离散数学
普及丛书

代数结构

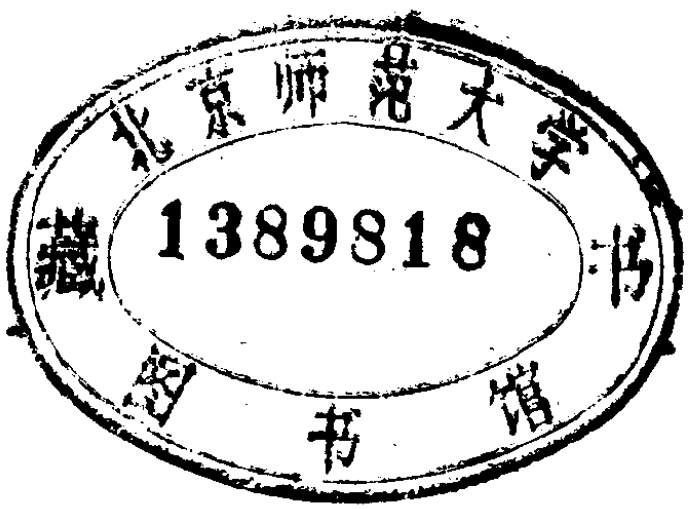
李为鉴 刘永才 编著

人民邮电出版社

离散数学普及丛书

代 数 结 构

李为镭 刘永才 编著



人民邮电出版社

内 容 提 要

本书是离散数学普及丛书的第三分册，主要介绍的是代数系统中的基本内容，其中包括群论、环、格及布尔代数等几个方面，内容叙述比较严谨、推演详尽，大部分概念都结合有适当的实例说明。并附有习题及参考答案。

本书可作为非计算机专业的大、中专学生学习离散数学用，也可供有关专业的工程技术人员及具有高中文化水平的读者学习参考。

离散数学普及丛书

代 数 结 构

李为鑑 刘永才 编著

人民邮电出版社出版

北京东长安街27号

河北省邮电印刷厂印刷

新华书店北京发行所发行

各地新华书店经售

开本：787×1092 1/32 1986年5月 第一版

印张：7 15/32 页数：120 1986年5月河北第一次印刷

字数：170 千字 印数：1-5,000 册

统一书号：15045·总3136-有5444

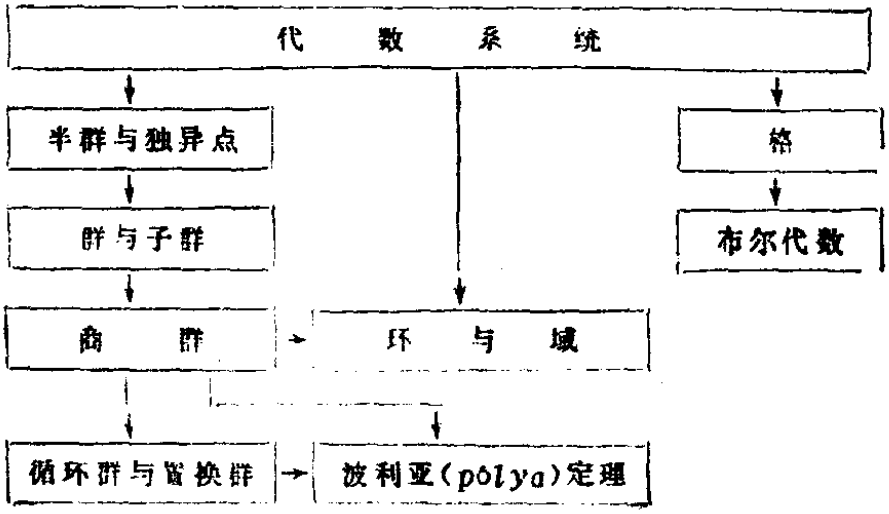
定价：1.65 元

序　言

作为离散数学的一个重要方面，我们将在本书中研究代数系统。代数系统不仅与数学的不少分支有着密切的联系，而且它在计算机科学的某些领域中也是不可缺少的，在近代物理和化学中也有很多重要的应用。

尽管代数系统的研究已经形成一门学科，通常称之为“近世代数”或“抽象代数”，涉及到的内容不仅十分丰富而且也相当抽象，至今已有不少专著，然而，我们在本书中将尽可能通俗地向读者介绍代数系统中最基本的内容，并就某些重要方面作些专门的讨论。

