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"。

■ 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 代数系统
- 3 半群与群
- 4 子群和陪集
- 5 循环群

- 1 代数运算
- 2 代数系统
- 3 半群与群
- 4 子群和陪集
- 5 循环群

群、环、域

- 1 代数运算
- 2 代数系统
- 3 半群与群
- 4 子群和陪集
- 5 循环群

群、环、域

- 1 代数运算
- 2 代数系统
- 3 半群与群
- 4 子群和陪集
- 5 循环群

群、环、域

- 1 代数运算
- 2 代数系统
- 3 半群与群
- 4 子群和陪集
- 5 循环群

定义1 (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。

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。

 $\exists n = 1$ 时,f被称为X上的一元运算 $\exists n = 2$ 时、f被称为X上的二元运算



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。

 $\exists n = 1$ 时,f被称为X上的一元运算 $\exists n = 2$ 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。

 $\exists n = 1$ 时,f被称为X上的一元运算 $\exists n = 2$ 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。

 $\exists n = 1$ 时,f被称为X上的一元运算 $\exists n = 2$ 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。



$(\mathbb{N},+)$	(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 (\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 $(\mathbb{Z}_m,+_m)$ \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 (\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) $(\rho(A),\cup)$ \checkmark $(\mathbb{Z}_m,+_m)$ \checkmark $(\hat{M}_n(R),+)$ \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) $(M_n(R),+)$ $(\hat{M}_n(R),+)$

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

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

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 $\forall x, y \in X$, 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

代数运算

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

代数运算

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 $\forall x, y \in X$,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

代数运算

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 $\forall x, y \in X$,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					
	(77)	(15 (D))	(3^r (D))	(())	((>
	$(\mathbb{Z}_m, imes_m)$	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
等幂律	(\mathbb{Z}_m, \times_m)	$(M_n(R),+)$	$(M_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
等幂律 等幂元	(\mathbb{Z}_m, \times_m) $0, 1$		$(M_n(R), \times)$ I_n	$(\rho(X), \cup)$ $\forall A \in \rho(X)$	1
	×	×	×	1	/
等幂元	×	×	I_n	1	√

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\mathbb{R}^*, \div)	$(\mathbb{Z}_m,+_m)$
等幂律	×				
等幂元					
交换律					
结合律					
	(\mathbb{Z}_m, \times_m)	$(M_n(R),+)$	$(\hat{M}(R) \vee)$	$(o(X) \perp \downarrow)$	$(\rho(X),\cap)$
	$(\underline{\omega}_m, \wedge_m)$	(mn(10), 1)	$(m_n(n), \wedge)$	$(p(X), \cup)$	$(\rho(X), \Box)$
等幂律	$(2m, \land m)$	(11111(111), 11)	$(m_n(n), \wedge)$	$(\rho(X), \bigcirc)$	(ρ(Λ'), Γ')
	$(2m, \times m)$ $0, 1$	0_n	I_n	$\forall A \in \rho(X)$	√
等幂元	×	×	×	V	√
等 幂 等 幂 元 交 换 律 结 合 律	×	×	I_n	V	√











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					
交换律					
结合律					

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	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					
交换律					
结合律					

代数运算 ○○○●○○○○○○○ 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	0, 1	0	1	0
交换律					
结合律					
	(77)	(14 (D))	(1 [^] (D))	((37))	((37) -)
	(\mathbb{Z}_m, \times_m)	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
等幂律	(\mathbb{Z}_m, \times_m)	$(M_n(R),+)$	$(M_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
等幂律 等幂元		$(M_n(R), +)$ 0_n	I_n	$(\rho(X), \cup)$ $\forall A \in \rho(X)$	*
	×	×	×	√	· · · · · · · · · · · · · · · · · · ·
等幂元	×	×	I_n	√	· · · · · · · · · · · · · · · · · · ·

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

代数运算 ○○○●○○○○○○○ 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	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	×	×	×	√ · · · ·	(() ()
等幂律 等幂元	× 0,1	\mathbf{x} 0_n	I_n	$\forall A \in \rho(X)$	/
	· · ·	- ' '	I_n	$\forall A \in \rho(X)$	/
等幂元	· · ·	- ' '	I_n \checkmark	$\forall A \in \rho(X)$	/

