第2章 纠错编码的代数基础

第2章 纠错编码的代数基础

- ◈2.1整数的有关概念　◈整数与多项式
- ◈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

第2讲 加法群与乘法群

2.2 群的基本概念

2.2.1 群的定义

2.2.2 循环群

2.2.3 子群和陪集

2.2.1 群的定义

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

$$a * e = e * a = a$$

4.对任何$a \in G$有逆元$a^{-1} \in G$，使

$$a * a^{-1} = a^{-1} * a = e$$

习惯上，若群的运算是加法，则简称加群；若群的运算是乘法，则简称乘群。

2.2.1 群的定义—加法群

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。

	封闭性	结合律	单位元	x的逆元	构成群
<Z, +>	√	√	0	$-x$	√
<2Z, +>	√	√	0	$-x$	√
<Q, +>	√	√	0	$-x$	√
<R, +>	√	√	0	$-x$	√
<C, +>	√	√	0	$-x$	√
<M_n(R), +>	√	√	0矩阵	$-x$	√

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。

	封闭性	结合律	单位元	x的逆元	构成群
<Z, ×>	√	√	1	$1^{-1}=1$，$(-1)^{-1}=-1$，	否
<2Z, ×>	√	√	无	无	否
<Q*, ×>	√	√	1	$x^{-1}=1/x$	√
<R*, ×>	√	√	1	$x^{-1}=1/x$	√
<C*, ×>	√	√	1	$x^{-1}=1/x$	√
<M_n(R), ×>	√	√	I_n	可逆矩阵有逆元	否

7

2.2.1 群的定义

交换群 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实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。

8

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:

$\oplus$	0	1	…	d-2	d-1
0	0	1	…	d-2	d-1
1	1	2	…	d-1	0
…	…	…	…	…	…
d-2	d-2	d-1	…	d-4	d-3
d-1	d-1	0	…	d-3	d-2

构成交换加群，该群的阶为d，是有限群，记为<Z_d, ⊕>

9

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？

10

模$p(x)= x^3 + x + 1$的加法

$\oplus$	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
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<$Z_2[x]_{p(x)}$,⊕>。
交换加群，
有限群，阶为8。

11

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, ⊕>。

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<$F[x]_{f(x)}$，⊕>。

12

模5乘法

例 模5的非零剩余类Z_5^*对模5的乘法运算如下表:

⊗	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

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

构成群，
记为$<Z^*_5,⊗>$。
交换乘群，
有限群，阶为4。

13

模7乘法

例 模7的非零剩余类对模7的乘法运算如下表:

⊗	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

14

模7乘法

例 模7的非零剩余类对模7的乘法运算如下表:

⊗	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

构成群，记为$<Z^*_7,⊗>$。

15

模p乘法群

定理：若p为素数，模p的所有非零剩余类的集合Z_p^*，关于模p的乘法，构成乘法交换群，阶为p-1，记为$<Z_p^*,⊗>$。

证明：

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

$(p,a)=1$,
$mp+na=1$
$(mp+na)_p=1$
$mp⊕na=1$
$(na)_p=1$
$(n)_p⊗a=1$
$a^{-1}=(n)_p$

16

模p乘法群中元素的逆元

例：求模5乘法群$<Z_5^*,⊗>$中元素的逆元。

答： $1^{-1}=1$,
$2^{-1}=3$,
$3^{-1}=2$,
$4^{-1}=4$

17

模p乘法群中元素的逆元

例：求模7乘法群$<Z_7^*,⊗>$中元素的逆元。

答： $1^{-1}=1$，
$2^{-1}=4$，
$3^{-1}=5$，
$4^{-1}=2$，
$5^{-1}=3$，
$6^{-1}=6$.

