离 散 数 学

西北工业大学

2022年5月18日 星期三

第十二章 群

1. 半群与含幺半群
2. 群及其性质
3. 特殊群
4. 陪集与拉格朗日定理
5. 正规子群

12.1 本章学习要求


重点掌握
一般掌握
了解
1
1 半群、群、子群及性质
2 元素的周期及计算
3 生成元与循环群
4 陪集与拉氏定理
2
正规子群性质与同态核
3
商群及性质

12.2半群与含幺半群

定义12.2.1 在二元代数<S, *>中，若二元运算“*”满足结合律，则称<S, *>为**半群**；特别地，若半群<S, *>中的二元运算“*”满足交换律，则称<S, *>为**可交换半群**。

定义12.2.2 设<S, *>为半群，若S中存在关于运算“*”的幺元e，则称此半群为**独异点（或含幺半群）**，有时也记为<S, *, e>；

若独异点<S, *, e>中运算“*”满足交换律，则称<S, *, e>为**可交换独异点（可交换含幺半群）**。

例

设$\underline{n}=\{0, 1, 2, \cdots, n-1\}$，定义$\underline{n}$上的运算$+_n$如下：

$$x, y\in\underline{n}, x+_n y=x+y \pmod n$$

（即x＋y除以n的余数）。

证明$<\underline{n}, +n>$是含么半群。

证明：**封闭性**：$x, y\in\underline{n}$，令$k=x+y \pmod n$，则

$$0\leqslant k<n-1, \text{即} k\in\underline{n},$$

所以封闭性成立；

例（续）

结合律：x, y, z∈$\underline{n}$, 有

$$(x+_n y)+_n z = x+y+z \pmod n = x+_n (y+_n z)$$

所以结合律成立。

单位元： x∈$\underline{n}$, 显然有

$$0+_n x = x+_n 0 = x$$

所以0是单位元。故<$\underline{n}$, $+_n$>是含么半群。

子半群和子含幺半群

将子代数应用于半群，可得下面的定义：

定义12.2.3　如果<S，*>是半群，T是S的非空子集，且运算“*”　对T封闭，则称<T，*>是半群<S，*>的子半群；

如果<S，*，e>是含幺半群，T是S的非空子集，e∈T。且运算“*”对T封闭，则称<T，*，e>是含幺半群<S，*，e>的子含幺半群。

半群同态

利用代数系统中同态与同构概念，得到半群（含幺半群）的同态与同构。

设<S, o>和<T, *>是两个半群，映射f：S→T，对任意元素a, b∈S，都有

$$f(a \circ b) = f(a) * f(b),$$

则映射f就是半群<S, o>到半群<T, *>的同态映射。

半群同态（续）

如果半群<S，o>和<T，*>是含幺半群，其中e，1分别是<S，o >和<T，*>的幺元，而且映射f满足：

$$\forall\ a,\ b\in S,\ f(aob) = f(a)\ *f(b),\ 且$$

$$f(e) = 1。$$

则映射f就是含幺半群<S，o，e>到<T，*，1>的同态映射。

当f是单射、满射、双射时，相应的同态为单同态、满同态、同构。

例

设映射f：N→$\underline{6}$，且∀x∈N，

$f(x) = x \pmod 6$，则

（1）f是半群$\langle N, + \rangle$到$\langle \underline{6}, +_6 \rangle$的同态映射；

（2）f是含幺半群$\langle N, +, 0 \rangle$到$\langle \underline{6}, +_6, 0 \rangle$的同态映射。

分析　（1），需证明∀ a，b∈N，有$f(a + b) = f(a) +_6 f(b)$；

（2），在（1）的基础上，还需说明$f(0) = 0$。

例（续）

证明 （1）$\forall\ a,\ b\in N$，有

$$
\begin{aligned}
f\ (a\ +\ b) &= (a\ +\ b)(\mathrm{mod}\ 6)\\
&= (a\ (\mathrm{mod}\ 6)\ +\ b\ (\mathrm{mod}\ 6))(\mathrm{mod}\ 6)\\
&= a\ (\mathrm{mod}\ 6)+_6\ b\ (\mathrm{mod}\ 6)\\
&= f(a)\ +_6\ f(b),
\end{aligned}
$$

所以f是同态映射。

（2）根据f的定义，显然有f(0) = 0，又根据（1），则f是含幺半群$\langle N,\ +,\ 0\rangle$到$\langle \underline{6},\ +_6,\ 0\rangle$的同态映射。

结论

设f是二元代数<A, >到<B, *>的满同态，则根据第五章同态的性质，容易得到如下结论：

（1）若<A, o>是半群，则<B, *>也是半群；

（2）若<A, o>含幺半群，则<B, *>也是含幺半群。

12.2.2 元素的幂

设〈S, *〉是一个半群，对∀x∈ S，可定义：

$$x^1=x, \qquad x^2=x * x,$$

$$x^3=x* x^2= x^2 * x=x * x * x,$$

……

$$x^n=x^{n-1} * x=x * x^{n-1}=x * x * x * \ldots\ldots * x。$$

……

如果〈S, *〉有单位元e，可以定义：$x^0=e$

元素的幂（续）

由于结合律的满足，同样有 如下的公式：

$a^x * a^y = a^{x+y}$　　$(a^x)^y = a^{xy}$

例

（1）设<S, *>是半群，a∈S,

$M = \{a^n \mid n \in Z^+\}$,

则<M, *>是<S, *>的子半群；

（2）设<S, *, e>是含幺半群，a∈S,

$M = \{a^n \mid n \in N\}$,

则<M, *>是<S, *>的子含幺半群；

分析 （1）M是非空子集，运算“*” 封闭。

（2）还需说明幺元e在M中。

例（续）

证明 （1）$a = a^1 \in M$，所以M是非空集合。

对$\forall n \in Z^+$，$a^n \in S$，因此M是S的非空子集。

对$\forall a^n$，$a^m \in M$，n，$m \in Z^+$，则

$$a^n * a^m = a^{n+m},$$

$$n + m \in Z^+, \quad a^n * a^m \in M。$$

故运算“*” 封闭。$\langle M, * \rangle$是$\langle S, * \rangle$的子半群。

（2）幺元$e = a^0 \in M$，即幺元在M中。类似（1），同理可证$\langle M, * \rangle$是$\langle S, * \rangle$的子含幺半群。

12.2.3 循环半群

定义12.2.4 （1）在半群<S, *>中，若存在一个元素a∈S，使得对任意x∈S，都有

$$x = a^n，其中n \in Z^+，$$

则称<S, *>为**循环半群**，并称a为该循环半群的一个**生成元**，M = {a | (a∈S)且a是S的生成元}称为该循环半群的**生成集**；

定义12.2.4（续）

（2）在含幺半群<S, *, e>中，若存在一个元素a∈S，使得对任意x∈S，都有

$$x = a^n, \text{ 其中} n \in N,$$

则称此循环含幺半群为**循环含幺半群（或循环独异点）**，并称a为该循环含幺半群的一个**生成元**，M = {a | (a∈S)且a是S的生成元}称为该循含幺半群的**生成集**。