$(\mathbb{N},+)$ (\mathbb{N},\times) $(\mathbb{R},-)$ (\mathbb{R}^*,\div) $(\mathbb{Z}_m,-)$ 等幂律 \times	
等幂元 0 0,1 0 1 0 χ 交换律 χ χ χ χ χ 4 χ 5 χ 4 χ 6 χ 6 χ 6 χ 6 χ 6 χ 7 χ 6 χ 7 χ 7 χ 8 χ 9	
交換律 \times \times \times 结合律 (\mathbb{Z}_m,\times_m) $(M_n(R),+)$ $(\hat{M}_n(R),\times)$ $(\rho(X),\cup)$ $(\rho(X),0)$	
结合律 $ (\mathbb{Z}_m, \times_m) (M_n(R), +) (\hat{M}_n(R), \times) (\rho(X), \cup) \qquad (\rho(X), 0) $	
(\mathbb{Z}_m, \times_m) $(M_n(R), +)$ $(\hat{M}_n(R), \times)$ $(\rho(X), \cup)$ $(\rho(X), \cup)$	
等幂律 × ×	$(,\cap)$
44 - 14 - 14 - 14 - 14 - 14 - 14 - 14 -	
等幂元 $0,1$ 0_n I_n $\forall A \in \rho(X)$ $\forall A \in I_n$	
交换律	
结合律	

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	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					

代数运算 ○○○●○○○○○○○ 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	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		
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	×	×	×	\checkmark	\checkmark
等幂元	0, 1	0_n	I_n	$\forall A \in \rho(X)$	
交换律					
结合律					

X

0



代数运算 00000000000 二元运算的性质

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					1
	(\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					1
结合律					



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					

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	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					

X

0

代数运算 00000000000 二元运算的性质

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	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					

代数运算 ○○○●○○○○○○○ 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	0, 1	0	1	0
交换律	\checkmark	\checkmark	×	×	\checkmark
结合律	\checkmark	\checkmark	X	×	
	(\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					

代数运算 00000000000 二元运算的性质



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	\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	✓	✓	✓	

代数运算 ○○○●○○○○○○○ 二元运算的性质



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

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

■ 若 $\forall x, y \in X$,有 $x \circ (x * y) = x$, $x * (x \circ y) = x$ 则

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o对*满足分配律。

■ 若 $\forall x, y \in X$, 有 $x \circ (x * y) = x$, $x * (x \circ y) = x$ 则



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 $\forall x, y \in X$, 有 $x \circ (x * y) = x$, $x * (x \circ y) = x$ 则



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

■ 若 $\forall x, y \in X$, 有 $x \circ (x * y) = x$, $x * (x \circ y) = x$ 则



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o对*满足右分配律

■ 若 $\forall x, y \in X$,有 $x \circ (x * y) = x$, $x * (x \circ y) = x$ 则 称*和o满足吸收律



00000000000 二元运算的性质

代数运算

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

分配率

吸收律

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

```
(\rho(X), \cap, \cup)
              (\mathbb{N}, +, \times)
                              (\mathbb{Z}_m, +_m, \times_m)
                                                     (M_n(R),+,\times)
分配率
                \times对+
```

吸收律

吸收律

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

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

代数运算 ○○000●000000 二元运算的性质

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

代数运算

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 $\forall x \in X$ 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)

如果 θ 既是左零元又是右零元,则称 θ 是*的零元

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

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

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

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

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

零元

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

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

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

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

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

寒力

代数运算

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)

如果 θ 既是左零元又是右零元,则称 θ 是*的零元

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

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

寒元



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)如果 θ 既是左零元又是右零元,则称 θ 是*的零元

(N,+)
 (N,×)
 (R,-)
 (R*,÷)
 (
$$\mathbb{Z}_m,+_m$$
)

 零元
 九
 九
 九

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

《日》《圖》《意》《意》

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} $\mathcal{$

代数运算

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

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} $\mathcal{$

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

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

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

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				

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			

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		

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	X	

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, \times_m)	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
零元	0	无	无	X	Ø

代数运算

定义5 (单位元)

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

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

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

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 $e_l(\dot{\mathfrak{q}}e_r)$ 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)

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)

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

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)

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

代数运算

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)

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

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)

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

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 $e_l(\underline{\mathfrak{q}}e_r)$ 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)

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

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

代数运算 ○○00000●0000 二元运算的性质

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 $e_l(\underline{\mathfrak{q}}e_r)$ 是*运算的左单位元(<u>\mathred</u>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)

