高等代数

何立国　赵雪梅　编著

科学出版社

高等代数

何立国　赵雪梅　编著

科学出版社

北京

内 容 简 介

本书是一本高等院校数学专业的高等代数教材, 共 10 章, 内容包括基本知识、一元 n 次方程、行列式、矩阵、线性方程组、向量空间、线性变换及二次型等. 每章后配有一定量的习题和补充习题, 习题主要针对课程的基本要求, 补充习题主要是难度更大一些的题目, 并附所有问题的参考答案或提示. 如同家风、家训一样, 每门课程都有自身所秉承的一些理念、思想, 本书在阐述高等代数的基本理念、基本概念、基本方法的同时, 特别注重指导学生运用这些理念、思想理解高等代数的理论体系, 提升解决实际问题的能力.

本书可作为综合性大学、理工科大学、高等师范院校的高等代数教材, 也可作为实际工作者的自学参考书.

图书在版编目(CIP)数据

高等代数/何立国, 赵雪梅编著. —北京: 科学出版社, 2018.5

ISBN 978-7-03-054107-9

Ⅰ. ①高… Ⅱ. ①何… ②赵… Ⅲ. ①高等代数-教材 Ⅳ. ①O15

中国版本图书馆 CIP 数据核字(2017) 第 191795 号

责任编辑: 王胡权 李 萍 / 责任校对: 张凤琴

责任印制: 吴兆东 / 封面设计: 陈 敬

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

北京九州迅驰传媒文化有限公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 5 月第 一 版 开本: 720 × 1000 1/16

2018 年 5 月第一次印刷 印张: 19

字数: 381 000

定价: 59.00 元

(如有印装质量问题, 我社负责调换)

前　言

本书以读者熟悉的一元 n 次方程及 n 元一次方程组解的三个基本问题为中心组织各部分的内容. 所谓方程 (组) 解的三个基本问题是解的存在性问题、解的数量问题和解的公式 (表达式) 问题. 叙述上, 尽量采用通俗而不失严谨的风格. 章节名称上, 尽量采用简洁而对仗比较工整的方式. 高等代数是一门理论性较强的课程, 多年的教学经验告诉我们, 这样的处理方式更容易让学生捋顺本课程各部分内容间的结构关系, 便于学生更好地理解、记忆、升华所学知识.

作者讲授高等代数课程多年, 知道学生的普遍感受是高等代数抽象难懂, 而且越往后学习主动性越差, 甚至有些同学消极对待; 而少数成绩好的同学也往往是熟记概念、定理、公式, 虽会灵活运用, 但对它们所反映的内涵也常常不会去深究. 导致这种现象的原因当然是多方面的, 我们认为如果有一部既贴近学生又贴近高等代数课程内涵的接地气的教材会解决这一现状. 高等代数在形式上可能抽象了一些, 但它所反映的内容一点儿也不抽象, 是具体的、形象的、生动的. 高等代数的每一部分内容的背后都有数学家们为解决某个 (些) 问题所留下的痕迹, 都有具体的问题可查. 只是由于某些教材没有提及或少许提及, 没有引起学生的注意与好奇, 而给学生一种错误感觉, 高等代数很抽象难懂, 甚至认为数学家们都是些奇人怪人, 考虑问题也很离谱. 实际上, 并非如此, 数学家们考虑的大多问题都是很实际的, 通俗地讲出来, 很多人都能明白, 有些问题经常是很多人都没办法, 但数学家们有奇妙的想法使之得以解决、这才是我们真正想让学生意识到的东西. 由此学生才会意识到概念、定理等所要反映的内涵及公理化思想的必要性.

一提到代数, 学生们自然想到解方程 (组). 他们在初中就开始解一元二次方程、二元一次方程组, 三元一次方程组等, 所以如果对方程 (组) 提出新的问题, 他们便会感觉自然 (至少没有茫然的感觉), 不会因为背景知识的不足影响学习的进程, 而且还会使他们原有的方程 (组) 知识进一步得到升华, 对学生创新思维很有帮助. 实际上, 代数是起源于解方程 (组), 拿解方程 (组) 说事, 与高等代数中很多理论产生的历史背景是一致的. 我们以这种接地气的方式给学生讲授高等代数课程多年, 学生普遍没有本课程抽象、难以接受的感觉. 同时我们讲授的内容不但没有降低要求, 反而提高了要求.

