第2章 纠错编码的代数基础

第2章 纠错编码的代数基础

第3讲 群、环、域

2.2 群的基本概念

2.2.2循环群的概念

循环群：由元素α的一切幂次构成的群

$$\{\alpha^0 = e,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$$

称为循环群。α称为生成元。

幂次的意义：

- 乘群：$<G, * >, \alpha^2 = \alpha * \alpha$
- 加群：$<G, + >, \alpha^2 = \alpha + \alpha$

$$\{0\alpha = e,\ \alpha,\ 2\alpha,\ \ldots,\ (n-1)\alpha\}$$

循环群的生成元

循环群：由元素α的一切幂次构成的群

$$\{\alpha^0 = e,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$$

称为循环群。α称为生成元。

幂次的意义：

- 乘群：$<G, * >, \alpha^2 = \alpha * \alpha$
- 加群：$<G, + >, \alpha^2 = \alpha + \alpha$

$$\{0\alpha = e,\ \alpha,\ 2\alpha,\ \ldots,\ (n-1)\alpha\}$$

元素的阶：使$\alpha^n = e$的最小正整数n称为元素α的阶。

生成元：若元素α的阶等于循环群G的阶，则α称为群G的生成元。

因为$\alpha^m * \alpha^n = \alpha^{m+n} = \alpha^{n+m} = \alpha^n * \alpha^m$,所以循环群是交换群。

$$m\alpha + n\alpha = (m+n)\alpha = (n+m)\alpha = n\alpha + m\alpha$$

循环群的生成元

例：模9的全体剩余类{0，1，2，3，4，5，6，7，8}，在模9加法运算⊕下构成群，记为<Z$_9$,⊕>，

(1)求出各个元素的幂次；

(2)求出各个元素的阶；

(3)指出哪些元素是模9加群的生成元。

循环群的生成元

例：模9的全体剩余类{0，1，2，3，4，5，6，7，8}，在模9加法运算⊕下构成群，记为<Z$_9$,⊕>，

(1)求出各个元素的幂次；

(2)求出各个元素的阶；

(3)指出哪些元素是模9加群的生成元。

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	元素的阶	生成元
0	0										1	×
1	0	1	2	3	4	5	6	7	8	0	9	√
2	0	2	4	6	8	1	3	5	7	0	9	√
3	0	3	6	0							3	×
4												
5												
6												
7												
8												

循环群的生成元

例：模9的全体剩余类{0，1，2，3，4，5，6，7，8}，在模9加法运算⊕下构成群，记为<Z$_9$,⊕>，

(1)求出各个元素的幂次；

(2)求出各个元素的阶；

(3)指出哪些元素是模9加群的生成元。

生成元：**1，2，4，5，7，8**

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	元素的阶	生成元
0	0										1	×
1	0	1	2	3	4	5	6	7	8	0	9	√
2	0	2	4	6	8	1	3	5	7	0	9	√
3	0	3	6	0							3	×
4	0	4	8	3	7	2	6	1	5	0	9	√
5	0	5	1	6	2	7	3	8	4	0	9	√
6	0	6	3	0							3	×
7	0	7	5	3	1	8	6	4	2	0	9	√
8	0	8	7	6	5	4	3	2	1	0	9	√

循环群的生成元

例：模9的全体剩余类{0，1，2，3，4，5，6，7，8}，在模9加法运算⊕下构成群，记为<Z$_9$,⊕>，

(1)求出各个元素的幂次；

(2)求出各个元素的阶；

(3)指出哪些元素是模9加群的生成元。

(4) 用2的幂次表示Z$_9$中的各个元素。

生成元：**1，2，4，5，7，8**

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	元素的阶	生成元
1	0	1	2	3	4	5	6	7	8	0	9	√
2	0	2	4	6	8	1	3	5	7	0	9	√

0	1	2	3	4	5	6	7	8
2^0	2^5	2^1	2^6	2^2	2^7	2^3	2^8	2^4

循环群的生成元

例：模9的全体剩余类{0，1，2，3，4，5，6，7，8}，在模9加法运算⊕下构成群，记为<Z$_9$,⊕>，

(1)求出各个元素的幂次；

(2)求出各个元素的阶；

(3)指出哪些元素是模9加群的生成元。

(4) 课堂练习：用5的幂次表示Z$_9$中的各个元素。

生成元：**1，2，4，5，7，8**

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	元素的阶	生成元
1	0	1	2	3	4	5	6	7	8	0	9	√
5	0	5	1	6	2	7	3	8	4	0	9	√

0	1	2	3	4	5	6	7	8
5^0	5^2	5^4	5^6	5^8	5^1	5^3	5^5	5^7

元素的阶

元素阶的性质：

(1) 若a是n阶元素，则$a^m = e$的充要条件是n整除m。

(2) 若某一群中，a是n阶元素，b是m阶元素，且（n，m）=1，则元素ab的阶为nm。

(3) 若a是n阶元素，则a^k的阶为n/(n,k).

