21世纪 高等学校本科系列教材

总主编　吴中福

高等代数

(5)

蔺大正　陈宝根 编著

重庆大学出版社

高等代数

蔺大正　陈宝根　编　著

重庆大学出版社

内 容 提 要

本书由9章及2个附录组成．第1章是预备知识；第3、4、5、7章是线性代数的基本内容(包括行列式、矩阵、向量组的线性相关性、线性方程组、特征理论、二次型等)；第6章、第8章对线性代数的某些内容做了深入一些的讨论(包括线性空间、线性变换、矩阵标准型等)；第2章、第9章对"近世"代数的对象做了初等介绍(包括多项式、群、环、域及同构等)；每章末附有一些注释与数量不等的习题；附录2为习题答案；附录1是用软件Mathematica作高等代数的要点与编程示例；本书起点较低，信息量及跨度较大，可供一般工科院校计算机专业作为高等代数课教材或非计算机专业作为线性代数教材使用，也可供数学爱好者及广大师生参考6

图书在版编目(CIP)数据

高等代数/蔺大正，陈宝根编著．—重庆：重庆大学出版社，2001.11

计算机科学与技术专业本科系列教材

ISBN 7-5624-2335-0

Ⅰ.高… Ⅱ.①蔺…②陈… Ⅲ 高等代数-高等学校-教材 Ⅳ.015

中国版本图书馆CIP数据核字(2001)第055028号

高 等 代 数

蔺大正 陈宝根 编 著

责任编辑 周 立 彭 宁

*

重庆大学出版社出版发行

新 华 书 店 经 销

重庆大学建大印刷厂印刷

*

开本：787×1092 1/16 印张：12.75 字数：318千

2001年11月第1版 2001年11月第1次印刷

印数：1—5000

ISBN 7-5624-2335-0/O·191 定价：20.00元

前言

现代大学数学教育可分为4块:连续量数学(微积分)、离散量数学(代数)、随机量数学(概率统计)与实验数学(数学实验与数学建模),但由于代数在数学中的特有地位,它与数学中其他科目的关联,它在对计算机学习者的逻辑训练中表现出的卓有成效,使得它在计算机科学相关的专业人才培养中的作用是不可缺少,也是不可被代替的.

为适应信息社会越来越多的对"信息"人才的需求,根据国家教委颁发的《高等工业学校高等数学与线性代数课程教学基本要求》,考虑到面向21世纪计算机与信息科学的特点,我们以长期教学实践为基础,编写了这本起点较低、跨度较大的《高等代数》,以适应当前一般工科院校师生(特别是计算机专业的师生)对高等代数教学的需要.

解线性方程组、求矩阵的特征值与特征向量已成为广大工程技术人员常见的问题.线性代数向高等代数的扩展也常见不鲜,现代控制理论已大量用到矩阵及多项式的各种知识;基于线性代数的线性规划已成为管理科学的不可缺少的必修课,更不用说高等代数与下述分科的紧密联系:计算数学的基础计算方法、数值分析与数值线性代数;近代数学分支的近世(抽象)代数、群论、数论(特别是其中的代数数论,有限域理论已成为近代密码学的基础之一);组合论与图论;计算机科学基础课数据结构;抽象计算机模型(如图灵机、神经网络等);计算机图形学;计算几何(用于飞机汽车等外形设计).这样,高等代数明显地已成为计算机科学软件、硬件专业的学生必不可少的基础课,甚至也成为广大理科、工科、管理学科学生不可缺少的基础课.

在内容取舍方面,本书注意了以下几点:重视基础,讨论了最基本的概念(定义、性质、定理及方法等);略去了某些较繁难的证明;从方法的角度简要地介绍了某些较深刻的内容(如Jordan标准形理论);在各章末的注释中介绍了与各章内容有关的数学对象,以扩展学习者的知识面并增强其想象力;最后联系到当今计算机应用于数学的特点,编写了附录1:用数学软件Mathematica做高等代数的常用语句和程序示例,目的是使学习者的动手能力得到初步训练.希望本书能在对学生素质教育、创新意识和实践能力培养方面发挥一点效果.

从教学角度讲，本书第3，4，5，7章大致可作为30学时《线性代数》课的基本教材；再加上2，6，8，9章就可以作为64学时《高等代数》课教材．而附录1可以作为附加教材，或用于数学实验的教学中，或作为课外科技活动的辅导材料等．各章中介绍了少数较难的问题可作为数学爱好者的研讨参考资料．

本书第2至5章由陈宝根执笔．第1、6至9章及附录1由蔺大正执笔．全书由蔺大正统稿，张文忠审定．希望本书能在高等代数（包括线性代数）的教学中起到积极作用．限于编者水平，有不妥及错漏之处，请读者指正．

编　者

2001.5

目录

第 1 章
预备知识

1.1 整数、有理数、实数与复数

众所周知,在整数范围内可以进行加、减、乘法的运算,但除法不一定能进行.而在有理数、实数或复数范围内,总可以进行加、减、乘、除(除数不为0)四则运算.在代数中把四则运算都能进行的数集称为数域.称有理数集、实数集与复数集为有理数域、实数域与复数域,分别用记号 **Q**、**R**、**C** 表示,而整数集则称为整数环,用记号 **Z** 表示.

