第14章

代数系统

计算机科学的迅速发展在很大程度上受益于数学工具的前所未有的进步。除了逻辑学、集合论、图论和组合数学等的巨大推动作用外，近百年发展起来的代数系统理论对于可计算模型研究、抽象数据结构、形式语言理论、程序设计语言语义分析等许多方面产生的影响也是深远的。代数系统理论提供了对各种表面上不同的实际问题调试抽象的途径，使人们更能把握住事物的本质，进行形式化的研究，又反过来指导实践的深入。

代数系统又称为代数结构。群、环、域、格和布尔代数是典型的系统。

14.1 二元运算及其性质

客观世界的统一性是通过事物之间的联系体现出来的，这些联系可以从不同的角度加以观察和研究。二元关系和函数是这类关系的重要方面。除此而外，我们还注意到通过对象物的“合成”或运算产生一个新对象的联系方式，例如两个命题的析取、两个集合的交、两个函数的复合、两个数的和、两个多项式的积、矩阵的逆等。从这些具体事物中抽象出它们的共性，把注意力集中在运算的一些基本性质上，就可以发现包含于对象中的更一般的规律性。

定义 14.1 设 S 是一个非空集合，映射 $f: S^n \to S$ 称为 S 上的一个 **n 元运算**。

n 元运算也可以看成 $n+1$ 元关系。最常见的是一元运算 $f: S \to S$ 和二元运算 $g: S \times S \to S$。例如数的相反数、命题的否定、集合的补、矩阵的逆等都是一元运算。不过本章中除特别声明外所说的运算都指的是二元运算。对于二元运算 $g: S \times S \to S$，元素 x 和 y 的运算结果 $g(x, y)$ 习惯上用中缀形式 xgy 表示。例如，数 a 和 b 的和运算，在习惯上表示成 $a+b$ 而不表示成 $+(a, b)$ 的形式。

为叙述统一起见，我们采用符号“$\cdot$”，“$*$”等表示一般的二元运算符，其具体意义由上下文确定。在描述一个二元运算时，有时也采用一个表的形式表示。

【例 14.1】 设集合 $S=\{a, b, c, d\}$。在 S 上定义一个二元运算“$\cdot$”如表 14-1 所示，称这种表为**运算表**。从运算表看出，$a \cdot a=a$，$b \cdot b=b$，$c \cdot d=d$，$d \cdot b=d$。当集合 S 所含元素较少时，用运算表的形式定义运算显得一目了然。 ■

表 14-1

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	b	d
d	a	d	c	b

对于运算，重要和基本的问题是它具有哪些基本性质。

定义 14.2 设“·”是定义在集合 S 上的二元运算。如果

①$\forall x, y\in S, x\cdot y\in S$，则称“·”在 S 上是**封闭**的。

②$\forall x, y\in S, x\cdot y=y\cdot x$，则称“·”在 S 上是**可交换**的。

③$\forall x, y, z\in S, x\cdot(y\cdot z)=(x\cdot y)\cdot z$，则称“·”是**可结合**的。

④$\forall x\in S, x\cdot x=x$，则称“·”是**幂等**的。

【例 14.2】 定义在自然数集 $\mathbf{N}$ 上的加法和乘法运算满足封闭性、可换性和可结合性，但定义在 $\mathbf{N}$ 上的减法运算则不满足封闭性、可换性和可结合性；此外，算术运算也不满足幂等性。

定义在幂集 2^A 上的运算 $\cup$ 和 $\cap$ 都同时满足封闭、可交换、可结合和幂等四个性质。 ■

定义 14.3 设·和 $*$ 是同时定义在 S 上的两个二元运算。如果

①$\forall x, y, z\in S, x*(y\cdot z)=(x*y)\cdot(x*z)$ 且 $(y\cdot z)*x=(y*x)\cdot(z*x)$，则称运算 $*$ 关于·是**可分配**的。

②$*$ 和·是可换运算，且 $\forall x, y\in S, x*(x\cdot y)=x$ 及 $x\cdot(x*y)=x$，则称运算 $*$ 和·满足**吸收律**。

【例 14.3】 在数集合上，乘法关于加法是可分配的，即有

$$a\times(b+c)=a\times b+a\times c$$

及

$$(b+c)\times a=b\times a+c\times a$$

但加法关于数的乘法不是可以分配的。

在幂集上 2^A 上，集合交运算 $\cap$ 和并运算 $\cup$ 是相互可分配的，并且都满足吸收律，这些都是集合论中已知的事实。 ■

【例 14.4】 设运算“$\vee$”，“$\wedge$”分别是实数集 $\mathbf{R}$ 上的最大值和最小值运算，即对任意的 $a, b\in\mathbf{R}$，$a\vee b=\max(a, b)$，$a\wedge b=\min(a, b)$，试判断运算“$\vee$”与“$\wedge$”是否满足分配律和吸收律。

【解】 对任意的 $a, b, c\in\mathbf{R}$，有

$$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)$$

$$a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$$

显然成立，又因为“$\vee$”和“$\wedge$”满足交换律，由定义，“$\vee$”与“$\wedge$”之间满足分配律。同理，

$$a\vee(a\wedge c)=a,\ a\wedge(a\vee c)=a$$

因此“$\vee$”与“$\wedge$”之间满足吸收律。所以，“$\vee$”与“$\wedge$”满足分配律和吸收律。 ■

14.2 代数系统的定义与特异元

定义 14.4 一个非空集合 S 连同若干个定义在 S 上的运算 $f_1, f_2, \cdots, f_k$ 所组成的系统称为一个**代数系统**，记为 $\langle S, f_1, f_2, \cdots, f_k\rangle$。

判断集合 S 及其上的代数运算是否是代数系统，关键是判断两点：一是集合 S 非空，二是这些运算关于 S 是否满足封闭性。

现实世界中有很多代数系统。对于具有相同性质的代数系统，我们没必要分散进行个别研究，而是进行集中研究，这就形成了特定的代数系统。本教材只介绍半群、群、环、域、格、布尔代数等典型的代数系统，其中重点是半群、群、格与布尔代数。

【例 14.5】 常见的代数系统如 $\langle\mathbf{Z}, +\rangle$，$\langle\mathbf{Q}, +, \times\rangle$，$\langle 2^A, \cap, \cup\rangle$ 等。如果设 M_n 是全体 n 阶满秩阵构成的集合，那么，M_n 与矩阵乘法“·”构成代数系统 $\langle M_n, \cdot\rangle$。另

外，同一个集合与不同的运算构成不同的代数系统。例如，在整数集上既可定义运算“+”，也可定义“×”，还可以定义运算“max”（即求两个数中的最大值），相应的代数系统可以表示为〈**Z**，+〉，〈**Z**，×〉和〈**Z**，max〉。 ■

在同一个代数系统中，有一些特殊元素与所定义的运算紧密相关，在系统结构中起着重要的作用，这些元素被称为**特异元**。

定义 14.5　设〈S，$\cdot$〉是一个代数系统，则

①如果$\exists e\in S$使$\forall x\in S$，$e\cdot x=x\cdot e=x$，则称e为（代数系统）的**幺元**（或**单位元**）。

②如果存在$\theta\in S$，使$\forall x\in S$，$\theta\cdot x=x\cdot\theta=\theta$，则称$\theta$为系统的**零元**。

③$a\in S$，如果$a\cdot a=a$，则称a是系统的**幂等元**。

【例 14.6】 在代数系统〈**Z**，+〉中，数 0 是单位元，也是唯一幂等元，但是没有零元。在代数系统〈**Z**，×〉中，数 1 是幺元，数 0 是零元，1 和 0 都是幂等元。

在代数系统〈2^S，$\cup$〉中，空集$\varnothing$是幺元，因为任何集合与空集的并仍是这个集合本身；集合 S 是系统的零元，因为对任何 $X\in 2^S$，$X\cup S=S$。请读者想一想，代数系统〈2^S，$\cap$〉的幺元和零元是什么？ ■

定义 14.6　设在代数系统〈S，$\cdot$〉中，e是幺元，a是S中的一个元素。如果存在$b\in S$使得$a\cdot b=b\cdot a=e$，则称b是a的**逆元**，记为$b=a^{-1}$。

由定义可知，如果 b 是 a 的逆元，则 a 也是 b 的逆元。要注意，在一个代数系统中，并不是每个元都存在着逆元。

【例 14.7】 在代数系统〈**Z**，+〉中，每个元$a\in\mathbf{Z}$的逆元是$-a$。在代数系统〈M_n，$\cdot$〉中，由于单位元是 n 阶单位阵，因此，元素 $A\in M_n$ 的逆是 A^{-1}。

对于代数系统〈**Z**，×〉而言，除了幺元 1 以自身为逆元外，其他元素均无逆元。 ■

接下来的问题是，在一个代数系统中如果存在幺元、零元或某元有逆元，这些元素是否唯一？

定理 14.1　设〈S，$\cdot$〉是一个代数系统。如果存在幺元，则幺元是唯一的；如果存在零元，则零元是唯一的；如果元a有逆元，且“$\cdot$”可结合，则逆元是唯一的。

【证明】 反设〈S，$\cdot$〉含有幺元 e_1 和 e_2，按定义应该有 $e_1=e_1\cdot e_2=e_2$，故是唯一的。同理，如果 S 中有两个零元 θ_1 和 θ_2，由定义 $\theta_1=\theta_1\cdot\theta_2=\theta_2$，故零元也是唯一的。

