第 5 章 代数系统的一般性质

代数系统也是一种数学模型，可以用它表示现实世界中的离散结构。例如，在形式语言中，常将有穷字符集表示为 Σ。由 Σ 上的有限个字符（包括 0 个字符）可以构成一个字符串，称为 Σ 上的字。Σ 上的全体字符串构成集合 Σ^*。设 α、β 是 Σ^* 上的两个字，将 β 连接在 α 后面，得到 Σ^* 上的字 $\alpha\beta$。如果将这种连接看作 Σ^* 上的一种运算，那么这种运算不可交换，但是可结合。集合 Σ^* 关于连接运算就构成了一个代数系统，它恰好是代数系统（半群）的一个实例。代数系统在计算机中有着广泛的应用，例如自动机理论、编码理论、形式语义学、代数规范、密码学等，都要用到代数系统的知识。代数结构的主要研究对象就是各种典型的代数系统。

构造一个代数系统，需要 3 方面的要素：集合、集合上的运算、说明运算性质或运算之间关系的公理。请看下面的例子：

（1）整数集合$\mathbb{Z}$与普通加法＋构成代数系统$<\mathbb{Z}$；＋＞。

（2）n 阶实数矩阵的集合 $\boldsymbol{M}_n(R)$与矩阵加法＋构成代数系统$<\boldsymbol{M}_n(R)$；＋＞。

（3）幂集 $P(B)$与集合的对称差运算⊕构成代数系统$<P(B)$；⊕＞。

类似的代数系统可以列举出许多，它们都是具体的代数系统。考察它们的共性，不难发现它们都含有一个集合、一个二元运算，并且这些运算都具有交换性、结合性等性质。

为了概括这类代数系统的共性，可以定义一个抽象的代数系统$<A$，∘＞。其中，A 是一个集合，∘是 A 上的可交换、可结合的运算。这类代数系统实际上就是可交换半群。

为了研究抽象的代数系统，需要先定义一元和二元运算以及二元运算的性质，并通过选择不同的运算性质来规定各种抽象代数系统的定义。在此基础上，再深入研究这些抽象代数系统的内在特性和应用。

本章主要包括代数运算的表示、代数运算的运算律、代数系统、代数常数以及代数系统的同态和同构。

5.1 相关历史背景

代数（algebra）一词最早来源于阿拉伯数学家、天文学家花拉子密。1859 年，中国数学家李善兰首次将 algebra 翻译为代数。清代学者华蘅芳和英国人傅兰雅合译英国瓦里斯的《代数学》，卷首有“代数之法，无论何数，皆可以任何记号代之”等语，也就是说，代数就是运用文字符号来代替数字的一种数学方法。

目前代数已经发展成为一门关于形式运算的一般学说。一个带有形式运算的集合称为代数系统，因此，代数是研究一般代数系统的一门科学。

5.1.1　代数之父花拉子密

花拉子密(Al-Khwarizmi)是阿拉伯阿拔斯王朝著名数学家、天文学家、地理学家。花拉子密是代数与算术的整理者，被誉为“代数之父”。花拉子密的研究兴趣十分广泛，包括数学、天文、历法、历史学、地理学等。在数学方面，花拉子密编著了两部传世之作：《代数学》和《印度的计算术》，其著作通过后来的拉丁文译本对欧洲近代科学的诞生产生过积极影响。

花拉子密汲取和综合了古巴比伦、古希腊和古印度的数学成果，促进了数学向深度和广度发展。公元830年，花拉子密写了一本有关代数的书，这本书被翻译成欧洲文字，书名逐渐简化，被直接译成了《代数学》，代数学一词即由此书而来。书中阐述了解一次方程、二次方程的基本方法及二次平方根的计算公式，明确提出了代数、已知数、未知数、根、移项、集项、无理数等一系列概念，并附有例题800多道，提供了代数计算方法，把代数学发展成为一门与几何学相提并论的独立学科。

此外，印度数码(0～9)也通过他的著作传入西方，欧洲人称之为阿拉伯数字。《代数学》系统地叙述了十进制记数法和小数的运算法，对普及十进制起了很大作用。花拉子密展示了数字加、减、乘、除的基本方法，甚至展示了如何求平方根和π。这些方法被称为“运算法则”。

