21st CENTURY
规划教材
面向21世纪高等院校计算机系列规划教材
COMPUTER COURSES FOR UNDERGRADUATE EDUCATION

# 计算机代数基础

## ——代数与符号计算的基本原理

张树功　雷　娜　刘停战　编

科学出版社
www.sciencep.com


面向21世纪高等院校计算机系列规划教材
COMPUTER COURSES FOR UNDERGRADUATE EDUCATION

# 计算机代数基础

## ——代数与符号计算的基本原理

张树功　雷　娜　刘停战　编

科学出版社

北京

## 内 容 简 介

随着计算机技术的飞速发展,计算机代数系统已经被广泛地应用于科研、教学以及工程技术,其中比较有名的有 Maple, Mathematica 等. 本书主要介绍这些系统中基本问题的数学原理和基本算法,即计算机代数的基本知识.

本书是为数学、计算数学和计算机科学专业的高年级本科生和低年级研究生编写的教材,也可供相关专业的学生、教师以及科技工作者参考.

**图书在版编目(CIP)数据**

计算机代数基础:代数与符号计算的基本原理/张树功等编.—北京:科学出版社,2005

(面向 21 世纪高等院校计算机系列规划教材)

ISBN 7-03-015325-1

Ⅰ.计… Ⅱ.张… Ⅲ.电子计算机-数值计算 Ⅳ.TP301.6

中国版本图书馆 CIP 数据核字(2005)第 028854 号

责任编辑:李 娜 丁 波/责任校对:刘彦妮

责任印制:吕春珉/封面设计:三函设计

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

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2005 年 5 月第 一 版 开本:787×1092 1/16

2005 年 5 月第一次印刷 印张:14 1/2

印数:1—3 000 字数:340 000

**定价:19.00 元**

(如有印装质量问题,我社负责调换〈环伟〉)

销售部电话:010-62136131 编辑部电话:010-62138978-8004 (HI02)

# 前　言

在人类生活、经济建设和科技发展过程中，“计算”始终都扮演着非常重要的角色. 在对自然界和人类社会各种事物发展规律的研究中，当从定性分析过渡到定量分析时，就必然涉及计算. 例如每天的天气预报，就是根据当前的气温、气压数据按某种方法和程序计算出明、后天的天气甚至以后更长时间的各种气象指标；至于人造飞船上天、原子能的开发和利用以及各种矿藏的勘探与开采等高科技活动就更离不开计算。因此，计算能力的强弱直接制约着一个国家的经济和科技发展速度.

人类的计算能力与计算工具密切相关，早期的计算主要是靠人的大脑再加上一些简单的计算工具来完成，计算效率低，可靠性也很差. 电子计算机的出现大大地提高了人类的计算能力，从而也促进了科学技术的迅猛发展. 最初的电子计算机多用于一般规模的数值计算，因此计算机的出现也催生了计算数学——研究在计算机上实现数值计算的理论与算法的数学分支.

实际上，对科学与工程技术以及数学研究本身的发展需要而言，不仅需要数值计算，还需要公式推导、表达式的化简、函数的微分及积分、精确地解各种方程等计算. 这种计算的特点是对一些符号按确定的规则进行的演算，并且计算过程都是精确的，人们称这种计算为符号计算、公式推演或者代数计算. 这种计算的需求在实践中是大量存在的，例如，1847 年法国天文学家 Delaunay 花了 10 年的时间推导出了月球的轨道公式，又花了另外 10 年来检查他的结果，并于 1867 年将其公布于世. 其结果是非数值的，主要部分都是以公式的形式给出，全部结果长达 128 页之多. 另一个有名的例子是 19 世纪海王星的发现. 人们发现天王星的实际运行轨道与当时的理论不符，猜想它可能受到其他未知行星的干扰. 经过计算，当然包含大量的公式推导，并在计算结果的指导下进行观测，终于发现了海王星.

这些计算的特点都是将计算对象代数化，然后利用代数中的理论及算法进行计算. 人们把这种研究可代数化的数学对象的计算理论与方法的学科，或者说符号计算与代数计算的学科称为计算机代数，或者数学机械化. 简而言之，计算机代数是计算机科学与数学交叉融合的产物，是符号、代数算法的设计、分析、实现和应用的学科. 作为代数算法，它有简单的形式界定（formal specification），有建立在相应数学理论基础之上的正确性证明和渐进时间界限的估计（即所谓计算的复杂性）. 而且代数对象可在计算机的内存中准确地表现出来，因而代数计算可以精确地进行；因为计算是精确的，所以可用的代数算法都必定在有限步内完成运算.