除运算外,在计算上整数和有理数是可以精确表示和精确、无误差地计算的.当然,考虑到比如 $\frac{2}{3}=0.666\cdots$ 的左边与右边的差别,等式左边的 $\frac{2}{3}$ 是精确的,而等式右边的 0.666 是不精确的.在计算机的浮点实数的表示中,它只能是 0.666 7 或 0.666 667 等.尽管 $0.666\cdots$ 在人们的感觉是留下一个"无限下去是精确的"这样一种理念,或者以无穷级数中取 $\sum_{k=1}^{\infty}\frac{6}{10^k}$ 这一类无穷级数表达式,但这已与无误差计算有大的差异了.无误差的计算,实际是进行有限次的某种规则的变换,不能"无限"地进行下去.当然,对于实数和复数,情况比上面更坏,比如 $\sqrt{2}$ 可以用方程 $x^2-2=0$ 的惟一正根加以规定,但人们对它的(无限不循环的)小数表示 $\sqrt{2}=1.414\,213\,562\cdots$ 能有一个什么样的想像呢?

整数中最基本的是自然数集 $\{1,2,3,\cdots\}$,常记为 **N**. 自然数中加法可以通行无阻,但减法则不行:$1-1,1-2$ 不是自然数,为了减法的通行,人们定义出 0 与负整数及自然数,一起合称整数.自然数中的 1 是最基本的.一方面任一个自然数可以由 1 进行有限次加法加出来 $\underbrace{n=1+1\cdots+1}_{n\text{次}}$,另一方面,任意自然数与 1 之积仍是这个自然数,1 是自然数的单位.

讨论自然数的乘法性质时,或者在小学中学习分数的约分、通分时,自然要涉及到整除、因子(约数,因数)、倍数、最大公因子、最小公倍数、素数(质数)等一系列概念.

整数的表示法中,下列命题是基本的:

命题 设给定自然数 $m>1$,则任一自然数可写为下列形式:

$$n=a_km^k+a_{k-1}m^{k-1}+\cdots+a_1m+a_0$$

其中 k 是一个非负整数,a_i 是满足 $0\leqslant a_i\leqslant m-1$ 的整数,$i=0,1,2,\cdots,k$,且 $a_k\neq 0$.

常常将上式简记为 $n=(a_ka_{k-1}\cdots a_1a_0)_m$,称为整数 n 的 m 进位制表示,当 $m=10$ 时,即通常用的 10 进位制,此时 m 常省略不写,记成 $n=a_ka_{k-1}\cdots a_1a_0$.

例 1 $59 = 5 \times 10 + 9$,求 59 的二进制表示 .

解 $59 = 32 + 27 =$

$32 + 16 + 11 =$

$32 + 16 + 8 + 3 =$

$32 + 16 + 8 + 2 + 1 =$

$2^5 + 2^4 + 2^3 + 0 \times 2^2 + 2 + 1 =$

$(111011)_2$.

带余除法,即如果用一个自然数 m 除一个整数 n,必有下式成立

$$n = qm + r$$

其中 q 为整数,$0 \leqslant r \leqslant m - 1$,式中的 r 称为余数 . 余数为 0 时,称 m 整除 n(或 n 可被 m 整除),记为 $m \mid n$. 也称 n 是 m 的一个倍数 . 当 $r \neq 0$ 时,称 m 不整除 n(或 n 不能被 m 整除,m 不是 n 的因子,n 不是 m 的倍数).

若 a 是 b 与 c 的因子,就称 a 是 b, c 的公因子 . 公因子中最大的称为最大公因子 . a 是 b, c 的最大公因子,用记号 $a = (b, c)$ 或 $a = \gcd(b, c)$ 等表示(不同的书籍或软件中有不一致的表示). 最大公因子常用短除法(b, c 较小时)及辗转相除法(b, c 较大时及计算机上使用的算法,又名 Euclid 算法)求得 .

例 2 试约分 $\frac{24}{60}$.

解 1

2	24	60
2	12	30
3	6	15
	2	5

故最大公因子 $(24,60) = 2 \times 2 \times 3 = 12$,于是 $\frac{24}{60} = \frac{24 \div 12}{60 \div 12} = \frac{2}{5}$.

解 2 $60 = 2 \times 24 + 12$

$24 = 2 \times 12 + 0$

故 $(24,60) = 12$,因而 $\frac{24}{60} = \frac{24 \div 12}{60 \div 12} = \frac{2}{5}$.

如果两个数的最大公因子是 1,则称这两个数为互素的(互质的). 例如 2 与 5 是互素的 .

