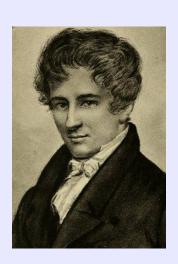
应用离散数学

离散数学课程组

2014年1月17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."不能任竟二等分鱼"."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"。

- 1 代数运算
- 2 半群与群
- 3 群的性质、循环群
- 4 子群
- 5 陪集

- 1 代数运算
- 2 半群与群
- 3 群的性质、循环群
- 4 子群
- 5 陪集

- 1 代数运算
- 2 半群与群
- 3 群的性质、循环群
- 4 子群
- 5 陪集

- 1 代数运算
- 2 半群与群
- 3 群的性质、循环群
- 4 子群
- 5 陪集

群、环、域

- 1 代数运算
- 2 半群与群
- 3 群的性质、循环群
- 4 子群
- 5 陪集



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。

- X上任怠两个元素都可以进行运算,且运算结果唯一;
- 封闭性: X上任怠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,

■ A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。



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。

- 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。

- 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。

- 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。

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{array}{ccccc} (\mathbb{N},+) & \checkmark & (\mathbb{N}, 相反数) & \times \\ (\mathbb{N},-) & \times & (\mathbb{R}, 求倒数) & \times \\ (\mathbb{R},\times) & \checkmark & (\mathbb{R},\div) & \times \\ (\rho(A),\cup) & \checkmark & (\mathbb{Z}_m,+_m) & \checkmark \\ (\mathbb{Z}_m,\times_m) & \checkmark & (M_n(R),+) & \checkmark \\ (\hat{M}_n(R),+) & \times & (\hat{M}_n(R),\times) & \checkmark \end{array}$$

群的性质、循环 00000000 子群

代数运算

练 为 1 (P118-1)



定义2 (等幂律、交换律、结合律)

- 若 $\forall x \in X$,都有x * x = x,则称*满足等幂律
- $\forall x, y \in X$, 有x * y = y * x, 则称*满足交换律
- \overrightarrow{A} $\forall x, y, z \in X$, (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)

- 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
- $\forall x, y \in X$, 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)

- 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
- $\overrightarrow{A} \forall x, y \in X$, 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)

- 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

- 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

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律					
等幂元					
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					
交换律					
结合律					

代数运算 00000000000 二元运算的性质

代数运算 00000000000 二元运算的性质

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×				
等幂元	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					
交换律					
200011					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×			
等幂元	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					
交换律					
7 L. A. 7-L-					
结合律					



	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×			
等幂元	0	0, 1			
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					
交换律					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×		
等幂元	0	0, 1			
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					
交换律					
/ 上 人 /士					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×		
等幂元	0	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					
等幂元 交换律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	
等幂元	0	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					
交换律					
从 人独					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	
等幂元	0	0, 1	0	1	
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					
寸かし					
交换律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	
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					
等幂元 交换律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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				
等幂元 交换律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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				
守布儿	0, 1				
交换律	0,1				
	0,1 ✓				

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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				
交换律					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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			
交换律					
结合律					

$(\mathbb{N},+)$ (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,$ 等幂律 \times	
等幂元 0 0,1 0 1 0	
交换律 × × × × × 结合律 × × × × × × × × × × × × × × × × × × ×	
结合律	
$(\mathbb{Z}_{++} \times_{++}) (M_{+}(R) +) (\hat{M}_{+}(R) \times) (\rho(X) +) (\rho(X) +)$	
$(2m, \wedge m)$ $(mn(1c), \wedge)$ $(p(21), \circ)$ $(p(21), \circ)$	$),\cap)$
等幂律 × × × ×	
等幂元 $0,1$ 0_n I_n $\forall A \in \rho(X)$ $\forall A \in P(X)$	
交换律	
结合律 ✓ ✓ ✓	



	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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	×	×	×	\checkmark	
等幂元	0, 1	0_n	I_n		
交换律					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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	×	×	×	\checkmark	
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	
交换律					
结合律					