由于代数算法都是建立在数学基础之上的，所以代数及代数几何的发展为代数计算提供了广泛的数学理论基础，同时代数计算的研究也促进了代数理论，特别是构造性代数及代数几何理论的发展. 近年来产生了计算交换代数与计算代数几何等新的研究领域，或者可以说是更为一般的数学机械化的新的研究领域.

如果我们把计算数学理解为研究在计算机上进行计算的数学理论与算法的学科分支，那么以往的计算数学主要研究数值算法的设计、分析、实现和应用及相应的数学理论，而计算机代数则研究符号计算的相关理论，是计算数学发展的新阶段. 与数值计算相比，代数计算要求计算机有高速度与大存储量，所以它与计算机技术发展的联系更为密切. 计算机代数作为新的计算工具，在理论物理、高能物理、天体力学、化学化工、机械学、机器人设计以及计算机的各种应用领域都有广泛的应用，同时也成为数学教学与数学研究的重要工具.

在实际应用中，符号计算、公式推演或者说代数计算的问题很多，而且门类繁杂，在理论基础方面几乎涉及数学的各个分支，在应用方面涉及各个行业领域. 然而由于计算机的计算速度、存储空间限制等诸多原因，这类计算的自动化过程进展十分缓慢，直到 1953 年，Kahrimanian 与 Nolan 才分别在他们的论文中给出第一个计算形式微分的计算机程序，其后这类计算的自动化进程一直徘徊不前. 随着计算机技术的迅速发展，高性能计算机的普及，以及科技工程等实际问题对符号计算的迫切需要，人们开始重视这类计算的理论与算法的研究. 经过近 30 年的发展，符号计算的研究与应用才算真正得到长足的进步.

计算机代数是从 20 世纪 60 年代中期发展起来的，与此同时，一些学术机构和团体也相继成立. 比较有名的如 ACM (the association for computing machinary) 的 SIGSAM (special interest group on symbolic and algebraic manipulation)，该团体还出版了季刊 "SIGSAM Bulletin"；此外还有欧洲的 SAME (symbolic and algebraic manipulation in Europe)，日本与前苏联也成立了相应的研究机构；我国也在中国科学院建立了数学机械化中心，简称 MMRC. 世界各国对符号计算的研究都非常重视，相继设立了一些大型的研究项目，如原欧共体（现称欧盟）的 POSSO 计划及其后继 FRISCO，我国 "八五" 期间的攀登计划项目 "机器证明及其应用"，"九五" 期间的 973 项目 "数学机械化与自动推理平台" 等. 这些项目在理论与应用方面，例如几何定理证明与发现、代数方程、微分方程求解、实多项式系统问题以及诸多计算机应用领域都取得了丰硕的成果.

国际上有关计算机代数的学术交流活动也十分活跃，比如定期举行的综合性系列国际学术会议有 ISSAC (international symposium on symbolic and algebraic computation)，ASCM (asian symposium on computer mathematics)，此外还有许多其他比较专门的系列国际会议，在互联网上用 Symbolic, Algebraic, Geometric, Computation 等关键词搜索，就可以获得相应的信息，这里不再赘述.

计算机代数方向已出版了专门的国际学术刊物 "Journal of Symbolic Computation"，此外，"SIAM Journal on Computer"，"ACM Transactions on Mathematical Software" 也刊登了这方面的论文；Springer 的丛书 "Lecture Notes in Computer Science" 中陆续出版了不少计算机代数的专集；自 20 世纪 90 年代起，已陆续出版了计算交换代数、计算代数几何、算法代数等方面的专著.

与数值计算不同，代数算法的研究与计算机代数的软件系统的研制几乎是同时的. 随着理论研究的深入，一些多层次、多用途的计算机代数软件，例如比较早期的

$\mu$-Math (Derive), Reduce, 后起之秀 Mathematica, Maple, 我国自行开发的 MMP 以及比较专业的 CoCoA 等, 也相继开发出来. 有些计算机代数软件还允许用户定义抽象的代数结构 (例如环和代数), 并对其元素进行操作, 具有这一功能的软件有 Axiom 等.

