21世纪高等院校教材　　云南省“十二五”规划教材

# 高等代数

郭龙先 张毅敏 何建琼 编

科学出版社

21 世纪高等院校教材　　云南省“十二五”规划教材

# 高等代数

郭龙先　张毅敏　何建琼　编

本书由昭通师范高等专科学校教材专项出版基金资助出版

科学出版社

北京

## 内 容 简 介

本书从师范院校数学专业的特点和要求出发，借鉴参考国内外优秀教材编写体例，注重高等代数知识的系统性和适用性，以及内容的可读性；渗透数学文化教育，关注科学精神的培养. 通过专栏的形式，介绍代数学思想发展史，为培养学生的人文素养提供素材，帮助学生树立正确的数学观. 精选例题、习题，注重层次及难易程度，满足学生专业发展需要. 全书包括9章内容：预备知识，多项式，行列式，线性方程组，矩阵，二次型，向量空间，线性变换，欧氏空间和酉空间.

本书可作为高等师范院校数学教育专业高等代数的教材和参考书，也可以作为综合性大学数学专业的教学参考书.

**图书在版编目(CIP)数据**

高等代数/郭龙先，张毅敏，何建琼编. —北京：科学出版社，2011
21世纪高等院校教材·云南省"十二五"规划教材
ISBN 978-7-03-031599-1

Ⅰ.①高… Ⅱ.①郭…②张…③何… Ⅲ.①高等代数-师范大学-教材
Ⅳ.①O15

中国版本图书馆CIP数据核字(2011)第114380号

责任编辑：胡云志 任俊红 房 阳 / 责任校对：陈玉凤
责任印制：张克忠 / 封面设计：华路天然工作室

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
保定市中画美凯印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2011年6月第 一 版 开本：720×1000 1/16
2011年6月第一次印刷 印张：20
印数：1—2 000 字数：400 000

**定价：39.00元**

(如有印装质量问题，我社负责调换)

# 前　　言

高等代数是数学专业的重要基础课．一方面，它是中学代数的扩展和提高，是代数理论的进一步深化；另一方面，它又为继续学习数学奠定坚实的基础．通过本课程的学习，掌握多项式及线性代数的基本知识和基础理论，理解符号化、抽象化、公理化、形式化及结构化的代数方法，提高分析处理数学问题的能力．

高等代数相对于初等数学而言，研究对象经过多次推广和抽象，很多内容缺乏直观的几何背景，只能用公理方法形式化地处理．为了帮助读者尽快掌握高等代数的基本理论和方法，本书注重对重要概念和基本定理进行解析，力求做到深入浅出，通俗易懂．精选具有典型性、代表性的问题作为例题，便于读者学习借鉴．每节给出思考习题，从基本要求到较高要求，学习时可以根据教学实际选择练习；每章给出综合练习题，充分考虑到学生专业发展的需要．每章均给出主要内容，目标要求及要点总结，其目的是让读者对章节内容框架有总体的把握．另外，为了增加可读性，培养学习兴趣，继承数学文化的优秀传统，本书以专栏的形式适当扩展相关主题，介绍代数学曲折的发展历程以及宽广的应用范围，让读者从中体会代数学深刻的内涵，克服功利主义思想，培养求真务实的科学精神，树立正确的数学价值观．

本书由多项式和线性代数两部分构成．多项式是人们深刻理解的函数，是中学数学的主要内容．多项式部分紧紧围绕多项式因式分解这条主线，阐述多项式的整除性、多项式的最大公因式、多项式的根等理论．线性代数部分，通过引入行列式和矩阵这样的新工具，研究一般线性方程组、二次型、向量空间、欧氏空间的理论问题．

教材由郭龙先教授组织编写，参编的教师从教近三十年，在该邻域具有丰富的教学积累和研究成果．本书是为配合云南省高等代数精品课程建设，为师范院校本专科数学专业学生编写的教材．本书的出版，得到昭通师范高等专科学校教材出版基金的资助，在此表示衷心的感谢！

由于编者水平有限，疏漏和不足在所难免，希望读者批评指正．

编　者

2011 年 2 月 10 日

# 目　　录

# 第1章 预备知识

**本章导读**

高等代数是大学数学的重要基础课.通过本课程的学习,把握具体与抽象、特殊与一般、有限与无限等辩证关系.提高抽象思维、逻辑推理及运算能力,为进一步学习提供必备的代数知识.

**主要内容** 本章主要介绍高等代数中经常用到的一些概念和基本性质.由四部分构成:①介绍集合的基本概念和运算;②给出映射、单射、满射等概念,揭示其本质特征;③介绍整数的整除性概念及其简单性质,为多项式学习做准备;④介绍数域的概念及其性质.数域是高等代数研究对象的基础域.

