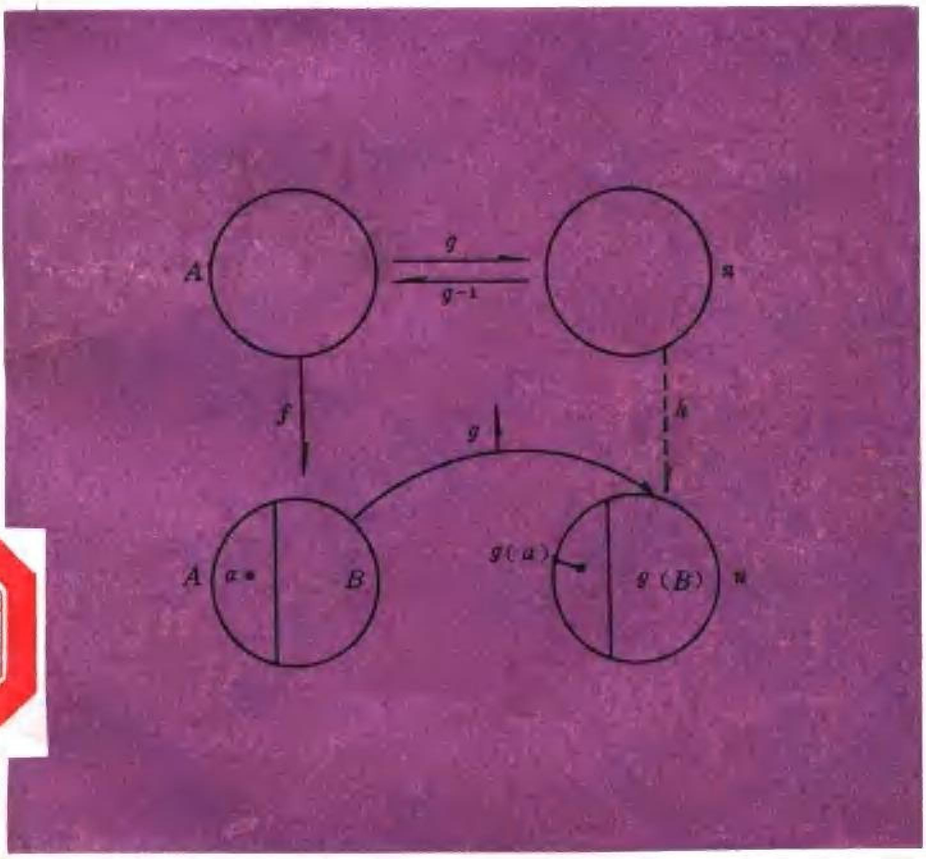
北京市高等教育自学考试用书

离散数学

（下）

陈进元 屈婉玲 编



北京市高等教育自学考试用书

离 散 数 学

（下）

耿素云　方新贵　编

北 京 大 学 出 版 社

内 容 提 要

本书系统地介绍了代数结构和图论的基本内容。包括代数系统、群、环、域、格与布尔代数、图的基本概念、欧拉图、哈密尔顿图、树、平面图等。另外还附有部分习题的提示和解答。

本书适用于自学青年阅读，并且可供高等院校数学专业、计算机专业学生学习参考。

北京市高等教育自学考试用书

离 散 数 学

（下）

耿素云 方新贵 编

责任编辑：王明舟

*

北京大学出版社出版

（北京大学校内）

北京大学印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

850×1168毫米 32开本 9.75印张 244千字

1989年7月第一版 1989年7月第一次印刷

印数：0001—8,000册

ISBN 7-301-00648-9/O·120

定价：2.40元

前　言

为了适应社会主义现代化建设的需要，我国实行了高等教育自学考试制度。它是个人自学、社会助学和国家考试相结合的一种新的教育形式，是我国社会主义高等教育体系的一个组成部分。实行这种高等教育自学考试制度，是实行宪法规定的“鼓励自学成才”的重要措施，也是造就和选拔人才的一种新途径。