例

判断含幺半群<N, +>是否是一个循环含幺半群？

分析　根据定义，判别含幺半群（或半群）是循环含幺半群（循环半群）的关键是计算生成元。

如何计算生成元呢？

首先假设生成元存在，然后根据定义得到方程，通过解这个方程来计算生成元。

例（续）

如在本例中，不妨假设$a \in N$是$\langle N, + \rangle$的生成元，则根据生成元的定义，对$\forall n \in N$，$\exists m \in N$，使得

$$n = a^m = ma$$

让$n = 1$，有$1 = ma$，因此$a = 1$。这说明，如果$\langle N, + \rangle$有生成元，则生成元必须为1。下面还需验证1是生成元。

例（续）

解 由于存在元素1∈N，使得对任意n∈N，都有：

$$n = (n-1)+1 = 1+(n-1)$$

$$= 1+1+1+\cdots\cdots+1 = 1^n,$$

特别对幺元0∈N，有$0 = 1^0$。

所以，“1”是生成元。

因此，该半群一定是循环含幺半群。

定理12.2.1

循环半群都是可交换半群。

分析 由于循环半群中的每个元素都可以表示为生成元的方幂形式，可以使用这种表示形式来证明。

证明 设$a \in S$是循环半群$\langle S, * \rangle$的生成元。则对$\forall x, y \in S$，存在$m, n \in Z^+$，使得

$$x = a^m, \ y = a^n, \text{ 所以}$$

$$x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x,$$

故运算“*”是可交换的，即$\langle S, * \rangle$是可交换半群。

推论12.2.1 循环含幺半群都是可交换含幺半群。

例

判断含幺半群$\langle \underline{6}, +_6 \rangle$是否是循环含幺半群？若是，请求出其所有的生成元。

分析 $\underline{6} = \{0, 1, 2, 3, 4, 5\}$，共有6个元素，则可以判别每一个元素是否是生成元。

解 由于$\underline{6} = \{0, 1, 2, 3, 4, 5\}$，0是幺元，则0肯定不是生成元，对其他元，有：

①、$1^0 = 0$，$1^1 = 1$，$1^2 = 2$，$1^3 = 3$，$1^4 = 4$，$1^5 = 5$，

所以“1”是$\langle \underline{6}, +_6 \rangle$的生成元；

例12.2.8（续）

②、$2^0 = 0,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 0, \cdots\cdots,$

所以“2”不是$\langle \underline{6},\ +_6\rangle$的生成元；

③、$3^0 = 0,\ 3^1 = 3,\ 3^2 = 0,\ 3^3 = 3, \cdots\cdots,$

所以“3”不是$\langle \underline{6},\ +_6\rangle$的生成元；

④、$4^0 = 0,\ 4^1 = 4,\ 4^2 = 2,\ 4^3 = 0, \cdots\cdots,$

所以“4”不是$\langle \underline{6},\ +_6\rangle$的生成元；

⑤、$5^0 = 0,\ 5^1 = 5,\ 5^2 = 4,\ 5^3 = 3,\ 5^4 = 2,\ 5^5 = 1,$

所以“5”是$\langle \underline{6},\ +_6\rangle$的生成元。

例12.2.8（续）

因此，含幺半群$\langle \underline{6}, +_6 \rangle$有两个生成元“1”、“5”，则$\langle \underline{6}, +_6 \rangle$是循环含幺半群。

另解　不妨设$a \in \underline{6}$是生成元，则

$$\forall x \in \underline{6}, \exists m \in \mathbf{N}, \text{有} x = a^m = ma \pmod 6,$$

特别地，当$x = 1$时，有$1 = ma \pmod 6$，即

$$\exists k \in \mathbf{Z}, \text{使得} ma = 6k + 1, \text{即}$$

$$ma + (-k)6 = 1。$$

因此，$(a, 6) = 1$，即a与6的最大共因子为1。

例12.2.8（续）

反之，对$\forall\ a\in\underline{6}$，如果$(a,\ 6) = 1$，则

$$\exists k\in Z，使得 1 = ma + 6k，$$

因此，对$\forall x\in\underline{6}$，有

$$x = (xm)a + 6(xk)，\ xm，\ xk\in Z，$$

根据“$+_6$”的定义，则

$$x = a^{xm}，\ xm\in Z，$$

因此，a是生成元。

例12.2.8（续）

综上所述，$a \in \underline{6}$是生成元的充分必要条件是

$$(a, 6) = 1。$$

考虑集合$\underline{6}$中，可得“1”、“5”是$\langle \underline{6}, +_6 \rangle$的生成元，则$\langle \underline{6}, +_6 \rangle$是循环含幺半群。

计算生成元方法：

首先假设生成元存在，然后根据定义得到方程，通过解这个方程来计算生成元。

推广

（1）$\langle \underline{n}, +n\rangle$是循环含幺半群；

（2）对$\forall a \in \underline{n}$，若$(a, n) = 1$，则a是$\langle \underline{n}, +_n\rangle$的生成元；