	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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	×	×	×	\checkmark	\checkmark
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	
交换律					
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark				
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	×	×	×	\checkmark	\checkmark
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					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark	\checkmark	×		
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	×	×	×	\checkmark	\checkmark
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					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*,\div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0,1	0	1	0
交换律	\checkmark	\checkmark	×	×	
结合律					
	$(\mathbb{Z}_m, imes_m)$	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
等幂律	×	X	×	\checkmark	\checkmark
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					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark	✓	×	×	\checkmark
结合律					√
	$(\mathbb{Z}_m, imes_m)$	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
等幂律	×	×	×	\checkmark	\checkmark
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					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark	\checkmark	×	×	\checkmark
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	×	×	×	\checkmark	\checkmark
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	$\forall A \in \rho(X)$
交换律	\checkmark				
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark	\checkmark	×	×	\checkmark
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	×	×	×	\checkmark	\checkmark
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	$\forall A \in \rho(X)$
交换律	✓	\checkmark			
结合律					



	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark	\checkmark	×	×	\checkmark
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	×	×	×	\checkmark	\checkmark
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	$\forall A \in \rho(X)$
交换律	\checkmark	✓	×	\checkmark	
结合律					

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×	×	×	×	×
等幂元	0	0, 1	0	1	0
交换律	\checkmark	\checkmark	×	×	\checkmark
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	×	×	×	\checkmark	\checkmark
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	$\forall A \in \rho(X)$
交换律	\checkmark	\checkmark	×	\checkmark	\checkmark
结合律					

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

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

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

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

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





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

代数运算 ○○○●○○○○○○○ 二元运算的性质

定义3 (分配率、吸收律)

设*,○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o对*满足分配律。

定义3(分配率、吸收律)

设*,○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o对*满足分配律。

若仅有第一式子成立,则称o对*满足左分配律 若仅有第二式子成立,则称o对*满足右分配律



定义3(分配率、吸收律)

设*,○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o对*满足分配律。

若仅有第一式子成立,则称0对*满足左分配律

若仅有第二式子成立,则称0对*满足右分配律



定义3 (分配率、吸收律)

设*,o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o对*满足分配律。

若仅有第一式子成立,则称o对*满足左分配律 若仅有第二式子成立,则称o对*满足右分配律



定义3(分配率、吸收律)

设*,○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o对*满足分配律。

若仅有第一式子成立,则称o对*满足左分配律 若仅有第二式子成立,则称o对*满足右分配律



$$(\mathbb{N},+,\times)$$
 $(\mathbb{Z}_m,+_m,\times_m)$ $(M_n(R),+,\times)$ $(\rho(X),\cap,\cup)$ 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

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

	$(\mathbb{N},+, imes)$	$(\mathbb{Z}_m,+_m,\times_m)$	$(M_n(R),+,\times)$	$(\rho(X),\cap,\cup)$
分配率	$\times $ $ +$	$\times_m abla +_m$	\times \not $\!$	都有
吸收律	×	×		

	$(\mathbb{N},+, imes)$	$(\mathbb{Z}_m,+_m,\times_m)$	$(M_n(R),+,\times)$	$(\rho(X),\cap,\cup)$
分配率	$\times $ $\!$	$\times_m abla +_m$	$ imes$ $\!$	都有
吸收律	×	×	×	

	$(\mathbb{N},+, imes)$	$(\mathbb{Z}_m, +_m, \times_m)$	$(M_n(R),+,\times)$	$(\rho(X),\cap,\cup)$
分配率	$\times $ $ +$	$\times_m abla +_m$	\times \not $\!$	都有
吸收律	×	×	×	\checkmark

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

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

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

如果 θ 既是左零元又是右零元,则称 θ 是*的零元

$$(\mathbb{N},+)$$

$$(\mathbb{N}, \times)$$

$$(\mathbb{R},-)$$

$$(\mathbb{R}^*, \div)$$

$$(\mathbb{Z}_m,+_m$$

零九

$$\mathbb{Z}_m, \times_m)$$

$$(M_n(R),+)$$

$$(\hat{M}_n(R), \times)$$

$$(\rho(X), \cup)$$

$$(\rho(X), \cap$$

寒力

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

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

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

如果 θ 既是左零元又是右零元,则称 θ 是*的零元

$$(\mathbb{N},+)$$
 $(\mathbb{R},+)$ $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$

$$(\mathbb{Z}_m, \times_m)$$
 $(M_n(R), +)$ $(M_n(R), \times)$ $(\rho(X), \cup)$ $(\rho(X), \cap$

寒元



代数运算

○○○○○○ 二元运算的性质

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

$$\theta_l * x = \theta_l, (\mathbf{A} x * \theta_r = \theta_r)$$

则称 $\theta_l($ 或 $heta_r)$ 为st的左零元(或右零元)