## 1.1 集合

集合的概念是19世纪70年代由德国数学家康托尔首先引入的,它的观点和方法已渗透到数学的各个分支,对现代数学的发展产生了巨大的推动作用.

集合是数学中一个非常基本的概念(原始概念),很难再用其他的词语来定义,只能用描述性的语言加以说明.我们把一些确定的、彼此不同的事物作为一个整体来考虑时,这个整体便称为一个集合或集,组成集合的每一个事物叫做这个集合的元素.例如,一间教室里的椅子,天上的星星,全世界所有活着的鱼,一切正实数等.这些都组成集合.

通常用大写英文字母 $A,B,C,\cdots$ 表示集合,用小写英文字母 $a,b,c,\cdots$ 表示元素.如果 $a$ 是集合 $A$ 的元素,记作 $a\in A$,读作 $a$ 属于 $A$;如果 $a$ 不是集合 $A$ 的元素,记作 $a\notin A$,读作 $a$ 不属于 $A$.不含任何元素的集合叫做空集,用 $\varnothing$ 来表示.

只含有有限个元素的集合叫做有限集合.例如,0到6之间的整数的集合,一个班里全体学生的集合等都是有限集合.由无限多个元素组成的集合,叫做无限集合.例如,全体整数的集合,0到1之间的实数的集合等都是无限集合.

如果一个集合是由有限个元素组成的,而且这些元素又是完全清楚的,那么就把这些元素一一列举出来,写在大括号里,元素之间用逗号隔开,这种表示法叫列举法.如一个含有 $n$ 个元素 $a_1,a_2,\cdots,a_n$ 的有限集合记作 $\{a_1,a_2,\cdots,a_n\}$.大于1小于5的整数的集合就记为 $A=\{2,3,4\}$.

有些集合即便是由有限个元素组成,但其元素太多,无法一一列举,如全世界的人;或者其元素还不能完全确知,如方程 $x^3-2x^2+4x-5=0$ 的根;还有些集合是由无限多个元素组成,如全体实数的集合,不能用列举法来表示,这时只能用元素的特

征或性质来刻画，表示为

$$A=\{x\mid x\text{ 具有性质 P}\}.$$

这种表示法叫做特征法或描述法，如用

$$A=\{x\mid x^3-2x^2+4x-5=0\}$$

表示方程 $x^3-2x^2+4x-5=0$ 的根的集合；而 $B=\{x|0<x<1\}$ 表示一切大于 0 小于 1 的实数的集合；适合方程

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$$

的所有点的集合 $C$ 可写为

$$C=\left\{(x,y)\middle|\frac{x^2}{a^2}+\frac{y^2}{b^2}=1\right\}.$$

对于两个集合 $A,B$. 若 $A$ 的每一个元素都是 $B$ 的元素，则称 $A$ 是 $B$ 的子集，记作 $A\subseteq B$（读作 $A$ 包含于 $B$），或记作 $B\supseteq A$（读作 $B$ 包含 $A$）. 根据这个定义，$A$ 是 $B$ 的子集的充要条件是对于每一个元素 $x$，如果 $x\in A$，就有 $x\in B$.

例如，集合 $\{1,2,3\}$ 是集合 $\{1,2,3,4,5\}$ 的子集.

如果 $A$ 不是 $B$ 的子集，就记作 $A\not\subseteq B$ 或 $B\not\supseteq A$. 因此，$A$ 不是 $B$ 的子集必要且只要 $A$ 中至少有一个元素不属于 $B$，即存在一个元素 $x_0$，$x_0\in A$ 但 $x_0\notin B$.

根据定义，一个集合 $A$ 是它自己的子集，即 $A\subseteq A$. 我们约定空集是任意集合的子集，即对任意集合 $A$，$\varnothing\subseteq A$.

如果集合 $A$ 与 $B$ 的元素完全相同，则称 $A$ 与 $B$ 相等，记作 $A=B$. 根据定义，集合 $A$ 与 $B$ 相等的充要条件是 $A\subseteq B$ 且 $B\subseteq A$.

集合的包含关系具有传递性，即 $A\subseteq B$ 且 $B\subseteq C$，那么 $A\subseteq C$.

两个集合之间的包含与相等，类似于两个数之间的大小和相等关系. 我们知道两数之间可以进行加减乘除等运算，同样两个集合之间也有它们的运算.