5.1.2　布尔代数

布尔代数(或逻辑代数)是计算机的基础，没有布尔代数，就不会有计算机。19世纪早期，英国数学家乔治·布尔(George Boole)提出一个问题：人的思想能不能用数学表达？在此之前，数学只用于计算；没有人意识到，数学还能表达人的逻辑思维。为了研究逻辑学，特别是数理逻辑，布尔正式提出了布尔代数。

布尔代数发展到今天已经非常抽象了，但是它的核心思想很简单。简单而言，所谓布尔代数，是指一个有序四元组$<S;\vee,\wedge,*>$，其中S是一个非空集合，$\vee$与$\wedge$是定义在S上的两个二元运算，$*$是定义在B上的一个一元运算。布尔代数虽然和普通代数一样也用字母表示变量，但变量的值只有1和0，所谓逻辑1、逻辑0分别代表两种相反的逻辑状态。在布尔代数中，只有逻辑乘(与运算)、逻辑加(或运算)、求反(非运算)这3种基本运算。

20世纪初，英国科学家香农(C.E.Shannon)指出，布尔代数可以用来描述电路，或者说，电路可以模拟布尔代数。于是，人类的推理和判断就可以用电路实现了。这就是计算机的实现基础。到了20世纪三四十年代，布尔代数又有了新的进展。大约在1935年，斯通(M.H.Stone)指出布尔代数与环之间有明确的联系。他还得到了斯通定理：任意一个布尔代数一定同构于某个集合上的一个集域，任意一个布尔代数也一定同构于某个拓扑空间的闭开代数等。这使布尔代数在理论上有了一定的发展。布尔代数在代数学(代数结构)、逻辑演算、集合论、拓扑空间理论、测度论、概率论、泛函分析等数学分支中均有应

用。1967 年后，在公理化集合论以及模型论的理论研究中，布尔代数也起着一定的作用。近几十年来，布尔代数在自动化技术、电子计算机的逻辑设计等工程技术领域中有重要的应用。

布尔代数的运算法则与集合论很像。

(1) 交集的运算法则如下：

$$1\times 1=1$$
$$1\times 0=0$$
$$0\times 0=0$$

(2) 并集的运算法则如下：

$$1+1=1$$
$$1+0=1$$
$$0+0=0$$

集合论可以描述逻辑推理过程，布尔代数可以判断某个命题是否符合这个过程。人类的推理和判断由此就变成了数学运算。

虽然布尔代数可以判断命题真伪，但是无法取代人类的理性思维，原因是布尔代数有一个局限：布尔代数必须依据一个或几个已经明确知道真伪的命题，才能做出判断。例如，只有知道“所有人都会死”“苏格拉底是人”这两个命题是真的，才能得出结论“苏格拉底会死”。也就是说，布尔代数只能保证推理过程正确，无法保证推理所依据的前提是否正确。如果前提是错的，正确的推理过程也会得到错误的结果。而前提的真伪要由科学实验和观察来决定，布尔代数无能为力。

5.2 代数运算的表示

为了引入代数运算的抽象定义，首先分析代数运算的例子，说明代数运算与映射的联系。

例 5.1 下面是几个代数运算的例子。

(1) 任意非零实数 $X\in\mathbb{R}-\{0\}$，有唯一倒数 $X^{-1}\in\mathbb{R}-\{0\}$。因此，求倒数运算是非零实数集合上的映射，可以记作 $^{-1}:\mathbb{R}-\{0\}\to\mathbb{R}-\{0\}$。

(2) 任意两个实数 $X\in\mathbb{R}$、$Y\in\mathbb{R}$ 有相应的唯一的实数积 $X*Y$。因此，乘法运算是从 $\mathbb{R}\times\mathbb{R}$ 到 $\mathbb{R}$ 的映射，可以记作 $\times:\mathbb{R}\times\mathbb{R}\to\mathbb{R}$。

(3) 全集 E 的任意两个子集 $A\subseteq E$、$B\subseteq E$ 有唯一的并集 $A\cup B\subseteq E$。因此，集合的并运算是从 $P(E)\times P(E)$ 到 $P(E)$ 的映射，可以记作 $\cup:P(E)\times P(E)\to P(E)$。