高等代数课程一般包括七大部分内容, 即多项式、行列式、矩阵、向量空间、线性方程组、线性变换、二次型. 我们按照 "问题解决" 的模式, 以解决方程 (组) 解的三个基本问题为中心编排各章内容. 我们选择方程 (组) 为中心统一认识高等代

数的观点, 主要是因为方程 (组) 是大一学生都熟悉的对象 (贴近学生), 学生学起来自然, 避免了很多同学学完本课程之后, 只会对多项式、行列式、矩阵、向量等对象进行计算及一些相关结论的证明, 而没有体会到这些相关理论是如何在解决具体问题中产生的、又是如何运用到具体背景中解决具体问题的; 为学生进一步感悟、创新留有充足的余地.

我们从一元二 (三、四) 次方程入手, 引入多项式, 运用多项式的方法深入研究了一元 n 次方程解的三个基本问题, 并在这一过程中详细阐述了多项式理论; 从二 (三) 元一次方程组入手, 引入行列式、矩阵、向量空间, 利用行列式的方法、矩阵的方法及向量空间的方法分别对 n 元一次方程组 (线性方程组) 解的三个基本问题进行详尽的分析和完全的解决, 并在这一过程中分别细致介绍了行列式理论、矩阵理论、向量空间理论, 还利用欧氏空间理论进一步研究了线性方程组的近似解问题, 这些构成了本书的大部分内容. 在介绍向量空间维数的概念时, 我们反复强调对于我们所说的 $n(\geqslant 4)$ 维向量空间只是解方程组的一种方法、线性变换部分是作为方阵的一种简洁的表示形式进行阐述的. 二次型部分是作为对称矩阵的应用进行阐述的. 在叙述各个部分的主要概念、结论的时候, 我们都提及一些相关的数学家的名字、生卒年等信息, 以便同学学习这些知识有一些直观感触, 也便于同学在网上或纸媒上进一步查询获得更感兴趣的信息.

如同家风、家训一样, 每门课程都有自身所秉承的一些理念、思想, 我们在第 1 章简单而通俗地介绍了高等代数所秉持的基本理念, 所使用的基本概念、基本方法, 为进一步学习本课程做好基本的铺垫; 第 2 章详细地讨论了一元 n 次方程解的问题, 并在这一过程中介绍了一元多项式理论; 第 3 章介绍了行列式理论, 并利用行列式理论讨论了有解情况下的线性方程组的公式解; 第 4 章介绍了矩阵理论, 并用矩阵理论讨论了线性方程组解的问题; 第 5 章介绍了向量空间理论, 并用向量空间理论讨论了线性方程组解的问题. 通过第 3, 4, 5 章的学习, 可以体会到利用矩阵的方法研究线性方程组是三种方法中最好的一个, 这三种方法不是彼此孤立的, 而是相互渗透、密切联系的. 矩阵及其行、列均可看作向量, 向量可视为列矩阵或行矩阵, 衡量矩阵的最重要的量即矩阵的秩, 可以用行列式定义, 也可以通过向量定义. 由于矩阵的重要作用, 我们在第 6, 7 章深入分析了方阵及其简洁表示形式 —— 线性变换, 以及方阵的标准形问题. 实际上, 进一步的学习, 学生会发现矩阵是数学中少有的可以雅俗共赏的数学工具, 应用它可以解决很多实际问题, 很多深刻的数学理论用它往往能给出更清晰的解释说明; 第 8 章介绍了欧氏空间理论, 并用欧氏空间理论讨论了线性方程组的近似解问题, 并集线性方程组三种解法的长处对其三个问题给出简洁清晰的回答; 第 9 章二次型是作为对称矩阵的应用进行阐述的, 实际上通过本章的学习, 读者可以体会到一种理论 (矩阵理论) 如何应用于实际问题 (化二次型为标准形), 并将这一问题解决的全过程; 第 10 章介绍了利用多项式理论

解决向量空间的分解问题, 同时简单介绍了代数的一个经典观点: 代数主要是研究带有运算的集合. 利用代数的概念可以对多项式的未定元给出清楚的说明.

本书可作为综合性大学、理工科大学、高等师范院校的高等代数教材, 分上、下两学期开设, 总计 130 学时左右. 为了使学生对本课程知识有一个比较全面的了解, 学起来自然、有实在感、不抽象, 我们对所涉及的问题都给出比较全面的叙述, 但有些内容超出本课程的要求 (例如, 8.5 节, 有星号的节), 有些在课堂上讲授并不流畅, 意义也不是很大 (例如, 3.5 节、8.4 节), 教师在讲授过程中可以依据实际情况对内容进行适当修整. 每一章配有一定量的习题和补充习题. 习题主要针对课程的基本要求, 补充习题难度更大一些, 并附所有问题的参考答案或提示.

感谢沈阳工业大学教务处领导、理学院的同仁, 以及科学出版社的编辑对本书的关心与支持, 是他们的大力支持与辛勤劳动才使得本书得以顺利出版.

