代数结构

代数运算

基本概念

设X是一个非空集合，从X^n到X上的函数f称为集合X上

的n元代数运算，称n为该运算的阶

在X上的二元运算满足:

X上的任意两个元素都可以进行这种运算，且运算的结果唯一

X上任意两个元素的运算结果都属于X

二元运算的性质

- 交换律：$x*y=y*x$
- 结合律：$(x*y)*z=x*(y*z)$
- 分配律：$x\circ(y*z)=(x\circ y)*(x\circ z)$
- 幂等律：$x\circ x=x$

二元运算中的特殊元

设$*$为非空集合X上的二元运算

如果存在元素e_l(或e_x) $\in X$都有$e_l*x=x$(或$x*e_x=x$)

称e_l(或e_r)为左单位元(右单位元)

左、右零元和左、右逆元(同理)

若左、右单位元都存在，则必相等且唯一

若$x*y=x*z$则$y=z$(左消去律),$y*x=z*x$则$y=z$(右消去律)

对于群|G|>1,零元与单位元相等

代数系统

基本概念

非空集合G上的k个代数运算$f_1,f_2,f_3,\ldots,f_k$(f_i是n元代数运算)

组成的系统称为代数系统

1. 若$\phi : G \to H$是满射，则称ϕ为满同态
2. 若$\phi : G \to H$是单射，则称ϕ为单同态
3. 若$\phi : G \to H$是双射，则称ϕ为同构

定理：设$< G, * >$,$< H, \cdot >$是代数系统，$*$，$\cdot$是二元运算,ϕ是从G到H的同态映射

1. $\cdot$是$\phi(G)$上的运算，即$< \phi(G), \cdot >$是代数系统
2. 如果*在G上满足交换律,则$\cdot$在$\phi(G)$上满足交换律
3. 如果*在G上满足结合律，则$\cdot$在$\phi(G)$上满足结合律
4. 如果e是$< G, * >$的单位元,则$\phi(e)$是$< \phi(G), \cdot >$的单位元
5. 如果θ是$< G, * >$的零元，则$\phi(\theta)$是$< G, \cdot >$的零元

群

基本概念

设$< G, * >$是代数系统,*是二元运算,如果在G上运算*满足结合律,则称$< G, * >$为半群。如果G中关于运算$*$还有单位元e存在，则称$< G, * >$为有幺半群。

设$< G, * >$为有幺半群,如果对于G中的任何元素x都有逆元,则称$< G, * >$为群。进一步如果满足交换律,则称为交换群（阿贝尔群）。

幂运算

定义在半群中，$x^n = \begin{cases} x & n = 1 \\ x^{n-1} * x & n \geq 2 \end{cases}$

- $\forall m, n \in Z, x^m * x^n = x^{m+n}, (x^m)^n = x^{m*n}$
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$
- $(x_1 * x_2 * x_3 \ldots x_n)^{-1} = x_n^{-1} * \cdots * x_2^{-1} * x_1^{-1}$

群的性质

对于一个有限群，该群的元素个数称为该群的阶数，记为|G|,阶数为1的群为平凡群，只含有一个单位元。

对于G中的元素，$x^n = e$则称x为n次元，记作$|x| = n$

群的判断

(方程的唯一可解性)设$< G, * >$为半群，则$< G, * >$是群的充分必要条件是对于$\forall a, b \in G$,方程$a * x = b$和方程$x * a = b$在G中有唯一解。

群元素次数

设$< G, * >$是群，e为其单位元,$a \in G$的次数为n,有以下定理：

- $|a| = |a^{-1}|$
- $a^k = e$的充要条件是k是n的倍数，即$n|k$
- a^k的次数等于$\frac{lcm(k,n)}{k}$,$lcm(k, n)$为k和n的最小公倍数
- $s = t \mod n$，则$a^s = a^n$

设<G,*>是群,$a, b \in G$是有限元，则：

- $|b^{-1}ab| = |a|$
- $|a * b| = |b * a|$

设$< G, * >$是群，令C是G的所有元素可交换的元素构成的集合，称为G的中心。

子群与陪集

设$< G, * >$是群，H是G的非空子集，如果H对二元运算$*$构成群，则称H是G的群

万能判定：
设$< G, * >$是群，H是G的非空子集，则H为G的子群的充分必要条件是，$\forall a, b \in H$,有$a * b^{-1} \in H$

设$< G, * >$是群，$\forall a \in G$,则$H =< a >= \{a^k, k \in Z\}$称为$a$生成的子群

陪集

设$< G, * >$是群，H为其子群。对$a \in G$,称集合$aH = \{a * h | h \in H\}$为子群H相应元素a的左陪集，右陪集同理

所有（右）左陪集构成G的一个划分。

群$< G, * >$的子群H的左(右)陪集组成的集合的基数称为H在G中的指数记作$[G : H]$

拉格朗日定理

设有限群$< G, * >$则$|G| = [G : H] \times |H|$,即子群的阶数一定是子群结束的因子

正规子群和商群

不考

设$< G, * >$是群，H是其子群，如果$\forall a \in G$都有$aH = Ha$,称H为G的正规子群。

判定

- H是正规子群当且仅当$\forall \in G$，$h \in H$,都有$a * h * a^{-1} \in H$
- H是正规子群当且仅当$\forall a \in G$，都有$aHa^{-1} = H$

循环群，置换群

设$< G, * >$是群，若存在$a \in G$,使得$\exists a \in G, \forall x \in G$都有$x = a^k (k \in Z)$，则称$< G, * >$为循环群，$a$为这个循环群的生成元

- 循环群的子群也是循环群
- 每个正因子d含有d阶子群