如果 θ 既是左零元又是右零元,则称 θ 是*的零元

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

零元

$$(\mathbb{Z}_m, \times_m)$$
 $(M_n(R), +)$ $(\hat{M}_n(R), \times)$ $(\rho(X), \cup)$ $(\rho(X), \cap)$

東元

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

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

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

零元
$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$ 零元 \mathcal{H} $\mathcal{$

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

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

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

零元
$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$ 表元 \mathcal{H} $\mathcal{$

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

$$\theta_l * x = \theta_l, (\mathbf{A} x * \theta_r = \theta_r)$$

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

零元
$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$ 零元 \mathcal{H} $\mathcal{$

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

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

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

零元
$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$ 零元 \mathcal{H} $\mathcal{$

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

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

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

零元
$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$ 零元 \mathcal{E} $\mathcal{$

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

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

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

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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					

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

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

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

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

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

$$\theta_l * x = \theta_l, (\mathbf{A} x * \theta_r = \theta_r)$$

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

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

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

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

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

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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		

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

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

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

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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	

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

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

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

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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	Ø

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

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

则称 $e_i($ 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)

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

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

则称 $e_l(\mathbf{d}e_r)$ 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)

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

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

则称 $e_l(\dot{\mathfrak{q}}e_r)$ 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)

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

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

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)

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

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

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)

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

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

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

则称 $e_l(\mathbf{d}e_r)$ 是*运算的左单位元(或右单位元)

单位元
$$(\mathbb{N},+)$$
 (\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 0 0 0

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

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

则称 $e_l($ 或 $e_r)$ 是*运算的左单位元(或右单位元)

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

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

则称 $e_l(\mathbf{d}e_r)$ 是*运算的左单位元(或右单位元)

単位元
$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,+_m)$ 单位元 (\mathbb{Z}_m,\times_m) $(M_n(R),+)$ $(\hat{M}_n(R),\times)$ $(\rho(X),\cup)$ $(\rho(X),\cap)$ 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

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

则称 $e_l(\mathbf{d}e_r)$ 是*运算的左单位元(或右单位元)

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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					

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

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

则称 $e_l(\mathbf{d}e_r)$ 是*运算的左单位元(或右单位元)

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

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

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

则称 $e_l($ 或 $e_r)$ 是*运算的左单位元(或右单位元)

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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			

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

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

则称 $e_l($ 或 $e_r)$ 是*运算的左单位元(或右单位元)

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

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

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

则称 $e_l(\mathbf{d}e_r)$ 是*运算的左单位元(或右单位元)

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

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

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

则称 $e_l(\mathbf{d}e_r)$ 是*运算的左单位元(或右单位元)

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

代数运算

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 $y_1 \in X$ (或 $y_r \in X$),使得

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

则称 $y_l($ 或 $y_r)$ 是x关于st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}

逆元		
逆元		

代数运算

00000000000

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

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

则称 $y_l(\mathbf{d}y_r)$ 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 $(M_n(R),+)$ $(\hat{M}_n(R),\times)$ $(\rho(X),\cup)$ $(\rho(X),\cap)$ 逆元 $A^{-1}=A$ A^{-1} 是其連矩阵 $(M^{-1}=0)$ $X^{-1}=X$

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

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

则称 $y_l(\mathbf{d}y_r)$ 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<mark>逆元</mark>,记为 x^{-1}

$$(\mathbb{N},+)$$
 (\mathbb{N},\times) $(\mathbb{Z}_m,+_m)$ (\mathbb{Z}_m,\times_m) 逆元 $(M_n(R),+)$ $(\hat{M}_n(R),\times)$ $(\rho(X),\cup)$ $(\rho(X),\cap)$ 逆元 $(M_n(R),\times)$ $(M_n(R),\times$

代数运算

○○○○○○○○ 二元运算的性质 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 $y_1 \in X$ (或 $y_r \in X$), 使得

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

则称 $y_l(\mathbf{d}y_r)$ 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<mark>逆元</mark>,记为 x^{-1}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\mathbb{Z}_m, \times_m)
逆元				
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
·* —				

逆元 $A^{-1} = -A$ A^{-1} 是具逆矩阵 $\emptyset^{-1} = \emptyset$ $X^{-1} = X$

代数运算

○○○○○○○○ 二元运算的性质

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

则称 $y_l(\mathbf{d}y_r)$ 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}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\mathbb{Z}_m, \times_m)
逆元	$0^{-1} = 0$			
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
774 —				

