example* 11. 例如普通的加法和乘法, 在自然数集 $\mathbb{N}$, 整数集 $\mathbb{Z}$, 有理数集 $\mathbb{Q}$, 实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$ 上都是可结合的. 减法就不满足结合律:

$$(a - b) - c \neq a - (b - c), \quad \text{除非 } c = 0.$$

# 8.1.2 二元运算的性质

例：I为整数集合，I上的二元运算⊕和∘定义为：对任何a,b∈I，a⊕b=a+b-1，a∘b=a+b-ab，求证：⊕和∘在I上是封闭的、可结合的，并且∘对⊕可分配。

证明：1)封闭性：任取a,b∈I，a+b-1∈I，所以a⊕b∈I。a+b-ab∈I，所以a∘b∈I。即⊕和∘在I上封闭。

2)可结合性：任取a,b,c∈I，

$$a\oplus(b\oplus c) = a+(b+c-1)-1 = (a+b-1)+c-1$$
$$=(a\oplus b)\oplus c$$

$$a\circ(b\circ c) = a+(b+c-bc)-a(b+c-bc)$$
$$=a+b+c-bc-ab-ac+abc$$
$$=(a+b-ab)+c-(a+b-ab)c =(a\circ b)\circ c$$

即⊕和∘在I上可结合。

3)证∘对⊕可分配：任取a,b,c∈I，

$$a\circ(b\oplus c) = a+(b+c-1)-a(b+c-1)$$
$$= a+b+c-1-ab-ac+a$$
$$= (a+b-ab)+(a+c-ac)-1$$
$$= (a\circ b)\oplus(a\circ c)$$

即∘对⊕可分配。

# 8.1.3 二元运算的特异元素

## ➢ 单位元

定义：设$\circ$为$S$上的二元运算，如果存在$e_l$（或$e_r$）$\in S$，使得对任意$x\in S$都有 $e_l \circ x = x$（或$x \circ e_r = x$），则称$e_l$（或$e_r$）是$S$中关于$\circ$运算的左（或右）单位元.

若$e\in S$关于$\circ$运算既是左单位元又是右单位元，则称$e$为$S$上关于$\circ$运算的单位元，单位元也叫做幺元.

- 实数集合R上的加法+运算，幺元是0；
  因为 $0+a=a+0=a$ ($a$为任意实数)
- 乘法×运算，幺元是1；
- 集合族上的并运算∪，幺元是Φ；
  因为 $\Phi\cup A=A\cup\Phi=A$ (A为任意集合)
- 交运算∩，幺元是全集E。
  因为 $E\cap A=A\cap E=A$

# 8. 1. 3 二元运算的特异元素

*Example* 22. 设 $S=\{\alpha,\beta,\gamma,\delta\}$, $*$ 运算由下表定义, 指出 $*$ 运算是否有左幺元, 右幺元?

| $*$ | $\alpha$ | $\beta$ | $\delta$ | $\gamma$ |
|---|---|---|---|---|
| $\alpha$ | $\delta$ | $\alpha$ | $\beta$ | $\gamma$ |
| $\beta$ | $\alpha$ | $\beta$ | $\delta$ | $\gamma$ |
| $\delta$ | $\alpha$ | $\beta$ | $\delta$ | $\gamma$ |
| $\gamma$ | $\delta$ | $\gamma$ | $\alpha$ | $\beta$ |

# 8. 1. 3 二元运算的特异元素

*Example* 22. 设 $S=\{\alpha,\beta,\gamma,\delta\}$, $*$ 运算由下表定义, 指出 $*$ 运算是否有左幺元, 右幺元?

| $*$ | $\alpha$ | $\beta$ | $\delta$ | $\gamma$ |
|---|---|---|---|---|
| $\alpha$ | $\delta$ | $\alpha$ | $\beta$ | $\gamma$ |
| $\beta$ | $\alpha$ | $\beta$ | $\delta$ | $\gamma$ |
| $\delta$ | $\alpha$ | $\beta$ | $\delta$ | $\gamma$ |
| $\gamma$ | $\delta$ | $\gamma$ | $\alpha$ | $\beta$ |

解: $\beta$ 和 $\delta$ 都是 $S$ 中关于 $*$ 运算的左幺元; $*$ 运算没有右幺元.

# 8.1.3 二元运算的特异元素

➢ 零元

定义：设$\circ$为 $S$ 上的二元运算, 如果存在$\theta_l$（或$\theta_r$）$\in S$，使得对任意 $x\in S$ 都有 $\theta_l\circ x=\theta_l$（或 $x\circ\theta_r=\theta_r$），则称$\theta_l$（或$\theta_r$）是 $S$ 中关于$\circ$运算的 左（或右）零元.

若$\theta\in S$关于$\circ$运算既是左零元又是右零元，则称$\theta$为 $S$ 上关于运算$\circ$的零元.

*Example* 24. 例如自然数集合上 0 是普通乘法的零元, 而加法没有零元.

*Example* 25. 指出幂集 $\mathscr{P}(S)$ 上, $\cup$ 运算和 $\cap$ 运算的零元.

解: $\cup$ 运算的零元是 $S$, $\cap$ 运算的零元是 $\varnothing$.

# 8.1.3 二元运算的特异元素

➢ 可逆元素及其逆元

定义：令 $e$ 为 $S$ 中关于运算$\circ$的单位元. 对于 $x\in S$，如果存在$y_l$（或 $y_r$）$\in S$ 使得 $y_l\circ x=e$（或 $x\circ y_r=e$），则称 $y_l$( 或 $y_r$ )是 $x$ 的 左逆元 ( 或右逆元 ).

关于$\circ$运算，若 $y\in S$ 既是 $x$ 的左逆元又是 $x$ 的右逆元，则称 $y$ 为 $x$ 的逆元. 如果 $x$ 的逆元存在，就称 $x$ 是可逆的.

*Example* 29. 例如, 在整数集合 $\mathbb{Z}$ 上, 加法的幺元是 0. 对任何整数, 它的加法逆元都存在, 即它的相反数 $-x$.

# 8.1.3 二元运算的特异元素

例：实数集合$R$上的+和×，$x \in R$

- 对加法+：$x^{-1} = -x$

  因为$e=0$，$x+(-x)=0$

- 对乘法×：$x^{-1}=1/x\ (x\neq 0)$

- 因为$e=1$，$x \times 1/x = 1$

- 从运算表找$x$的左逆元$x_L^{-1}$：

  在$x$列向下找到$e$后，再向左到左表头元素即是$x_L^{-1}$。

- 从运算表找$x$的右逆元$x_R^{-1}$：

  在$x$行向右找到$e$后，再向上到上表头元素即是$x_R^{-1}$。

| $\circ$ | S | R | A | L |
|---|---|---|---|---|
| S | S | R | A | L |
| R | R | A | L | S |
| A | A | L | S | R |
| L | L | S | R | A |

$x_R^{-1}$

$x_L^{-1}$

# 8.1.3 二元运算的特异元素

| 集合 | 运算 | 单位元 | 零元 | 逆元 |
|---|---|---|---|---|
| Z, Q, R | 普通加法+ | 0 | 无 | $X$ 的逆元 $-x$ |
| | 普通乘法× | 1 | 0 | $X$ 的逆元 $x^{-1}$ ($x^{-1}$属于给定集合) |
| $M_n$(R) | 矩阵加法+ | $n$阶全0矩阵 | 无 | $X$逆元$-X$ |
| | 矩阵乘法× | $n$阶单位矩阵 | $n$阶全0矩阵 | $X$的逆元 $X^{-1}$ （$X$是可逆矩阵） |
| $P(B)$ | 并∪ | ∅ | $B$ | ∅ 的逆元为 ∅ |
| | 交∩ | $B$ | ∅ | $B$ 的逆元为 $B$ |
| | 对称差⊕ | ∅ | 无 | $X$ 的逆元为 $X$ |

# 8.1.3 二元运算的特异元素

- **唯一性定理**

定理　设 $\circ$ 为 $S$ 上的二元运算，$e_l$ 和 $e_r$ 分别为 $S$ 中关于运算的左和右单位元，则 $e_l = e_r = e$ 为 $S$ 上关于 $\circ$ 运算的惟一的单位元.

证：　$e_l = e_l \circ e_r = e_l \circ e_r = e_r$

所以 $e_l = e_r$，将这个单位元记作 $e$. 假设 $e'$ 也是 $S$ 中的单位元，则有 $e' = e \circ e' = e$，惟一性得证.

证唯一性：假设有两个幺元 $e_1$、$e_2$，因为 $e_1$ 是幺元，$e_2 \in X$，所以 $e_1 \star e_2 = e_2$；又因 $e_2$ 是幺元，$e_1 \in X$，所以 $e_1 \star e_2 = e_1$；于是 $e_1 = e_2 = e$。即幺元是唯一的。

类似地可以证明关于零元的惟一性定理.

注：当 $|S| \geq 2$，单位元与零元是不同的；当 $|S| = 1$ 时，这个元素既是单位元也是零元.

# 8.1.3 二元运算的特异元素

设 $\circ$ 为 $A$ 上的二元运算, $e$ 和 $\theta$ 分别为 $\circ$ 运算的幺元和零元, 如果 $A$ 至少有两个元素, 则 $e \neq \theta$.

证: 用反证法. 假设 $e = \theta$, 则对 $\forall x \in A$ 有

$$
\begin{aligned}
x &= x \circ e && (e \text{ 是幺元}) \\
&= x \circ \theta && (e = \theta) \\
&= \theta && (\theta \text{ 是零元})
\end{aligned}
$$

此式说明 $A$ 中只有惟一的元素 $\theta$, 与 $A$ 中至少含有两个元素矛盾. □

- 当 $|X| > 1$，幺元与零元一定是不同的；
- 当 $|X| = 1$，这个集合中只包含一个元素，如果运算是封闭的，

| $\star$ | $a$ |
|---|---|
| $a$ | $a$ |

则这个元素既是幺元也是零元。

# 8.1.3 二元运算的特异元素

- **惟一性定理**

**定理** 设 $\circ$ 为 $S$ 上可结合的二元运算, $e$ 为该运算的单位元, 对于 $x \in S$ 如果存在左逆元 $y_l$ 和右逆元 $y_r$, 则有 $y_l = y_r = y$, 且 $y$ 是 $x$ 的惟一的逆元.

证 由 $y_l \circ x = e$ 和 $x \circ y_r = e$ 得

$$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r$$

令 $y_l = y_r = y$, 则 $y$ 是 $x$ 的逆元.

假若 $y' \in S$ 也是 $x$ 的逆元, 则

$$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y$$

所以 $y$ 是 $x$ 惟一的逆元.

说明：对于可结合的二元运算，可逆元素 $x$ 只有惟一的逆元，记作 $x^{-1}$.

# 8.1.3 二元运算的特异元素

## ➢ 惟一性定理

**定理** 设 $\circ$ 为 $S$ 上可结合的二元运算, $e$ 为该运算的单位元, 对于 $x \in S$ 如果存在左逆元 $y_l$ 和右逆元 $y_r$, 则有 $y_l = y_r = y$, 且 $y$ 是 $x$ 的惟一的逆元.

注意

对于给定的集合和二元运算来说,

- 如果幺元或零元存在, 一定是惟一的.
- 而逆元能否存在, 与元素有关. 有的元素有逆元, 有的元素没有逆元, 不同的元素对应着不同的逆元.
  - 一个元素的左逆元不一定等于它的右逆元.
  - 一个元素可以有左逆元不一定有右逆元.
  - 甚至一个元素的左 (右) 逆元不一定是惟一的.

# 8.1.3 二元运算的特异元素

- **消去律**

定义 设$\circ$为$V$上二元运算，如果$\forall\, x, y, z \in V$，

若 $x \circ y = x \circ z$，且 $x$不是零元，则 $y = z$

若 $y \circ x = z \circ x$，且 $x$ 不是零元，则 $y = z$

那么称$\circ$运算满足 消去律.

实例: Z, Q, R 关于普通加法和乘法满足消去律.

$M_n$(R) 关于矩阵加法满足消去律，但是关于矩阵乘法不满足消去律.

$Z_n$关于模 $n$ 加法满足消去律，当 $n$ 为素数时关于模 $n$乘法满足消去律. 当 $n$ 为合数时关于模 $n$ 乘法不满足消去律.

# 8.1.3 二元运算的特异元素

## ➢ 消去律

$Z_n$关于模 $n$ 加法满足消去律，当 $n$ 为素数时关于模 $n$乘法满足消去律. 当 $n$ 为合数时关于模 $n$ 乘法不满足消去律.

1. **关于模n的加法满足消去律：**
   - 对于模n的加法，如果 $a+b \equiv a+c \pmod{n}$，则可以通过减去$a$两边的同余式来得到 $b \equiv c \pmod{n}$。因此，模n的加法满足消去律。
2. **当n为素数时，关于模n的乘法满足消去律：**
   - 如果 $ab \equiv ac \pmod{n}$，其中$a$不是n的倍数，那么我们可以左边两边同乘以$a^{-1}$（$a^{-1}$是$a$的模n乘法逆元素），得到 $b \equiv c \pmod{n}$。这说明在模n的乘法下，当n是素数时，消去律成立。
3. **当n为合数时，关于模n的乘法不满足消去律：**
   - 如果n是合数，即可以分解为两个大于1的整数的乘积，例如$n=pq$，其中p和q是素数，那么在模n的乘法下，消去律不一定成立。例如，取 $a \equiv 0 \pmod{p}$ 和 $b \equiv 0 \pmod{q}$，则 $ab \equiv 0 \pmod{n}$。现在如果我们取 $c \equiv 1 \pmod{p}$ 和 $c \equiv 1 \pmod{q}$，则 $ac \equiv c \pmod{p}$ 和 $bc \equiv c \pmod{q}$，但 $ac \equiv bc \pmod{n}$。因此，消去律不成立。

# 8.1.3 二元运算的特异元素

| * | a | b | c |
|---|---|---|---|
| a | c | a | b |
| b | a | b | c |
| c | b | c | a |

| ∘ | a | b | c |
|---|---|---|---|
| a | a | a | a |
| b | b | b | b |
| c | c | c | c |

| · | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | c | c |
| c | c | c | c |

解：(1) * 运算满足交换律、结合律，不满足幂等律.

∘ 运算不满足交换律，满足结合律，满足幂等律.

· 运算满足交换律，满足结合律，不满足幂等律.

(2) * 运算的幺元为 $b$，没有零元，$a^{-1}=c$，$c^{-1}=a$，$b^{-1}=b$。

∘ 运算的幺元和零元都不存在，$a, b, c$ 均是左零元，没有可逆元素.

· 运算的单位元为 $a$，零元为 $c$，$a^{-1}=a$，$b, c$ 不是可逆元素。

# 8. 1. 3 二元运算的特异元素

例6 设$\circ$运算为 Q 上的二元运算，

$$\forall x, y \in Q, \quad x \circ y = x+y+2xy,$$

(1) $\circ$运算是否满足交换和结合律？说明理由.

(2) 求$\circ$运算的单位元、零元和所有可逆元.

解：(1) $\circ$运算可交换，可结合. 任取$x, y \in Q$,

$$x \circ y = x+y+2xy = y+x+2yx = y \circ x,$$

任取$x, y, z \in Q$,

$$(x \circ y) \circ z = (x+y+2xy) + z + 2(x+y+2xy)\, z$$

$$= x+y+z+2xy+2xz+2yz+4xyz$$

$$x \circ (y \circ z) = x + (y+z+2yz) + 2x(y+z+2yz$$

$$= x+y+z+2xy+2xz+2yz+4xyz$$

# 8. 1. 3 二元运算的特异元素

(2) 设∘运算的单位元和零元分别为 $e$ 和 θ，则对于任意 $x$ 有 $x \circ e = x$ 成立，即 $x+e+2xe = x \Rightarrow e = 0$

由于∘运算可交换，所以 0 是幺元.

对于任意 $x$ 有 $x \circ \theta = \theta$ 成立，即

$$x+\theta+2x\theta = \theta \Rightarrow x + 2x\theta = 0 \Rightarrow \theta = -1/2$$

给定 $x$，设 $x$ 的逆元为 $y$, 则有 $x \circ y = 0$ 成立，即

$$x+y+2xy = 0 \Rightarrow y=-\frac{x}{1+2x} \ (x \neq = -1/2)$$

因此当 $x \neq -1/2$时， $y=-\frac{x}{1+2x}$ 是 $x$ 的逆元.