设 $A,B$ 是两个集合. 由 $A$ 的所有元素和 $B$ 所有元素组成的集合叫做 $A$ 与 $B$ 的并集（简称并），记作 $A\cup B$. 例如，$A=\{1,3,5\}$，$B=\{2,3,4\}$，则

$$A\cup B=\{1,2,3,4,5\}.$$

又如，$A$ 是一切有理数的集合，$B$ 是一切无理数的集合，则 $A\cup B$ 是一切实数的集合. 显然 $A\subseteq A\cup B$，$B\subseteq A\cup B$.

根据定义，我们有

$$A\cup B=\{x\mid x\in A\text{ 或 }x\in B\}.$$

因此，如果 $x\notin A\cup B$，那么 $x\notin A$ 且 $x\notin B$.

由集合 $A$ 与 $B$ 的公共元素所组成的集合叫做 $A$ 与 $B$ 的交集（简称交），记作 $A\cap B$，即

$$A\cap B=\{x\mid x\in A\text{ 且 }x\in B\}.$$

显然，$A\cap B\subseteq A$，$A\cap B\subseteq B$.

例如,$A=\{a,b,c,d\}$,$B=\{e,d,f\}$,则

$$A \cap B = \{d\}.$$

**例 1.1.1**　证明(分配律)

(1) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$;

(2) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$.

只证明等式(1),等式(2)留给读者证明.

设 $x\in A\cap(B\cup C)$. 那么 $x\in A$ 且 $x\in B\cup C$,于是 $x\in A$ 且 $x$ 至少属于 $B$ 与 $C$ 之一. 若 $x\in B$,那么因为 $x\in A$,所以 $x\in A\cap B$;同样若 $x\in C$,则 $x\in A\cap C$. 不论哪一种情形都有 $x\in(A\cap B)\cup(A\cap C)$. 所以

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$

反之,若 $x\in(A\cap B)\cup(A\cap C)$,那么 $x\in A\cap B$ 或者 $x\in A\cap C$,但 $B\subseteq B\cup C$,$C\subseteq B\cup C$,所以不论那一种情形都有 $x\in A\cap(B\cup C)$,所以

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C).$$

两个集的并与交的概念可以推广到任意 $n$ 个集合上去,设 $A_1,A_2,\cdots,A_n$ 是给定的集合. 由 $A_1,A_2,\cdots,A_n$ 的一切元素所成集合叫做 $A_1,A_2,\cdots,A_n$ 的并. 由 $A_1$,$A_2,\cdots,A_n$ 的一切公共元素所成的集合叫做 $A_1,A_2,\cdots,A_n$ 的交. $A_1,A_2,\cdots,A_n$ 的并与交分别记作 $A_1\cup A_2\cup\cdots\cup A_n$ 和 $A_1\cap A_2\cap\cdots\cap A_n$. 因此,若 $x\in A_1\cup A_2\cup\cdots\cup A_n$,则 $x$ 至少属于某一 $A_i$,$i=1,2,\cdots,n$;若 $x\in A_1\cap A_2\cap\cdots\cap A_n$,则 $x$ 属于每一 $A_i$,$i=1,2,\cdots,n$.

我们通常用 $\mathbf{N}$ 代表自然数集,$\mathbf{Z}$ 代表整数集,$\mathbf{Q}$ 代表有理数集,$\mathbf{R}$ 代表实数集,$\mathbf{C}$ 代表复数集.

下面我们给出集合的差与积的概念.

设 $A,B$ 是两个集合. 由一切属于 $A$ 但不属于 $B$ 的元素所组成的集合,称为 $A$ 与 $B$ 的差,记作 $A-B$,即

$$A - B = \{x \mid x \in A \text{ 但 } x \notin B\}.$$

例如 $\mathbf{Z}-\mathbf{N}$ 就是一切负整数所组成的集合.

由一切元素对$(a,b)$所成的集合,其中第一个位置的元素 $a$ 取自 $A$,第二个位置的元素 $b$ 取自 $B$. 这样的集合称为 $A$ 与 $B$ 的笛卡儿积(简称积),记作 $A\times B$,即

$$A \times B = \{(a,b) \mid a \in A, b \in B\}.$$

这个概念可以推广到 $n$ 个集合上去,即

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1,a_2,\cdots,a_n) \mid a_i \in A_i, i = 1,\cdots,n\}.$$

称为 $A_1,A_2,\cdots,A_n$ 的积.