经 30 余年的发展, 许多计算机代数系统已投入使用, 这些系统的功能日益强大, 效率不断提高. 这些代数系统的主要功能如下。

1) 提供一基本命令集, 可使机器做许多复杂的计算, 包括数值的和符号的计算. 这个特点使得代数系统具有可用性.

2) 提供一种能定义高层命令或扩展原始命令的程序语言, 使得系统具有可开发性.

现有的代数系统可处理的问题如下.

1) 数的计算, 包括整数、有理数、实数和复数的计算, 且既可进行浮点计算又可进行精确计算.

2) 多项式、有理式的各种计算.

3) 矩阵的计算, 且其元素可为符号的.

4) 数学分析中微分、积分、级数和微分方程等计算.

5) 其他各种代数问题的计算.

利用这些计算机代数系统, 已经基本上可以解决实际中出现的绝大部分问题。当然对某些问题其效能还不是很高, 尚有待于进一步的研究和完善.

这些软件已经发挥了很大的作用, 例如, 美国西雅图波音科学研究实验室为利用 Delaunay 的结果推导人造卫星的运行轨道, 使用计算机代数系统重新推导, 结果发现了 3 处错误. 又如, 人们利用计算机代数系统验算了早期的不定积分表, 发现错误高达 1/5～1/4. 在数学教育中, 已经可以使用计算机证明与发现几何定理.

由于计算机代数在科学研究与工程技术中越来越广泛的应用, 每个科研工作者, 包括数学、计算数学、计算机科学以及其他领域的研究人员, 必须掌握计算机代数的基本知识与熟练使用相关的计算机代数软件. 为适应形势发展的需要, 我们从 1992 年开始为吉林大学计算专业的研究生和本科生开设计算机代数课程, 并在 1997 年由吉林大学出版社出版了计算机代数教材, 讲述计算机代数的基本原理与算法. 经过几年的教学实践, 发现原书有很多错误与疏漏之处, 实感确有修订之必要, 在吉林大学教材科和科学出版社的支持下, 我们进行了修订工作. 本次修订主要是修正原书的错误, 补充疏漏和一些不完善的地方. 考虑到作为计算机代数的入门教材, 不宜过多地引入新的内容, 因此本次修订未对结构做调整.

在学习计算机代数的过程中, 对计算数学、抽象代数以及交换代数等有关基本知识有一些必要的了解是大有裨益的. 考虑到一般学生可能没有学过抽象代数, 我们在第 1 章及附录中介绍了必要的抽象代数与交换代数的基本内容. 此外, 因为计算机代数中有些算法理论涉及比较深刻的专门知识, 我们感到要想做到教材内容的自包含是比较困难的, 在有些情况下不得不放弃某些算法所依据的理论而仅仅描述算法本身. 虽然计算机代数所包含的内容十分广泛, 但由于篇幅所限, 本书仅仅选取了与多项式问题紧密相关的那些内容的基本部分.

张树功对第1～6章及附录A进行修订；附录B由雷娜和刘停战编写.

冯果忱教授一直对本书的编写给予了关心和鼓励，在此表示感谢.

本书是作者在计算机代数教学方面的一个尝试，由于作者水平有限，不可避免地存在这样或那样的错误和不足，殷切希望各位专家和同行们提出宝贵意见和建议.

# 目　录

# 第 1 章　代数基本知识与大整数的处理

本章简要地介绍一些代数基本知识和大整数的表示与处理方法，其中的代数内容是学习本书的必备基础知识，而大整数的处理是计算机代数的最基本问题. 因为计算机代数中的计算大都是精确计算，不允许使用浮点数，所以无论在计算的过程中，还是在计算的结果里，数据的位数可能都很长，这就要求必须对整数的表示与计算加以研究，以便设计出最经济的表示方式与最高效的算法.

## 1.1　代数基本知识

### 1.1.1　基本概念

**定义1.1.1**　设 $\boldsymbol{G}$ 是一非空集合，如果其上定义了一个双项运算“$\circ$”，$\boldsymbol{G}$ 在该双项运算下是封闭的，且满足下述公理：

$A_1$(结合律)：对所有 $a$，$b$，$c \in \boldsymbol{G}$，成立

$$a \circ (b \circ c) = (a \circ b) \circ c; \tag{1.1.1}$$

$A_2$(单位元)：存在 $e \in \boldsymbol{G}$，使得对任何 $a \in \boldsymbol{G}$，成立

$$e \circ a = a \circ e = a; \tag{1.1.2}$$

$A_3$(逆元素)：对每个 $a \in \boldsymbol{G}$，存在元 $a^{-1} \in \boldsymbol{G}$，使得

$$a \circ a^{-1} = a^{-1} \circ a = e; \tag{1.1.3}$$

则称 $(\boldsymbol{G}, \circ)$ 为一个**群**. 有时简单地记作 $\boldsymbol{G}$.