本书各章之间的基本联系如下面的框图所示：



目　　录

第一章　代数系统的一般概念……（ 1 ）

§ 1　几个实例……（ 1 ）

§ 2　二元运算……（ 3 ）

§ 3　代数系统……（ 8 ）

§ 4　同构与同态……（ 10 ）

§ 5　商代数系统……（ 15 ）

第二章　半群与独异点……（ 22 ）

§ 1　半群……（ 22 ）

§ 2　独异点……（ 27 ）

第三章　群与子群……（ 32 ）

§ 1　群……（ 32 ）

§ 2　子群……（ 39 ）

§ 3　群的同态与同构……（ 42 ）

第四章　循环群与置换群……（ 46 ）

§ 1　循环群……（ 46 ）

§ 2　置换群……（ 54 ）

第五章　商群……（ 72 ）

§ 1　陪集……（ 72 ）

§ 2　正规子群与商群……（ 77 ）

*§ 3　群同态定理……（ 84 ）

§ 4　直积……（ 89 ）

第六章　波利亚(Pólya)定理 ……（ 97 ）
§ 1　作用于集合 X 的群……（ 97 ）
§ 2　伯恩赛德（*Burnside*）定理……（ 100 ）
§ 3　波利亚(*Pólya*)定理 ……（ 109 ）
第七章　环和域……（ 117 ）
§ 1　环……（ 117 ）
§ 2　整环与域……（ 125 ）
§ 3　多项式环……（ 128 ）
§ 4　分式域……（ 131 ）
§ 5　理想、商环、环同态定理……（ 134 ）
第八章　格……（ 143 ）
§ 1　引言……（ 143 ）
§ 2　格与格所定义的代数系统……（ 146 ）
§ 3　格的一些性质……（ 148 ）
§ 4　格的同态与同构……（ 155 ）
§ 5　几种类型的格……（ 159 ）
第九章　布尔代数……（ 174 ）
§ 1　引言……（ 174 ）
§ 2　布尔代数的基本性质……（ 176 ）
§ 3　子布尔代数和布尔同态……（ 177 ）
§ 4　有限布尔代数的表示定理……（ 180 ）
§ 5　布尔表达式与布尔函数……（ 187 ）
习题解答 ……（ 195 ）
符号表 ……（ 230 ）

第一章　代数系统的一般概念

为了让读者对代数系统有一个总的认识，我们在这一章中首先介绍代数系统的一般概念。

§1　几个实例

例 1　自然数集合N，在N上有普通的加法运算“+”，这个运算由表1.1给出

表 1.1

+	0	1	2	3	4	5	…
0	0	1	2	3	4	5	…
1	1	2	3	4	5	6	…
2	2	3	4	5	6	7	…
3	3	4	5	6	7	8	…
4	4	5	6	7	8	9	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

例如，$2+3=5$，$4+3=7$ 等等。

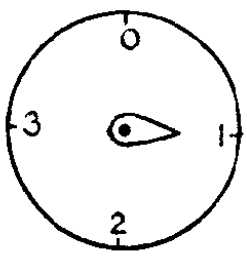


图 1.1

例 2　具有旋钮开关的一台电风扇，它有三个变速档，且开关按顺时针方向转动。如图1.1所示。

其中，0 是停，1、2、3 依次是快速档、中速档、慢速挡。

若每次均按顺时针方向转动不超过 3 的整数格，则两次转

动就可看作一种“加”法运算，然而，这种“加”法已经与普通加法不完全相同了，我们给这种“加”法运算以一个特殊的运算码号⊕。譬如，从0开始，当先转动3格后再转动1格，就又回到0了，即有 $3 \oplus 1 = 0$。运算⊕可由表1.2给出。

表 1.2

⊕	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

因此，⊕就是集合 $S=\{0, 1, 2, 3\}$ 上的一个运算。例如，$2 \oplus 3 = 1$，$3 \oplus 3 = 2$ 等等，运算结果仍在 S 中。