注：当p较小时，元素的逆元可以通过查询运算表或依次检验得到。

18

模p乘法群中元素的逆元

例：求$<Z_{31}^*, \otimes>$中8的逆元。

辗转相除法：

$31 = 3\times8+7$,
$8 = 1\times7+1$,
$7 = 7\times1+0$,

$(31,8) = 1$

$1 = 8 - 7$
$= 8-(31-3\times8)$
$= -31+4\times8$

$1 = -31+4\times8$

$1 = -31+4\times8$
$(1)_{31} = (-31+4\times8)_{31}$
$= (4\times8)_{31}$
$= 4\otimes8$

$\therefore\ 8^{-1}=4$

注：当p较大时，元素的逆元要通过辗转相除法得到。

19

模p乘法群中元素的逆元

✓ 课堂练习：求$<Z_{101}^*, \otimes>$中31, 42, 55的逆元。

辗转相除法：

$31 = 3\times8+7$,
$8 = 1\times7+1$,
$7 = 7\times1+0$,

$(31,8) = 1$

$1 = 8 - 7$
$= 8-(31-3\times8)$
$= -31+4\times8$

$1 = -31+4\times8$

$1 = -31+4\times8$
$(1)_{31} = (-31+4\times8)_{31}$
$= (4\times8)_{31}$
$= 4\otimes8$

$\therefore\ 8^{-1}=4$

注：当p较大时，元素的逆元要通过辗转相除法得到。

20

模p乘法群中元素的逆元

✓ 课堂练习：求$<Z_{101}^*, \otimes>$中31, 42, 55的逆元。

✓ 答案：$31^{-1}=88$, $42^{-1}=89$, $55^{-1}=90$

21

模6乘法

例 模6的非零剩余类对模6的乘法运算如下表：

⊗	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

不构成群，因为2,3,4没有逆元。

22

模8乘法

例 模8的非零剩余类对模8的乘法运算如下表：

⊗	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							

23

模8乘法

例 模8的非零剩余类对模8的乘法运算如下表：

⊗	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

不构成群，因为2,4,6没有逆元。

24

模p乘法群

定理：若m为合数，模m的所有非零剩余类的集合Z_m^*，关于模m的乘法，无法构成群。

证明：

1.封闭性，
2.结合律，
3.存在单位元$e=1$，
4.对任何a 有逆元a^{-1} 。
不成立。
反例：Z_6^* ，Z_8^*

$(p,a)=1$,
$mp+na=1$
$(mp+na)_p=1$
$mp\oplus na=1$
$(na)_p=1$
$(n)_p\otimes a=1$
$a^{-1}=(n)_p$

25

模$Z_2[x]^*_{p(x)}$关于模$p(x)$的乘法

例：系数取自{0,1}上的任意多项式以$p(x)=x^3+x+1$为模，全体非零剩余类的集合为：

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

问该集合关于模$p(x)$的乘法是否构成群？

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.

$(p(x), a(x))=1$,
$m(x)p(x)+n(x)a(x)=1$
$(m(x)p(x)+n(x)a(x))_{p(x)}=1$
$(n(x)a(x))_{p(x)}=1$
$(n(x))_{p(x)}\otimes a(x)=1$
$a(x)^{-1}=(n(x))_{p(x)}$

∴构成交换乘群，记为$\langle Z_2[x]^*_{p(x)},\otimes\rangle$，阶为7。

26

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

$\otimes$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1							
x							
$x+1$							
x^2							
x^2+1							
x^2+x							
x^2+x+1							

27

$F[x]^*_{p(x)}$关于模$p(x)$的乘法

定理：若$p(x)$是$F[x]$中的不可约多项式，模$p(x)$的所有非零剩余类$F[x]^*_{p(x)}$，关于模$p(x)$的乘法构成乘法交换群，记为$\langle F[x]^*_{p(x)}\ \otimes\rangle$。

证明：

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.

28

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$\langle Z_2[x]_{p(x)}^*,\otimes\rangle$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表示成$p(x)$和x的线性组合为：

$1=p(x)+(x^2+1)x$,

（3）写出x^{-1}：

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

29

模$p(x)$乘法群中元素的逆元

✓ 课堂练习：$p(x)=x^3+x+1$,

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

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

30

模$p(x)$乘法群中元素的逆元

✓ 课堂练习： $p(x) = x^3 + x + 1$,

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

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

答案：$1^{-1}=1$,

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

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

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

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

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

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

31

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：

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

问该集合关于模$f(x)$的乘法是否构成群？

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

判断：

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.

∴不构成群。 不成立。 $x+2$无逆元

32

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：

33

✓ 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 $\otimes$构成一个有限域，请求出x^2+1 的逆元；

34

✓ 答案：

（1）$\because f(0) = 1 \neq 0$, ）$f(1) = 1 \neq 0$, $\therefore f(x) = 0$在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）$^{-1} = x^2 + x + 1$

35