第5章　群、环和域

接下来的两章将介绍常见的几种代数结构，它们是用代数方法建立的数学模型. 本章着重讨论具有一个二元运算的代数系统，包括半群、独异点和群以及具有两个二元运算的代数系统，包括环和域. 群、环和域在组合计数、编码理论、形式语言与自动机理论等学科中都发挥了重要作用，而群是抽象代数中最古老且发展得最完善的代数系统. 在计算机科学中，对于代码的查错和纠错、自动机理论等各个方面的应用的研究，群是其基础.

本章的主要内容为半群、独异点和群的定义和基本性质，子群及其陪集，环和域的定义和基本性质等.

5.1　半群和独异点

5.1.1　半群和独异点的基本概念

定义 5.1　设 S 是一个非空集合，$*$ 是 S 上的一个二元运算，如果运算 $*$ 是可结合的，则称代数系统 $<S;*>$ 是**半群**.

若在半群 $<S;*>$ 中，运算 $*$ 满足交换律，则称 $<S;*>$ 为**交换半群**.

例如，(1) 代数系统 $<\mathbf{N};+>$ 和 $<\mathbf{N};\cdot>$、$<\mathbf{Z};+>$ 和 $<\mathbf{Z};\cdot>$、$<\mathbf{R};+>$ 和 $<\mathbf{R};\cdot>$ 都是半群，且都是交换半群. 但 $<\mathbf{Z};->$ 和 $<\mathbf{R}-\{0\};/>$ 不是半群，因为运算不满足结合律.

(2) 代数系统 $<M_n(\mathbf{R});+>$，$<M_n(\mathbf{R});\cdot>$ 都是半群，$<M_n(\mathbf{R});+>$ 是交换半群，$<M_n(\mathbf{R});\cdot>$ 不是交换半群.

(3) 代数系统 $<2^U;\cup>$ 和 $<2^U;\cap>$ 都是半群，且都是交换半群.

(4) 设 $S=\{R\mid R$ 是集合 A 上的关系$\}$，则对于关系的复合运算$\circ$，代数系统 $<S;\circ>$ 是半群，但不是交换半群.

若 $F=\{f\mid f$ 是 A 上的函数$\}$，则对于函数的复合运算$\circ$，代数系统 $<F;\circ>$ 也是半群，但不是交换半群.

【例 5.1】　设 S 是非空集合，对任意的 $x,y\in S$，定义 $x*y=y$，则代数系统 $<S;*>$ 是半群，但不是交换半群.

【例 5.2】　设代数系统 $<S;*>$ 是半群，$a\in S$，如果对任意的 $x,y\in S$，每当 $a*x=a*y$ 都有 $x=y$，则称元素 a 是**左可约的**. 试证明，如果 a,b 是左可约的，则 $a*b$ 也是左可约的.

证明　对任意的 $x,y\in S$，假设有 $(a*b)*x=(a*b)*y$.

因为 $<S;*>$ 是半群，所以 $*$ 是可结合的，有

$$(a*b)*x=a*(b*x),\quad (a*b)*y=a*(b*y)$$

则由假设有

$$a*(b*x)=a*(b*y)$$

因为 a 是左可约的，所以 $b*x=b*y$.

又因为 b 是左可约的，所以 $x=y$.

即对任意的 $x,y\in S$，如果 $(a*b)*x=(a*b)*y$，则有 $x=y$. 所以由左可约的定义可知，$a*b$ 也是左可约的.

因为半群 $<S;*>$ 中运算 $*$ 是可结合的，所以可以定义元素的幂.

定义 5.2 设 $<S;*>$ 是一个半群，则对任意的 $x\in S$ 和任意正整数 n，定义 x 的 ***n* 次幂**为

$$x^1=x,x^{n+1}=x^n*x(n\in \mathbf{Z}^+) \tag{5.1}$$

并称 n 为 x 的**指数**.