现在设 e 是系统的单位元，元素 a 有两个逆元 a_1 和 a_2，那么

$$a_1=a_1\cdot e=a_1\cdot(a\cdot a_2)=(a_1\cdot a)\cdot a_2=e\cdot a_2=a_2$$

这说明逆元也是唯一的。 ■

根据运算满足的性质条件，可以把含单个二元运算的代数系统进行分层。

定义 14.7　设〈S，$\cdot$〉是一个代数系统，则

①当“$\cdot$”是封闭的，称〈S，$\cdot$〉为**广群**。

②如果〈S，$\cdot$〉是广群，且“$\cdot$”是可结合运算，则称〈S，$\cdot$〉是**半群**。

③如果〈S，$\cdot$〉是半群，且存在幺元，则称〈S，$\cdot$〉为**含幺半群**。

④如果〈S，$\cdot$〉是含幺半群，且每个元素都有逆元，则称〈S，$\cdot$〉为**群**。

从定义看，全部群$\subset$全部含幺半群$\subset$全部半群$\subset$全部广群。群的条件最多，可用闭、结、幺、逆四个字加以概括。

习题十四

1. 列出以下运算的运算表：

(1) $A=\left\{1, 2, \frac{1}{2}\right\}$，$\forall x\in A$，$\circ x$ 是 x 的倒数，即 $\circ x=\frac{1}{x}$。

(2) $A=\{1, 2, 3, 4\}$，$\forall x, y\in A$，有 $x\circ y=\max(x, y)$，$\max(x, y)$ 是 x 和 y 中较大的数。

2. 判断下列集合对所给的二元运算是否封闭：

(1) 整数集合 $\mathbf{Z}$ 和普通的减法运算。

(2) 非零整数集合 $\mathbf{Z}^*$ 和普通的除法运算。

(3) 全体 $n\times n$ 实矩阵集合 $M_n(\mathbf{R})$ 和矩阵加法及乘法运算，其中 $n\geqslant 2$。

(4) 全体 $n\times n$ 实可逆矩阵集合关于矩阵加法和乘法运算，其中 $n\geqslant 2$。

(5) 正实数集合 $\mathbf{R}^+$ 和 $\circ$ 运算，其中 $\circ$ 运算定义为：$\forall a, b\in\mathbf{R}^+$，$a\circ b=ab-a-b$。

(6) $n\in\mathbf{Z}^+$，$n\mathbf{Z}=\{nz\mid z\in\mathbf{Z}\}$，$n\mathbf{Z}$ 关于普通的加法和乘法运算。

(7) $A=\{a_1, a_2, \cdots, a_n\}$，$n\geqslant 2$，$\circ$ 运算定义如下：$\forall a_i, a_j\in A$，$a_i\circ a_j=a_j$。

(8) $S=\{2x-1\mid x\in\mathbf{Z}^+\}$ 关于普通的加法和乘法运算。

(9) $S=\{0, 1\}$，S 关于普通的加法和乘法运算。

(10) $S=\{x\mid x=2^n, n\in\mathbf{Z}^+\}$，$S$ 关于普通的加法和乘法运算。

3. 对于上题中封闭的二元运算判断是否适合交换律、结合律和分配律。

4. 设 $S=\{a, b, c\}$，运算“$\cdot$”由表 14-2 定义。

表 14-2

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

判断代数系统 $\langle S, \cdot\rangle$ 是否为广群、半群，是否含幺半群、群。

5. 表 14-3 中所列运算定义在实数集 $\mathbf{R}$ 上，请在下表的各栏填上该运算是否具有指定性质。

表 14-3

	$+$	$-$	$\times$	max	min	$\lvert x-y\rvert$
封闭性						
可结合性						
可换性						
存在幺元						
存在零元						
每元有逆元						

6. 设 $\langle S, \cdot\rangle$ 是一个代数系统，e_l 和 e_r 是 S 中两元。如果 $\forall x\in S$，都有 $e_l\cdot x=x$（或 $x\cdot e_r=x$），则称 e_l（或 e_r）为左幺元（或右幺元）。

(1) 试构造一个代数系统，使其只有左幺元。

(2) 证明：如果 $\langle S, \cdot\rangle$ 中既有左幺元 e_l 又有右幺元 e_r，则 $e_l=e_r$。

7. 设 $\langle S, \cdot\rangle$ 是一个含幺元 e 的代数系统，且满足结合律，$a\in S$，如果存在元 b，$c\in S$ 使得 $b\cdot a=e$（或 $a\cdot c=e$），则称 b 是 a 的左逆元（或 c 是 a 的右逆元）。证明：如果一个元既有左逆元 b 又有右逆元 c，则必 $b=c$。

第15章

半群与群

群是一种特殊的代数系统，是最重要的代数系统之一。群的理论广泛应用于数学、物理、化学以及很多人们不太熟悉的领域如社会学等。对计算机科学而言，群在自动化理论、形式语言、语法分析、编码理论等方面都有直接应用，并显示出其强大功能。

15.1 半群

上一章中已经给出了半群的定义，它要求运算是可结合的。许多常见的代数系统都是半群，甚至是含幺半群。下面是一些典型的半群例子。

【例 15.1】 〈**R**，＋〉满足封闭、可结合、有幺元 0 的条件，因而是含幺半群。另外，它还满足可换性，每个元 $x\in\mathbf{R}$ 都有加法逆元 $-x$，因此，〈**R**，＋〉也是一个可换群。

〈**R**，×〉满足封闭。可结合、有幺元 1，因此是含幺半群。注意，因为 0 无乘法逆元，所以〈**R**，×〉只能是含幺半群。 ■

【例 15.2】 设 $M_{m,n}$ 表示全体 m 行 n 列矩阵构成的集合，＋是矩阵加法，那么〈$M_{m,n}$，＋〉满足封闭、可结合的条件。元素全为 0 的 m 行 n 列矩阵是幺元，因此〈$M_{m,n}$，＋〉是含幺半群。此外，$M_{m,n}$ 中每个矩阵 $\mathbf{A}_{m,x,n}$ 都有加法逆矩阵 $-\mathbf{A}_{m\times n}$，因而〈$M_{m,n}$，＋〉还满足逆元条件。 ■

【例 15.3】 设 F 是由定义在非空集合 S 上的全体函数构成的集合，即 $F=\{f: S\to S\}$。对于函数的复合运算，〈F，∘〉满足封闭性和可结合性，所以是半群。此外，定义在 S 上的恒等函数 I_S 是〈F，∘〉的幺元，所以〈F，∘〉又是含幺半群。 ■

【例 15.4】 设 Σ 是非空有限字母表，Σ^* 是由定义在 Σ 上的全体有限长字母串构成的集合，或叫做 Σ 上全体字的集合。在 Σ^* 上定义运算“∘”为字的连接，例如设 $\Sigma=\{0, 1\}$，$\mu=0110$，$v=11$，μ，$v\in\Sigma^*$ 则 $\mu\circ v=011011$。则〈Σ^*，∘〉满足封闭和可结合的条件，并且空字 λ 是系统的幺元，所以〈Σ^*，∘〉是一个含幺半群。 ■

半群或含幺半群在计算机科学中有广泛的应用，尤其在从编译技术发展起来的形式语言与自动机理论领域，含幺半群是很重要的的内容之一。下面是半群的一个简单的应用例子。

【例 15.5】 设一个简单的液晶显示电子表仅有显示时、分的两个功能，有 0，1 两个按键（如图 15-1a 所示）。按 1 键时由正常状态转入调分状态，此时按 0 键 m 次可以调增分数 m；再按 1 键则转入调时状态，此时按 0 键 n 次，则时数增加 n；最后再按 1 键回复到正常状态。这一调节过程如图 15-1b 所示。

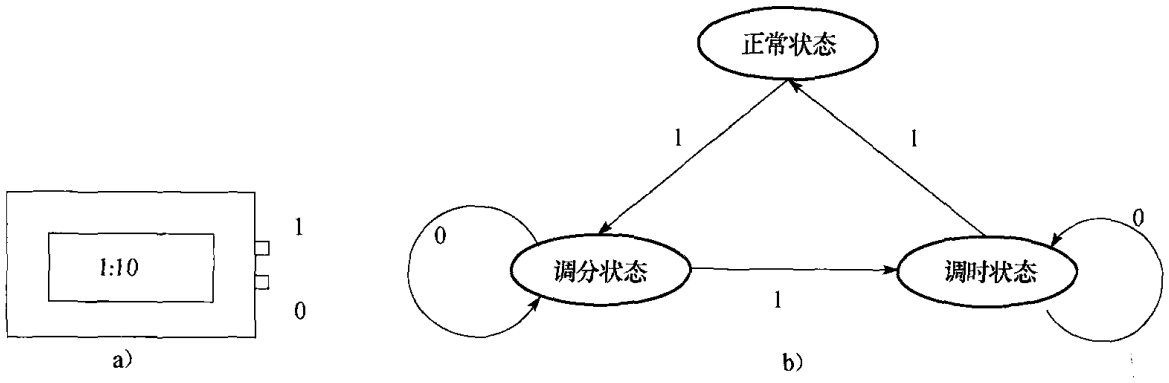

图 15-1

上面的调分和调时过程可表示为如图 15-2 所示，或由符号 1 和 0 组成的形如 10^m10^n1 的字符串集，即字母表 $\Sigma=\{0,1\}$ 上的一个语言 $L=\{10^m10^n1 \mid m, n\geqslant 0\}$。这种字母串可以被电子表中的微处理器（可以看成是一个小小的计算机）识别并执行，其动作原理就是图 15-1b 所示的状态图，称为一个**有限自动机**，它反映了电子表依令而行的规则。语言 L 被相应地称为这个自动机所识别的语言。■