(4) 任意两个非零自然数 $n\in\mathbb{N}^+$、$m\in\mathbb{N}^+$ 有唯一的有理数商 $q=n/m\in\mathbb{Q}$。因此，除法运算是从 $\mathbb{N}^+\times\mathbb{N}^+$ 到 $\mathbb{Q}$ 的映射，可以记作 $\div:\mathbb{N}^+\times\mathbb{N}^+\to\mathbb{Q}$。

(5) 运算规则△是集合{2,3,4,6,12}上的二元运算，是从{2,3,4,6,12}×{2,3,4,6,12}到{0,1}的映射。△的运算表如表 5.1 所示。

表 5.1　集合{2,3,4,6,12}上△的运算表

△	2	3	4	6	12
2	1	0	1	1	1
3	0	1	0	1	1
4	0	0	1	0	1
6	0	0	0	1	1
12	0	0	0	0	1

分析以上例子可以发现：运算的本质其实是集合到集合的映射。

定义 5.1　设 S 是集合，定义如下映射：

$f: S \to S$ 称为 S 上的**一元运算**(unary operation)，$a \in S$ 是运算数，$b = f(a)$是运算结果。

$f: S \times S \to S$ 称为 S 上的**二元运算**(binary operation)。$<a_1, a_2> \in S \times S$，$a_1$、$a_2$ 是运算数，$b = f(<a_1, a_2>)$是运算结果。通常也表示成 $b = a_1 f\ a_2$。

$f: S^n \to S$ 称为 S 上的 ***n* 元运算**(n-ary operation)，其中 n 是自然数，S^n 是 S 的 n 重笛卡儿积。

集合 S 上的代数运算并非只有加、减、乘、除运算，它的意义具有广泛性。表示代数运算的符号(运算符)有多种，可以用∘、*、·、⊕、⊗等符号表示二元运算或一元运算。对于二元运算·，如果运算数 x、y 经过·运算得到运算结果 z，那么记作 $x \cdot y = z$。对于一元运算符∘，运算数 a 的运算结果记作∘a。

例 5.2　下面是集合上一元运算的实例。

(1) 求一个数的相反数是整数集合$\mathbb{Z}$、有理数集合$\mathbb{Q}$、实数集合$\mathbb{R}$上的一元运算。

(2) 求一个数的倒数是非零有理数集合$\mathbb{Q}^*$、非零实数集合$\mathbb{R}^*$上的一元运算。

(3) 在幂集合 $P(S)$上，求集合绝对补的运算～是 $P(S)$上的一元运算。

(4) A 为集合 S 上所有双射函数的集合，求双射函数的反函数是 A 上的一元运算。

(5) 在 $n(n \geqslant 2)$阶实矩阵集合 $\boldsymbol{M}_n(R)$上，求矩阵的转置矩阵是 $\boldsymbol{M}_n(R)$上的一元运算。

(6) 定义 upper：$\Sigma \to \Sigma$，满足对于任意 $\sigma \in \Sigma$，upper(σ)将 σ 中所有小写字母改为大写字母。upper 是 Σ 上的一元运算。

小结：一元运算是集合上的变换。

在本章中，主要考虑二元运算及其性质。判断一个运算是否为集合 S 上的二元运算，主要考虑以下两点：

(1) S 中任意两个元素都可以进行这种运算，且运算结果是唯一的。

(2) S 中任意两个元素的运算结果都属于 S，即 S 对该运算是**封闭的**(closed)。

例 5.3　下面是几个集合上二元运算、三元运算的实例。

(1) 定义 $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$，$f(<x, y>) = x + y$，$f$ 是自然数集合$\mathbb{N}$上的二元运算，即加法运算。

(2) 并运算∪、交运算∩、对称差运算⊕均为集合 S 的幂集 $P(S)$上的二元运算。

(3) 在集合 $\Sigma=\{\sigma|\sigma$ 是英文字母符号串$\}$上,定义 $\&:\Sigma\times\Sigma\to\Sigma$,对于任意$<\sigma_1,\sigma_2>\in\Sigma\times\Sigma$,有 $\sigma_1\&\sigma_2=\sigma_1\sigma_2$。$\&$ 为 Σ 上的二元运算,称为**字符串的连接运算**。