例如,取定一个坐标系以后,平面上的点的坐标是一对实数$(x,y)$. 平面上所有点的坐标的集合就是 $\mathbf{R}$ 与 $\mathbf{R}$ 的积:

$$\mathbf{R}^2 = \mathbf{R} \times \mathbf{R} = \{(x,y) \mid x,y \in \mathbf{R}\};$$

空间中所有点的坐标的集合为

$$\mathbf{R}^3=\mathbf{R}\times\mathbf{R}\times\mathbf{R}=\{(x,y,z)\mid x,y,z\in\mathbf{R}\}.$$

以此类推，

$$\mathbf{R}^n=\mathbf{R}\times\mathbf{R}\times\cdots\times\mathbf{R}=\{(x_1,x_2,\cdots,x_n)\mid x_i\in\mathbf{R},i=1,\cdots,n\}.$$

**专栏一**

## 康　托　尔

G. Cantor，德国数学家，集合论的创始人. 1874 年，29 岁的 Cantor 在《数学杂志》上发表了关于无穷集合论方面的第一篇开创性和奠基性的论文. 由于他的工作直接冲击了许多前人的想法和传统观念，因而遭到了保守思潮的强烈反对，尤其是他的老师，当时数学界的权威教授克罗内克对他的攻击最为激烈和粗暴，他对 Cantor 的攻击达十年之久. 由于得不到当时权威数学家的支持，加上紧张的论战，Cantor 于 1884 年精神失常，他的余生一直处在一种严重的抑郁状态中，最后病死在精神病院. 更为严重的是由于克罗内克的攻击，数学家们对 Cantor 的工作在很长时间内都持怀疑态度.

从历史和现实的角度看，几乎每一个数学新分支的诞生，数学研究对象的每一次再扩充，总要受到传统思想的反对和攻击，只是程度有所不同而已，即使在人类智慧的未来发展中，仍将会遇到类似的情况. 然而，不论传统观念如何反对新思想，随着时间的推移，新思想和新方法终究会被人们所理解和接受，Cantor 的思想和工作也不例外. 1897 年在苏黎世举行的第一次国际数学家会议上，Hurwitz 与 Hadamard 指出了超限数理论在分析中的重要应用. Hilbert 在德国传播了 Cantor 的思想，他说："没有人能把我们从 Cantor 为我们创造的乐园中驱赶出去."他把 Cantor 的超限算术赞誉为"数学思想的最惊人的产物，在纯粹理性的范畴中人类活动的最美的表现之一."Russell 把 Cantor 的工作描述为"可能是这个时代所能夸耀的最巨大的工作".

集合论的创立，其最重要的历史意义有两点：第一扩充了数学研究对象；第二为整个经典数学的各个分支提供了一个共同的理论基础.

### 习　题　1.1

1. 设 $S,T$ 是任意两个非空集合，且 $S\not\subset T,T\not\subset S$，令 $X=S\cap T$，那么 $S\cup X$ 为(　　).

A. $X$　　B. $T$　　C. $\varnothing$　　D. $S$

2. 下列论断正确的是(　　).

A. 若 $x\notin A\cup B$，则 $x\notin A$ 或 $x\notin B$　　B. 若 $x\notin A\cap B$，则 $x\notin A$ 且 $x\notin B$

C. 若 $x\in A\cup B$，则 $x\in A$ 且 $x\in B$　　D. 若 $x\in A\cup B$，且 $x\notin A$，则 $x\in B$

3. 设 $A$ 是含有 $n$ 个元素的集合，那么 $A$ 一共有多少个子集？$A$ 中含有 $k(k\leqslant n)$ 个元素的子集

共有多少个?

4. 对任意的集合 $A,B,C$. 证明:

$$C-(A\cup B)=(C-A)\cap(C-B)\quad (\text{De Morgan 律}).$$

5. 证明下列等式:

(1) $(A\cup B)\cup C=A\cup(B\cup C)$;

(2) $A\cap(A\cup B)=A$;

(3) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$;

(4) $A\cap(B-C)=(A\cap B)-C$;

(5) $A-B=\varnothing\Leftrightarrow A\subseteq B$.

6. 集合 $A=\{1,2,3\}$, $B=\{-1,4,-5\}$, 写出 $A\times B$ 与 $B\times A$ 的所有元素, 由此可得出什么结论.

## 1.2 映 射

映射是近现代数学中一个非常重要的概念,其思想已渗透到整个数学领域. 映射是集合之间的一种对应关系,是在两个集合之间建立联系的一种手段.

**定义 1.2.1** 设 $A,B$ 是两个非空集合. 如果存在对应法则 $f$, 对于集合 $A$ 中每一个元素 $x$, 通过法则 $f$, 都有 $B$ 中唯一确定的元素 $y$ 与之对应, 那么法则 $f$ 称为 $A$ 到 $B$ 的一个映射. 记作

$$f:A\to B \text{ 或 } f:x\mapsto y.$$

$A$ 到 $B$ 的映射也叫做定义在 $A$ 上, 取值在 $B$ 内的函数, $f(x)$ 叫做 $x$ 的函数值. 如果通过映射 $f$, $A$ 中元素 $x$ 对应的 $B$ 中元素为 $y$, 那么 $y=f(x)$ 叫做元素 $x$ 在 $f$ 之下的象, $x$ 称为 $y$ 的原象. 集合 $A$ 称为 $f$ 的定义域, $f(A)=\{f(x)\mid x\in A\}$ 称为 $f$ 的值域, 也叫做 $A$ 在 $f$ 之下的象, 或者映射 $f$ 的象. 映射一般用英文字母 $f,g$ 等表示, 也可用希腊字母 $\sigma,\tau$ 等表示.