子群和陪集---子群

子群：若群G的非空子集G'对于群G中所定义的代数运算也构成群，则称G'为G的子群。

例：< 2Z, + >是< Z, + >的子群；
< *m*Z, + >是< Z, + >的子群。

注：交换群<α >的任意元素都能生成一个循环子群<α^r >，元素的α^r阶 就是循环子群<α^r >的阶。

13

子群和陪集---子群

注：交换群<α >的任意元素都能生成一个循环子群<α^r >，元素的α^r阶 就是循环子群<α^r >的阶。

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	元素的阶	生成元
0	0										1	×
1	0	1	2	3	4	5	6	7	8	0	9	√
2	0	2	4	6	8	1	3	5	7	0	9	√
3	0	3	6	0							3	×
4	0	4	8	3	7	2	6	1	5	0	9	√
5	0	5	1	6	2	7	3	8	4	0	9	√
6	0	6	3	0							3	×
7	0	7	5	3	1	8	6	4	2	0	9	√
8	0	8	7	6	5	4	3	2	1	0	9	√

<Z_9,⊕>：Z_9 = <1 > = <2 > = <4 > = <5 > = <7 > = <8 > 。
<3 > = <6 > = {3^0, 3^1, 3^2}={0, 3, 6}
<6 > = {6^0, 6^1, 6^2}={0, 6, 3}
<3 > = <6 > = {0, 3, 6}　<{0, 3, 6} ,⊕>

定理2-3 有限群的子群的阶一定整除群的阶。

14

子群和陪集---陪集

设G'为群G的非空子群，取*h* ∈ G，则称*h* ∗ G'为G'的**左陪集**，称G'∗ *h* 为G'的**右陪集**。当G是交换群时，子群G'的左、右陪集是相等的，元素*h* 称作**陪集首**。

设子群G'= { g_1 , g_2 , … , g_n }，G'的阶为*n* ，又设G'为群G的子集，由定理2-3可知，若G的阶为*n*·*m*，可将G完备地分成*m*个陪集（子群本身也是一个陪集）。

例：群G=<Z_9,⊕>：子群G'=<3 > = <{0, 3, 6} ,⊕>
0 ⊕ G' =0 ⊕ {0, 3, 6}={0 ⊕0, 0 ⊕3, 0 ⊕6}={0, 3, 6}　　0 ⊕ G'=3 ⊕ G' =6 ⊕ G'
1 ⊕ G' =1 ⊕ {0, 3, 6}={1 ⊕0, 1 ⊕3, 1 ⊕6}={1, 4, 7}　　1 ⊕ G' =4 ⊕ G' =7 ⊕ G'
2 ⊕ G' =2 ⊕ {0, 3, 6}={2 ⊕0, 2 ⊕3, 2 ⊕6}={2, 5, 8}　　2 ⊕ G' =5 ⊕ G' = 8⊕ G'

G=<Z_9,⊕>= G' ∪ （1⊕ G'） ∪ （2 ⊕ G'）

15

子群和陪集---陪集

陪　集	说　明
h_1*g_1 =g_1 =*e*, g_2 , … , g_n	陪集首h_1=*e*，子群G'
h_2*g_1 , h_2*g_2 , … , h_2*g_n	陪集首h_2，子群h_2*G'
…　…　…	…　…　…
h_{m-1}*g_1 , h_{m-1}*g_2 , … , h_{m-1}*g_n	陪集首h_{m-1}，子群h_{m-1}*G'
h_m*g_1 , h_m*g_2 , … ,h_m*g_n	陪集首h_m，子群h_m*G'

16

子群和陪集

关于陪集首的几点说明：

- 若陪集首*h*是子群G'中的元素，则陪集*h** G'与子群G'相同。
- 若陪集首*h*不是子群G'中的元素，则陪集*h** G'与子群G'相交为空集。
- 若陪集首h_j 不是陪集h_i * G'中的元素，则两陪集h_i * G'与h_j * G'相交为空集。
- 陪集*h** G'中的每一个元素都可作为其陪集首，陪集元素不变，仅排列顺序改变。

17

子群和陪集

由以上性质可知，两个陪集要么相等要么不相交。为使群的分解完备，应选择前面未出现过的元素作为当前陪集的陪集首，这样，整个群将分解成若干个不相交的陪集，无一遗漏，无一重叠。