（3）当n是素数时，$\underline{n}$中除幺元“0”以外，其他一切元素都是生成元。

12.3 群及其性质

定义12.3.1 设<G, *>为二元代数系统，满足如下性质：

（1）“*”在G中满足结合律，即∀a, b, c∈G，有

(a*b) *c = a* (b*c)；

（2）G中存在关于“*”的幺元e，即∃e∈G，使得

∀a∈G, e*a = a*e = a；

■概括：群是满足结合律、有幺元，每个元有逆元的二元代数系统为群

定义12.3.2

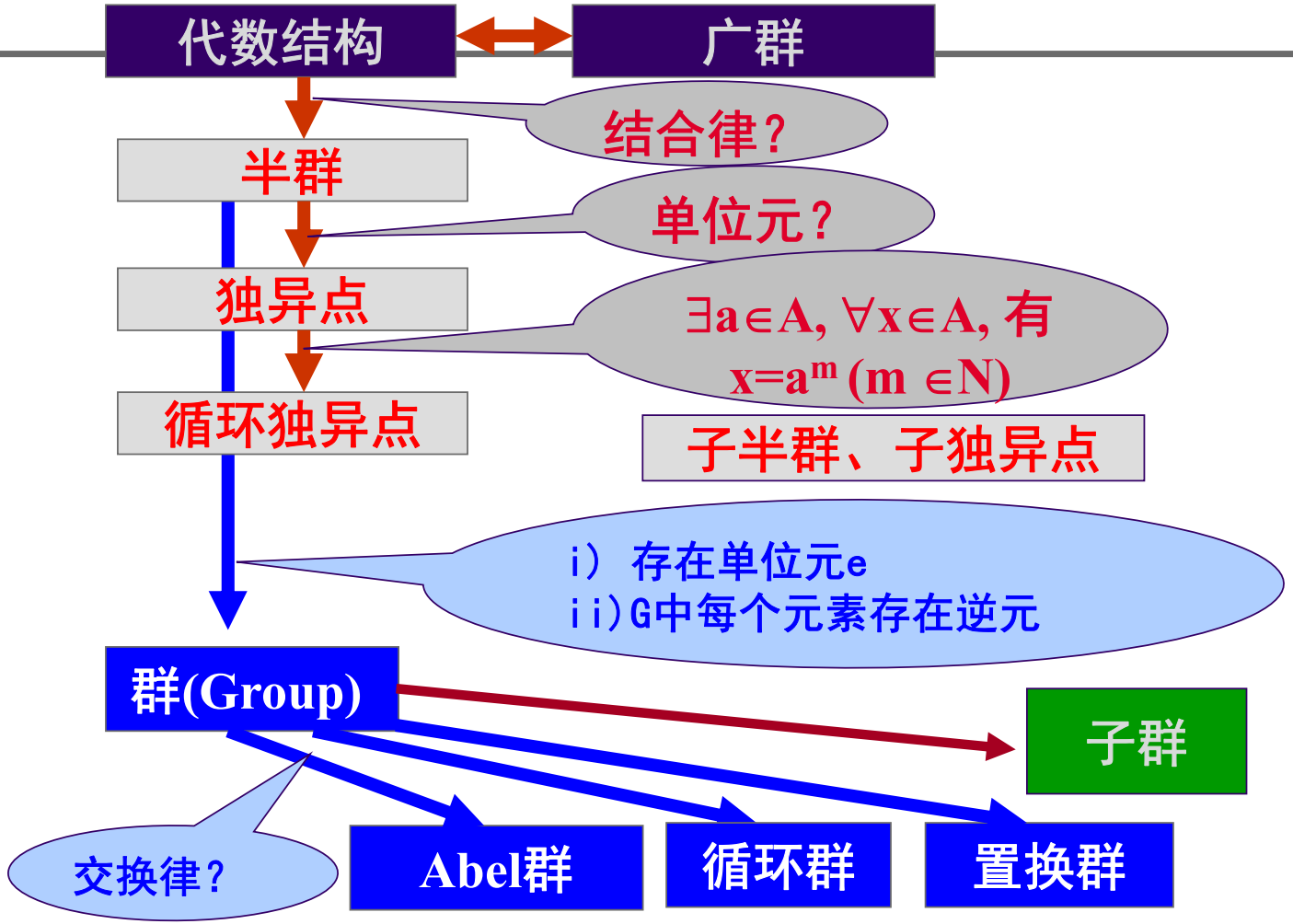
在群<G, *>中，

（1）若运算“*”满足交换律，即∀a, b∈G，都有

$$a*b = b*a,$$

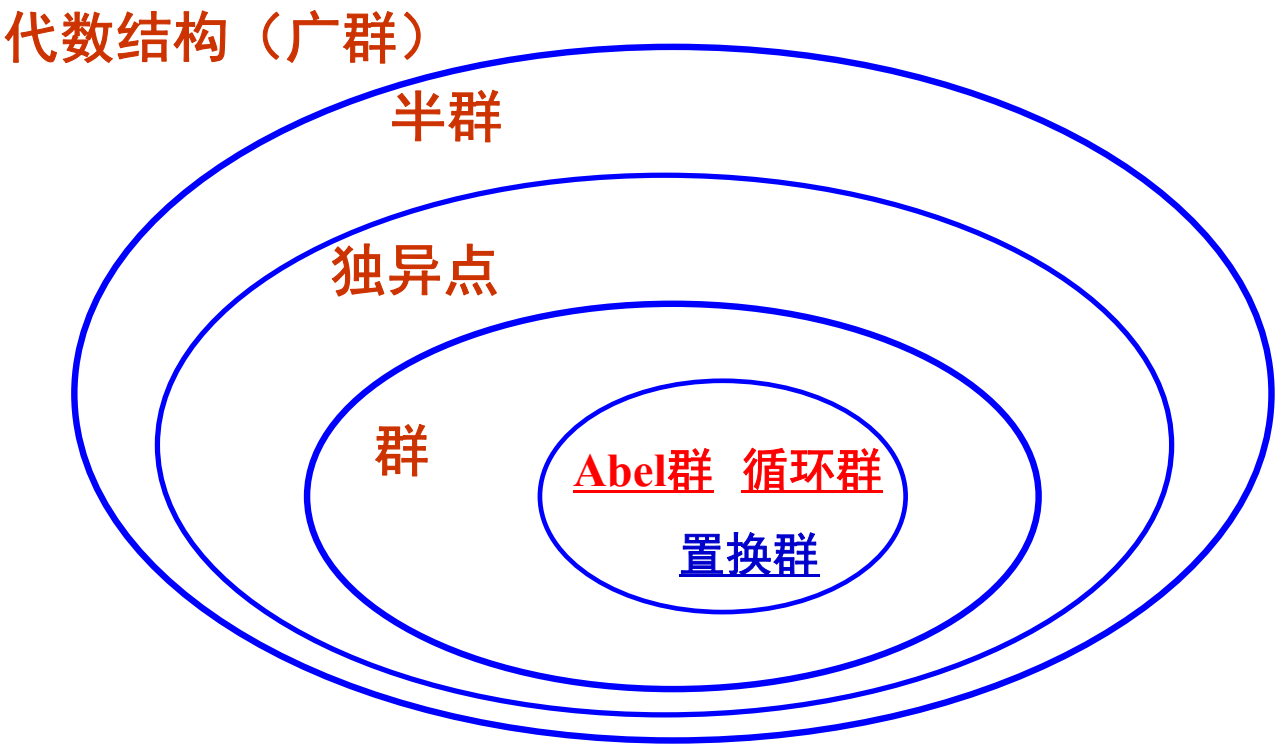
则称<G, *>为可换群或阿贝尔(Abel)群；

（2）集合G的基数称为群G的阶(Order)，记为|G|。若群<G, *>的阶有限，则称之为有限群，否则称为无限群。


代数结构
广群
结合律?
半群
单位元?
独异点
∃a∈A, ∀x∈A, 有
x=a^m (m ∈N)
循环独异点
子半群、子独异点
i） 存在单位元e
ii)G中每个元素存在逆元
群(Group)
子群
交换律?
Abel群
循环群
置换群


(R, +, ·)
(R, +)
+封闭性
原群
+结合律
半群
+单位元
幺半群
+逆元
群
+交换律
阿贝尔群
(R, ·)
+封闭性
原群
+结合律
半群
+乘法对加法满足分配律
环
(R, +, ·)
(R, +)
+封闭性
原群
+结合律
半群
+单位元
幺半群
+逆元
群
+交换律
阿贝尔群
(R, ·)
+封闭性
原群
+结合律
半群
+交换律
+乘法对加法满足分配律
交换环
(R, +, ·)
(R, +)
+封闭性
原群
+结合律
半群
+单位元
幺半群
+逆元
群
+交换律
阿贝尔群
(R, ·)
+封闭性
原群
+结合律
半群
+单位元
幺半群
+逆元
群
+交换律
阿贝尔群
(R−{0}, ·)
+乘法对加法满足分配律
域