若 a 既是 b 的倍数,又是 c 的倍数,a 就称为 b, c 的公倍数 . b, c 的最小定公倍数,称为 b 与 c 的最小公倍数 . 记为 $[b, c]$ 或 $\operatorname{lcm}(a, b)$. 对于自然数 b, c 有等式 $bc = (b, c)[b, c]$.

由一个数的因子的多寡把自然数分为 3 类:

$\{1\}$;

$\{2,3,5,7,11,13,17,19,23,\cdots\}$;

$\{4,6,8,9,10,12,14,15,16,\cdots\}$.

第一类中只有数 1,它只有一个不同的因子 . 第二类中的数称为素数,它恰有两个不同因子:1 和它自身 . 第 3 类中的数有 3 个或 3 个以上的不同因子,称为合数 . 人们常将素数编号

记为 $p_1=2,p_2=3,p_3=5,\cdots$. 但根据上下文,$p_1,p_2,\cdots$也常表示第一个素数,第 2 个素数,…,并不一定指 2,3,…. 比如下列的惟一分解定理就是如此.

定理 1　任一自然数可以写成若干个素数因子之积. 若不计因子的顺序,这个分解是惟一的.

证明　略.

常将这个分解写成标准分解式

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},p_1<p_2<\cdots<p_s,\alpha_i\geqslant 1,i=1,2,\cdots,s.$$

整数与实数常由一个"取整函数"关联起来,这个函数记为$[x]$,定义是

$$[x]=\text{不超过 } x \text{ 的最大整数}.$$

于是,它的定义域是实数集,而值域是整数集. 例如$[\pi]=3,[-\pi]=-4,[3]=3$($[x]$只是这个函数记号之一,后来又有人用记号[x]来表示此函数,在 Basic 程序中,这个函数为 INT(x),在 Mathematica中这个函数为 Floor[x],…).

从整数发展到有理数形式上的办法是定义商$\frac{a}{b}$或二元组$(a,b),b\neq 0$,其中 a,b 均为整数. 用如下定义的等价关系对(a,b)进行分类:

$$(a,b)=(c,d)\text{ 当且仅当 }ad=bc.$$

$$(a,b)+(c,d)=(ad+bc,bd),(a,b)(c,d)=(ac,bd).$$

等价类中的数认为是相同的. 等价类中的代表(a,b)(实际上可视为既约分数或最简分数$\frac{a}{b}$)与加法、乘法运算就构成了有理数域. 可以验知,它们也满足整数环上的运算性质,并且使除法也能进行运算(当 $c\neq 0$ 时,定义$(a,b)\div(c,d)=(ad,bc)$).

从有理数域到实数域的扩张主要是通过添加方程的根来实现的. 如添加$\sqrt{2}$($x^2-2=0$ 的根)到有理数域中,形成一类新的实数的例子. 设 a,b 为有理数,则可以验证:

集合

$$\{a+b\sqrt{2}\mid a,b\in \boldsymbol{Q}\}$$

满足四则运算(除数不为零),且满足与有理数运算大致相同的运算性质.

从实数到复数的扩张可以看成是实数域上添加方程 $x^2+1=0$ 的根$\sqrt{-1}$得到的.

即

$$\boldsymbol{C}=\{a+b\sqrt{-1}\mid a,b\in \boldsymbol{R}\}$$

还有一种不常见的域:复有理域,即

$$C_Q=\{a+b\sqrt{-1}\mid a,b\in \boldsymbol{Q}\}$$

这些内容在代数的域扩张理论中有详尽阐述,这里不过是写出这些精细概念的一个简单说明,希望读者有一个简易通俗的了解而已.

1.2　数组、下标、和号与积号

计算机科学中的一维数组,对应于一个有限数列. 常记为

$$x=\{x_1,x_2,\cdots,x_n\}=\{x_k\}_{k=1}^n$$

这个数组中包含了 n 个元素. $x_1,x_2,\cdots,x_n$ 分别称为数组 x 的第一个元素,第二个元素,

…,第 n 个元素;1,2,…,n 分别称为元素 $x_1, x_2, \cdots, x_n$ 的下标,它标明了对应元素在 x 中的位置.下标在数学上常用右下角较小的数字表示.而在不同程序设计语言中数组常表示为 $x(1), x(2), \cdots, x(n)$,或 $x[1], x[2], \cdots, x[n]$,甚至 $x[[1]], x[[2]], \cdots, x[[n]]$等.

