

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; < mZ, +>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'>,元 素的α'阶就是循环子群<α'>的阶。

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'>。元 素的α/阶 就是循环子群<α/> < >的阶。 1 2 3 4 5 6 7 8 0 0 4 8 3 7 2 6 1 5 0 <Z₀. \oplus >: Z₀= <1>= <2>= <4>= <5>= <7>= <8>₀ $<3>=<6>={30, 31, 32}={0, 3, 6}$ $<6>=\{6^0, 6^1, 6^2\}=\{0, 6, 3\}$ $<3>=<6>=\{0,3,6\}$ $<\{0,3,6\}$, $\oplus>$

定理2-3 有限群的子群的阶一定整除群的阶。

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/ 称作陪集首。

设子群 $G'=\{g_1,g_2,\ldots,g_n\}$, 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 成加个陪集 (子群本身也是一个陪集)。

例: 群G=<Z₉, ⊕>: 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' $1 \oplus G' = 1 \oplus \{0, 3, 6\} = \{1 \oplus 0, 1 \oplus 3, 1 \oplus 6\} = \{1, 4, 7\}$ $2 \oplus G' = 2 \oplus \{0, 3, 6\} = \{2 \oplus 0, 2 \oplus 3, 2 \oplus 6\} = \{2, 5, 8\}$

1 @ G' =4 @ G' =7 @ G' $2 \oplus G' = 5 \oplus G' = 8 \oplus G'$

 $G=\langle Z_9, \oplus \rangle = G' \cup (1 \oplus G') \cup (2 \oplus G')$

子群和陪集----陪集 说明 陪集 $h_1*g_1=g_1=e, g_2, \ldots, g_n$ 陪集首h1=e, 子群G' 陪集首h2, 子群h2*G' $h_2*g_1, h_2*g_2, \ldots, h_2*g_n$ $h_{m-1}*g_1, h_{m-1}*g_2, \ldots, h_{m-1}*g_n$ 陪集首h_{m-1}, 子群h_{m-1}*G' $h_m * g_1, h_m * g_2, \dots, h_m * g_n$ 陪集首hm, 子群hm*G'

子群和陪集

关于陪集首的几点说明:

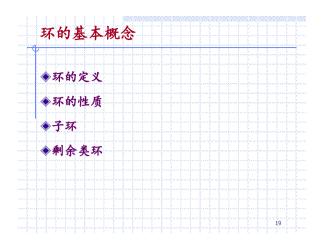
- > 若陪集首/1是子群G'中的元素,则陪集/1* G'与子群G'相同
- > 若陪集首h不是子群G'中的元素,则陪集h* G'与子群G'相 交为空集。
- ≥ 若陪集首h; 不是陪集h; * G'中的元素,则两陪集h; * G'与h; * G'相交为空集。
- ≥ 陪集h* G'中的每一个元素都可作为其陪集首,陪集元素不 变, 仅排列顺序改变。

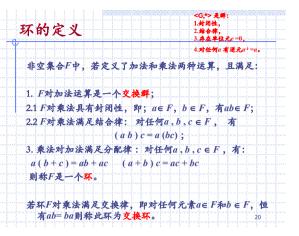
子群和陪集

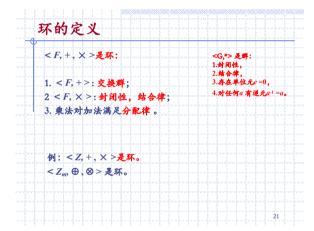
由以上性质可知,两个陪集要么相等要么不相交。 为使群的分解完备、应选择前面未出现过的元素作为 当前陪集的陪集首,这样,整个群将分解成若干个不 相交的陪集、无一遗漏、无一重叠。

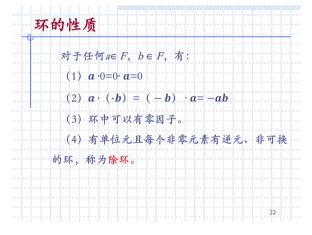
例2-10模9加法运算下、群G={0,1,2,3,4,5,6,7,8}的一个 子群G'={0,3,6}的陪集分解。

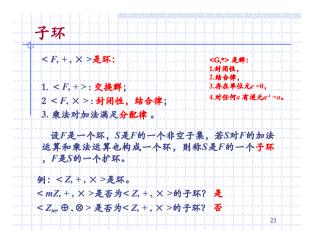
✓ 课堂练习: 求出群G={0,1,2,3,4,5,6,7,8,9,10,11}的所 有子群G',并求出G关于三阶子群的陪集分解。

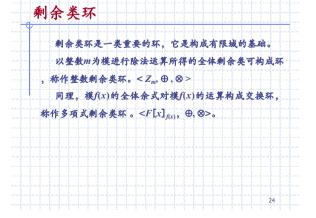


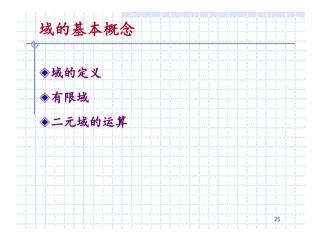


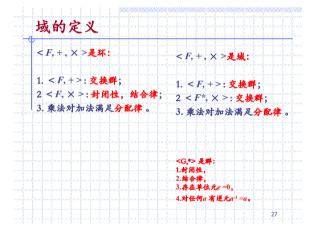


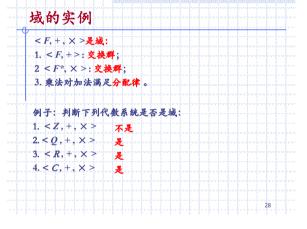


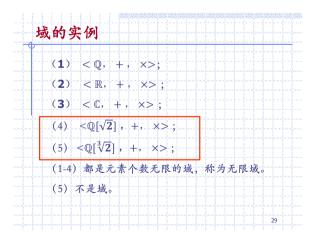


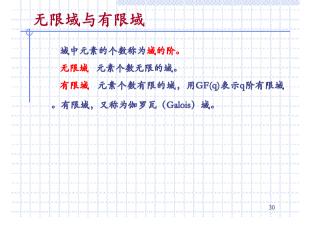


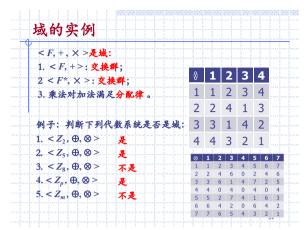


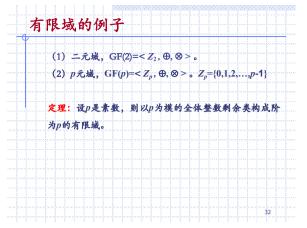












有限域的构造

构造有限域<F[x]_{f(x)}, ⊕, ⊗>

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),并没 f(x)的加法和乘法构成城,记为F[x] f(x), Φ 、 \otimes >。

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

- (2) n=1时, $< F[x]_{f(x)}$, \oplus , $\otimes > \mathfrak{P}F$,
- (3) F是<F[x]_{f(x)}, ⊕, ⊗>的子域。

33

有限域的结构

ightarrow 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_n ;

> 对任意的正整数n,在 $Z_n[x]$ 上一定存在n次不可约多项式f(x);

ightarrow 因此,一定存在个元素的有限城,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pⁿ,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+...+1≠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")中,对于任意的两个元素α和β,一定有(α+β)=α"+β"。(二项式展开每项系数都含p)

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a的阶,记为ord(a)。这里的阶是关于乘法。

元素的阶: 使α"= 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。

	α¹	α²	α^3	α^4	ord(a)	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

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 $\alpha''=e$ 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(a)	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。													