(4) 在实数集合$\mathbb{R}$上,定义三元函数 Mean:$\mathbb{R}\times\mathbb{R}\times\mathbb{R}\to\mathbb{R}$,$\text{Mean}(x,y,z)=(x+y+z)/3$。Mean 是实数集合$\mathbb{R}$上的三元运算。

(5) 减法运算不是自然数集合$\mathbb{N}$上的二元运算。因为两个自然数相减可能得到负数,而负数不是自然数。称集合$\mathbb{N}$对减法运算不封闭,或者称减法运算在集合$\mathbb{N}$上不封闭。

(6) 除法运算在实数集合$\mathbb{R}$上不封闭。因为 $0\in\mathbb{R}$,而 0 不能作除数。

除法运算在非零实数集合$\mathbb{R}^*=\mathbb{R}-\{0\}$上封闭,因为$\forall x,y\in\mathbb{R}^*$都有 $x/y\in\mathbb{R}^*$。

(7) 加法、乘法运算是自然数集合$\mathbb{N}$上的二元运算。

减法、除法运算不是自然数集合$\mathbb{N}$上的二元运算。

(8) 加法、减法、乘法运算都是整数集合$\mathbb{Z}$上的二元运算。

除法运算不是整数集合$\mathbb{Z}$上的二元运算。

(9) 乘法、除法运算都是非零实数集$\mathbb{R}^*$上的二元运算。

加法、减法运算不是非零实数集$\mathbb{R}^*$上的二元运算,两个非零实数相加或相减可能得 0。

(10) 设 $\boldsymbol{M}_n(R)$为 n 阶($n\geqslant 2$)实矩阵的集合,矩阵加法和乘法运算都是 $\boldsymbol{M}_n(R)$上的二元运算。

小结:二元运算是从笛卡儿积 $S\times S$ 到集合 S 的映射。

运算表是表示一元运算或二元运算的重要方法。表 5.2 和表 5.3 分别是一元运算表和二元运算表的一般形式,其中 $a_1,a_2,\cdots,a_n$ 是 S 中的元素,$\circ$为运算符。

表 5.2　一元运算表

a_i	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
⋮	⋮
a_n	$\circ a_n$

表 5.3　二元运算表

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1\circ a_1$	$a_1\circ a_2$	$\cdots$	$a_1\circ a_n$
a_2	$a_2\circ a_1$	$a_2\circ a_2$	$\cdots$	$a_2\circ a_n$
⋮	⋮	⋮	⋮	⋮
a_n	$a_n\circ a_1$	$a_n\circ a_2$	$\cdots$	$a_n\circ a_n$

例 5.4　分别给出 $S=\{1,2\}$的幂集 $P(S)$上的$\sim$运算表和$\oplus$运算表。$P(S)$上的$\sim$运算表如表 5.4 所示。$P(S)$上的$\oplus$运算表如表 5.5 所示。

表 5.4　$P(S)$上的$\sim$运算表

a_i	$\circ a_i$
$\varnothing$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\varnothing$

表 5.5　$P(S)$上的$\oplus$运算表

$\oplus$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\varnothing$

例 5.5　在集合 $S=\{a,b,c\}$ 上可以定义多少个二元运算？

解：集合 $S=\{a,b,c\}$ 上的二元运算可以定义为 $f: S\times S\to S$。$|S\times S|=9$，$|S|=3$，所以集合 S 上可以定义的二元运算的总个数是 3^9。