**例 1.1.1**　所有整数全体$\mathbb{Z}$在通常的加法之下构成一群，0 是其加法单位元；所有 $m \times n$ 阶矩阵在通常的矩阵加法之下也构成一群，0 矩阵为其加法单位元；又如所有 $n$ 阶可逆方阵在通常的乘法之下也构成一群，单位阵为其乘法单位元.

**定义 1.1.2**　一个群 $\boldsymbol{G}$ 称为**交换群**，或称 **Abel 群**，如果其上的双项运算还满足

$A_4$(交换律)：对所有 $a$，$b \in \boldsymbol{G}$，成立

$$a \circ b = b \circ a. \tag{1.1.4}$$

**例 1.1.2**　例 1.1.1 中的整数加法群是交换群；$m \times n$ 阶矩阵的加法群也是交换群，但 $n$ 阶可逆矩阵的乘法群却不是交换群，因为矩阵的乘法一般是不可交换的.

**定义 1.1.3**　设 $\boldsymbol{R}$ 为一非空集合，如果在其上定义了两个双项运算“+”和“$\cdot$”使得 $(\boldsymbol{R}, +)$ 是一交换群，“$\cdot$”运算满足结合律且有单位元，并对所有 $a$，$b$，$c \in \boldsymbol{R}$ 满足

$A_5$(分配律)：

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c), \end{aligned} \tag{1.1.5}$$

则称 $(\boldsymbol{R}, +, \cdot)$ 是一个**环**.

如果 $(\boldsymbol{R}, +, \cdot)$ 是一个环且运算“$\cdot$”还是交换的，则称其为一**交换环**.

对于一般的交换环，我们通常称运算“+”为加法，运算“$\cdot$”为乘法，并记交换环上的

加法单位元为 0，乘法单位元为 1.

**例 1.1.3** 整数全体$\mathbb{Z}$在通常的加法和乘法之下构成一交换环；$n$ 阶矩阵全体在通常的加法和乘法之下却不是交换环，但如果仅考虑所有关于乘法可交换的 $n$ 阶矩阵全体，则其在通常的加法与乘法之下构成一交换环.

**定义 1.1.4** 如果 $(\boldsymbol{R}, +, \cdot)$ 是一交换环且运算"·"还满足下述公理：

$A_6$(消去律)：对所有 $a, b, c \in \boldsymbol{R}$，有

$$a \cdot b = a \cdot c,\ a \neq 0 \text{ 蕴含 } b = c, \tag{1.1.6}$$

则称其为**一整环**.

上述定义等价于：$a, b \in \boldsymbol{R}$，

$$a \cdot b = 0,\ a \neq 0 \text{ 蕴含 } b = 0.$$

该等价定义无非是说，没有零因子的交换环即为整环. 整数环$\mathbb{Z}$是整环，而在例 1.1.3 中提到的所有可交换的 $n$ 阶矩阵全体在通常的加法与乘法之下却不是整环，因为两个非零 $n$ 阶方阵的乘积可以是零矩阵.

**定义 1.1.5** 如果集合 $\boldsymbol{K}$ 上定义了双项运算 + 和·，并且 $(\boldsymbol{K}, +)$ 和 $(\boldsymbol{K} - \{0\}, \cdot)$ 都是一交换群. 又运算·关于运算 + 满足分配律，则称 $(\boldsymbol{K}, +, \cdot)$ 是**一域**. 换言之，如果一交换环上的每个非零元都有乘法逆，则该交换环就是一个域.

为了方便，我们将省略运算符·，而将 $a \cdot b$ 简单地记作 $ab$.

**例 1.1.4** 整数环$\mathbb{Z}$在通常的加法与乘法之下虽然构成一整环，但它不是域，因为除了 1 和 −1 之外，其他整数都没有乘法逆. 但所有有理数的集合$\mathbb{Q}$在通常的加法和乘法之下构成一域. 在域中，因为非零元有乘法逆，所以相当于可以进行除法运算.