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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 $e_l(\underline{\mathfrak{q}}e_r)$ 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)

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

代数运算 ○○00000●0000 二元运算的性质 代数运算

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)

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

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)

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

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

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

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}

逆元		

代数运算 ○○000000●000 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 $y_l \in X(\underline{\mathfrak{q}}y_r \in X)$, 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 λx^{-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} 是其連集権 $(M^{-1}=0)$ $X^{-1}=X$

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 $y_l \in X$ (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}

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

(4日) (日) (日) (日) (日) (日)

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	$0^{-1} = 0$			
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
/ 本一				

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

代数运算 ○○000000●000 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

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

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	$0^{-1} = 0$	$1^{-1} = 1$		
	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$	$(\rho(X),\cap)$
) JA				

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

代数运算 ○○000000●000 二元运算的性质 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 $y_l \in X$ (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}

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

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

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 $y_l \in X(\underline{\mathfrak{q}}y_r \in X)$, 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 λx^{-1}

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

沙兀

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 $y_l \in X(\underline{\mathfrak{q}}y_r \in X)$, 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 λx^{-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	$A^{-1} - A$			

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 $y_2 \in X$), 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		

代数运算 ○○000000●000 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 $y_l \in X(\underline{\mathfrak{q}}y_r \in X)$, 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 λx^{-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	$\emptyset^{-1} = \emptyset$	

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 $(\mathbf{d}$ 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	$\emptyset^{-1}=\emptyset$	$X^{-1}=X$

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

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

- *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*是非空集合X上的二元运算,则

- 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。
- 圆 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

- 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。



定理1

设*是非空集合X上的二元运算,则

- 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_1 和右零元 θ_r 、则 $\theta_1 = \theta_r$ 、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_1 和右逆元 y_r ,则 $y_1 = y_r$,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, 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

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



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, \dots, 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 $\langle G, f_1, \dots, f_k \rangle$,而 $\langle n_1, \dots, n_k \rangle$ 称为该代数系统的类型。

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

 $\phi(f_i(x_1,\cdots,x_{n_i})) = g_i(\phi(x_1),\cdots,\phi(x_{n_i})), i = 1,\cdots,k,$ $4b \neq 0 \text{ and } 0 \text{ an$



定义8(代数系统)

非空集合G和G上的k个代数运算 f_1, \dots, 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、 i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)

 $\mathcal{C}(G, f_1, \cdots, f_k), \langle H, g_1, \cdots, g_k \rangle$ 是两个同类型的代数系 统、映射 $\phi: G \to H$ 。若

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

则称 ϕ 是G到H的同态映射,简称同态。



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

$$\phi(x) = \begin{cases} 0 & x \neq x \\ 1 & x \neq x \end{cases}$$

证明 0是 同态。

《日》《圖》《意》《意》

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

$$\phi(x) = \begin{cases} 0 & x \neq x \\ 1 & x \neq x \end{cases}$$

证明∂是同态。

定义10

 $\dot{\mathbf{z}} \phi: G \to H$ 是同态映射,且其是满射/单射/双射,则 ϕ 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。



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。

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



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∂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, ϕ : G → H 是同态映射, 则

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, ϕ : G → H 是同态映射, 则

- $1 \langle \phi(G), \cdot \rangle$ 是代数系统;

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, ϕ : G → H 是同态映射, 则

- $1 \langle \phi(G), \cdot \rangle$ 是代数系统;
- \mathbf{Z} 若*在 \mathbf{G} 上满足交换律,则·在 $\phi(\mathbf{G})$ 上满足交换律;

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

- $1 \langle \phi(G), \cdot \rangle$ 是代数系统;
- 若*在G上满足交换律、则·在φ(G)上满足交换律;
- 3 若*在G上满足结合律、则·在 $\phi(G)$ 上满足结合律;

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

- $1 \langle \phi(G), \cdot \rangle$ 是代数系统;
- 若*在G上满足交换律、则·在φ(G)上满足交换律;
- 3 若*在G上满足结合律、则·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;

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, ϕ : G → H 是同态映射、则

- $1 \langle \phi(G), \cdot \rangle$ 是代数系统;
- 若*在G上满足交换律、则·在φ(G)上满足交换律;
- 3 若*在G上满足结合律、则·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 θ 是 $\langle G, * \rangle$ 的零元,则 $\phi(\theta)$ 是 $\langle \phi(G), \cdot \rangle$ 的零元;