逆兀

代数运算

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

则称 $y_l(\mathbf{d}y_r)$ 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}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	$(\mathbb{Z}_m, imes_m)$
逆元	$0^{-1} = 0$	$1^{-1} = 1$		
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$

逆元

代数运算

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

则称 $y_l(\mathbf{d}y_r)$ 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}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\mathbb{Z}_m, \times_m)
逆元	$0^{-1} = 0$	$1^{-1} = 1$	$x^{-1} = m - x$	
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
) JA				

逆兀

代数运算

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

则称 $y_l(\mathbf{d}y_r)$ 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}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\mathbb{Z}_m, \times_m)
逆元	$0^{-1} = 0$	$1^{-1} = 1$	$x^{-1} = m - x$	$1^{-1} = 1$
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
/7K —				

逆兀

代数运算

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

则称 $y_l(\mathbf{d}y_r)$ 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}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	$(\mathbb{Z}_m, imes_m)$
逆元	$0^{-1} = 0$	$1^{-1} = 1$	$x^{-1} = m - x$	$1^{-1} = 1$
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
油量	$A^{-1} - A$			

代数运算

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

则称 $y_l(\mathbf{d}y_r)$ 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}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\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		

代数运算

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 $y_1 \in X$ (或 $y_r \in X$), 使得

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

则称 $y_l(\mathbf{d}y_r)$ 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<mark>逆元</mark>,记为 x^{-1}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\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	$\emptyset^{-1} = \emptyset$	

代数运算

○○○○○○○○ 二元运算的性质

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 $y_1 \in X$ (或 $y_r \in X$), 使得

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

则称 $y_l(\mathbf{d}y_r)$ 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<mark>逆元</mark>,记为 x^{-1}

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{Z}_m,+_m)$	(\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

代数运算

○○○○○○○○○ 二元运算的性质

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

设 $S = \mathbb{O} \times \mathbb{O}$.*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

练习2 (P119-4)

代数运算

○○○○○○○○○ 二元运算的性质

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 θ_l 和右零元 θ_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。

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 θ_l 和右零元 θ_r ,则 $\theta_l = \theta_r$,即 其就是零元,且零元如存在必定唯一。
- 图 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。

代数运算

○○○○○○○ 二元运算的性质

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 θ_l 和右零元 θ_r ,则 $\theta_l = \theta_r$,即其就是零元,且零元如存在必定唯一。
- 图 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。



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 θ_l 和右零元 θ_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。



代数运算

○○○○○○○ 二元运算的性质

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



代数运算

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

作业1 (P119-5)



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

作业1 (P119-5)



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

作业1 (P119-5)



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。

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。

(N,+)
 (N,×)
 (R,-)
 (R*,÷)

 半群
 是
 者
 者

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

 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

有幺半群

$$(\mathbb{Z}_m, \times_m)$$
 $(M_n(R), +)$ $(\hat{M}_n(R), \times)$ $(\rho(X), \cup)$

半群

有幺半群

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。

$$(\mathbb{N},+) \qquad \quad (\mathbb{N},\times) \qquad \quad (\mathbb{R},-) \qquad \quad (\mathbb{R}^*,\div)$$

半群

是

是

否

否

有幺半群

$$(\mathbb{Z}_m, \times_m)$$
 $(M_n(R), +)$ $(\hat{M}_n(R), \times)$ $(\rho(X), \cup)$

半群

有幺半群

是

是 是

◆ロト ◆団ト ◆豆ト ◆豆 ・ りへぐ

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。

$$(\mathbb{N},+) \qquad \quad (\mathbb{N},\times) \qquad \quad (\mathbb{R},-) \qquad \quad (\mathbb{R}^*,\div)$$

半群

是

是

否

否

有幺半群

$$(\mathbb{Z}_m, \times_m)$$
 $(M_n(R), +)$ $(\hat{M}_n(R), \times)$ $(\rho(X), \cup)$

半群

有幺半群

是

是是

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。

半群
 足
 是
 否
 否

 有幺半群
 是
 と
 否

 (
$$\mathbb{Z}_m, \times_m$$
)
 ($M_n(R), +$)
 ($\hat{M}_n(R), \times$)
 ($\rho(X), \cup$)

 半群

有幺半群

是

是是

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。

(N,+)
 (N,×)
 (R,-)
 (R*,÷)