上述两个例子分别是在某个确定集合上规定了一个运算，而且运算的结果又都分别属于相应的集合，具有这种性质的运算称为闭运算。

一个集合 A 上确定了一个运算 $*$，运算 $*$ 还可以具有某些性质。这就构成最简单的代数系统，记作 $(A, *)$。

我们知道，在一个集合上，也可以确定若干个运算。

例 3 复数集合 C，在 C 上有普通的复数加法和复数乘法运算，即对于任意的 $a+bi$，$c+di \in C$，有

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)\cdot(c+di)=(a\cdot c-b\cdot d)+(a\cdot d+(b\cdot c)i$$

显然，复数加法和复数乘法都是闭运算。这就构成了在集合 C 上确定了两个运算“+”和“·”的代数系统，记作 $(C, +, \cdot)$。

§2 二元运算

我们可以形象地把一个运算看作是一只“黑箱”，即把一个运算过程看为是：从集合 S 中取出几个元素通过“黑箱”的几个入口输入，并在“黑箱”中由某种方式结合成 S 中的一个元素，再通过“黑箱”的一个出口输出。

如果“黑箱”有两个输入，使得集合中的两个元素 a 和 b 运算结合成元素 $a \bullet b$，这样的运算就称为二元运算。如图1.2(a)所示。上节所述的三个例子中的运算都是二元运算。如果“黑箱”仅有一个输入，使得集合中的一个元素 c 经过运算后得到元素 c'，这样的运算就称为一元运算。如图1.2(b)所示。例如，求非零实数的倒数就是一种一元运算。

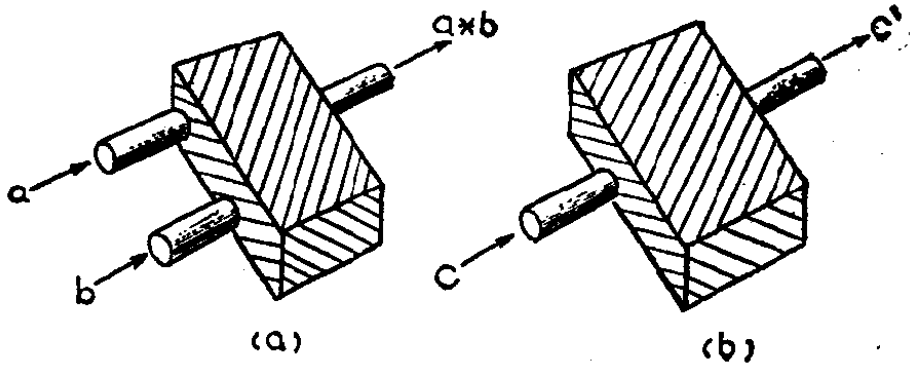


图 1.2

在集合 S 上的一个二元运算可以用一个从笛卡尔积 $S \times S$ 到 S 的函数 f 来描述，即 $f[(a_1, a_2)]$表示 $S \times S$ 中的有序对 (a_1, a_2)的象，为简单起见，我们可以用 $a \bigstar b$ 来表示有序对 (a, b)在函数 f 作用下的象，这时，★就作为二元运算的一个“运算符号”来使用。如果 $a, b \in S$，而 $a \bigstar b \in S$，就称运算★是封闭的。今后，我们常用的二元运算符号有★、$\bullet$、$\oplus$、$\square$、$\triangle$、$\odot$、$+$、$\cdot$、$-$、$\cdot$、$\div$、$\cup$、$\cap$、$\vee$和$\wedge$等。若

不特别申明，集合上的运算通常是指闭运算。

在集合S上的一个一元运算实际上就是一个从S到S的函数。S中元素c的象通常用c'、$\overline{c}$、c^{-1}、$(-c)$等这样一些记号来表示。

设$I_+=\{1, 2, 3, \cdots\}$是正整数集合，对于任意的x、$y\in I_+$，如果定义二元运算□和△分别为：

$$x \square y = x'$$

$$x \triangle y = GCD(x, y)$$

这里$GCD(x, y)$表示x与y的最大公约数。因为$x'\in I_+$，$GCD(x, y)\in I_+$，所以，运算□、△都是I_+上的闭二元运算。然而，由于$1-3=-2\notin I_+$，所以减法不是I_+上的闭二元运算。

设R是所有实数的集合，对于任意的x，$y\in R$，因为$x+y$、$x\cdot y$、$x-y$都是实数，所以，$+$、$\cdot$、$-$都是R上的闭二元运算。但是除法就不是R上的闭二元运算，因为$x\div 0$没有意义。然而，在非零实数集合$R-\{0\}$上，$\div$就是一个闭二元运算了。由此可见，运算总是与集合密切相关的。

