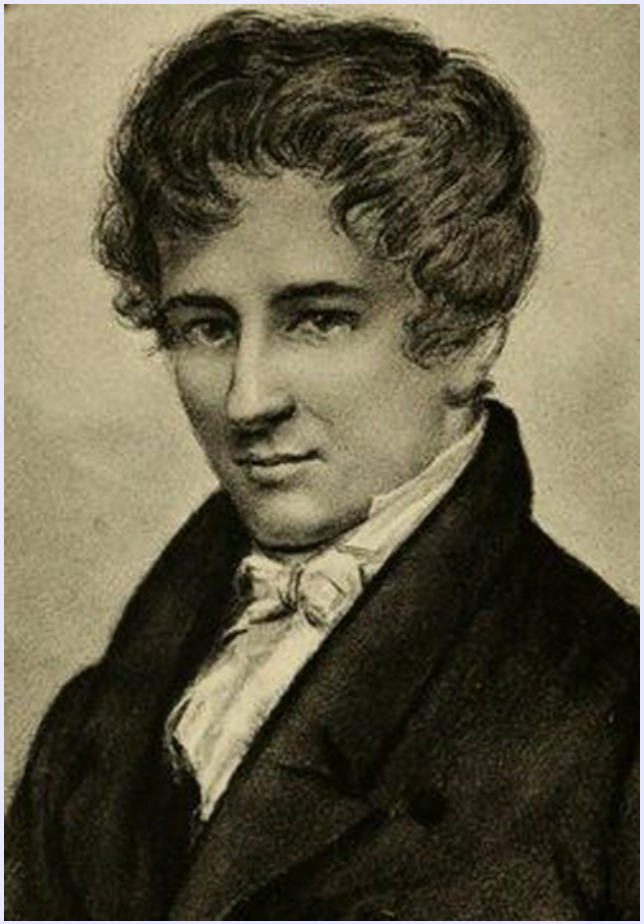
# 应用离散数学

离散数学课程组

2015 年 4 月 28 日



- 阿贝尔：挪威数学家，证明五次或更高次代数方程一般不能用根式求解，由此引起可交换群（即阿贝耳群）的概念。研究了二项级数的性质、阿贝耳积分和阿贝尔函数。在与雅可比的竞赛中共同完成了椭圆函数论的基础工作。
- 埃瓦里斯特·伽罗瓦：法国数学家.伽罗瓦提出的伽罗瓦理论是当代代数与数论的基本支柱之一。它直接推论的结果十分丰富：他系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解；证明高斯的论断：若用尺规作图能作出正$p$边形，$p$ 为质数(所以正十七边形可做图)；解决了古代三大作图问题中的两个:“不能任意三等分角”,“倍立方不可能”。

- 阿贝尔：挪威数学家，证明五次或更高次代数方程一般不能用根式求解，由此引起可交换群（即阿贝耳群）的概念。研究了二项级数的性质、阿贝耳积分和阿贝尔函数。在与雅可比的竞赛中共同完成了椭圆函数论的基础工作。
- 埃瓦里斯特·伽罗瓦：法国数学家.伽罗瓦提出的伽罗瓦理论是当代代数与数论的基本支柱之一。它直接推论的结果十分丰富：他系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解；证明高斯的论断：若用尺规作图能作出正$p$边形，$p$ 为质数(所以正十七边形可做图)；解决了古代三大作图问题中的两个:“不能任意三等分角”,“倍立方不可能”。

# 群、环、域

# 群、环、域

# 群、环、域

# 群、环、域

# 群、环、域

## 定义1 ($n$元运算)

设$X$是非空集合，从$X^n$到$X$上的函数$f$被称为集合$X$上的$n$元运算。

当$n=1$时，$f$被称为$X$上的一元运算

当$n=2$时，$f$被称为$X$上的二元运算

对于二元运算，

- $X$上任意两个元素都可以进行运算，且运算结果唯一；
- 封闭性：$X$上任意两个元素的运算结果仍然属于$X$。

## 定义1 ($n$元运算)

设$X$是非空集合，从$X^n$到$X$上的函数$f$被称为集合$X$上的$n$元运算。

当$n=1$时，$f$被称为$X$上的一元运算

当$n=2$时，$f$被称为$X$上的二元运算

对于二元运算，

- $X$上任意两个元素都可以进行运算，且运算结果唯一；
- 封闭性：$X$上任意两个元素的运算结果仍然属于$X$。

## 定义1 ($n$元运算)

设$X$是非空集合，从$X^n$到$X$上的函数$f$被称为集合$X$上的$n$元运算。

当$n=1$时，$f$被称为$X$上的一元运算

当$n=2$时，$f$被称为$X$上的二元运算

对于二元运算，

- $X$上任意两个元素都可以进行运算，且运算结果唯一；
- 封闭性：$X$上任意两个元素的运算结果仍然属于$X$。

## 定义1 ($n$元运算)

设$X$是非空集合，从$X^n$到$X$上的函数$f$被称为集合$X$上的$n$元运算。

当$n=1$时，$f$被称为$X$上的一元运算

当$n=2$时，$f$被称为$X$上的二元运算

对于二元运算，

- $X$上任意两个元素都可以进行运算，且运算结果唯一；
- 封闭性：$X$上任意两个元素的运算结果仍然属于$X$。

## 定义1 ($n$元运算)

设$X$是非空集合，从$X^n$到$X$上的函数$f$被称为集合$X$上的$n$元运算。

当$n=1$时，$f$被称为$X$上的一元运算

当$n=2$时，$f$被称为$X$上的二元运算

对于二元运算，

- $X$上任意两个元素都可以进行运算，且运算结果唯一；
- 封闭性：$X$上任意两个元素的运算结果仍然属于$X$。

## 定义1 ($n$元运算)

设$X$是非空集合，从$X^n$到$X$上的函数$f$被称为集合$X$上的$n$元运算。

当$n=1$时，$f$被称为$X$上的一元运算

当$n=2$时，$f$被称为$X$上的二元运算

对于二元运算，

- $X$上任意两个元素都可以进行运算，且运算结果唯一；
- 封闭性：$X$上任意两个元素的运算结果仍然属于$X$。

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | $\times$ |
| $(\mathbb{N}, -)$ | $\times$ | $(\mathbb{R}, \text{求倒数})$ | $\times$ |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | $\times$ |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | $\times$ | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | $\times$ |
| $(\mathbb{N}, -)$ | $\times$ | $(\mathbb{R}, \text{求倒数})$ | $\times$ |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | $\times$ |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | $\times$ | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | × |
| $(\mathbb{N}, -)$ | × | $(\mathbb{R}, \text{求倒数})$ | × |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | × |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | × | $(\hat{M}_n(R), \times)$ | ✓ |

| | | | |
|---|---|---|---|
| $(\mathbb{N}, +)$ | ✓ | $(\mathbb{N}, \text{相反数})$ | $\times$ |
| $(\mathbb{N}, -)$ | $\times$ | $(\mathbb{R}, \text{求倒数})$ | $\times$ |
| $(\mathbb{R}, \times)$ | ✓ | $(\mathbb{R}, \div)$ | $\times$ |
| $(\rho(A), \cup)$ | ✓ | $(\mathbb{Z}_m, +_m)$ | ✓ |
| $(\mathbb{Z}_m, \times_m)$ | ✓ | $(M_n(R), +)$ | ✓ |
| $(\hat{M}_n(R), +)$ | $\times$ | $(\hat{M}_n(R), \times)$ | ✓ |

## 定义2 (等幂律、交换律、结合律)

设$*$是非空集合$X$上的二元运算,

- 若$\forall x \in X$, 都有$x * x = x$, 则称$*$满足等幂律
  若$a \in X$满足$a * a = a$, 则称$a$是等幂元
- 若$\forall x, y \in X$, 有$x * y = y * x$, 则称$*$满足交换律
- 若$\forall x, y, z \in X$, $(x * y) * z = x * (y * z)$, 则称$*$满足结合律

## 定义2 (等幂律、交换律、结合律)

设$*$是非空集合$X$上的二元运算，

- 若$\forall x \in X$，都有$x * x = x$，则称$*$满足等幂律

  若$a \in X$满足$a * a = a$，则称$a$是等幂元

- 若$\forall x, y \in X$，有$x * y = y * x$，则称$*$满足交换律

- 若$\forall x, y, z \in X$，$(x * y) * z = x * (y * z)$，则称$*$满足结合律

## 定义2 (等幂律、交换律、结合律)

设$*$是非空集合$X$上的二元运算，

- 若$\forall x \in X$，都有$x * x = x$，则称$*$满足等幂律

  若$a \in X$满足$a * a = a$，则称$a$是等幂元
- 若$\forall x, y \in X$，有$x * y = y * x$，则称$*$满足交换律
- 若$\forall x, y, z \in X$，$(x * y) * z = x * (y * z)$，则称$*$满足结合律

## 定义2 (等幂律、交换律、结合律)

设$*$是非空集合$X$上的二元运算，

- 若$\forall x \in X$，都有$x * x = x$，则称$*$满足等幂律

  若$a \in X$满足$a * a = a$，则称$a$是等幂元
- 若$\forall x, y \in X$，有$x * y = y * x$，则称$*$满足交换律
- 若$\forall x, y, z \in X$，$(x * y) * z = x * (y * z)$，则称$*$满足结合律

## 定义2 (等幂律、交换律、结合律)

设$*$是非空集合$X$上的二元运算,

- 若$\forall x \in X$, 都有$x * x = x$, 则称$*$满足等幂律

  若$a \in X$满足$a * a = a$, 则称$a$是等幂元
- 若$\forall x, y \in X$, 有$x * y = y * x$, 则称$*$满足交换律
- 若$\forall x, y, z \in X$, $(x * y) * z = x * (y * z)$, 则称$*$满足结合律

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A \in \rho(X)$ | $\forall A \in \rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A \in \rho(X)$ | $\forall A \in \rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A \in \rho(X)$ | $\forall A \in \rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | $0,1$ | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A \in \rho(X)$ | $\forall A \in \rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A \in \rho(X)$ | $\forall A \in \rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | 0 | 0, 1 | 0 | 1 | 0 |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | 0, 1 | $0_n$ | $I_n$ | $\forall A \in \rho(X)$ | $\forall A \in \rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | × | × | × | × | × |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | × | × | ✓ |
| 结合律 | ✓ | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | × | × | × | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | × | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ | $(\mathbb{Z}_m,+_m)$ |
|---|---|---|---|---|---|
| 等幂律 | $\times$ | $\times$ | $\times$ | $\times$ | $\times$ |
| 等幂元 | $0$ | $0,1$ | $0$ | $1$ | $0$ |
| 交换律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| 结合律 | ✓ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ | $(\rho(X),\cap)$ |
| 等幂律 | $\times$ | $\times$ | $\times$ | ✓ | ✓ |
| 等幂元 | $0,1$ | $0_n$ | $I_n$ | $\forall A\in\rho(X)$ | $\forall A\in\rho(X)$ |
| 交换律 | ✓ | ✓ | $\times$ | ✓ | ✓ |
| 结合律 | ✓ | ✓ | ✓ | ✓ | ✓ |

## 定义3 (分配率、吸收律)

设$*, \circ$是非空集合$X$上的二元运算，

- 若$\forall x, y, z \in X$，有

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

则称$\circ$对$*$满足分配律。

若仅有第一式子成立，则称$\circ$对$*$满足左分配律

若仅有第二式子成立，则称$\circ$对$*$满足右分配律

- 若$\forall x, y \in X$，有$x \circ (x * y) = x, \quad x * (x \circ y) = x$则称$*$和$\circ$满足吸收律

## 定义3 (分配率、吸收律)

设$*, \circ$是非空集合$X$上的二元运算，

- 若$\forall x, y, z \in X$，有

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

则称$\circ$对$*$满足分配律。

若仅有第一式子成立，则称$\circ$对$*$满足左分配律

若仅有第二式子成立，则称$\circ$对$*$满足右分配律

- 若$\forall x, y \in X$，有$x \circ (x * y) = x, \quad x * (x \circ y) = x$则称$*$和$\circ$满足吸收律

## 定义3 (分配率、吸收律)

设$*, \circ$是非空集合$X$上的二元运算，

- 若$\forall x, y, z \in X$，有

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

则称$\circ$对$*$满足分配律。

若仅有第一式子成立，则称$\circ$对$*$满足左分配律

若仅有第二式子成立，则称$\circ$对$*$满足右分配律

- 若$\forall x, y \in X$，有$x \circ (x * y) = x, \quad x * (x \circ y) = x$则称$*$和$\circ$满足吸收律

## 定义3 (分配率、吸收律)

设$*, \circ$是非空集合$X$上的二元运算，

- 若$\forall x, y, z \in X$，有

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

则称$\circ$对$*$满足分配律。

若仅有第一式子成立，则称$\circ$对$*$满足左分配律

若仅有第二式子成立，则称$\circ$对$*$满足右分配律

- 若$\forall x, y \in X$，有$x \circ (x * y) = x, \quad x * (x \circ y) = x$则称$*$和$\circ$满足吸收律

## 定义3 (分配率、吸收律)

设$*, \circ$是非空集合$X$上的二元运算，

- 若$\forall x, y, z \in X$，有

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

则称$\circ$对$*$满足分配律。

若仅有第一式子成立，则称$\circ$对$*$满足左分配律

若仅有第二式子成立，则称$\circ$对$*$满足右分配律

- 若$\forall x, y \in X$，有$x \circ (x * y) = x, \quad x * (x \circ y) = x$则称$*$和$\circ$满足吸收律

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | $\surd$ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | $\surd$ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | $\surd$ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | × | × | × | ✓ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | × | × | × | ✓ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | $\surd$ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | $\surd$ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | ✓ |

| | $(\mathbb{N},+,\times)$ | $(\mathbb{Z}_m,+_m,\times_m)$ | $(M_n(R),+,\times)$ | $(\rho(X),\cap,\cup)$ |
|---|---|---|---|---|
| 分配率 | $\times$对$+$ | $\times_m$对$+_m$ | $\times$对$+$ | 都有 |
| 吸收律 | $\times$ | $\times$ | $\times$ | ✓ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (或 x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的*左零元*(或*右零元*)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的*零元*

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |

| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
|---|---|---|---|---|---|
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |

| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
|---|---|---|---|---|---|
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |

| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
|---|---|---|---|---|---|
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义4 (零元)

设$*$是非空集合$X$上的二元运算，如果存在$\theta_l \in X$(或$\theta_r \in X$)，使得$\forall x \in X$有

$$\theta_l * x = \theta_l, (\text{或} x * \theta_r = \theta_r)$$

则称$\theta_l$(或$\theta_r$)为$*$的左零元(或右零元)

如果$\theta$既是左零元又是右零元，则称$\theta$是$*$的零元

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 零元 | 无 | 0 | 无 | 无 | 无 |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 零元 | 0 | 无 | 无 | $X$ | $\emptyset$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的*左单位元*(或*右单位元*)

如果$e$既是左单位元，又是右单位元，则称其是*单位元*(*幺元*)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | 0 | 1 | $e_l = 0$ | $e_r = 1$ | 0 |

| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
|---|---|---|---|---|---|
| 单位元 | 1 | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |

| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
|---|---|---|---|---|---|
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |

| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
|---|---|---|---|---|---|
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义5 (单位元)

设$*$是非空集合$X$上的二元运算，如果存在$e_l \in X$(或$e_r \in X$)，使得$\forall x \in X$有

$$e_l * x = x \quad (\text{或} x * e_r = x)$$

则称$e_l$(或$e_r$)是$*$运算的左单位元(或右单位元)

如果$e$既是左单位元，又是右单位元，则称其是单位元(幺元)

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{R}, -)$ | $(\mathbb{R}^*, \div)$ | $(\mathbb{Z}_m, +_m)$ |
|---|---|---|---|---|---|
| 单位元 | $0$ | $1$ | $e_r = 0$ | $e_r = 1$ | $0$ |
| | $(\mathbb{Z}_m, \times_m)$ | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 单位元 | $1$ | $0_n$ | $I_n$ | $\emptyset$ | $X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的*左逆元*(或*右逆元*)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的*逆元*，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的左逆元(或右逆元)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的逆元，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 定义6 (逆元)

设$*$是非空集合$X$上的二元运算，$e$是其单位元。对于$x \in X$，如果存在$y_l \in X$(或$y_r \in X$)，使得

$$y_l * x = e, \quad (\text{或} x * y_r = e)$$

则称$y_l$(或$y_r$)是$x$关于$*$的**左逆元**(或**右逆元**)

如果$y$既是$x$的左逆元，又是$x$的右逆元，则称其是$x$的**逆元**，记为$x^{-1}$

| | $(\mathbb{N}, +)$ | $(\mathbb{N}, \times)$ | $(\mathbb{Z}_m, +_m)$ | $(\mathbb{Z}_m, \times_m)$ |
|---|---|---|---|---|
| 逆元 | $0^{-1} = 0$ | $1^{-1} = 1$ | $x^{-1} = m - x$ | $1^{-1} = 1$ |
| | $(M_n(R), +)$ | $(\hat{M}_n(R), \times)$ | $(\rho(X), \cup)$ | $(\rho(X), \cap)$ |
| 逆元 | $A^{-1} = -A$ | $A^{-1}$是其逆矩阵 | $\emptyset^{-1} = \emptyset$ | $X^{-1} = X$ |

## 例1

设$S = \mathbb{Q} \times \mathbb{Q}$,$*$是$S$上的二元运算: $\forall \langle u, v\rangle, \langle x, y\rangle \in S$

$$\langle u, v\rangle * \langle x, y\rangle = \langle u \cdot x, u \cdot y + v\rangle$$

1. $*$是否满足交换律、结合律、等幂率?
2. $*$是否有单位元、零元? 如果有，请指出，并求$S$中所有可逆元素的逆元

## 定理1

设$*$是非空集合$X$上的二元运算，则

1. 如果$X$中有关于$*$的左单位元$e_l$和右单位元$e_r$，则$e_l = e_r$，即其就是单位元，且单位元如存在必定唯一。
2. 如果$X$中有关于$*$的左零元$\theta_l$和右零元$\theta_r$，则$\theta_l = \theta_r$，即其就是零元，且零元如存在必定唯一。
3. 设$X$对运算$*$满足结合律，且$*$有单位元$e$。如果对于$x \in X$存在左逆元$y_l$和右逆元$y_r$，则$y_l = y_r$，即其就是$x$的逆元，且逆元如果存在必定唯一。

## 定理1

设$*$是非空集合$X$上的二元运算，则

1. 如果$X$中有关于$*$的左单位元$e_l$和右单位元$e_r$，则$e_l = e_r$，即其就是单位元，且单位元如存在必定唯一。
2. 如果$X$中有关于$*$的左零元$\theta_l$和右零元$\theta_r$，则$\theta_l = \theta_r$，即其就是零元，且零元如存在必定唯一。
3. 设$X$对运算$*$满足结合律，且$*$有单位元$e$。如果对于$x \in X$存在左逆元$y_l$和右逆元$y_r$，则$y_l = y_r$，即其就是$x$的逆元，且逆元如果存在必定唯一。

## 定理1

设$*$是非空集合$X$上的二元运算，则

1. 如果$X$中有关于$*$的左单位元$e_l$和右单位元$e_r$，则$e_l = e_r$，即其就是单位元，且单位元如存在必定唯一。
2. 如果$X$中有关于$*$的左零元$\theta_l$和右零元$\theta_r$，则$\theta_l = \theta_r$，即其就是零元，且零元如存在必定唯一。
3. 设$X$对运算$*$满足结合律，且$*$有单位元$e$。如果对于$x \in X$存在左逆元$y_l$和右逆元$y_r$，则$y_l = y_r$，即其就是$x$的逆元，且逆元如果存在必定唯一。

## 定理1

设$*$是非空集合$X$上的二元运算，则

1. 如果$X$中有关于$*$的左单位元$e_l$和右单位元$e_r$，则$e_l = e_r$，即其就是单位元，且单位元如存在必定唯一。
2. 如果$X$中有关于$*$的左零元$\theta_l$和右零元$\theta_r$，则$\theta_l = \theta_r$，即其就是零元，且零元如存在必定唯一。
3. 设$X$对运算$*$满足结合律，且$*$有单位元$e$。如果对于$x \in X$存在左逆元$y_l$和右逆元$y_r$，则$y_l = y_r$，即其就是$x$的逆元，且逆元如果存在必定唯一。

## 定义7 (消去律)

设$*$是非空集合$X$上的二元运算，如果$\forall x, y, z \in X$，$x \neq \theta$有

$$x * y = x * z \Rightarrow y = z, y * x = z * x \Rightarrow y = z$$

则称$*$满足消去律

如果只有第一式成立，则称其满足左消去律

如果只有第二式成立，则称其满足右消去律

## 定义7 (消去律)

设$*$是非空集合$X$上的二元运算，如果$\forall x, y, z \in X$，$x \neq \theta$有

$$x * y = x * z \Rightarrow y = z, y * x = z * x \Rightarrow y = z$$

则称$*$满足消去律

如果只有第一式成立，则称其满足左消去律

如果只有第二式成立，则称其满足右消去律

## 定义7 (消去律)

设$*$是非空集合$X$上的二元运算，如果$\forall x, y, z \in X$，$x \neq \theta$有

$$x * y = x * z \Rightarrow y = z, y * x = z * x \Rightarrow y = z$$

则称$*$满足消去律

如果只有第一式成立，则称其满足左消去律

如果只有第二式成立，则称其满足右消去律

## 定义8 (代数系统)

非空集合$G$和$G$上的$k$个代数运算$f_1, \cdots, f_k$(其中$f_i$是$n_i$元代数运算)组成的系统称为**代数系统**，简称**代数**，记为$\langle G, f_1, \cdots, f_k \rangle$，而$\langle n_1, \cdots, n_k \rangle$称为该代数系统的**类型**。

## 定义9 (同态映射)

设$\langle G, f_1, \cdots, f_k \rangle, \langle H, g_1, \cdots, g_k \rangle$是两个同类型的代数系统，映射$\phi : G \to H$。若

$$\phi(f_i(x_1, \cdots, x_{n_i})) = g_i(\phi(x_1), \cdots, \phi(x_{n_i})), i = 1, \cdots, k,$$

则称$\phi$是$G$到$H$的同态映射，简称同态。

## 定义8 (代数系统)

非空集合$G$和$G$上的$k$个代数运算$f_1, \cdots, f_k$(其中$f_i$是$n_i$元代数运算)组成的系统称为**代数系统**，简称**代数**，记为$\langle G, f_1, \cdots, f_k \rangle$，而$\langle n_1, \cdots, n_k \rangle$称为该代数系统的**类型**。

## 定义9 (同态映射)

设$\langle G, f_1, \cdots, f_k \rangle, \langle H, g_1, \cdots, g_k \rangle$是两个同类型的代数系统，映射$\phi : G \to H$。若

$$\phi(f_i(x_1, \cdots, x_{n_i})) = g_i(\phi(x_1), \cdots, \phi(x_{n_i})), i = 1, \cdots, k,$$

则称$\phi$是$G$到$H$的**同态映射**，简称**同态**。

## 例2

对于两个代数系统$\langle \mathbb{Z}, +, \times \rangle$、$\langle \{0,1\}, \leftrightarrow, \wedge \rangle$，定义映射

$$\phi(x) = \begin{cases} 0 & x\text{是偶数} \\ 1 & x\text{是奇数} \end{cases}$$

证明$\phi$是同态。

## 定义10

若$\phi: G \to H$是同态映射，且其是满射/单射/双射，则称$\phi$是满同态/单同态/同构。特别地，如果$G = H$，则分别称其为自同态/满自同态/单自同态/自同构。

## 例2

对于两个代数系统$\langle \mathbb{Z}, +, \times \rangle$、$\langle \{0,1\}, \leftrightarrow, \wedge \rangle$，定义映射

$$\phi(x) = \begin{cases} 0 & x\text{是偶数} \\ 1 & x\text{是奇数} \end{cases}$$

证明$\phi$是同态。

## 定义10

若$\phi : G \to H$是同态映射，且其是满射/单射/双射，则称$\phi$是满同态/单同态/同构。特别地，如果$G = H$，则分别称其为自同态/满自同态/单自同态/自同构。

## 例3

设$S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$，证明

$$\phi(a + b\sqrt{2}) = a - b\sqrt{2}$$

是$\langle S, + \rangle$的自同构。

## 例4

设$\phi$是$\langle M_n(\mathbb{R}), \times \rangle$与$\langle \mathbb{R}, \times \rangle$之间的映射

$$\phi(A) = |A|,$$

证明$\phi$是满同态。

## 例3

设$S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$，证明

$$\phi(a + b\sqrt{2}) = a - b\sqrt{2}$$

是$\langle S, + \rangle$的自同构。

## 例4

设$\phi$是$\langle M_n(\mathbb{R}), \times \rangle$与$\langle \mathbb{R}, \times \rangle$之间的映射

$$\phi(A) = |A|,$$

证明$\phi$是满同态。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 定理2

设$\langle G,*\rangle,\langle H,\cdot\rangle$是两个代数系统，其中$*,\cdot$都是二元运算，$\phi:G\to H$是同态映射，则

1. $\langle\phi(G),\cdot\rangle$是代数系统；
2. 若$*$在$G$上满足交换律，则$\cdot$在$\phi(G)$上满足交换律；
3. 若$*$在$G$上满足结合律，则$\cdot$在$\phi(G)$上满足结合律；
4. 若$e$是$\langle G,*\rangle$的单位元，则$\phi(e)$是$\langle\phi(G),\cdot\rangle$的单位元；
5. 若$\theta$是$\langle G,*\rangle$的零元，则$\phi(\theta)$是$\langle\phi(G),\cdot\rangle$的零元；
6. 若$a^{-1}$是$a$在$\langle G,*\rangle$中的逆元，则$\phi(a^{-1})$是$\phi(a)$在$\langle\phi(G),\cdot\rangle$中的逆元。

## 例5

证明不存在由$\langle \mathbb{Q}, + \rangle$到$\langle \mathbb{Q}^*, \times \rangle$的同构映射。

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |

| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |

| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |

| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 定义11 (半群)

设$G$是非空集合，$*$是$G$上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

| | $(\mathbb{N},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},-)$ | $(\mathbb{R}^*,\div)$ |
|---|---|---|---|---|
| 半群 | 是 | 是 | 否 | 否 |
| 有幺半群 | 是 | 是 | | |
| | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cup)$ |
| 半群 | 是 | 是 | 是 | 是 |
| 有幺半群 | 是 | 是 | 是 | 是 |

## 例6

设集合

$$G=\left\{\left.\begin{pmatrix}a_{11} & a_{12}\\ 0 & 0\end{pmatrix}\right| a_{11},a_{12}\in\mathbb{R}\right\}$$

$*$表示矩阵乘法，试问$\langle G,*\rangle$是否是半群，是否是有幺半群？

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

## 定义12 (群)

设$\langle G, * \rangle$是有幺半群，如果$\forall x \in G$，都存在逆元$x^{-1} \in G$，则称$\langle G, * \rangle$是群。

1. $G$非空
2. $*$是$G$上的运算
3. $*$满足结合律
4. 存在单位元
5. $G$中的每个元素都有逆元

若$\langle G, * \rangle$是群且$*$满足交换律，则称$\langle G, * \rangle$为交换群或阿贝尔群

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | $\times$ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | $\times$ | ✓ | $\times$ | $\times$ |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | $\times$ | $\times$ | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | $\times$ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | $\times$ | ✓ | $\times$ | $\times$ |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | $\times$ | $\times$ | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | $\times$ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | $\times$ | ✓ | $\times$ | $\times$ |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | $\times$ | $\times$ | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | $\times$ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | $\times$ | ✓ | $\times$ | $\times$ |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | $\times$ | $\times$ | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | $\times$ | ✓ | $\times$ | $\times$ | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | $\times$ | ✓ | $\times$ | $\times$ |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | $\times$ | $\times$ | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

| | $(\mathbb{N},+)$ | $(\mathbb{R},+)$ | $(\mathbb{N},\times)$ | $(\mathbb{R},\times)$ | $(\mathbb{R}^*,\times)$ |
|---|---|---|---|---|---|
| 群 | × | ✓ | × | × | ✓ |
| | $(\mathbb{Z}_m,+_m)$ | $(\mathbb{Z}_m,\times_m)$ | $(M_n(R),+)$ | $(M_n(R),\times)$ | $(\hat{M}_n(R),+)$ |
| 群 | ✓ | × | ✓ | × | × |
| | $(\hat{M}_n(R),\times)$ | $(\rho(X),\cap)$ | $(\rho(X),\cup)$ | | |
| 群 | ✓ | × | × | | |

## 例7

在整数集合$\mathbb{Z}$上定义运算$*$如下

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

判断$\langle \mathbb{Z}, * \rangle$是否是群?

## 例8

设$\langle G, * \rangle$是群，$\forall a \in G$，定义$G \to G$的映射$f_a$如下:

$$f_a(x) = x * a, \forall x \in G$$

令$H = \{f_a | a \in G\}$，证明$\langle H, \circ \rangle$是群，其中$\circ$表示复合运算。

## 例7

在整数集合$\mathbb{Z}$上定义运算$*$如下

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

判断$\langle \mathbb{Z}, * \rangle$是否是群?

## 例8

设$\langle G, * \rangle$是群，$\forall a \in G$，定义$G \to G$的映射$f_a$如下:

$$f_a(x) = x * a, \forall x \in G$$

令$H = \{f_a | a \in G\}$，证明$\langle H, \circ \rangle$ 是群，其中$\circ$表示复合运算。

## 定义13 (幂)

设$\langle G,*\rangle$是半群，$x\in G, n\in\mathbb{Z}^+$，定义

$$x^n=\begin{cases}x & n=1\\ x^{n-1}*x & n\geq 2\end{cases}$$

若$\langle G,*\rangle$还是有幺半群，$e$为单位元，则定义$x^0=e$

若$x$在$G$中存在逆元$x^{-1}$，则定义

$$x^{-n}=(x^{-1})^n.$$

## 定义13 (幂)

设$\langle G,*\rangle$是半群，$x\in G, n\in\mathbb{Z}^+$，定义

$$x^n=\begin{cases}x & n=1\\ x^{n-1}*x & n\geq 2\end{cases}$$

若$\langle G,*\rangle$还是有幺半群，$e$为单位元，则定义$x^0=e$

若$x$在$G$中存在逆元$x^{-1}$，则定义

$$x^{-n}=(x^{-1})^n.$$

## 定义13 (幂)

设$\langle G,*\rangle$是半群，$x\in G, n\in\mathbb{Z}^+$，定义

$$x^n=\begin{cases}x & n=1\\ x^{n-1}*x & n\geq 2\end{cases}$$

若$\langle G,*\rangle$还是有幺半群，$e$为单位元，则定义$x^0=e$

若$x$在$G$中存在逆元$x^{-1}$，则定义

$$x^{-n}=(x^{-1})^n.$$

## 定义13 (幂)

设$\langle G,*\rangle$是半群，$x\in G, n\in\mathbb{Z}^+$，定义

$$x^n=\begin{cases}x & n=1\\ x^{n-1}*x & n\geq 2\end{cases}$$

若$\langle G,*\rangle$还是有幺半群，$e$为单位元，则定义$x^0=e$

若$x$在$G$中存在逆元$x^{-1}$，则定义

$$x^{-n}=(x^{-1})^n.$$

## 例9

- 分别在群$\langle \mathbb{R}^*, \times \rangle, \langle \mathbb{R}, + \rangle$中计算$0.5^4, 0.5^0, (-2)^3, (-2)^{-3}$
- 分别在$\langle \hat{M}_r(R), \times \rangle, \langle M_2(R), + \rangle$中计算$\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}$的2、-1，-2次幂

## 定理3

设$\langle G, * \rangle$是一个群，则

- $\forall x \in G, (x^{-1})^{-1} = x$;
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$;
- $\forall m, n \in \mathbb{Z}, x^m * x^n = x^{m+n}, (x^m)^n = x^{mn}$;

## 例9

- 分别在群$\langle \mathbb{R}^*, \times \rangle, \langle \mathbb{R}, + \rangle$中计算$0.5^4, 0.5^0, (-2)^3, (-2)^{-3}$
- 分别在$\langle \hat{M}_r(R), \times \rangle, \langle M_2(R), + \rangle$中计算$\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}$的2、-1，-2次幂

## 定理3

设$\langle G, * \rangle$是一个群，则

- $\forall x \in G, (x^{-1})^{-1} = x;$
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1};$
- $\forall m, n \in \mathbb{Z}, x^m * x^n = x^{m+n}, (x^m)^n = x^{mn};$

## 例9

- 分别在群$\langle \mathbb{R}^*, \times \rangle, \langle \mathbb{R}, + \rangle$中计算$0.5^4, 0.5^0, (-2)^3, (-2)^{-3}$
- 分别在$\langle \hat{M}_r(R), \times \rangle, \langle M_2(R), + \rangle$中计算$\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}$的2、-1，-2次幂

## 定理3

设$\langle G, * \rangle$是一个群，则

- $\forall x \in G, (x^{-1})^{-1} = x;$
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1};$
- $\forall m, n \in \mathbb{Z}, x^m * x^n = x^{m+n}, (x^m)^n = x^{mn};$

## 例9

- 分别在群$\langle \mathbb{R}^*, \times \rangle, \langle \mathbb{R}, + \rangle$中计算$0.5^4, 0.5^0, (-2)^3, (-2)^{-3}$
- 分别在$\langle \hat{M}_r(R), \times \rangle, \langle M_2(R), + \rangle$中计算$\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}$的*2*、*-1*，*-2*次幂

## 定理3

设$\langle G, * \rangle$是一个群，则

- $\forall x \in G, (x^{-1})^{-1} = x;$
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1};$
- $\forall m, n \in \mathbb{Z}, x^m * x^n = x^{m+n}, (x^m)^n = x^{mn};$

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是**有限群**，$G$中元素的个数被称为其**阶数**，记为$|G|$。阶等于$1$的群被称为**平凡群**，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是**无限群**。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是**有限群**，$G$中元素的个数被称为其**阶数**，记为$|G|$。阶等于$1$的群被称为**平凡群**，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是**无限群**。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

**定义14 (有限群、无限群、阶数、平凡群)**

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果$G$是有限集合，则称$\langle G,*\rangle$是有限群，$G$中元素的个数被称为其阶数，记为$|G|$。阶等于$1$的群被称为平凡群，即其只有一个元素(单位元)。若$G$是无限集合，则称$\langle G,*\rangle$是无限群。

## 定义15 (次数)

设$\langle G,*\rangle$是一个群，$e$为其单位元。对于$x\in G$，使得$x^n=e$成立的最小正整数$n$被称为是$x$的次数，记为$|x|=n$。若不存在这样的正整数$n$，则称$x$是无限次元。

注1 (若$\langle G,*\rangle$是一个群，$x\in G$且$|x|=n$，则)

## 定义15 (次数)

设$\langle G,*\rangle$是一个群，$e$为其单位元。对于$x\in G$，使得$x^n=e$成立的最小正整数$n$被称为是$x$的次数，记为$|x|=n$。若不存在这样的正整数$n$，则称$x$是无限次元。

### 注1 (若$\langle G,*\rangle$是一个群，$x\in G$且$|x|=n$，则)

- $x^n=e$;
- $x^k\neq e, k=1,2,\cdots,n-1$;

**定义15 (次数)**

设$\langle G,*\rangle$是一个群，$e$为其单位元。对于$x\in G$，使得$x^n=e$成立的最小正整数$n$被称为是$x$的次数，记为$|x|=n$。若不存在这样的正整数$n$，则称$x$是无限次元。

**注1 (若$\langle G,*\rangle$是一个群，$x\in G$且$|x|=n$，则)**

- $x^n=e$;
- $x^k\neq e, k=1,2,\cdots,n-1$;

**定义15 (次数)**

设$\langle G,*\rangle$是一个群，$e$为其单位元。对于$x\in G$，使得$x^n=e$成立的最小正整数$n$被称为是$x$的次数，记为$|x|=n$。若不存在这样的正整数$n$，则称$x$是无限次元。

**注1 (若$\langle G,*\rangle$是一个群，$x\in G$且$|x|=n$，则)**

- $x^n=e$;
- $x^k\neq e, k=1,2,\cdots,n-1$;

**定义15 (次数)**

设$\langle G,*\rangle$是一个群，$e$为其单位元。对于$x\in G$，使得$x^n=e$成立的最小正整数$n$被称为是$x$的次数，记为$|x|=n$。若不存在这样的正整数$n$，则称$x$是无限次元。

**注1 (若$\langle G,*\rangle$是一个群，$x\in G$且$|x|=n$，则)**

- $x^n=e$;
- $x^k\neq e, k=1,2,\cdots,n-1$;

**定义15 (次数)**

设$\langle G,*\rangle$是一个群，$e$为其单位元。对于$x\in G$，使得$x^n=e$成立的最小正整数$n$被称为是$x$的次数，记为$|x|=n$。若不存在这样的正整数$n$，则称$x$是无限次元。

**注1 (若$\langle G,*\rangle$是一个群，$x\in G$且$|x|=n$，则)**

- $x^n=e$;
- $x^k\neq e, k=1,2,\cdots,n-1$;

例10 (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

例10 (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

例10 (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

例10 (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

**例10** (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

**例10** (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

**例10** (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

**例10** (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

**定理4 (方程的唯一可解性)**

设$\langle G,*\rangle$是一个半群，则$\langle G,*\rangle$是群的充要条件是：
$\forall a,b\in G$，方程$a*x=b,x*a=b$在$G$中都有唯一解。

**定理5**

设$\langle G,*\rangle$是一个群，$e$为单位元，则

**定理4 (方程的唯一可解性)**

设$\langle G,*\rangle$是一个半群，则$\langle G,*\rangle$是群的充要条件是：
$\forall a,b\in G$，方程$a*x=b,x*a=b$在$G$中都有唯一解。

**定理5**

设$\langle G,*\rangle$是一个群，$e$为单位元，则

1. 若$|G|>1$，则$\langle G,*\rangle$没有零元；
2. 除单位元以外，群$\langle G,*\rangle$中没有其他等幂元

## 定理4 (方程的唯一可解性)

设$\langle G,*\rangle$是一个半群，则$\langle G,*\rangle$是群的充要条件是:
$\forall a,b\in G$，方程$a*x=b,x*a=b$在$G$中都有唯一解。

## 定理5

设$\langle G,*\rangle$是一个群，$e$为单位元，则

1. 若$|G|>1$，则$\langle G,*\rangle$没有零元;
2. 除单位元以外，群$\langle G,*\rangle$中没有其他等幂元

## 定理4 (方程的唯一可解性)

设$\langle G,*\rangle$是一个半群，则$\langle G,*\rangle$是群的充要条件是:
$\forall a,b\in G$，方程$a*x=b,x*a=b$在$G$中都有唯一解。

## 定理5

设$\langle G,*\rangle$是一个群，$e$为单位元，则

1. 若$|G|>1$，则$\langle G,*\rangle$没有零元;
2. 除单位元以外，群$\langle G,*\rangle$中没有其他等幂元

## 定理6 (消去律)

设$\langle G,*\rangle$是群，则运算$*$在$G$上满足消去律。

即$\forall x,y,z\in G$，有

$$x*y=x*z\Rightarrow y=z,\qquad y*x=z*x\Rightarrow y=z$$

## 例11

设$\langle G,*\rangle$是有限群，$G=\{x_1,\cdots,x_n\}$。令

$$x_iG=\{x_i*x_j|j=1,2,\cdots,n\}$$

证明$x_iG=G$。

## 定理6 (消去律)

设$\langle G, * \rangle$是群，则运算$*$在$G$上满足消去律。

即$\forall x, y, z \in G$，有

$$x * y = x * z \Rightarrow y = z, \qquad y * x = z * x \Rightarrow y = z$$

## 例11

设$\langle G, * \rangle$是有限群，$G = \{x_1, \cdots, x_n\}$。令

$$x_i G = \{x_i * x_j | j = 1, 2, \cdots, n\}$$

证明$x_i G = G$。

## 定理7

设$\langle G, * \rangle$是群，$e$为单位元，$a \in G$且$|a| = n$，则

1. $a^k = e$的充要条件是$n \mid k$;
2. $|a^k| = \frac{n}{\gcd(k,n)} = \frac{\mathrm{lcm}(k,n)}{k}$;
3. $|a| = |a^{-1}|$;
4. $a^s = a^t$的充要条件是$s \equiv t \mod n$;

## 定理7

设$\langle G,*\rangle$是群，$e$为单位元，$a\in G$且$|a|=n$，则

1. $a^k=e$的充要条件是$n\mid k$;
2. $|a^k|=\frac{n}{\gcd(k,n)}=\frac{\mathrm{lcm}(k,n)}{k}$;
3. $|a|=|a^{-1}|$;
4. $a^s=a^t$的充要条件是$s\equiv t \mod n$;

## 例12

设$\langle G,*\rangle$是群，$e$是单位元，$a\in G$且$|a|=12$，

1. 求$a^2,a^5,a^{-3}$的次数；
2. 求整数$t,0\le t\le 11$，使得$a^{-14}=a^t$；
3. 求所有满足$a^t=a^7$的整数$t$；

## 例13

设$\langle G,*\rangle$是群，$a,b\in G$是有限次元，证明

$$|b^{-1}*a*b|=|a|$$

## 例12

设$\langle G,*\rangle$是群，$e$是单位元，$a\in G$且$|a|=12$，

1. 求$a^2,a^5,a^{-3}$的次数;
2. 求整数$t,0\leq t\leq 11$，使得$a^{-14}=a^t$;
3. 求所有满足$a^t=a^7$的整数$t$;

## 例13

设$\langle G,*\rangle$是群，$a,b\in G$是有限次元，证明

1. $|b^{-1}*a*b|=|a|$
2. $|a*b|=|b*a|$

## 定义16 (子群)

设$\langle G, * \rangle$是群，$H$是$G$的非空子集。若$H$对于运算$*$也构成群，则称$H$是$G$的子群。

- $\langle G, * \rangle, \{e\}$是$G$的子群，被称为平凡子群。
- 如$\langle \mathbb{Z}, + \rangle$是$\langle \mathbb{Q}, + \rangle$的子群。
- $\langle \mathbb{Z}_6, +_6 \rangle$有哪些子群？

## 定义16 (子群)

设$\langle G, * \rangle$是群，$H$是$G$的非空子集。若$H$对于运算$*$也构成群，则称$H$是$G$的子群。

- $\langle G, * \rangle, \{e\}$是$G$的子群，被称为平凡子群。
- 如$\langle \mathbb{Z}, + \rangle$是$\langle \mathbb{Q}, + \rangle$的子群。
- $\langle \mathbb{Z}_6, +_6 \rangle$有哪些子群？

## 定义16 (子群)

设$\langle G,*\rangle$是群，$H$是$G$的非空子集。若$H$对于运算$*$也构成群，则称$H$是$G$的子群。

- $\langle G,*\rangle,\{e\}$是$G$的子群，被称为平凡子群。
- 如$\langle\mathbb{Z},+\rangle$是$\langle\mathbb{Q},+\rangle$的子群。
- $\langle\mathbb{Z}_6,+_6\rangle$有哪些子群？

## 定义16 (子群)

设$\langle G, * \rangle$是群，$H$是$G$的非空子集。若$H$对于运算$*$也构成群，则称$H$是$G$的子群。

- $\langle G, * \rangle, \{e\}$是$G$的子群，被称为平凡子群。
- 如$\langle \mathbb{Z}, + \rangle$是$\langle \mathbb{Q}, + \rangle$的子群。
- $\langle \mathbb{Z}_6, +_6 \rangle$有哪些子群？

## 定理8 (子群的判定1)

设$\langle G,*\rangle$是群，$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

1. $\forall a\in H, a^{-1}\in H$
2. $\forall a,b\in H,\ a*b\in H$

## 定理9 (子群的判定2)

设$\langle G,*\rangle$是群，$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

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

## 定理8 (子群的判定1)

设$\langle G,*\rangle$是群，$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

1. $\forall a\in H, a^{-1}\in H$
2. $\forall a,b\in H,\ a*b\in H$

## 定理9 (子群的判定2)

设$\langle G,*\rangle$是群,$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

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

## 定理8 (子群的判定1)

设$\langle G,*\rangle$是群，$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

1. $\forall a\in H, a^{-1}\in H$
2. $\forall a,b\in H$，$a*b\in H$

## 定理9 (子群的判定2)

设$\langle G,*\rangle$是群,$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

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

## 定理8 (子群的判定1)

设$\langle G,*\rangle$是群，$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

1. $\forall a\in H, a^{-1}\in H$
2. $\forall a,b\in H$，$a*b\in H$

## 定理9 (子群的判定2)

设$\langle G,*\rangle$是群,$H$是$G$的非空子集，则$H$是$G$的子群的充要条件是

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

## 例14

若$\langle G,*\rangle$是群，$\forall a\in G$，则$H=\langle a\rangle=\{a^k|k\in\mathbb{Z}\}$是$G$的子群，被称为由$a$生成的子群。

## 例15

设$\langle G,*\rangle$是群，令$C$是$G$中与$G$中所有元素都可交换的元素构成的集合，即

$$C=\{a|a\in G\wedge\forall x\in G(a*x=x*a)\}$$

则$C$是$G$的子群，被称为$G$的中心。

## 例14

若$\langle G,*\rangle$是群，$\forall a\in G$，则$H=\langle a\rangle=\{a^k|k\in\mathbb{Z}\}$是$G$的子群，被称为由$a$生成的子群。

## 例15

设$\langle G,*\rangle$是群，令$C$是$G$中与$G$中所有元素都可交换的元素构成的集合，即

$$C=\{a|a\in G\wedge\forall x\in G(a*x=x*a)\}$$

则$C$是$G$的子群，被称为$G$的中心。

## 例16

设$\langle G,*\rangle$是群，$H,K$都是$G$的子群，证明

1. $H\cap K$是$G$的子群；
2. $H\cup K$是$G$的子群的充要条件是$H\subseteq K$或$K\subseteq H$

## 例16

设$\langle G,*\rangle$是群，$H,K$都是$G$的子群，证明

1. $H\cap K$是$G$的子群；
2. $H\cup K$是$G$的子群的充要条件是$H\subseteq K$或$K\subseteq H$

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

## 注2

- 一般情况下$aH$与$Ha$不相等；
- 当$G$是交换群时，$aH$与$Ha$相等。

## 例17 (已知$\langle Z_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

## 注2

- 一般情况下，左、右陪集并不相等；
- 当$G$是交换群时，左、右陪集相等；

例17 (已知$\langle Z_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

### 注2

- 一般情况下，左、右陪集并不相等；
- 当$G$是交换群时，左、右陪集相等；

例17 (已知$\langle\mathbb{Z}_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

## 注2

- 一般情况下，左、右陪集并不相等；
- 当$G$是交换群时，左、右陪集相等；

例17 (已知$\langle\mathbb{Z}_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

## 注2

- 一般情况下，左、右陪集并不相等；
- 当$G$是交换群时，左、右陪集相等；

例17 (已知$\langle\mathbb{Z}_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

## 注2

- 一般情况下，左、右陪集并不相等；
- 当$G$是交换群时，左、右陪集相等；

例17 (已知$\langle\mathbb{Z}_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定义17 (陪集)

设$\langle G,*\rangle$是群，$H$是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为$H$相应于$a$的左陪集
- $Ha=\{h*a|h\in H\}$为$H$相应于$a$的右陪集

## 注2

- 一般情况下，左、右陪集并不相等；
- 当$G$是交换群时，左、右陪集相等；

## 例17 (已知$\langle\mathbb{Z}_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

## 定理10

设$\langle G, * \rangle$是群，$H$是$G$的子群，定义$G$上的二元关系

$$R = \{\langle a, b \rangle | a \in G \wedge b \in G \wedge b^{-1} * a \in H\}$$

证明

1. $R$是$G$上的等价关系；
2. $[a]_R = aH$；

## 定理11

设$\langle G,*\rangle$是群，$H$是其子群，则$H$的所有左陪集构成$G$的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\varnothing$
- $\bigcup\limits_{a\in G}aH=G$

## 定理12

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a,b\in G$，有

- $aH=H\Leftrightarrow a\in H\Leftrightarrow aH\cap H\neq\varnothing$
- $aH=bH\Leftrightarrow ab^{-1}\in H\Leftrightarrow Ha^{-1}=Hb^{-1}$

## 定理11

设$\langle G,*\rangle$是群，$H$是其子群，则$H$的所有左陪集构成$G$的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\emptyset$
- $\bigcup\limits_{a\in G} aH=G$

## 定理12

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a,b\in G$，有

1. $a\in bH\Leftrightarrow b^{-1}*a\in H\Leftrightarrow aH=bH$
2. $a\in Hb\Leftrightarrow a*b^{-1}\in H\Leftrightarrow Ha=Hb$

## 定理11

设$\langle G,*\rangle$是群，$H$是其子群，则$H$的所有左陪集构成$G$的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\emptyset$
- $\bigcup\limits_{a\in G}aH=G$

## 定理12

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a,b\in G$，有

1. $a\in bH\Leftrightarrow b^{-1}*a\in H\Leftrightarrow aH=bH$
2. $a\in Hb\Leftrightarrow a*b^{-1}\in H\Leftrightarrow Ha=Hb$

## 定理11

设$\langle G,*\rangle$是群，$H$是其子群，则$H$的所有左陪集构成$G$的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\emptyset$
- $\bigcup\limits_{a\in G}aH=G$

## 定理12

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a,b\in G$，有

1. $a\in bH\Leftrightarrow b^{-1}*a\in H\Leftrightarrow aH=bH$
2. $a\in Hb\Leftrightarrow a*b^{-1}\in H\Leftrightarrow Ha=Hb$

## 定理11

设$\langle G,*\rangle$是群，$H$是其子群，则$H$的所有左陪集构成$G$的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\emptyset$
- $\bigcup\limits_{a\in G}aH=G$

## 定理12

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a,b\in G$，有

1. $a\in bH\Leftrightarrow b^{-1}*a\in H\Leftrightarrow aH=bH$
2. $a\in Hb\Leftrightarrow a*b^{-1}\in H\Leftrightarrow Ha=Hb$

## 定理11

设$\langle G,*\rangle$是群，$H$是其子群，则$H$的所有左陪集构成$G$的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\emptyset$
- $\bigcup\limits_{a\in G}aH=G$

## 定理12

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a,b\in G$，有

1. $a\in bH\Leftrightarrow b^{-1}*a\in H\Leftrightarrow aH=bH$
2. $a\in Hb\Leftrightarrow a*b^{-1}\in H\Leftrightarrow Ha=Hb$

## 定理13

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a\in G, H\sim aH, H\sim Ha$。

**定义18 (指数)**

## 定理13

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a\in G, H\sim aH, H\sim Ha$。

## 定义18 (指数)

群$\langle G,*\rangle$的子群$H$的左(右)陪集组成集合的基数被称为$H$在$G$中的指数，记为$[G:H]$。

## 定理13

设$\langle G,*\rangle$是群，$H$是其子群，则$\forall a\in G, H\sim aH, H\sim Ha$。

## 定义18 (指数)

群$\langle G,*\rangle$的子群$H$的左(右)陪集组成集合的基数被称为$H$在$G$中的指数，记为$[G:H]$。

## 定理14 (拉格朗日定理)

设$\langle G,*\rangle$是有限群，$H$是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

推论1 (设$\langle G,*\rangle$是$n$阶群，$a\in G$，则)

**定理14 (拉格朗日定理)**

设$\langle G,*\rangle$是有限群，$H$是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

**推论1 (设$\langle G,*\rangle$是$n$阶群，$a\in G$，则)**

1. $a^n=e$;
2. $|a|$是$n$的因子;
3. 若$n$是质数，则存在$a\in G$，使得$G=\langle a\rangle$，即质数阶群都是循环群。

**定理14 (拉格朗日定理)**

设$\langle G,*\rangle$是有限群，$H$是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

**推论1 (设$\langle G,*\rangle$是$n$阶群，$a\in G$，则)**

1. $a^n=e$;
2. $|a|$是$n$的因子;
3. 若$n$是质数，则存在$a\in G$，使得$G=\langle a\rangle$，即质数阶群都是循环群。

**定理14 (拉格朗日定理)**

设$\langle G,*\rangle$是有限群，$H$是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

**推论1 (设$\langle G,*\rangle$是$n$阶群，$a\in G$，则)**

1. $a^n=e$;
2. $|a|$是$n$的因子;
3. 若$n$是质数，则存在$a\in G$，使得$G=\langle a\rangle$，即质数阶群都是循环群。

**定理14 (拉格朗日定理)**

设$\langle G,*\rangle$是有限群，$H$是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

**推论1 (设$\langle G,*\rangle$是$n$阶群，$a\in G$，则)**

1. $a^n=e$;
2. $|a|$是$n$的因子;
3. 若$n$是质数，则存在$a\in G$，使得$G=\langle a\rangle$，即质数阶群都是循环群。

**定理14 (拉格朗日定理)**

设$\langle G,*\rangle$是有限群，$H$是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

**推论1 (设$\langle G,*\rangle$是$n$阶群，$a\in G$，则)**

1. $a^n=e$;
2. $|a|$是$n$的因子;
3. 若$n$是质数，则存在$a\in G$，使得$G=\langle a\rangle$，即质数阶群都是循环群。

## 例18

设$\langle G,*\rangle$是群，$a\in G$，记

$$\langle a\rangle=\{a^k|k\in\mathbb{Z}\}$$

证明

1. 当$a$是无限次元时，$\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
2. 当$|a|=n$时，$\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}$
3. $\langle\langle a\rangle,*\rangle$是群

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是**循环群**，$a$是其**生成元**，记为$G=\langle a\rangle$。

### 注3

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是循环群，$a$是其生成元，记为$G=\langle a\rangle$。

## 注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若$a$是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle$,$|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是$n$阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且$a$是生成元

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是循环群，$a$是其生成元，记为$G=\langle a\rangle$。

## 注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若$a$是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle,|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是$n$阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且$a$是生成元

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是循环群，$a$是其生成元，记为$G=\langle a\rangle$。

## 注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若$a$是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle,|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是$n$阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且$a$是生成元

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是循环群，$a$是其生成元，记为$G=\langle a\rangle$。

## 注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若$a$是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle,|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是$n$阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且$a$是生成元

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是**循环群**，$a$是其**生成元**，记为$G=\langle a\rangle$。

## 注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若$a$是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle$,$|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是$n$阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且$a$是生成元

## 定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是循环群，$a$是其生成元，记为$G=\langle a\rangle$。

## 注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若$a$是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle,|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是$n$阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且$a$是生成元

## 定理15

设$G = \langle a \rangle$是循环群，$a^0 = e$是单位元，则

1. 若$a$是无限次元，即$G = \{e, a^{\pm 1}, a^{\pm 2}, \cdots\}$，则$G$中只有2个生成元$a, a^{-1}$
2. 若$|a| = n$，即$G = \{e, a^1, a^2, \cdots, a^{n-1}\}$，则$a^k, 1 \leq k \leq n$是生成元的充要条件是

$$\gcd(k, n) = 1$$

即$G$中只有$\varphi(n)$个生成元，其中$\varphi(n)$表示$[1, n]$中与$n$互质的整数个数

## 定理15

设$G=\langle a\rangle$是循环群，$a^0=e$是单位元，则

1. 若$a$是无限次元，即$G=\{e,a^{\pm1},a^{\pm2},\cdots\}$，则$G$中只有$2$个生成元$a,a^{-1}$
2. 若$|a|=n$，即$G=\{e,a^1,a^2,\cdots,a^{n-1}\}$，则$a^k,1\leq k\leq n$是生成元的充要条件是

$$\gcd(k,n)=1$$

即$G$中只有$\varphi(n)$个生成元，其中$\varphi(n)$表示$[1,n]$中与$n$互质的整数个数

## 定理15

设$G=\langle a\rangle$是循环群，$a^0=e$是单位元，则

1. 若$a$是无限次元，即$G=\{e,a^{\pm1},a^{\pm2},\cdots\}$，则$G$中只有$2$个生成元$a,a^{-1}$
2. 若$|a|=n$，即$G=\{e,a^1,a^2,\cdots,a^{n-1}\}$，则$a^k,1\leq k\leq n$是生成元的充要条件是

$$\gcd(k,n)=1$$

即$G$中只有$\varphi(n)$个生成元，其中$\varphi(n)$表示$[1,n]$中与$n$互质的整数个数

## 定理15

设$G=\langle a\rangle$是循环群，$a^0=e$是单位元，则

1. 若$a$是无限次元，即$G=\{e,a^{\pm1},a^{\pm2},\cdots\}$，则$G$中只有$2$个生成元$a,a^{-1}$
2. 若$|a|=n$，即$G=\{e,a^1,a^2,\cdots,a^{n-1}\}$，则$a^k,1\leq k\leq n$是生成元的充要条件是

$$\gcd(k,n)=1$$

即$G$中只有$\varphi(n)$个生成元，其中$\varphi(n)$表示$[1,n]$中与$n$互质的整数个数

## 例19 (求出以下各个循环群所有的生成元)

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}_7^*, \times_7 \rangle$
3. 循环群$G = \{e, a, a^2, \cdots, a^{14}\}$

## 例20

设$G$是$n$阶循环群, $\forall m \in \mathbb{Z}, m|n$, 则必定存在$a \in G$, 使得$|a| = m$

## 例19 (求出以下各个循环群所有的生成元)

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}_7^*, \times_7 \rangle$
3. 循环群$G = \{e, a, a^2, \cdots, a^{14}\}$

## 例20

设$G$是$n$阶循环群, $\forall m \in \mathbb{Z}, m|n$, 则必定存在$a \in G$, 使得$|a| = m$

## 例19 (求出以下各个循环群所有的生成元)

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}_7^*, \times_7 \rangle$
3. 循环群$G = \{e, a, a^2, \cdots, a^{14}\}$

## 例20

设$G$是$n$阶循环群, $\forall m \in \mathbb{Z}, m|n$, 则必定存在$a \in G$, 使得$|a| = m$

## 练习1 (P130-9)

## 例19 (求出以下各个循环群所有的生成元)

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}_7^*, \times_7 \rangle$
3. 循环群$G = \{e, a, a^2, \cdots, a^{14}\}$

## 例20

设$G$是$n$阶循环群，$\forall m \in \mathbb{Z}, m|n$，则必定存在$a \in G$，使得$|a| = m$

### 练习1 (P130-9)

## 例19 (求出以下各个循环群所有的生成元)

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}_7^*, \times_7 \rangle$
3. 循环群$G = \{e, a, a^2, \cdots, a^{14}\}$

## 例20

设$G$是$n$阶循环群，$\forall m \in \mathbb{Z}, m|n$，则必定存在$a \in G$，使得$|a| = m$

## 练习1 (P130-9)