# 8.1.3 二元运算的特异元素

- 例8 设 $A = \{a, b, c\}$, 构造 $A$ 上的二元运算* 使得 $a*b = c$, $c*b = b$, 且*运算是幂等的、可交换的，给出关于*运算的一个运算表，说明它是否可结合，为什么?

| * | a | b | c |
|---|---|---|---|
| a | a | c | □ |
| b | c | b | b |
| c | □ | b | c |

根据幂等律和已知条件$a*b = c$, $c*b = b$ 得到运算表

根据交换律得到新的运算表

方框 □ 可以填入$a, b, c$中任一选定的符号, 完成运算表

不结合，因为 (a*b)*b = c*b = b, a*(b*b) = a*b = c

# 8.1.3 二元运算的特异元素

1. 判断下列集合对所给的二元运算是否封闭。

（1）集合 $n\mathbf{Z}=\{n\times z \mid z\in\mathbf{Z}\}$ 关于普通的加法和普通乘法运算，其中 $n$ 是一个正整数。

2. 判断下列集合对所给的二元运算是否封闭。

（1）正实数集合 $\mathbf{R}^+$ 和*运算，其中*运算定义为：

$$\forall a,\ b\in\mathbf{R}^+,\ a*b=ab-a-b$$

（2）$A=\{a_1,\ a_2,\ \cdots,\ a_n\}$，$n\geq 2$。*运算定义为：

$$\forall a,\ b\in A,\ a*b=b$$

对于封闭的二元运算，判断它们是否满足交换律、结合律和等幂律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

# 8.1.3 二元运算的特异元素

1. 判断下列集合对所给的二元运算是否封闭。

（1）集合 $n\mathbf{Z}=\{n\times z \mid z\in\mathbf{Z}\}$ 关于普通的加法和普通乘法运算，其中 $n$ 是一个正整数。

**解**：（1）任意 $a,b\in Z$，

$n\times a+n\times b\in nZ$，所以对普通的加法运算封闭。

$n\times a\times(n\times b)=n^2\times a\times b\in nZ$，所以对普通的乘法运算封闭。

2. 判断下列集合对所给的二元运算是否封闭。

（1）正实数集合 $\mathbf{R}^+$ 和*运算，其中*运算定义为：

$$\forall a，b\in\mathbf{R}^+，a*b=ab-a-b$$

（2）$A=\{a_1，a_2，\cdots，a_n\}$，$n\geq 2$。*运算定义为：

$$\forall a，b\in A，a*b=b$$

对于封闭的二元运算，判断它们是否满足交换律、结合律和等幂律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

# 8.1.3 二元运算的特异元素

2. 判断下列集合对所给的二元运算是否封闭。

（1）正实数集合$\mathbf{R}^+$和*运算，其中*运算定义为：

$$\forall a，b\in\mathbf{R}^+，a*b=ab-a-b$$

（2）$A=\{a_1，a_2，\cdots，a_n\}$，$n\geq 2$。*运算定义为：

$$\forall a，b\in A，a*b=b$$

对于封闭的二元运算，判断它们是否满足交换律、结合律和等幂律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

解：（1）不封闭。例如$3*1=3\times1-1-3=3-1-3=-1$，$-1\notin R^+$ 。

（2）封闭。$\forall a，b\in A，a*b=b\in A$，所以*运算在$A$上是封闭的。

$\forall a，b,c\in\mathbf{R}^+$，　有：

$a*b=b$，而$b*a=a$，因为$a=b$不恒成立，即$a*b\neq b*a$，
所以$*$不满足交换律。

因为$(a*b)*c=a*c=a$，$a*(b*c)=a*b=a$，

所以$(a*b)*c=a*(b*c)$，所以$*$满足结合律。

又因为$a*a=a$，所以$*$满足等幂律。

设$e$为单位元，则因有$\forall a\in A$，$a*e=e*a=a$，即$a=e=a$，由$a$的任意性可知，单位元不存在。

# 8.1.3 二元运算的特异元素

4. **R** 为实数集合，定义以下六个函数 $f_1$，…，$f_6$。$\forall x$，$y \in \mathbf{R}$ 有

$$f_1(<x, y>) = x + y, \qquad f_2(<x, y>) = x - y,$$

$$f_3(<x, y>) = |x - y|, \qquad f_4(<x, y>) = xy,$$

$$f_5(<x, y>) = \min(x, y), \qquad f_6(<x, y>) = \max(x, y)$$

（1）指出哪些函数是 **R** 上的二元运算。

（2）若是 **R** 上的二元运算，说明是否可交换的、可结合的、等幂的？

# 8.1.3 二元运算的特异元素

设代数系统 $\langle A, *\rangle$, 其中 $A = \{a, b, c\}$, $A$ 上的二元运算 $*$ 定义如表: 试分析 $*$ 运算的封闭性, 交换性, 等幂性. $A$ 中关于 $*$ 是否有幺元和零元? 如有幺元, 每个元素是否有逆元? 如有, 求出逆元.

| $*$ | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | a | c |
| c | c | c | c |

解: 这些运算性质可直接从运算表看出:

- $*$ 运算是封闭的, 因为表中每个元素都属于 $A$.
- $*$ 运算可交换, 因运算表关于主对角线对称.
- $*$ 运算不等幂, 因运算表主对角线有的元素与所在行列表头元素不同.
- $*$ 运算有零元 $c$, 因为 $c$ 所在行列中的元素都是与它相同.
- $*$ 运算有幺元 $a$, 因为 $a$ 所在行列中的元素依次与表头行列一致.
- $a$ 和 $b$ 均以自身为逆元, 因为 $a$, $b$ 所在行和列交汇处的元素为幺元.

# 8.1.3 二元运算的特异元素

- **由运算表判别算律的一般方法**
- 交换律：运算表关于主对角线对称
- 幂等律：主对角线元素排列与表头顺序一致
- 消去律：所在的行与列中没有重复元素
- 单位元：所在的行与列的元素排列都与表头一致
- 零元：元素的行与列都由该元素自身构成
- $A$ 的可逆元：$a$ 所在的行中某列 (比如第 $j$ 列) 元素为 $e$，且第 $j$ 行 $i$ 列的元素也是 $e$，那么 $a$ 与第 $j$ 个元素互逆
- 结合律：除了单位元、零元之外，要对所有3个元素的组合验证表示结合律的等式是否成立

# 8.1.3 二元运算的特异元素

*Example* 32. 设 $\mathbb{N}_k = \{0, 1, 2, \cdots, k-1\}$, 在 $\mathbb{N}_k$ 定义运算 $+_k$ 如下: 对任意 $x, y \in \mathbb{N}_k$

$$x +_k y = \begin{cases} x + y, & x + y < k \\ x + y - k, & x + y \geqslant k \end{cases}$$

试分析 $\mathbb{N}_k$ 中的每个元素是否有逆元? 如有, 求出逆元.

解: 因为对任意 $x \in \mathbb{N}_k$, $x + 0 = x < k$, 所以

$$x +_k 0 = 0 +_k x = x + 0 = x,$$

故 0 是幺元.

对任意 $x \in \mathbb{N}_k$, 令 $x +_k y = 0$, 分两种情况讨论:

(1) 如果 $x + y < k$, 按运算 $+_k$ 的定义, 有 $x +_k y = x + y = 0$, 因 $x, y \in \mathbb{N}_k$, 可知 $x = y = 0$, 因此 0 以自身为逆元;

(2) 如果 $x + y \geqslant k$, 则有 $x +_k y = x + y - k = 0$, 解出 $y = k - x$. 即每个非 0 元素 $x$ 都有逆元 $k - x$. □

# 8.1.3 二元运算的特异元素

## 从运算表看运算的性质

对代数系统 $\langle A, *\rangle$, 其二元运算 $*$ 的性质可以根据运算表表现出来:

- 运算 $*$ 具有封闭性, 当且仅当运算表中的每个元素都属于 $A$.
- 运算 $*$ 具有可交换性, 当且仅当运算表关于主对角线是对称的.
- 运算 $*$ 具有等幂性, 当且仅当运算表的主对角线上的每一元素与它所在行 (列) 的表头元素相同.
- $A$ 中关于运算 $*$ 具有零元, 当且仅当该元素所对应的行和列中的元素都与该元素相同.
- $A$ 中关于运算 $*$ 具有幺元, 当且仅当该元素所对应的行和列依次与运算表的行和列相一致.
- 设 $A$ 中关于运算 $*$ 具有幺元, $a$ 和 $b$ 互逆, 当且仅当位于 $a$ 所在行和 $b$ 所在列的元素及 $b$ 所在行和 $a$ 所在列的元素都是幺元.

# 作业20

- 书上P226
- 9.10
- 9.12

# 8.2 代数系统

- 代数系统定义
- 同类型与同种的代数系统
- 子代数
- 积代数

# 8. 2. 1 代数系统定义

- 定义
- 非空集合 $S$ 和 $S$ 上 $k$ 个一元或二元运算 $f_1, f_2, \cdots, f_k$ 组成的系统称为一个代数系统, 简称代数，记做 $V=<S, f_1, f_2, \cdots, f_k>$.
- $S$ 称为代数系统的载体， $S$ 和运算叫做代数系统的成分. 有的代数系统定义指定了$S$中的特殊元素，称为代数常数, 例如二元运算的单位元.有时也将代数常数作为系统的成分.

# 8. 2. 1 代数系统定义

实例:

$<N,+>$, $<Z,+,\cdot>$, $<R,+,\cdot>$是代数系统，

$+$ 和 $\cdot$ 分别表示普通加法和乘法.

$<M_n(R),+,\cdot>$是代数系统，

$+$ 和 $\cdot$ 分别表示$n$ 阶 ($n\geq 2$) 实矩阵的加法和乘法.

$<Z_n,\oplus,\otimes>$是代数系统，$Z_n=\{0, 1, \ldots, n-1\}$，

$\oplus$ 和 $\otimes$ 分别表示模 $n$ 的加法和乘法，$\forall x,y\in Z_n$，

$$x\oplus y = (x+y) \bmod n，\quad x\otimes y = (xy) \bmod n$$

$<P(S),\cup,\cap,\sim>$ 也是代数系统，

$\cup$和$\cap$为并和交，$\sim$为绝对补

# 8. 2. 2 同类型与同种代数系统

- 定义 (1) 如果两个代数系统中运算的个数相同，对应运算的元数相同，且代数常数的个数也相同，则称它们是 同类型的 代数系统.
- (2) 如果两个同类型的代数系统规定的运算性质也相同，则称为 同种的 代数系统.
- 例1 $V_1 = <\mathrm{R}, +, \cdot, 0, 1>$,
- $V_2 = <M_n(\mathrm{R}), +, \cdot, \theta, E>$,
- $\theta$ 为 $n$ 阶全 0 矩阵，$E$ 为 $n$ 阶单位矩阵
- $V_3 = <P(B), \cup, \cap, \varnothing, B>$

# 8. 2. 2 同类型与同种代数系统

| $V_1$ | $V_2$ | $V_3$ |
|---|---|---|
| + 可交换, 可结合<br>· 可交换, 可结合<br>+ 满足消去律<br>· 满足消去律<br>· 对+可分配<br>+ 对 · 不可分配<br>+与 · 没有吸收律 | + 可交换, 可结合<br>· 可交换, 可结合<br>+ 满足消去律<br>· 满足消去律<br>· 对+可分配<br>+ 对 · 不可分配<br>+与 · 没有吸收律 | ∪可交换, 可结合<br>∩可交换, 可结合<br>∪不满足消去律<br>∩不满足消去律<br>∩对∪可分配<br>∪对∩可分配<br>∪与∩满足吸收律 |

- $V_1, V_2, V_3$是同类型的代数系统
- $V_1, V_2$是同种的代数系统
- $V_1, V_2$与$V_3$不是同种的代数系统

# 8.2.3 子代数

- 定义　设$V=<S, f_1, f_2, \ldots, f_k>$ 是代数系统，$B$ 是 $S$ 的非空子集，如果 $B$ 对 $f_1, f_2, \ldots, f_k$ 都是封闭的，且 $B$ 和 $S$ 含有相同的代数常数，则称 $<B, f_1, f_2, \ldots, f_k>$ 是 $V$ 的子代数系统，简称 子代数. 有时将子代数系统简记为 $B$.
- 实例　N是<Z,+> 和<Z,+,0>的子代数. N−{0}是<Z,+>的子代数，但不是<Z,＋,0>的子代数
- 说明：子代数和原代数是同种的代数系统
- 　　对于任何代数系统 $V$，其子代数一定存在.
- 1、N: 非负整数集合或自然数集合{0,1,2,3,...}2、N*或N+: 正整数集合{1,2,3,..}
- 3、Z: 整数集合{..,-1,0,1,...}
- 4、Q:有理数集合　5、Q+: 正有理数集合　6、Q-:负有理数集合
- 7、R: 实数集合(包括有理数和无理数 )8、R+: 正实数集合9、R-: 负实数集合

# 8.2.3 子代数

- 最大的子代数就是$V$本身. 如果$V$中所有代数常数构成集合 $B$，且 $B$ 对$V$ 中所有运算封闭，则 $B$ 就构成了$V$ 的最小的子代数.
- 最大和最小子代数称为$V$ 的平凡的子代数. 若 $B$ 是 $S$ 的真子集，则 $B$ 构成的子代数称为$V$ 的真子代数 .
- 例2 设$V=<Z,+,0>$，令 $nZ = \{ nz \mid z \in Z\}$，$n$ 为自然数，则 $nZ$ 是 $V$ 的子代数，当 $n = 1$ 和 0 时，$nZ$ 是 $V$ 的平凡子代数，其他的都是 $V$ 的非平凡真子代数.

# 8. 2. 3 子代数

- **积代数**

定义 设 $V_1=<S_1,\circ>$和 $V_2=<S_2,*>$是代数系统，其中 $\circ$ 和 $*$ 是二元运算. $V_1$ 与 $V_2$ 的 积代数 是$V=<S_1\times S_2,\cdot>$,

$\forall <x_1,y_1>, <x_2,y_2>\in S_1\times S_2$ ,

$$<x_1,y_1>\cdot<x_2,y_2>=<x_1\circ x_2, y_1*y_2>$$

例3 $V_1=<Z,+>$, $V_2=<M_2(R),\cdot>$, 积代数$<Z\times M_2(R),\circ>$

$\forall <z_1,M_1>, <z_2,M_2>\in Z\times M_2(R)$ ,

$$<z_1,M_1>\circ<z_2,M_2> = <z_1+z_2, M_1\cdot M_2>$$

$$<5,\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}>\circ<-2,\begin{pmatrix}2 & -1\\ 0 & 1\end{pmatrix}>=<3,\begin{pmatrix}2 & -1\\ 2 & 0\end{pmatrix}>$$

# 8.2.3 子代数

- **积代数的性质**

设 $V_1 = <S_1,\circ>$和 $V_2 = <S_2,*>$是代数系统，其中 $\circ$ 和 $*$是二元运算. $V_1$ 与 $V_2$ 的积代数是 $V=<S_1\times S_2,\cdot>$

(1) 若 $\circ$ 和 $*$ 运算是可交换的，那么$\cdot$ 运算也是可交换的

(2) 若 $\circ$ 和 $*$ 运算是可结合的，那么$\cdot$ 运算也是可结合的

(3) 若 $\circ$ 和 $*$ 运算是幂等的，那么$\cdot$ 运算也是幂等的

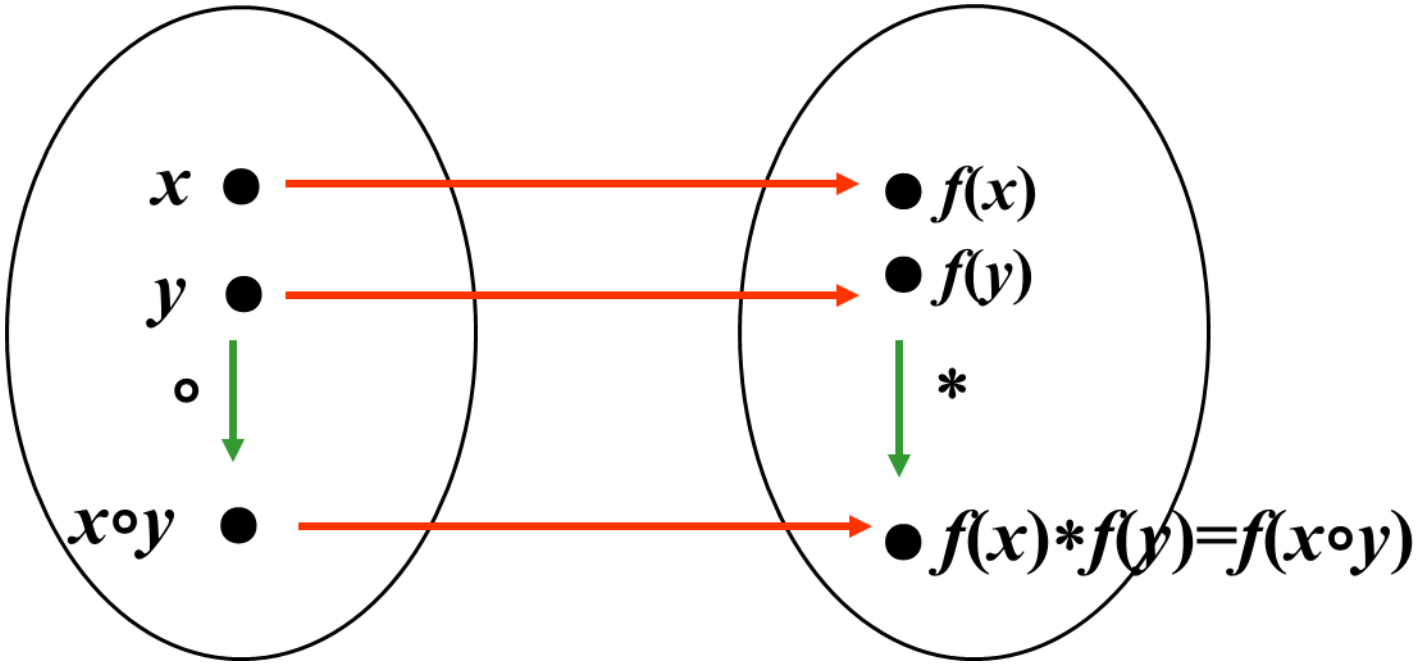
(4) 若 $\circ$ 和 $*$ 运算分别具有单位元 $e_1$ 和 $e_2$，那么$\cdot$ 运算也具有单位元$<e_1,e_2>$

(5) 若 $\circ$ 和 $*$ 运算分别具有零元 $\theta_1$ 和 $\theta_2$，那么$\cdot$ 运算也具有零元$<\theta_1, \theta_2>$

(6) 若 $x$ 关于 $\circ$ 的逆元为 $x^{-1}$, $y$ 关于 $*$ 的逆元为 $y^{-1}$，那么$<x,y>$关于$\cdot$ 运算也具有逆元$<x^{-1},y^{-1}>$

# 8. 2. 3 同态映射

- 定义 设 $V_1=<S_1,\circ>$和 $V_2=<S_2,*>$是代数系统，其中 $\circ$ 和 $*$是二元运算. $f: S_1\to S_2$, 且$\forall x,y\in S_1$, $f(x\circ y) = f(x) * f(y)$, 则称 $f$ 为$V_1$到 $V_2$ 的同态映射，简称同态.

