# 代数结构

# Algebra Structures

**$\langle G,*\rangle$是一个群, $A,B\in P(G)$,且$A\neq\varnothing,B\neq\varnothing$, 定义:**

$$AB = \{a*b \mid a\in A \text{且} b\in B\}$$

$$A^{-1} = \{a^{-1} \mid a\in A\}$$

**称AB为A,B的积，$A^{-1}$为A的逆 。**

## 陪集

**设$\langle H,*\rangle$是群$\langle G,*\rangle$的一个子群,$a\in G$则:**

**左陪集: $aH ::= \{a\}H$，由a所确定的H在G中的左陪集.**

**右陪集: $Ha::=H\{a\}$**

**陪集是左陪集与右陪集的统称.**

例： 设$G=\{e,a,b,c\}$是Klein四元群，$H=\langle a\rangle$是$G$的子群.

$H$所有的右陪集是：

$He=\{e,a\}=H$，$Ha=\{a,e\}=H$，$Hb=\{b,c\}$，$Hc=\{c,b\}$

不同的右陪集只有两个，即$H$和$\{b,c\}$.

# 陪集性质

设$H$是群$G$的子群，则

① $He = H$

② $\forall a \in G$ 有$a \in Ha$

③ $\forall a,b \in G$有：$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha=Hb$

④ 在$G$上定义二元关系$R$：

$$\forall a,b \in G, \langle a,b \rangle \in R \Leftrightarrow ab^{-1} \in H$$

则 $R$是$G$上的等价关系，且$[a]_R = Ha$.

⑤ $|Ha|=|H|$

## Lagrange定理

设$G$是有限群，$H$是$G$的子群，则

$$|G| = |H|\cdot[G:H]$$

其中$[G:H]$ 是$H$在$G$中的不同右陪集(或左陪集) 数，称为$H$在$G$ 中的**指数**.

**推论:**

（1） 设$G$是$n$阶群，则$\forall a\in G$，$|a|$是$n$的因子，且$a^n = e$.

（2） 对阶为素数的群$G$，必存在$a\in G$使得$G = \langle a\rangle$.

# 4、阿贝尔群和循环群

概念：

阿贝尔群(交换群)，循环群，生成元

## 阿贝尔 (Abel) 群

若群$G$中的运算是可交换的，则称$G$为交换群或阿贝尔 群。

例：（1）<Z,+>和<R,+>，$<\mathrm{Z}_n,\oplus>$、Klein四元群均是阿贝尔群。

（2）$n$阶$(n\geq 2)$实可逆矩阵集合关于矩阵乘法构成的群不是阿贝尔群。

## 循环群（Cyclic group）

设$G$是群，若存在$a\in G$使得

$$G=\{a^k \mid k\in Z\}$$

则称$G$是循环群，记作$G=\langle a\rangle$，称 $a$ 为$G$ 的生成元.

### 循环群的分类

(1) $n$ 阶循环群：设$G=\langle a\rangle$是循环群，若$a$是$n$ 阶元，则

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

(2)无限循环群：若$a$ 是无限阶元，则

$$G = \{ a^0=e, a^{\pm 1}, a^{\pm 2}, \ldots \}$$

# 循环群的生成元

设$G=\langle a\rangle$是循环群。

(1) 若$G$是无限循环群，则$G$只有两个生成元，即$a$和$a^{-1}$.

(2) 若$G$是 $n$ 阶循环群，则$G$含有$\phi(n)$个生成元. 对于任何小于$n$且与 $n$ 互质的数$r\in\{0,1,\ldots,n-1\}$, $a^r$是$G$的生成元.

# 实例

(1) 设$G=\{e, a, \ldots , a^{11}\}$是12阶循环群，则$\phi(12)=4$. 小于12且与12互素的数是1, 5, 7, 11, 由定理10.13可知 $a$, $a^5$, $a^7$ 和 $a^{11}$是$G$的生成元.

(2) 设$G=<Z_9,\oplus>$是模9的整数加群，则$\phi(9)=6$. 小于9且与9互素的数是 1, 2, 4, 5, 7, 8. 根据定理10.13，$G$的生成元是1, 2, 4, 5, 7和8.

(3) 设$G=3Z=\{3z \mid z\in Z\}$, $G$上的运算是普通加法. 那么$G$只有两个生成元：3和–3.