**例 1.1.5** 有理数域$\mathbb{Q}$上的一元多项式全体，记为 $\mathbb{Q}[x]$，在通常的多项式加法和乘法之下构成一交换环. 下面来证$\mathbb{Q}[x]$是整环，即要证明下述事实：如果 $A, B \in \mathbb{Q}[x]$ 且 $B \neq 0, AB = 0$，则必有 $A = 0$. 不妨设

$$A = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0, B = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0,\ b_n \neq 0,$$

考虑乘积

$$AB = \sum_{l=0}^{m+n}\Big(\sum_{i+j=l} a_i b_j\Big)x^l = 0$$

的 $n \sim m + n$ 次幂的系数，可得

$$\begin{aligned}
a_m b_n &= 0,\\
a_m b_{n-1} + a_{m-1} b_n &= 0,\\
a_m b_{n-2} + a_{m-1} b_{n-1} + a_{m-2} b_n &= 0,\\
&\cdots\cdots\\
a_m b_{n-m} + a_{m-1} b_{n-m+1} + \cdots + a_0 b_n &= 0(\text{若 } n \geqslant m),\\
a_m b_0 + a_{m-1} b_1 + \cdots + a_{m-n} b_n &= 0(\text{若 } m \geqslant n),\\
&\cdots\cdots\\
a_n b_0 + a_{n-1} b_1 + \cdots + a_0 b_n &= 0.
\end{aligned}$$

因为 $b_n \neq 0$，由第一个方程可以推出 $a_m = 0$，再由第二个方程可以推出 $a_{m-1} = 0$，进而可推出 $a_m = a_{m-1} = \cdots = a_0 = 0$，这就证明了 $A = 0$.

### 1.1.2 可除性与整环中的分解

除法的概念在符号计算中起着非常重要的作用. 当然一提到除法,就意味着运算总是在域里进行的. 在环里进行一般的除法运算是不可能的. 但是在环里可以有因子分解的概念, 下面就来讨论这个问题. 除非特别说明, 此后所提及的环 $\boldsymbol{D}$ 都是指整环.

**定义 1.1.6** 设 $a$, $b \in \boldsymbol{D}$, $a$ 称为 $b$ 的一个**因子**, 如果存在 $c \in \boldsymbol{D}$ 使得 $b = ac$, 此时也称 $a$ **整除** $b$, 记作 $a \mid b$, 相应地称 $b$ 为 $a$ 的**倍式**.

对于 $a$, $b \in \boldsymbol{D}$, 如果存在 $c \in \boldsymbol{D}$, 使得 $c$ 为 $a$ 和 $b$ 的公因子且 $a$ 和 $b$ 的其他公因子都整除 $c$, 则称 $c$ 为 $a$ 和 $b$ 的**最大公因子**(greatest common divisor), 记作 $c = \gcd(a, b)$.

设 $a$, $b \in \boldsymbol{D}$, 如果存在 $c \in \boldsymbol{D}$, 使得 $c$ 为 $a$ 和 $b$ 的倍式且 $a$ 和 $b$ 的其他倍式都是 $c$ 的倍式, 则称 $c$ 为 $a$ 和 $b$ 的**最小公倍式**(least common multiple), 记作 $c = \operatorname{lcm}(a, b)$.

例如,对于整数 6 和 $-9$, 按照定义, 其最大公因子既可取为 3, 也可以取为 $-3$, 即最大公因子是不唯一的. 同样,最小公倍式也存在这个问题. 但是仔细分析会发现, 如果整环中的两个元有多个最大公因子, 它们必定都是相互整除的. 这就引出了如下的定义.

**定义 1.1.7** 设 $a$, $b \in \boldsymbol{D}$, 如果同时成立 $a \mid b$ 与 $b \mid a$, 则称 $a$, $b$ 是**相伴的**.

在整数环$\mathbb{Z}$中, 1 和 $-1$ 是相伴的. 在$\mathbb{Q}[x]$中,对任意的 $a \in \mathbb{Q}$, $a \neq 0$, $a(x+1)$ 与 $(x+1)$ 相伴.

