同余关系复习

<Z,+>上的关系$R = \{(x,y)|x,y\in Z, x-y$能被3整除$\}$，是一个等价关系，它将$Z$划分成三个等价类：

[0]={…,-6,-3,0,3,6,…}

[1]={…,-5,-2,1,4,7,…}

[2]={…,-4,-1,2,5,8,…}

发现：[1]和[2]中元素相加后结果在[0]中

-4+（-2）= -6　　2+4=6　-4+7=3.....

关系R使[0], [1], [2]中任意两个类的元素+运算后所得的结果均在同一个类内

概括：$x_1 R x_1' \wedge x_2 R x_2' \rightarrow (x_1 + x_2) R (x_1' + x_2')$（同余）

第六章 群论

- 半群与单位半群
- 群的基本概念
- 变换群
- 有限群
- 循环群
- 子群及陪集分解
- 正规子群与同态

6.1 半群与单位半群

- 半群、子半群的定义
- 循环半群的定义
- 单元半群的定义和基本性质

半群、子半群的定义

定义6.1 设$V=<S,\circ>$是代数系统，$\circ$为二元运算，如果$\circ$运算满足结合律，则称V为半群. 如果半群运算还满足交换律, 则称其为可换半群.

定理6.1 设$V=<S,\circ>$是半群，如果V有子代数$<M,\circ>$，则此子代数也是半群.

定义6.2 半群$<S,\circ>$的子代数亦是半群, 称为半群$<S,\circ>$的子半群.

实例

例1

(1) $<Z^+,+>,<N,+>,<Z,+>,<Q,+>,<R,+>$都是半群，+是普通加法.

(2) 设n是大于1的正整数，$<M_n(R),+>$和$<M_n(R),\cdot>$都是半群，其中+和 $\cdot$分别表示矩阵加法和矩阵乘法.

(3) $<P(B),\oplus>$为半群，其中$\oplus$为集合对称差运算.

(4) $<Z_n,\oplus>$为半群，其中$Z_n=\{0,1,\ldots,n-1\}$，$\oplus$为模n加法 .

(5) $<A^A,\circ>$为半群，其中$\circ$为函数的复合运算.

(6) $<R^*,\circ>$为半群，其中R^*为非零实数集合，$\circ$运算定义如下：

$\forall x,y\in R^*, x\circ y=y$.

实数集合上取min、max运算

实例

∘	a	b	p	q
a	q	p	b	a
b	b	b	b	b
p	p	p	p	p
q	a	b	p	q

结合律： $x \circ (y \circ z) = (x \circ y) \circ z$

循环半群

对半群 $<S,\circ>$的任一元素a, 可以定义它的幂:

(1) $a^0=e$　$a^1=a$;

(2) $a^2=a\circ a$;

(3) $a^{j+1}=a^j\circ a$.

由结合律成立, 若m, n为正整数, 则

(1) $a^n\circ a^m = a^m\circ a^n = a^{n+m}$

(2) $(a^n)^m = a^{n\times m}$

如果$a^2=a$, 则称a为幂等元素.

定义6.3 如果半群$<S, \circ>$的每个元素均为S内的某个固定元素a的幂, 则此半群称为由a生成的循环半群, a叫做此循环半群的生成元素.

<N,+,0>　0是么元，生成元是1.

循环半群的性质

例2
代数系统<Z^+,+>中, Z^+是正整数集, 此代数系统是一个循环半群, 它的生成元素是1.

定理6.2 循环半群一定是可换半群.
证明 设循环半群 <S,∘>的生成元素为a, 则它的任意两个元素$b = a^m$, $c = a^n$, 且有:

$$b \circ c = a^m \circ a^n = a^{n+m} = a^n \circ a^m = c \circ b$$

定理6.3 半群内任一元素和它所有的幂组成一个由该元素生成的循环子半群.
证明 显然.

单元半群

定义6.4 设$V=<S,\circ>$是半群，若$e\in S$是关于$\circ$运算的单位元，则称V是单元半群(含幺半群, 独异点)，有时也将单元半群V记作$V=<S,\circ,e>$.

例3 整数集Z上的模m相等关系R给出Z的一个划分, 等价类为[0], [1], [2], … ,[m-1], 它的商集Z/R可记为Z_m, 即

$$Z_m=\{[0],[1],[2],\ldots,[m-1]\}$$

在Z_m上分别定义二元运算$\oplus,\otimes$, 对$[i],[j]\in Z_m$有

$$[i]\oplus[j]=[(i+j) \bmod m]$$

$$[i]\otimes[j]=[(i\times j) \bmod m]$$

此时, $<Z_m,\oplus>$和$<Z_m,\otimes>$都是单元半群, 单位元分别为: [0]和[1].

单元半群的性质

单元半群是半群的扩充, 有比半群更多的性质.

定理6.4 一个有可列个元素的单元半群的运算表, 每行(列)均不相等.

证明 由于单位元的存在, 造成运算表中每行第一个元素及每列第一个元素均不相同.

$\circ$	1	a	b	c	d	$\cdots$
1	1	a	b	c	d	$\cdots$
a	a					
b	b					
c	c					
d	d					
$\cdots$	$\cdots$					

Note: 一个单元半群也可以有子单元半群和循环单元半群.

单元半群的性质

定理6.5 如果单元半群$<M,\circ>$存在一个子系统$<M',\circ>$, 且其单位元$e \in M'$, 则$<M',\circ>$也是一个单元半群.

证明 显然.

定义6.5 称以上$<M',\circ>$为$<M,\circ>$的子单元半群.

定义6.6 如果一个单元半群由它的一个元素a所生成(令$a^0 = e$, 故单位元也可由a生成), 则称其为由a所生成的循环单元半群, 把a称为此单元半群的生成元素.

定理6.6 循环单元半群是可换单元半群.

证明 与定理6.2证明类似.

单元半群的性质

定理6.7 可换单元半群的所有幂等元素构成一个子单元半群.

证明 设$<M,\circ>$是一个可换单元半群, 它的幂等元素组成的集合为M'.

思路: (1)证M'是一个代数系统; (2)证M'是M的子半群; (3)证M的单位元也是M'的单位元

(1)设$a, b \in M'$, 且它们是幂等元素, 所以有$a\circ a = a$, $b\circ b = b$, 又"$\circ$"满足结合律和交换律, 则

$$(a\circ b)\circ(a\circ b) = (a\circ a)\circ(b\circ b) = a\circ b$$

由此可知$a\circ b$亦是幂等元素, 所以$a \circ b \in M'$, "$\circ$"对M'封闭, $<M',\circ>$是一个代数系统.

(2) $M' \subseteq M$, 所以$<M',\circ>$是$<M,\circ>$的一个子系统, 是子半群.

(3)由于$e\circ e = e$, 所以单位元亦为幂等元素, $e \in M'$.

6.1 群

- 群的基本概念和性质
- 变换群
- 对称群, 置换群
- 循环群
- 子群及陪集分解
- 正规子群与同态

6.1 群的定义及其性质

定义6.7 设$V=<S,\circ>$是单元半群，$e\in S$是关于$\circ$运算的单位元，若$\forall a\in S$，$a^{-1}\in S$，则称V是**群**. 通常将群记作G.

实例：

$<\mathbf{Z},+>$和$<\mathbf{R},+>$是群，$<\mathbf{Z}_n,\oplus>$是群.

n阶($n\geq 2$)实可逆矩阵集合关于矩阵乘法构成群.

群的定义

定义6.8 (1) 若群G是有穷集，则称G是有限群，否则称为无限群. 群G 的基数称为群 G 的阶，有限群G的阶记作$|G|$.

(2) 只含单位元的群称为平凡群.

(3) 若群G中的二元运算是*可交换*的，则称G为交换群或阿贝尔 (Abel) 群.

实例：

$<Z,+>$和$<R,+>$是无限群，$<Z_n,\oplus>$是有限群，也是 n 阶群.

$<\{0\},+>$是平凡群.

上述群都是交换群，n阶($n\geq 2$)实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

群的性质

性质1：群满足消去律 G为群，则G中满足消去律，即对任意$a,b,c \in G$有

(1) 若 $a \circ b = a \circ c$，则 $b = c$.

(2) 若 $b \circ a = c \circ a$，则 $b = c$.

证明略

例4 设$G = \{a_1, a_2, \ldots, a_n\}$是$n$阶群，令

$$a_iG = \{a_i \circ a_j \mid j=1,2,\ldots,n\}$$

证明 $a_iG = G$.

证 由群中运算的封闭性有 $a_iG \subseteq G$. 假设$a_iG \subset G$，即 $|a_iG| < n$.

必有$a_j, a_k \in G$使得

$$a_i \circ a_j = a_i \circ a_k \quad (j \neq k)$$

由消去律得 $a_j = a_k$, 与 $|G| = n$矛盾.

五阶群

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

群的性质

性质2：方程存在惟一解 G为群，$\forall a,b\in G$，方程$a\circ x=b$和$y\circ a=b$在G中有解且仅有惟一解.

证 $a^{-1}\circ b$ 代入方程左边的x 得

$$a\circ(a^{-1}\circ b)=(a\circ a^{-1})\circ b=e\circ b=b$$

所以$a^{-1}\circ b$ 是该方程的解.

下面证明惟一性. 假设c是方程$a\circ x=b$的解，必有$a\circ c=b$，从而有

$$c=e\circ c=(a^{-1}\circ a)\circ c=a^{-1}\circ(a\circ c)=a^{-1}\circ b$$

同理可证$b\circ a^{-1}$是方程 $y\circ a=b$的惟一解.

例5 设群$G=<P(\{a,b\}),\oplus>$，其中$\oplus$为对称差. 解下列群方程：

$$\{a\}\oplus X=\varnothing,\quad Y\oplus\{a,b\}=\{b\}$$

解 $X=\{a\}^{-1}\oplus\varnothing=\{a\}\oplus\varnothing=\{a\}$，

$Y=\{b\}\oplus\{a,b\}^{-1}=\{b\}\oplus\{a,b\}=\{a\}$

群的性质

性质3：一个阶大于1的群一定没有零元

证 因为零元不存在逆元，故得证.

性质4：除了单位元外，一个群一定没有幂等元素

证 若存在幂等元，即$a \circ a = a$, 则必有

$$e = a^{-1} \circ a = a^{-1} \circ (a \circ a) = (a^{-1} \circ a) \circ a = e \circ a = a$$

即幂等元只能是单位元.

群的第二种定义

性质5：如果一个代数系统满足结合律和性质(2), 则它是群

证 (1)找单位元 因为$a \circ x=b$, 设对某一个a, 满足方程$a \circ x=a$的x为e_r, 对$\forall b$有$y \circ a=b$的解c. 此时

$$b \circ e_r = (c \circ a) \circ e_r = c \circ (a \circ e_r) = c \circ a = b$$

同理可得e_l, 对$\forall b$有 $e_l \circ b = b$, 由于$e_l = e_r = e$, 得到单位元

(2) 找逆元 由$y \circ a=e$, 可得a的唯一左逆元， 由$a \circ x=e$,可得a的唯一右逆元, 由于左右逆元相等, 因此可得到逆元.

得证.

定义6.9 一个代数系统G若满足下列条件, 则称为群

(1) 满足结合律;

(2) $\forall a,b \in G$， 方程$a \circ x=b$和$y \circ a=b$在G中有解且仅有惟一解.

群的同态和同构

定义6.10 设$<G,\circ>$和$<H,*>$是两个群, 若存在一个函数$f:G\to H$使得$\forall a,b\in G$, 有 $f(a\circ b)=f(a)*f(b)$, 则称f是从$<G,\circ>$到$<H,*>$的群同态；如果f是双射函数，则称为群同构.

定理6.8 对群满同态f有

$$f(e_G)=e_H$$

$$f(a^{-1})=[f(a)]^{-1}$$

其中e_G和e_H分别为$<G,\circ>$和$<H,*>$的单位元.

证 用同态性质易证.

定理6.9 如果群G与代数系统$<H,*>$满同态或同构, 则$<H,*>$也是群.

证 用满同态和同构性质易证.

作业

徐 p99 6.1 6.4 6.5

P113 19