- 

# 8. 2. 3 同态映射

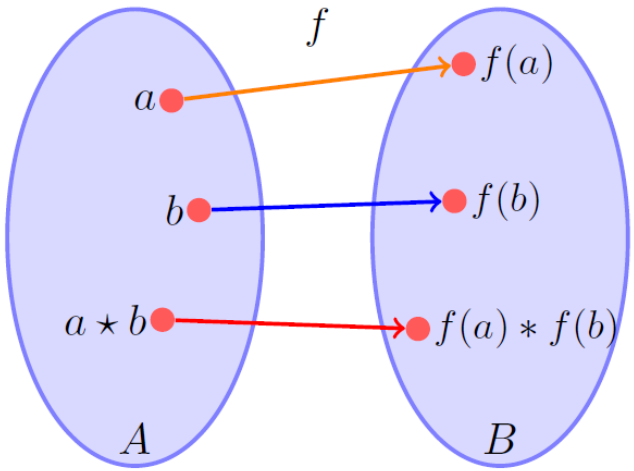
- 定义 设 $V_1=<S_1,\circ,\cdot>$和 $V_2=<S_2,*,\Diamond>$是代数系统，其中 $\circ$和 $*$是二元运算. $f: S_1\to S_2$, 且$\forall x,y\in S_1$
- $f(x\circ y)=f(x)*f(y)$， $f(x\cdot y)=f(x)\Diamond f(y)$
- 则称 $f$ 为$V_1$到 $V_2$ 的同态映射，简称同态.

- 设 $V_1=<S_1,\circ,\cdot,\Delta>$和 $V_2=<S_2,*,\Diamond,\nabla>$是代数系统，其中$\circ$ 和 $*$ 是二元运算. $\Delta$ 和 $\nabla$是一元运算， $f: S_1\to S_2$, 且$\forall x,y\in S_1$
- $f(x\circ y)=f(x)*f(y)$, $f(x\cdot y)=f(x)\Diamond f(y)$, $f(\Delta x)=\nabla f(x)$
- 则称 $f$ 为$V_1$到 $V_2$ 的同态映射，简称同态.

# 8. 2. 3 同态映射

**Definition 76.** 设 $\langle A, \star\rangle$ 和 $\langle B, *\rangle$ 是两个代数系统, $\star$ 和 $*$ 分别是 $A$ 和 $B$ 上的二元运算. 如果存在映射 $f: A \longmapsto B$, 对任意 $a_1, a_2 \in A$, 有

$$f(a_1 \star a_2) = f(a_1) * f(a_2)$$




(1) 称 $f$ 是 $\langle A, \star\rangle$ 到 $\langle B, *\rangle$ 的一个同态映射 (homomorphism), 简称同态;

(2) 称 $\langle A, \star\rangle$ 同态于 $\langle B, *\rangle$, 记作 $A \sim B$;

(3) 称 $\langle f(A), *\rangle$ 为 $\langle A, \star\rangle$ 的一个同态象 (image under homomorphism). 其中

$$f(A) = \{x \mid x = f(a),\ a \in A\} \subseteq B.$$

# 8.2.3 同态映射

- 同态映射如果是单射，则称为单同态；
- 如果是满射，则称为 满同态，这时称 $V_2$ 是 $V_1$ 的同态像，记作 $V_1 \sim V_2$；
- 如果是双射，则称为 同构，也称代数系统 $V_1$ 同构于$V_2$，记作 $V_1 \cong V_2$ .
- 对于代数系统 $V$，它到自身的同态称为自同态.

$f$ 是 $<X,\bigstar>$ 到 $<X,\bigstar>$ 的同态(同构)

- 类似地可以定义单自同态、满自同态和自同构.

# 8. 2. 3 同态映射

- 例1 $V=<R^*,\cdot>$, 判断下面的哪些函数是$V$ 的同态?
- (1) $f(x)=|x|$ (2) $f(x)=2x$ (3) $f(x)=x^2$
- (4) $f(x)=1/x$ (5) $f(x)= -x$ (6) $f(x)=x+1$
- 解 (2) , (5), (6) 不是同态.
- (1) 是同态， $f(x\cdot y) = |x\cdot y| = |x| \cdot |y| = f(x) \cdot f(y)$
- (3) 是同态， $f(x\cdot y) = (x\cdot y)^2 = x^2 \cdot y^2 = f(x) \cdot f(y)$
- (4) 是同态， $f(x\cdot y) = 1/(x\cdot y) =1/x \cdot 1/y = f(x) \cdot f(y)$

# 8.2.3 同态映射

- 代数系统间的同构关系 ≅ 是等价关系，满足自反性、对称性、传递性.
- $N_k$上的运算$+_k$和$\times_k$：

❖ 设 $I$ 是整数集合，$R$ 是 $I$ 上模 k (k是正整数)同余关系，因 $R$ 是 $I$ 上等价关系，所以得商集 $I/R$，将 $I/R$ 记作$N_k$，即：$N_k=\{[0],[1],[2],\ldots,[k-1]\}$

❖ 在 $N_k$ 上定义运算 $+_k$ 和 $\times_k$，我们分别称之为以 $k$ 为模的加法和乘法。定义为：

任取$[x],[y]\in N_k$，$[x]+_k[y]=[(x+y)(\mathrm{mod}\ k)]$；

$[x]\times_k[y]=[(x\times y)(\mathrm{mod}\ k)]$

❖ 为了方便，将$N_k=\{[0],[1],[2],\ldots,[k-1]\}$简记成：

$N_k=\{0,1,2,\ldots,k-1\}$

# 8.2.3 同态映射

- 代数系统间的同构关系 $\cong$ 是等价关系，满足自反性、对称性、传递性.

证: ① 设任意 $\langle A,*\rangle \in G$, 令 $f: A \longmapsto A$, $f(a)=a$, $a \in A$. 从而

$$\langle A,*\rangle \cong \langle A,*\rangle.$$

即同构关系是自反的.

② 设 $\langle A,*\rangle \cong \langle B,\star\rangle$, 那么存在双射 $f: A \longmapsto B$, 故 $f^{-1}: B \longmapsto A$ 也是双射, 所以

$$\langle B,\star\rangle \cong \langle A,*\rangle.$$

因而该关系是对称的.

③ 设 $\langle A,*\rangle \cong \langle B,\star\rangle$, $\langle B,\star\rangle \cong \langle C,\oplus\rangle$, 则存在双射 $f: A \longmapsto B$ 和 $g: B \longmapsto C$, 那么 $g \circ f: A \longmapsto C$ 也是双射, 所以

$$\langle A,*\rangle \cong \langle C,\oplus\rangle.$$

因而该关系是传递的.

因此, 同构关系是等价关系. □

# 8. 2. 3 同态映射

设 $A=\{1,2,3\}$, $\overline{A}=\{4,5,6\}$. $A$ 与 $\overline{A}$ 的代数运算 $\star$ 与 $*$ 分别为

| $\star$ | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 3 | 3 | 3 |
| 2 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 |

| $*$ | 4 | 5 | 6 |
|---|---|---|---|
| 4 | 6 | 6 | 6 |
| 5 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 |

那么

$$1 \longrightarrow 4, \quad 2 \longrightarrow 5, \quad 3 \longrightarrow 6$$

是一个 $A$ 与 $\overline{A}$ 间的同构映射. 因为

$$a \star b = 3 \longrightarrow 6 = \overline{a} * \overline{b}.$$

☞ $A$ 同 $\overline{A}$ 没有什么本质上的区别, 惟一的区别只是命名的不同而已.

代数系统 $\langle B, \oplus\rangle$, 和 $\langle C, *\rangle$ 都是与 $\langle A, \star\rangle$ 同构的:

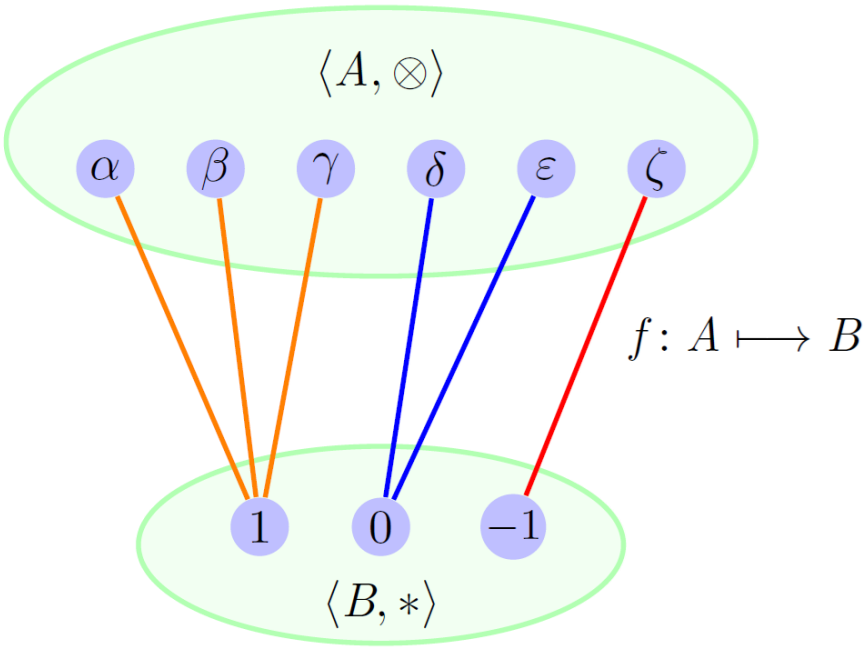
**研究同构的意义**

假定对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说, $A$ 与 $\overline{A}$ 同构. 那么

- 对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说, $A$ 与 $\overline{A}$ 这两个集合, 抽象地来看, 没有什么区别 (只有命名上的不同).
- 若一个集合有一个只与这个集合的代数运算有关的性质, 那么另一个集合有一个完全相同的性质. (比如结合律, 交换律等.)

# 8. 2. 3 同态映射

$$f(\alpha) = f(\beta) = f(\gamma) = 1,\ f(\delta) = f(\varepsilon) = 0,\ f(\zeta) = -1:$$




例如,

$$\beta \otimes \zeta = \varepsilon, \quad 1 * (-1) = 0;$$

$$f(\beta \otimes \zeta) = f(\varepsilon) = 0 = 1 * (-1) = f(\beta) * f(\zeta).$$

# 8. 2. 3 同态映射

- 普通的映射讨论的是两个集合 $A$ 和 $B$ 的关系;
- 同态讨论的是与代数运算也发生关系的映射. 即两个代数系统之间的联系.
- 若 $f$ 是 $\langle A,\star\rangle$ 到 $\langle B,*\rangle$ 的一个同态映射, 则任意 $a_1, a_2 \in A$, 只要

$$a_1 \longrightarrow b_1, \qquad a_2 \longrightarrow b_2,$$

就有

$$a_1 \star a_2 \longrightarrow b_1 * b_2.$$

**例如代数系统 $<N_4, +_4>$:**

$N_4=\{0,1,2,3\}$

**任何 $x,y \in N_4$, $x +_4 y = (x+y)(\mathrm{mod}\ 4)$**

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

# 8.2.3 同态映射

$<N_4,+_4>$

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

证明

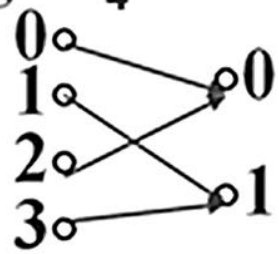
$<N_4, +_4> \backsim <B,\oplus>$

$<B, \oplus>$

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

构造映射

$g: N_4 \to B$




$g(1+_4 2)=g(3)=1$

$g(1)\oplus g(2) =1\oplus 0=1$

于是 $g(1+_4 2)=g(1)\oplus g(2)$

$g(2+_4 2)=g(0)=0$

$g(2)\oplus g(2)=0\oplus 0=0$

于是 $g(2+_4 2)=g(2)\oplus g(2)$

其余类似可以验证，因幺元不需验证，所以共需验证9个式子，然后可得出 $N_4 \backsim B$

# 8.2.3 同态映射

例：证明$<N_4,+_4>$与$<X,\circ>$同构。

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\circ$ | S | R | A | L |
|---|---|---|---|---|
| S | S | R | A | L |
| R | R | A | L | S |
| A | A | L | S | R |
| L | L | S | R | A |

构造映射

$N_4 \xrightarrow{f} X$

$0 \circ \longrightarrow \circ S$

$1 \circ \longrightarrow \circ R$

$2 \circ \longrightarrow \circ A$

$3 \circ \longrightarrow \circ L$

$f$是双射

$f(1+_4 2)=f(3)=L$

$f(1)\circ f(2)=R\circ A=L$

于是$f(1+_4 2)=f(1)\circ f(2)$

$f(2+_4 2)=f(0)=S$

$f(2)\circ f(2)=A\circ A=S$

于是$f(2+_4 2)=f(2)\circ f(2)$

其余式子可类似验证，最后可得出$N_4 \cong X$

# 8.2.3 同态映射

注意：代数系统$<X,\star>$和$<Y,\circ>$同构的必要条件：

1. $X$和$Y$的基数相同，即$K[X]=K[Y]$。
2. 运算$\star$和$\circ$是同类型的。
3. 存在双射$f:X\to Y$，且满足同构关系式。

❖ 并不是所有的双射$f:X\to Y$都满足同构关系式。

在构造双射时，要注意：
幺元与幺元对应；零元与零元对应；
逆元也要相互对应。

# 8.2.3 同态映射

- 含有两个运算的代数系统的同构

令 $<X,+,\times>$ 和 $<Y,\oplus,\blacklozenge>$ 是含有两个运算的代数系统，其中 $+$、$\times$、$\oplus$、$\blacklozenge$ 都是二元运算，如果存在双射 $f: X\to Y$，使得对任何 $x_1, x_2 \in X$，满足

$f(x_1+x_2)=f(x_1)\oplus f(x_2)$。（注意：$+$与$\oplus$对应）

$f(x_1\times x_2)=f(x_1)\blacklozenge f(x_2)$。（注意：$\times$与$\blacklozenge$对应）

则称这两个代数系统同构。

# 8.2.3 同态映射

(1) 如果 $f$ 是 $\langle A, *\rangle$ 到 $\langle A, *\rangle$ 的一个同态, 则称 $f$ 为自同态.

(2) 如果 $g$ 是 $\langle A, *\rangle$ 到 $\langle A, *\rangle$ 的一个同构, 则称 $g$ 为自同构.

设 $A = \{1, 2, 3\}$, 代数运算 $\star$ 由下表给定.

| $\star$ | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 3 | $\boxed{3}$ | 3 |
| 2 | $\boxed{3}$ | 3 | 3 |
| 3 | 3 | 3 | 3 |

那么

$$f: 1 \longrightarrow 2,\ 2 \longrightarrow 1,\ \boxed{3 \longrightarrow 3}$$

是一个对于 $\star$ 来说的 $A$ 的自同构.

# 8. 2. 3 同态映射

- 例2 设$V=<Z,+>$，$\forall a\in Z$，令
- $f_a$：$Z\to Z$，$f_a(x)=ax$
- 那么 $f_a$是$V$的自同态.
- 因为$\forall x,y\in Z$，有
- $f_a(x+y) = a(x+y) = ax+ay = f_a(x)+f_a(y)$
- 当 $a = 0$ 时称 $f_0$为零同态；
- 当$a=\pm1$时，称 $f_a$为自同构； $a=\pm1$ 时才是双射的
- 除此之外其他的 $f_a$ 都是单自同态（不是满射）

# 8. 2. 3 同态映射

例3 设$V_1$=<Q,+>, $V_2$= <Q*,·>，其中Q*= Q–{0}，令

$$f: \ Q \to Q^*, f(x)=e^x$$

那么 $f$ 是$V_1$到$V_2$的同态映射，因为$\forall x, y \in Q$，有

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

不难看出 $f$ 是单同态.