 半群
 是
 是
 否

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

 半群

有幺半群

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。

半群

有幺半群 是

是

正

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。

半群
 足
 足
 否
 管

 有幺半群
 是
 是
 否
 合

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

 半群

◆ロト ◆団ト ◆豆ト ◆豆 ◆ りへぐ

有幺半群

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。

半群
 足
 足
 否
 否

 有幺半群
 是
 是
 否
 否

 有幺半群
 是
 是
 と
 (
$$\hat{M}_n(R)$$
, ×)
 ($\rho(X)$, \cup)

 半群

4日 > 4周 > 4 国 > 4 国 >

有幺半群

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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			
有幺半群				

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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			
有幺半群	是			

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)
半群	是	是	否	否
有幺半群	是	是		
	(\mathbb{Z}_m, \times_m)	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X) \sqcup)$
	(,,	(11 ())	$(111111(10), \wedge)$	$(P(21), \circ)$
半群	是	是		(2(11), 3)

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。

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

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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	
有幺半群	是	是		

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。

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

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)
半群	是	是	否	否
有幺半群	是	是		
	(F77)	(1.5 (D))	(1)r (D)	/ (TT))
	(\mathbb{Z}_m, \times_m)	$(M_n(R),+)$	$(M_n(R),\times)$	$(\rho(X), \cup)$
半群	(\mathbb{Z}_m, \times_m) 是	$(M_n(R),+)$ 是	$(M_n(R), \times)$ 是	(ρ(X),∪) 是

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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

例2

设集合

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

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

例2

设集合

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

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

练习3 (P124-2)

マロケ マ倒す マラケ マラケ

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

 $\Xi\langle G,*
angle$ 是群且*满足交换律,则称 $\langle G,*
angle$ 为交换群或阿贝尔

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。

- 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

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。

- 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

 $\overline{A}\langle G,*
angle$ 是群且*满足交换律,则称 $\langle G,*
angle$ 为交换群或阿贝尔群

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。

- **I** 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

 $\Xi\langle G,*
angle$ 是群且*满足交换律,则称 $\langle G,*
angle$ 为交换群或阿贝尔

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。

- 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

 $\overline{A}\langle G,* \rangle$ 是群且*满足交换律,则称 $\langle G,* \rangle$ 为交换群或阿贝尔

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。

- 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

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

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。

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

 $\Xi\langle G,*
angle$ 是群且*满足交换律,则称 $\langle G,*
angle$ 为交换群或阿贝尔

群



	$(\mathbb{N},+)$	$(\mathbb{R},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R}, imes)$	$(\mathbb{R}^*, imes)$
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					

群
$$(\mathbb{N},+)$$
 $(\mathbb{R},+)$ (\mathbb{N},\times) (\mathbb{R},\times) (\mathbb{R}^*,\times) 群 \times \checkmark \times \times $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),+)$ $(\mathbb{M}_n(R),\times)$ $(\mathbb{M}_n(R),\times)$ $(\mathbb{M}_n(R),\times)$ $(\mathbb{M}_n(R),+)$

	$(\mathbb{N},+)$	$(\mathbb{R},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R}, imes)$	$(\mathbb{R}^*, imes)$
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					

	$(\mathbb{N},+)$	$(\mathbb{R},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R}, imes)$	$(\mathbb{R}^*, imes)$
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					

	$(\mathbb{N},+)$	$(\mathbb{R},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R}, imes)$	$(\mathbb{R}^*, imes)$
群	×	\checkmark	×	×	\checkmark
	$(\mathbb{Z}_m,+_m)$	(\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					

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

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

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

$$(\mathbb{N},+)$$
 $(\mathbb{R},+)$ (\mathbb{N},\times) (\mathbb{R},\times) (\mathbb{R}^*,\times) 群 \times \checkmark \times \times \checkmark $(\mathbb{Z}_m,+_m)$ (\mathbb{Z}_m,\times_m) $(M_n(R),+)$ $(M_n(R),\times)$ $(\hat{M}_n(R),+)$ 群

半群

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

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

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

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

例3

在整数集合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4

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

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

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



例3

在整数集合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4

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

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

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



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

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

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

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

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

 $\Xi\langle G,*\rangle$ 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

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

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

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

 $\ddot{A}\langle G,* \rangle$ 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

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

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

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

 $\ddot{A}\langle G,* \rangle$ 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

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

半群

例5

- 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

半群

例5

- 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

练ヲ4 (P124-11)

例5

- 分别在群 $(\mathbb{R}^*, \times), (\mathbb{R}, +)$ 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

练习4 (P124-11)

例5

- 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

练习4 (P124-11)

设 $\langle G, * \rangle$ 是一个群,则

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

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11(有限群、无限群、阶数、平凡群)

设(G,*)是一个群,如果G是有限集合,则称(G,*)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(G,*)是无限群。

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11 (有限群、无限群、阶数、平凡群)

设(G,*)是一个群,如果G是有限集合,则称(G,*)是有限群,G中元素的个数被称为其阶数,记为|G|。阶等于I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(G,*)是无限群。



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11 (有限群、无限群、阶数、平凡群)

设(G,*)是一个群,如果G是有限集合,则称(G,*)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(G,*)是无限群。

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11 (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I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。

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11 (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。



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11 (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<mark>阶数</mark>,记为|G|。阶等于I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。

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11 (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I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



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11 (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<mark>阶数</mark>,记为|G|。阶等于I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



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11 (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<mark>阶数</mark>,记为|G|。阶等于I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。



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。

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)

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

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 $1\left(oldsymbol{\Xi}\langle G,st angle$ 是一个群, $x\in G$ 且|x|=n,则)

 $\mathbf{x}^n = e;$

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

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。

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

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

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。

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

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

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。

$\overline{\pm 1}$ (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6 (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)

例6(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)



例6 (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)

例6(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)



例6(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)

例6 (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)

例6(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)

例6 (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)

例6(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)

定理3 (方程的唯一可解性)

 $\mathcal{G}\langle G,st
angle$ 是一个半群,则 $\langle G,st
angle$ 是群的充要条件是: $orall a,b\in G$,方程ast x=b,xst a=b在G中都有唯一解。

定理4

设 $\langle G, * \rangle$ 是一个群, ϵ 为单位元, 则

 $\mathcal{E}[G] > 1$,则(G,*)没有不元;

1 徐华位元以外,群(G,+)中没有其他等系元

定理3 (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4

设 $\langle G, * \rangle$ 是一个群, e为单位元, 则

- 若|G| > 1,则(G,*)没有零元;
- 除单位元以外,群(G,*)中没有其他等幂元

定理3 (方程的唯一可解性)

 $\langle G, * \rangle$ 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4

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〈G,*〉中没有其他等幂元

定理3(方程的唯一可解性)

定理4

设 $\langle G, * \rangle$ 是一个群, e为单位元, 则

- **■** $\dot{A}|G| > 1$,则⟨G, *⟩没有零元;
- 2 除单位元以外,群(G,*)中没有其他等幂元

定理5 (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

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

设(G,*)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5 (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

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

例7

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 $x_iG = G$ 。



练习5 (P129-1)

练习5 (P129-1)

定理6

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

- $\mathbf{1} a^k = e$ 的充要条件是 $n \mid k$:
- $|a^k| = \frac{n}{\gcd(k,n)} = \frac{\text{lcm}(k,n)}{k};$
- $|a| = |a^{-1}|$:
- $a^s = a^t$ 的充要条件是 $s \equiv t \mod n$;

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

- 求a², a⁵, 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;

(10, 1/201), a, o C O 201/1 [10, 0 C O 201/1 [

群的性质

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

- **1** 求a², a⁵, 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9

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

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

设 $\langle G, * \rangle$ 是群, $a \in G$, 记

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

群的性质、循环群 0000000

证明

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



循环群

定义13 (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 $G = \langle a \rangle$ 。

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 $G = \langle a \rangle$ 。

- **1** 若|a| = n,则 $G = \langle a \rangle = \{e, a^1, a^2, \dots, a^{n-1}\}$
- ② 若a是无限次元,则 $G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \cdots \}$
- 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

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 $G = \langle a \rangle$ 。

- **1** 若|a| = n,则 $G = \langle a \rangle = \{e, a^1, a^2, \dots, a^{n-1}\}$
- ② 若a是无限次元,则 $G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \cdots\}$
- 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

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 $G = \langle a \rangle$ 。

- **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 $G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \cdots\}$
- 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

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 $G = \langle a \rangle$ 。

- **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 $G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \cdots \}$
- 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

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 $G = \langle a \rangle$ 。

- **1** 若|a| = n, 则 $G = \langle a \rangle = \{e, a^1, a^2, \dots, a^{n-1}\}$
- 2 若a是无限次元,则 $G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \cdots \}$
- 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