代数结构之间的关系



例12.3.1

证明$\langle \underline{n}, +_n \rangle$是群，其中n是正整数。

分析　需要证明4点：封闭性；结合律；幺元存在；逆元存在。

证明　（1）封闭性：　$\forall x, y \in \underline{n}$，令

$$k = x + y \pmod{n}$$，则

$0 \leqslant k < n - 1$，即$k \in \underline{n}$，

所以封闭性成立。

例12.3.1（续）

（2）结合律：$\forall x, y, z \in \underline{n}$，有

$$(x +_n y) +_n z = x + y + z \pmod n$$
$$= x +_n (y +_n z),$$

所以结合律成立。

（3）幺元：$\forall x \in \underline{n}$，显然有

$$0 +_n x = x +_n 0,$$

因此，0是幺元。

例12.3.1（续）

（4）逆元存在：$\forall x \in \underline{n}$，如果$x = 0$，显然$0^{-1} = 0$，

如果$x \neq 0$，则有

$$n - x \in \underline{n},$$

显然

$$x +_n (n-x) = (n-x) +_n x = 0,$$

所以

$$x^{-1} = (n-x),$$

因此，$\forall x \in \underline{n}$，$x$有逆元。

综上，$\langle \underline{n}, +_n \rangle$是群。

例12.3.2

设X是任意集合，

$$S = \{f: X \to X \mid f\text{是双射函数}\},$$

运算“o”是函数的复合运算，证明<S, o>是群。

证明 （1）封闭性：$\forall f, g \in S$, f, g是双射，则fog也是双射，即$fog \in S$。故封闭性成立。

（2）结合律：由于函数的复合运算“o”满足结合律，因此，在集合S也满足结合律。

例12.3.2（续）

（3）幺元存在：恒等映射$I_X \in G$，且$\forall f \in S$，有

$$I_X \circ f = f \circ I_X = f,$$

因此，恒等映射I_X是幺元。

（4）逆元存在：$\forall f \in S$，f是双射，则$f^{-1} \in S$，且有

$$f^{-1} \circ f = f \circ f^{-1} = I_X,$$

因此，f^{-1}就是f关于“$\circ$”的逆元。

由（1）、（2）、（3）和（4）可知，$\langle S, \circ \rangle$是群。

说明

说明 $\langle S, \circ \rangle$被称为**变换群**，如果X是有限集合，设$|X| = n$，此时称$\langle S, \circ \rangle$为**n阶置换群**。变换群在几何学中有十分广泛的应用。

定理12.3.1

在群<G, *>中，有：

（1）群G中每个元素都是可消去的，即运算满足消去律；

（2）群G中除幺元e外无其他幂等元；

（3）阶大于1的群G不可能有零元；

（4）$\forall a, b \in G$，都有$(a*b)^{-1} = b^{-1}*a^{-1}$；

（5）群<G, *>的的运算表中任意一行(列)都没有两个相同的元素。

定理12.3.1（续）

分析 由于可逆元就是可消去元，因此（1）显然可证。

（2）和（3）分别是证明唯一性和存在性问题，通常采用反证法证明。

（4）显然。

（5）采用反证法证明。

（1）群G中每个元素都是可消去的，即运算满足消去律；
（2）群G中除幺元e外无其他幂等元；

证明 （1）由于可逆元就是可消去元，而群G中每个元素都是可逆元，则G中的任何元素都是可消去的，即运算满足消去律。

（2）对幺元e，由于e*e = e，所以e是幂等元。现假设a是群G中的幂等元，即

$$a*a = a,$$

则a*a = a*e，使用消去律，则有a = e。

因此，幺元e是G的唯一幂等元。

（3）阶大于1的群G不可能有零元；

（3）假设群G的阶大于1且有零元θ，则θ*θ = θ，即θ是幂等元，因此由（2）有

$$\theta = e,$$

由于|G|>1，则∃x∈G，x≠θ，由θ是零元，有

$$x*\theta = \theta,$$

又θ = e是幺元，则有

$$x*\theta = x*\theta = x,$$

则，θ = x，这与x≠θ矛盾。因此，G中无零元。

注意：如果|G| = 1，则有G = {e}，此时e既是幺元又是零元。

（4）$\forall a, b \in G$，都有$(a*b)^{-1} = b^{-1}*a^{-1}$；
（5）群$\langle G, * \rangle$的的运算表中任意一行(列)都没有两个相同的元素。

（4）由于群G中的运算满足结合律，且每个元素都有逆元，有推论12.3.1知，结论成立。

（5）假设群G的运算表中某一行(列)有两个相同的元素，设为a，并设它们所在行第一个元素为b，所在列第一个元素分别为c_1，c_2，这时显然有$c_1 \neq c_2$。而

$$a = b*c_1 = b*c_2$$，由消去律可得

$$c_1 = c_2$$，矛盾。

群中元素的周期

设〈G，*〉是一个群，对$\forall a \in G$，可定义：

$a^0=e$，$a^1=a$，$a^2=a*a$，……，

$a^n=a^{n-1}*a=a*a^{n-1}=a*a*\ldots\ldots*a$；

$a^{-1}=a^{-1}$，$a^{-2}=(a^{-1})^2$，……，

$a^{-n}=(a^{-1})^n=a^{-1}*a^{-1}*\ldots\ldots*a^{-1}$。

由幂方的定义知：

$a^m*a^n=a^{m+n}=a^{n+m}=a^n*a^m$；

$(a^m)^n=a^{mn}$。

元素的周期（续）

对群<G, *>中的元a，由幂方可得到如下的一个序列：

$\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots, a^n, \cdots,$

这个序列有周期吗？如果有周期，其最小正周期为多少？

分析　在上述序列中，如果存在整数p和q，其中p<q，使得$a^p = a^q$，则由消去律有

$$a^{q-p} = e,$$

元素的周期（续）

此时p–q就是序列的一个周期，因为对任意的整数m，有

$$a^{m+(p-q)} = a^m * e = a^m,$$

即，对任意的正整数n，如果$a^n = e$，则n是序列的周期。

元素的周期（续）

反之，如果n是序列的周期，肯定有$a^n = e$。

为什么呢？

因为由周期的定义可知，如果n是周期，则

对任意的整数m，由

$$a^{m+n} = a^m, \text{ 即} a^m * a^n = a^m,$$

由消去律，可得

$$a^n = e。$$

定义12.3.3

设e是群<G, *>的幺元，a∈G，

（1）使得$a^n = e$成立的最小正整数n称为a的**周期**或为元素a的**阶**，记为|a|；

（2）若不存在这样的正整数n，使得$a^n = e$，则称a的**周期无限**，即对$\forall n \in Z^+$，都有$a^n \neq e$。

显然，群<G, *>中幺元e的周期为1

定理12.3.3

设a是群<G, *>中的元素，则：

（1）如果a的周期为n，则对任意的整数i，有

$$a^i \in \{ a^1, a^2, \cdots, a^n \},$$

且对任意的p, q∈{1, 2, …., n}, p ≠ q，有

$$a^p \neq a^q;$$

（2）如果a的周期无限，则对任意的整数p, q, p ≠ q，有

$$a^p \neq a^q;$$

（3）a和它的逆元a^{-1}的周期相同。

例12.3.3

计算实数加群<R, +>中元素的周期。

分析 在<R, +>中幺元为“0”，所以有$0^1 = 0$，

而对$\forall a \in R$，且$a \neq 0$，及$\forall n \in Z^+$有

$$a^n = a^{n-1} + a = a + a^{n-1} = a + a + \cdots\cdots + a$$
$$= na \neq 0 ,$$

因此，此时仅有“0”有周期“1”，而其余元素的周期无限。

结论 在实数加群<R, +>中，0的周期为1，而其余实数的周期无限。

定理12.3.3

设<G, *>是一个群，∀a∈G，若a的周期为m，则a^n = e当且仅当m | n。

分析　a的周期为m，则根据以前的分析，序列

…, a^{-n}, …, a^{-2}, a^{-1}, a^0, a^1, a^2, …, a^n, …,

的最小正周期为m，因此，当m | n时，就有a^n = e。

反之，由于在一个周期{ a^1, a^2, …, a^m}中只有a^m = e，因此，如果a^n = e那么一定有m | n。

定理12.3.3（续）

证明 “⇒” （反证法）：设$a^n = e$，

若m不整除n，则$\exists q \in Z$，使得

$$n = mq + r \quad (1 \leqslant r \leqslant m-1),$$

由a的周期为m，且$a^n = e$，有：

$$a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$$

$$= e^q * a^r = a^r = e,$$

由于$1 \leqslant r \leqslant m-1$，这就与a的周期为m矛盾，所以有$m \mid n$。

定理12.3.3（续）

“⇐”：设$m \mid n$。则$\exists k \in Z$，使得$n = mk$，于是有：

$$a^n = a^{mk} = (a^m)^k = e^k = e,$$

总结 如果证明形如$m \mid n$这样的结论，可以采用反证法，即假设m不能整除n，则$\exists q \in Z$，使得$n = mq + r$（$1 \leqslant r \leqslant m-1$）。