# 8. 2. 3 同态映射

- 例4 $V_1$=<Z,+>，$V_2$=<$Z_n$,⊕ >，$Z_n$={0,1, … , $n$-1}, ⊕ 是模 $n$ 加. 令
- $f$: Z→$Z_n$，$f(x) = (x)\bmod n$

  则 $f$ 是$V_1$到 $V_2$ 的满同态. ∀$x$, $y$∈Z有
- $f(x+y) = (x+y)\bmod n$
- $= (x)\bmod n \oplus (y)\bmod n$
- $= f(x) \oplus f(y)$

# 8. 2. 3 同态映射

例5 设 $V=<Z_n,\oplus>$，可以证明恰有 $n$ 个$G$ 的自同态，

$f_p$： $Z_n \to Z_n$,

$f_p(x) = (px) \bmod n$， $p = 0,1, \ldots, n-1$

例如 $n = 6$, 那么

$f_0$为零同态；

$f_1$与 $f_5$为同构；

$f_2$ 与 $f_4$的同态像是{ 0, 2, 4 }；

$f_3$ 的同态像是{ 0, 3 }.

# 8. 2. 3 同态映射

- **同态映射保持运算的算律**

设$V_1$,$V_2$是代数系统. o,*是$V_1$上的二元运算，o',*'是$V_2$上对应的二元运算，如果 $f$: $V_1 \to V_2$是满同态，那么

(1)若o运算是可交换的（可结合、幂等的），则o'运算也是可交换的（可结合、幂等的）.

(2) 若o运算对*运算是可分配的，则o'运算对*'运算也是可分配的;

(3) 若o 和*运算是可吸收的，则 o'和*'运算也是可吸收的。

# 8.2.3 同态映射

- **同态映射保持运算的特异元素**

(4) 若$e$为x运算的单位元，则 $f(e)$为y运算的单位元.

证明：任取$y\in Y$，因 $f:X\to Y$ 是满射，所以存在 $x\in X$，使得 $y=f(x)$。而

$$y\oplus f(e_\star)=f(x)\oplus f(e_\star)=f(x\star e_\star)=f(x)=y$$

$$f(e_\star)\oplus y=f(e_\star)\oplus f(x)=f(e_\star\star x)=f(x)=y$$

# 8. 2. 3 同态映射

- **同态映射保持运算的特异元素**

(4) 若$e$为x运算的单位元，则 $f(e)$为y运算的单位元.

(5) 若 θ为x运算的零元，则 $f(\theta)$ 为y运算的零元.

证明：任取$y\in Y$，因 $f:X\to Y$ 是满射，所以存在 $x\in X$，使得 $y=f(x)$。而

$$y\oplus f(\theta_\star)=f(x)\oplus f(\theta_\star)=f(x\star\theta_\star)=f(\theta_\star)$$

$$f(\theta_\star)\oplus y=f(\theta_\star)\oplus f(x)=f(\theta_\star\star x)=f(\theta_\star)$$

所以$f(\theta_\star)$是$<Y,\oplus>$中的零元。即$f(\theta_\star)=\theta_\oplus$。

# 8. 2. 3 同态映射

- **同态映射保持运算的特异元素**

(4) 若$e$为$\circ$ 运算的单位元，则 $f(e)$为$\circ'$运算的单位元.

(5) 若 $\theta$为$\circ$ 运算的零元，则 $f(\theta)$ 为$\circ'$运算的零元.

(6) 设 $u\in V_1$，若 $u^{-1}$ 是 $u$ 关于$\circ$运算的逆元，则 $f(u^{-1})$ 是 $f(u)$关于$\circ'$运算的逆元。

证明：任取$y\in Y$，因 $f:X\to Y$ 是满射，所以存在 $x\in X$，使得 $y=f(x)$。(往证 $y\oplus f(x^{-1})=e_\oplus$ 和 $f(x^{-1})\oplus y=e_\oplus$)

设运算★的幺元$e_\star$，运算⊕的幺元$e_\oplus$，于是有$f(e_\star)=e_\oplus$。

$y\oplus f(x^{-1})=f(x)\oplus f(x^{-1})=f(x\star x^{-1})=f(e_\star)=e_\oplus$

$f(x^{-1})\oplus y=f(x^{-1})\oplus f(x)=f(x^{-1}\star x)=f(e_\star)=e_\oplus$

所以 $y^{-1}=(f(x))^{-1}=f(x^{-1})$。

# 8.2.3 同态映射

- **同态映射的性质**
- 说明:
- 上述性质仅在满同态时成立，如果不是满同态，那么相关性质在同态像中成立.
- 如果是满射，则称为 满同态，这时称 $V_2$是 $V_1$的同态像
- 同态映射不一定能保持消去律成立.
- 例如 $f: Z \to Z_n$ 是 $V_1=<Z,\cdot>$ 到 $V_2=<Z_n,\otimes>$的同态，$f(x)=(x) \bmod n$, $V_1$中满足消去律，但是当 $n$ 为合数时，$V_2$中不满足消去律.

# 8.2.3 同态映射

- 同态代数系统的运算性质保持

代数系统 $<X,\star>$ 与 $<Y,\oplus>$ 同态，$f$：$X\to Y$ 是同态映射，如果$<X,\star>$中$\star$满足交换、结合、有幺元、有零元、每个元素可逆，则 $<f(X),\oplus>$ 中 $\oplus$ 也满足上述性质。

❖证明的方法与前一样，所不同的是，不是在$Y$中取元素，而是在值域$f(X)$中取元素。因为$f$不一定是满射的。

❖由于同态关系$\backsim$不满足对称性，所以在同态的代数系统中运算性质的保持只是单向的。即$Y$中$\oplus$有的性质$X$中的$\star$不一定有。

# 8. 2. 3 同态映射

- 例6 设$V_1$=<Q,+> ，$V_2$=<Q*,·>，其中 Q 为有理数集合，Q*=Q–{0}，+ 和 · 分别表示普通加法和乘法.
- 证明不存在 $V_2$ 到 $V_1$ 的同构.

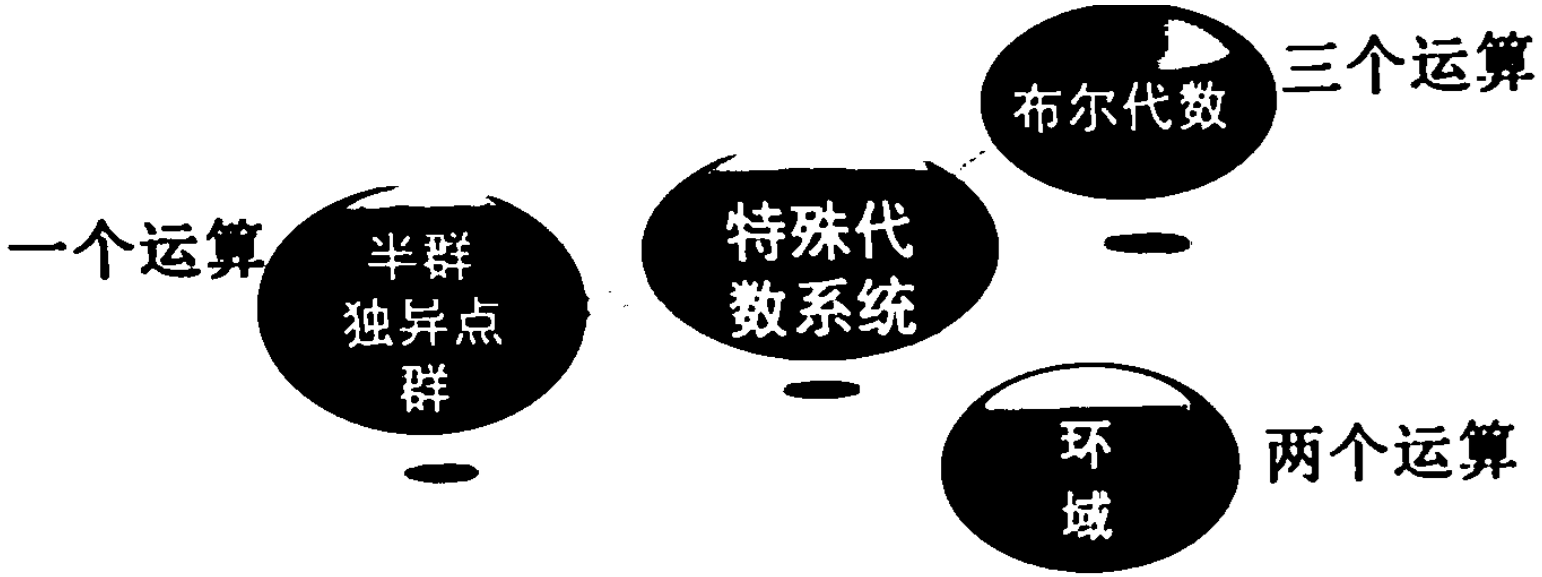
证 假设 $f$ 是 $V_2$ 到 $V_1$ 的同构，那么有$f$: $V_2 \to V_1$，$f(1)=0$. 于是有

$$f(-1)+f(-1) = f((-1)(-1))= f(1)=0$$

从而 $f(-1)=0$，又有 $f(1)=0$，这与 $f$ 的单射性矛盾.

# 8.3 几个典型的代数系统

- 8.3.1 半群、独异点与群
- 8.3.2 环与域




如果集合 $S$ 上的二元运算 $*$ 是封闭的, 则称代数系统 $\langle S, *\rangle$ 为广群 (groupoid). 也称为群坯.

# 8.3.1 半群、独异点与群

定义　设$V=<S,\circ>$是代数系统，$\circ$为二元运算.

(1) 如果$\circ$是封闭可结合的，则称$V=<S,\circ>$为半群.

(2) 如果半群$V=<S,\circ>$中的二元运算含有幺元，则称$V$为含幺半群，也可叫作独异点. 为了强调幺元$e$的存在，有时将独异点记为$<S,\circ,e>$.

(3) 如果半群$V=<S,\circ>$ (独异点$V=<S,\circ,e>$) 中的二元运算$\circ$是可交换的，则称$V$为可交换半群 (可交换独异点).

例：$<R,+>$，$<N,\times>$，$<P(E),\cap>$，$<P(E),\oplus>$ 都是可交换半群，亦是可交换独异点。

# 8.3.1 半群、独异点与群

设 $S=\{a, b, c\}$, 定义 $S$ 上的运算 $*$ 如表所示, 验证 $\langle S, *\rangle$ 是否为半群.

| $*$ | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | a | b | c |
| c | a | b | c |

解: 从运算可看出运算 $*$ 是封闭的.

另外 $a, b, c$ 皆为左幺元, 所以, 对任意 $x, y, z \in S$, 均有

$$x*(y*z)=y*z=(x*y)*z$$

所以 $*$ 运算是可结合的. 从而 $\langle S, *\rangle$ 是半群. □

☞ 代数系统 $\langle \mathbb{N}^+, -\rangle$ 和 $\langle \mathbb{R}, /\rangle$ 是半群吗? 这里 $\mathbb{N}^+$ 为正整数集, $\mathbb{R}$ 为实数集, $-$ 和 $/$ 是普通的减法和除法.

## 子半群

**Theorem 36.** 设 $\langle S, *\rangle$ 为一半群, $B \subseteq S$ 且 $*$ 在 $B$ 上封闭, 那么 $\langle B, *\rangle$ 也是一个半群. 通常称 $\langle B, *\rangle$ 为 $\langle S, *\rangle$ 的子半群.

# 8.3.1 半群、独异点与群

<N,+>、<R,×>、<P(E),∩>、<P(E),⊕>
是否是半群？是否是独异点？

<R,÷>、 <N,->是否是半群？是否是独异点？

# 8.3.1 半群、独异点与群

<N,+>、<R,×>、<P(E),∩>、<P(E),⊕>是否是半群？是否是独异点？

“+”法运算在自然数集合N上是封闭的、并且“+”法运算是可结合的，所以<N,+>是半群。

同样道理，<R,×>、<P(E),∩>、<P(E),⊕> 均是半群。

<N,+>的幺元是 0；<R,×>的幺元是 1；<P(E),∩>的幺元是 E；<P(E),⊕>的幺元是 Φ。 所以它们都是独异点。

<R,÷>、 <N,->是否是半群？是否是独异点？

因为“÷”、“-”均不满足结合律，所以<R,÷>、<N,->不是半群，更不是独异点

# 8.3.1 半群、独异点与群

实例

(1) $<Z^+,+>$,$<N,+>$,$<Z,+>$,$<Q,+>$,$<R,+>$都是可交换半群，除了$<Z^+,+>$外都是可交换独异点，+是普通加法.

(2) 设 $n$ 是大于1的正整数，$<M_n(R),\cdot>$是半群与独异点，其中 · 表示矩阵乘法.

(3) $<\Sigma^*,\circ>$是半群和独异点，其中$\Sigma$是有穷字母表，$\circ$表示连接运算，幺元是空串$\lambda$.

(4) $<P(B),\oplus>$为半群与独异点，其中$\oplus$为集合的对称差运算.

(5) $<Z_n, \oplus>$为半群与独异点，其中 $Z_n=\{0,1, \ldots, n-1\}$，$\oplus$ 为模 $n$ 加法.

# 8.3.1 半群、独异点与群

例：考察代数系统 $<N_6,+_6>$，$N_6=\{0,1,2,3,4,5\}$，根据$<N_6,+_6>$的定义，可以算出$<N_6,+_6>$的运算表如右图。问：$<N_6,+_6>$是否是独异点？

| $+_6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

解：从运算表可以看出，$+_6$运算在集合 $N_6=\{0,1,2,3,4,5\}$ 上是封闭的；幺元是 0；

可以验算，$+_6$ 运算在集合 $N_6$ 上是可结合的。

例如 $(2+_6 3)+_6 4=5+_6 4=3$，$2+_6(3+_6 4)=2+_6 1=3$，其它可类似验算。

所以 $<N_6,+_6>$ 是独异点。

# 8.3.1 半群、独异点与群

5、子半群

<S,★>是个半群，B⊆S，如果★在B上封闭，则称<B,★>是 <S,★>的子半群。

例：<N,+> 是 <I,+> 的子半群

6、子独异点

<M,★>是个独异点，B⊆ M，如果★在B上封闭，且幺元 e∈B，则称<B,★>是<M,★>的子独异点。

例：<I,+> 是 <R,+> 的子独异点。

# 8.3.1 半群、独异点与群

设<M,★>是可交换独异点，A是M中所有幂等元构成的集合，则<A,★>是<M,★>的子独异点。

# 8.3.1 半群、独异点与群

- **元素的幂运算**

设$V=<S, \circ>$为半群，对任意 $x\in S$，规定：

$$x^1 = x$$

$$x^{n+1} = x^n \circ x \qquad n\in \mathrm{Z}^+$$

在独异点$V=<S,\circ,e>$中，对任意 $x\in S$ ，规定:

$$x^0=e,$$

$$x^{n+1}=x^n\circ x \qquad n\in \mathrm{N}$$

幂运算规则：

$$x^n \circ x^m = x^{n+m}$$

$$(x^n)^m= x^{nm} \qquad m, n\in \mathrm{Z}^+$$

证明方法：数学归纳法

# 8.3.1 半群、独异点与群

设 $\langle S,*\rangle$ 是一个独异点，对于任意 $a,b\in S$，若 $a,b$ 均有逆元，则

(1) $(a^{-1})^{-1}=a$;

(2) $a*b$ 有逆元，且 $(a*b)^{-1}=b^{-1}*a^{-1}$.

证: ① 因 $a^{-1}$ 和 $a$ 为互为逆元，直接得到结论.