参照北京市计算机软件专业自学考试大纲，我们编写了《离散数学》(上、下)。它包括了大纲所要求的内容，选材较为精练，讲解较为详细，书内有大量的例题和习题，书后附有部分习题的提示或解答，便于自学参考。书中一些打有＊号的章节，其内容已超出大纲基本要求，仅作为参考材料提供给读者。

本书各部分内容安排及编者如下：

第一部分：数理逻辑（第1—7章），陈进元编；

第二部分：集合论（第8—12章），屈婉玲编；

第三部分：代数结构（第13—16章），方新贵编；

第四部分：图论（第17—21章），耿素云编。

本书分上、下两册出版。上册包括命题逻辑、谓词逻辑、集合代数、二元关系、函数、集合的基数、公理集合论系统等内容，下册包括代数系统、群、环、域、格与布尔代数、图的基本概念、欧拉图、哈密尔顿图、树、平面等内容。

本书不仅可以作为自学教材，其内容包括了高等院校计算机软件专业本课程所要求的全部内容，因而还可作为高等院校有关专业学生学习参考。

编写这样一部自学教材对我们来说还是初次尝试，可能有不少不妥之处，恳请读者提出批评。

编　者

1986年12月于北京大学计算机系

目　　录

第十三章 代数系统

§1 代数运算

在给出一般的代数运算定义之前先看两个熟悉的例子。

例13.1 用$\boldsymbol{Z}$表示全体整数的集合，考虑$\boldsymbol{Z}$中的普通整数加法运算$+$，则对于$\boldsymbol{Z}$中任意两个数a,b，根据整数加法运算法则，可得到$\boldsymbol{Z}$中唯一的一个整数c作为a加b的结果。我们记$c=a+b$。

例13.2 设$M_n(R)$是全体$n\times n$实矩阵的集合，考虑$M_n(R)$中普通的矩阵乘法，则对于任意两个$n\times n$实矩阵A,B，根据矩阵乘法法则，可得到$M_n(R)$中唯一的一个$n\times n$实矩阵C作为A乘B的结果。我们记$C=AB$。

上述两例虽然是对不同集合给出的不同运算，但它们都具有这样一个共同特点：它们都是某个特定的法则，对于某个特定集合A（上述两例中A分别为$\boldsymbol{Z}$和$M_n(R)$）中的任意一对有序取出的元素，根据这个法则可在A中找到唯一的一个元素与之对应。由此，我们抽象出在一个集合上的二元代数运算概念。

定义13.1 设A是个非空集合，$A^2=A\times A$到A的一个映射（或函数）f：$A^2\to A$称为A的一个**二元代数运算**，也简称为**二元运算**。

由二元运算的概念可得到一般n元运算的概念。

定义13.2 设A是个非空集合，n是正整数。对于$A^n=\underbrace{A\times A\times\cdots\times A}_{n个}$到$A$的一个映射$f$：$A^n\to A$称为$A$的一个**$n$元代数运算**，简称为**$n$元运算**。

对于集合A的一个n元运算f，若$\langle a_1,\cdots,a_n\rangle\in A^n$在$f$下的象是$c$，即$f$：$\langle a_1,\cdots,a_n\rangle\mapsto c$，则记$c=\circ(a_1,\cdots,a_n)$。当$n=2$时，我们常记$c=a_1\circ a_2$。

例13.3 设$A=\left\{1,2,\frac{1}{2}\right\}$。$A$到$A$的映射$f$规定为求倒数，即对于任意$a\in A$，$f$：$a\mapsto\frac{1}{a}$。容易看出$f$是$A$的一元运算，其中$\circ(a)=\frac{1}{a}$。

例13.4 设$A=\{1,2,\cdots,m\}$，m是一个正整数。A^2到A的映射规定为

$$f:\ \langle i,j\rangle\mapsto\max\{i,j\},\quad\forall\langle i,j\rangle\in A^2.$$

则f是A上的一个二元运算，其中$i\circ j=\max\{i,j\}$。

例13.5 设$A=\boldsymbol{Z}$，n是正整数。规定A^n到A的映射为f：$\langle a_1,\cdots,a_n\rangle\mapsto a_1$，对于任意$\langle a_1,\cdots,a_n\rangle\in A^n$。则$f$是$A$的一个$n$元运算。其中$\circ(a_1,\cdots,a_n)=a_1$。