真心希望读者对书中不妥之处批评指正, 以便进一步的改进和完善.

何立国

2017 年 5 月 10 日

目　　录

第 1 章　基础知识和基本理念

一说起代数, 人们自然想到解方程和方程组, 实际上这种感觉是对的, 代数就起源于解方程 (组). 早在公元前 1800 年左右, 古巴比伦人就知道了一些一元二次方程的解法; 而至迟成书于公元 1 世纪的我国数学名著《九章算术》就已利用方程组解决实际问题了. 实际上, 解方程 (组) 也是数学发展的主线索. 人们习惯于称中学时代的代数知识为初等代数, 大学所学代数知识为高等代数 (advanced algebra), 它们之间是一脉相承、逐步深入的关系.

我们认为高等代数主要研究的是: 一元 n 次方程和 n 元一次方程组解的问题, 并且对研究这一问题过程中所衍生的一些问题作了进一步的探讨. 方程 (组) 解的问题是指: 解的存在性问题、解的数量问题、解的公式 (表达式或结构) 问题. 本章首先简单介绍一下在进一步学习中经常使用的概念、方法及秉承的理念等.

1.1　基 本 概 念

读者对集合并不陌生, 它就是一些对象的集体, 其中的成员 (对象) 称为集合的元素, 具有无序性、互异性、确定性. 当集合中元素个数有限时, 称为有限集; 否则称为无限集. 集合通常用大写字母 $A, B, C, \cdots$ 表示, 其中的元素用小写字母 $a, b, c, \cdots$ 表示. 集合之间存在着交、并、补、差的运算. 设 I 是一个集合, A, B, C 分别是 I 的子集, 即由 I 中某些元构成的集合. A 与 B 的交 (集) 是刚好由两者共有的元构成的集合, 即 $A \cap B = \{x \mid x \in A \text{ 且} x \in B\}$. 而并集 $A \cup B = \{x \mid x \in A \text{ 或} x \in B\}$, 差集 $A - B = \{x \mid x \in A \text{ 但是} x \notin B\}$. 子集 A 在 I 中的补集 $A^{\mathrm{c}} = I - A$. 为了满足集合之间运算的需要, 我们约定: 不包含任何元素的集合为空集, 它是任意集合的子集, 记作 $\varnothing$. 这样, 我们有 $A - A = \varnothing$, $I^{\mathrm{c}} = \varnothing$ 等.

集合之间的交、并、补运算之间也满足一些运算律.

交换律　$A \cap B = B \cap A, A \cup B = B \cup A$;

结合律　$(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$;

分配律　$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

关于补运算　$(A \cup B)^{\mathrm{c}} = A^{\mathrm{c}} \cap B^{\mathrm{c}}$, $(A \cap B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B^{\mathrm{c}}$.

证明上述等式都是通过推导左右两侧相互包含实现的. 我们不妨通过下面命题的证明来观察具体过程.

命题 1.1.1　*假定集合 A, B, C 都是集合 I 的子集, 那么*

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

证明　任取 $x\in A\cap(B\cup C)$, 则 $x\in A$, 并且 $x\in B\cup C$. 由后一事实可得 $x\in B$ 或 $x\in C$. 所以 $x\in A$ 且 $x\in B$, 或者 $x\in A$ 且 $x\in C$, 即 $x\in(A\cap B)\cup(A\cap C)$. 因此, $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$.

任取 $x\in(A\cap B)\cup(A\cap C)$, 则 $x\in A\cap B$ 或 $x\in A\cap C$. 得 $x\in A$, 且 $x\in B$ 或 $x\in C$, 即 $x\in A\cap(B\cup C)$. 所以 $(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$, 因此等式成立. □

命题 1.1.2　*假定集合 A,B,C 都是集合 I 的子集, 那么*

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

证明　任选 $x\in A\cup(B\cap C)$, 则 $x\in A$ 或 $x\in B\cap C$, 后者表示 $x\in B$ 且 $x\in C$. 如果 $x\in A$, 那么 $x\in A\cup B$ 且 $x\in A\cup C$, 即 $x\in(A\cup B)\cap(A\cup C)$; 如果 $x\in B\cap C$, 那么也得 $x\in(A\cup B)\cap(A\cup C)$. 故总有 $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$. 反之, 如果 $x\in(A\cup B)\cap(A\cup C)$, 那么 $x\in A\cup B$ 且 $x\in A\cup C$. 故 x 至少属于下列四个集合之一: $A\cap A$, $A\cap C$, $B\cap A$, $B\cap C$, 故 $x\in A\cup(B\cap C)$, 故得 $(A\cup B)\cap(A\cup C)\subseteq A\cup(B\cap C)$. 因此得等式 $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$. □