② 必须证明两种情况:

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

和

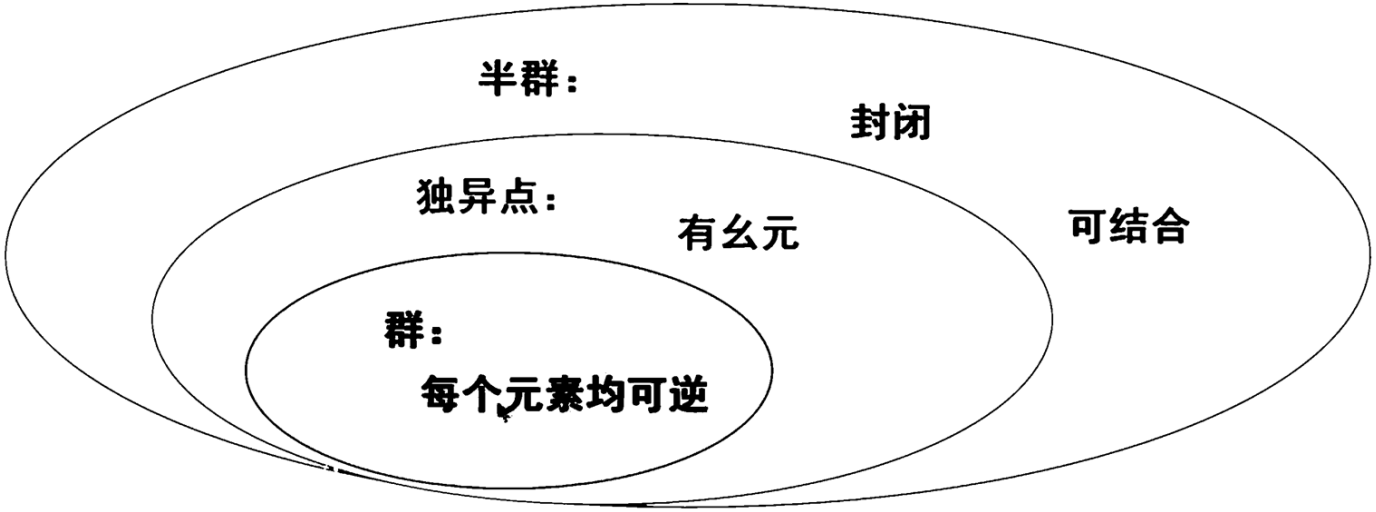
$$(b^{-1}*a^{-1})*(a*b)=e$$

利用结合律容易得出.

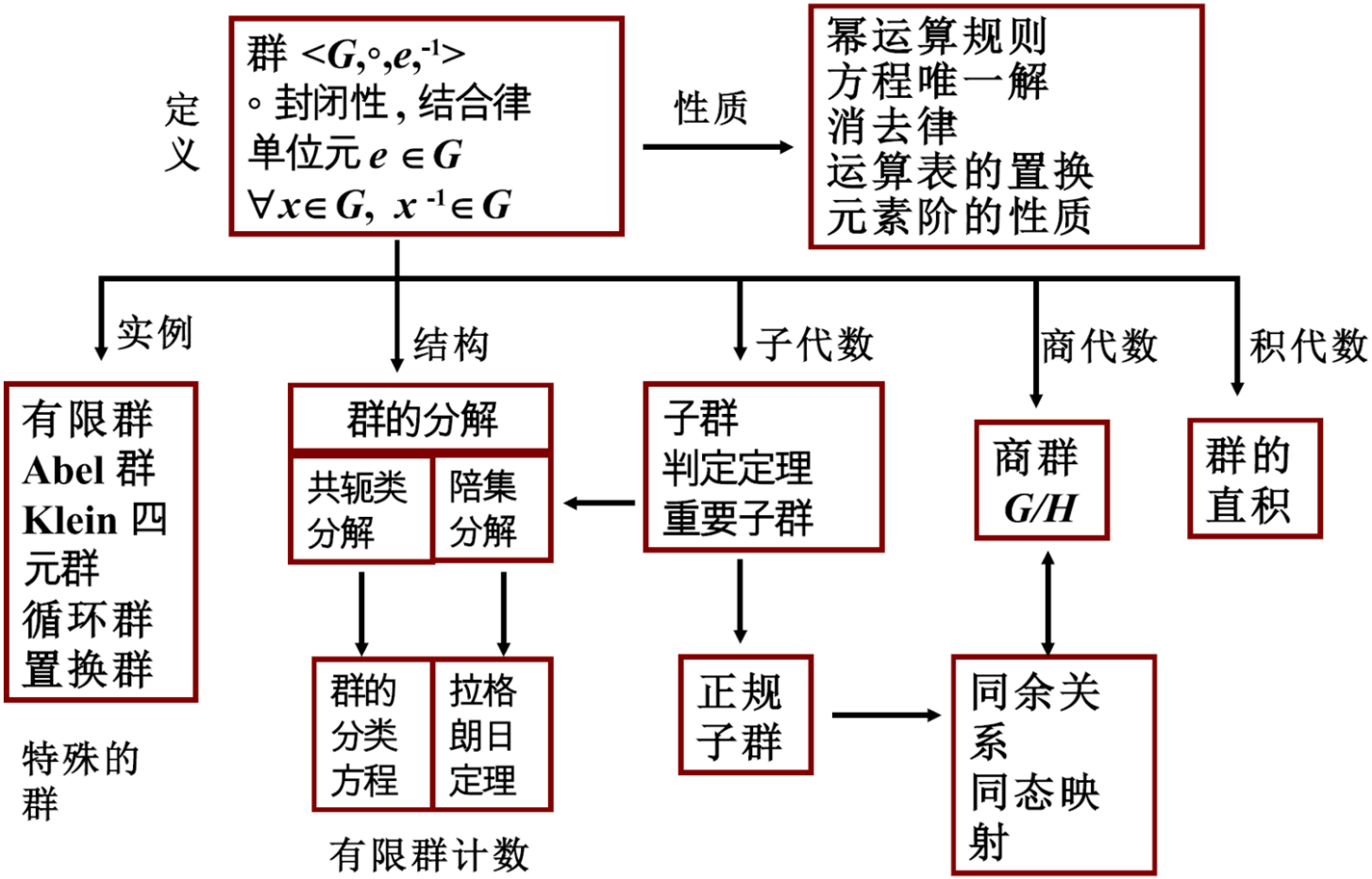
# 8.3.1 半群、独异点与群

定义 设<$G$,∘ >是代数系统，∘ 为二元运算. 如果∘ 运算是可结合的，存在单位元 $e \in G$，并且对 $G$ 中的任何元素 $x$ 都有 $x^{-1} \in G$，则称 $G$ 为 群.

群是抽象代数中最重要的代数系统。



# 8.3 几个典型的代数系统




1

# 8.3 几个典型的代数系统

- 设R是非空集合A上的等价关系，以R的不交的等价类为元素的集合称为A在R下的商集(等价类分类的结果)，记作A/R，即

$$A/R=\{[a]_R \mid a \in A\}$$

- 积代数

积代数的一个经典例子是直积 $\mathbb{R}^2$，即二维实数向量空间。考虑 $\mathbb{R}^2$ 中的元素为二维向量 $(x, y)$，并定义向量的加法和标量乘法：

- **加法：** $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
- **标量乘法：** $c \cdot (x, y) = (c \cdot x, c \cdot y)$，其中 $c$ 是实数。

这样定义的 $\mathbb{R}^2$ 成为一个实数域上的向量空间，同时也是一个代数。现在，考虑 $\mathbb{R}^2$ 中的元素除了向量加法和标量乘法外，还有逐分量的乘法运算：

- **逐分量乘法：** $(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2)$

这样构成的 $\mathbb{R}^2$ 对于向量的逐分量乘法运算封闭，因此成为一个积代数。

# 8.3 几个典型的代数系统

- 同余关系

**定义：** 对于给定的整数 $a$、$b$ 和正整数 $m$，如果 $m$ 能整除 $a-b$，即 $(a-b)$ 能被 $m$ 整除，则称 $a$ 与 $b$ 在模 $m$ 意义下是同余的，记作 $a \equiv b \pmod{m}$。

具体来说，如果 $a \equiv b \pmod{m}$，那么 $a$ 和 $b$ 除以 $m$ 的余数相同。同余关系的性质包括：

1. **自反性：** 对于任意整数 $a$，都有 $a \equiv a \pmod{m}$。
2. **对称性：** 如果 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$。
3. **传递性：** 如果 $a \equiv b \pmod{m}$ 且 $b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$。

- 群的直积

群的直积是指将两个或多个群组合成一个新的群的运算。设有两个群 $G_1$ 和 $G_2$，它们的运算分别为 $*_1$ 和 $*_2$。那么，它们的直积 $G_1 \times G_2$ 定义为：

1. **元素集合：** $G_1 \times G_2$ 的元素是形如 $(g_1, g_2)$ 的有序对，其中 $g_1 \in G_1$ 且 $g_2 \in G_2$。
2. **运算：** 定义 $(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$。这里 $*_1$ 和 $*_2$ 分别是 $G_1$ 和 $G_2$ 上的群运算。

直积 $G_1 \times G_2$ 是一个群，其群运算满足结合律、存在单位元、每个元素存在逆元等群的基本性质。直积的概念可以自然地推广到更多的群。

# 8.3.1 半群、独异点与群

**定义** 设<$G$,∘ >是代数系统，∘ 为二元运算. 如果∘ 运算是可结合的，存在单位元 $e\in G$，并且对 $G$ 中的任何元素 $x$ 都有 $x^{-1}\in G$，则称 $G$ 为 **群**.

**Definition 43.** 称代数系统 $\langle G, *\rangle$ 为群 (group), 如果

(1) 运算 $*$ 是封闭的.

(2) 运算 $*$ 是可结合的.

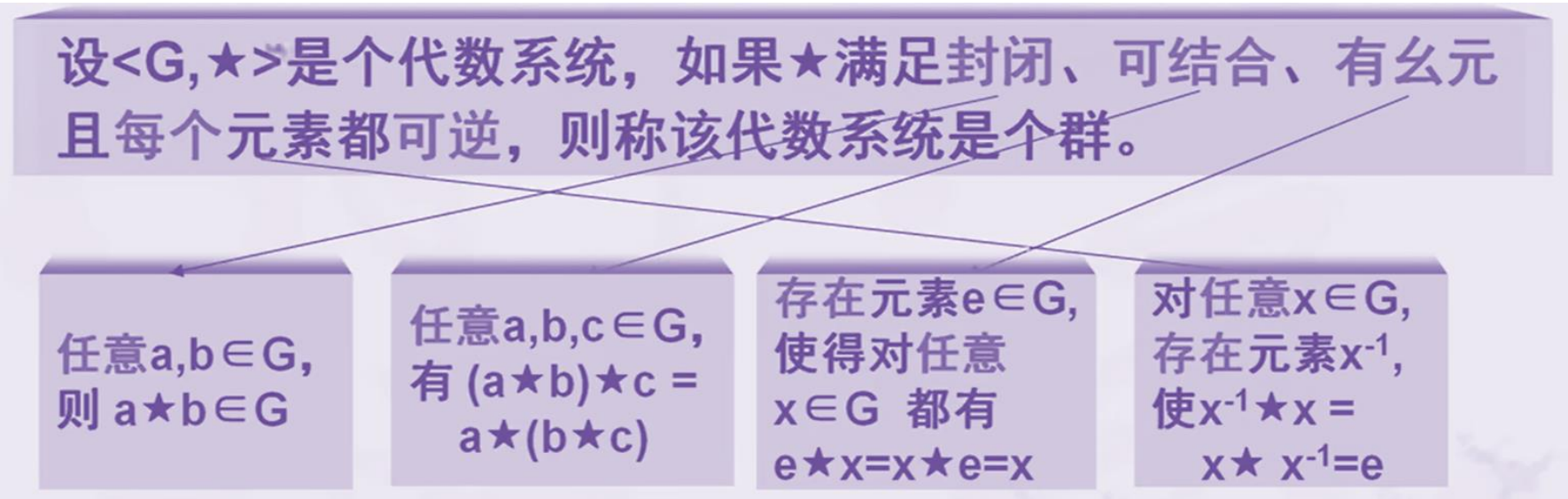
(3) 存在幺元 $e$.

(4) 每一元素 $x$ 都有逆元 $x^{-1}$.

上述四个条件, 依次得到概念: 广群 $\longrightarrow$ 半群 $\longrightarrow$ 独异点 $\longrightarrow$ 群.

# 8.3.1 半群、独异点与群

**定义** 设<$G$,∘ >是代数系统，∘ 为二元运算. 如果∘ 运算是可结合的，存在单位元 $e\in G$，并且对 $G$ 中的任何元素 $x$ 都有 $x^{-1}\in G$，则称 $G$ 为 **群**.



# 8.3.1 半群、独异点与群

**定义** 设<$G$,∘ >是代数系统，∘ 为二元运算. 如果∘运算是可结合的，存在单位元 $e\in G$，并且对 $G$ 中的任何元素 $x$ 都有 $x^{-1}\in G$，则称 $G$ 为 **群**.

**群的实例:**

(1) <Z,+>,<Q,+>,<R,+>是群；<$Z^+$,+>,<N,+>不是群.

(2) <$M_n$(R),+>是群，而<$M_n$(R),·>不是群.

(3) <$P(B)$,⊕>是群，⊕为对称差运算.

(4) <$Z_n$,⊕>，是群. $Z_n$={ 0,1, …, $n$–1}，⊕为模 $n$ 加.

– $\langle R-\{0\},*\rangle$ 的幺元为 1, 逆元 $x^{-1}=1/x$.

$\langle\mathbb{N},+\rangle$, $\langle\mathbb{R},*\rangle$ 不是群.

– $\mathbb{N}$ 中除幺元 0 外, 其余元素无逆元.

– $\mathbb{R}$ 中 0 无逆元.

# 8.3.1 半群、独异点与群

<R,+> 是独异点，幺元是 0，对任意实数 r，它的逆元是 −r 。

<P(E), ⊕>幺元是 Φ，因对任意集合 A∈P(E)，A⊕A=Φ，所以 $A^{-1}=A$

所以它们都是群。

<R,×>是独异点，幺元是 1，零元是 0。因为 0 没有逆元，所以<R,×> 不是群。

<P(E), ∩>是独异点，幺元是 E。对任意集合 A∈P(E) 且 A不等于全集 E，是否有这样的集合使得 A ∩ ？ = E ？没有这样的集合，即 A 没有逆元。所以<P(E), ∩>不是群。

# 8.3.1 半群、独异点与群

1. 设 $G$ 是所有形如

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

的矩阵组成的集合，*表示矩阵乘法。试问 $<G, *>$ 是半群吗？ 这里 $a_{11}$、$a_{12}$ 是实数。

2. 在正实数集合 $\mathbf{R}^+$ 上定义运算*如下

$$x * y = \frac{a+b}{1+ab}$$

试问 $<\mathbf{R}^+, *>$ 是半群吗？

**7. 设 Z 为整数集合，在 Z 上定义二元运算 * 如下：**

$$x * y = x + y - 2, \quad \forall x, y \in \mathbf{Z}$$

问 Z 关于 * 运算能否构成群？为什么？

# 8.3.1 半群、独异点与群

- **Klein四元群**

**设$G = \{ e, a, b, c \}$，$G$上的运算由下表给出，称为 Klein四元群**

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

运算表特征：

- 对称性---运算可交换
- 主对角线元素都是幺元
  ---每个元素是自己的逆元
- $a, b, c$ 中任两个元素运算都等于第三个元素.

# 8.3.1 半群、独异点与群

- **定义** 设$G$是群，$x\in G$，$n\in Z$，则 $x$ 的 $n$ 次幂 $x^n$ 定义为

$$x^n=\begin{cases} e & n=0 \\ x^{n-1}x & n>0 \\ (x^{-1})^m & m=-n, n<0 \end{cases} \qquad n\in Z$$

- 实例
- 在$<Z_3,\oplus>$中有 $2^{-3}=(2^{-1})^3=1^3=1\oplus1\oplus1=0$
- 在 $<Z,+>$ 中有 $(-2)^{-3}=2^3=2+2+2=6$
-

# 8.3.1 半群、独异点与群

设$G$是群，$x\in G$，使得等式 $x^k = e$ 成立的最小正整数 $k$ 称为 $x$ 的阶（或周期），记作 $|x| = k$，称 $x$为 $k$ 阶元. 若不存在这样的正整数 $k$，则称 $x$ 为无限阶元.

在$<Z_6,\oplus>$中，2 和 4 是 3 阶元，3 是 2 阶元，1 和 5 是 6 阶元，0 是 1 阶元

在$<Z,+>$中，0 是 1 阶元，其它整数的阶都不存在.

# 8.3.1 半群、独异点与群

- 若群$G$中的二元运算是可交换的，则称$G$为交换群或 阿贝尔(Abel)群
- 若群 $G$ 是有穷集，则称 $G$ 是有限群，否则称为无限群
- 群 $G$ 的基数称为群$G$的 阶，有限群 $G$ 的阶记作$|G|$

$<Z,+>$ 和 $<R,+>$是无限群，$<Z_n,\oplus>$是有限群，也是 $n$ 阶群，Klein四元群 $G = \{e, a, b, c\}$是 4 阶群

上述群都是交换群， $n$ 阶 ($n\geq 2$) 实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

# 8. 3. 1 半群、独异点与群

**例子 1: 整数模 $n$ 的加法群**

考虑整数模 $n$ 的加法群 $\mathbb{Z}_n$。这个群包含了模 $n$ 的所有整数，它的阶为 $n$，记作 $|\mathbb{Z}_n| = n$。例如，当 $n = 5$ 时，$\mathbb{Z}_5$ 的阶是 5，它包含元素 $\{0, 1, 2, 3, 4\}$。

**例子 2: 对称群**

考虑 $n$ 个元素的对称群 $S_n$，即所有对这 $n$ 个元素进行置换的操作所构成的群。这个群的阶是 $n!$（阶乘），即 $|S_n| = n!$。例如，当 $n = 3$ 时，$S_3$ 的阶是 $3! = 6$。

**例子 3: Klein 四群**

Klein 四群，通常表示为 $V_4$ 或 $K_4$，是一个包含四个元素的群。其阶为 $|V_4| = 4$。Klein 四群的元素可以表示为：

$$V_4 = \{e, a, b, c\}$$

其中，$e$ 是恒等元素，而 $a, b, c$ 是三个非恒等的元素。$V_4$ 的群操作可以通过一个对称表格表示。

# 8.3.1 半群、独异点与群

群中不可能有零元.