例 5.6　下面各集合都是自然数集合 $\mathbb{N}$ 的子集，在普通加法运算（+）下是否封闭？

（1）$\{x \mid x$ 的某次幂可以被 16 整除$\}$。

（2）$\{x \mid x$ 与 5 互质$\}$。

（3）$\{x \mid x$ 是 30 的因子$\}$。

（4）$\{x \mid x$ 是 30 的倍数$\}$。

解：（1）封闭。若 x^s、y^t 是 16 的倍数，则 $(x+y)^{s+t}$ 也是 16 的倍数。

（2）不封闭。反例：2 和 5 互质，3 也和 5 互质，但 2+3=5 不与 5 互质。

（3）不封闭。反例：3 和 5 都是 30 的因子，但 3+5=8 不是 30 的因子。

（4）封闭。x 是 30 的倍数，y 是 30 的倍数，$x+y$ 也是 30 的倍数。

例 5.7　在集合 $S=\{a,b\}$ 上可以定义多少个二元运算？

解：集合 $S=\{a,b\}$ 上的二元运算可以定义为 $f: S\times S\to S$。$|S\times S|=4$，$|S|=2$，所以集合 S 上可以定义的二元运算的个数是 2^4。

5.3　代数运算的运算律

定义 5.2　设 S 是集合，$\circ$ 和 $*$ 为集合 S 上不同的二元运算。

（1）如果 $\forall x,y\in S$，有 $x\circ y=y\circ x$，称运算 $\circ$ 在 S 上满足**交换律**（commutativity）。

（2）如果 $\forall x,y,z\in S$，有 $(x\circ y)\circ z=x\circ(y\circ z)$，称运算 $\circ$ 满足**结合律**（associativity）。

（3）如果 $\forall x\in S$，有 $x\circ x=x$，称运算 $\circ$ 在 S 上满足**幂等律**（idempotence）。

（4）如果 $\forall x,y,z\in S$，有 $(x*y)\circ z=(x\circ z)*(y\circ z)$，并且 $z\circ(x*y)=(z\circ x)*(z\circ y)$，称 $\circ$ 运算对 $*$ 运算满足**分配律**（distributivity）。

（5）如果运算 $\circ$ 和 $*$ 都可交换，并且 $\forall x,y\in S$，有 $x\circ(x*y)=x$ 和 $x*(x\circ y)=x$，称 $\circ$ 运算和 $*$ 运算满足**吸收律**（absorptive）。

表 5.6 给出了一些代数运算的性质，其中 $\mathbb{Z}$ 表示整数集，$\mathbb{Q}$ 表示有理数集，$\mathbb{R}$ 表示实数集，$\boldsymbol{M}_n(\mathbb{R})$ 表示 $n(n\geqslant 2)$ 阶实矩阵集合，A^A 是所有从集合 A 到集合 A 的函数集合。

表 5.6　一些代数运算的性质

集　合	运　算	交换律	结合律	幂等律	分配律	吸收律
$\mathbb{Z},\mathbb{Q},\mathbb{R}$	$+,\times$	√	√	×	×对+	×
$\boldsymbol{M}_n(\mathbb{R})$	矩阵加法（+） 矩阵乘法（×）	√ ×	√ √	× ×	×对+	×
$P(S)$	$\cup,\cap$	√	√	√	互相有	√
A^A	函数合成	×	√	×	×	×

例 5.8 分别判断下述二元运算是否满足交换律。

(1) 整数集合$\mathbb{Z}$上的减法。

(2) n 阶实矩阵集合$\boldsymbol{M}_n(\mathbb{R})$上的矩阵加法。

(3) $*$ 运算：任给 $a,b\in\mathbb{Z}$，$a*b=ab+a+b$。

(4) $\cdot$ 运算：集合$|S|\geqslant 2$，$\forall a,b\in S$，$a\cdot b=b$。

解：(1)、(4)不满足交换律，(2)、(3)满足交换律。

例 5.9 分别判断下述二元运算是否满足结合律。

(1) 整数集合$\mathbb{Z}$上的减法运算。

(2) n 阶实矩阵集合$\boldsymbol{M}_n(\mathbb{R})$上的矩阵加法。

(3) $*$ 运算：任给 $a,b\in\mathbb{Z}$，$a*b=ab+a+b$。

(4) $\cdot$ 运算：集合$|S|\geqslant 2$，$\forall a,b\in S$，$a\cdot b=b$。

解：(1)不满足结合律，(2)～(4)满足结合律。

例 5.10 判断下述每一对二元运算是否满足分配律。

(1) 在实数集合$\mathbb{R}$上，乘法对加法。

(2) 在实数集合$\mathbb{R}$上，加法对乘法。

(3) 在实数集合$\mathbb{R}$上，乘法对减法。

(4) 在正实数集合$\mathbb{R}^+$上，除法对加法。

(5) 集合 S 的幂集 $P(S)$上，交运算对并运算。

解：(1)、(3)、(5)满足分配律，(2)、(4)不满足分配律。

左分配律和右分配律是相互独立的。证明 $*$ 对$\circ$服从分配律时，必须证明左分配律和右分配律都成立。如果 $*$ 是可交换的，则只需验证一个分配律，因为左右分配律要么同时成立，要么同时不成立。