例2-10 模9加法运算下，群G={0,1,2,3,4,5,6,7,8}的一个子群G′ ={0,3,6}的陪集分解。

✓ 课堂练习：求出群G={0,1,2,3,4,5,6,7,8,9,10,11}的所有子群G′ ，并求出G关于三阶子群的陪集分解。

18

环的基本概念

◈环的定义

◈环的性质

◈子环

◈剩余类环

环的定义

<G,*> 是群：
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。

非空集合F中，若定义了加法和乘法两种运算，且满足：

1. F对加法运算是一个交换群；

2.1 F对乘法具有封闭性，即；$a\in F$，$b \in F$，有$ab\in F$；

2.2 F对乘法满足结合律： 对任何$a , b , c \in F$ ， 有

$$(a b) c = a (bc) ;$$

3. 乘法对加法满足分配律 ： 对任何$a , b , c \in F$ ， 有：

$a (b + c) = ab + ac$ $(a + b) c = ac + bc$

则称F是一个环。

若环F对乘法满足交换律，即对任何元素$a\in F$和$b \in F$，恒有$ab= ba$则称此环为交换环。

环的定义

$< F, +, \times >$是环：

<G,*> 是群：
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。

1. $< F, + >$: 交换群；
2 $< F, \times >$: 封闭性，结合律；
3. 乘法对加法满足分配律 。

例：$< Z, +, \times >$是环。
$< Z_m, \oplus, \otimes >$ 是环。

环的性质

对于任何$a\in F$，$b \in F$，有：

（1）$a \cdot 0=0 \cdot a=0$

（2）$a \cdot$（$-b$）＝（$-b$）$\cdot a= -ab$

（3）环中可以有零因子。

（4）有单位元且每个非零元素有逆元、非可换的环，称为除环。

子环

$< F, +, \times >$是环：

<G,*> 是群：
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。

1. $< F, + >$: 交换群；
2 $< F, \times >$: 封闭性，结合律；
3. 乘法对加法满足分配律 。

设F是一个环，S是F的一个非空子集，若S对F的加法运算和乘法运算也构成一个环，则称S是F的一个子环，F是S的一个扩环。

例：$< Z, +, \times >$是环。
$< mZ, +, \times >$是否为$< Z, +, \times >$的子环？ 是
$< Z_m, \oplus, \otimes >$ 是否为$< Z, +, \times >$的子环？ 否

剩余类环

剩余类环是一类重要的环，它是构成有限域的基础。

以整数m为模进行除法运算所得的全体剩余类可构成环，称作整数剩余类环。$< Z_m, \oplus, \otimes >$

同理，模$f(x)$的全体余式对模$f(x)$的运算构成交换环，称作多项式剩余类环 。$<F[x]_{f(x)}, \oplus, \otimes>$。

域的基本概念

◈域的定义

◈有限域

◈二元域的运算

25

域的定义

域是一些元素构成的集合，该集合中定义加法和乘法两种运算，满足：

（1）对加法构成交换加群；

（2）非零元素全体对乘法构成交换乘群；

（3）加法和乘法间具有分配律

$a(b+c) = ab + ac$，$(a+b)c = ac + bc$

域是一个可交换的、有单位元的、非零元素有逆元的环。

26

域的定义

$<F, +, \times>$是环：

1. $<F, +>$：交换群；
2 $<F, \times>$：封闭性，结合律；
3. 乘法对加法满足分配律 。

$<F, +, \times>$是域：

1. $<F, +>$：交换群；
2 $<F^*, \times>$：交换群；
3. 乘法对加法满足分配律 。

<G,*> 是群：
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。

27

域的实例

$<F, +, \times>$是域：
1. $<F, +>$：交换群；
2 $<F^*, \times>$：交换群；
3. 乘法对加法满足分配律 。

例子：判断下列代数系统是否是域：

1. $<Z, +, \times>$ 不是
2. $<Q, +, \times>$ 是
3. $<R, +, \times>$ 是
4. $<C, +, \times>$ 是