证: 设 $\langle G, *\rangle$ 为群.

① 当群的阶为 1 时, 它的惟一元素视作幺元 $e$.

② 设 $|G| > 1$ 且群有零元 $\theta$. 那么群中任何元素 $x \in G$, 都有

$$x * \theta = \theta * x = \theta \neq e.$$

所以, 零元 $\theta$ 就不存在逆元, 与 $\langle G, *\rangle$ 是群的假设矛盾.

在群 $\langle G, *\rangle$ 中, 除幺元 $e$ 之外, 不可能有任何别的等幂元.

证: 因为 $e * e = e$, 所以 $e$ 是等幂元.

现设 $a \in G$, $a \neq e$ 且 $a * a = a$, 则有

$$\begin{aligned} a &= e * a \\ &= (a^{-1} * a) * a \\ &= a^{-1} * (a * a) \\ &= a^{-1} * a && (\text{已假设 } a * a = a) \\ &= e. \end{aligned}$$

与假设 $a \neq e$ 相矛盾. □

# 8.3.1 半群、独异点与群

14. 设 $G=\{1, 2, 4, 7, 8, 11, 13, 14,\}$，对于 $G$ 上的二元运算“模 15 乘法 $\times_{15}$”：

$$i\times_{15} j=(i\times j)(\mathrm{mod}\ 15)$$

$<G, \times_{15}>$ 构成一个群。请

（1）给出 $<G, \times_{15}>$ 的运算表。

（2）给出每个元的逆元。

（3）给出每个元的次数。

# 8.3.1 半群、独异点与群

14. 设 $G=\{1, 2, 4, 7, 8, 11, 13, 14,\}$，对于 $G$ 上的二元运算“模 15 乘法 $\times_{15}$”：

$$i\times_{15} j=(i\times j)(\mathrm{mod}\ 15)$$

$<G, \times_{15}>$ 构成一个群。请

（1）给出 $<G, \times_{15}>$ 的运算表。　　（2）给出每个元的逆元。

（3）给出每个元的次数。

**解**：（1）

| $\times_{15}$ | 1 | 2 | 4 | 7 | 8 | 11 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 7 | 8 | 11 | 13 | 14 |
| 2 | 2 | 4 | 8 | 14 | 1 | 7 | 11 | 13 |
| 4 | 4 | 8 | 1 | 13 | 2 | 14 | 7 | 11 |
| 7 | 7 | 14 | 13 | 4 | 11 | 2 | 1 | 8 |
| 8 | 8 | 1 | 2 | 11 | 4 | 13 | 14 | 7 |
| 11 | 11 | 7 | 14 | 2 | 13 | 1 | 8 | 4 |
| 13 | 13 | 11 | 7 | 1 | 14 | 8 | 2 | 2 |
| 14 | 14 | 13 | 11 | 9 | 7 | 4 | 2 | 1 |

（2）逆元：$1^{-1}=1$，$2^{-1}=8$，$4^{-1}=4$，$7^{-1}=13$，$8^{-1}=2$，$11^{-1}=11$，$13^{-1}=7$，$14^{-1}=14$

（3）元素 1，2，4，7，8，11，13，14 的次数分别为 1，4，2，4，4，2，4，2。

# 8.3.1 半群、独异点与群

- **群的性质---幂运算规则**
- 定理1 设 $G$ 为群，则 $G$ 中的幂运算满足：

  (1) $\forall x \in G$，$(x^{-1})^{-1} = x$.

  (2) $\forall x, y \in G$，$(xy)^{-1} = y^{-1}x^{-1}$.

  (3) $\forall x \in G$，$x^n x^m = x^{n+m}$，$n, m \in \mathrm{Z}$.

  (4) $\forall x \in G$，$(x^n)^m = x^{nm}$，$n, m \in \mathrm{Z}$.
- 注意：
- $(xy)^n = (xy)(xy)\ldots(xy)$, 是 $n$ 个$xy$ 运算，$G$为交换群，才有 $(xy)^n = x^n y^n$.

$$(x_1 x_2 \ldots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \ldots x_2^{-1} x_1^{-1}$$

# 8.3.1 半群、独异点与群

- **群的性质---群方程存在唯一解**
- 定理2 $G$为群，$\forall a,b\in G$，方程 $ax=b$ 和 $ya=b$ 在$G$中有解且仅有惟一解.

  $a^{-1}b$ 是 $ax=b$的解. $ba^{-1}$ 是 $ya = b$ 的唯一解.

- 例 设 $G=<P(\{a,b\}),\oplus>$，其中$\oplus$为对称差. 群方程

  $$\{a\} \oplus X = \varnothing, \qquad Y \oplus \{a,b\} = \{b\}$$

  的解 $X = \{a\}^{-1}\oplus\varnothing = \{a\}\oplus\varnothing = \{a\}$，
- $$Y = \{b\}\oplus\{a,b\}^{-1} = \{b\}\oplus\{a,b\} = \{a\}$$

# 8.3.1 半群、独异点与群

例：设群 $G=<\mathcal{P}(\{a,b\}), \oplus>$，其中 $\oplus$ 为对称差运算。解下列群方程：

$\{a\}\oplus X=\Phi$ ， $Y\oplus\{a,b\}=\{b\}$

# 8.3.1 半群、独异点与群

- **群的性质---消去律（群中每个元素均是可消去元）**
- 定理3 $G$ 为群，则$G$适合消去律，即$\forall a,b,c\in G$ 有
  (1) 若 $ab = ac$，则 $b = c$.
  (2) 若 $ba = ca$，则 $b = c$.
- 
  例　设 $G = \{a_1, a_2, \ldots, a_n\}$ 是 $n$ 阶群，令
- $a_iG = \{ a_i a_j \mid j = 1,2, \ldots , n \}$
- 证明 $a_iG = G$.
  证 由群中运算的封闭性有 $a_iG\subseteq G$. 假设$a_iG\subset G$，即 $|a_iG|<n$. 必有$a_j, a_k\in G$使得

$$a_i a_j = a_i a_k \quad (j\neq k)$$

由消去律得 $a_j = a_k$, 与 $|G| = n$ 矛盾.

# 8.3.1 半群、独异点与群

**定理6** 设 $G$ 是有限半群，且不含零元. 若 $G$ 中成立消去律，则 $G$ 是群.

证 设 $G=\{a_1, a_2, \ldots, a_n\}$，任取 $a_i \in G$，

$$a_i G=\{a_i a_j \mid j=1, 2, \ldots, n\}$$

由封闭性, $a_i G \subseteq G$, 假设 $|a_i G|<n$, 则存在 $j, k$ 使得 $a_i a_j=a_i a_k$, 根据消去律，$a_j=a_k$, 矛盾. 所以 $a_i G=G$.

任取 $a_i, a_j$,

$$a_i, a_j \in G \Rightarrow a_j \in a_i G \Rightarrow \text{方程 } a_i x=a_j \text{ 有解.}$$

同理，方程 $y a_i=a_j$ 有解. $G$ 是群.

# 8.3.1 半群、独异点与群

2. 设$<G,*>$是群，证明$G$是交换群的充要条件是$\forall a,b\in G$有$(a*b)^2=a^2*b^2$。

**证**：充分性：

条件已知$(a*b)^2=a^2*b^2$，由于是群，运算满足结合律和消去律，有

$a*(b*a)*b=a*(a*b)*b$，故$a*b=b*a$，所以$G$是交换群。

必要性：

条件已知$G$是交换群，运算满足结合律和交换律，有

$$(a*b)^2=(a*b)*(a*b)=a*(b*a)*b=a*(a*b)*b=(a*a)*(b*b)=a^2*b^2,$$

即 $(a*b)^2=a^2*b^2$

证毕。

# 8.3.1 半群、独异点与群

- 群的性质---运算表排列规则

**定理4** 设 $G$ 为有限群，则 $G$ 的运算表中每行每列都是 $G$ 中元素的一个置换，且不同的行（或列）的置换都不相同，$G$中每个元素在运算表中的每行(列)都必出现且仅出现一次。

注意：是必要条件，用于判断一个运算表不是群.

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $b$ | $c$ | $d$ | $a$ |
| $b$ | $b$ | $a$ | $c$ | $d$ |
| $c$ | $c$ | $d$ | $b$ | $a$ |
| $d$ | $d$ | $b$ | $a$ | $c$ |

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $c$ | $d$ | $a$ | $b$ |
| $c$ | $b$ | $c$ | $d$ | $a$ |
| $d$ | $d$ | $a$ | $b$ | $c$ |

# 8.3.1 半群、独异点与群

- 群的性质---运算表排列规则

**定理4** 设 $G$ 为有限群，则 $G$ 的运算表中每行每列都是 $G$ 中元素的一个置换，且不同的行（或列）的置换都不相同，$G$中每个元素在运算表中的每行(列)都必出现且仅出现一次。

注意：是必要条件，用于判断一个运算表不是群.

$$aG = G \text{ 和 } Ga = G$$

说明：
运算表的行列构成置换的不一定是群
反例：缺少单位元

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 1 | 2 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 2 | 0 | 1 |

# 8.3.1 半群、独异点与群

2.群中元素的阶

定义：设<G,★>是群，a∈G，使得$a^k=e$成立的最小正整数k称为a的阶，记作|a|=k，称a为k阶元。若不存在这样的正整数k，则称a的阶是无限的。

例如：群<l,+>是一个无限群，只有幺元0的阶是1，其余元素的阶都是无限的。

# 8.3.1 半群、独异点与群

例： <X, ∘>的运算表如下图所示：<X, ∘>是否是群？若是群求各元素的阶。

| ∘ | S | R | A | L |
|---|---|---|---|---|
| S | S | R | A | L |
| R | R | A | L | S |
| A | A | L | S | R |
| L | L | S | R | A |

解：显然<X, ∘>是封闭的；可以验证<X, ∘>是可结合的；S是幺元；

S的逆元为S，A的逆元为A，R与 L 互为逆元。

所以<X, ∘>是群。

因为 $S^1=S$， $A\circ A=A^2=S$，$R^4=R^2\circ R^2=A\circ A=S$，

$L^4=L^2\circ L^2=A\circ A=S$ ，

所以 $|S|=1$， $|A|=2$， $|R|= 4$， $|L|=4$。

# 8.3.1 半群、独异点与群

**定理8** $G$为群，$a\in G$，且$|a|=r$，则

(1) $a^k=e \Leftrightarrow r\mid k$

(2) $|a|=|a^{-1}|$

(3) 若$|G|=n$，则$r\le n$.

证 (1) 充分性. $a^k=a^{rl}=(a^r)^l=e^l=e$

必要性. $k=rl+i$，$l\in Z$，$i\in\{0,1,\ldots,r-1\}$

$$\Rightarrow e=a^k=a^{rl+i}=a^i \Rightarrow i=0 \Rightarrow r\mid k$$

# 8.3.1 半群、独异点与群

- **子群**
- 定义 设 $G$ 是群，$H$ 是 $G$ 的非空子集，如果 $H$ 关于 $G$ 中的运算构成群，则称 $H$ 是 $G$ 的子群, 记作 $H \leq G$. 若 $H$ 是 $G$ 的子群，且 $H \subset G$，则称 $H$ 是 $G$ 的真子群，记作 $H < G$.
- 实例 $n\mathrm{Z}$（$n$是自然数）是整数加群 $<\mathrm{Z},+>$ 的子群. 当 $n \neq 1$ 时, $n\mathrm{Z}$ 是 $\mathrm{Z}$ 的真子群.
- 对任何群 $G$ 都存在子群. $G$ 和 $\{e\}$ 都是 $G$ 的子群，称为 $G$ 的平凡子群.

# 8.3.1 半群、独异点与群

- 子群
- 定义 设 $G$ 是群，$H$ 是 $G$ 的非空子集，如果 $H$ 关于 $G$ 中的运算构成群，则称 $H$ 是 $G$ 的子群, 记作 $H \leq G$. 若 $H$ 是 $G$ 的子群，且 $H \subset G$，则称 $H$ 是 $G$ 的真子群，记作 $H < G$.
- 实例 $n\mathrm{Z}$（$n$是自然数）是整数加群 $<\mathrm{Z},+>$ 的子群. 当 $n \neq 1$ 时, $n\mathrm{Z}$ 是 $\mathrm{Z}$ 的真子群.

说明：

1. 子群 $H$ 就是 $G$ 的子代数.
- 2. 若$H$ 的单位元为 $e'$, 且 $x$ 在 $H$ 中相对 $e'$ 的逆元为 $x'$, 则

$$x e' = x = x e \Rightarrow e' = e$$

$$x x' = e' = e = x x^{-1} \Rightarrow x' = x^{-1}$$

# 8.3.1 半群、独异点与群

$\langle \mathbb{Z}, + \rangle$ 是一个群, 设 $\mathbb{Z}_E = \{x \mid x = 2n, n \in \mathbb{Z}\}$, 证明 $\langle \mathbb{Z}_E, + \rangle$ 是 $\langle \mathbb{Z}, + \rangle$ 的一个子群.

证: 本题的实质是要证明 $\langle \mathbb{Z}_E, + \rangle$ 是群. 按群的定义证明如下:

(1) 证明 $+$ 运算在 $\mathbb{Z}_E$ 上封闭: 任取 $x, y \in \mathbb{Z}_E$, 可设 $x = 2n_1$, $y = 2n_2$, 其中 $n_1, n_2 \in \mathbb{Z}$. 那么 $x + y = 2(n_1 + n_2) \in \mathbb{Z}_E$, 故运算封闭.

(2) 因 $+$ 运算在 $\mathbb{Z}$ 上可结合, 而 $+$ 运算在 $\mathbb{Z}_E$ 上封闭, 所以, $+$ 运算在 $\mathbb{Z}_E$ 上可结合.

(3) 因 $\langle \mathbb{Z}, + \rangle$ 的幺元 0 在 $\mathbb{Z}_E$ 中, 所以 $\langle \mathbb{Z}_E, + \rangle$ 有幺元 0.

(4) 对任意 $x = 2n \in \mathbb{Z}_E$, 有 $2n + 2(-n)| = 0$, 而 $-n \in \mathbb{Z}$, 即 $2(-n) \in \mathbb{Z}_E$. 这说明 $\mathbb{Z}_E$ 中的任意元素有逆元.

所以 $\langle \mathbb{Z}_E, + \rangle$ 是群, 又因 $\mathbb{Z}_E \subseteq \mathbb{Z}$, 所以 $\langle \mathbb{Z}_E, + \rangle$ 是群 $\langle \mathbb{Z}, + \rangle$ 的子群. $\square$

# 8.3.1 半群、独异点与群

设 $G$ 为群，$H$ 是 $G$ 的非空子集. $H$ 是 $G$ 的子群当且仅当 $\forall x, y \in H$ 有 $xy^{-1} \in H$.

设 $G$ 为群，$a \in G$，令 $H = \{ a^k \mid k \in \mathrm{Z} \}$，则 $H$ 是 $G$ 的子群，称为由 $a$ 生成的子群，记作 $<a>$.

证 首先由 $a \in <a>$ 知道 $<a> \neq \varnothing$. 任取 $a^m, a^l \in <a>$,

$$a^m (a^l)^{-1} = a^m a^{-l} = a^{m-l} \in <a>$$

根据判定定理可知 $<a> \leq G$.

# 8.3.1 半群、独异点与群

证 充分性. $H \neq \varnothing \Rightarrow \exists b \in H$

$b \in H \Rightarrow b\,b^{-1} \in H \Rightarrow e \in H$

$\forall a,\quad a \in H \Rightarrow e\,a^{-1} \in H \Rightarrow a^{-1} \in H$

$\forall a,b,\quad a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow a\,b \in H$

**定理3** $G$ 是群，$H$ 是 $G$ 的有限非空子集，则

$H \leq G \Leftrightarrow \forall a, b \in H,\ a\,b \in H$

$H$ 非空，存在 $a$ 属于 $H$，

由条件2，$a^{-1}$ 属于 $H$，

由条件1，有 $a\,a^{-1}$ 属于 $H$，即 $e$ 属于 $H$

# 8.3.1 半群、独异点与群

2. $B$ 生成子群 $\langle B\rangle = \cap\{H \mid H \le G, B \subseteq H\}, B \subseteq G$

$$\langle B\rangle = \{b_1^{e_1} b_2^{e_2} \ldots b_n^{e_n} \mid b_i \in B, e_i = \pm 1, i = 1,2,\ldots,n, n \in Z^+\}$$

3. 中心 $C = \{a \mid a \in G, \forall x \in G\ (a\,x = x\,a)\}$

4. $a$ 的正规化子 $N(a) = \{x \mid x \in G, x\,a = a\,x\},\ a \in G$

5. $H$ 的正规化子 $N(H) = \{x \mid x \in G, x\,H\,x^{-1} = H\}, H \le G$

6. 共轭子群 $x\,H\,x^{-1} = \{x\,h\,x^{-1} \mid h \in H\}$

其中 $H \le G,\ x \in G$

7. 子群的交

$H, K \le G$, 则

(1) $H \cap K \le G$

(2) $H \cup K \le G \Leftrightarrow H \subseteq K \vee K \subseteq H$

# 8. 3. 1 半群、独异点与群

整数加群<Z,+>,

由 2 生成的子群是 $<2> = \{ 2k \mid k \in Z \} = 2Z$

模 6 加群 $<Z_6, \oplus>$中

由 2 生成的子群 $<2> = \{ 0, 2, 4 \}$

Klein四元群 $G = \{ e, a, b, c \}$ 的所有生成子群是:

$<e> = \{ e \}$,

$<a> = \{ e, a \}$, $<b> = \{ e, b \}$, $<c> = \{ e, c \}$.