例 5.11 $\forall x,y\in\mathbb{Q}$，$x*y=x+y-xy$，$*$ 运算是否满足交换律、结合律和幂等律？

解：$\forall x,y\in\mathbb{Q}$，交换律成立：

$$x*y=x+y-xy$$
$$y*x=y+x-yx$$
$$x*y=y*x$$

$\forall x,y,z\in\mathbb{Q}$，结合律成立：

$$\begin{aligned}(x*y)*z&=(x+y-xy)+z-(x+y-xy)z\\&=x+y+z-xy-yz+xyz\\x*(y*z)&=x+(y+z-yz)-x(y+z-yz)\\&=x+y+z-xy-xz-yz+xyz\\(x*y)*z&=x*(y*z)\end{aligned}$$

幂等律不成立。反例如下：

$$2*2=2+2-2\cdot 2=0\neq 2$$

所以，$*$ 运算满足交换律、结合律，不满足幂等律。

例 5.12 分别说明表 5.7 所示的二元运算 $*$、$\circ$、$\cdot$ 是否满足交换律、结合律和幂等律。

表 5.7　二元运算 $*$、$\circ$、$\cdot$ 运算表

$*$	a	b	c	$\circ$	a	b	c	$\cdot$	a	b	c
a	a	b	c	a	a	b	c	a	a	b	c
b	b	c	a	b	a	b	c	b	b	b	b
c	c	a	b	c	a	b	c	c	c	b	c

解：(1) $*$ 运算满足交换律和结合律，不满足幂等律。

(2) $\circ$ 运算不满足交换律，满足结合律和幂等律。

(3) $\cdot$ 运算满足交换律、结合律和幂等律。

如果二元运算由运算表给出，则需要检查运算表的特征。具体说明如下：

(1) 如果运算表关于主对角线是对称的，则该运算满足交换律。

(2) 如果运算表的主对角线元素排列顺序与表头元素顺序一致，则该运算是幂等的。

(3) 结合律的判断需要对所有可能的元素 x、y、z 验证关于结合律的等式。一般来说，如果集合中有 n 个元素，就需要验证 n^3 个等式。但是对于一些特殊情况，可以有某些简便的方法。总之，对于结合律的验证是相当烦琐的。至于分配律和吸收律，就更难判断了。

具体分析上面 3 个运算 $*$、$\circ$、$\cdot$ 的运算表：

(1) $*$ 和 $\cdot$ 的运算表，是对称的，所以 $*$ 和 $\cdot$ 的运算满足交换律。

(2) $\cdot$ 和 $\circ$ 主对角线元素是 a、b、c，与表头元素排列顺序一致，所以 $\cdot$ 和 $\circ$ 满足幂等律。

(3) 关于结合律的验证，$*$ 运算的单位元是 a，只需对 b 和 c 进行验证。又由于对称性，只要验证关于 bbb、bbc、ccc 的情况即可。$\circ$ 运算的每个元素都是右零元，不必验证。$\cdot$ 运算的 a 是单位元，b 是零元。又由于对称性，ccc 的情况显然为真。

5.4　代数系统与代数常数

定义 5.3　非空集合 A 及其上的若干个封闭运算 $f_1, f_2, \cdots, f_n$ 组成的系统称为**代数系统**(algebraic system)，记作 $<A; f_1, f_2, \cdots, f_n>$。