集合之间还可以通过对应关系联系起来. 设 G,N 是任意两个非空集合, 如果这两个集合的元之间存在对应关系使得 G 中任意一个元对应着 N 中唯一一个元, 则称这个对应关系是一个映射 (map); 我们用 f 表示这个映射. 具体地, 若在映射 f 之下, G 中元 x 映到 N 中的元 y, 即 $f:x\mapsto y$, $x\in G,y\in N$, 则记 $f(x)=y$. 通常称 y 是 x(在映射 f 下) 的象, 而 x 是 y (在映射 f 下) 的原象. 若所有 N 中元都有原象, 则称 f 是满射 (surjective map); 若任意两个不同的原象的象也不同, 则称 f 是单射 (injective map); 进一步, 若 f 既是单射又是满射, 则称 f 是双射 (bijective map). 当 f 是 G 到 N 的双射时, 它能唯一地确定一个 N 到 G 的映射 $g:y\mapsto x$, 对于上述的 y,x, 称 g 是 f 的逆映射 (方向与 f 刚好相反), 通常把 f 的逆映射记成形式 f^{-1}.

我们使用的集合常常是数集, 例如全体自然数 $\mathbb{N}$ (或用 $\mathbf{N}$ 表示), 全体整数 $\mathbb{Z}$(或用 $\mathbf{Z}$ 表示), 有理数域 $\mathbb{Q}$(或用 $\mathbf{Q}$ 表示), 实数域 $\mathbb{R}$ (或用 $\mathbf{R}$ 表示), 复数域 $\mathbb{C}$(或用 $\mathbf{C}$ 表示). 我们可以在数集之间建立一些对应关系.

例题 1.1.1　(1) $f:\mathbb{R}\longrightarrow\mathbb{R},x\mapsto|x|,\forall x\in\mathbb{R}$;

(2) $g:\mathbb{Z}\longrightarrow\mathbb{Z},n\mapsto 2n,\forall n\in\mathbb{Z}$;

(3) $h:\mathbb{Q}\longrightarrow\mathbb{Q},x\mapsto 2x,\forall x\in\mathbb{Q}$.

通过简单的分析可知: 上面例题中的三个对应都是映射; 其中 f 既不是单射也不是满射; g 是单的但不满; h 是个双射, 它的逆是 $h^{-1}(x)=\dfrac{1}{2}x$. 实际上映射 $f:\mathbb{R}\longrightarrow\mathbb{R}$ 就是我们通常所说的函数.

给定两个映射 $f: A \longrightarrow B, a \mapsto b$, $g: B \longrightarrow C, b \mapsto c$, 我们可以自然地构作一个新的映射 $A \longrightarrow C, a \mapsto c$, 这个映射称作 g 与 f 的复合映射 (或称 g 与 f 的积), 记作 $g \circ f$(简记 gf). 特别地, $gf(a) = g(f(a))$.

类似地, 给定两个集合 A, B, 我们也可构作一个新的集合, 记作 $A \times B$, 具体地, $A \times B = \{(a, b) \mid a \in A, b \in B\}$, 称之为 A 与 B 的卡氏积 (Cartersian product).

利用集合和映射的观点, 可以统一认识数学中的很多事情, 把它们说得更加清楚、充分、简洁. 例如, 关于无限集 S 的描述: S 不是一个有限集, S 中的元素取之不竭, S 的元素要多少有多少, S 中的元素当取到 n 个元时, 总能接着取到第 $n+1$ 个, 此处的 n 是任意自然数, 等等. 实际上, 利用映射可以给出无限集一个很简洁的描述: 如果 S 与其一个真子集之间存在一个双射, 则 S 就是一个无限集. 这是因为有限集不可能与其真子集之间存在双射. 算术里的加、减、乘运算就可以看作是 $A \times A \longrightarrow A$ 的映射, 其中 A 可以取数域 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等. 例如, $+: \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}, (a, b) \mapsto a + b$, 其中 $a, b \in \mathbb{Q}$, 减法及乘法同理可得. 除法可定义为 $\mathbb{Q} \times \mathbb{Q}^* \longrightarrow \mathbb{Q}, (a, b) \mapsto \dfrac{a}{b}$, 其中 $a \in \mathbb{Q}, b \in \mathbb{Q}^*$, 此处 $\mathbb{Q}^*$ 表示 $\mathbb{Q}$ 的全体非零元之集. 实际上, 我们学过的各种运算都可以通过映射以适当的方式加以表述.