# 8.3.1 半群、独异点与群

例：群$<N_6,+_6>$的运算表如右图：求 $<N_6,+_6>$的子群。

| $+_6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

$<N_6,+_6>$运算表

解：根据上面定理，使得 $+_6$ 运算封闭的子集可构成子群。

除了平凡子群 $<\{0\},+_6>$ 及 $<N_6,+_6>$ 外，考察子集 $H_1=\{0,3\}$，$H_2=\{0,2,4\}$，从运算表知，$+_6$运算在 $H_1$ 、 $H_2$ 上封闭，所以 $<H_1,+_6>$，$<H_2, +_6>$ 是 $<N_6,+_6>$ 的子群。

| $+_6$ | 0 | 3 |
|---|---|---|
| 0 | 0 | 3 |
| 3 | 3 | 0 |

$<H_1,+_6>$运算表

| $+_6$ | 0 | 2 | 4 |
|---|---|---|---|
| 0 | 0 | 2 | 4 |
| 2 | 2 | 4 | 0 |
| 4 | 4 | 0 | 2 |

$<H_2, +_6>$运算表

# 8.3.1 半群、独异点与群

练习：已知$<H_1,\star>$和$<H_2,\star>$是群$<G,\star>$的子群，求证$<H_1\cap H_2,\star>$是$<H_1,\star>$、$<H_2,\star>$和$<G,\star>$的子群。

(1) 先证明 $H_1\cap H_2$ 是 $H_1$、$H_2$ 及 G 的非空子集

显然 $H_1\cap H_2\subseteq H_1$，$H_1\cap H_2\subseteq H_2$，$H_1\cap H_2\subseteq G$；

因为$<H_1,\star>$和$<H_2,\star>$是群$<G,\star>$的子群，所以幺元 $e\in H_1$ 并且 $e\in H_2$，于是 $e\in H_1\cap H_2$，即

$H_1\cap H_2\neq\Phi$，

所以 $H_1\cap H_2$ 是 $H_1$、$H_2$ 及 G 的非空子集。

# 8.3.1 半群、独异点与群

练习：已知$<H_1,\star>$和$<H_2,\star>$是群$<G,\star>$的子群，求证$<H_1\cap H_2,\star>$是$<H_1,\star>$、$<H_2,\star>$和$<G,\star>$的子群。

(2) 再证明对任意 $a,b\in H_1\cap H_2$，$a\star b^{-1}\in H_1\cap H_2$

因为 $a,b\in H_1\cap H_2$，所以 $a,b\in H_1$ 且 $a,b\in H_2$；
又因为 $<H_1,\star>$和$<H_2,\star>$是群$<G,\star>$的子群，所以
$b^{-1}\in H_1$，$b^{-1}\in H_2$；再由封闭性知
$a\star b^{-1}\in H_1$，$a\star b^{-1}\in H_2$，即有 $a\star b^{-1}\in H_1\cap H_2$

综上 $<H_1\cap H_2,\star>$是$<H_1,\star>$,$<H_2,\star>$和$<G,\star>$的子群。

# 8.3.1 半群、独异点与群

设 $G$ 为群, 令 $C = \{ a \mid a \in G \wedge \forall x \in G(ax=xa)\}$，则 $C$ 是 $G$ 的子群，称为 $G$ 的中心.

证 $e \in C$. $C$是 $G$ 的非空子集.

任取 $a, b \in C$，证明 $ab^{-1}$与 $G$ 中所有的元素都可交换.

$\forall x \in G$，有

$$(ab^{-1})x = ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1}$$
$$= a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$$

由判定定理可知 $C \leq G$.

# 8. 3. 1 半群、独异点与群

**定义** 设 $G$ 是群，若存在 $a \in G$ 使得

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

称 $G$ 是**循环群**，记作 $G=\langle a \rangle$，称 $a$ 为 $G$ 的**生成元**.

实例：整数加群 $G = \langle Z,+ \rangle = \langle 1 \rangle = \langle -1 \rangle$

模 6 加群 $G = \langle Z_6,\oplus \rangle = \langle 1 \rangle = \langle 5 \rangle$

**解：$\langle N_4,+_4 \rangle$是以 1 为生成元的循环群，**

**因为显然 $2=1+_41=1^2$，$3=1+_41+_41=1^3$，$0=2+_42= 1^4$**

**所以 $N_4$ 可表示成 $N_4 =\{1^4,1,1^2,1^3\}$。**

**例2：$I=\{\ldots-3, -2, -1, 0, 1, 2, 3, \ldots\}$，$\langle I,+ \rangle$是群，**

**因为 $-1=1^{-1}$，$-2=(-1)+(-1)=1^{-1}+1^{-1}=(1^{-1})^2=1^{-2}$，……**

**$0=1^0$，$1=1^1$，$2=1^2$，……**

**所以 I 可以写成：$I=\{\ldots 1^{-3},1^{-2},1^{-1},1^0,1^1,1^2,1^3 \ldots\}$，**

**即 $\langle I,+ \rangle$ 是以 1 为生成元的循环群。**

# 8.3.1 半群、独异点与群

**定义** 设 $G$ 是群，若存在 $a\in G$ 使得

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

称 $G$ 是**循环群**，记作 $G=\langle a\rangle$，称 $a$ 为 $G$ 的**生成元**.

全体整数的集合 $\mathbb{Z}$ 关于普通加法构成一个群, 我们把它称为整数加群. 试说明整数加群 $\langle\mathbb{Z},+\rangle$ 是循环群.

**解:** 群 $\langle\mathbb{Z},+\rangle$ 的幺元是 0. 任意 $a\in\mathbb{Z}$, 其逆元为 $-a$.

这个群的全体的元都是 1 的乘方. (假如把 $\mathbb{Z}$ 的代数运算不用 $+$ 而用 $*$ 来表示, 就很容易明白了.)

假定 $m$ 是任意正整数, 则

$$m=\underbrace{1+1+\cdots+1}_{m}=\underbrace{1*1*\cdots*1}_{m}=1^m$$

所以, 对任意 $m\in\mathbb{Z}$, 有

$$m=\begin{cases}\underbrace{1+1+\cdots+1}_{m}=1^m, & m>0,\\ 0=1^0, & m=0,\\ \underbrace{(-1)+(-1)+\cdots+(-1)}_{|m|}=(-1)^{|m|}=(1^{-1})^{|m|}=1^m, & m<0.\end{cases}\quad\square$$

# 8.3.1 半群、独异点与群

**定义** 设 $G$ 是群，若存在 $a \in G$ 使得

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

称 $G$ 是**循环群**，记作 $G=\langle a \rangle$，称 $a$ 为 $G$ 的**生成元**.

设 $G = \langle a \rangle$，若$a$ 是 $n$ 阶元，则$G$为 $n$ 阶**循环群**，即

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

若 $a$ 是无限阶元，则 $G$ 为**无限循环群**，即

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

$\langle N_4,+_4 \rangle$，$N_4 = \{0,1,2,3\} = \{1^4,1,1^2,1^3\}, 1^4 = 0$，循环周期为4。

$\langle I,+ \rangle$，$I = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

# 8.3.1 半群、独异点与群

7. 证明循环群一定是交换群，举例说明交换群不一定是循环群。

**证**：若$<G,*>$为循环群，则$\exists a \in G$，使得$G=\{a^k \mid k \in Z\}$，

所以$\exists b,c \in G$，使得$b=a^m, c=a^n$，$m,n \in Z$

所以$b*c=a^m*a^n=a^{m+n}=a^{n+m}=a^n*a^m=c*b$，即$<G,*>$满足交换律，也即$<G,*>$是交换群。

不是所有的交换群都是循环群，例如：Klein 四元群是交换群，但不是循环群。

# 8. 3. 1 半群、独异点与群

- **循环群的生成元**

**定理** 设<G,★>是以 g 为生成元的有限循环群。则 |G|=n 当且仅当 |g|=n 。

设 $G = \langle a \rangle$ 是循环群.

(1) 若$G$是无限循环群，则 $G$ 只有 $a$ 和 $a^{-1}$ 两个生成元.

(2) 若 $G$ 是 $n$ 阶循环群，则 $a^r$ 是 $G$ 的生成元当且仅当 $r$ 是小于等于 $n$ 且与 $n$ 互质的正整数.

$\phi(n)$ 为欧拉函数，即小于或等于 n 且与 n 互素的正整数的个数。

G 含有 $\phi(n)$ 个生成元。

# 8.3.1 半群、独异点与群

例1： <G,★>是由 g 生成的循环群， |G|=12，

小于或等于 12 且与 12 互素的正整数有 4 个：

1, 5, 7, 11，即 $\phi(12)=4$。

于是<G,★>有 4 个生成元，分别是：g，$g^5$，$g^7$，$g^{11}$ 。

例2：设 <G,+>， $G=\{3z \mid z\in \mathbf{I}\}$， “+” 是普通加法运算，

则 <G,+> 为无限循环群，只有两个生成元：3 和 –3。

定理2 $G=<a>$是循环群，那么

(1) $G$ 的子群也是循环群

(2) 若$G$是无限阶，则$G$ 的子群除$\{e\}$外也是无限阶

(3) 若$G$是 $n$ 阶的，则$G$ 的子群的阶是$n$ 的因子，

对于$n$ 的每个正因子$d$，在 $G$ 中有且仅有一个$d$阶子群.

# 8.3.1 半群、独异点与群

(1) $< Z_{12}, \oplus >$, 求生成元、子群 .

生成元为与 12 互质的数： 1, 5, 7, 11

1. 以1为生成元：$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$。
2. 以5为生成元：$\langle 5 \rangle = \{0, 5, 10\}$。
3. 以7为生成元：$\langle 7 \rangle = \{0, 7\}$。
4. 以11为生成元：$\langle 11 \rangle = \{0, 11\}$。

(3) $< a >$ 为无限循环群，求生成元和子群 .

生成元为 $a, a^{-1}$；子群为 $<a^i>$， $i = 0,1,2,\ldots$;

(4) $G = < Z,+ >$，求生成元和子群 .

生成元： 1, –1; 子群 $nZ, n = 0,1,\ldots,$

# 8. 3. 1 半群、独异点与群

- **生成元的实例**

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

(2) 设$G=<Z_9,\oplus>$是模9的整数加群，则小于或等于 9且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理，$G$的生成元是 1, 2, 4, 5, 7 和 8.

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

# 8.3.1 半群、独异点与群

## ➢ 生成元的实例

所有复数

$$e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad (k = 0, 1, 2, \ldots, n-1)$$

作为一个 $n$ 阶有限循环群, $e^{\frac{2\pi i}{n}}$ 是它的一个生成元.

**阶数为 5、6、14、15 的循环群的生成元分别有多少个?**

**解:** 设 $a$ 是阶数为 5 的循环群的生成元，则因在比 5 小的正整数中有且仅有 2，3，4 与 5 互质，所以 $a^2$，$a^3$，$a^4$ 也是生成元，因此生成元个数为 4。

设 $a$ 是阶数为 6 的循环群的生成元，则因在比 6 小的正整数中有且仅有 5 与 6 互质，所以 $a^5$ 也是生成元，因此生成元个数为 2。

设 $a$ 是阶数为 14 的循环群的生成元，则因在比 14 小的正整数中有且仅有 3，5，9，11，13 与 14 互质，所以 $a^3$，$a^5$，$a^9$ $a^{11}$ $a^{13}$ 也是生成元，因此生成元个数为 6。

设 $a$ 是阶数为 15 的循环群的生成元，则因在比 15 小的正整数中有且仅有 2，4，8，11，13，14 与 15 互质，所以 $a^2$，$a^4$，$a^8$ $a^{11}$ $a^{13}$ $a^{14}$ 也是生成元，因此生成元个数为 7。

# 8.3.1 半群、独异点与群

- **循环群的子群**

定理

设$G=<a>$是循环群.

(1) 设$G=<a>$是循环群，则 $G$ 的子群仍是循环群.

(2) 若$G=<a>$是无限循环群，则 $G$ 的子群除$\{e\}$以外都是无限循环群.

(3) 若$G=<a>$是 $n$ 阶循环群，则对 $n$ 的每个正因子$d$，$G$ 恰好只含有一个$d$ 阶子群.

# 8.3.1 半群、独异点与群

- **子群的实例**

(1) $G=<Z,+>$是1无限循环群，对于自然数$m\in N$，1的 $m$ 次幂是 $m$，$m$ 生成的子群是 $mZ$，$m\in N$. 即

$$<0> = \{ 0 \} = 0Z$$

$$<m> = \{ mz \mid z\in Z \} = mZ,\quad m>0$$

# 8.3.1 半群、独异点与群

- **子群的实例**

(2) $G=Z_{12}$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 <12>=<0>={0}，2 阶子群 <6> = {0,6}
3 阶子群 <4>={0,4,8}，4 阶子群 <3> = {0,3,6,9}
6 阶子群<2>={0,2,4,6,8,10}，12 阶子群<1> = $Z_{12}$

- 1的阶是12，因为 $1^{12} \equiv 0 \pmod{12}$。
- 2的阶是6，因为 $2^{6} \equiv 0 \pmod{12}$。
- 3的阶是4，因为 $3^{4} \equiv 0 \pmod{12}$。
- 4的阶是3，因为 $4^{3} \equiv 0 \pmod{12}$。
- 6的阶是2，因为 $6^{2} \equiv 0 \pmod{12}$。

这些阶的取值正好是12的正因子。

# 8.3.1 半群、独异点与群

## ➢ 子群的实例

1. **正因子：**
   - **定义：** 正因子是指一个正整数的所有能够整除它的正整数。例如，12的正因子是1, 2, 3, 4, 6, 12。
   - **意义：** 正因子的研究涉及到数论，它用于描述一个数能够被哪些正整数整除，有助于理解数的性质和结构。
2. **生成元：**
   - **定义：** 在群论中，生成元是一个群中的元素，通过对群的运算进行重复操作，可以生成群中的所有元素。生成元是群的一个特殊元素，用于描述群的结构。
   - **意义：** 生成元在群论中非常重要，它们帮助我们理解群的性质和结构。在循环群中，生成元尤其重要，因为它们可以通过重复群的运算生成整个群。

# 8. 3. 1 半群、独异点与群

- ***n*元置换的定义**
- 定义 设 $S = \{1, 2, \ldots, n\}$，$S$上的双射函数 $\sigma: S \to S$ 称为 $S$上的 *n*元置换. 一般将 $n$ 元置换σ记为
- $$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$
- 例如 $S = \{1, 2, 3, 4, 5\}$, 则

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

- 都是 5元置换.

# 8. 3. 1 半群、独异点与群

- ***k* 阶轮换与对换**
- 定义 设$\sigma$是 $S = \{1, 2, \ldots, n\}$上的 $n$ 元置换. 若

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

- 且保持 $S$ 中的其他元素不变，则称$\sigma$为 $S$上的 $k$ 次
- 轮换，记作 $(i_1 i_2 \ldots i_k)$. 若 $k$=2，称$\sigma$为$S$上的对换.
- 例如 5元置换
- $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},\quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$
- 分别是 4 阶和 2 阶轮换$\sigma$=(1 2 3 4),$\tau$=(1 3), 其中 $\tau$也叫做对换

# 8. 3. 1 半群、独异点与群

- ***n*元置换分解为轮换之积**
- 例 设 $S = \{1, 2, \ldots, 8\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$$

- 从$\sigma$中分解出来的第一个轮换式 (1 5 2 3 6)；第二个轮换为(4)；第三个轮换为 (7 8). $\sigma$的轮换表示式

$$\sigma=(1\ 5\ 2\ 3\ 6)\ (4)\ (7\ 8)=(1\ 5\ 2\ 3\ 6)\ (7\ 8)$$

- 用同样的方法可以得到$\tau$的分解式

$$\tau=(1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)$$

- 注意：在轮换分解式中，1 阶轮换可以省略.

# 8.3.1 半群、独异点与群

- ***n*元置换的乘法与求逆**
- 两个 $n$ 元置换的乘法就是函数的复合运算
- $n$ 元置换的求逆就是求反函数.