例 5.13　下面是一些代数系统。

(1) $<\mathbb{N}; +, \times>$，表示自然数集合及自然数的加法运算和乘法运算。

(2) $<\Sigma; \&, \mathrm{Lt}, \mathrm{Rt}, \mathrm{Lower}, \mathrm{Upper}>$，表示字符串集合及字符串的连接运算、左截取运算、右截取运算、小写化运算和大写化运算。

(3) $<\mathbb{R}; +, -, \times>$，表示实数集合及实数的加法、减法和乘法运算。

(4) $<\mathbb{N}; \mathrm{Max}, \mathrm{Min}>$，表示自然数集合及自然数的求大值和求小值运算。

(5) $<\boldsymbol{T}_{n\times n}; +, -, \times>$，表示 n 阶方阵集合及矩阵的加法、减法和乘法运算。

(6) $<\mathbb{R}-\{0\}; \div>$，表示非零实数集合及实数除法运算。

(7) $<P(E); \cup, \cap, \sim>$，表示幂集及集合的并、交、补运算。

(8) $<P(E); \oplus>$，表示全集的幂集及集合的对称差运算。

(9) $<K; +_{\mathrm{m}}>$，$K=\{0,1,2,\cdots,k-1\}$，运算 $+_{\mathrm{m}}$：对于任意 $k_1, k_2 \in K$，有 $k_1 +_{\mathrm{m}} k_2 =$

$(k_1+k_2) \bmod k$。

检验以上的例子，可以发现所有运算都是在集合上封闭的，也就是说，运算数来自这个集合，运算结果属于这个集合。

例 5.14 下面的集合与运算不构成代数系统。

(1) $<\mathbb{N}；->$，表示自然数集合及减法运算。因为两个自然数相减，结果可能是负数。

(2) $<\mathbb{R}-\{0\}；+>$，表示非零实数集合及加法运算。非零实数-2和2进行加法运算的结果为0。

例 5.15 设 $S=\{1,2,5,6,8,9,10\}$，S 对于下面的运算能否构成代数系统？

(1) 求最大公约数。

(2) 求最小公倍数。

(3) 求两个数之中较大的数。

解：(1)、(2)不是，(3)是。

判断给定集合与运算能否构成代数系统，实际上是判断所有给定的运算是否为该集合上的运算。

(1) 6和9的最大公约数是3，3不在 S 中，运算不封闭。

(2) 6和9的最小公倍数是18，18不在 S 中，运算不封闭。

(3) S 中的任意两个元素 x、y(不妨设 $x<y$)，较大的数是 y，运算封闭。

在某些代数系统中，存在着一些特定的元素，它们对于代数系统的一元运算或二元运算起着重要的作用。在定义代数系统的时候，有时规定代数系统必须含有这些特定元素，作为代数系统的性质，例如，规定代数系统必须具有单位元和零元。

定义 5.4 设$\circ$为集合 S 上的二元运算，如果 $\exists e_l$(或 e_r)$\in S$，使得对 $\forall x \in S$，都有 $e_l \circ x=x$(或 $x \circ e_r=x$)，则称 e_l(或 e_r)是 S 中关于$\circ$运算的**左**(或**右**)**单位元**。若 $e \in S$ 关于$\circ$运算既是左单位元又是右单位元，则称 e 为 S 上关于$\circ$运算的**单位元**。单位元也称为**幺元**(identity element)，一般记作 e。

如果 $\exists \theta_l$(或 θ_r)$\in S$，使得对 $\forall x \in S$，都有 $\theta_l \circ x=\theta_l$(或 $x \circ \theta_r=\theta_r$)，则称 θ_l(或 θ_r)是 S 中关于$\circ$运算的**左**(或**右**)**零元**。若 S 关于$\circ$运算既是左零元又是右零元，则称 θ 为 S 上关于运算$\circ$的**零元**(zero element)，一般记作 θ。

令 e 为 S 中关于运算$\circ$的单位元。对于 $x \in S$，如果 $\exists y_l$(或 y_r)$\in S$，使得 $y_l \circ x=e$(或 $x \circ y_r=e$)，则称 y_l(或 y_r)是 x 的**左逆元**(或**右逆元**)。若 $y \in S$ 既是 x 的左逆元又是 x 的右逆元，则称 y 为 x 的**逆元**(inverse element)，一般记作 x^{-1}。如果 x 逆元存在，就称 x **可逆**。