若 $a$, $b \in \boldsymbol{D}$ 是相伴的, 则存在 $u_1$, $u_2 \in \boldsymbol{D}$, 使得 $a = u_1 b$, $b = u_2 a$. 将后式代入前式得 $a = u_1 u_2 a$, 再由消去律可得 $u_1 u_2 = 1$. 于是有如下定义。

**定义 1.1.8** 如果 $u$ 在 $\boldsymbol{D}$ 中有乘法逆元,元素 $u \in \boldsymbol{D}$ 称为**可逆的**.

在有理数域$\mathbb{Q}$中,每个非零元都是可逆元;在整数环$\mathbb{Z}$中, 可逆元只有两个, 即 1 和 $-1$. 因此两个相伴的整数可以有相同的符号, 也可以有相反的符号. 由此可知整数的最大公因子可以相差一个正负号. 两个整数的最小公倍式也是如此.

为了消除这种不确定性, 我们将整环 $\boldsymbol{D}$ 中的元按相伴关系分类, 两个元在一类,当且仅当它们是相伴的. 因为 0 没有相伴的元, 故其自己划为一类. 容易证明相伴关系是等价关系,这种类称为**相伴类**. 例如整数环的相伴类为

$$\{0\},\ \{1,\ -1\},\ \{2,\ -2\},\ \cdots$$

我们可以按照某种确定的规则在每个相伴类里选出一个代表元, 称这个代表元为**规范元**. 例如在整数环的情形, 可以定义非负整数为规范元. 对任何域 $\boldsymbol{K}$, 因为其上的每个非零元都是可逆的, 因此域上的相伴类只有两个, 即$\{0\}$和 $\{a \mid 0 \neq a \in \boldsymbol{K}\}$, 此时定义其规范元为 0 和 1.

现在可以来解决最大公因子的不唯一问题了.

设 $\boldsymbol{D}$ 为一整环, 在其上定义了规范元. 对 $a$, $b \in \boldsymbol{D}$, 如果 $c$ 是 $a$, $b$ 的最大公因子且 $c$ 为规范的, 则称 $c$ 为 $a$, $b$ 的**规范最大公因子**, 仍记作 $c = \gcd(a, b)$. 显然对于整环中给定的两个元, 其规范最大公因子是唯一的. 我们约定以后所说的最大公因子都是指规范最大公因子.

在选择相伴类的代表元时, 所采用的规则最好满足以下几个条件.

1) 0 是规范元.

2) 1 是可逆元所在相伴类的规范元.

3) 若 $a$, $b$ 是规范元, 则其乘积 $ab$ 也是规范元.

因为在同一相伴类中任何两个元素都相差一个可逆元. 因此对给定的任何一元, 可以将其写成它所在的相伴类的代表元与一可逆元的乘积, 且容易证明这样的可逆元是唯一的. 更准确地说, 我们有如下定义.

**定义 1.1.9** 设 $\boldsymbol{D}$ 为一整环, 在其上定义了规范元. 对任何 $a \in \boldsymbol{D}$, $a$ 的**规范部分**记作 $n(a)$, 定义为包含 $a$ 的相伴类的规范元. $a$(当 $a \neq 0$ 时)的**可逆部分** 记作 $u(a)$, 为 $\boldsymbol{D}$ 中使得 $a = u(a)n(a)$ 成立的唯一可逆元. 对于 $0 \in \boldsymbol{D}$, 易见 $n(0) = 0$. 为方便计算, 定义 0 的可逆部分为 $u(0) = 1$.

例如对整数环$\mathbb{Z}$, 其上的整数 $a$ 的规范部分可定义为 $n(a) = |a|$, 而其可逆部分则可定义为 $u(a) = \text{sign}(a)$. 其中, sign$(\cdot)$ 为符号函数.

对于整环中任意两个元素, 如果它们的最小公倍式存在, 可以利用下述方法将其唯一化. 容易验证, 若 $a$, $b \in \boldsymbol{D}$ 为两个给定元素, 则 $ab/\gcd(a, b)$ 为 $a$, $b$ 的一个最小公倍式. 因此可以定义 $a$, $b$ 的最小公倍式的规范元为 $n(ab)/\gcd(a, b)$.

为了讨论环中元素的分解问题, 我们需要下列定义.

**定义 1.1.10** 设 $\boldsymbol{D}$ 为整环, 若 $p \in \boldsymbol{D} - \{0\}$ 满足如下两个条件:

1) $p$ 不是可逆元.

2)如果 $p$ 可以写成 $p = ab$, 则 $a$, $b$ 二者之一必为可逆元, 则称 $p$ 为**素元**或**不可约元**.