在有限集合上的一个二元运算可以方便地用一张运算表来表示。例如，在集合$T=\{a, b, c, d\}$上的一个二元运算$\cdot$由表1.3所定义：

表 1.3

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

如果 a， b， c， d 分别是以下的四个二阶矩阵

$$a=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad b=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

$$c=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\quad d=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

而二元运算·是矩阵相乘，那么，容易验证其对应的运算表就是表1.3。

例 4 设平面上一个正方形，四只角画上扑克牌的四种不同花样，记作W；将此正方形绕 x 轴旋转180°得到的结果记为 X；再将此正方形绕 y 轴旋转180°得到的结果记为 Y；而将此正方形先绕 x 轴旋转180°再绕 y 轴旋转180°所得到的结果记作 Z。如图1.3所示

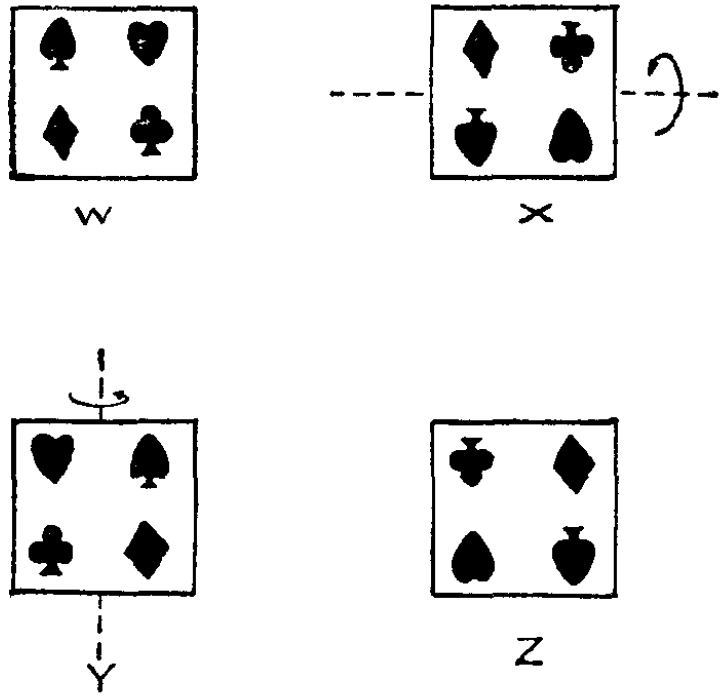


图 1.3

由这四种状态组成集合 $S=\{W, X, Y, Z\}$，在集合 S 上定义二元运算·，$X\cdot Y$ 表示先绕 x 轴旋转180°再绕 y 轴旋转180°

所得的结果，即$X \cdot Y = Z$；$Z \cdot X$表示在已有的先绕x轴旋转180°再绕y轴旋转180°所得结果Z的基础上，再绕x轴旋转180°所得的结果，即$Z \cdot X = Y$，等等。由此可得S上的二元运算·的运算表，如表1.4所示

表 1.4

·	W	X	Y	Z
W	W	X	Y	Z
X	X	W	Z	Y
Y	Y	Z	W	X
Z	Z	Y	X	W

对于一个二元运算，我们常常会遇到以下一些性质中的一个或者几个。设★是集合S上的一个二元运算

（1）如果对于任意的a，$b \in S$，有$a \bigstar b = b \bigstar a$，则称运算★是可交换的。

（2）如果对于任意的a，b，$c \in S$，有$a \bigstar (b \bigstar c) = (a \bigstar b) \bigstar c$，则称运算★是可结合的。

（3）如果存在着$e \in S$，对于任意的$a \in S$，都有$e \bigstar a = a \bigstar e = a$，则称$e$是$S$中关于运算★的幺元。

（4）如果存在着$\theta \in S$，对于任意的$a \in S$，都有$\theta \bigstar a = a \bigstar \theta = \theta$，则称$\theta$是$S$中关于运算★的零元。

例如，在实数集合R上的加法和乘法运算，我们都熟知，这两个二元运算都是可交换和可结合的。关于加法的幺元是0，关于乘法的幺元是1。另外，关于乘法的零元是0，而关于加法不存在零元。