# 循环群的子群

设$G=\langle a\rangle$是循环群。

**(1)** 设$G=\langle a\rangle$是循环群，则$G$的子群仍是循环群；

**(2)** 若$G=\langle a\rangle$是无限循环群，则$G$的子群除$\{e\}$以外都是无限循环群；

**(3)** 若$G=\langle a\rangle$是$n$阶循环群，则对$n$的每个正因子$d$，$G$恰好含有一个$d$阶子群。

# 实例

**(1) $G$=<Z,+>是无限循环群，其生成元为1和−1. 对于自然数 $m\in N$，1的$m$次幂是$m$，$m$生成的子群是$m$Z，$m\in$N. 即**

**$\langle 0\rangle = \{0\} = 0Z$**

**$\langle m\rangle = \{mz \mid z\in Z\} = mZ$，  $m>0$**

**(2) $G$=$Z_{12}$是12阶循环群. 12正因子是1,2,3,4,6和12，$G$ 的子群:**

**1阶子群  $\langle 12\rangle=\langle 0\rangle=\{0\}$**

**2阶子群  $\langle 6\rangle=\{0,6\}$**

**3阶子群  $\langle 4\rangle=\{0,4,8\}$**

**4阶子群  $\langle 3\rangle=\{0,3,6,9\}$**

**6阶子群  $\langle 2\rangle=\{0,2,4,6,8,10\}$**

**12阶子群  $\langle 1\rangle=Z_{12}$**

# 5、环与域

概念：

环，交换环，含幺环，整环，域

## 环（Ring）

设$<R,+,\cdot>$是代数系统，+和·是二元运算. 如果满足以下条件:

(1) $<R,+>$构成交换群;

(2) $<R,\cdot>$构成半群;

(3) · 运算关于+运算适合分配律,

则称$<R,+,\cdot>$是一个环.

通常称+运算为环中的加法，·运算为环中的乘法.

环中加法单位元记作 **0**，乘法单位元（如果存在）记作**1**.

对任何元素 $x$，称 $x$ 的加法逆元为负元，记作$-x$.

若 $x$ 存在乘法逆元的话，则称之为逆元，记作$x^{-1}$.

例：

(1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数环Q，实数环R和复数环C.

(2) $n(n\geq 2)$阶实矩阵的集合$M_n$(R)关于矩阵的加法和乘法构成环，称为 $n$ 阶实矩阵环.

(3) 集合的幂集$P(B)$关于集合的对称差运算和交运算构成环，称为子集环.

(4) 设$Z_n=\{0,1, \ldots , n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$<Z_n,\oplus,\otimes>$构成环，称为模 $n$的整数环.

# 环的运算性质

设$<R,+,\cdot>$是环，则

(1) $\forall a \in R$，$a0 = 0a = 0$

(2) $\forall a,b \in R$，$(-a)b = a(-b) = -ab$

(3) $\forall a,b,c \in R$，$a(b-c) = ab-ac$， $(b-c)a = ba-ca$

(4) $\forall a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m \in R$ $(n,m \geq 2)$

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

例：在环中计算$(a+b)^3$, $(a-b)^2$

解： $(a+b)^3 = (a+b)(a+b)(a+b)$

$$= (a^2+ba+ab+b^2)(a+b)$$

$$= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$$

$$(a-b)^2 = (a-b)(a-b) = a^2-ba-ab+b^2$$

# 特殊的环

设<$R$,+,·>是环

(1) 若环中乘法 · 适合交换律，则称$R$是交换环；

(2) 若环中乘法 · 存在单位元，则称$R$是含幺环；

(3) 若$\forall a,b\in R$，$ab=0 \Rightarrow a=0 \vee b=0$，则称$R$是无零因子环。

例：

(1) 整数环Z交换 环，含幺环，无零因子环。

(2) 令$2Z=\{2z \mid z\in Z\}$，则<2Z,+,·>构成交换环和无零因子环，

但不是含幺环。

## 整环(Integrel Domain)

设<R,+,•>是一个代数系统,若满足:

(1) <R,+>是阿贝尔群;

(2) <R,•>是可交换独异点，且无零因子，即对$\forall a,b\in R$, $a\neq 0, b\neq 0$ 则$a\bullet b\neq 0$;

(3) 运算•对+是可分配的,

则称<R,+,•>是整环。

注:（1）既是交换环、含幺环、无零因子环 的代数系统是整环。

（2）整环中的无零因子条件等价于乘法消去律，即

对于$c\neq 0$ 和$c\bullet a = c\bullet b$,有$a = b$.

## 域 (Field)

设<R,+,•>是一个代数系统,若满足:

(1) <R,+>是阿贝尔群;

(2) <R-{0},•>是阿贝尔群;

(3) 运算•对+是可分配的,

则称<R,+,•>是域。

例: 整数环Z整环，但不是域；实数环R既是是域。

两点结论:

(1) 域一定是整环。

(2) 有限整环必是域。