记号 $\{x_k\}_{k=1}^{n}$ 实际上使用了一种"活动下标"记法.k 称为活动的下标,表示 x_k 中的 k 从 1(通过 1 与 n 之间的所有整数)变到 n. x_k 也称为数组的一般项或通项.如果有一解析表达式把数组的一般项表示出来,例如 $x_k = k^2$,则数组 x 实际上就是

$$x = \{1, 4, 9, \cdots, n^2\} = \{k^2\}_{k=1}^{n}$$

这个命题的逆命题比较麻烦.习惯约定:例如一个 100 元数组 $x = \{1, 3, 5, 7, \cdots, 199\}$,把中间省略的元素理解成 9,11,13,…,197 等.其二是很多情况下求这个通项公式并不容易.当然,当前的问题并不难,可以写 $x = \{2k-1\}_{k=1}^{100}$.其三是这个通项公式不是惟一的,是随下标的写法"可平移的".例如,也可写

$$x = \{2k+1\}_{k=0}^{99} = \{2k+3\}_{k=-1}^{98}$$

等.它们其实与 $x = \{2k-1\}_{k=1}^{100}$ 是同一个数组.最后,活动下标可选用不同的字母.例如上面的 x 还可写成

$$x = \{2m+1\}_{m=0}^{99} = \{2n+3\}_{n=-1}^{98}$$

等.经常用于作活动下标的字母有 i, j, k, l, m, n 等.经常用于起点的值(常称为下标基)是 1 和 0.当下标从 0 变化到 n 时,数组的元素有 $n+1$ 个.

将数组与向量联系起来,此时,数组的元素对应于向量的"分量".

作为二维数组的例子,可举出小学算术中的九九表

$$\begin{aligned}
&1\times1=1,\quad 1\times2=2,\quad 1\times3=3,\quad \cdots,\quad 1\times9=9,\\
&2\times1=2,\quad 2\times2=4,\quad 2\times3=6,\quad \cdots,\quad 2\times9=18,\\
&\cdots\cdots\\
&9\times1=9,\quad 9\times2=18,\quad 9\times3=27,\quad \cdots,\quad 9\times9=81.
\end{aligned}$$

及著名的杨辉三角(外国书籍也称为 Pascal 三角)

$$\begin{array}{c}
1\\
1\quad 1\\
1\quad 2\quad 1\\
1\quad 3\quad 3\quad 1\\
1\quad 4\quad 6\quad 4\quad 1\\
1\quad 5\quad 10\quad 10\quad 5\quad 1
\end{array}$$

为例.第一个数组(略去"="号及等式左端)可写成

$$\{i\cdot j\}_{i=1,2,\cdots,9,j=1,2,\cdots,9} \text{或} \{i\cdot j\}_{\substack{1\leqslant i\leqslant 9\\ 1\leqslant j\leqslant 9}}.$$

这可与矩阵联系起来,它是一个矩形(方形)数组.第二个数组可写成

$$\{C_n^m\}_{n=0,\cdots,5,m=0,\cdots,n}.$$

其中 $C_n^m = \dfrac{n!}{m!\,(n-m)!} = \binom{n}{m}$ 是二项式系数(或从 n 件不同事物中取 m 件的方法数、组合数),它是一个三角形的数组.

当变下标的上限是 ∞ 时,一维数组与二维数组就变得与"无穷数列"和"二重无穷数列"(或

“无穷方阵”)相似．这样的数组,相当于一个自变量在 x 轴的正(非负)整数点上取值的函数或在(x,y)平面上第一象限整点上取值的函数．

把二维矩形数组排成一维,常采用字典顺序,如 $\{a_{ij}\}_{\substack{1\leqslant i\leqslant 2\\ 1\leqslant j\leqslant 3}}$ 数组可排成一维数组$\{a_{11},a_{12},a_{13},a_{21},a_{22},a_{23}\}$,把一维数组记为$\{c_1,c_2,c_3,c_4,c_5,c_6\}$,容易给出这个一维数组的第 k 个元素 C_k 与原矩形数组的(i,j)元 a_{ij}的关系和逆关系．

介绍三角形数组下标转换的一个结论:

引理　当 m 及 n 经过各自然数时

$$k=m+\frac{1}{2}(m+n-1)(m+n-2)$$

亦经过所有自然数,无重复也无遗漏．

如果要证明这个引理,只要把(m,n)的值列在平面的整点上给出示意,就可将证明写出.

n \ m	1	2	3	4	5	6	…
1	(1,1) 1	(1,2) 2	(1,3) 4	(1,4) 7	(1,5) 11	(1,6) 16	…
2	(2,1) 3	(2,2) 5	(2,3) 8	(2,4) 12	(2,5) 17	(2,6) 23	…
3	(3,1) 6	(3,2) 9	(3,3) 13	(3,4) 18	(3,5) 24	(3,6) 31	…
4	(4,1) 10	(4,2) 14	(4,3) 19	(4,4) 25	(4,5) 32	(4,6) 40	…
5	(5,1) 15	(5,2) 20	(5,3) 26	(5,4) 33	(5,5) 41	(5,6) 50	…
6	(6,1) 21	(6,2) 27	(6,3) 34	(6,4) 42	(6,5) 51	(6,6) 61	…
…	…	…	…	…	…	…	…

这里,值得注意的是,不只是任给一组确定的(m,n),可算出 k(也易算出 k);反之,给出自然数 k,也可以由此公式确定惟一的(m,n)(如何计算?).