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, ϕ : G → H 是同态映射、则

- $\mathbf{I}(\phi(G),\cdot)$ 是代数系统;
- 若*在G上满足交换律、则·在φ(G)上满足交换律;
- 3 若*在G上满足结合律、则·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 θ 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。



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。

(N,+)
 (N,×)
 (R,-)
 (R*,÷)

 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

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

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

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

4日 > 4周 > 4 3 > 4 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。

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

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

4日 > 4周 > 4 国 > 4 国 >

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
 足
 と
 否

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

半群

有幺半群

4日 > 4周 > 4 国 > 4 国 >

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

4日 > 4周 > 4 国 > 4 国 >

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

4日 > 4周 > 4 国 > 4 国 >

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
 是
 是
 否
 管

 有幺半群
 是
 是
 否
 管

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

半群

有幺半群

4日 > 4周 > 4 国 > 4 国 >

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

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。

	$(\mathbb{N},+)$	$(\mathbb{N}, imes)$	$(\mathbb{R},-)$	(\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)	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\rho(X), \cup)$
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		
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	

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		
	(Z, ×, ,)	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(o(X) \perp \downarrow)$
	$(\underline{\omega}m, \wedge m)$	(mn(10), 1)	$(M_n(H), \wedge)$	(p(X), O)
半群	是 是	是	(<i>M_n</i> (<i>R</i>), ^)	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		
	(7 ×)	$(M_n(R),+)$	$(\hat{M}_n(R), \times)$	$(\circ(\mathbf{V}) \perp)$
	$(\angle m, \land m)$	$(M_n(n), \pm)$	$(M_n(n), \times)$	$(\rho(\Lambda), \cup)$
半群	(<i>a</i> _m , ∧ _m) 是	$\mathbb{R}^{(M_n(R),+)}$	$\mathbb{R}^{(M_n(\mathbf{R}),\times)}$	(ρ(A), U) 是

基本概念

例6

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?



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。

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

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

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

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

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。

半群与群

- 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

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





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

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

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

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

(4日) (個) (注) (注) 注 り(で)

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

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

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

基本概念

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?

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



基本概念

例7

在整数集合Z上定义运算*如下

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

半群与群

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:

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

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



定义13 (幂)

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

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

定义13 (幂)

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

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

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

幂运算

定义13(幂)

 $\mathcal{C}(G,*)$ 是半群, $x \in G, n \in \mathbb{Z}^+$,定义

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

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

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

定义13 (幂)

 $\mathcal{C}(G,*)$ 是半群, $x \in G, n \in \mathbb{Z}^+$,定义

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

半群与群 00000000000000

 $\dot{\mathbf{z}}(G,*)$ 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

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

幂运算

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

设
$$\langle G, * \rangle$$
是一个群,则

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

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

幂运算

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

设
$$\langle G, * \rangle$$
是一个群,则

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

例9

幂运算

- 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

设
$$\langle G, * \rangle$$
是一个群,则

- $\forall x \in G, (x^{-1})^{-1} = x$:
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$:

例9

■ 分别在群 $\langle \mathbb{R}^*, \times \rangle$, $\langle \mathbb{R}, + \rangle$ 中计算 $[0.5^4, 0.5^0, (-2)^3, (-2)^{-3}]$

半群与群 0000000000000

■ 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

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



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

群的性质

定义14 (有限群、无限群、阶数、平凡群)

 $\mathcal{C}(G,*)$ 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

 $\mathcal{C}(G,*)$ 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

 $\mathcal{C}(G,*)$ 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

 $\mathcal{C}(G,*)$ 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 $\langle G,*\rangle$ 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

半群与群

群的性质

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。

群的性质

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。

半群与群

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

- $x^n = e$:
- $x^k \neq e, k = 1, 2, \dots, n-1$:

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。

半群与群 0000000000000

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

- $x^n = e$:
- $x^k \neq e, k = 1, 2, \dots, n-1$:

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。

半群与群 0000000000000

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

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

		3	5	
1				
3				
5				

\times_7	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

\times_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2						
3						
4						
5						
6						

\times_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3						
4						
5						
6						

\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						
5						
6						

\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						
6						

\times_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6		3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6						

\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(G,*)是一个群, e为单位元, 则

 $\mathcal{E}[G] > 1$,则(G,*)没有不元;