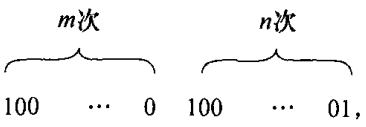

图 15-2

设〈S, $\cdot$〉是半群，$a\in S$，n 是正整数，约定符号 a^n 表示 n 个 a 在运算“$\cdot$”下的结果。可以递归定义如下：

①$a^1=a$

②$a^{n+1}=a^n\cdot a$

当〈S, $\cdot$〉是含幺半群，e 为幺元时，可以把上述归纳基础改为①$a^0=e$。可以证明 a^n 满足下面的代数性质。

定理 15.1 设〈S, $\cdot$〉是半群，$a\in S$，m 和 n 是正整数，则

①$a^m\cdot a^n=a^{m+n}$

②$(a^m)^n=a^{mn}$

当〈S, $\cdot$〉是含幺半群时，上述结论对任意非负整数 m 和 n 都成立。

【证明】 设 m 是一个固定的正整数，再对 n 进行归纳。

对于①，当 $n=1$ 时，根据递归定义中的递归语句②知结论成立。现在假设等式对 $n=k$ 时是成立的，那么

$$\begin{aligned} a^m\cdot a^{k+1} &= a^m\cdot(a^k\cdot a) && \text{（由 } a^{k+1} \text{ 定义）}\\ &= (a^m\cdot a^k)\cdot a && \text{（可结合性）}\\ &= (a^{m+k})\cdot a && \text{（归纳假设）}\\ &= a^{m+(k+1)} \end{aligned}$$

根据数学归纳法原理，①式对任何正整数 n 都成立。

对于②式，可以类似地归纳证明，其证明留作读者练习。此外，当〈S, $\cdot$〉是含幺半群时，只需把上述证明中的归纳基础换成 $n=0$ 的情形，这是容易做到的。■

注意，当运算为加法“+”时，定理 15.1 的两个式子可以写成

①$ma+na=(m+n)a$

②$n(ma)=(mn)a$

的形式。自然地，对应的递归定义式也要作相应的变动。

定理 15.2　设〈S, $\cdot$〉是一个半群，如果 S 是有限集，则必有 $a\in S$ 使得 $a^2=a$。

【证明】 因为〈S, $\cdot$〉是半群，并且 S 是有限集，任取 $b\in S$，则元素 b^1，b^2，b^3，…中必有重复的，设 b^i，$=b^j$，其中 $j>i$，由

$$b^j=b^{j-i}\cdot b^i$$

则对任何 $t\geqslant i$，都得到

$$b^t=b^{j-i}\cdot b^t$$

利用上式反复迭代，则对任何正整数 $k\geqslant 1$

$$b^t=b^{k(j-i)}\cdot b^t \quad (t\geqslant i)$$

特别地，取 k 使得 $k(j-i)\geqslant i$，同时令 $t=k(j-i)$，则得到幂等元。 ■

注意，若 S 不是有限集，则不一定有幂等元。例如，正整数集关于加法运算是一个半群，但是不存在幂等元。含幺半群至少含有一个幂等元，那就是幺元。一个半群甚至含幺半群也可以含有多个幂等元。不难验证〈2^S, $\cap$〉是以 S 为幺元的含幺半群。由于集合交运算是幂等的，所以 2^S 中每个元都是幂等元。

定义 15.1　设〈S, $\cdot$〉是一个半群，非空集合 $A\subseteq S$，并且〈A, $\cdot$〉也是半群，则称〈A, $\cdot$〉是〈S, $\cdot$〉的**子半群**。

【例 15.6】 已知〈$\mathbf{Z}$, $+$〉是半群，设 $\mathbf{E}=\{x\mid x\in\mathbf{Z}\wedge(\exists y)[y\in\mathbf{Z}\wedge x=2y]\}$，$\mathbf{O}=\mathbf{Z}-\mathbf{E}$，换言之，$\mathbf{E}$ 是偶数集，$\mathbf{O}$ 是奇数集，那么〈$\mathbf{E}$, $+$〉是半群，因而〈$\mathbf{E}$, $+$〉是〈$\mathbf{Z}$, $+$〉的子半群；但是〈$\mathbf{O}$, $+$〉不是半群，因为不满足封闭性，所以〈$\mathbf{O}$, $+$〉不是〈$\mathbf{Z}$, $+$〉的子半群。 ■

在证明〈A, $\cdot$〉是半群〈S, $\cdot$〉的子半群时，只需证明 $A\subseteq S$ 并且运算“$\cdot$”在集合 A 内是封闭的，运算的可结合性是可以继承的。也就是说，只要〈A, $\cdot$〉是半群〈S, $\cdot$〉的子代数，就必是〈S, $\cdot$〉的子半群。

【例 15.7】 设〈S, $\cdot$〉是含幺半群，A 是 S 中全体对“$\cdot$”可换的元素构成的集合，即

$$A=\{x\mid x\in S\wedge(\forall y\in S)[x\cdot y=y\cdot x]\}$$

证明〈A, $\cdot$〉是〈S, $\cdot$〉的含幺子半群。

【证明】 因为 $e\in A$，所以 $A\neq\varnothing$。

对任何 a，$b\in A$，必然 $a\cdot b\in A$。这是因为对任何 $y\in A$，由运算的可结合性及 A 的定义，有

$$(a\cdot b)\cdot y=a\cdot(b\cdot y)=a\cdot(y\cdot b)=y\cdot(a\cdot b)$$

即 $a\cdot b\in A$。这说明运算在 A 内是封闭的，〈A, $\cdot$〉是〈S, $\cdot$〉的子代数，因此是子半群。 ■

15.2　群和子群

在 14.2 节中已经为群下了定义，把群看成是在含幺半群的基础上加上每元有逆元的条件，其核心内容可用“闭、结、幺、逆”四个字予以概括。下面是一些典型的群的例子。

【例 15.8】 已经知道〈$\mathbf{Z}$, $+$〉是含幺半群，由于每个整数 a 都有加法逆元 $-a$，所以〈$\mathbf{Z}$, $+$〉是群，一般叫做**整数加群**。

同理，〈$\mathbf{R}$, $+$〉是**实数加群**，〈$\mathbf{Q}$, $+$〉是**有理数加群**。对于数的乘法，〈$\mathbf{Z}$, $\times$〉是含幺半群而不是群，因为整数一般无 $\mathbf{Z}$ 中的乘法逆元。〈$\mathbf{R}-\{0\}$, $\times$〉是**实数乘群**，它的幺元

是1，每元 $a\in\mathbf{R}-\{0\}$ 的乘法逆元为 $1/a$。 ■

【例 15.9】 设 $\mathbf{Z}_k$ 表示整数集 $\mathbf{Z}$ 上的模 k 剩余类集合，即

$$\mathbf{Z}_k=\{[0],[1],[2],\cdots[k-1]\}$$

在 $\mathbf{Z}_k$ 上定义运算⊕和⊗如下：

$$[i]\oplus[j]=[t]\Leftrightarrow(i+j)\equiv t(\mathrm{mod}\ k)$$
$$[i]\otimes[j]=[t]\Leftrightarrow ij\equiv t(\mathrm{mod}\ k)$$

那么，$\langle\mathbf{Z}_k,\oplus\rangle$ 是群。这是因为封闭性和可结合性是明显成立的，$[0]$ 是幺元，每元 $[i]$ 的⊕逆元是 $[k-i]$。群 $\langle\mathbf{Z}_k,\oplus\rangle$ 习惯上又称为**剩余类加群**。

至于 $\langle\mathbf{Z}_k,\otimes\rangle$，它满足封闭性和可结合性，有幺元 $[1]$，所以是含幺半群。然而，由于 $[0]$ 无⊗逆元，所以 $\langle\mathbf{Z}_k,\otimes\rangle$ 不是群。

那么，$\langle\mathbf{Z}_k-\{[0]\},\otimes\rangle$ 是否群？答案是不一定。例如，对于

$$\mathbf{Z}_4-\{[0]\}=\{[1],[2],[3]\},[2]\otimes[2]=[0]\notin\mathbf{Z}_4-\{[0]\}$$

所以 $\langle\mathbf{Z}_4-\{[0]\},\otimes\rangle$ 不是群。但是，对于

$$\mathbf{Z}_5-\{[0]\}=\{[1],[2],[3],[4]\}$$

运算表如表 15-1 所示。

表 15-1

⊗	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

可见运算是封闭的、可结合的，$[1]$ 是幺元，每个元皆有逆元（$[1]$ 和 $[4]$ 的逆元是自身，$[2]$ 和 $[3]$ 互为逆元），因而 $\langle\mathbf{Z}_5-\{[0]\},\otimes\rangle$ 是群。