设★是集合S上的二元运算，且在S中存在着关于运算★的幺元e。对于$a \in S$，如果存在$b \in S$，使得

$$a \bigstar b = b \bigstar a = e$$

则称 b 是 a 关于★的逆元，我们通常用 a^{-1} 来表示 a 的逆元。如果运算是加法运算，那么常常用 $-a$ 来表示 a 的逆元。

例如，在实数集合 R 上，每个实数 a 关于加法都有逆元，就是它的负数 $-a$，每个非零实数 a 都有乘法逆元，就是它的倒数 $\frac{1}{a}$。

设★和 $\cdot$ 是 S 上的两个二元运算，如果对于任意的 a，b，$c \in S$，都有

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

和

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

则称 $\cdot$ 对于★是可分配的。

显然，在实数集合 R 上，乘法对于加法是可分配的，因为对任意的 a，b，$c \in R$，都有

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

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

然而，加法对于乘法并不是可分配的，这是因为在一般情况下，$a + (b \cdot c) \neq (a + b) \cdot (a + c)$。

例 5 设 $\mathscr{M}(n; R)$ 表示 n 阶实矩阵的集合。矩阵乘法是 $\mathscr{M}(n; R)$ 上的一个二元运算，它是一个可结合运算，但是，当 $n \neq 1$ 时，它不是一个可交换运算。n 阶单位矩阵是 $\mathscr{M}(n; R)$ 中的乘法幺元。对于 $\mathscr{M}(n; R)$ 中的每一个非奇矩阵 A（即 $|A| \neq 0$），都有唯一的逆矩阵 A^{-1} 存在，使得 $A^{-1}A =$

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$A A^{-1}=E$。矩阵加法也是$\mathscr{M}(n; R)$上的一个二元运算，它是一个可交换运算也是一个可结合运算。n阶零矩阵是$\mathscr{M}(n; R)$中的加法幺元。对于$\mathscr{M}(n; R)$中的任意一个矩阵A，都有唯一的矩阵$-A$存在，使得$A+(-A)=(-A)+A=0$。另外，矩阵乘法对于矩阵加法是可分配的，即对于任意的A，B，$C\in\mathscr{M}(n; R)$都有

$$A\cdot(B+C)=A\cdot B+A\cdot C$$

$$(B+C)\cdot A=B\cdot A+C\cdot A$$

§3 代数系统

一个集合A，连同定义在A上的一个或若干个运算所构成的系统称为代数系统。通常，我们用记号$(A, \bigstar, \odot, \triangle, \square)$来表示一个代数系统，这里$\bigstar$，$\odot$，$\triangle$，$\square$都是定义在集合$A$上的闭运算。一般地，如果在$A$上定义了$n$个运算$f_1$，$f_2$，…，$f_n$，那么，这个代数系统就表示为$(A, f_1, f_2, \cdots, f_n)$。

例4中描述的例子实际上就是代数系统$(\{W, X, Y, Z\}, \cdot)$，它是具有一个二元运算的代数系统。例5中所描述的例子实际上就是代数系统$(\mathscr{M}(n; R), +, \cdot)$，这里$+$、$\cdot$分别是$\mathscr{M}(n; R)$上的矩阵加法运算和矩阵乘法运算，它就是具有两个二元运算的代数系统。

代数系统是一个相当一般的概念。我们不妨看如下的例子。

例6 玻璃有透明和彩色之分，设$A=\{$透明，彩色$\}$，在A上定义一个二元运算$*$，它表示两种玻璃的叠合，那么，二元运算$*$便可用表1.5来描述。

表 1.5

*	透　明	彩　色
透　明	透　明	彩　色
彩　色	彩　色	彩　色

在这个代数系统（{透明，彩色}，*）中，二元运算*是可交换的，并且也是可结合的。在此代数系统中，彩色和透明分别是关于运算*的零元和幺元。

人们还可以去构造各种各样的代数系统，因此，代数系统有着极为广泛的意义，只是人们在平时不太注意罢了。我们经常用到的是实数集合R、整数集合I和复数集合C，在这些集合上都有我们所熟知的加法运算和乘法运算，就可分别构成代数系统$(R, +, \cdot)$、$(I, +, \cdot)$和$(C, +, \cdot)$，显然，它们都是具有两个二元运算的代数系统。这些代数系统都有以下一些共同的运算规律．即对集合中任意的x、y　z，都有