当集合$A=\{a_1,a_2,\cdots a_m\}$是个有限集合时，A上的一元运算、二元运算可以分别通过运算表13.1和13.2给出。

表 13.1

a_i	$\circ(a_i)$
a_1	$\circ(a_1)$
a_2	$\circ(a_2)$
$\vdots$	$\vdots$
a_m	$\circ(a_m)$

表 13.2

$\circ$	a_1	a_2	$\cdots$	a_m
a_1	$a_1\circ a_1$	$a_1\circ a_2$	$\cdots$	$a_1\circ a_m$
a_2	$a_2\circ a_1$	$a_2\circ a_2$	$\cdots$	$a_2\circ a_m$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
a_m	$a_m\circ a_1$	$a_m\circ a_2$	$\cdots$	$a_m\circ a_m$

请读者自己列出例13.3和例13.4的运算表。

下面讨论二元运算的一些简单性质。

定义13.3 设$\circ$是集合A的一个二元运算，如果对于任意a，$b\in A$都有$a\circ b=b\circ a$，则称$\circ$在A上是**可交换的**（或称$\circ$适合**交换律**）。

显然，例13.1和例13.4中的二元运算都是适合交换律的，而例13.2中的二元运算则不适合交换律。

当$\circ$是一个有限集合$A=\{a_1,a_2,\cdots,a_m\}$上的二元运算时，容易看出$\circ$适合交换律的充分必要条件是：$m\times m$矩阵X是对称矩阵，其中

$$X=\begin{pmatrix} a_1\circ a_1 & a_1\circ a_2 & \cdots & a_1\circ a_m \\ a_2\circ a_1 & a_2\circ a_2 & \cdots & a_2\circ a_m \\ \cdots & \cdots & \cdots & \cdots \\ a_m\circ a_1 & a_m\circ a_2 & \cdots & a_m\circ a_m \end{pmatrix}.$$

定义13.4 设$\circ$是集合A的一个二元运算，如果对于任意a，$b,c\in A$都有

$$a\circ(b\circ c)=(a\circ b)\circ c,$$

则称$\circ$在A上是**可结合的**（或称$\circ$适合**结合律**）。

不难看出例13.1，例13.2和例13.4都适合结合律。

例13.6 设$\mathbf{Q}$是全体有理数的集合，规定$\mathbf{Q}^2$到$\mathbf{Q}$映射f：$\langle q_1,q_2\rangle\mapsto q_1$，对于任意$\langle q_1,q_2\rangle\in\mathbf{Q}^2$。则$f$是$A$上的一个二元运算。对于任意$q_1,q_2,q_3\in\mathbf{Q}$，因为

$$(q_1\circ q_2)\circ q_3=q_1,\quad q_1\circ(q_2\circ q_3)=q_1,$$

所以$\circ$也适合结合律。

若A上的二元运算$\circ$适合结合律，则我们常用$a\circ b\circ c$来表示$a\circ(b\circ c)=(a\circ b)\circ c$这个结果。

进一步，把结合律推广到任意多个元素的情形，得到

定义13.5 设$\circ$是A的一个二元运算，$n=2,3,\cdots$。如果对于A中任意n个元素$a_1,a_2,\cdots,a_n$，在$a_1\circ a_2\cdots\circ a_n$中任意加括号进行运算所得的结果都一样，则称$\circ$是**广义可结合的**（或称$\circ$

适合广义结合律)。我们通常用没有括号的 $a_1\circ a_2\circ\cdots\circ a_n$ 来表示这个结果。

若二元运算 $\circ$ 适合广义结合律，则 $\circ$ 一定适合结合律。反之我们有

定理13.1 若二元运算 $\circ$ 适合结合律，则 $\circ$ 适合广义结合律。

证明 设 $a_1,a_2,\cdots,a_n$ 是 A 中任意 n 个元素，我们对 $a_1\circ a_2\circ\cdots\circ a_n$ 按次序由左到右加括号先得到一个特殊运算结果

$$c=((\cdots(((a_1\circ a_2)\circ a_3)\circ a_4)\circ\cdots)\circ a_{n-1})\circ a_n.$$