对任意的正整数 m,n 和任意的 $x\in S$，有

$$x^m*x^n=x^{m+n},\quad (x^m)^n=x^{mn} \tag{5.2}$$

定理 5.1 设 $<S;*>$ 是一个有限的半群，则必有 $a\in S$，使得 a 是一个幂等元.

证明 对任意的 $x\in S$，因为 $<S;*>$ 是半群，故由运算 $*$ 的封闭性和结合律知，

$$x^2=x*x\in S,\quad x^3=x^2*x=x*x^2\in S,\quad \cdots$$

因为 S 是有限集，所以根据鸽笼原理知，必存在正整数 $j>i$，使得 $x^i=x^j$.

令 $p=j-i$，便有 $x^i(=x^j=x^{p+i})=x^p*x^i$.

由此可得 $x^q=x^p*x^q$（正整数 $q\geqslant i$）.

因为 $p\geqslant 1$，所以总可以找到正整数 $k\geqslant 1$，使得 $kp\geqslant i$.

对于 S 中的元素 x^{kp}，就有

$$\begin{aligned}x^{kp}&=x^p*x^{kp}\\&=x^p*(x^p*x^{kp})\\&=x^{2p}*x^{kp}\\&=\cdots\\&=x^{kp}*x^{kp}.\end{aligned}$$

此即证得，在 S 中存在元素 $a=x^{kp}$，使得 $a*a=a$. ■

定义 5.3 若半群 $<S;*>$ 中的运算 $*$ 有单位元，则称该半群为**含幺半群**，常称为**独异点**.

若独异点 $<S;*>$ 中的运算 $*$ 满足交换律，则称该独异点为**交换独异点**.

例如，(1) 代数系统 $<\mathbf{N};+>$ 和 $<\mathbf{N};\cdot>$、$<\mathbf{Z};+>$ 和 $<\mathbf{Z};\cdot>$、$<\mathbf{R};+>$ 和 $<\mathbf{R};\cdot>$ 都是独异点，且都是交换独异点. 但 $<\mathbf{Z};->$ 和 $<\mathbf{R}-\{0\};/>$ 不是独异点.

(2) 代数系统 $<M_n(\mathbf{R});+>$，$<M_n(\mathbf{R});\cdot>$ 都是独异点，$<M_n(\mathbf{R});+>$ 是交换独异点，$<M_n(\mathbf{R});\cdot>$ 不是交换独异点.

(3) 代数系统 $<2^U;\cup>$ 和 $<2^U;\cap>$ 都是独异点，且都是交换独异点.

(4) 设 $S=\{R\mid R$ 是集合 A 上的关系$\}$，则对于关系的复合运算 $\circ$，代数系统 $<S;\circ>$ 是独异点，但不是交换独异点.

若 $F=\{f\mid f$ 是 A 上的函数$\}$，则对于函数的复合运算 $\circ$，代数系统 $<F;\circ>$ 也是独异点，但不是交换独异点.

注意：

(1) 独异点中唯一的单位元常记为 e.

(2) 设$<S;*>$为独异点，则关于运算$*$的运算表中没有两行或两列是相同的.

事实上，对任意的$x,y\in S$，当$x\neq y$时，总有$x*e=x\neq y=y*e$和$e*x=x\neq y=e*y$，所以在$*$的运算表中不可能有两行或两列是相同的.

在独异点$<S;*>$中也可定义元素的幂.

定义 5.4　设$<S;*>$是一个独异点，则对任意的$x\in S$和任意非负整数n，定义x的**n次幂**为

$$x^0=e,x^{n+1}=x^n*x(n\in\mathbf{N}) \tag{5.3}$$

并称n为x的**指数**.

对任意的非负整数m,n和任意的$x\in S$，有

$$x^m*x^n=x^{m+n},(x^m)^n=x^{mn} \tag{5.4}$$

定义 5.5　在独异点$<S;*>$中，如果存在元素$g\in S$，使得S中的每一元素a都能写成$g^i(i\in\mathbf{N})$的形式，则称独异点$<S;*>$为**循环独异点**，元素g称为该循环独异点的**生成元**.