(1)　$x+y=y+x$

　　$x \cdot y=y \cdot x$　　（交换律）

(2)　$(x+y)+z=x+(y+z)$

　　$(x \cdot y) \cdot z=x \cdot (y \cdot z)$　　（结合律）

(3)　$x \cdot (y+z)=x　y+x \cdot z$　　（分配律）

今后，我们把那些具有运算个数相等以及基本运算规律也相同的代数系统称为同类型的代数系统．

子代数系统

设有一个代数系统$(A, f_1, f_2, \cdots, f_n)$，如果$B \subseteq A$，而且运算$f_1$，$f_2$，…，$f_n$在$B$上也是封闭的，那么，代数系统

$(B, f_1, f_2, \cdots, f_n)$就称为$(A, f_1, f_2, \cdots, f_n)$的子代数系统。

例如，实数集合R是复数集合C的子集，而任意两个实数之间的加法和乘法运算可以看作是两个虚部均为零的复数之间的加法和乘法运算，因此，$(R, +, \cdot)$是$(C, +, \cdot)$的子代数系统。

§4 同构与同态

这一节将讨论两个代数系统之间的两种重要关系。

同构

设$(S, \bigstar)$和$(T, \circ)$是两个代数系统，$\bigstar$和$\circ$分别是S和T上的二元运算。设f是从S到T的一个双射（即一一对应），使得对于任意的$x, y \in S$，都有

$$f(x \bigstar y) = f(x) \circ f(y)$$

则称f是从$(S, \bigstar)$到$(T, \circ)$的同构映射。如图1.4所示。称$(S, \bigstar)$与$(T, \circ)$同构，记作$S \cong T$。

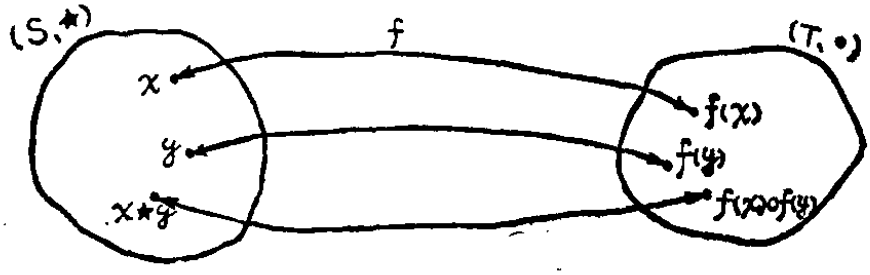


图 1.4

例7 设两个代数系统$(R, +)$和$(R_+, \cdot)$，其中，R是实数集合，$+$是普通加法运算，R_+是正实数集合，$\cdot$是普通乘法运算。定义$R \to R_+$的函数f为：对于每一个

$x \in R$，有

$$f(x)=e^{x}$$

则 f 是从 R 到 R_{+} 的双射，并且对于任意的 x，$y \in R$，有

$$f(x+y)=e^{x+y}=e^{x}\cdot e^{y}=f(x)\cdot f(y)$$

所以，f 是从 R 到 R_{+} 的一个同构映射。f 的逆映射 f^{-1} 为：

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

由于这个同构关系，使我们能够利用对数表来做两个正实数 a 和 b 的乘法运算，即 $z=a\cdot b=e^{\ln(a\cdot b)}=e^{\ln a+\ln b}$，因此，可先查对数表得到 $\ln a$ 和 $\ln b$，将它们相加后的结果再查反对数表，便得 $z=a\cdot b$。这个例子说明了在 R_{+} 中正实数之间的乘法运算，可以利用查对数表并通过加法运算来实现。

例 8 设 $A=\{a, b, c\}$，$B=\{\alpha, \beta, \gamma\}$，在 A 和 B 上分别定义二元运算★和•，如表1.6和表1.7所示。

表 1.6

★	a	b	c
a	a	c	b
b	b	a	b
c	c	b	a

表 1.7

•	α	β	γ
α	α	γ	β
β	β	α	β
γ	γ	β	α

定义一个从 A 到 B 的映射 f，使得

$$f(a)=\alpha,\quad f(b)=\beta,\quad f(c)=\gamma$$

显然，f 是一个从 A 到 B 的双射。由表1.6和表1.7，容易验证