除字位元以外,称 (G, η) 中没有其他等条元

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: $\forall a, b \in G$, $\forall a, b \in G$, $\forall a \in G$, $\forall a$

半群与群

设 $\langle G, * \rangle$ 是一个半群,则 $\langle G, * \rangle$ 是群的充要条件是: $\forall a, b \in G$, $\forall a, b \in G$, $\forall a \in G$, $\forall a$

定理5

 $\mathcal{C}(G,*)$ 是一个群, e为单位元, 则

- **■** 若|G| > 1,则⟨G,*⟩没有零元;

群的性质

设 $\langle G, * \rangle$ 是一个半群,则 $\langle G, * \rangle$ 是群的充要条件是: $\forall a, b \in G$, $\forall a, b \in G$, $\forall a \in G$, $\forall a$

定理5

 $\mathcal{C}(G,*)$ 是一个群, e为单位元, 则

- **■** 若|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

群的性质

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

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

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

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

半群与群

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 $x_iG = G_0$



群的性质

定理7

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

半群与群 00000000000000

定理7

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

半群与群 00000000000000

- $\mathbf{1} a^k = e$ 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 $s \equiv t \mod n$;

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 < t < 11, 使得 $a^{-14} = a^t$;
- ③ 求所有满足 $a^t = a^7$ 的整数t;

(ロ) (個) (重) (重) (重) の(の)

群的性质

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

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

定义16 (子群)

- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为<mark>平凡子群</mark>。

- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为<mark>平凡子群</mark>。
- 如⟨ℤ, +⟩是⟨ℚ, +⟩的子群。

定义16 (子群)

- $\langle G, * \rangle$, $\{e\}$ 是G的子群,被称为<mark>平凡子群</mark>。
- 如⟨ℤ, +⟩是⟨ℚ, +⟩的子群。
- ⟨ℤ₆, +₆⟩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

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

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(G,*)是群, H是G的非空子集, 则H是G的子群的充 要条件是

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



定理8(子群的判定1)

设(G,*)是群, H是G的非空子集, 则H是G的子群的充 要条件是

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



定理8(子群的判定1)

设(G,*)是群, H是G的非空子集, 则H是G的子群的充 要条件是

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

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

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



群,被称为由a生成的子群。

 $\dot{\mathbf{z}}\langle G,*\rangle$ 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(G,*)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

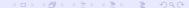
$$C = \{a | a \in G \land \forall x \in G(a * x = x * a)\}$$

则C是G的子群,被称为G的中心。

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

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 $K \subseteq H$



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;

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。

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。

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。)

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

- \blacksquare 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

- $\forall a,b \in G, \ faH = bH \otimes aH \cap bH = \emptyset$
- \blacksquare \Box aH = G

陪集

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

- $\forall a,b \in G$, $faH = bH \not aH \cap bH = \emptyset$
- \blacksquare \Box aH = G

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

- $\forall a,b \in G$, $faH = bH \not aH \cap bH = \emptyset$
- \blacksquare $\bigcup aH = G$ $a \in G$

陪集

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 $aH \cap bH = \emptyset$
- \blacksquare $\bigcup aH = G$ $a \in G$

定理12

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

陪集

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 $aH \cap bH = \emptyset$
- \blacksquare $\bigcup aH = G$ $a \in G$

定理12

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

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

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 $aH \cap bH = \emptyset$
- \blacksquare $\bigcup aH = G$ $a \in G$

定理12

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

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



陪集

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18 (指数)

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(G,*)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)

《日》《圖》《圖》《圖》

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] imes |H|。特别地|H|||G|。

- $1 \quad a^n = e;$
- 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|||G|。

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|||G|。

- 1 $a^n = e;$

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|||G|。

- 1 $a^n = e$:
- 2 |a|是n的因子;

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|||G|。

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

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 $G = \langle a \rangle$ 。

- 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
- \mathbf{A} 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+ 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
- \mathbf{A} 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
- \mathbf{A} 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

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

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

- 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}

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

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 $G = \{e, a^1, a^2, \dots, a^{n-1}\}$, 则 $a^k, 1 < k < n$ 是 生成元的充要条件是

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

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

- $1 \langle \mathbb{Z}, + \rangle$

- $1 \langle \mathbb{Z}, + \rangle$
- $2 \langle \mathbb{Z}_7^*, \times_7 \rangle$

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

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

例20

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

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

例20

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

练习1 (P130-9)