结论 1　给定三角形二维数组$\{x_{mn}\}_{1\leqslant m\leqslant M,1\leqslant n\leqslant m}$,可以排成一维数组$\{y_k\}_{1\leqslant k\leqslant \frac{M(M+1)}{2}}$,使 $y_k=x_{mn}$,取引理中的 k 的算法也得出这种排法．

结论 2　任给数组$\{y_k\}_{1\leqslant k\leqslant \frac{M(M+1)}{2}}$,可将其数组排列成二维三角形数组$\{x_{mn}\}_{m=1,2,\cdots,M;n=1,2,\cdots,m}$,结论 2 仍依赖于引理,由 k 求(m,n)的计算方法希望读者自己写出．

至于三维和三维以上的数组,这里不再介绍,读者可以自己思考它们的形状和各种排列形式.

连加和式常常有初等写法及和号写法．有限和式及无限和式大致相当于有限数列与无限数列的求和(后者常理解为无穷级数或形式级数等概念),定义如下:

$$\sum_{k=1}^{n}a_k=a_1+a_2+\cdots+a_k+\cdots+a_n;$$

$$\sum_{k=1}^{\infty}a_k=a_1+a_2+\cdots+a_k+\cdots.$$

这里 k 称为求和变量,和式的性质有点像定积分的性质:

①
$$\sum_{k=1}^{n}a_k=\sum_{m=1}^{n}a_m$$

和式的值与求和变量无关,相应于定积分中的积分值与积分变量无关:

$$\int_a^b f(x)\mathrm{d}x=\int_a^b f(t)\mathrm{d}t.$$

② $$\sum_{k=1}^{n} a_k \overset{k=m+1}{=} \sum_{m=0}^{n-1} a_{m+1}$$

对和式的求和变量可进行“平移”，相应于定积分中可对自变量进行平移变换：

$$\int_a^b f(x)\mathrm{d}x \overset{x=t+c}{=} \int_{a-c}^{b-c} f(t+c)\mathrm{d}t$$

③ $$\sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$$

相应于 $\int_a^b (f(x) + g(x))\mathrm{d}x = \int_a^b f(x)\mathrm{d}x + \int_a^b g(x)\mathrm{d}x$

④ $$\sum_{k=1}^{n}(ca_k) = c\sum_{k=1}^{n} a_k$$

相应于 $\int_a^b cf(x)\mathrm{d}x = c\int_a^b f(x)\mathrm{d}x$

对应于二维数组，有一重和式与二重和式的以下定义：

$$\sum_{i=1}^{n} a_{ij} = a_{1j} + a_{2j} + \cdots + a_{nj}.$$

$$\sum_{j=1}^{n} a_{ij} = a_{i1} + a_{i2} + \cdots + a_{in}.$$

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} = \sum_{i=1}^{m}(a_{i1} + a_{i2} + \cdots + a_{in}) =$$

$$a_{11} + a_{12} + \cdots + a_{1n} +$$

$$a_{21} + a_{22} + \cdots + a_{2n} +$$

$$\cdots +$$

$$a_{m1} + a_{m2} + \cdots + a_{mn} =$$

$$\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\text{（当 } m = n \text{ 时，此和式也可写成 } \sum_{i,j=1}^{n} a_{ij}\text{）}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{i} a_{ij} = \sum_{i=1}^{n}(a_{i1} + a_{i2} + \cdots + a_{ii}) =$$

$$a_{11} +$$

$$a_{21} + a_{22} +$$

$$a_{31} + a_{32} + a_{33} +$$

$$\cdots +$$

$$a_{n1} + a_{n2} + a_{n3} + \cdots + a_{nn}$$

$$\sum_{i=1}^{n}\sum_{j=i}^{n} a_{ij} = \sum_{i=1}^{n}(a_{ii} + a_{i,i+1} + \cdots + a_{in}) =$$

$$a_{11} + a_{12} + \cdots + a_{1n} +$$

$$a_{22} + \cdots + a_{2n} +$$

$$\cdots +$$

$$a_{nn}$$

二重和式也有与某些特定区域上的二重积分类似的性质，包括和式交换顺序也是这样．

如,你能(用定义)证明 $\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}=\sum_{j=1}^{n}\sum_{i=1}^{n}a_{ij}$ 吗?

有时和号中也有些隐含或省略.如

$$\sum_{i+j=3}a_ib_j=a_0b_3+a_1b_2+a_2b_1+a_3b_0$$

省略了 $0\leqslant i\leqslant 3,0\leqslant j\leqslant 3$. 又如

$$\sum_{i+j+k=3}a_ib_jc_k=a_0b_0c_3+a_0b_1c_2+a_0b_2c_1+a_1b_0c_2+a_1b_1c_1+a_1b_2c_0+a_2b_0c_1+a_2b_1c_0+a_3b_0c_0$$

实际上也是一个多重和式.