1.2 整数知识

我们学习整数知识实际是从算术开始的, 最初是自然数的加法、减法, 由于实际需要, 算的对象范围扩大到整数, 之后算的对象的范围进一步扩大到有理数域、实数域、复数域, 而算的种类逐步扩大到加、减、乘、除、乘方、开方 (六则运算). 简单地说, 数学发展的标志就是 "算" 的对象的范围不断扩大、"算" 的种类不断增加的过程. 我们最初算的对象是数, 之后是式 (单项式、多项式等), 进一步学习会发现更大的算的范围、更多的算的方式. 有些同学认为算的对象就应当是数, 不应是别的. 这种理念是有偏颇的, 实际 "算术" 一词可以直白地解释为: 算的术, 即算的技巧、方法、方式. 但它并没有指出算的对象. 为方便进一步学习, 我们想回顾和丰富一下整数知识.

我们分别用 $\mathbb{N}, \mathbb{Z}$ 表示全体自然数集和全体整数集. 我们会发现 $\mathbb{N}$ 的任一非空子集必有最小数, 这一基本的事实通常称为自然数的最小数原理. 对于两个整数 a, b, 当 $|a| > |b| > 0$ 时, 总可以相除, 得 $a = bq + r$, 其中 q 称为商, $0 \leqslant r < |b|$ 称为余数, 并且 q, r 都是唯一的; 实际上, 当 $|a| = |b|$ 时, 也可以写成这种形式. 具体地, 若 $a = b$, 有 $a = b \cdot 1 + 0$; 若 $a = -b$, 有 $a = b \cdot (-1) + 0$; 若 $|a| < |b|$, 且 a, b 均正时, 有 $a = b \cdot 0 + a$, 其他情况同学自己给出. 总之, 在任何情况下, 总有表达式 $a = bq + r$, 其中的 $q, r (0 \leqslant r < |b|)$ 是唯一的, 通常称之为关于整数 a, b 的带余除法表示形式.

在上述带余除法表示式中, 若 $r=0$, 则称 b 整除 a. 由于整数之间的整除关系在整数理论中很重要, 我们给出一个更清晰的定义: 对于任意两个整数 a,b, 若存在整数 q 满足条件 $a=bq$, 则称 b 整除 a, 记作 $b\mid a$. 此时通常称 b 是 a 的一个因数, a 是 b 的一个倍数. 注意由于 $0=0\cdot 0$, 故表达式 $0\mid 0$ 是有意义的 $\left(\text{虽然表达式 } \dfrac{0}{0} \text{ 没有意义}\right)$. 当 b 不整除 a 时, 记作 $b\nmid a$.

关于整数间的整除关系有下列基本性质. 这些性质利用整除定义易导出.

(1) **传递性**　若 $a\mid b,\quad b\mid c$, 则 $a\mid c$;

(2) **和差性**　若 $a\mid b,\quad a\mid c$, 则 $a\mid (b\pm c)$;

(3) **积性**　若 $a\mid b,\quad c\in\mathbb{Z}$, 则 $a\mid cb$;

(4) **组合性**　若 $a\mid b_i,\quad c_i\in\mathbb{Z},\ 1\leqslant i\leqslant n$, 则 $a\mid (c_1b_1+c_2b_2+\cdots+c_nb_n)$;

(5) **相互整除性** 若 $a\mid b$ 且 $b\mid a$, 则 $a=\pm b$.

如果 $c\mid a$ 且 $c\mid b$, 则称 c 是 a,b 的一个公因数, 当 a,b 不全为零时, 称它们的公因数中最大者为 a,b 的最大公因数 (greatest common divisor), 记作 (a,b). 当 a,b 全为零时, 由于任意整数均是它们的公因数, 故公因数中没有最大者; 另外, 两个零的最大公因数比两个不全为零的数的最大公因数小, 会让我们感觉更自然些, 于是我们规定两个零的最大公因数是零, 记作 $(0,0)=0$. 这种最大公因数的定义虽然比较通俗、直观, 但有些烦琐. 我们可以给出一个清晰, 可操作的定义.

定义 1.2.1　*设 a,b,c 是三个整数, 若 c 满足如下两个条件:*

(1) *c 是 a,b 的一个公因数;*

(2) *a,b 的所有公因数都整除 c,*

则称 c 是 a,b 的最大公因数.

由上述新定义可知, 若 c 是 a,b 的最大公因数, 则 $-c$ 也是, 通常将其中的非负最大公因数记作 (a,b). 注意新定义是采用另一种方式反映出最大公因数是公因数中的最大者这样一种理念. 而这两种定义方式本质上是一致的.

命题 1.2.2　*设 d 是 a,b 的最大公因数, 则存在 $s,t\in\mathbb{Z}$ 满足 $d=sa+tb$.*

证明　若 $a=b=0$, 则结论显然. 设 a,b 不全为零, 假定 $S=\{sa+tb>0\mid s,t\in\mathbb{Z}\}$, 则 S 是自然数集的一个非空子集. 由最小数原理, S 中必有最小数, 不妨设其为 h, 故有 $h=sa+tb$. 若 $h\nmid a$, 则由带余除法知 $a=hq+r$, $0<r<h$, 故 $r=a-hq=a-(sa+tb)q=(1-sq)a+(-tq)b$, 这与 h 是 S 中最小数矛盾, 所以 $h\mid a$; 同理可得 $h\mid b$, 因此 h 是 a,b 的一个公因数. 若 $c\mid a,\ c\mid b$, 则 $c\mid sa+tb$, 即 $c\mid h$. 所以 h 是最大公因数, 可知若 $d\geqslant 0$, 则 $d=h$, 若 $d\leqslant 0$, 则 $d=-h$. □

类似地可以给出 n 个整数 $a_1,a_2,\cdots,a_n$ 的最大公因数 d 的定义为: d 是这 n 个数的一个公因数, 并且这 n 个数的所有公因数都整除 d. 可以证明: 存在整数 $s_1,s_2,\cdots,s_n$ 满足 $d=s_1a_1+s_2a_2+\cdots+s_na_n$. 记非负最大公因数为 $(a_1,a_2,\cdots,a_n)$.

当 $(a_1, a_2, \cdots, a_n) = 1$ 时, 通常称 $a_1, a_2, \cdots, a_n$ 是互素的.

命题 1.2.3 *n 个整数 $a_1, a_2, \cdots, a_n$ 互素的充要条件是存在整数 $s_1, s_2, \cdots, s_n$ 满足 $s_1a_1 + s_2a_2 + \cdots + s_na_n = 1$.*

证明 必要性显然. 我们证明充分性: 设 d 是非负最大公因数, 则得 $d \mid a_i, i = 1, 2, \cdots, n$, 故得 $d \mid s_1a_1 + s_2a_2 + \cdots + s_na_n$, 所以 $d \mid 1$, 因此 $d = 1$. □

互素还有如下基本性质. (作为练习, 请同学自己证明.)

(1) 若 $(a, b) = 1$, $(a, c) = 1$, 则 $(a, bc) = 1$;

(2) 若 $a \mid bc$, 且 $(a, b) = 1$, 则 $a \mid c$;

(3) 若 $a \mid c$, $b \mid c$, 且 $(a, b) = 1$, 则 $ab \mid c$.

对于两个整数 a, b, 若有整数 m 满足 $a \mid m$, $b \mid m$, 则称 m 是 a, b 的一个公倍数. 若 a, b 的一个公倍数 c 能整除它的所有公倍数, 则称 c 是 a, b 的最小公倍数. 可证两整数必存在最小公倍数. 若 c 是最小公倍数, 则 $-c$ 也是最小公倍数, 记其中的非负者为 $[a, b]$. 注意到最小公倍数有与最大公因数类似的定义方式.

设 p 是一个正整数, 若它只有因数 $\pm 1, \pm p$, 则称 p 为素数 (也称质数). 除 1 外, 素数是含有因数个数最少的正整数, 它有如下基本性质. (请同学自证.)

(1) 设 p 是一个素数, a 是一个整数, 则 $p \mid a$ 或 $(p, a) = 1$;

(2) 若 $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$.

对于整数间的除法, 当只关心余数, 而不计较商时, 有所谓同余 (congruence) 的概念. 具体地, 当整数 a, c 分别除以正整数 m, 所得余数相同时, 我们称 a, c 模 (modulo) m 同余, 记作 $a \equiv c \bmod m$. 易证, $a \equiv c \bmod m$ 的充要条件是 $m \mid (a - c)$. 易证同余有如下关于四则运算的基本性质. (请同学自己证明.)

对于整数 a, b, c, d, 如果 $a \equiv b \bmod m$, $c \equiv d \bmod m$, 那么 $a + c \equiv b + d \bmod m$, $a - c \equiv b - d \bmod m$, $ac \equiv bd \bmod m$. 如 $ac \equiv bc \bmod m$ 并且 $(c, m) = 1$ 时, $a \equiv b \bmod m$. 同余还有下列费马 (P. Fermat, 1601—1665) 和欧拉 (L. Euler, 1707—1783) 的著名结果.

以 m 为模可以将整数集按余数分为 m 个不交子集, 每一子集称作一个剩余类, 这些类分别包含余数 $0, 1, \cdots, m - 1$, 包含 i 的类为 $\{mx + i \mid x \in \mathbb{Z}\}$. 每一类中任取一个数作这个类的代表元, 可得一数集 $a_1, a_2, \cdots, a_m$, 称为模 m 的一个完全剩余系. 当在与 m 互素的类中各取一代表元时, 也可得一数集 $b_1, b_2, \cdots, b_t$, 通常称此数集为模 m 的一个缩剩余系. 注意一个剩余类中若有一个数与 m 互素, 则此类中任一数均与 m 互素. 同余式有很多与等式相同的性质, 故有的学者称同余式为 "粗 (糙) 等式".

定理 1.2.4 (费马) *设 p 是一个素数, a 是一个整数且 $p \nmid a$, 则 $a^{p-1} \equiv 1 \bmod p$.*

证明 由于 $a^p = ((a - 1) + 1)^p$, 利用二项式定理得 $a^p \equiv (a - 1)^p + 1 \bmod p$; 反复利用二项式定理可得 $a^p \equiv (a - 2)^p + 2 \equiv \cdots \equiv a \bmod p$, 进而得 $a^p \equiv a \bmod p$,

即 $p \mid a(a^{p-1}-1)$. 因 $p \nmid a$, 故 $p \mid (a^{p-1}-1)$, 即 $a^{p-1} \equiv 1 \bmod p$. □

为了给出欧拉的结果, 我们首先介绍欧拉函数 $\phi(n)$: n 取正整数, $\phi(n)$ 表示不大于 n 的正整数中与 n 互素的正整数的个数. 例如, $\phi(1)=1$, $\phi(2)=1, \phi(4)=2$, $\phi(10)=4$. 易见模 m 剩余类中缩剩余系有 $\phi(m)$ 个代表元.

命题 1.2.5　*设 m 是一个正整数, k 是一个与 m 互素的整数. 在模 m 的剩余类中, 若 $a_1, a_2, \cdots, a_{\phi(m)}$ 是一个缩剩余系, 则 $ka_1, ka_2, \cdots, ka_{\phi(m)}$ 也是一个缩剩余系.*

证明　因为 $(a_i, m)=1, (k, m)=1$, 所以 $(ka_i, m)=1$. 故再要证明 $ka_1, ka_2, \cdots, ka_{\phi(m)}$ 中两两互不同余即可. 若其中某两项, 不妨设 ka_i, ka_j 同余, 则有 $m \nmid k(a_i - a_j)$, 又因 $(k, m)=1$, 故得 $m \mid (a_i - a_j)$, 即 $a_i \equiv a_j \bmod m$, 矛盾. □

定理 1.2.6 (欧拉)　*设 m 是一个正整数, k 是一个整数且 $(m, k)=1$, 则 $k^{\phi(m)} \equiv 1 \bmod m$.*

证明　设 $a_1, a_2, \cdots, a_{\phi(m)}$ 是一个缩剩余系, 则由上述命题知 $ka_1, ka_2, \cdots, ka_{\phi(m)}$ 也是一个缩剩余系. 因此前一个缩剩余系中任一代表元, 在后一个缩剩余系中刚好有一个代表元与之同余, 所以得到一个积同余式 $a_1 a_2 \cdots a_{\phi(m)} \equiv ka_1 ka_2 \cdots ka_{\phi(m)} \equiv k^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} \bmod m$, 又因 $(a_1 a_2 \cdots a_{\phi(m)}, m)=1$, 故得 $k^{\phi(m)} \equiv 1 \bmod m$. □

易见欧拉定理是费马定理的推广, 故费马定理可以作为欧拉定理的推论出现. 由于此两定理的证明方法是同余方法的经典应用, 故均给出了证明. 同余的概念很早就有, 我国古代著名的同余问题 "物不知其数" 已有 1500 多年的历史. 同余也是很有用的概念. 例如, 我们知道, 任何一个分数都可以写成一个循环小数的形式. 利用同余知识可以给出一个很简洁的证明. 设一个分数 $\frac{n}{m}, m, n > 0$, 可得 n 除以 m 所得余数至多有 m 种情形, 因此连续作 $m+1$ 次除法, 必有某两次余数相同, 因此出现循环小数.

为了把一些结果及证明过程表述得简洁清楚, 我们要经常使用连加号 $\sum$(也称为和号), 偶尔使用连乘号 $\prod$, 因此介绍它们的一些基本性质.

我们经常把 $a_1 + a_2 + \cdots + a_n$ 记作

$$\sum_{i=1}^{n} a_i.$$

例如

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \sum_{i=1}^{n} i^3,$$

也可写成

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \sum_{t=1}^{n} t^3.$$

可见, 指标变量可以取 i, 也可以取 t, 即和与指标变量取法没关系. 和号 $\sum$ 有下列基本性质.

$$\sum_{i=1}^{n}(a_i \pm b_i) = \sum_{i=1}^{n} a_i \pm \sum_{i=1}^{n} b_i, \quad \sum_{i=1}^{n} k a_i = k \sum_{i=1}^{n} a_i, \quad k\text{是与}i\text{无关的数.}$$

通常规定

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} \triangleq \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij}\right),$$

易见双重求和可以交换和号位置, 即

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}.$$

设一组 mn 个数按如下方式排列:

$$\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array}$$

我们可以用两种方式求这组数的和, 先将每行求和, 之后再将这 m 个和相加, 即 $\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} a_{ij}$. 另一方面也可以先将每列求和, 之后将这 n 个和再相加, 即 $\sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m} a_{ij}$, 故上面等式成立.

和号也可以分割, 例如

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_i, \quad \text{其中} 1 \leqslant k < n.$$

也可以用和号表示一组数中某部分数的和, 例如

$$\sum_{i+j=5} a_i a_j = a_1 a_4 + a_2 a_3 + a_3 a_2 + a_4 a_1 = 2a_1 a_4 + 2a_2 a_3,$$

又如

$$\sum_{j=2}^{n}\sum_{i<j} a_{ij} = a_{12} + (a_{13} + a_{23}) + \cdots + (a_{1n} + \cdots + a_{n-1,n}),$$

$$\sum_{i+r=t}\sum_{j+k=r} a_i b_j c_k = \sum_{i+j+k=t} a_i b_j c_k.$$

连加号还有更加灵活的形式, 例如

$$\sum_{j_1,j_2,\cdots,j_n} a_{1j_1}a_{2j_2}\cdots a_{nj_n} = \left(\sum_{j_1} a_{1j_1}\right)\left(\sum_{j_2} a_{2j_2}\right)\cdots\left(\sum_{j_n} a_{nj_n}\right),$$

其中 $j_1, j_2, \cdots, j_n$ 是指标变量, 一般地, 指标变量没有标明范围表示取遍所有可能的自然数, 但有时在上下文背景清晰的情况下, 为了形式简洁也不标明指标变量的范围.

类似于连加号, 我们用 $\prod\limits_{i=1}^{n} a_i$ 表示 n 个数 $a_1, a_2, \cdots, a_n$ 的连乘积, 即

$$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n.$$

则 n 的阶乘可表示成 $\prod\limits_{i=1}^{n} i$ 或 $\prod\limits_{j=1}^{n} j$. 而乘积

$$\prod_{1\leqslant i<j\leqslant n} (a_j - a_i)$$

表示所有较大下标的元减去较小下标的元的差之积, 即

$$\begin{aligned}\prod_{1\leqslant i<j\leqslant n} (a_j - a_i) \quad = \quad & (a_2 - a_1)(a_3 - a_1)\cdots(a_n - a_1)\\ & (a_3 - a_2)\cdots(a_n - a_2)\\ & \cdots \quad \cdots \quad \cdots\\ & (a_n - a_{n-1}).\end{aligned}$$

最后我们想简要介绍一下整数的唯一分解定理, 这个定理也被称作算术基本定理, 可见它的重要性.

定理 1.2.7　*设 $n > 1$ 是一个正整数, 那么 n 可以唯一地表示成按自然顺序排列的素数的幂的积的形式, 即 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, 其中 p_i 是素数, 整数 $\alpha_i > 0, i = 1, \cdots, t$, $p_1 < p_2 < \cdots < p_t$.*

证明　如果 n 是一个素数, 可认为定理是正确的. 若 n 是非素数, 则 n 有分解 $n = n_1 n_2$. 对 n_1, n_2 分别进行同样的分析过程, 因为 n 是个有限数, 这样的分析过程至多进行有限步, 可得分解式 $n = m_1 m_2 \cdots m_s$, 其中每个因数 m_i 是素数. 将其中相同的素数写成幂的形式便得 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, 其中 p_i 是素数, 整数 $\alpha_i > 0, i = 1, \cdots, t$, $p_1 < p_2 < \cdots < p_t$.

若 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, q_i 是互不相同的素数. 由于 p_1, q_1 均是 n 的最小素因数, 故 $p_1 = q_1$. 又由等式可得 $p_1^{\alpha_1}$ 整除 $q_1^{\beta_1}$ 和 $q_1^{\beta_1}$ 整除 $p_1^{\alpha_1}$, 所