单位元和零元称为代数系统的**代数常数**。表5.8给出了一些代数系统的代数常数。

表 5.8 一些代数系统的代数常数

集　合	运　算	单 位 元	零　元	逆　元
$\mathbb{Z},\mathbb{Q},\mathbb{R}$	$+$ $\times$	0 1	无 0	$-x$ $1/x(x\neq 0)$

续表

集　合	运　算	单位元	零　元	逆　元
$\boldsymbol{M}_n(R)$	矩阵加法(+) 矩阵乘法(×)	零矩阵 单位矩阵	无 零矩阵	$-\boldsymbol{M}$ $\boldsymbol{M}^{-1}$($\boldsymbol{M}$ 为可逆矩阵)
$P(S)$	$\cup$ $\cap$	$\varnothing$ S	S $\varnothing$	只有$\varnothing$有逆元$\varnothing$ 只有 S 有逆元S

关于代数系统的单位元、零元与逆元，有下述定理。

定理 5.1　设$\circ$为集合 S 上的二元运算，e_l 为 S 中关于$\circ$运算的左单位元，e_r 为 S 中关于$\circ$运算的右单位元。记作 $e_l=e_r=e$，这是集合 S 上关于$\circ$运算的唯一单位元。

证明：因为 e_r 为右单位元，所以 $e_l\circ e_r=e_l$。

因为 e_l 为左单位元，所以 $e_l\circ e_r=e_r$。

所以 $e_l=e_r$，将这个单位元记作 e。

假设 $e'(e'\neq e)$也是 S 中的单位元，则有 $e'=e\circ e'=e$。

因此，集合 S 上关于$\circ$运算单位元是唯一的。

类似地可以证明关于零元的唯一性。

定理 5.2　设$\circ$为集合 S 上可结合的二元运算，e 为$\circ$运算的单位元。对于 $x\in S$，如果存在左逆元 y_l 和右逆元 y_r，则有 $y_l=y_r=y$，且 y 是 x 唯一的逆元。

证明：如果 $x\in S$ 存在左逆元 y_l 和右逆元 y_r，e 为$\circ$运算的单位元，那么 $y_l\circ x=e$，$x\circ y_r=e$。

$$y_l=y_l\circ e=y_l\circ(x\circ y_r)=(y_l\circ x)\circ y_r=e\circ y_r=y_r$$

令 $y_l=y_r=y$，y 是 x 的逆元。

若 $y'\in S(y'\neq y)$也是 x 的逆元，则 $y'=y'\circ e=y'\circ(x\circ y)=(y'\circ x)\circ y=e\circ y=y$。

所以 y 是 x 唯一的逆元。

由定理 5.2 可知，对于可结合的二元运算，可逆元素 x 只有唯一逆元，通常记作 x^{-1}。

用反证法可以证明，单位元与零元是不同的，除非集合 S 只有一个元素。在集合 S 只有一个元素的情况下，这个唯一的元素既是单位元也是零元。

由上述定理可以得到下面两个推论。

推论 5.1　代数系统中的单位元 e 是可逆元素，其逆元是它自己(e)。

推论 5.2　代数系统中的零元素 θ 不是可逆元素。

对于一个代数系统，如何求代数系统的单位元和零元？对于代数系统中的元素 x，如何求 x 的逆元？一般把单位元 e、零元 θ 或逆元 x^{-1}分别带入公式，然后求解。

例 5.16　在有理数集合$\mathbb{Q}$上定义 $*$ 运算：$\forall x,y\in\mathbb{Q}$，$x*y=x+y-xy$。求出 $*$ 运算的单位元、零元和$\mathbb{Q}$上所有可逆元素的逆元。

解：$\forall x\in\mathbb{Q}$，有 $x*e=e*x=x$，即 $x+e-xe=e+x-ex=x+e(1-x)=0$。由 x 的任意性可得 $e=0$。

$\forall x\in\mathbb{Q}$，有 $x*\theta=\theta*x=x$，即 $x+\theta-x\theta=\theta+x-\theta x=\theta$，$x(1-\theta)=0$，由 x 的任意性可得 $\theta=1$。