连乘积的记号 $\prod$ 的定义与用法与和式类似,只要将其中的加号"+"换为乘号"·"即得.

例 3

$$\prod_{1\leqslant i<j\leqslant 4}(x_j-x_i)=\prod_{i=1}^{3}\prod_{j=i+1}^{4}(x_j-x_i)=\prod_{i=1}^{3}(x_{i+1}-x_i)(x_{i+2}-x_i)\cdots(x_4-x_i)=(x_2-x_1)(x_3-x_1)(x_4-x_1)(x_3-x_2)(x_4-x_2)(x_4-x_3)$$

一般地 $\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)=\prod_{i=1}^{n-1}\prod_{j=i+1}^{n}(x_j-x_i)$,是双重乘积写成单重乘积的简记法.它表示对所有满足条件 $1\leqslant i<j\leqslant n$ 的下标对 (i,j) 求其积.

1.3　集合、映射与代数运算

对于最常见的集合,简单地用一个大写字母加以表示.如 $\boldsymbol{N},\boldsymbol{Z},\boldsymbol{Q},\boldsymbol{R},\boldsymbol{C}$ 分别表示自然数集、整数集、有理数集、实数集和复数集.借助列表与自然想象,有时也可表示一些常见的集合:

$A=\{2,4,6,\cdots,100\}$,不超过 100 的偶自然数集

$B=\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots\}$,所有自然数的倒数所成的集合(或数列)

等.不过这种表述不如描述性来得确切.如上两个例中的集合可写为

$A=\{x=2n\mid n\in N,n\leqslant 50\}$ 或 $\{2n\mid n\in N,n\leqslant 50\}$

$B=\left\{\frac{1}{n}\mid n\in N\right\}$

这种描述性的表示还可以表述更复杂的集合.例如

$P_c=\{(x,y)\mid x^2+y^2<1,x,y\in R\}$——单位圆内的所有点的集合

$L=\{Ax+By+C=0\mid A,B,C\in R,A^2+B^2\neq 0\}$——平面上所有直线的集合

等.离开集合中元素的性质去考查集合的性质照理说应当不大可能.整数集 $\boldsymbol{Z}$,已经包含了

它中间元素的有序性、可加性、可积性，甚至包含了数论中各种定理所描述整数的性质．用记号$\{Z,+,\cdot\}$表示整数环(有时乘号"·"也可省略)，此表示中的Z，不考虑加法与乘法，可以理解为是为了强调集合与其中运算的显著关系(而暂不考虑其他关系)而采用的一种手法．

一个集合中既有代数结构又有拓扑结构．代数结构主要考虑集合上定义关系、运算及考察它们的性质．拓扑结构则主要考虑集合中元素与元素之间相互关系，特别是"相互邻近"这种关质．要考虑集合之间的映射(或变换)(映射这一术语就是从几何中借用过来的)，主要考虑保持某种关系的映射及保持某种运算的映射，代数中主要考虑后者．

两个集合之间的映射大致类似于(更推广了)函数的概念．

定义1 设S、T是两个集合．如果有一个确定的法则σ，使对S中每个元素都通过这个法则找到T中一个元素与之对应，就称这个法则σ是S到T的一个映射，记为$\sigma: S\to T$. 对于上述σ，当$a\in S, b\in T$时也写$\sigma(a)=b$，称b为a在σ下的像，a为b(在σ下)的原像．

例4 设$S=\mathbf{R}, T=\mathbf{R}$，这里$\mathbf{R}$是实数集．而$f$是从一个实数计算出另一实数的计算规则，则$f:\mathbf{R}\to\mathbf{R}$是一个映射．这种映射称为实变函数．

例5 设$S=\mathbf{C}, T=\mathbf{C}$，这里$\mathbf{C}$是复数集．而$f$是一个从一个复数计算出另一复数的计算规则，则$f:\mathbf{C}\to\mathbf{C}$是一个映射，这种映射称为复变函数．

例6 设$S=\mathbf{N}, T=\mathbf{R}$，而$f(n)$是由$n$计算出$t_n=f(n)$的计算公式．则$f:\mathbf{N}\to\mathbf{R}$是一个映射．这个映射称为正整变量函数或数列．

例如，泊松分布$P\{X=k\}=\dfrac{\lambda^k}{k!}e^{-\lambda}, k=0,1,2,\cdots$，是一个$\mathbf{N}_0$到$\mathbf{R}$的映射，这里$\mathbf{N}_0=\{0\}\cup\mathbf{N}$.