如果对于每一 $x\in A$, $f(x)$ 都已给出, 那么映射 $f$ 就完全确定了. 需要特别指出的是, 在映射这个定义中, 集合 $A,B$ 不再局限于实数集, 可以是任意非空集合, 它们的元素除了实数之外, 还可以是我们在后面章节要接触到的研究对象, 包括向量、函数、多项式、矩阵、线性变换等. 因此, 映射是函数概念的推广.

**例 1.2.1** 设 $\mathbf{Z}$ 是一切整数的集合. 对每一整数 $n$, 令 $f(n)=2n-1$ 与它对应. 那么 $f$ 是 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的一个映射.

**例 1.2.2** 设 $\mathbf{R}$ 是一切实数的集合, $B$ 是一切非负实数的集合. 对于每一个 $x\in\mathbf{R}$, $f:x\mapsto|x|$, 那么 $f$ 是 $\mathbf{R}$ 到 $B$ 的一个映射.

**例 1.2.3** 设 $A$ 是一切非负实数的集合, $B$ 是一切实数的集合. 对于每一个 $x\in A$, 令 $f(x)=\pm\sqrt{x}$ 与它对应. $f$ 不是 $A$ 到 $B$ 的映射, 因为当 $x>0$ 时, $f(x)$ 不能由 $x$ 唯一确定.

**例 1.2.4** 设 $A$ 是任意一个集合, 对于每一 $x\in A$, $f:x\mapsto x$. 这是 $A$ 到自身的一个映射, 称为集合 $A$ 的恒等映射或单位映射.

与通常函数相等一样,我们通过函数值相等来定义(证明)两个映射相等.

如果 $f,g$ 都是 $A$ 到 $B$ 的映射,且对于每一 $x\in A$ 都有 $f(x)=g(x)$,那么映射 $f$ 与 $g$ 相等,记作 $f=g$.

**例 1.2.5**　令

$$f:\mathbf{R}\to\mathbf{R},x\mapsto 1,$$
$$g:\mathbf{R}\to\mathbf{R},x\mapsto\sin^2 x+\cos^2 x.$$

那么 $f=g$.

在映射的定义中,只要求对于 $A$ 中每一个元素 $x$,有 $B$ 中唯一确定的元素 $y$ 与之对应,但是 $A$ 中不同的元素的象可以相同,也可以不同. 例 1.2.1 中的映射就满足 $\mathbf{Z}$ 中任意两个不同的元素有不同的象. 关于这样的映射,我们给出

**定义 1.2.2**　设 $f:A\to B$ 是一个映射. 如果对于 $A$ 中任意两个元素 $x_1$ 和 $x_2$,只要 $x_1\neq x_2$,就一定有 $f(x_1)\neq f(x_2)$,则称 $f$ 是 $A$ 到 $B$ 的一个单映射,简称单射.

在上面的例 1.2.1 里,当 $m,n\in\mathbf{Z}$ 且 $m\neq n$ 时,有 $2m-1\neq 2n-1$,即 $f(m)\neq f(n)$,因此 $f$ 是单射. 进一步研究我们发现 $f$ 的象的集合 $f(\mathbf{Z})$是一切奇数的集合,是 $\mathbf{Z}$ 的一个真子集,即 $f(\mathbf{Z})\subseteq\mathbf{Z}$,而在例 1.2.2 中,$f(\mathbf{R})=B$. 对于后一情形,我们引入

**定义 1.2.3**　设 $f$ 是 $A$ 到 $B$ 的一个映射. 如果 $f(A)=B$,则称 $f$ 是 $A$ 到 $B$ 上的一个映射或满射.

根据这个定义,$f:A\to B$ 为满射的充分必要条件是对于 $B$ 中每一个元素 $y$,都有 $A$ 中元素 $x$,使得 $f(x)=y$.

**例 1.2.6**　设 $A=B=\mathbf{Z}$,$f:\mathbf{Z}\to\mathbf{Z}$,$n\mapsto n+1$,$n\in\mathbf{Z}$. 证明 $f$ 是 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的满射.

**证明**　首先,$f$ 是 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的一个映射. 其次,对 $\mathbf{Z}$ 中的任一元素 $y$,都有 $\mathbf{Z}$ 中的元素 $x=y-1$,使得

$$f(x)=x+1=(y-1)+1=y.$$

所以 $f$ 是 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的一个满射.

关于映射还可以定义乘法. 设 $f$ 是 $A$ 到 $B$ 的一个映射,$g$ 是 $B$ 到 $C$ 的一个映射. 乘积 $gf$ 定义为

$$(gf)(x)=g(f(x)),\quad x\in A.$$

$gf$ 是 $A$ 到 $C$ 的一个映射,是相继施行 $f$ 和 $g$ 的结果.

**例 1.2.7**　设 $A=\{1,2,3\}$.

$$f:A\to A;1\mapsto 2,2\mapsto 3,3\mapsto 1,$$
$$g:A\to A;1\mapsto 3,2\mapsto 1,3\mapsto 2,$$

那么

$$gf:A\to A;1\mapsto 1,2\mapsto 2,3\mapsto 3.$$

映射的乘积是复合函数概念的推广. 映射的乘法满足结合律,给定映射

$$f:A\to B,\quad g:B\to C,\quad h:C\to D,$$

那么

$$h(gf)=(hg)f, \tag{1.2.1}$$

$h(gf)$和$(hg)f$都是$A$到$D$的映射.要证明它们相等只需证明对于$A$的任意元素$x$,它们的作用相同或函数值相等,即对任意$x\in A$,有

$$(h(gf))(x)=((hg)f)(x).$$

事实上,令$u=gf$,$v=hg$.那么,

$$(hu)(x)=h(u(x))=h(g(f(x))),$$
$$(vf)(x)=v(f(x))=h(g(f(x))).$$

所以$hu=vf$,等式(1.2.1)成立.

若映射$f:A\to B$既是满射又是单射,则称$f$是$A$到$B$的一个**双射**或**一一对应**.

对于$A$到$B$的一个双射$f$,我们自然可以定义它的逆映射,记为$f^{-1}$,它是$B$到$A$的一个映射.且$ff^{-1}$是$B$到自身的一个恒等映射,$f^{-1}f$是$A$到自身的一个恒等映射.

映射$f:A\to B$存在逆映射的充要条件是$f$为$A$到$B$的双射.因此,双射和映射可逆本质上是一致的.

任意集合$A$的恒等映射是$A$到自身的一个双射.特别地,我们把一个有限集合$A$到自身的双射叫做$A$的一个**置换**.

通常整数的加法实际上是一个映射

$$\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}.$$

在这个映射之下,对于$(a,b)\in\mathbf{Z}\times\mathbf{Z}$,

$$(a,b)\mapsto a+b,$$

即对于任意一对整数$(a,b)$,有唯一确定的整数$a+b$与它对应.这样的映射就称为整数的一个“代数运算”.同样,实数的乘法也是一个$\mathbf{R}\times\mathbf{R}$到$\mathbf{R}$映射:$(a,b)\mapsto ab$,$a,b\in\mathbf{R}$,称为$\mathbf{R}$的一个代数运算.

一般地,设$A$是一个非空集合.我们把$A\times A$到$A$的一个映射叫做集合$A$的一个**代数运算**.

**专栏二**

## 希尔伯特旅馆——神奇的对应

数学家经常会提到一间著名的“希尔伯特旅馆”.据说这是希尔伯特在一篇讨论无穷大的演讲中提出的,他所构造的这座神奇旅馆,某种程度上讲述了无穷大的全部故事(虽然生动有趣,但深藏于无限之中的奥秘,依然让许多人感到莫名其妙).他说:

我们设想有一家旅馆,内设有限个房间,而所有的房间都已客满.这时来了一位新客,想订个房间,“对不起”,旅馆主人说,“所有的房间都住满了.”

现在再设想另一家旅馆,内设无限个房间,所有的房间也都客满了.这时也有一位新客,想订个房间.“不成问题!”旅馆主人说.接着他就把1号房间的旅客移到2号

房间，2 号房间的旅客移到 3 号房间，3 号房间的旅客移到 4 号房间等，这样继续移下去. 由此，新客就被安排住进了已被腾空的 1 号房间.