例如：8元置换 $\sigma=(132)(5648)$，$\tau=(18246573)$，则

$$\sigma\tau=(15728)(3)(4)(6)=(15728)$$

置换求逆：求反函数

$$\sigma=(132)(5648),\quad \sigma^{1}=(8465)(231),$$

令 $S_n$ 为 $\{1,2,\ldots,n\}$ 上所有 $n$ 元置换的集合.

$S_n$ 关于置换乘法构成群，称为 $n$ 元对称群.

$S_n$ 的子群称为 $n$ 元置换群.

- 例 设 $\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix}$, $\tau=\begin{pmatrix}1&2&3&4&5\\4&3&1&2&5\end{pmatrix}$

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix},\quad \tau\sigma=\begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}$$

$$\sigma^{-1}=\begin{pmatrix}5&3&2&1&4\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&3&2&5&1\end{pmatrix}$$

# 8. 3. 1 半群、独异点与群

- ***n*元置换的乘法与求逆**
- 两个 $n$ 元置换的乘法就是函数的复合运算
- $n$ 元置换的求逆就是求反函数.
- 例 设

$$\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4&5\\4&3&1&2&5\end{pmatrix}$$

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix},\quad \tau\sigma=\begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}$$

- $$\sigma^{-1}=\begin{pmatrix}5&3&2&1&4\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&3&2&5&1\end{pmatrix}$$
- 使用轮换表示是:
- $\sigma\tau = (1\ 5\ 4)\ (2\ 3)\ (1\ 4\ 2\ 3) = (1\ 5\ 2)$
- $\tau\sigma = (\ 1\ 4\ 2\ 3)\ (1\ 5\ 4)\ (2\ 3) = (3\ 5\ 4)$
- $\sigma^{-1} = (1\ 5\ 4)^{-1}\ (2\ 3)^{-1} = (4\ 5\ 1)\ (2\ 3) = (1\ 4\ 5)\ (2\ 3)$

# 8.3.1 半群、独异点与群

- **$n$元置换群及其实例**

考虑所有的 $n$ 元置换构成的集合 $S_n$

$S_n$关于置换的乘法是封闭的. 置换的乘法满足结合律. 恒等置换(1)是 $S_n$ 中的单位元. 对于任何 $n$元置换 $\sigma \in S_n$，逆置换$\sigma^{-1}$是$\sigma$ 的逆元. 这就证明了$S_n$关于置换的乘法构成一个群，称为 $n$元对称群. $n$元对称群的子群称为 $n$元置换群.

$k$ 阶轮换 $(i_1\ i_2 \ldots i_k)$ 的阶为 $k$

例 设 $S = \{1, 2, 3\}$，3元对称群

$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

# 8.3.1 半群、独异点与群

- $S_3$ 的运算表

| | (1) | (1 2) | (1 3) | (2 3) | (1 2 3) | (1 3 2) |
|---|---|---|---|---|---|---|
| (1) | (1) | (1 2) | (1 3) | (2 3) | (1 2 3) | (1 3 2) |
| (1 2) | (1 2) | (1) | (1 2 3) | (1 3 2) | (1 3) | (2 3) |
| (1 3) | (1 3) | (1 3 2) | (1) | (1 2 3) | (2 3) | (1 2) |
| (2 3) | (2 3) | (1 2 3) | (1 3 2) | (1) | (1 2) | (1 3) |
| (1 2 3) | (1 2 3) | (2 3) | (1 2) | (1 3) | (1 3 2) | (1) |
| (1 3 2) | (1 3 2) | (1 3) | (2 3) | (1 2) | (1) | (1 2 3) |

# 8. 3. 1 半群、独异点与群

- $S_3$的子群

$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$,

$A_3 = \langle(1\ 2\ 3)\rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$,

$\langle(1)\rangle = \{(1)\}$

$\langle(1\ 2)\rangle = \{(1), (1\ 2)\}$,

$\langle(1\ 3)\rangle = \{(1), (1\ 3)\}$,

$\langle(2\ 3)\rangle = \{(1), (2\ 3)\}$

# 8.3.2 环的定义

定义　设$<R,+,\cdot>$是代数系统，+和·是二元运算.如果满足以下条件:

(1) $<R,+>$构成交换群

(2) $<R,\cdot>$构成半群　　$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ 及 $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$

(3) ·运算关于+运算适合分配律

则称$<R,+,\cdot>$是一个环.

通常称+运算为环中的加法，· 运算为环中的乘法.

环中加法单位元记作 0, 乘法单位元(若存在)记作 1.

对任何元素 $x$，称 $x$ 的加法逆元为负元，记作$-x$.

乘法逆元(若存在)称为逆元，记作 $x^{-1}$.

# 8. 3. 2 环的定义

<R, + ,· >、 <$\mathcal{P}$ (E), ⊕, ∩ >是否是环？

因为 <R, +> 是交换群； <R, ·> 是半群；
并且 · 对 + 可分配，所以 <R, + , ·> 是环。
<$\mathcal{P}$(E), ⊕, ∩>是环，因为 <$\mathcal{P}$ (E), ⊕> 是交换群；
<$\mathcal{P}$ (E), ∩ >是半群，并且 ∩ 对 ⊕ 可分配，
所以 <$\mathcal{P}$(E), ⊕, ∩> 是环。

**<$\mathcal{P}$(E),∩, ∪> 、 <$\mathcal{P}$ (E), ⊕, ∪>是否是环？**

因为 <$\mathcal{P}$ (E), ∩ > 不是群，所以 <$\mathcal{P}$(E),∩, ∪> 不是环。
因为 ∪ 对 ⊕ 不可分配，所以 <$\mathcal{P}$ (E), ⊕, ∪> 不是环。

# 8. 3. 2 环的定义

环的实例

(1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数环Q，实数环R 和 复数环C.

(2) $n(n\geq 2)$阶实矩阵的集合$M_n(\mathrm{R})$关于矩阵的加法和乘法构成环，称为$n$阶实矩阵环.

(3) 集合的幂集$P(B)$关于集合的对称差运算和交运算构成环.

(4) 设$\mathrm{Z}_n=\{0,1,\ldots,n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$<\mathrm{Z}_n,\oplus,\otimes>$构成环，称为模$n$的整数环.

# 8.3.2 环中的计算

- **环的性质**
- 定理 设$<R,+,\cdot>$是环，则

(1) $\forall a\in R$， $a\cdot 0 = 0\cdot a = 0$

(2) $\forall a,b\in R$， $(-a)b = a(-b) = -ab$

(3) $\forall a,b\in R$， $(-a)(-b) = ab$

(4) $\forall a,b,c\in R$，$a(b-c) = ab-ac$，$(b-c)a = ba-ca$

例 在环中计算 $(a+b)^3$, $(a-b)^2$

解 $(a+b)^3 = (a+b)(a+b)(a+b)= (a^2+ba+ab+b^2)(a+b)$

$= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$

$(a-b)^2 = (a-b)(a-b)=a^2-ba-ab+b^2$

# 8. 3. 2 环中的零因子

- 设$<R,+,\cdot>$是环，若存在 $ab=0$, 且 $a\neq 0$, $b\neq 0$, 称 $a$ 为左零因子，$b$为右零因子.
- 实例
- $<Z_6,\oplus,\otimes>$，其中 $2\otimes 3=0$，2 和 3 都是零因子.

  例如：$<\mathcal{P}(A),\oplus,\cap>$是环，$\Phi$ 是零元。

  设 $A=\{a,b\}$，$\{a\}$ 和 $\{b\}$ 都不是零元，但 $\{a\}\cap\{b\}=\Phi$。
- 无零因子的条件：$ab=0\rightarrow a=0\vee b=0$
- 可证明无零因子的充要条件是：乘法满足消去律

对任意 $a,b\in A$，若 $a\neq 0\wedge b\neq 0$ 必有 $a\cdot b\neq 0$，则称环 $<A,+,\cdot>$ 中无零因子。

# 8. 3. 2 特殊的环

$\langle A,+,\cdot\rangle$ 是无零因子环，当且仅当 运算 · 满足可消去性。

证明：充分性 设环$\langle A,+,\cdot\rangle$中 · 满足可消去性。

任取 $a,b\in R$，设有 $a\cdot b=0$ （往证$a=0\vee b=0$）（反证法）

(1) 假设 $a\neq 0$，因 $a\cdot 0=0$，于是 $a\cdot b=a\cdot 0$，由可消去性得 $b=0$；

(2) 假设 $b\neq 0$，因 $0\cdot b=0$，于是 $a\cdot b=0\cdot b$，由可消去性得 $a=0$ 。

由 $a\cdot b=0$ 推出 $a=0\vee b=0$ ，

因此$\langle R,+,\cdot\rangle$中无零因子。

证明：必要性 设$\langle R,+,\cdot\rangle$ 是无零因子环，

任取 $a,b,c\in R$，a不是零元且有 $a\cdot b=a\cdot c$ （往证$b=c$）

由 $a\cdot b=a\cdot c$，于是 $a\cdot b-a\cdot c=0$，于是 $a\cdot(b-c)=0$。

因$\langle R,+,\cdot\rangle$是无零因子环，a不是零元，所以 $b-c=0$

即 $b+(-c)=0$，于是 $b=-(-c)=c$ 。

由 $a\cdot b=a\cdot c$ 推出 $b=c$，所以 · 满足可消去性。

# 8.3.2 环中的计算

设 $\langle A, +, \circ\rangle$ 是环, 如果存在 $a, b \in A$, 且 $a \neq \theta$, $b \neq \theta$, 使得 $a \circ b = \theta$, 则称 $\langle A, +, \circ\rangle$ 是含零因子环. $a$ 和 $b$ 称为零因子.

注

- 零因子: "两个非零的数相乘等于零";
- 强调这个概念, 是因为
$$a \circ b = 0 \Rightarrow a = 0 \text{ 或 } b = 0$$
这一条普通的计算规则, 在一般的环里并不一定成立;
- 一个环当然可以没有零因子, 比如整数环;
- 显然, 在而且只在一个没有零因子的环里, (48) 式才会成立.

# 8.3.2 特殊的环

定义　设$<R,+,\cdot>$是环，

(1) 若环中乘法$\cdot$适合交换律，则称 $R$是交换环.

(2) 若环中乘法$\cdot$存在单位元，则称 $R$是含幺环.

(3) 若$\forall a, b\in R$，$a\,b=0 \Rightarrow a=0\vee b=0$，则称$R$是无零因子环.

(4) 若 $R$ 既是交换环、含幺环，也是无零因子环，则称 $R$ 是整环.

(5) 若 $R$为整环，$|R|>1$, 且$\forall a\in R^*=R-\{0\}$，$a^{-1}\in R$, 则称 $R$ 为域.

因为 0 是 <A, · > 的零元，它没有逆元，如要<A, · >构成群，必须将零元抠掉。

# 8.3.2 环中的计算

*Example* 98. 一个数域 $F$ 上的一切 $n \times n$ 矩阵对于矩阵的加法和乘法来说, 构成一个环. 这个环有幺元, 即单位矩阵. 当 $n \geqslant 2$ 时, 这个环是非交换环, 有零因子 (或者说, 不满足消去律).

以上我们认识了一个环可能满足的三种附加条件: (1) 乘法满足交换律, (2) 存在幺元, (3) 零因子不存在 (满足消去律). 一个环当然可以满足其中的一个或多个附加条件. 同时满足以上三个条件的环, 称为整环.

# 8.3.2 特殊的环

比较环与域的差别：

| 整环 | 域 |
| --- | --- |
| (1) <A,+>是交换群； | (1) <A,+>是交换群； |
| (2) <A, · >是可交换独异点； | (2) <A-{0}, · >是交换群；<br><A, ·>是可交换独异点；<br>对任意 $a \in A \wedge a \neq 0$，均有$a^{-1} \in A$； |
| (3) 无零因子； | |
| (4) · 对 + 可分配。 | (3) · 对 + 可分配。 |

# 8.3.2 特殊的环

## 比较环与域的差别：

如果整环 $R$ 至少含有 2 个元素，且每个元素 $x(x\neq 0)$ 都有逆元 $x^{-1}\in R$，则称 $R$ 是域.

有理数集 $\mathbf{Q}$、实数集 $\mathbf{R}$、复数集 $\mathbf{C}$ 关于数的加法和乘法分别构成有理数域、实数域和复数域. 但整数集 $\mathbf{Z}$ 关于数的加法和乘法只能构成整环，但不是域. 模 $n$ 整数环 $<\mathbf{Z}_n,\oplus,\odot>$ 当 $n$ 为合数时不是整环，也不是域；但当 $n$ 为素数时构成域.

**9.22** 令 $\mathbf{Z}[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbf{Z}\}$，其中 i 为虚数单位，即 $\mathrm{i}^2=-1$，那么 $\mathbf{Z}[\mathrm{i}]$ 对于普通加法和乘法能否构成环？为什么？

(1) $S_1=\{0,\pm 1,\pm 2,\cdots,\pm n\}$，$+$ 为普通加法，则 $S_1$ 是 $\boxed{\text{A}}$.

(2) $S_2=\left\{\frac{1}{2},0,2\right\}$，$*$ 为普通乘法，则 $S_2$ 是 $\boxed{\text{B}}$.

(3) $S_3=\{0,1,\cdots,n-1\}$，$n$ 为任意给定的正整数且 $n\geqslant 2$，$*$ 为模 $n$ 乘法，$\circ$ 为模 $n$ 加法，则 $S_3$ 是 $\boxed{\text{C}}$.

(5) $S_5=M_n(\mathbf{R})$，$+$ 为矩阵加法，则 $S_5$ 是 $\boxed{\text{E}}$.

# 8.3.2 特殊的环

### 模n整数环的定义：

给定一个正整数n，我们可以定义模n整数环（通常表示为 $\mathbb{Z}_n$ 或 $\mathbb{Z}/n\mathbb{Z}$）为所有与n互素的非负整数构成的集合。两个整数a和b在模n整数环中被认为是相等的，如果它们对n取余相同，即 $a \equiv b \pmod{n}$。

### 当n是合数时：

1. **不是整环：** 整环要求没有零因子，即非零元素的乘积不等于零。当n是合数时，存在大于1的整数a和b，使得 $a \cdot b \equiv 0 \pmod{n}$，因此模n整数环不是整环。
2. **不是域：** 域要求每个非零元素都有乘法逆元素。当n是合数时，存在与n不互素的整数，这些整数在模n意义下没有乘法逆元素，因此模n整数环不是域。

### 当n是素数时：

1. **构成域：** 当n是素数时，对于任意非零整数a，由费马小定理可知 $a^{n-1} \equiv 1 \pmod{n}$，因此a在模n意义下有乘法逆元素。这意味着模n整数环对于素数n构成域。

总结起来，当n是合数时，模n整数环不是整环，也不是域；而当n是素数时，模n整数环构成域。这是因为素数的特殊性质导致了每个非零元素都有乘法逆元素。

# 8. 3. 2 特殊的环

## 有限整环必是域 。

域 必是 整环。

证明：因为 域 是 可交换的含幺环，又无零因子，
所以域是整环。 。

整环 未必 是域。

例：<I,+, · > 是整环，但不是域。
因为对 · 运算，除 1 外的任何整数均不可逆
( 1/n不是整数 )，所以 <I-{0}, · > 不是群。

设 $\langle A, +, \circ \rangle$ 是环,

- 对含幺环, $\langle A, \circ \rangle$ 是独异点;
- 一般, 一个环未必有一个乘法幺元. 例如 $\mathbb{Z}_E = \{$所有偶数$\}$, 对普通加法和乘法构成一个环, 但是没有乘法幺元.

# 8. 3. 2 特殊的环

- **特殊环的实例**

(1)整数环Z、有理数环Q、实数环R、复数环C都是交换环、含幺环、无零因子环和整环. 其中除Z之外都是域

(2)令2Z={ $2z \mid z \in Z$ }，则<2Z,+,·>构成交换环和无零因子环. 但不是含幺环和整环.

(3)设$n \in Z$, $n \geq 2$, 则 $n$ 阶实矩阵的集合 $M_n(R)$关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环.

(4)<$Z_6$,⊕,⊗>构成环，它是交换环、含幺环，但不是无零因子环和整环.

注意：对于一般的 $n$, $Z_n$是整环且是域 ⇔ $n$是素数.

# 8. 3. 2 特殊的环

判断下列集合和给定运算是否构成环、整环和域.

(1) $A=\{a+bi \mid a,b\in \mathrm{Q}\}$, $i^2=-1$, 运算为复数加法和乘法.

(2) $A=\{2z+1 \mid z\in \mathrm{Z}\}$, 运算为普通加法和乘法

(3) $A=\{2z \mid z\in \mathrm{Z}\}$, 运算为普通加法和乘法

(4) $A=\{x \mid x\geq 0 \wedge x\in \mathrm{Z}\}$, 运算为普通加法和乘法.

(5) $A=\{a+b\sqrt[4]{5} \mid a,b\in \mathrm{Q}\}$, 运算为普通加法和乘法

- 解 (2), (4), (5) 不是环. 为什么?
- (1) 是环, 是整环, 也是域.
- (3) 是环, 不是整环和域.

# The End

机器人与信息自动化研究所

Institute of Robotics & Automatic Information System

南開大學

Nankai University