【例 5.3】　试证$<\mathbf{N};+>$是循环独异点，并求其生成元.

证明　$<\mathbf{N};+>$是独异点，且0是加法运算的单位元.

对任意的$i\in\mathbf{N}$，若$i\neq0$，则$i=1+1+\cdots+1$(i个1相加)$=1^i$；若$i=0$，则有$0=1^0$.

故$<\mathbf{N};+>$为循环独异点，其生成元为1.

【例 5.4】　$<S;*>$是一个独异点，其中$S=\{1,a,b,c,d\}$，$*$是S上的二元运算，其运算表如表5.1所示.

表　5.1

$*$	1	a	b	c	d
1	1	a	b	c	d
a	a	a	b	d	d
b	b	b	d	a	a
c	c	d	a	b	b
d	d	d	a	b	b

因为1是单位元，a是幂等元，$b^3=d^3=a$，因此$1,a,b,d$的任意非负整数次幂最多只能表示S中4个不同元. 而

$$c^0=1,c^1=c,c^2=b,c^3=a,c^4=d$$

所以独异点$<S;*>$是一个循环独异点，其中c是生成元.

定理 5.2　每一个循环独异点都是交换独异点.

证明　设$<S;*>$为循环独异点且g为其生成元，则对任意的$x,y\in S$，存在$m,n\in\mathbf{N}$，使得$x=g^m,y=g^n$. 于是

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

所以$<S;*>$是交换独异点. ■

定理 5.3　设$<S;*>$是一个有限的独异点，则对每一个$x\in S$存在正整数j，使得x^j

是一个幂等元.

证明 见定理 5.1 的证明. ■

例如,例 5.4 中 $1, a, b^3(=a), d^3(=a), c^3(=a)$ 是幂等元.

定理 5.4 设$<S; *>$是独异点,$a, b \in S$ 且可逆,则

(1) $(a^{-1})^{-1}=a$.

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

证明 (1) 设 a^{-1} 是 a 的逆元,则有 $a*a^{-1}=a^{-1}*a=e$,因此 a^{-1} 可逆,且 $(a^{-1})^{-1}=a$.

(2) 设 a^{-1} 是 a 的逆元,b^{-1} 是 b 的逆元,因为

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

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

所以 $a*b$ 可逆,且 $(a*b)^{-1}=b^{-1}*a^{-1}$. ■

5.1.2 子半群和子独异点

定义 5.6 设$<S; *>$是一个半群,若$<H; *>$是$<S; *>$的子代数,则称$<H; *>$为$<S; *>$的**子半群**.

设$<S; *>$是一个独异点,若$<H; *>$是$<S; *>$的子代数,且单位元 $e \in H$,则称$<H; *>$为$<S; *>$的**子独异点**.

由定义知,子半群(子独异点)是一个半群(独异点);半群(独异点)是自身的一个子半群(子独异点). 此外,$<\{e\}; *>$也是独异点$<S; *>$的子独异点.

【例 5.5】 对于半群$<S; *>$的任一元素 $x \in S$,令集合 $H=\{x, x^2, x^3, \cdots\}$,则$<H; *>$是$<S; *>$的子半群.

【例 5.6】 对于半群$<\mathbf{Z}^+; +>$,$\mathbf{Z}^+$ 的子集

$$A_2 = \{2n \mid n \in \mathbf{Z}^+\},\quad A_3 = \{3n \mid n \in \mathbf{Z}^+\},\quad A_4 = \{4n \mid n \in \mathbf{Z}^+\},\quad \cdots$$

都是$<\mathbf{Z}^+; +>$的子半群.

【例 5.7】 对于独异点$<\mathbf{N}; +>$,子集 $A_2, A_3, A_4, \cdots$(同例 5.6)均不能形成$<\mathbf{N}; +>$的子独异点;而

$$B_2 = \{2n \mid n \in \mathbf{N}\}, B_3 = \{3n \mid n \in \mathbf{N}\}, B_4 = \{4n \mid n \in \mathbf{N}\}, \cdots$$

都能形成$<\mathbf{N}; +>$的子独异点.