28

域的实例

（1） $<\mathbb{Q}, +, \times>$；

（2） $<\mathbb{R}, +, \times>$；

（3） $<\mathbb{C}, +, \times>$；

（4） $<\mathbb{Q}[\sqrt{2}], +, \times>$；

（5） $<\mathbb{Q}[\sqrt[3]{2}], +, \times>$；

（1-4）都是元素个数无限的域，称为无限域。

（5）不是域。

29

无限域与有限域

域中元素的个数称为域的阶。

无限域 元素个数无限的域。

有限域 元素个数有限的域，用GF(q)表示q阶有限域。有限域，又称为伽罗瓦（Galois）域。

30

域的实例

$<F, +, \times>$是域：

1. $<F, +>$：交换群；
2. $<F^*, \times>$：交换群；
3. 乘法对加法满足分配律。

例子：判断下列代数系统是否是域：

1. $<Z_2, \oplus, \otimes>$ 是
2. $<Z_5, \oplus, \otimes>$ 是
3. $<Z_8, \oplus, \otimes>$ 不是
4. $<Z_p, \oplus, \otimes>$ 是
5. $<Z_m, \oplus, \otimes>$ 不是

⊗	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	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

31

有限域的例子

（1）二元域，$GF(2)=<Z_2, \oplus, \otimes>$。

（2）p元域，$GF(p)=<Z_p, \oplus, \otimes>$。$Z_p=\{0,1,2,\dots,p-1\}$

定理：设p是素数，则以p为模的全体整数剩余类构成阶为p的有限域。

32

有限域的构造

构造有限域$<F[x]_{f(x)}, \oplus, \otimes>$

定理：若$f(x)$为$F[x]$上的n次不可约多项式，则$F[x]$关于模$f(x)$的全体剩余类的集合记为$F[x]_{f(x)}$，$F[x]_{f(x)}$关于模$f(x)$的加法和乘法构成域，记为$<F[x]_{f(x)}, \oplus, \otimes>$。

注：（1）若F是q个元素的有限域，则$<F[x]_{f(x)}, \oplus, \otimes>$为$q^n$个元素的有限域。

（2）$n=1$时，$<F[x]_{f(x)}, \oplus, \otimes>$即$F$，

（3）F是$<F[x]_{f(x)}, \oplus, \otimes>$的子域。

33

有限域的结构

- 对任意素数p，一定存在p个元素的有限域，即$<Z_p, \oplus, \otimes>$，记为$GF(p)$，或F_p；
- 对任意的正整数n，在$Z_p[x]$上一定存在n次不可约多项式$f(x)$；
- 因此，一定存在个元素的有限域，即$<Z_p[x]_{f(x)}, \oplus, \otimes>$，记为$GF(p^n)$；
- 反之，任意有限域的元素个数一定是p^n，p为素数，n为正整数。

34

有限域的特征（加法结构）

定义（特征）：若存在某个正整数m，使得m个1的和为0，则称域的特征为m，若对任意的正整数m，m个1的和均不为0，则称域的特征为0.

（1）无限域中，$1+1+\dots+1\neq 0$，所以无限域的特征为0；

（2）有限域$GF(p^n)$的特征为p，特征为p的有限域一定可以记为$GF(p^n)$。

（3）在特征为p的有限域$GF(p^n)$中，对于任意的两个元素α和β，一定有$(\alpha+\beta)^p=\alpha^p+\beta^p$。(二项式展开每项系数都含$p$)

35

有限域的本原元

定义（本原元）：在有限域$GF(q)$中，若某一元素α的阶为$q-1$，则称α为该域中的本原元。

元素α的阶，记为$ord(\alpha)$。这里的阶是关于乘法。

元素的阶：使$\alpha^n=e$的最小正整数n称为元素α的阶。

例：在有限域$GF(5)$中，求出所有元素的阶，找出本原元。

	α^1	α^2	α^3	α^4	$ord(\alpha)$	本原元
1	1				1	×
2	2	4	3	1	4	√
3	3	4	2	1	4	√
4	4	1			2	×

2、3是有限域GF(5)中的本原元。

36

有限域的本原元

定义（本原元）：在有限域GF(q)中，若某一元素α的阶为q-1，则称α为该域中的本原元。

元素α的阶，记为$ord(\alpha)$。这里的阶是关于乘法。

元素的阶：使$\alpha^n = e$的最小正整数n称为元素α的阶。

课堂练习：在有限域GF(7)中，求出所有元素的阶，找出本原元。

	α^1	α^2	α^3	α^4	$ord(\alpha)$	本原元
1	1				1	×
2	2	4	3	1	4	√
3	3	4	2	1	4	√
4	4	1			2	×

2、3是有限域GF(5)中的本原元。

有限域的本原元

答案：在有限域GF(7)中，求出所有元素的阶，找出本原元。

	α^1	α^2	α^3	α^4	α^5	α^6	$ord(\alpha)$	本原元
1	1						1	×
2	2	4	1				3	×
3	3	2	6	4	5	1	6	√
4	4	2	1				3	×
5	5	4	6	2	3	1	6	√
6	6	1					2	×

3, 5 是有限域GF(7)中的本原元。