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 $G = \langle a \rangle$ 。

- **1** 若|a| = n, 则 $G = \langle a \rangle = \{e, a^1, a^2, \dots, a^{n-1}\}$
- 2 若a是无限次元,则 $G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \cdots \}$
- 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

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

- **II** 若a是无限次元,即 $G = \{e, a^{\pm 1}, a^{\pm 2}, \dots\}$,则G中只有2个生成元 a, a^{-1}
- ② 若|a| = n,即 $G = \{e, a^1, a^2, \dots, a^{n-1}\}$,则 $a^k, 1 \le k \le n$ 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

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 $G = \{e, a^1, a^2, \dots, a^{n-1}\}$,则 $a^k, 1 \le k \le n$ 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

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



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

- **I** 若a是无限次元,即 $G = \{e, a^{\pm 1}, a^{\pm 2}, \dots\}$,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



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

例12

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

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

例12

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



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

例12

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



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

例12

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6 (P130-9)

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

例12

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6 (P130-9)



- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为平凡子群
- $\overline{A}\langle G, * \rangle$ 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。
- 循环群的子群也必定是循环群。

定义14 (子群)

- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为<mark>平凡子群</mark>。
- $\overline{A} \langle G, * \rangle$ 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。
- 循环群的子群也必定是循环群。

定义14 (子群)

- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为<mark>平凡子群</mark>。
- $\overline{A}\langle G, * \rangle$ 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 \underline{a} 生成的子群。
- 循环群的子群也必定是循环群。

定义14 (子群)

- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为<mark>平凡子群</mark>。
- $\overline{A}\langle G, * \rangle$ 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 \underline{a} 生成的子群。
- ■循环群的子群也必定是循环群。

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

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

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

- $2 \ \forall a,b \in H, \ a*b \in H$

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

- $2 \forall a, b \in H, \ a * b \in H$

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)

 $\mathcal{C}(G,*)$ 是群,H是G的非空子集,则H是G的子群的充要条件是

- $2 \forall a, b \in H, a * b \in H$

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

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



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

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

则C是G的子群,被称为G的中心。

设(G,*)是群,H,K都是G的子群,证明

例13

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

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

则C是G的子群,被称为G的中心。

例14

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

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



作业3 (P134-3、4)

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

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3

- 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;



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3

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

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3

- 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15 (已知 $(\mathbb{Z}_6, +_6)$ 是群,求子群 $\{0, 2, 4\}$ 所有的陪集。

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3

- 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15 (已知 $(\mathbb{Z}_6, +_6)$ 是群,求子群 $\{0, 2, 4\}$ 所有的陪集。

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3

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

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3

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

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

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

证明

- R是G上的等价关系;
- $[a]_R = aH;$

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

- $\forall a, b \in G, \ \mathbf{f} aH = bH \mathbf{J} aH \cap bH = \emptyset$

设(G,*)是群, H是其子群, 则∀a,b ∈ G, 有

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 $aH \cap bH = \emptyset$

定理12

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

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

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

- $\forall a,b \in G$, f(aH) = bH $f(aH) \cap bH = \emptyset$

定理12

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

 $\blacksquare a \in bH \Leftrightarrow b^{-1} * a \in H \Leftrightarrow aH = bH$

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

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 $aH \cap bH = \emptyset$

定理12

 $\mathcal{C}(G,*)$ 是群,H是其子群,则 $\forall a,b \in G$,有

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

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 $aH \cap bH = \emptyset$

定理12

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

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



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 $aH \cap bH = \emptyset$

定理12

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

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



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

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

定义16 (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]。

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

定义16 (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]。

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

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

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

- $\blacksquare \ a^n = e;$
- 2 |a|是n的因子;
- $\exists n$ 是质数,则存在 $a \in G$,使得 $G = \langle a \rangle$,即质数阶群都是循环
- 作业4 (P140-3、4、7)

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

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

- $1 \quad a^n = e;$
- 2 |a|是n的因子;

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

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

推论 $1(\mathcal{C}(G,*)$ 是n阶群, $a \in G$, 则)

- $1 a^n = e;$
- 2 |a|是n的因子;

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

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

推论 $1(\mathcal{C}(G,*)$ 是n阶群, $a \in G$, 则)

- $1 a^n = e;$
- 2 |a|是n的因子;