定理 5.5 设$<S; *>$是一个交换独异点,则 S 的所有幂等元的集合 H 形成$<S; *>$的一个子独异点.

证明 由于 S 中单位元 e 适合 $e^2=e$,所以 $e \in H$,于是 H 是 S 的非空子集且包含 S 中的单位元 e.

对任意的 $x, y \in H$,由 $x^2=x, y^2=y$ 和运算 $*$ 是可交换的得知

$$(x*y)^2 = x^2*y^2 = x*y$$

因此 $x*y \in H$,于是 H 对于运算 $*$ 是封闭的,从而$<H; *>$是$<S; *>$的一个子独异点. ■

【思考 5.1】 设代数系统$<S; *>$和$<H; *>$都是独异点,若 $H \subseteq S$,则$<H; *>$是$<S; *>$的子独异点吗?

5.1.3　半群和独异点的同态

代数系统的同态(单同态、满同态)、同构和积代数的概念以及一些有关的结论可以推广到半群和独异点中.

定理 5.6　设 h 是从代数系统 $V_1=<S_1;*>$ 到代数系统 $V_2=<S_2;\circ>$ 的满同态,其中运算 $*$ 和 $\circ$ 都是二元运算,则

(1) 若 V_1 是(交换)半群,则 V_2 也是(交换)半群.

(2) 若 V_1 是(交换)独异点,则 V_2 也是(交换)独异点.

推论 5.1　(交换)半群的同态像是(交换)半群,(交换)独异点的同态像是(交换)独异点.

定理 5.7　给定代数系统 $V_1=<S_1;*>$ 和 $V_2=<S_2;\circ>$,其中运算 $*$ 和 $\circ$ 都是二元运算,则

(1) 若 V_1 和 V_2 是(交换)半群,则 $V_1\times V_2$ 也是(交换)半群.

(2) 若 V_1 和 V_2 是(交换)独异点,则 $V_1\times V_2$ 也是(交换)独异点.

5.2　群

5.2.1　群的基本概念

1. 群的定义

定义 5.7　设 $<G;*>$ 是一个代数系统,如果 G 上的二元运算 $*$ 满足下列条件,则称 $<G;*>$ 是一个**群**,简记成群 G.

(1) 运算 $*$ 是可结合的;

(2) 存在单位元 $e\in G$;

(3) G 中所有元素都可逆.

如果群 $<G;*>$ 的运算 $*$ 是可交换的,则称该群为**交换群**或**阿贝尔群**.

例如,代数系统 $<\mathbf{Z};+>$、$<\mathbf{R};+>$、$<\mathbf{R}-\{0\};\cdot>$、$<M_n(\mathbf{R});+>$、$<2^U;\cup>$、$<2^U;\cap>$ 都是群,且为交换群. 但 $<\mathbf{N};+>$、$<\mathbf{Z};\cdot>$、$<\mathbf{R};\cdot>$、$<M_n(\mathbf{R});\cdot>$ 都不是群,因为不是所有元都可逆.

【例 5.8】　代数系统 $<\mathrm{N}_n;\oplus_n>$ 为群,且为交换群.

证明　(1) 先证运算满足结合律.

对任意的 $a,b,c\in\mathrm{N}_n$,令

$$a+b=nm_1+\mathrm{res}_n(a+b),\quad b+c=nm_2+\mathrm{res}_n(b+c)$$

则有

$$\begin{aligned}(a\oplus_n b)\oplus_n c&=\mathrm{res}_n(a+b)\oplus_n c=\mathrm{res}_n(\mathrm{res}_n(a+b)+c)\\&=\mathrm{res}_n((nm_1+\mathrm{res}_n(a+b))+c)=\mathrm{res}_n((a+b)+c),\\a\oplus_n(b\oplus_n c)&=a\oplus_n\mathrm{res}_n(b+c)=\mathrm{res}_n(a+\mathrm{res}_n(b+c))\\&=\mathrm{res}_n(a+(nm_2+\mathrm{res}_n(b+c)))=\mathrm{res}_n(a+(b+c))\\&=\mathrm{res}_n((a+b)+c),\end{aligned}$$

因此$(a\oplus_n b)\oplus_n c=a\oplus_n(b\oplus_n c)$，即$\oplus_n$满足结合律.

(2) 再证单位元的存在性.

0是单位元.

(3) 最后证逆元的存在性.

$x=0$的逆元是0，$x\neq 0$的逆元是$n-x$.

综上所述，$<\mathrm{N}_n;\oplus_n>$是一个群.

由于运算可交换，故$<\mathrm{N}_n;\oplus_n>$也是一个交换群.

【例5.9】 设$<G;*>$是群，$g\in G$，定义$a\circ b=a*g*b$，证明$<G;\circ>$是群.

证明 对任意的$x,y\in G$，由$x\circ y=x*g*y$可知，$\circ$在G上是封闭的，因此$<G;\circ>$是一个代数系统.

(1) 对任意的$x,y,z\in G$，有

$$(x\circ y)\circ z=(x*g*y)\circ z=(x*g*y)*g*z$$

$$x\circ(y\circ z)=x\circ(y*g*z)=x*g*(y*g*z)$$

由$<G;*>$是群可知，$*$是可结合的，所以

$$(x*g*y)*g*z=x*g*(y*g*z)$$

于是有$(x\circ y)\circ z=x\circ(y\circ z)$，所以$\circ$是可结合的.

(2) 令$e'=g^{-1}$，则对任意的$x\in G$，有

$$x\circ e'=x*g*e'=x*g*g^{-1}=x$$

同理可证，$e'\circ x=x$.

所以$e'=g^{-1}$是G中关于$\circ$的单位元.

(3) 对任意的$x\in G$，令$y=g^{-1}*x^{-1}*g^{-1}$，有

$$x\circ y=x*g*(g^{-1}*x^{-1}*g^{-1})=g^{-1}$$

同理可证，$y\circ x=g^{-1}$.

所以G的每个元素都有逆元.

综上所述，$<G;\circ>$是群.

定义5.8 设$<G;*>$是一个代数系统，如果$<G;*>$是独异点，且G中所有元素都可逆，则$<G;*>$是一个群.

注意：

(1) 一个群必是独异点，也必是半群，因此群也可以如下定义.

(2) 若$<G;*>$是群，且$\sharp G>1$，则$<G;*>$无零元.

设e是群$<G;*>$的单位元. 若$<G;*>$中存在零元，不妨记为θ，则由前面的定理知，$e\neq\theta$.

对任意的$x\in G$有$\theta*x=\theta\neq e$，故θ没有逆元，与$<G;*>$是群矛盾，所以$<G;*>$中没有零元.

(3) 若$<G;*>$是群，则$<G;*>$中唯一的幂等元是单位元e.

设$a\in G$是幂等元，则$a*a=a$，因而

$$e=a^{-1}*a=a^{-1}*(a*a)=(a^{-1}*a)*a=e*a=a$$

所以G中唯一的幂等元是单位元e.

2. 群中元素的幂

设$<G;*>$是群，因$<G;*>$是独异点，故对任意的$x\in G$，有

$$x^0=e,x^{n+1}=x^n*x(n\in\mathbf{N})$$

由于$x^{-1}\in G$，故有

$$(x^{-1})^0=e,(x^{-1})^{n+1}=(x^{-1})^n*x^{-1}(n\in\mathbf{N}) \tag{5.5}$$

引入记号$x^{-n}=(x^{-1})^n=x^{-1}*x^{-1}*\cdots*x^{-1}$（$n$个$x^{-1}$），则式(5.5)可表示为

$$(x^{-1})^0=e,x^{-n-1}=x^{-n}*x^{-1}(n\in\mathbf{N})$$

因此群$<G;*>$中任意元素x可定义整数次幂.

定义 5.9　设$<G;*>$是群，则对任意的$x\in G$，定义x的**幂**为

$$x^0=e,x^{n+1}=x^n*x,\quad x^{-n}=(x^{-1})^n \tag{5.6}$$

其中$n\in\mathbf{N}$.

对任意的整数m,n和任意$x\in G$，下面两式仍然成立：

$$x^m*x^n=x^{m+n},(x^m)^n=x^{mn} \tag{5.7}$$

因此又有

$$x^{-n}=(x^{-1})^n=(x^n)^{-1} \tag{5.8}$$

例如，$x^5*x^{-2}=x^{5-2}=x^3$.

因为$x^5*x^{-2}=x^5*(x^{-1})^2$

$$\begin{aligned}&=(x*x*x*x*x)*(x^{-1}*x^{-1})\\&=(x*x*x)*(x*x*x^{-1}*x^{-1})\\&=(x*x*x)*(x*(x*x^{-1})*x^{-1})\\&=(x*x*x)*(x*e*x^{-1})\\&=(x*x*x)*(x*x^{-1})\\&=(x*x*x)*e\\&=x*x*x=x^3.\end{aligned}$$

又如，$(x^2)^{-3}=x^{-6}$.

$$(x^2)^{-3}=((x^2)^{-1})^3=(x^2)^{-1}*(x^2)^{-1}*(x^2)^{-1}=(x*x)^{-1}*(x*x)^{-1}*(x*x)^{-1}$$

根据结合律

$$(x*x)*(x^{-1}*x^{-1})=(x^{-1}*x^{-1})*(x*x)=e$$

所以$(x*x)^{-1}=x^{-1}*x^{-1}$.

因此$(x^2)^{-3}=(x^{-1}*x^{-1})*(x^{-1}*x^{-1})*(x^{-1}*x^{-1})$

$$\begin{aligned}&=x^{-1}*x^{-1}*x^{-1}*x^{-1}*x^{-1}*x^{-1}\\&=(x^{-1})^6=x^{-6}.\end{aligned}$$

3. 群的阶和元素的周期

定义 5.10　设$<G;*>$是群，如果G是有限集，则称$<G;*>$是**有限群**，G中元素的个数称为群$<G;*>$的**阶**；若G是无限集，则称$<G;*>$是**无限群**.

定义 5.11　设$<G;*>$是一个群，$a\in G$，若存在正整数r，使得$a^r=e$，则称元素a具有**有限周期**或**有限阶**. 使$a^r=e$成立的最小正整数r称为a的**周期**或**阶**.

如果对于任何正整数 r 均有 $a^r \neq e$，则称 a 具有**无限周期**或**无限阶**.

显然，群中单位元具有有限周期，且周期是 1.

【例 5.10】 在群 $<\mathbf{R}-\{0\};\cdot>$ 中，因为

$$(-1)^2 = (-1)^4 = (-1)^6 = \cdots = 1, (-1)^1 = -1 \neq 1$$

所以 -1 的周期为 2.

其他元(1 和 -1 除外)的周期为无限.

【例 5.11】 在群 $<N_6;\oplus_6>$ 中，单位元 0 的周期是 1；1 和 5 的周期均为 6；2 和 4 的周期为 3；3 的周期为 2，它们都不超过群 $<N_6;\oplus_6>$ 的阶 6.

5.2.2 群的基本性质

定理 5.8 设 $<G;*>$ 是一个群，则对任意的 $a,b\in G$，

(1) 存在唯一的元素 $x\in G$，使 $a*x=b$.

(2) 存在唯一的元素 $y\in G$，使 $y*a=b$.

证明 (1) 因为 $a,b\in G$，所以 $a^{-1}*b\in G$.

令 $x=a^{-1}*b$，则 $a*(a^{-1}*b)=(a*a^{-1})*b=e*b=b$.

因此，$a^{-1}*b$ 是方程 $a*x=b$ 的解.

假设 $x'\in G$ 也使得 $a*x'=b$ 成立，则

$$x' = e*x' = (a^{-1}*a)*x' = a^{-1}*(a*x') = a^{-1}*b$$

因此 $x=a^{-1}*b$ 是满足 $a*x=b$ 的唯一元素.

(2) 同法可证. ■

注意：*定理说明在群中方程 $a*x=b$ 与 $y*a=b$ 有唯一解.*

定理 5.9 设 $<G;*>$ 是一个群，则运算 $*$ 满足**消去律**，即对任意的 $a,b,c\in G$，

(1)(**左消去律**)若 $a*b=a*c$，则 $b=c$；

(2)(**右消去律**)若 $b*a=c*a$，则 $b=c$.

证明 (1) 令 $a*b=a*c=d$，根据定理 5.8，方程 $a*x=d$ 在 G 中只有唯一的解，故得 $b=c$.

(2) 同法可证. ■

推论 5.2 有限群 $<G;*>$ 的运算表中的每一行或每一列都是 G 的元素的一个排列.

【例 5.12】 设 $<G;*>$ 是一个群，且对任意的 $a,b\in G$，有 $(a*b)^2=a^2*b^2$，则 $<G;*>$ 是阿贝尔群.

证明 对任意的 $x,y\in G$，由已知 $(x*y)^2=x^2*y^2$ 有

$$(x*y)*(x*y) = (x*x)*(y*y)$$

于是

$$x*(y*x)*y = x*(x*y)*y$$

利用定理 5.9 的消去律得 $y*x=x*y$. 故 $<G;*>$ 是阿贝尔群.

显然，该命题的逆命成立，且对任意正整数 n 有 $(a*b)^n=a^n*b^n$.

定理 5.10 设 $<G;*>$ 是一个群，则对任意的 $x,y\in G$，有

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

证明　因为 $x^{-1}*x=x*x^{-1}=e$,故$(x^{-1})^{-1}=x$.

又因为$(x*y)*(x*y)^{-1}=e$,及

$$(x*y)*(y^{-1}*x^{-1})=x*(y*y^{-1})*x^{-1}=x*x^{-1}=e$$

因此

$$(x*y)*(x*y)^{-1}=(x*y)*(y^{-1}*x^{-1})$$

根据定理 5.9,有$(x*y)^{-1}=y^{-1}*x^{-1}$. ■

推论 5.3　设$<G;*>$是一个群,则对任意的 $a_1,a_2,\cdots,a_n\in G$,有

$$(a_1*a_2*\cdots*a_n)^{-1}=a_n^{-1}*a_{n-1}^{-1}*\cdots*a_1^{-1}$$

特别是在交换群中,$(a_1*a_2*\cdots*a_n)^{-1}=a_1^{-1}*a_2^{-1}*\cdots*a_n^{-1}$.

定理 5.11　若群$<G;*>$中的元素 a 具有有限周期 r,则 $a^k=e$ 当且仅当 $r|k$,即 k 是 r 的整数倍.

证明　若 $r|k$,则必存在整数 m 使得 $k=mr$,所以有

$$a^k=a^{mr}=(a^r)^m=e^m=e$$

反过来,根据带余除法,存在整数 m 和 i 使得

$$k=mr+i,\quad 0\leqslant i<r$$

从而有

$$e=a^k=a^{mr+i}=(a^r)^m*a^i=e*a^i=a^i$$

因为 a 的周期为 r,故必有 $i=0$. 这就证明了 $r|k$. ■

定理 5.12　群中任一元素与它的逆元具有相同的周期.

证明　设 g 为群$<G;*>$中任一元素,则 g 与 g^{-1}的周期中有一个为有限时,另一个一定也是有限的. 假定 g 有有限周期 r,则由$(g^{-1})^r=(g^r)^{-1}=e^{-1}=e$ 知,g^{-1}必有有限周期.

设 g^{-1}的周期为 t,根据定理 5.11 有 $t|r$.

这说明 g 的逆元的周期是 g 的周期的因子.

而 g 又是 g^{-1}的逆元,所以 g 的周期也是 g^{-1}的周期的因子,故有 $r|t$.

于是 $r=t$. 即 g 的周期与 g^{-1}的周期相同. ■

定理 5.13　在有限群$<G;*>$中,每个元素均具有有限周期,且周期不超过群$<G;*>$的阶.

证明　设$<G;*>$是有限群,$\sharp G=n$,对任意的 $a\in G$,构造 G 中的序列 $a,a^2,a^3,\cdots,a^n,a^{n+1}$.

因为$\sharp G=n$,所以由鸽笼原理知,序列中必存在 $a^i=a^j(1\leqslant i<j\leqslant n+1)$,于是有

$$e=a^i*a^{-i}=a^j*a^{-i}$$

即

$$a^{j-i}=e(0<j-i\leqslant n)$$

因此 a 的周期至多为 $j-i$,而 $j-i\leqslant\sharp G$. ■

注意：定理 5.13 的结论对于无限群不成立. 例如,群$<\mathbf{Z};+>$中,除单位元 0 外,其他元素的周期都为无限.

【例 5.13】　设 a,b 为群$<G;*>$中的两个元素,它们的周期分别为 r,s,又设 $a*b=b*a$,并且$(r,s)=1$,则元素 $a*b$ 的周期为 rs.

证明 由 $a*b=b*a$ 可得

$$(a*b)^{rs}=a^{rs}*b^{rs}=(a^r)^s*(b^s)^r=e^s*e^r=e$$

因此，$a*b$ 有有限周期，设为 d，则 $d|rs$，即 rs 是 d 的倍数.

另一方面，因为 $(a*b)^d=e$，且 $a*b=b*a$，故有

$$(a*b)^d=a^d*b^d=e$$

因此，$a^d=b^{-d}$，于是有

$$(a^d)^s=(b^{-d})^s=(b^s)^{-d}=e^{-d}=e$$

从而 $r|ds$.

由于 $(r,s)=1$，故有 $r|d$，即 d 是 r 的倍数.

同法可证 $s|d$，即 d 是 s 的倍数.

于是 d 是 r,s 的公倍数，即 $[r,s]|d$.

又由于 r,s 互素，故 $[r,s]=rs$，从而又得到 $rs|d$.

综上所述，$d|rs,rs|d$，故 $d=rs$.

【思考 5.2】 在群 $<G;*>$ 中，元素 a 和 b 有有限周期时，$a*b$ 一定有有限周期吗？元素 a 或 b 有无限周期时，$a*b$ 的周期一定无限吗？

5.2.3 群的同态

代数系统的同态（单同态、满同态）、同构和积代数的概念以及一些有关的结论也可以推广到群中.

定理 5.14 设 h 是从代数系统 $V_1=<G_1;*>$ 到代数系统 $V_2=<G_2;\circ>$ 的满同态，其中运算 $*$ 和 $\circ$ 都是二元运算，若 V_1 是（交换）群，则 V_2 也是（交换）群.

推论 5.4 （交换）群的同态像是（交换）群.

定理 5.15 给定代数系统 $V_1=<G_1;*>$ 和 $V_2=<G_2;\circ>$，其中运算 $*$ 和 $\circ$ 都是二元运算，若 V_1 和 V_2 是（交换）群，则 $V_1\times V_2$ 也是（交换）群.

5.3 置换群与循环群

1. 置换的概念

定义 5.12 设 $A=\{a_1,a_2,\cdots,a_n\}$ 是一个非空有限集合，A 上的双射函数 f 称为 A 的 n 元**置换**.

一个 n 元置换 f：$A\to A$ 常表示成如下形式：

$$f=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ f(a_1) & f(a_2) & \cdots & f(a_n)\end{pmatrix} \tag{5.9}$$

这里 n 个列的次序是任意的.

【例 5.14】 设集合 $A=\{a,b,c\}$，则 A 上的所有三元置换为

$$1=\begin{pmatrix}a & b & c\\ a & b & c\end{pmatrix},\quad \alpha=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix},\quad \beta=\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}$$

$$\gamma=\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix},\quad \delta=\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix},\quad \varepsilon=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}$$