我们再设想一个有无限个房间的旅馆，各个房间也都住满了客人. 这时又来了无穷多位要求订房的客人. "好的，先生们，请等一会儿."旅馆主人说. 于是他把 1 号房间的旅客移到 2 号房间，2 号房间的旅客移到 4 号房间，3 号房间的旅客移到 6 号房间，如此等等. 现在，所有的单号房间都腾出来了，新来的无穷多位客人可以住进去，问题解决了！

希尔伯特旅馆的神奇之处，还在于即使来了无穷多个具有无穷成员的旅行团，在旅馆满员的情况下，店主依然有妙计让客人住宿. 其巧妙的安排如下：

原来的客人仍然统统安排到 2 号、4 号、6 号等这些偶数号码的房间去，剩下的奇数号码房间这样安排：

第一旅行团的成员住这些房间，号码是：$3,9,27,\cdots,3^n,\cdots$；

第二旅行团的房间号码是：$5,25,125,625,\cdots,5^n,\cdots$；

第三旅行团：$7,49,343,\cdots,7^n\cdots$；

第四旅行团：$11,121,1331,\cdots,11^n,\cdots$；

……

一般规律是：奇素数排成一列：$3,5,7,11,\cdots$.

设第 $m$ 个奇素数是 $P_m$，那么，第 $m$ 旅行团的第 $n$ 号成员的房间号码就是$(P_m)^n$. 这样，无穷多个无穷旅行团的成员都有了自己的房间. 店主这一次还留下了无穷个空床位，它们的号码是那些不能表为奇素数方幂的正奇数，如 $1,15,21,35,45,63,75,\cdots$.

为什么仅仅通过让房客从一个房间搬到另一个房间，第一个房间就能空出来呢？据说这种做法，曾使一位顾客百思不得其解，无法入睡. 事实上，这个无穷大数的性质与我们在普通算术中所遇到的一般数字大不一样. 希尔伯特旅馆对应于：

$$\aleph_0+1=\aleph_0\text{(阿列夫零)},$$

旅馆满员，意味着有$\aleph_0$个旅客到来. 考虑两个集合 $A$ 与 $B$ 的元素：

$$A{:}1\quad 2\quad 3\quad 4\quad 5\quad 6\quad 7\quad \cdots,$$

$$B{:}6\quad 7\quad 8\quad 9\quad 10\quad 11\quad 12\quad \cdots.$$

$A,B$ 两集合明显地一一对应，因为在集合 $A$ 中的每一个数，对应于集合 $B$ 中的一个数，反之亦然. 因此，两个集合中元素的数量都是自然数集的基数$\aleph_0$. 但是第二个集合比第一个集合含有的数量少 5 个. 也就是

$$\aleph_0-5=\aleph_0. \tag{1}$$

方程(1)说明，从一个无穷数中减去一个有限量，依然得到相同的无穷量.

由于正偶数集能与自然数集建立一一对应，而正偶数与正奇数一样多，因此奇数的数量与偶数的数量都是$\aleph_0$. 但所有正偶数、正奇数的集合并在一起正好就是自然数的集合. 前者包含有$\aleph_0+\aleph_0$，即 $2\aleph_0$个元素，而自然数集合包含$\aleph_0$个元素，因此

$$\aleph_0 = 2\,\aleph_0. \tag{2}$$

不仅如此，从康托尔利用对角线方法证明有理数集可数时，所构造的无穷方阵可以得到：

$$\aleph_0 \cdot \aleph_0 = \aleph_0. \tag{3}$$

这说明可数集的可数无穷多的并集仍然可数.

希尔伯特旅馆的容量，及其安排住宿客人的技巧已经是令人惊叹和炫目的了.但故事还没完，据说后来饭店老板的女儿进了大学数学系.有一天，康托尔教授来上课，他问："要是区间[0,1]上每一点都占一个房间，是不是还能安排？"她绞尽脑汁，终于失败了.康托尔教授告诉她，用对角线方法证明一切想安排完的方案都是行不通的.

康托尔证明了存在不可数的实数集.他指出并不是所有的无限集都有相同的大小——有一个完整（无穷）的无限数等级.就像有一个有限数的无穷序列 1,2,3,…一样，也存在一个无限数的无穷序列$\aleph_0,\aleph_1,\aleph_2,\aleph_3,\cdots$，其中后一个都比前一个"大".

康托尔把所有适合 $0\leqslant x\leqslant 1$ 的实数 $x$ 的集合叫做连续统，记为 $C$，他在 1874 年、1879 年，庞加莱在 1910 年曾用不同的方法证明 $C$ 是不可数的，也就是说 $C$ 大于（或强于）$\aleph_0$.但 $C$ 是否等于$\aleph_1$？康托尔在 1878 年作出了一项意义重大的"猜测"$C=\aleph_1$，这就是著名的"连续统假设".

看来只要有$\aleph_1$位客人到来，就会使这间曾经牛气冲天的神奇旅馆因客人爆满而关门.正好应了中国人的那句老话：店大欺客，客大欺店！希尔伯特旅馆的故事所涉及的令人惊奇的悖论，曾使人类困惑了两千余年.