例7 设S为平面上点$P(x,y)$的集合(记为$\mathbf{R}^2$或$\mathbf{R}\times\mathbf{R}$). $\mathbf{T}=\mathbf{R}$，d是从$P(x,y)$算出$\sqrt{x^2+y^2}$(点P到原点的距离)的算法．则$d:\mathbf{R}^2\to\mathbf{R}$是一个映射．

例8 设$\mathbf{N}$为自然数集，又设$N_2=\{2n\mid n\in\mathbf{N}\}$定义$f(n)=2n$，则$f$是$\mathbf{N}\to N_2$的一个映射．又定义$g(n)=4n$，则$g$也是$\mathbf{N}\to N_2$的一个映射．

在映射下S的像的全体：

$f(S)=\{b\in T\mid$存在$a\in S$，使$f(a)=b\}$，称为像集合．显然$f(S)\subset T$. 如果$f(S)=T$，则映射称为映上的或满射．例8中的f是映上的，而g则不是．例7中的映射d也不是映上的，但如果在例7中将T改为$\mathbf{R}^+\cup\{0\}$(非负实数集合)，则d就是映上的了．

如果不同的元素在映射f下对应不同的像，则映射称为一一映射．例8中的f与g都是一一映射．例7中的d则不是，确定例6中的f是否为一一映射要根据具体情况而定．

如果一个映射$f: S\to T$既是映上的，又是一一映射的，则称f为S到T的一个一一对应．例8中的f是一个一一对应，g不是．对于有限集合S，T而言如果有一一对应关系，则S中元素个数$|S|$与T中元素个数$|T|$相等：$|S|=|T|$；反之，如果$|S|=|T|$，则必然存在一个S到T的一一对应．

代数运算从广泛的意义来讲，可以看成一种映射．

定义2 $S\times T$到U上的一个代数运算，是指一个算法．使对于任意给定的$S\times T$中的一对元素$\{a,b\}(a\in S, b\in T)$，有U中由此算法确定的惟一一个元素与之对应．

经常见到的算法是$S\times T$到S，$S\times T$到T或$S\times S$到S的．

例如，自然数集上定义的加法，就是$\mathbf{N}\times\mathbf{N}$到$\mathbf{N}$的一个映射，因而是一个代数运算．

$$\text{Plus}:\mathbf{N}\times\mathbf{N}\to\mathbf{N}$$

Plus$[a,b]=a+b$ 是加法的定义映射．

从更广泛的意义上讲，映射与运算又是集合上定义的一种“关系”集合．例如 **N** 上的加法可以看成集合：

$$\{\{\{1,1\},2\},\{\{1,2\},3\},\{\{2,1\},3\},\{\{1,3\},4\}\cdots\}$$

这种冗繁的原始归纳，掌握得好，可使某些概念及分类等更加清晰，掌握得不好，或许会导致更多的混乱．故在学习过程中加深对所学概念的深入理解是很有必要的，古人曰：“学而不思则惘”．

运算所用的记号，除常用的“+”、“-”、“×”（也写成“·”或不用符号或 Mathematica 中 Times，某些软件中的甚至用“$\otimes$”）、“÷”（软件或有些文章中常写为“/”）、乘方等外，最大公约数、最小公倍数及其他多种二元函数，向量乘法中的点乘（数量积）、叉乘（向量积）等，都是（二元）运算．求数 a 的绝对值 $|a|$，求一个函数 $f(x)$ 的导数等，则是（一元）运算．

1.4　数学证明与数学归纳法

数学书籍中的定义和定理是非常重要的．定义是数学对象的规定或约定．定理则是数学对象的某些特性的深入发掘．定理具有抽象性、一般性、应用广泛性，也有许多较为容易、特殊的定理．比如性质、推论（由前面的一个定理容易导出的某些结论）、某些命题（有的书中将命题视为未经证明的语句，有的书中将命题视为一些不十分值得提出的定理）、某些引理（通常是定理的证明太长，分为一个一个的小定理来证，这些小定理称为引理；也有由于历史关系，将前人的某些结论作为引理；也有定理的核心部分其实就是一个引理的）、证明性质的习题（许多习题就是课程的历史发展早期的定理）等．

数学定理一般都有条件与结论．假定 P,Q 等都是某些命题．数学定理的一般形式是：如果 P 成立，则 Q 成立．在符号的规定下，某些公式本身就是定理．例如：$3\mid n(n+1)(2n+1)$，用语言叙述翻译成：如果 n 是整数，则 $n(n+1)(2n+1)$ 是 3 的倍数．这里 $P=$“n 是整数”，$Q=$“$n(n+1)(2n+1)$ 是 3 的倍数”．定理的一种形式是 P 成立的充分必要条件是 Q 成立，或简略地 P 成立的充要条件是 Q 成立，或更简略地 $P\Leftrightarrow Q$；这种定理，实际上是两个定理：如果 P 成立则 Q 成立（把条件 Q 成立称为（P 成立的）必要条件）与如果 Q 成立，则 P 成立（这时我们把条件 Q 成立称为（P 成立的）充分条件）．定理的其他多种形式都可分解成若干个如果 P 成立，则 Q 成立这个标准形式．其中包括 P 或 Q 本身也是一个复合语句的情况，例如：如果可导函数 $f(x)$ 有两个不同的零点 x_1，x_2，则存在一点 ξ，$\xi\in(x_1,x_2)$ 使 $f'(\xi)=0$．（$f(x)$ 在 $x\in[a,b]$ 有定义，$a\leqslant x_1<x_2\leqslant b$ 或 $a\leqslant x_2<x_1\leqslant b$）．这里的 P 是“可导函数 $f(x)$ 有两个不同的零点”，不能认为它是一个定理，而只能视为一个述语，应将“如果 P”理解成“假如可导函数 $f(x)$ 有两个不同的零点”或者“可导函数 $f(x)$ 有两个不同的零点为真的话”．