下面只要证明在 $a_1\circ a_2\circ\cdots\circ a_n$ 中任意加括号进行运算的结果都与 c 相等。我们对 n 用数学归纳法。

$n=2$，$\circ$ 适合 $a_1\circ a_2=a_1\circ a_2$，结论真。设小于 n 时结论真，考察 n 时的情形。对于 $a_1\circ a_2\circ\cdots\circ a_n$，设任意取定的一种加括号方式后所得的运算结果是 c'，求证 $c'=c$。不妨设 c' 的最后一次计算是在 α,β 两部分之间进行的，即 $c'=\alpha\circ\beta$。由于 β 中出现的元素个数少于 n，由归纳所设可知 $\beta=(\cdots)\circ a_n$。由此得到 $c'=\alpha\circ((\cdots)\circ a_n)$。由 $\circ$ 适合结合律又有 $c'=(\alpha\circ(\cdots))\circ a_n$。注意到 $\alpha\circ(\cdots)$ 中元素个数少于 n，再由归纳所设可知

$$\alpha\circ(\cdots)=(\cdots((a_1\circ a_2)\circ a_3)\circ\cdots)\circ a_{n-1}.$$

最后得到

$$c'=((\cdots((a_1\circ a_2)\circ a_3)\circ\cdots)\circ a_{n-1})\circ a_n=c. \quad \blacksquare$$

设 $\circ$ 是 A 的一个适合结合律的二元运算，由定理13.1得知 $\circ$ 适合广义结合律。于是对于任意 $a\in A$ 和正整数 n，表达式 $\underbrace{a\circ a\circ\cdots\circ a}_{n\text{个}}$ 有意义。我们规定

$$a^1=a,\ a^{n+1}=a^n\circ a\ (n=1,2,\cdots).$$

称 a^n 是 a 的 n 次幂，并称 n 为 a 的**指数**。对于正整数 m，n，这时有

$$a^m\circ a^n=a^{m+n},\ (a^m)^n=a^{mn}.$$

这两个结论的证明是简单的，请读者自行验证。

定义13.6 设$\oplus$，$\circ$是集合A上的两个二元运算，如果对于任意$a,b,c\in A$，有

$$a\circ(b\oplus c)=(a\circ b)\oplus(a\circ c), \quad (1)$$

$$(b\oplus c)\circ a=(b\circ a)\oplus(c\circ a), \quad (2)$$

则称$\circ$对于$\oplus$是**分配的**（或$\circ$对于$\oplus$适合**分配律**）。若上述两式分别只有（1）或（2）式成立，这时我们也分别称$\circ$对于$\oplus$适合**左分配律**或**右分配律**。

例如，在$M_n(R)$中分别取二元运算$+$，$\circ$为矩阵的加法和乘法，则$\circ$对于$+$适合分配律。

应该指出，对于一些算律的验证（如结合律）经常是十分困难的。这只能对于具体对象进行讨论。

另外，对于集合A上的一个n元运算$\circ$，我们也常说成A对于运算$\circ$是**封闭的**。

§2 代数系统

定义13.7 设A是一个非空集合，$\circ_1,\circ_2,\cdots,\circ_r$分别是$A$的$k_1,k_2,\cdots,k_r$元运算，$k_i$是正整数，$i=1,2,\cdots,r$。称集合$A$和运算$\circ_1,\circ_2,\cdots,\circ_r$所组成的系统为一个**代数系统**，用记号$\langle A;\circ_1,\cdots,\circ_r\rangle$来表示这个代数系统。当$A$是有限集合时，也称该系统是个**有限代数系统**。

例13.7 设B是一个集合，$A=P(B)$。在A中考虑集合的求补$\sim$，求并$\cup$和求交$\cap$运算，则它们是A上的代数运算（其中求补是一元运算，求并和交是二元运算）。于是$\langle P(B);\cup,\cap,\sim\rangle$构成一个代数系统，该系统也称为**集合代数**。

例13.8 用$\boldsymbol{R}^*$表示全体非零实数的集合，在$\boldsymbol{R}^*$中定义二元运算$\circ$为$a\circ b=a$，对于任意$a,b\in\boldsymbol{R}^*$。则$\langle\boldsymbol{R}^*;\circ\rangle$是一个代数系统。

例13.9 设 $A=\{a,b\}$，A 上的二元运算 $+$ 和 $\circ$ 分别由表13.3和13.4给出，

表 13.3

$+$	a	b
a	a	b
b	b	a

表 13.4

$\circ$	a	b
a	a	a
b	a	a

于是得到一个有限代数系统 $\langle\{a,b\};+,\circ\rangle$。

由代数系统的定义可知，一个代数系统是由一个非空集合和该集合上的若干个代数运算相结合而成的。集合和代数运算是一个代数系统的两要素，缺一不可。

下面着重讨论两个代数系统之间的关系。

定义13.8 设 $V_1=\langle A;\circ_1,\cdots,\circ_r\rangle$ 和 $V_2=\langle B;\bar{\circ}_1,\cdots,\bar{\circ}_r\rangle$ 是两个代数系统。若 $\circ_i$ 和 $\bar{\circ}_i$ 都是 k_i 元运算，$i=1,2,\cdots,r$，则说这两个代数系统是**同类型的**。

例如，在 $M_n(R)$ 中用 $\perp$，$+$，$\bullet$ 分别表示求转置，矩阵加法和矩阵乘法的代数运算，则代数系统 $\langle M_n(R);+,\bullet,\perp\rangle$ 和集合代数 $\langle P(B);\cup,\cap,\sim\rangle$ 是同类型的。

例13.10 设 $B=\{0,1\}$，B 中的代数运算 $\oplus$，$\otimes$ 分别由表13.5和表13.6给出，

表 13.5

$\oplus$	0	1
0	0	1
1	1	0

表 13.6

$\otimes$	0	1
0	0	0
1	0	0

于是得到代数系统 $\langle\{0,1\};\oplus,\otimes\rangle$。我们令 V_1 和 V_2 分别是例

13.9和例13.10所给出的两个代数系统，则 V_1 和 V_2 是同类型的。进一步考察 V_1,V_2 的运算表将会发现：只要把 V_1 运算表中的元素 a,b 分别用 0,1 替换，运算符号 $+$，$\circ$ 分别用 $\oplus$，$\otimes$ 替换，则可得到 V_2 的运算表。这表明，只要在 $A=\{a,b\}$ 和 $B=\{0,1\}$ 之间建立一个映射 φ，其中 $\varphi(a)=0$，$\varphi(b)=1$，则对于任意 $x,y\in A$，有

$$\varphi(x+y)=\varphi(x)\oplus\varphi(y),$$

$$\varphi(x\circ y)=\varphi(x)\otimes\varphi(y)$$

成立。即映射 φ 是**保持运算的**。

定义13.9 设 $V_1=\langle A;\circ_1,\circ_2,\cdots,\circ_r\rangle$ 和 $V_2=\langle B;\bar{\circ}_1,\bar{\circ}_2,\cdots,\bar{\circ}_r\rangle$ 是同类型的代数系统，φ 是 A 到 B 的一个映射。对于 k_i 元运算 $(i=1,2,\cdots,r)$，若任意 $\langle x_1,\cdots,x_{k_i}\rangle\in A^{k_i}$，都有 $\varphi(\circ_i(x_1,\cdots,x_{k_i}))=\bar{\circ}_i(\varphi(x_1),\cdots,\varphi(x_{k_i}))$，则称 φ 是 V_1 到 V_2 的一个**同态映射**（或简称为**同态**）。当同态映射 φ 分别是单射，满射和双射时，分别称 φ 是**单同态，满同态**和**同构**。我们用 $V_1\overset{\varphi}{\sim}V_2$ 表示 V_1 到 V_2 的一个满同态，并称 V_2 是 V_1 的一个**同态象**（在映射 φ 的作用下）。我们用 $V_1\overset{\varphi}{\cong}V_2$ 表示 V_1 到 V_2 的同构。

当 V_1,V_2 中的代数运算均为二元运算时，对于映射 φ 判断是否是 V_1 到 V_2 的同态，只要对于任意 $a,b\in A$，考察

$$\varphi(a\circ_i b)=\varphi(a)\bar{\circ}_i\varphi(b)\quad(i=1,2,\cdots,r)$$

是否成立。

例13.11 设 $V_1=\langle M_n(\boldsymbol{R});\cdot\rangle$，$V_2=\langle \boldsymbol{R};\times\rangle$，$V_1,V_2$ 中的代数运算分别是矩阵的乘法和数的乘法。建立 $M_n(R)$ 到 $\boldsymbol{R}$ 的映射

$$\varphi:\ X\mapsto \det X\text{①},\quad \forall X\in M_n(R).$$

由行列式性质容易知道，对于任意 $X,Y\in M_n(R)$，有

$$\varphi(X\cdot Y)=\det X\cdot Y=\det X\times\det Y=\varphi(X)\times\varphi(Y).$$

于是 φ 是 V_1 到 V_2 的同态映射。注意到 φ 是满射而不是单射，故 φ 是一个满同态而不是一个同构。

---

① $\det A$ 表示 A 的行列式 $|A|$。

当代数系统 $V_1=V_2$ 时，则对于 V_1 到自身的同态和同构分别称为 V_1 的**自同态**和**自同构**。

例13.12 设 $\boldsymbol{Z}^+$ 表示全体正整数的集合，对于数的加法运算 $+$ 可得到代数系统 $V=\langle \boldsymbol{Z}^+;+\rangle$。设 φ 是 $\boldsymbol{Z}^+$ 到 $\boldsymbol{Z}^+$ 的恒等映射，即任意 $a\in \boldsymbol{Z}^+$，$\varphi(a)=a$，则 V 的自同构只有 φ。

证明 恒等映射 φ 显然是 $\boldsymbol{Z}^+$ 到 $\boldsymbol{Z}^+$ 的双射。对于任意 a，$b\in \boldsymbol{Z}^+$，有

$$\varphi(a+b)=a+b=\varphi(a)+\varphi(b)$$

于是 φ 是 V 的一个自同构。

设 ψ 是 V 的任一个自同构，并设 $\psi(i)=1, i\in \boldsymbol{Z}^+$。若 $i\neq 1$，则

$$i=\underbrace{1+1+\cdots+1}_{i\text{ 个}}.$$

于是由 ψ 是同构条件得知 $\psi(i)=i\psi(1)=1$. 由 $\psi(1)\in \boldsymbol{Z}^+$ 和 $i>1$，得到矛盾。从而只有 $\psi(1)=1$。于是，对于任意 $n\in \boldsymbol{Z}^+$，有

$$\psi(n)=\psi(\underbrace{1+1+\cdots+1}_{n\text{ 个}})=n\psi(1)=n.$$

即 ψ 是恒等映射。

定理13.2 设 φ 是代数系统 $V_1=\langle A;\circ_1,\cdots,\circ_r\rangle$ 到代数系统 $V_2=\langle B;\overline{\circ}_1,\cdots,\overline{\circ}_r\rangle$ 的满同态映射，又设 $\circ_i$ 是二元运算，那么

1) 若 $\circ_i$ 适合交换律，则 $\overline{\circ}_i$ 也适合交换律；

2) 若 $\circ_i$ 适合结合律，则 $\overline{\circ}_i$ 也适合结合律；

3) 若 $\circ_j$ 也是二元运算，并且 $\circ_i$ 对于 $\circ_j$ 是可分配的，则 $\overline{\circ}_j$ 也是二元运算，并且 $\overline{\circ}_i$ 对于 $\overline{\circ}_j$ 是可分配的。

证明 我们仅对第一条结论进行证明。其余两条留为习题。

1) 对于 B 中任意两个元素 b_1,b_2，由 φ 是满射可知，存在 a_1，$a_2\in A$，使得

$$\varphi(a_1)=b_1,\varphi(a_2)=b_2,$$

又根据 φ 是同态以及 $\circ_i$ 适合交换律，得到

$$\begin{aligned} b_1 \overline{\circ}_i b_2 &= \varphi(a_1) \overline{\circ}_i \varphi(a_2) = \varphi(a_1 \circ_i a_2) \\ &= \varphi(a_2 \circ_i a_1) = \varphi(a_2) \overline{\circ}_i \varphi(a_1) \\ &= b_2 \circ_i b_1. \end{aligned}$$

即 $\overline{\circ}_i$ 适合交换律。▌

定理13.2的结论表明，一个代数系统 V_1 中的二元运算适合的一些特殊算律(在这里指交换律，结合律和分配律)，则 V_1 的同态象 V_2 中相应的二元运算也适合这些算律。

以上仅对一般的代数系统之间的同态和同构概念进行了一个简单介绍。以后，我们还要对一些特殊的代数系统讨论同态和同构的问题。请读者注意：只有两个同类型的代数系统之间才可能考虑同态问题，同态的两要素是映射和保持运算(对系统的各个代数运算)。

§3 单位元、零元、逆元

在本节所讨论的代数系统都是只有一个二元运算 $\circ$ 的代数系统。

定义13.10 对于代数系统 $V=\langle A;\circ\rangle$，如果存在一个元素 e_l(或者 e_r)$\in A$，使得对于 A 中任意一个元素 a，有

$$e_l \circ a = a(\text{或 } a \circ e_r = a),$$

则称 e_l(或 e_r)是 A 上关于运算 $\circ$ 的一个**左(或右)单位元**；若 e 既是一个左单位元又是右单位元，则称 e 是 A 上关于运算 $\circ$ 的一个**单位元**。我们也分别简称 e_l,e_r 和 e 是一个左单位元，右单位元和单位元。①

例如，在例13.8中的代数系统 $V=\langle \boldsymbol{R}^*;\circ\rangle$ 中无左单位元，而 $\boldsymbol{R}^*$ 中的任意一个元素都是右单位元。在例13.11中所给出的

① 有时也称左，右单位元和单位元是左，右幺元和幺元。

两个代数系统 V_1, V_2，它们分别有唯一的单位元 E（n 阶单位矩阵）和 1。

定理13.3 若代数系统 $V=\langle A;\circ\rangle$ 分别存在一个左单位元 e_l 和一个右单位元 e_r，则有 $e_l=e_r=e$，并且 e 是 A 中唯一的一个单位元。

证明 由于 e_l 是一个左单位元，于是有

$$e_l\circ e_r=e_r.$$

又由于 e_r 是一个右单位元，于是又有

$$e_l\circ e_r=e_l.$$

从而，

$$e_l\circ e_r=e_r=e_l=e,$$

即 e 是一个单位元。设 e' 是 A 中的任一个单位元，则有

$$e'=e'\circ e=e.$$

由此证明了 A 中的单位元是唯一的。▌

定义13.11 对于代数系统 $V=\langle A;\circ\rangle$，如果存在一个元素 Z_l（或 Z_r）$\in A$，使得对于 A 中任意一个元素 a 都有

$$Z_l\circ a=Z_l(\text{或 } a\circ Z_r=Z_r),$$

则称 Z_l（或 Z_r）是 A 上关于运算 $\circ$ 的一个**左零元**(或**右零元**)；若存在 $Z\in A$ 既是左零元又是右零元，则称 Z 是 A 上关于运算 $\circ$ 的一个**零元**。我们也分别简称 Z_l, Z_r 和 Z 是一个左零元，右零元和零元。

例如，在例13.8中的代数系统里无右零元，且每个元都是左零元。

定理13.4 若代数系统 $V=\langle A;\circ\rangle$ 分别存在一个左零元 Z_l 和右零元 Z_r，则有 $Z_l=Z_r=Z$，并且 Z 是 A 中唯一的一个零元。

该定理的证明与定理13.3的证明相类似，请读者自行完成。

定义13.12 设代数系统 $V=\langle A;\circ\rangle$。对于 $a\in A$，若有

$$a\circ a=a^2=a,$$

则称 a 是 A 上关于运算 $\circ$ 的一个**幂等元**，也简称为**幂等元**。