例12.3.4

设<G, *>是一个群，对∀a，b∈G，若a的周期为3，b的周期为5，且有：a*b = b*a，

则a*b的周期为15。

证明 设a*b的周期为n，由于a*b = b*a，且运算“*”满足结合律，所以有：

$$(a*b)^{15} = a^{15}*b^{15} = e*e = e,$$

由定理12.3.3可知：n|15，即n可能是1，3，5，15。

例12.3.4（续）

当n = 1，3，5，有：

$$(a*b)^1 = a*b \neq e$$

（若a*b = e，则a = b^{-1}，故b^{-1}的周期为3，则b的周期也为3，矛盾），

$$(a*b)^3 = a^3*b^3 = e*b^3 = b^3 \neq e$$

（因b的周期为5），

$$(a*b)^5 = a^5*b^5 = a^5*e = a^3*a^2 = a^2 \neq e$$

（因a的周期为3），

n = 15时，才有$(a*b)^n = e$。故a*b的周期为15。

推广

设<G, *>是一个群，对∀a，b∈G，若a的周期为n，b的周期为m，且有：a*b = b*a，则：

（1）若(n, m) = 1，则a*b的周期为nm；

（2）若(n, m)≠1，则a*b的周期为[n, m]（[n, m]表示n与m的最小共倍数）。

定理12.3.5

有限群<G, *>中每个元素的周期都有限，且不大于群G的阶。

证明 对∀a∈G，构造

$$a,\ a^2,\ a^3,\ \cdots,\ a^n,\ \cdots$$

由运算“*”的满足封闭性知：

$$a,\ a^2,\ a^3,\ \cdots,\ a^n,\ \cdots \in G,$$

因为|G|是有限的，所以$a,\ a^2,\ a^3,\ \cdots,\ a^n,\ \cdots$中必有相同的元素，不妨假设：

$$a^x = a^y \quad (y>x) \cdots\cdots ①,$$

定理12.3.5（续）

在①式的左右两端同时作用一个a^{-x}，有：

$$a^x * a^{-x} = a^y * a^{-x} = e,$$

即有：

$$a^{y-x} = e \quad (y-x>0),$$

由周期定义可知：元素a的周期一定小于等于(y−x)，所以a的周期有限。

如果(y−x)大于群G的阶，类似可找到小于G的阶的n，使得$a^n = e$

12.3.3 子群

定义12.3.4 设<G, *>是群，如果

（1）S是G的非空子集；

（2）S在运算“*”下也是群，即<S, *>是群。

则称<S, *>是<G, *>的子群。

对任意的群<G, *>，<{e}, *>和<G, *>是群G的子群。由于任何群<G, *>都有这两个子群，故称之为平凡子群，将<G, *>的非平凡子群称为真子群。

引理12.3.1

设<G, *>是一个群，<S, *>是<G, *>的子群，则：

（1）子群<S, *>的幺元e_S也是<G, *>的幺元e_G；

（2）对$\forall a \in S$，a在S中的逆元a_S^{-1}就是a在G中的逆元a_G^{-1}。

证明 （1）e_S是<S, *>的幺元，则

$$e_S^2 = e_S,$$

又$S \subseteq G$，则$e_S \in G$，由上式可知e_S也是群<G, *>的一个幂等元。所以有：

$$e_S = e_G。$$

引理12.3.1（续）

（2）对$\forall a \in S$，a在S中的逆元为$a_S^{-1} \in S$，则有

$$a * a_S^{-1} = a_S^{-1} * a = e_S = e_G,$$

由于$S \subseteq G$，所以a，$a_S^{-1} \in G$，有

$$a_S^{-1} = a_G^{-1}。$$

引理12.3.1说明，如果S是G的子群，则S的幺元就是G的幺元，S中任意元a在S中的逆元也是a在G中的逆元。

定理12.3.5

如何判别一个子集是子群？

定理12.3.5 设S是群<G, *>的非空子集，S是群G的子群的充分必要条件是：

（1）对∀a, b∈S，都有a*b∈S；

（2）对∀a∈S，都有a^{-1}∈S。

证明 **充分性**：要证明<S, *>是群，需证明运算“*”对S封闭，结合律成立，S有幺元和S中的任意元有逆元。

必要性：即证明当<S, *>是<G, *>的子群时，条件(1)和条件(2)成立。

定理12.3.6

设S是群<G, *>的非空子集，S是子群的充分必要条件是：

对∀a，b∈S，都有$a*b^{-1}\in S$。

分析　根据定理12.3.5证明

证明　略

例12.3.6

设$\langle G, *\rangle$是一个群，对任意的$a\in G$，令

$$S = \{a^n \mid n\in Z, Z是整数\},$$

证明$\langle S, *\rangle$是子群。

分析 使用定理12.3.6来证明。

证明 显然S非空。对$\forall x, y\in S$，则存在$n, m\in Z$，

$$x = a^n, \ y = a^m,$$

则

$$x*y^{-1} = a^n* (a^m)^{-1} = a^{n-m},$$

且$n-m\in Z$，所以

$$x*y^{-1} = a^{n-m}\in S,$$

故由定理12.3.6可得，$\langle S, *\rangle$是$\langle G, *\rangle$的子群。

推论与定理

推论12.3.1　对群<G, *>中的任意元a的整数方幂组成的子集是子群，即S = { a^n | n∈Z，Z是整数}是<G, *>的子群。

如果S是群<G, *>的有限非空子集，则S还有更弱的判断定理：

定理12.3.7　设S是群<G, *>的有限非空子集，则S是子群的充分必要条件是

∀a, b∈S，有a*b∈S。

子群判别方法总结

根据子群的定义，要证明以下5点：

①、S非空子集；　　②、运算对S的封闭性；

③、运算在S上结合律成立；　④、S上存在幺元；

⑤、S中的每个元都存在逆元。

判别定理12.3.5将5点减少为3点：

①、S非空子集；　　②、运算对S的封闭性；

③、S中的每个元的逆元都在S中。

子群判别方法总结（续）

判别定理12.3.6将后两点融合，并将以上3点进一步减少为2点：

①、S非空子集； ②、对$\forall a, b \in S$，有$a*b^{-1} \in S$。

如果S是有限子集，根据定理12.3.7，则此时只需证明2点：

①、S非空子集； ②、运算对S的封闭性。

在具体应用中，一般都使用判别定理，特别是定理12.3.5和12.3.6来证明一个非空子集是子群。

例12.3.6

设<G, *>是一个交换群，令

$$S=\{a \mid a\in G且a = a^{-1}\},$$

证明<S, *>是<G, *>的一个子群。

分析　用定理12.3.6证明，即只需证明两点：①、S非空子集；②、对$\forall a, b\in S$，有$a*b^{-1}\in S$。

对幺元e，有$e = e^{-1}$，因此，

$e\in S$，所以S非空。

另一方面，要证明$a*b^{-1}\in S$，即是证明

$$(a*b^{-1}) = (a*b^{-1})^{-1},$$

例12.3.6（续）

又$(a*b^{-1})^{-1} = b*a^{-1}$，因此，只需证明

$$a*b^{-1} = b*a^{-1},$$

又a，b∈S，可得

$$a = a^{-1}, \quad b = b^{-1}。$$

则只需证明$a*b = b*a$，

由于<G，*>是交换群，故

$a*b = b*a$成立。

证明　略。

例12.3.7

设<G, *>是一个群，H_1，H_2是G的两个子群，证明H = $H_1 \cap H_2$是G的子群。

分析　根据定理12.3.5，需要证明3点：

①、H非空子集；②、运算对H的封闭性；

③、H中的每个元的逆元都在H中。

证明　（1）非空性：由于H_1，H_2是G的两个子群，所以有

$e \in H_1$，$e \in H_2$，即有$e \in H_1 \cap H_2$，故H非空。

例12.3.9（续）

（2）**封闭性**：对a，b∈H，有a，b∈$H_1 \cap H_2$，即

a，b∈H_1，a，b∈H_2，

由H_1，H_2是子群，有

a*b∈H_1，a*b∈H_2，即有a*b∈$H_1 \cap H_2$。

（3）**逆元存在**：对a∈H，有 a∈$H_1 \cap H_2$，即a∈H_1，a∈H_2。由H_1，H_2是子群，有

a^{-1}∈H_1，a^{-1}∈H_2，即有a^{-1}∈$H_1 \cap H_2$。

由（1）、（2）、（3）知：<H，*>可作成<G，*>的子群。

推广

设〈G，*〉是一个群，H_1，H_2，……H_n是G的n个子群，则有H=$H_1 \cap H_2 \cap \cdots\cdots \cap H_n$是G的子群。

12.3.4 群的同态

设<G, * >和<H, ∘ >是两个群，映射ψ：G→H， 且

$$\forall a, b \in G, \text{有} \psi(a * b) = \psi(a) \circ \psi(b),$$

则ψ就是从<G, >到<H, * >的**群同态映射**。

当ψ是单射、满射和双射，群同态分别称为**单一群同态、满群同态和群同构**。

定理12.3.8

设ψ是<G, * >到<H, o >的群同态，则

（1）若e是群G的幺元，则ψ(e)是群H的幺元；

（2）$\forall a \in G$，有$\psi(a^{-1}) = (\psi(a))^{-1}$。

证明 （1）由于e * e = e，ψ又是同态映射，则

$$\psi(e) = \psi(e * e) = \psi(e) \circ \psi(e),$$

可见ψ(e)是群H中的幂等元，

所以ψ(e)是群H的幺元。

定理12.3.8（续）

（2）由ψ是同态映射，可得

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

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

ψ(e)是群H的幺元，因此有

$$\psi(a^{-1}) = (\psi(a))^{-1}。$$

此定理说明，群同态映射将幺元映射为幺元，逆元映射为逆元。

两个定理(作业)

定理12.3.9　设ψ是<G, o>到<H, *>的群同态，则<G, o >在ψ下的同态象<ψ(G), *>是<H, *>的子群。

定理12.3.10　设<G, o >是一个群，<H, *>是一个代数系统，若存在从<G, o >到<H, *>满同态，则<H, *>是群。

群同构

同构的群可以看作是相同的群。

对有限群<G，*>而言，其运算“*”可以通过运算表给出，设$G=\{x_1, x_2, \cdots x_i, \cdots x_j, \cdots x_n\}$.

根据定理12.3.1，运算表中每行的元素应互不相同，每列的元素也应互不相同，因此当n＝3时，则运算表只能是下表：

群同构（续）

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

所以当n＝3时，在同构的意义下只有一个群。

群同构（续）

当n=4时，其运算表如下：

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

单位元：e

$a^{-1}=a$

$b^{-1}=b$

$c^{-1}=c$

阶都等于2

Klein四元群

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

单位元：e

$a^{-1}=a$

$b^{-1}=c$

$c^{-1}=b$

生成元b, c

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

单位元：e

$b^{-1}=b$

$a^{-1}=c$

$c^{-1}=a$

生成元a, c

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

单位元：e

$c^{-1}=c$

$b^{-1}=a$

$a^{-1}=b$

生成元a, b

其中，后三个都是循环群且同构，所以4元群在同构意义下有两个。

群同构（续）

通过讨论可以得到如下结论：

(1) 若|G|≤3，则群G在同构的意义之下只有唯一的一个；

(2) 若|G|＝4，则群G在同构的意义之下只有两个。

定理： 每一个n阶有限群，同构于n次置换群

12.4 特殊群

特殊群主要有三类：

交换群、循环群、变换群（置换群）

12.4.1 交换群（阿贝尔群）

若群<G, *>中的运算“*”满足交换律，则称<G, *>是一个**交换群（阿贝尔（Abel）群）**。

由于加法运算“+”满足交换律，因此群<Z, + >，<R, +>，<Q, +>都是交换群。

定理12.4.1

设<G, *>是一个群，则<G, *>是交换群的充分必要条件是：

对a, b∈G，有$(a*b)^2 = a^2*b^2$。

证明 略

12.4.2 循环群

定义12.4.2 在群<G, *>中，若存在元素g∈G，使得对∀a∈G，都有：

$$a = g^i \quad (i \in Z, Z\text{为整数集合}),$$

则称<G, *>为**循环群**，记为G = <g>(或<G, *>=<g>)，并称g为该循环群的一个**生成元**。G的所有生成元的集合称为G的**生成集**。

计算群的生成元是判别一个群是否是循环群的关键。

定理12.4.2

每个循环群都是阿贝尔群。

证明 设$g \in G$是循环群$\langle G, * \rangle$的生成元，对$n, m \in G$，存在$x, y \in Z$，有

$$n = g^x, \ m = g^y,$$

则

$$n*m = g^x*g^y = g^{x+y} = g^{y+x} = g^y*g^x = m*n,$$

所以，循环群$\langle G, * \rangle$是阿贝尔群。

例12.4.1

证明整数加法群<Z, +>是循环群，并求其所有的生成元。

分析　不妨设a∈Z是生成元，则由生成元的定义，对n∈Z，存在k∈Z，使得

$$n = a^k = ka,$$

特别取n = 1，则有

$$1 = ak,$$

又a, k都是整数，所以必然有

$$a = 1，或a = -1。$$

以上说明，如果a是生成元，则a必须是1或者–1，因此，还需进一步验证±1是否是<Z，+>的生成元。

结论

判别群是否是循环群主要就是计算生成元，而计算生成元有两步：

①、假设生成元存在，并根据定义计算它；

②、验证计算的结果是否是生成元，如果是，则该群是循环群。

例12.4.2

证明群$\langle \underline{n}, +_n \rangle (n \in Z^+)$是循环群，并求出生成集。

证明 设a是生成元，则对$m \in \underline{n}$，存在$k \in Z$，使得

$$m = a^k = ka \pmod{n},$$

特别取$m = 1$，则有

$$1 = ka \pmod{n},$$

即存在$s \in Z$，使得

$$ns + ka = 1,$$

所以有$(a, n) = 1$，即a与n互质。

例12.4.2（续）

这说明，如果a是生成元，则有a与n互质。

反之，如果(a, n) = 1，则

∃s, t∈Z，有

$$ns+ta = 1，即$$

$$1 = ta(\mathrm{mod}\ n)，$$

所以有

$$1 = a^t\ (t\in Z)，$$

例12.4.2（续）

则对$m \in \underline{n}$，有

$$m = 1^m = (a^t)^m = a^{tm}(tn \in Z),$$

故a是生成元。

因此a是生成元的充要条件是$(a, n) = 1$。

群$\langle \underline{n}, +_n \rangle$的生成集为

$$M = \{a \mid (a \in \underline{n}) \wedge ((n, a) = 1)\},$$

显然$1 \in M$，所以1是$\langle \underline{n}, +_n \rangle$的生成元，即对$m \in \underline{n}$，

$$m = 1^m,$$

故$\langle \underline{n}, +_n \rangle$是循环群。

结论

（1）群$\langle \underline{n}, +_n \rangle$是一个循环群，其生成集为

$$M = \{a \mid (a \in \underline{n}) \wedge ((n, a) = 1)\};$$

（2）素数阶的循环群$\langle \underline{n}, +_n \rangle$，除幺元以外的一切元素都是群$\langle \underline{n}, +_n \rangle$的生成元。

两类循环群

G = <g>是循环群，根据生成元g的周期，可得两类循环群：

（1）当g的周期无限时，<g>是无限阶循环群，则

$$\langle g\rangle = \{g^k \mid k\in Z;\ 若 i\neq j,\ 则 g^i \neq g^j\};$$

（2）当g的周期有限时，<g>是有限阶循环群，若g的周期为n，则有

$$\langle g\rangle = \{e,\ g,\ g^2,\ g^3, \cdots,\ g^{n-1}\}。$$

定理12.4.3（作业）

设<G, *>是以g为生成元的循环群，则

（1）若G是无限集，则G与整数加法群<Z, +>同构；

（2）若|G| = n，则G与n阶剩余类加群$<\underline{n}, +_n>$同构。

证明 略。

结论

（1）无限循环群有且仅有两个生成元；

（2）阶为素数的循环群除幺元以外的一切元素都是G的生成元；

（3）阶为正整数n的循环群$G = \langle a \rangle$，对$y = a^x \in G$，只要$(n, x) = 1$，则y一定是G的生成元；

结论（续）

（4）循环群的子群一定是循环群；

（5）若G = <a>是一个n阶的循环群，则由n的一切因子d都可对应产生一个且仅一个d阶子群，该d阶循环子群的生成元为a^x，其中x = n/d；

（6）阶为素数p的循环群G = <a>不含有非平凡的真子群。

特殊群小结

1、循环群是研究较为透彻的群，其中整数加群和n阶剩余类加群都是循环群，而且从同构的角度看，循环群也只有这两类循环群. 因此以后涉及到循环群，就只需考虑这两者即可。

2、判别是否是循环群关键在于计算生成元. 计算生成元的一般方法与计算幺元、零元类似，即首先假定存在，然后根据定义得到方程，再求解，最后验证是否是生成元。

12.5 陪集与拉格朗日定理

12.5.1 陪集

定义12.5.1 设<G, *>是群，<H, *>是<G, *>的任意子群，对a, b∈G，如果有$a*b^{-1}\in H$，则称a, b为模H同余关系，此时记为a≡b(modH)。

定理12.5.1

设<H, *>是<G, *>的任一个子群，证明模H同余关系是G上的等价关系。

证明 （1）自反性：对a∈G，有a^{-1}∈G，所以

$$a*a^{-1} = e \in H,$$

即

$$a \equiv a \pmod{H},$$

所以模H同余关系是自反关系。

定理12.5.1（续）

（2）对称性：a，b∈G，如有a≡b(modH)，即

$$a*b^{-1}\in H,$$

因H是一个群，所以有

$$b*a^{-1} = (b^{-1})^{-1}*a^{-1} = (a*b^{-1})^{-1}\in H,$$ 即

$$b\equiv a(\mathrm{mod}H),$$

所以模H同余关系是对称关系。

定理12.5.1（续）

（3）传递性：a，b，c∈G，如有a≡b(modH)，b≡c(modH)，则

$$a*b^{-1}\in H,\ b*c^{-1}\in H,$$

因H是一个群，所以有

$$a*c^{-1}=(a*b^{-1})*(b*c^{-1})\in H,\ 即$$

$$a\equiv c(\mathrm{mod}H),$$

所以模H同余关系是传递关系。

由（1）、（2）、（3）得证。

陪集和拉氏定理

考虑其等价类：对$\forall a\in G$，有：

$$[a]_R=\{x\mid(\text{一切}x\in G)\wedge(x\equiv a(\mathrm{mod}H))\}$$

$$=\{x\mid(\text{一切}x\in G)\wedge(h=x*a^{-1}\in H)\}$$

$$=\{h*a\mid(\text{一切}h\in H)\}$$

记$Ha=\{h*a\mid(\text{一切}h\in H)\}=[a]_R$，

称Ha为H在〈G，*〉中的一个右陪集。

同理，可定义〈G，*〉的左陪集。

定义12.5.2

设<H, *>是群<G, *>的子群，a是G中任意元素，称

（1）aH = {a*h | h∈H}为子群H在群G中的一个左陪集；

（2） Ha = {h*a | h∈H}为子群H在群G中的一个右陪集。

a称为左陪集aH（或右陪集Ha）的代表元。

例12.5.1

计算群<6，$+_6$>的子群 <{0，2，4}，$+_6$>的一切左、右陪集。

解 令H = {0, 2, 4}，则所有的右陪集有：

H0 = {0, 2, 4}0 = {0, 2, 4}}，

H1 = {0, 2, 4}1 = {1, 3, 5}，

H2 = {0, 2, 4}2 = {2, 4, 0}，

H3 = {0, 2, 4}3 = {3, 5, 1}，

H4 = {0, 2, 4}4 = {4, 0, 2}，

H5 = {0, 2, 4}5 = {5, 1, 3}，

例12.5.1（续）

即 H0 = H2 = H4, H1 = H3= H5, H0∪H1 = 6;