数学定理的产生常常是：实例试算（若干同类的具体演算）—猜想（抽象成命题）—证明（用严格的形式演绎说明其正确性）．例如可以计算

n	1	2	3	4	5
n^3-n	0	6	24	60	120

发现 n^3-n 都是 6 的倍数，于是提出猜想：对于自然数 n，$6\mid n^3-n$．提出猜想后，还可以再验

证,比如

n	6	7	8	0	-1	-2	-3
n^3-n	210	336	504	0	0	-6	-24

于是增强了这个猜想是定理的信心,还可以把从自然数 n 扩展到整数 n. 但,即使如此,即使用计算机验证了成千上万个 n,这个命题都正确,也不能确定这个命题的真伪. 或者说,在证明之前,它仍不能成为定理,数学中定理都要证明.

数学定理是通过归纳得出的命题,再经过严格的逻辑证明后产生的. 在公理、定义、语义理解相同的条件下是一种"绝对"真理,尽管它有相对的形式.

对于要想证明的定理:如果 P 成立,则 Q 成立,证明的目的是用演绎方式的形式逻辑推演阐明如果 P 成立,则 Q 一定成立. 例如如果 $x>3$,则 $x\geqslant 3$ 的推理是正确的. 而反过来推理就不正确. 在定理"P 成立的充要条件是 Q 成立"或"P 成立当且仅当 Q 成立"之中.

演绎中使用的材料必须是绝对可靠的,可以是公理、约定、定义、性质、已证明过的定理等. 演绎过程必须有逻辑的严密性:无漏洞(不能有些该证明的没有证明),无逻辑环,无大跨越的推理(如果有,可以将这些先写成引理,事先加以证明). 也要尽量避免冗余性(多说些无关的话)以保持思路的清晰性.

由于形式逻辑中关于命题有这样一个原理:原命题与逆否命题同时成立或同时不成立(逆命题与否命题也是一样),所以数学证明中可以使用反证法. 即证明它的逆否命题成立,从而得知原命题成立. 如果原命题的形式是如果 P 成立则 Q 成立,那么逆否命题的形式是如果非 Q,则非 P,非 Q 的意义是 Q 不成立.

例 9 试证明:如果 n 是自然数,则 n^3-n 是 6 的倍数.

证明Ⅰ $n^3-n=(n-1)n(n+1)$ 是 3 个连续的非负整数之积,而 3 个连续整数中至少有一个是偶数,故 n^3-n 是 2 的倍数;又 3 个连续整数中必有一个是 3 的倍数. 因而 n^3-n 是 6 的倍数.

注:这一证明不够严密,问题是少了一个引理:

引理 如果 a,b 互素,且 $a\mid c,b\mid c$,则 $ab\mid c$.

加入此引理,注意到 2,3 互素,可重新正确地写出证明Ⅰ. 当然,3 个连续整数中必有一个是 3 的倍数,也应是一个引理,不过有时为简洁,写书时将其略去.

证明Ⅱ 任一自然数用 6 除余数为 1,2,3,4,5 或 0. 故任一自然数 n 可写为 $6k,6k+1,6k+2,6k+3,6k+4,6k+5,k\in N$ 之一.

如果 $n=6k$,则 $n^3-n=(6k)^3-6k=6(36k^3-k)$,是 6 的倍数.

如果 $n=6k+1$,则 $n^3-n=(6k+1)^3-(6k+1)=216k^3+108k^2+48k$ 是 6 的倍数.

同法可证,$n=6k+2,\cdots,n=6k+5$ 时 n^3-n 均是 6 的倍数.

证毕.

注:这一证明基本无问题,为简明计,使用了同法可证一词. 这一词的结论确是正确的. 稍有一点不足的是,加入:因 k 是整数,故 $36k^3-k$ 也是整数及因 $36k^3+18k^2+8k$ 是整数,就更详尽一些.

证明Ⅲ ① 对 $n=1,n^3-n=1^3-1=0$,是 6 的倍数.

② 设命题对 $n(\geqslant 1)$ 成立,即 n^3-n 是 6 的倍数. 考虑 $n+1$ 的情况: