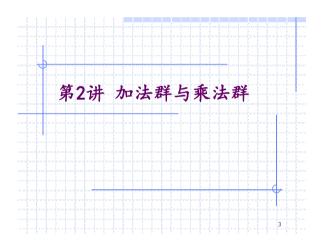
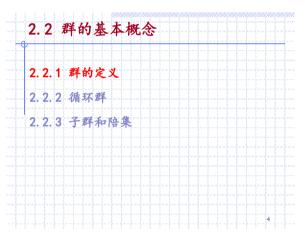


第2章 纠错编码的代数基础 ◆2.1整数的有关概念 ◆2.2群的基本概念 ◆加法群与乘法群 ◆2.3环的基本概念 ◆群、环、域 ◆2.4域的基本概念 ◆有限域上的运算





定义2-1 群 G 是一些元素构成的集合,该集合中定义一种 运算"*" (加法或乘法) ,满足: 1.封闭性,对任何 $a,b \in G$,有 $a*b \in G$ 2.结合律,对任何 $a,b,c \in G$, (a*b)*c=a*(b*c) 3.存在单位元 $e \in G$,使对任何 $a \in G$ 有 a*e=e*a=a	2.2.1 群的定义
 1.封闭性, 对任何a,b∈G, 有a*b∈G 2.结合律, 对任何a,b,c∈G, (a*b)*c=a*(b*c) 3.存在单位元e∈G, 使对任何a∈G有 	定义2-1 群G是一些元素构成的集合,该集合中定义一种运算"*" (加法或乘法) ,满足:
3.存在单位元e∈G,使对任何a∈G有	1.封闭性, 对任何 $a,b \in G$, 有 $a*b \in G$
a * e = e * a = a	
4.对任何a ∈ G有逆元a·1 ∈ G,使	
a*a ⁻¹ = a ⁻¹ *a = e 习惯上,若群的运算是加法,則简称加群;若群的运算	
才顶上,右折的远升及加宏,则同称加峰,右折的远升 是乘法,则简称 <mark>乘弊</mark> 。	

2. 2. 1	群的	定义	-加法	鲜	
		₹合及其. 位元和4		运算是? 的逆元。	5构
	封闭性	结合律	单位元	x的逆元	构成群
<z, +=""></z,>	V	√	0	-x	V
<2 Z , +>	√	V	0	-X	\checkmark
<q, +=""></q,>	V	V	0	-x	1
<r, +=""></r,>	√	V	0	-x	√
<c, +=""></c,>	√	√	0	-X	V
<m<sub>n(R), +></m<sub>	√	√	0矩阵	-X	1
					6

2.2.1 群的定义--乘法群

例: 判断下列集合及其上的二元运算是否构成群,指出单位元和每一元素的逆元。

- 8							
I		封闭性	结合律	单位元	x的逆元	构成群	
1	< Z , ×>	1	√	1 1-1	=1, (-1)-1=-1	, 否	
	<2 Z , ×>	$\sqrt{}$	\checkmark	无	无	否	
	< Q *, ×>	V	√	1	x=1=1/x	\checkmark	
	< R *, ×>	1	√	1	x-1=1/x	√	
	< C *, ×>	√	√	1	x-1=1/x	\checkmark	
	<m<sub>n(R), ×></m<sub>	√	√	I_n	可逆矩阵有 逆元	否	

2.2.1 群的定义

交換群 如果 "*" 运算还满足交换律,即对任何a,b $\in G$,有a*b=b*a,则G称作交换群。

加法群是交换群, 而乘法群不一定是交换群, 如矩阵 乘法不满足交换律。

群的阶 群的阶就是群中所含元素的个数。如整数加 法群和非0字数乘法群的阶都是无穷值。

有限群 阶为有限值的群称作有限群。

模d加法

例:模d的全体剩余类对模d的加法运算如下表所示:

7	\oplus	0	1	•••	<i>d</i> -2	<i>d</i> -1	<u>~</u>
	0	0	1	•••	d -2	d -1	×
	1	1	2		d -1	0	
	<i>d</i> -2	d -2	d -1		d -4	d -3	
	<i>d</i> -1	d -1	0		d -3	d -2	Ľ

构成交换加群,该群的阶为d,是有限群,记为< Z_d , \oplus >

模p(x)的加法

例:系数取自 $\{0,1\}$ 上的任意多项式以 $p(x) = x^3 + x + 1$ 为模,**全体剩余类的集合**为:

 $Z_2[x]_{p(x)} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ 问该集合关于模p(x)的加法是否构成群?

模 $p(x) = x^3 + x + 1$ 的加法

J. W. J									
Ф	0	1	x	x + 1	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	
0	0	1	x	x + 1	x^2	x^2+1	$x^2 + x$	$x^2 + x + 1$	ŀ
1	1	0							
x	x		0						
x + 1	x + 1			0					
x^2	x^2				0				
x^2+1	x^2+1					0			
$x^2 + x$	$x^2 + x$						0		
$x^2 + x + 1$	$x^2 + x + 1$							0	

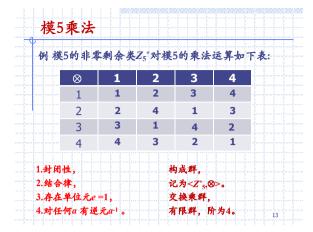
1.封闭性, 2.结合律, 3.存在单位元e=0, 4.对任何a 有逆元a-1=a。

构成群, 记为<Z₂[x] _{p(x)},⊕>。 交换加群, 有限群,阶为8。

加法群

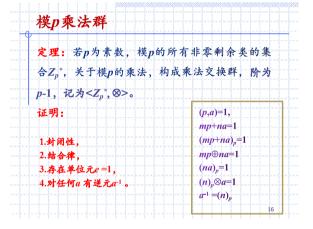
结论1:对于任意正整数d,模d的所有剩余类的集合 Z_d ,关于模d的加法构成加法交换群,阶为d,记为 $< Z_d$, $\oplus >$ 。

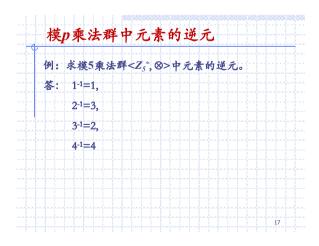
结论2: 对于F[x]中的任意多项式f(x),模f(x)的所有剩余类 $F[x]_{f(x)}$,关于模f(x)的加法构成加法交换群,记为 $< F[x]_{f(x)}$, $\oplus>$ 。

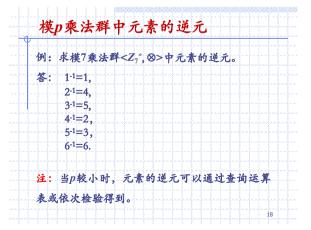


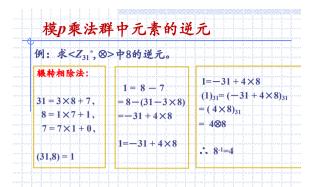
模7	乘法	ŧ .							
例模	7的非	零剩.	余类x	 模76	负乘法	运算	四下表		
	8	1	2	3	4	5	6		
	1								
	2								
	3								
	4								
	5								
	6								
								14	

例模	7的非	零剩	余类对	 模7的	负乘法	运算如	口下表	법
	8	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	

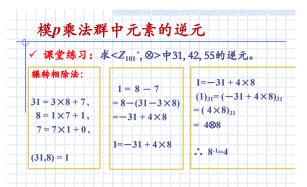






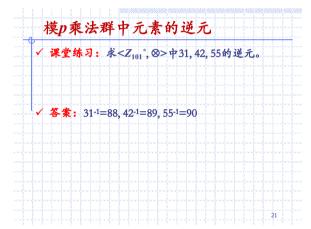


注: 当p较大时,元素的逆元要通过辗转相除法得到。



注: 当p较大时,元素的逆元要通过辗转相除法得到。

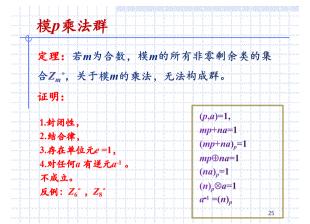
20

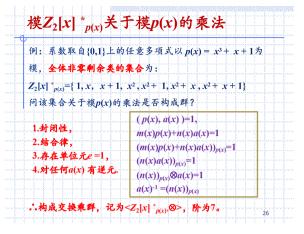


列模	6的非	零剩余	类对模	6的乘	法运算	如下扌	ŧ:
	8	1	2	3	4	5	
	1	1	2	3	4	5	
	2	2	4	0	2	4	
	3	3	0	3	0	3	
	4	4	2	0	4	2	
	5	5	4	3	2	1	

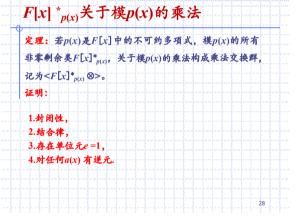
4444	44									
模	8乘	法								
•										
例本	莫8的	非零	剩余	类对相	莫8的	乘法:	运算女	中下:	表:	
	\otimes	1	2	3	4	5	6	7		
	1									
	2									
	3									
	4									
	5									
	6									
	7									
		ШП								
										23



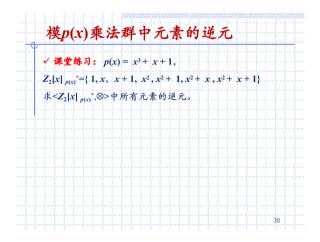




模 $Z_2[x]_{p(x)}$ *关于模 $p(x)=x^3+x+1$ 的乘法表 ② 1 x x+1 x^2 x^2+1 x^2+x+1 1 x^2 x^2+1 x^2+



模p(x)乘法群中元素的逆元 例: $p(x) = x^3 + x + 1$, $Z_2[x]_{p(x)}^* = \{1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$ 求 $< Z_2[x]_{p(x)}^*, \otimes >$ 中元素的逆元。 求 x^{-1} 解: (1) 辗转相除法求p(x)和x的最大公因子: $p(x) = (x^2 + 1)x + 1$, $\therefore (p(x), x) = 1$ (2) 将1表示或p(x)和x的线性组合为: $1 = p(x) + (x^2 + 1)x$, (3) 写出 x^{-1} : $x^{-1} = x^2 + 1$



模p(x)乘法群中元素的逆元

✓ 课堂练习: $p(x) = x^3 + x + 1$,

 $Z_2[x]_{n(x)} = \{1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

求 $< Z_2[x]_{p(x)}^*, \otimes >$ 中所有元素的逆元。

答案: 1-1=1.

 $x^{-1}=x^2+1$.

 $(x+1)^{-1}=x^2+x$,

 $(x^2)^{-1}=x^2+x+1,$ $(x^2+1)^{-1}=x$,

 $(x^2 + x)^{-1} = x + 1$

 $(x^2 + x + 1)^{-1} = x^2$

模 $F[x]_{f(x)}$ *关于模f(x)的乘法

例:系数取自 $\{0,1,2\}$ 上的任意多项式以 $f(x) = x^3 + x + 1$

为模,全体非零剩余类的集合为:

 $Z_3[x]_{f(x)}^* = \{ax^2 + bx + c | a,b,c \in Z_3\}$

问该集合关于模f(x)的乘法是否构成群?

 $f(x) = x^3 + x + 1 \pi Z_3[x] \perp$ 的不可约多项式。

1.封闭性,

2.结合律, 3.存在单位元e=1,

4.对任何a(x) 有逆元.

不成立。x+2无逆元 ... 不构成群。

模 $F[x] *_{f(x)}$ 关于模f(x)的乘法

定理: 若f(x) 是F[x]上的可约多项式。那么F[x]中以f(x) 为模的全体非零剩余类的集合F[x]* f(x) 关于模f(x)的乘法不能构成群。

证明:

✓ 课堂练习:

考察 $Z_2[x]$ 中多项式 $f(x) = x^3 + x^2 + 1$,

- (1) 试说明f(x) 是 $Z_{2}[x]$ 上的不可约多项式;
- (2) 在 $Z_2[x]_{f(x)}$ 上定义加法运算 \oplus 和乘法运算 \otimes 分 别为:

$$a(x) \oplus b(x) = a(x) + b(x)$$

$$a(x) \otimes b(x) = (a(x) b(x))_{f(x)}$$

请求出 (x^2+1) \oplus (x+1) 和 (x^2+1) \otimes (x+1) 的值。

(3) $Z_2[x]_{f(x)}$ 对于上面定义的加法运算 \oplus 和乘法运 算 ⊗构成一个有限域, 请求出x2+1 的逆元;

√ 答案:

(1) $: f(0) = 1 \neq 0$, $f(1) = 1 \neq 0$, f(x) = 0 f(x) = 0 Z_2 上无根,即无一次因式,又因为f(x)是3次的,所 以也无二次因式,所以是 $Z_2[x]$ 中的不可约多项式。

(2)
$$(x^2 + 1) \oplus (x + 1) = x^2 + x$$

$$(x^2+1)\otimes(x+1)=(x^3+x^2+x+1)_{f(x)}=x$$

(3)
$$(x^2+1)^{-1}=x^2+x+1$$