## 习 题 1.2

1. 令 $A=B=\{$正整数$\}$，$f:n\mapsto n^2-3$. $f$ 是否为 $A$ 到 $B$ 的映射？
2. 找一个全体实数集到闭区间[0,1]的映射.
3. 设 $f$ 定义如下：

$$f(x)=\begin{cases}2x+1, & x<0,\\ 1, & 0\leqslant x<1,\\ 2x-1, & x\geqslant 1.\end{cases}$$

$f$ 是不是 $\mathbf{R}$ 到 $\mathbf{R}$ 的映射？是不是单射？是不是满射？

4. 设 $A=\mathbf{R}$，$B=\{x\mid x\in\mathbf{R}, x>0\}=\mathbf{R}^+$，$f:A\to B$，$x\mapsto e^x$，对任意的 $x\in\mathbf{R}$. 证明 $f$ 是 $A$ 到 $B$ 的满射.
5. 令 $A=\{a,b,c\}$，写出 $A$ 到自身的一切映射.在这些映射中哪些是双射？
6. 设 $f:A\to B$，$g:B\to C$ 是映射，又令 $h=gf$，证明：

(1) 如果 $h$ 是单射，那么 $f$ 也是单射；

(2) 如果 $h$ 是满射，那么 $g$ 也是满射；

(3) 如果 $f,g$ 都是双射，那么 $h$ 也是双射，并且

$$h=(gf)^{-1}=f^{-1}g^{-1}.$$

7. 判断下表中的规则是不是所给集合 $A$ 的代数运算.

| 序　号 | 集合 $A$ | 规　则 |
|---|---|---|
| (1) | 全体整数 | $(a,b)\mapsto a^b$ |
| (2) | 全体整数 | $(a,b)\mapsto -ab$ |
| (3) | 全体有理数 | $(a,b)\mapsto a^b$ |
| (4) | 全体实数 | $(a,b)\mapsto \dfrac{b}{a}$ |

## 1.3　整数的整除性理论

在后面的章节中,我们要用到整数整除性理论的基本思想和方法.

**定义 1.3.1**　设 $a,b$ 是两个整数. 若存在一个整数 $d$,使得 $b=ad$,则称 $a$ 整除 $b$(或 $b$ 被 $a$ 整除),记作 $a|b$. 这时 $a$ 叫做 $b$ 的一个因数(或约数),而 $b$ 叫做 $a$ 的一个倍数.

如果 $a$ 不整除 $b$,就记作 $a\nmid b$.

我们引入符号"$\Rightarrow$",表示"若…,则…";"$\Leftrightarrow$"表示"当且仅当"或"充要条件".

由整除的定义及乘法运算可以推出整除关系具有下列基本性质:

(1) $a|b,b|c\Rightarrow a|c$.

(2) $a|b$,而 $c\in \mathbf{Z}\Rightarrow a|bc$.

(3) $a|b,a|c\Rightarrow a|(mb+nc),m,n\in \mathbf{Z}$.

把(3)推广为

(4) $a|b_i$,而 $c_i\in \mathbf{Z},i=1,2,\cdots,s\Rightarrow a|(b_1c_1+b_2c_2+\cdots+b_sc_s)$.

(5) $a|b\Leftrightarrow |a|\,|\,|b|$.

(6) 每一个整数都可以被 1 和 $-1$ 整除;每一个整数 $a$ 都可以被它自己和它的相反数 $-a$ 整除.

(7) $a|b$ 且 $b|a\Rightarrow b=\pm a$.

(8) 设 $m\neq 0$,那么 $a|b\Leftrightarrow ma|mb$.

我们用 $\mathbf{N}$ 表示全体非负整数的集合:

$$\mathbf{N}=\{0,1,2,\cdots\}.$$

用 $\mathbf{N}^*$ 表示全体正整数的集合:

$$\mathbf{N}^*=\{1,2,3,\cdots\}.$$

**最小数原理**　设 $S$ 是正整数集 $\mathbf{N}^*$ 的一个非空子集,那么必有 $x_0\in S$,使得对于任意 $x\in S$ 都有 $x\geqslant x_0$,即 $x_0$ 是 $S$ 中的最小自然数.

值得注意的是,最小数原理并不适合于所有数集. 例如,全体整数的集合 $\mathbf{Z}$ 就没有最小数. 但是,如果令

$$\mathbf{M}_c=\{x\in \mathbf{Z}\mid x\geqslant c,c\text{ 是任一整数}\}.$$

那么最小数原理对于 $\mathbf{M}_c$ 仍然成立. 也就是说,$\mathbf{M}_c$ 的任意一个非空子集必含有一个最小数.

由最小数原理可以推出我们熟知的数学归纳法原理. 下面利用最小数原理证明