可以证明，当 k 是素数时，$\langle\mathbf{Z}_k-\{[0]\},\otimes\rangle$ 一定是群。首先，运算是封闭的，因为不存在元素 x，$y\in\mathbf{Z}_k-\{[0]\}$ 使 $x\otimes y$ 为素数 k 的整数倍。可结合性来自于数的乘法的可结合性，幺元是 $[1]$。至于元素 $[i]$ 的逆元，由于 i 和 k 互素，所以，存在整数 x 和 y 使 $ix+ky=1$，由此可得 $ix\equiv1(\mathrm{mod}\ k)$，因此 $[i]$ 的逆元是 $[x]$。 ■

【例 15.10】 设 n 个元素的集合 A 上的全体置换构成集合 S_n。由第6章中关于置换的讨论，S_n 中两个置换的复合仍然是 A 上的一个置换，因而运算是封闭的；其次，由于函数的复合是可结合的，因而置换的复合也是可结合的；在 S_n 中存在幺置换 $\pi=(1)$，使对任何 S_n 中的置换 σ 均有 $\pi\circ\sigma=\sigma\circ\pi=\sigma$，因而 $\pi=(1)$ 是幺元；把每个元素的 x 变成 y 的置换，其逆置换则把元素 y 变成 x，因而每个置换都有逆。由此可知 $\langle S_n,\circ\rangle$，构成群，这个群一般称为 ***n* 次对称群**，是一类重要的群。 ■

群尽管是用“闭、结、幺、逆”四个条件来定义的，但是它还可以用别的形式等价地定义。

定理 15.3 *如果 $\langle G,\cdot\rangle$ 是半群，并且对任意 a，$b\in G$，都存在 x，$y\in G$ 使*

$$x\cdot a=b,a\cdot y=b$$

则 $\langle G,\cdot\rangle$ 是群。

【证明】 设 $a\in G$，方程 $x\cdot a=a$ 的解为 e_1，那么对任何 $t\in G$，必有 $e_1\cdot t=t$。这是因为方程 $a\cdot y=t$ 有解 y_0，于是

$$e_1\cdot t=e_1\cdot(a\cdot y_0)=(e_1\cdot a)\cdot y_0=a\cdot y_0=t$$

这说明 e_1 是 G 中的左幺元（见习题十四第6题）。同样，可以证明 G 中有右幺元 e_2，因而 G 中有幺元 $e(=e_1=e_2)$。

同理，对任何 $b\in G$，方程 $x\cdot b=e$ 有解 x_0，这个 x_0 是 b 的左逆元。同时，由方程 $b\cdot y=e$ 容易得到解 y_0 是 b 的右逆元，从而 b 有逆元 $x_0(=y_0)$。

根据已知条件和上面的证明，$\langle G,\cdot\rangle$ 是群。 ■

这个定理说明，在群的定义中幺元及逆元的条件可用方程有解来代替。另外，群定义中的幺元条件可以用存在左幺元（或右幺元）的条件代替，逆元的条件可以用左逆元（或右逆元）代替。

定理 15.4　*在群* $\langle G,\cdot\rangle$ *中消去律成立，即如果* $a\cdot b=a\cdot c$，*则必有* $b=c$。

【证明】　群中每元都有逆元，在等式 $a\cdot b=a\cdot c$ 两端同时与 a^{-1} 左运算

$$a^{-1}\cdot a\cdot b=a^{-1}\cdot a\cdot c$$

由此得到 $b=c$。 ■

推论 15.4.1　*群* $\langle G,\cdot\rangle$ *的运算表中每行和每列都没有重复元素。*

【证明】　由群的运算表构造法则，如果元素 a 对应行上有两个元素相同，如设 $a\cdot x=a\cdot y$，由消去律可得 $x=y$，这说明每行中没有重复元素。同理，运算表中每列也没有重复元素。 ■

由一个已知的群可以构造出一个新的群。

定理 15.5　*设* $\langle G,\cdot\rangle$ *是群，* $a\in G$，*构造映射* $\varphi_a: G\to G$，*使得对任意* $x\in G$，$\varphi_a(x)=a\cdot x$，*令* $H=\{\varphi_a\mid a\in G\}$，*则对于函数的复合运算“∘”，*$\langle H,\circ\rangle$ *是群。*

【证明】　留作读者练习。 ■

定义 15.2　*设* $\langle G,\cdot\rangle$ *是群，* S *是* G *的非空子集。如果* $\langle S,\cdot\rangle$ *也是群，则称* S *是* G *的* **子群**。

例如，$\langle\mathbf{Z},+\rangle$ 是 $\langle\mathbf{Q},+\rangle$ 的子群，$\langle\mathbf{Q},+\rangle$ 是 $\langle\mathbf{R},+\rangle$ 的子群，$\langle\{[1],[2],[3],[4]\},\otimes\rangle$ 是剩余类乘群 $\langle\mathbf{Z}_7,-\{[1]\},\otimes\rangle$ 的子群。

每个群含有两个自然的子群：一个是群自身，另一个是幺元子群 $\langle\{e\},\cdot\rangle$。此外，还有由群中一个元素生成的子群。为此，需要把群中元素的幂扩充到负指数的情形，即定义 $a^{-k}=(a^k)^{-1}$。

定理 15.6　*设* $\langle G,\cdot\rangle$ *是群，* $a\in G$，*记* $S=\{a^n\mid n\in\mathbf{Z}\}$，*则* $\langle S,\cdot\rangle$ *是* $\langle G,\cdot\rangle$ *的子群。*

【证明】　设 a^{n_1}，$a^{n_2}\in S$，则 $a^{n_1}\cdot a^{n_2}=a^{n_1+n_2}\in S\subseteq G$，所以运算关于“·”是封闭的；由于 S 是 G 的子集，因而结合律在 $\langle S,\cdot\rangle$ 中自然成立；由于 $e=a^0\in S$，所以 S 中有幺元；最后，$a^n\in S$ 有逆元 $a^{-n}\in S$ 使 $a^n\cdot a^{-n}=e$。

综上所述，$\langle S,\cdot\rangle$ 是 $\langle G,\cdot\rangle$ 的子群。 ■

特别把由群的一个元素 a 生成的子群记为 (a)。例如在 $\langle\mathbf{Z},+\rangle$ 中，由元素 2 生成的子群 (2) 是由全体偶数关于加法构成的群，而由元素 1 生成的子群正好是 $\mathbf{Z}$ 本身。

定理 15.7　*子群的幺元与群的幺元相同。*

【证明】　设群 $\langle G,\cdot\rangle$ 的幺元为 e，G 的子群 $\langle S,\cdot\rangle$ 的幺元为 e'，$x\in S$，那么 $e\cdot x=x=e'\cdot x$，利用群的消去律即得到 $e=e'$。 ■

现在再介绍一个判别子群的方法。

定理 15.8　*设* $\langle G,\cdot\rangle$ *是群，* S *是* G *的非空子集。*$\langle S,\cdot\rangle$ *是* $\langle G,\cdot\rangle$ *的子群当且仅当对任何* a，$b\in S$，$a\cdot b^{-1}\in S$。

【证明】　当 $\langle S,\cdot\rangle$ 是 $\langle G,\cdot\rangle$ 的子群时，由群的条件，对任何 a，$b\in S$，$a\cdot b^{-1}\in S$。

现在设对任何 a，$b\in S$，$a\cdot b^{-1}\in S$。那么，当 $a=b$ 时，$e\in S$，即幺元在 S 中；其次，如果令 $a=e$，那么 $b\in S$ 时必然 $b^{-1}\in S$，即 S 中每元都有逆；结合律继承于群 G；至于封闭性，当 a，$b\in S$ 时，由于 $b^{-1}\in S$，所以 $a\cdot b=a\cdot(b^{-1})^{-1}\in S$。由闭、结、幺、逆四条 $\langle S,\cdot\rangle$ 是群，因而是 G 的子群。 ■

【例 15.11】　设 $\langle G,\cdot\rangle$ 是群，定义 $H=\{h\mid h\in G\wedge(\forall x)[x\in G\to x\cdot h=h\cdot x]\}$，即

H 是由 G 中可以和每个元交换的运算的元素构成的集合。证明 $\langle H,\cdot\rangle$ 是 G 的一个子群。

【证明】 首先，幺元 $e\in H$，所以 $H\neq\varnothing$。再设 a，b 是 H 中任何两个元素，对每个 $x\in G$，若有 $b\cdot x=x\cdot b$，必有 $b^{-1}\cdot x=x\cdot b^{-1}$，从而

$$(a\cdot b^{-1})\cdot x=a\cdot x\cdot b^{-1}=x\cdot(a\cdot b^{-1})$$

即 $a\cdot b^{-1}\in H$。根据定理 15.8，H 是 G 的一个子群。 ■

利用定理 15.8 判别一个集合是否子群显得更方便，然而毕竟要考虑元素的逆。可以证明，当 G 是有限群时，判别子集 S 是否是 G 的子群，可以只判别在 S 中是否封闭就行了。也就是说，如果对任何 a，$b\in S$ 都能证明 $a\cdot b\in S$，则 S 就是 G 的子群。

15.3 交换群和循环群

本节主要介绍群的重要子类——循环群，以及群的生成元和元素周期的概念。

定义 15.3 *如果群 $\langle G,\cdot\rangle$ 的运算满足交换律，则称群 G 为* **交换群**（或 **Abel 群**）。

【例 15.12】 整数加群 $\langle\mathbf{Z},+\rangle$，剩余类乘群 $\langle\mathbf{Z}_{17}-\{[0]\},\otimes\rangle$，实数乘群 $\langle\mathbf{R}-\{0\},\times\rangle$ 等都是交换群；而 n 阶非奇异矩阵成群 $\langle M_n,\cdot\rangle$，n 阶置换群 $\langle S_n,\circ\rangle$ 等不是交换群。 ■

“可换性”是代数运算的一个重要性质。习惯上都把数的加法运算作为可换性的代表，因而交换群又常被称为**加群**。

定理 15.9 *群 $\langle G,\cdot\rangle$ 为交换群的充要条件是：对任意 a，$b\in G$，$(a\cdot b)^2=a^2\cdot b^2$。*

【证明】 如果 G 是交换群，则 $a\cdot b=b\cdot a$，故

$$(a\cdot b)^2=(a\cdot b)\cdot(b\cdot a)=a\cdot(b\cdot a)\cdot b=a\cdot(a\cdot b)\cdot b=a^2\cdot b^2$$

反之，如果 $(a\cdot b)^2=a^2\cdot b^2$，即

$$a\cdot(b\cdot a)\cdot b=a\cdot(a\cdot b)\cdot b$$

由群的消去律可得 $b\cdot a=a\cdot b$，可知 G 是交换群。 ■

在交换群中，循环群占有特殊的地位。

定义 15.4 *如果群 $\langle G,\cdot\rangle$ 中存在一个元 a，使得 G 能由 a 生成，即 $G=(a)$，则称 G 为* **循环群**，*称 a 是 G 的一个* **生成元**。

【例 15.13】 由 n 次代数方程 $x^n-1=0$ 的全部复根构成的集合 Root 在复数乘法运算下构成群。此时，

$$\text{Root}=\left\{\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\,\middle|\,k=0,1,2,\cdots,n-1\right\}$$

如果记

$$a=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

那么 $\text{Root}=\{1,a,a^2,\cdots,a^{n-1}\}$。显然，群 $\langle\text{Root},\times\rangle$ 可以由元 a 生成，因此是循环群。 ■

【例 15.14】 剩余类加群 $\langle\mathbf{Z}_k,\oplus\rangle$ 是循环群。元素 $[a]$ 只要满足 $\gcd(a,k)=1$，就可以成为生成元。此时，对任何 $[b]\in\mathbf{Z}_k$，由于 $\gcd(ab,kb)=b$，所以 $[b]=[a]\oplus[a]\oplus\cdots\oplus[a]$。

同样，当 k 是素数时，剩余类乘群 $\langle\mathbf{Z}_k-\{[0]\},\oplus\rangle$ 也是循环群。这时，除幺元外的每个元素 $[a]$ 都满足 $\gcd(a,k)=1$，因而每个非幺元素都是群的生成元。对于 $[b]\in\mathbf{Z}_k-\{[0]\}$，可以由 $[a]$ 的幂生成。 ■

【例 15.15】 整数加群 $\langle\mathbf{Z},+\rangle$ 是一个无限的循环群。很明显，整数 1 是生成元，同样，整数 -1 也是生成元。容易看出，除 1 和 -1 外，$\langle\mathbf{Z},+\rangle$ 别无其他的生成元。 ■

从上面三个例子看出，元素 a 生成的循环群（或循环子群）$(a)=\{a^n\mid n\in\mathbf{Z}\}$，可以有两种不同的情况：

1）存在整数 i，j $(i\neq j)$，使得 $a^i=a^j$。如例 15.13 和例 15.14 分别有 $i[a]=(i+k)[a]$ 和 $[a]^i=[a]^{i+k}$。

2）对任何整数 i，j $(i\neq j)$，$a^i=a^j$。如例 15.15 中由 1 生成的元素互不相同，由 -1 生成的元素也互不相同。

在这两种情况中，第一种尤其值得注意，它表明有无限多个整数 n，使得 $a^n=e$。由此，引出元素周期的概念。

定义 15.5　设 $\langle G,\cdot\rangle$ 是群，$a\in G$，称使得 $a^n=e$ 的最小正整数 n 为元素 a 的**周期**。如果不存在这种最小正整数，则称 a 的周期为 ∞。

【例 15.16】　在剩余类加群 $\langle \mathbf{Z}_6,\oplus\rangle$ 中，元素 $[1]$，$[5]$ 的周期都是 6。可以验证

$$[5]\oplus[5]=[4]$$
$$[5]\oplus[5]\oplus[5]=[3]$$
$$[5]\oplus[5]\oplus[5]\oplus[5]=[2]$$
$$[5]\oplus[5]\oplus[5]\oplus[5]\oplus[5]=[1]$$
$$[5]\oplus[5]\oplus[5]\oplus[5]\oplus[5]\oplus[5]=[0]$$

但是，元素 $[3]$ 的周期为 2，因为 $[3]\oplus[3]=[0]$。由 $[3]$ 生成的元素只有 $[0]$ 和 $[3]$。 ■

定理 15.10　设群 $\langle G,\cdot\rangle$ 中元素 a 的周期为正整数 n，则

①$a^m=e$，当且仅当 $n\mid m$。

②$a^i=a^j$，当且仅当 $n\mid(i-j)$。

③由 a 生成的子群恰有 n 个元素，即 $(a)=\{e,a,a^2,\cdots,a^{n-1}\}$。

【证明】　①整数 m 可以唯一地表示成

$$m=nq+r,0\leqslant r<n$$

的形式。$a^m=a^{nq+r}=(a^n)^q\cdot a^r=a^r$，于是 $a^m=e$ 当且仅当 $a^r=e$。由于 $0\leqslant r<n$ 及周期的最小性，必然 $r=0$，所以 $n\mid m$。

②由群的消去律，$a^i=a^j$，当且仅当 $a^{i-j}=e$，再由①的结论知道 $n\mid(i-j)$。

③由②的结论，e，a，a^2，$\cdots$，a^{n-1} 中没有两个是相同的；此外，由①得证明过程知道，对任何使 $a^m=e$ 的 m，都存在 $0\leqslant r<n$ 使 $a^m=a^r\in\{e,a,a^2,\cdots,a^{n-1}\}$，因而

$$(a)=\{e,a,a^2,\cdots,a^{n-1}\}$$ ■

一般把群中元素数目称为群的阶。容易证明，有限群中的每个元素的周期都是有限数，而无限阶群中的元素周期可以是有限的，也可以是无限的。元素的周期与群的阶之间有着密切的关系，这是下一节导出的重要结论。

15.4　陪集与拉格朗日定理

现在，考虑群的另一重要特性：由群的子群来构造群的分划，从而导出群论中著名的拉格朗日定理。

定义 15.6　设 $\langle H,\cdot\rangle$ 是群 $\langle G,\cdot\rangle$ 的一个子群，$a\in G$，记 $aH=\{a\cdot h\mid h\in H\}$，称 aH 是 H 在 G 中关于元 a 的**左陪集**。同样，称 $Ha=\{h\cdot a\mid h\in H\}$ 为 H 在 G 中关于元 a 的**右陪集**。由左（右）陪集构成的集合的基数称为**子群的指数**。

【例 15.17】　三次对称群 $\langle S_3,\circ\rangle$ 的一个子群为 $H=\{(1),(1\ \ 2)\}$，由此可得到左陪集

$$(1)H=(1\ \ 2)H=H$$
$$(1\ \ 3)H=(1\ \ 2\ \ 3)H=\{(1\ \ 3),(1\ \ 2\ \ 3)\}$$
$$(2\ \ 3)H=(1\ \ 3\ \ 2)H=\{(2\ \ 3),(1\ \ 3\ \ 2)\}$$

同样，可以得到右陪集为

$$H(1)=H(1\ \ 2)=\{(1),(1\ \ 2)\}$$
$$H(1\ \ 3)=H(1\ \ 3\ \ 2)=\{(1\ \ 3),(1\ \ 3\ \ 2)\}$$
$$H(2\ \ 3)=H(1\ \ 2\ \ 3)=\{(2\ \ 3),(1\ \ 2\ \ 3)\}$$ ■

从这个例子可以看出以下事实：

1）H 关于同一元素的左陪集和右陪集可能不相同，如 $(1\ \ 3)H\neq H(1\ \ 3)$。

2）凡是同属某个左（右）陪集的元素，它们对应的左（右）陪集相同。

3）任何两个左（右）陪集要么相同，要么无公共元素。

4）所有左（右）陪集的元素数目相同。

由这些事实可以建立群中元素间的等价二元关系。

由于左陪集和右陪集在概念上是对应的，因此只需讨论其中一种就行了。

定理 15.11 *设 H 是群 G 的子群，a，$b\in G$。在 G 中建立二元关系如下*

$$aRb\Leftrightarrow b\in aH$$

则 R 是 G 上的一个等价关系。

【证明】 由于 $e\in H$，$a\in aH$，即 aRa，说明 R 是自反的。

如果 aRb，则 $b\in aH$，即存在 $h\in H$ 使 $b=a\cdot h$，或 $a=b\cdot h^{-1}\in bH$，说明 R 是对称的。

最后，设 aRb 且 bRc，根据定义必存在 h_1，$h_2\in H$ 使 $b=ah_1$，且 $c=bh_2$，于是 $c=bh_2=ah_1h_2\in aH$，说明 aRc 成立。

综合上述，R 是 G 上的一个等价关系。 ■

实际上，这里定义的等价关系 R 是以同一个左陪集为判断标准。等价关系 R 可以确定群 G 的一个分划，每个左陪集就是分划中的一个块（等价类），因而 G 可以表示为

$$G=H\cup a_1H\cup a_2H\cup\cdots \tag{15-1}$$

称为 G 的左陪集分解式。同样，也可以得到 G 的右陪集分解式

$$G=H\cup Ha_1\cup Ha_2\cup\cdots \tag{15-2}$$

为了导出本节的主要结果，先证明一个明显的结论。

定理 15.12 *群 G 中子群 H 的所有左（右）陪集都是等势的。*

【证明】 只需证明对任何 $a\in H$ 都有 $aH\sim H$ 就行了。为此，定义映射 f：$H\to aH$ 如下：对任何 $h\in H$，$f(h)=ah$。首先，f 是单射，因为：如果 $ah_1=ah_2$，由群中消去律可得到 $h_1=h_2$；其次，f 是满射，因为对任何 $ah\in aH$ 都有 $h\in H$ 使 $f(h)=ah$。这说明 f 是双射，定理结论成立。 ■

如果子群 H 是有限集，我们知道，H 的所有左陪集的元素数目都是相同的。

定理 15.13 拉格朗日定理 *n 阶群 $\langle G,\cdot\rangle$ 的任何子群 $\langle H,\cdot\rangle$ 的阶必是 n 的因子。*

【证明】 由 G 的左陪集分解式（15.1）可以得到

$$|G|=|H|+|aH|+|a_2H|+\cdots+|a_kH|=(k+1)|H|$$

这表明 $|H|$ 是 $|G|$ 的因子。 ■

推论 15.13.1 *n 元群 G 中任何元素的周期必是 n 的因子。*

【证明】 设 $a\in G$，则 $(a)=\{e,a,a^2,\cdots,a^{n-1}\}$ 是 G 的一个子群，故 $m|n$，而 m 是元素 a 的周期，所以每个元素的周期必是 n 的因子。 ■

拉格朗日定理从元素数目的角度给出了群的子集成为子群的必要条件，但它不是充分条件，也就是说，当 m 是 n 的因子时，n 阶群不一定有 m 阶子群。例如，尽管 8 次对称群是

24 的因子，4 次对称群 $\langle S_4, \circ \rangle$ 中却不存在 8 阶子群。

15.5　正规子群与商群

前面已指出，子群 H 关于元素 a 的左、右陪集一般是不同的，即 $aH \neq Ha$。但是，却也存在子群，它关于任何元素的左陪集和右陪集都是相同的，这类子群是重要的一类子群。

定义 15.7　设 $\langle H, \cdot \rangle$ 是群 $\langle G, \cdot \rangle$ 的一个子群。如果对于任何 $a \in G$，$aH = Ha$，则称 H 是 G 的**正规子群**（或**不变子群**）。

【例 15.18】　在对称群 $\langle S_3, \circ \rangle$ 中，子群 $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ 是 S_3 的一个正规子群。它有两个左陪集 $(1)H$ 和 $(1\ 2)H = \{(1\ 2), (1\ 3), (2\ 3)\}$。容易验证，这两个左陪集又是右陪集，即有 $(1)H = H(1)$，$(1\ 2)H = H(1\ 2)$。

但是，子群 $G = \{(1), (1\ 2)\}$ 不是正规子群。因为 $(1\ 3)G = \{(1\ 3), (1\ 2\ 3)\}$，而 $G(1\ 3) = \{(13), (132)\}$，所以，$(1\ 3)G \neq G(1\ 3)$，即 G 不是 S_3 的正规子群。 ■

在群中，仅由幺元构成的子群以及群自身都是群的正规子群，它们是平凡的正规子群。我们主要关心群是否存在非平凡正规子群。根据拉格朗日定理，素数阶的群没有非平凡正规子群。

很显然，交换群的所有的子群都是正规子群，因为这时对任何 $h \in H$ 都有 $a \cdot h = h \cdot a$，因此 $aH = Ha$。但是对于非交换群而言，正规子群的条件 $aH = Ha$ 并不意味着对任何 $h \in H$ 都满足 $a \cdot h = h \cdot a$，而只是说明运算结果仍在同一集合中。

在证明 H 是 G 的正规子群时，不必实际构造 aH 和 Ha 后再比较它们的元素，可以利用下面的定理来证明 H 满足定义条件。

定理 15.14　设 H 是群 G 的正规子群，则 H 是正规子群，当且仅当对任何 $a \in G$，$aHa^{-1} \subseteq H$。

【证明】　如果 H 是 G 的正规子群，根据定义 $aH = Ha$，即对任何 $h_1 \in H$，必有 $h_2 \in H$ 使 $ah_1 = h_2 a$，或 $ah_1 a^{-1} = h_2$，这就证明了 $aHa^{-1} \subseteq H$。

反之，如果对任何 $a \in G$，$aHa^{-1} \subseteq H$，即对任何 $h_1 \in H$，必有 $h_2 \in H$ 使 $ah_1 a^{-1} = h_2$，由此可得 $ah_1 = h_2 a$。根据 h_1 和 h_2 的任意性，可以得到 $aH = Ha$。于是，H 为 G 的正规子群。 ■

这个定理说明，只要证明对每个 $a \in G$ 和任何 $h \in H$，$aha^{-1} \in H$，就可以证明 H 是 G 的正规子群。

【例 15.19】　证明：群 $\langle G, \cdot \rangle$ 中每个元素都可交换运算的元素全体构成的集合 H，是 G 的正规子群。

【证明】　在例 15.11 中已经证明 $\langle H, \cdot \rangle$ 是 G 的子群。现设 a 是 G 的任何一个元素，根据 H 中元素的定义方式，对任何 $h \in H$，都能得到

$$a \cdot h \cdot a^{-1} = a \cdot a^{-1} \cdot h = h \in H$$

由定理 15.14 知道，H 是 G 的正规子群。 ■

还可以看出，交换群的任何子群都是正规子群。

设 H 为 G 的正规子群，则 H 的任一左陪集 aH 也是 H 的右陪集 Ha，于是不必区分 H 的左陪集与 H 的右陪集，而把 H 的任一左陪集（也是右陪集）称为 H 的陪集。令 G/H 表示 H 的所有陪集所组成的集合，即 $G/H = \{aH \mid a \in G\}$。

下面来定义 G/H 的乘积“$\cdot$”运算，并证明 $\langle G/H, \cdot \rangle$ 是群。

设 $aH, bH \in G/H$，令

$$aH \cdot bH = \{ah_1 \cdot bh_2 \mid h_1, h_2 \in G/H\}$$

因为对任意的 $h_1, h_2 \in H$，有

$$ah_1 \cdot bh_2 \in aH \cdot bH = a(Hb)H = a \cdot bH \cdot H = abH$$

所以，$aH \cdot bH \subset abH$。

又因为 $abH = ae \cdot bH \subset aH \cdot bH$，所以，$aH \cdot bH = abH$。

这说明，陪集 aH 与 bH 的乘积是陪集 abH。所以，陪集的乘积为 G/H 的代数运算，即 $\langle G/H, \cdot \rangle$ 是代数系统。并且对 $\forall a, b, c \in G$，有

$$(ah \cdot bH) \cdot cH = abH \cdot cH = (ab)cH = a(bc)H = aH \cdot bcH = aH \cdot (bH \cdot cH)$$

即运算满足结合律。

对 $\forall a \in G$，有

$$H \cdot aH = eH \cdot aH = eaH = aH$$

$$aH \cdot H = aH \cdot eH = (ae)H = aH$$

所以，$H \cdot aH = aH \cdot H$，这说明幺元的陪集（即正规子群 H）是 $\langle G/H, \cdot \rangle$ 的幺元。

对 $\forall a \in G$，有

$$a^{-1}H \cdot aH = eH = H = aH \cdot a^{-1}H$$

所以，$a^{-1}H$ 是 aH 的逆元，即 $(aH)^{-1} = a^{-1}H$。

根据群的定义，我们证明了 $\langle G/H, \cdot \rangle$ 是群。这个群为 $\langle G, * \rangle$ 的商群。

定义 15.8 设 $\langle H, * \rangle$ 是 $\langle G, * \rangle$ 的一个正规子群，G/H 表示 G 的所有陪集的集合，则 $\langle G/H, \cdot \rangle$ 是一个群，称为**商群**。其中“$\cdot$”定义为

$$\forall aH, bH \in G/H, aH \cdot bH = (a * b)H$$

如果 G 是有限群，则根据拉格朗日定理，商群 $\langle G/H, \cdot \rangle$ 的阶等于群 G 的阶除以 H 的阶。

还可以证明，交换群的任一子群都是交换群，且其商群也是交换群；循环群的任一商群也都是循环群。

【例 15.20】 设 $G = S_3$，$H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$，则 H 是 G 的子群，且 $G/H = \{H, (1\ 2)H\}$，是一个循环群，其生成元是 $(1\ 2)H$。 ■

15.6 群的同态与同构

在考虑问题时，对于设定的考察原则常常需要注意对象间的共性，以便忽略非实质的差别，把握事物的本质。例如，从基数的角度看，凡是等势的集合都是同一类集合，而不管它们究竟有些什么元素。从代数系统的观点来看，习题十五第 8 题定义的由函数构成的群与 3 次对称群 $\langle S_3, \circ \rangle$ 在运算规律上完全一致。诸如此类的事例说明，只要在对象物间能建立某种联系，就可以通过去粗取精、由表及里的过程把它们纳入统一的处理范围中。

定义 15.9 设 $\langle S, \cdot \rangle$ 和 $\langle T, \circ \rangle$ 是两个代数系数，其中“$\cdot$”和“$\circ$”分别是 S 和 T 的二元运算。如果存在映射 $f: S \to T$ 使得对任意 $a_1, a_2 \in S$

$$f(a_1 \cdot a_2) = f(a_1) \circ f(a_2)$$

则称 f 是 S 到 T 的**同态映射**，或者 S 和 T（在影射 f 下）**同态**，记为 $S \sim T$；称 $f(S) \subseteq T$ 为 S 的**同态像**。

当 f 是满射时，称 f 为**满同态**；当 f 是双射时，称 f 为**同构映射**。代数系统 S 和 T（在 f 下）同构记为 $S \cong T$。

当 $S = T$ 时，上述同态和同构，分别叫做**自同态**和**自同构**。

【例 15.21】 在自然数加半群 $\langle \mathbf{N}, + \rangle$ 和乘余类加群 $\langle \mathbf{Z}_2, \oplus \rangle$ 之间可定义映射 $f: \mathbf{N} \to \mathbf{Z}_2$ 如下

$$f(n) = \begin{cases} [0] & \text{当 } n \text{ 是偶数} \\ [1] & \text{当 } n \text{ 是奇数} \end{cases}$$

容易验证 f 是 $\mathbf{N}$ 到 $\mathbf{Z}_2$ 的满同态映射。事实上，对任意 n_1，$n_2\in\mathbf{N}$，当 n_1 和 n_2 同奇偶时，$f(n_1+n_2)=0$，而 $f(n_1)$ 和 $f(n_2)$ 要么同为 $[0]$，要么同为 $[1]$，从而 $f(n_1)\oplus f(n_2)=[0]$；当 n_1 和 n_2 不同奇偶时，$f(n_1+n_2)=[1]$，这时和 $f(n_2)$ 中一个是 $[0]$，另一个是 $[1]$，从而 $f(n_1)\oplus f(n_2)=[1]$，于是 $\mathbf{N}\sim\mathbf{Z}_2$。 ■

【例 15.22】 整数加群 $\langle\mathbf{Z},+\rangle$ 和非零复数乘群 $\langle C-\{0\},\times\rangle$ 之间存在同态关系。为此，定义映射 g：$\mathbf{Z}\to C-\{0\}$ 如下：

$$g(n)=i^n，\text{其中 } i=\sqrt{-1}$$

于是，对任何 n，$m\in\mathbf{Z}$，$g(n+m)=i^{n+m}=i^n\times i^m=g(n)\times g(m)$，即 g 是同态映射，且 $g(\mathbf{Z})=\{1,-1,i,-i\}$。 ■

【例 15.23】 记矩阵

$$\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}=z(\theta)$$

复数 $\cos\theta+i\sin\theta=e^{i\theta}$，$S=\{z(\theta)\mid\theta\in\mathbf{R}\}$，$T=\{e^{i\theta}\mid\theta\in\mathbf{R}\}$。容易证明 S 在矩阵乘法“$\cdot$”运算下成群 $\langle S,\cdot\rangle$，T 在复数乘法“$\times$”运算下也成为群 $\langle T,\times\rangle$。现在定义映射 h：$S\to T$ 使得 $h(z(\theta))=e^{i\theta}$，由于对任何 θ，$\varphi\in\mathbf{R}$，有

$$\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\cdot\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}=\begin{pmatrix}\cos(\theta+\varphi) & \sin(\theta+\varphi)\\ -\sin(\theta+\varphi) & \cos(\theta+\varphi)\end{pmatrix}$$

于是

$$h(z(\theta)\cdot z(\varphi))=h(z(\theta+\varphi))=e^{i(\theta+\varphi)}=h(z(\theta))\times h(z(\varphi))$$

这说明 h 是 S 到 T 得同态映射。

进一步，由于映射 h 实质上是实数 θ 与自身的对应，因而是双射，即 h 是 S 到 T 的同构映射。 ■

同态映射不仅确定了不同集合元素间的对应关系，而且还保持了代数系统的运算性质。

定理 15.15 *设 f 是从代数系统 $\langle S,\cdot\rangle$ 到代数系统 $\langle T,\circ\rangle$ 的同态映射，则*

①如果运算“$\cdot$”在 S 中是封闭的，那么运算“$\circ$”在 $f(S)$ 中也是封闭的。

②如果运算“$\cdot$”在 S 中可结合，那么运算“$\circ$”在 $f(S)$ 中也可结合。

③如果运算“$\cdot$”在 S 中可交换，那么运算“$\circ$”在 $f(S)$ 中也可交换。

④如果运算“$\cdot$”在 S 中有幺元，那么运算“$\circ$”在 $f(S)$ 中也有幺元。

⑤如果 S 中每元关于运算“$\cdot$”有逆元，那么 $f(S)$ 中每元关于运算“$\circ$”也有逆元。

【证明】 ①任取 a，$b\in S$，由于“$\cdot$”在 S 中封闭，因此 $a\cdot b\in S$。又因为 f 是 S 到 T 的同态映射，所以 $f(a\cdot b)\in f(S)\subseteq T$，即 $f(a)\circ f(b)$ 属于 $f(S)$。根据 a，b 的任意性知道，运算“$\circ$”在 $f(S)\subseteq T$ 中是封闭的。

②如果运算“$\cdot$”在 S 中是可结合的，则对任何 a，b，$c\in S$，$(a\cdot b)\cdot c=a\cdot(b\cdot c)$，于是 $f((a\cdot b)\cdot c)=f(a\cdot(b\cdot c))$。但是

$$f((a\cdot b)\cdot c)=f(a\cdot b)\circ f(c)=(f(a)\circ f(b))\circ f(c)$$

$$f(a\cdot(b\cdot c))=f(a)\circ(f(b)\circ f(c))$$

所以在 $f(S)$ 中运算“$\circ$”是可结合的。

③如果运算“$\cdot$”在 S 中可交换，则对任何 a，$b\in S$，$a\cdot b=b\cdot a$，于是 $f(a\cdot b)=f(b\cdot a)$。但是 $f(a\cdot b)=f(a)\circ f(b)$，$f(b\cdot a)=f(b)\circ f(a)$，即 $f(a)\circ f(b)=f(b)\circ f(a)$，所以在 $f(S)$ 中运算“$\circ$”是可交换的。

④设 e 是运算“$\cdot$”在 S 中的幺元，则对任何 $a\in S$，$e\cdot a=a=a\cdot e$，$f(a\cdot e)$，$f(e\cdot a)=$

$f(a)=f(a\cdot e)$。于是 $f(e)\circ f(a)=f(a)=f(a)\circ f(e)$，说明 $f(e)$ 是运算“$\circ$”在 $f(S)$ 中的幺元，f 把 S 的幺元映射到 $f(S)$ 的幺元。

⑤设 $a\in S$ 在 S 中关于运算“$\cdot$”有逆元 a^{-1}，那么 $a\cdot a^{-1}=e$，于是 $f(a\cdot a^{-1})=f(e)$，即 $f(a)\circ f(a^{-1})=f(e)$。这说明 $f(a)\in f(S)$ 有逆元 $f(a^{-1})$(或 $f^{-1}(a)=f(a^{-1})$)，映射 f 把 S 中元素 a 的逆元映射到 $f(S)$ 中元素 $f(a)$ 的逆元。 ■

这个定理突出地说明了同态映射把像源代数系统的运算性质一一反映到像集代数系统上，或者说同态映射是保持运算性质的映射，因此，能够建立同态映射的代数系统之间有着很大的一致性。

定理 15.16 *如果 f 是代数系统 $\langle S,\cdot\rangle$ 到 $\langle T,\circ\rangle$ 的满同态，那么*

①如果 S 是半群，则 T 也是半群。

②如果 S 是群，则 T 也是群。

【证明】 ①根据定理 15.15 的第①、②条，当运算“$\cdot$”在 S 中满足封闭、可结合性质时，运算“$\circ$”在 $T=f(S)$ 也具有封闭和可结合性质，从而是半群。如果再加上定理 15.15 第④条，则当 S 是含幺半群时，T 也是含幺半群。

②据定理 15.15 第①、②、④、⑤条，当 S 是群时，则 T 也是群。 ■

在同态映射下，像源的代数性质都为像集所具有，但是，需注意的是，像集所具有的代数性质却未必能为像源所具备。如在例 15.21 中，$\langle \mathbf{Z}_2,\oplus\rangle$ 是群，而 $\langle \mathbf{N},+\rangle$ 却不是群。

现在，从另一角度来观察同态。从前面几个例子（比如例 15.22）可以看出，同态映射 f 把所有形如 $4m+1$ 的整数映射到复数 i，把形如 $4m+2$ 的整数映射到复数 -1 等，这些数之间是互有区别、各不相干的，而同态却忽略了它们的区别，按一定模式把它们统统与另一个元素对应起来，实际是按一定法则把像源的元素进行了归类。那么，这种归类具有什么特点？它们的本质是什么？下面通过考察像源中被映射到像集幺元的那些元素具有的代数特征来揭示同态的分类特征。

定义 15.10 *设 f 使群 $\langle G,\cdot\rangle$ 到 $\langle H,\circ\rangle$ 的同态映射，e' 是 H 的幺元，记*

$$\mathrm{Ker}(f)=\{x\mid x\in G\wedge f(x)=e'\}$$

*则称 $\mathrm{Ker}(f)$ 为 f 的**同态核**。*

例如，在例 15.21 中，$[0]$ 是 $\mathbf{Z}_2$ 中的幺元，$(f)=\{0,\pm4,\pm8,\cdots\}$。在例 15.23 中，1 是 T 中的幺元，因而映射 h 的同态核是 2 阶单位矩阵。

定理 15.17 *设 f 使群 $\langle G,\cdot\rangle$ 到 $\langle H,\circ\rangle$ 的同态映射，则 f 的同态核 $\mathrm{Ker}(f)$ 是 G 的正规子群。*

【证明】 设 G 的幺元是 e，H 的幺元是 e'。对任意 x，$y\in\mathrm{Ker}(f)$，根据定义 $f(x)=f(y)=e'$，根据定理 15.15，$f(y^{-1})=f^{(-1)}(y)=e'$，因而

$$f(x\cdot y^{-1})=f(x)\circ f(y^{-1})=e'e'=e'$$

于是 $x\cdot y^{-1}\in\mathrm{Ker}(f)$。根据定理 15.8，$\mathrm{Ker}(f)$ 是 G 的一个子群。

现在，进一步证明 $\mathrm{Ker}(f)$ 是 G 的正规子群。为此，设 x 是 G 中任意元素，k 是 $\mathrm{Ker}(f)$ 中任意元素，则

$$f(x\cdot k\cdot x^{-1})=f(x)\circ e'\circ f(x^{-1})=f(x)\circ f^{-1}(x)=e'$$

于是 $x\cdot k\cdot x^{-1}\in\mathrm{Ker}(f)$。根据定理 15.14，$\mathrm{Ker}(f)$ 是 G 的正规子群。 ■

由定理 15.17 不难进一步证明，在同态映射下，像源集 G 具有陪集分解式，其中每个陪集是像集中某个元素的像源。

习题十五

1. 证明定理 15.1 中的②式。
2. 判断下述代数系统中哪些是半群：
   (1) 数集 A 上定义运算 max(求两元中较大元)。
   (2) 正实数集 $\mathbf{R}^+$ 上定义的除法运算“/”。
   (3) 正整数集 $\mathbf{Z}^+$ 上定义运算 gcd(求两正整数的最大公约数)。
3. 在实数集 $\mathbf{R}$ 上定义二元运算“$*$”如下：$\forall a, b\in\mathbf{R}$，$a*b=a+b+ab$。证明：$\langle\mathbf{R}, *\rangle$ 是含么半群。
4. 设半群 $\langle A, \cdot\rangle$ 中任何两个不同元素关于运算“$\cdot$”不可交换。证明：对任何 $a\in A$，$a\cdot a=a$。
5. 设 $S=\{00,111,1010\}$ 是字符集 $\Sigma=\{0,1\}$ 上的字集合。试构造 Σ^* 的一个包含集合 S 的最小的含么子半群。
6. 证明：群中只有么元是幂等元。
7. 证明定理 15.5。
8. 设 S 是由 0 和 1 之外的实数构成的集合。在 S 上定义 6 个映射 σ_1，σ_2，…，σ_6 如下：对每个 $x\in S$，$\sigma_1(x)=x$，$\sigma_2(x)=x^{-1}$，$\sigma_3(x)=1-x$，$\sigma_4(x)=(1-x)^{-1}$，$\sigma_5(x)=(x-1)x^{-1}$，$\sigma_6(x)=x(x-1)^{-1}$。证明：$\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ 关于函数的复合运算“$\circ$”构成群(列出运算表，并加以判别)。
9. 现在在整数集 $\mathbf{Z}$ 上用加法运算+和−定义新运算“Δ”如下：对任何 $a, b\in\mathbf{Z}$，$a\Delta b=a+b-2$。证明：$\langle\mathbf{Z},\Delta\rangle$ 是群。
10. 写出 $\langle S_3, \circ\rangle$ 的全部子群。
11. 设 $\langle S, \cdot\rangle$ 和 $\langle T, \cdot\rangle$ 都是 $\langle G, \cdot\rangle$ 的子群，令 $S\cap T=\{x\mid x\in S\wedge x\in T$，$ST=\{s.t\mid s\in S\wedge t\in T\}$。证明：$\langle S\cap T, \cdot\rangle$ 和 $\langle ST, \cdot\rangle$ 也都是 $\langle G, \cdot\rangle$ 的子群。
12. 设 $\langle G, \cdot\rangle$ 和 $\langle H, \circ\rangle$ 是两个群，现在在直积 $G\times H$ 上定义运算“Δ”如下：对任何 g_1，$g_2\in G$ 及 h_1，$h_2\in H$，$(g_1, h_1)\Delta(g_2, h_2)=(g_1\cdot g_2, h_1\circ h_2)$。证明：$\langle G\times H,\Delta\rangle$ 是群。
13. 证明：群中两个不同元素生成的子群有且仅有一个公共元素。
14. 设 S 是群 $\langle G, \cdot\rangle$ 的任一个非空集合，定义 $S^*=\{x\cdot y\mid x\in S, y\in S\}$ 为 S 的闭包。证明：$\langle S^*\cdot\rangle$ 是 $\langle G, \cdot\rangle$ 的子群(称为由 S 生成的子群)，并且是 G 中所有包含 S 的子群的交集。
15. 证明：阶数小于 6 的群必是交换群。举出一个不是交换群的 6 阶群。
16. 证明：每个阶数大于 1 的群必含有阶数大于 1 的交换子群。
17. 证明：循环群的子群必是循环群。
18. 证明：群中的每个元素和它的逆元素有相同的周期。
19. 设 n 阶群 $\langle G, \cdot\rangle$ 中每个元素的周期要么是 1，要么是 3。证明：n 必是奇数。
20. 设 $A=(a^i)$ 和 $B=(a^j)$ 是循环群 $G=(a)$ 的两个子群。试求 $A\cap B$，并证明你的结果。
21. 设 G 是以 a 为生成元的 n 阶循环群，正整数 r 和 n 的最大公约数为 d。
   (1) 求元素 a^r 的周期。
   (2) 求使 a^r 为 G 的生成元时，r 应满足的条件。
   (3) 确定 G 的生成元数目。
22. 3 次对称群 $\langle S_3, \circ\rangle$ 是 4 次对称群 $\langle S_4, \circ\rangle$ 的子群，写出 S_3 的所有左陪集。
23. 找出同余类加群 $\langle\mathbf{Z}_9, \oplus\rangle$ 的全部三阶子群及相应的陪集。
24. 设 $\langle H, \cdot\rangle$ 是群 $\langle G, \cdot\rangle$ 的子群，a，$b\in G$。求证下面六条等价：
   (1) $b^{-1}\cdot a\in H$　(2) $a^{-1}\cdot b\in H$　(3) $b\in aH$

(4) $a\in bH$　　(5) $aH=bH$　　(6) $aH\cap bH\neq\varnothing$

这些条件说明了什么？

25. 证明下述结论：

(1) 群中指数为 2 的子群是正规子群。

(2) 两个正规子群 S 和 T 的交 $S\cap T$ 仍是正规子群。

(3) 两个正规子群 S 和 T 之“积” ST（见第 11 题）也是正规子群。

26. 在所有由含一个二元运算的代数系统构成的集合上，同态是代数系统间的二元关系，这个二元关系具有什么性质？同构呢？

27. 设 f 是群 $\langle G,\cdot\rangle$ 到群 $\langle H,\circ\rangle$ 的同态映射，S 是 G 的子群。证明：$f(S)$ 是 H 的子群。

28. 设 f 是群 $\langle G,\cdot\rangle$ 到群 $\langle H,\circ\rangle$ 的同态映射，任取 x'，$y'\in f(G)$，记

$$f^{-1}(x')=\{x\mid x\in G\wedge f(x)=x'\}$$

$$f^{-1}(y')=\{y\mid y\in G\wedge f(y)=y'\}$$

证明：$f^{-1}(x')$ 与 $f^{-1}(y')$ 是等势的。

29. 设 f 是群 G_1 到群 G_2 的同态映射，g 是群 G_2 到群 G_3 的同态映射。求证：$g\circ f$ 是 G_1 到 G_3 的同态映射，并确定它的同态核。

30. 设 $\langle G,\cdot\rangle$ 是群，a 是 G 中一个固定元素。定义映射 $f:G\to G$ 使得对任何 $x\in G$，

$$f(x)=a\cdot x\cdot a^{-1}$$

求证：f 是 G 的自同构映射。

31. 证明：循环群的同态像也是循环群。

32. 证明：任意 n 元群必同构于 n 次对称群 $\langle S_n,\circ\rangle$ 的一个子群。