同理，所有的左陪集有

0H = 0{0, 2, 4} = {0, 2, 4},

1H = 1{0, 2, 4} = {1, 3, 5},

2H = 2{0, 2, 4} = {2, 4, 0},

3H = 3{0, 2, 4} = {3, 5, 1},

4H = 4{0, 2, 4} = {4, 0, 2},

5H = 5{0, 2, 4} = {5, 1, 3},

有:0H = 2H = 4H, 1H = 3H= 5H, 0H∪1H = 6。

例12.5.2

设$G = \langle Z, + \rangle$，$H = \{km \mid k \in Z\}$，则H是G的子群，计算H的左、右陪集。

解 根据定义，所有的左、右陪集为：

$OH = HO = H = \{km \mid k \in Z\}$，

$1H = H1 = \{km+1 \mid k \in Z\}$，

…… ……

$(m-1)H = H(m-1) = \{km+m-1 \mid k \in Z\}$。

性质12.5.1

设<H, *>是群<G, *>的子群，e是幺元，a，b∈G，则

（1）eH = H = He；

（2）Ha = H ⇔ a∈H（aH = H ⇔ a∈H）；

（3）a∈Hb ⇔ Ha = Hb ⇔ $a*b^{-1}$∈H（a∈bH ⇔ aH = bH ⇔ $a^{-1}*b$∈H）。

求陪集的方法

设H是有限群G的一个子群，求H的左、右陪集：

(1) 首先H本身是G的一个左、右陪集；

(2) 任取a∈G，但a ∉ H，求aH，Ha，此时有：

H∩aH＝Φ，H∩Ha＝Φ；又得一个左、右陪集；

(3)任取b∈G，但b ∉ H∪Ha，求bH，Hb，此时

H∩aH∩bH＝Φ，H∩Ha∩Hb＝Φ；

又得一个左、右陪集；

求陪集的方法（续）

(4)反复上述过程，有：

$$G=\ H\cup aH\cup bH\cup\cdots\cdots=\ H\cup Ha\cup Hb\cup\cdots\cdots。$$

12.5.2 拉格朗日定理

有限群<G, *>的阶n一定被它的任意子群<H, *>的阶m所等分，即k = |G| / |H| = n / m是整数，称k为G内H的**指数**，k正好是关于H的一切不同左(右)陪集的个数。

证明 令所有不同的左陪集有k个，设为S = {a_1H, a_2H, …, a_kH}，则S就是G的一个划分，此时有

$$n = |G| = |\bigcup_{i=1}^{k} Ha_i| = \sum_{i=1}^{k} |Ha_i| = km$$

12.5.2 拉格朗日定理

即子群H的阶m整除群G的阶n，而且其整除的倍数就是不相同的左陪集的个数（同样，如果使用右陪集，会得到同样的结果）。

结论

结论1 设H是有限群G的子群，则H的阶整除G的阶，即|H| | |G|。

结论2 素数阶有限群<G, *>只有平凡子群，而无真子群。

证明 设<H, *>是G的任意子群，则|G| / |H|是整数，因为|G|是素数，则

$$|H| = 1 \text{或} |H| = |G|,$$

所以H只能是G的平凡子群，进而G没有真子群。

结论（续）

结论3 有限群<G, *>中任意元素a的周期都整除群的阶。

证明 设G的阶为n，a的周期为m，则集合H = {a, a^2, …, a^m}是G的子群，由拉格朗日定理，有k = |G| / |H|是整数，即m整除n。

结论4 阶为n的有限群<G, *>中，对a∈G，有

$$a^n = e。$$

结论5 阶为n的有限群<G, *>都有循环子群存在，该子群的生成元的周期均能整除n。

结论（续）

结论6 素数阶有限群G都是循环群，并且除幺元以外的其他元素都是其生成元。

证明 设G的阶为p，则p>1，任意取定a∈G，且a≠e，则a的周期m必大于1，由a生成的循环子群：

$$H = \{a, a^2, \cdots, a^m\},$$

的阶为m，由拉格朗日定理知：

$$m \mid p,$$

由于p是素数，且m>1，所以m = p，

结论（续）

又H是G的子集，且G是有限集，所以有

$$G = H。$$

H是循环群，所以G是循环群，且任意的非幺元a也是G的生成元。

小结

1、同余关系与陪集之间的联系：任意群的任何子群就可以定义同余关系，并且是等价关系，即可求得等价类，其对应得等价类就是相应的陪集。

2、拉格朗日定理说明了子群和群之间的关系，因此，应用该定理就可以根据需要构建子群，并通过该子群利用拉格朗日定理得到所要求的结论。

12.6.1正规子群（不变子群）

定义12.6.1 设<H, *>是群<G, *>的子群，如果对∀a∈G，都有

$$aH = Ha,$$

则称H是G的**正规子群**（或称为**不变子群**），此时左陪集和右陪集简称为**陪集**。

显然，两个平凡子群<G, *>和<{e}, *>是<G, *>的正规子群。

例12.6.1

设$\langle H_1, *\rangle$和$\langle H_2, *\rangle$是群$\langle G, *\rangle$的正规子群，证明$\langle H_1 \cap H_2, *\rangle$也是正规子群。

证明 对$\forall a \in G$，$\forall x \in a\ (H_1 \cap H_2)$，则存在$b \in H_1 \cap H_2$，使得

$$x = a*b,$$

由$b \in H_1 \cap H_2$，可得

$$x = a*b \in a\ H_1,\ x = a*b \in a\ H_2,$$

因此，$x = a*b \in aH_1 \cap aH_2$。故

$$a(H_1 \cap H_2) \subseteq aH_1 \cap aH_2。$$

例12.6.1（续）

$\forall x \in aH_1 \cap aH_2$，即$x \in aH_1$和$x \in aH_2$，则存在$x_1 \in H_1$，$x_2 \in H_2$，使得

$$x = a*x_1,\ x = a*x_2,$$

则$a*x_1 = a*x_2$。群$\langle G, * \rangle$满足消去律，有

$$x_1 = x_2,$$

因此，$x_1 \in H_2$，又$x_1 \in H_1$，得到$x_1 \in H_1 \cap H_2$，故

$$x = a*x_1 \in a\ (H_1 \cap H_2),$$

因此，$aH_1 \cap aH_2 \subseteq a\ (H_1 \cap H_2)$

由上可知，

$$a(H_1 \cap H_2) = aH_1 \cap aH_2,$$

同理可证，

$$(H_1 \cap H_2)a = H_1a \cap H_2a。$$

例12.6.1（续）

由H_1和H_2是正规子群，有

$$aH_1 = H_1a,\quad aH_2 = H_2a,$$

因此，

$$a(H_1 \cap H_2) = aH_1 \cap aH_2 = H_1a \cap H_2a = (H_1 \cap H_2)a,$$

即对$\forall a \in G$，有

$$a(H_1 \cap H_2) = (H_1 \cap H_2)a。$$

故$\langle H_1 \cap H_2, * \rangle$是正规子群。

定理12.6.1

设<H, *>是群<G, *>的子群，则H是G的正规子群的充分必要条件是：

对∀a∈G, h∈H，都有$a*h*a^{-1}\in H$。

证明 必要性：若H是G的正规子群，则a∈G, h∈H，有a*h∈aH = Ha，即存在$h_1\in H$，使得

$a*h = h_1*a$，于是

$a*h*a^{-1} = h_1\in H$，故$a*h*a^{-1}\in H$。

定理12.6.1（续）

充分性： $\forall a*h \in aH$，因$a*h*a^{-1} \in H$，所以，存在$h_1 \in H$，使得

$$a*h*a^{-1} = h_1，于是$$

$$a*h = h_1*a,$$

从而$aH \subseteq Ha$。

又$\forall h*a \in Ha$，则

$$a^{-1}*h*(a^{-1})^{-1} = a^{-1}*h*a \in H,$$

定理12.6.1（续）

所以，存在$h_2 \in H$，使得

$$a^{-1}*h*a = h_2，于是$$

$$h*a = a*h_2，$$

从而$Ha \subseteq aH$。故对

$\forall a \in G$，都有$aH = Ha$。即H是G的正规子群。

推论12.12.1　交换群的任何子群是正规子群。