如果 $\gcd(a, b) = 1$, 两个元素 $a$, $b \in \boldsymbol{D}$ 称为**互素的**.

例如在整数环$\mathbb{Z}$中, 素元就是通常的素数; 而在有理数域$\mathbb{Q}$中没有素元.

**定义 1.1.11** 一整环 $\boldsymbol{D}$ 称为**唯一分解整环**, 简记为 UFD, 如果对所有 $a \in \boldsymbol{D} - \{0\}$, 或者 $a$ 是一可逆元, 或者 $a$ 可以表示为有限多个素元 $p_1$, $p_2$, …, $p_n$ 的乘积 $a = p_1 p_2 \cdots p_n$. 并且这种表示在不考虑相伴元和次序时是唯一的.

上述定义中后一句话的含义是: 若 $a$ 有 $a = p_1 p_2 \cdots p_n$ 和 $a = q_1 q_2 \cdots q_m$ 这两种表示, 其中 $p_i$, $q_i (i \in n, i \in m)$ 为素元, 则必有 $m = n$, 且当重新排列 $q_i$ 的次序后 $p_i$ 与 $q_i$ 相伴.

注意, 在上述定义中并没有要求 $p_i$ 是两两互异的.

唯一分解整环中素元的一个基本性质是: 如果 $p$ 为素元, 且 $p \mid ab$, 则必有 $p \mid a$ 或者 $p \mid b$.

如果考虑到上述定义中 $p_i$ 有相同的可能并利用规范表示, 则有下列定义.

**定义 1.1.12** 设 $\boldsymbol{D}$ 为 UFD, 且其上定义了规范元, 则 $a \in \boldsymbol{D}$ 的素分解形式

$$a = u(a) p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n} \tag{1.1.7}$$

称为一个**规范可逆分解**, 如果 $p_i$, $1 \leqslant i \leqslant n$, 为规范素元, $d_i$, $1 \leqslant i \leqslant n$, 为正整数, 且当 $i \neq j$ 时, $p_i \neq p_j$.

应该说明的是, 并非每个整环都是 UFD, 而且整环中的元素也未必都有最大公因子. 但是在 UFD 中, 最大公因子总是存在的.

**定理 1.1.1** 若 $\boldsymbol{D}$ 为 UFD 并且 $a$, $b \in \boldsymbol{D}$ 不同时为零, 则 $\gcd(a, b)$ 存在且唯一.

**证明** 利用规范元, 可使唯一性得到保证. 为证明存在性, 假设 $a \neq 0$, $b \neq 0$ 的唯

一规范可逆分解为

$$a = u(a)p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}, \quad b = u(b)q_1^{e_1}q_2^{e_2}\cdots q_m^{e_m}. \tag{1.1.8}$$

其中 $p_i$, $q_i(i \in n, i \in m)$ 为规范元. 记 $r_1$, $r_2$, …, $r_l$ 为 $\{p_1, \cdots, p_n, q_1, \cdots, q_m\}$ 中那些不同的元素, 则分解式(1.1.8)可以写成

$$a = u(a)\prod_{i=1}^{l} r_i^{t_i}, \quad b = u(b)\prod_{i=1}^{l} r_i^{s_i}. \tag{1.1.9}$$

式中某些 $t_i$, $s_i$ 可能为0. 显然 $d = \prod_{i=1}^{l} r_i^{\min(t_i, s_i)}$ 是$a$, $b$ 的最大公因子. 如果 $a$, $b$ 之一为 0, 不妨设 $b = 0$, 则 $d = \prod_{i=1}^{n} p_i^{d_i}$ 即为$a$, $b$ 的最大公因子.

在多项式的各种运算中, 一个很重要的运算就是所谓的带余除法, 而带余除法在一般的整环中未必成立, 因此需要引入新的定义.

**定义 1.1.13** 设 $\boldsymbol{D}$ 为整环, 如果在其上定义了一个**赋值**

$$v: \boldsymbol{D} - \{0\} \longrightarrow \boldsymbol{N}.$$

此处 $\boldsymbol{N}$ 为非负整数集合, 且 $v$ 具有下述性质.

$P_1$: 对所有 $a$, $b \in \boldsymbol{D} - \{0\}$, $v(ab) \geqslant v(a)$ 成立.

$P_2$: 对所有 $a$, $b \in \boldsymbol{D}$, 其中 $b \neq 0$, 存在 $q$, $r \in \boldsymbol{D}$ 使得

$$a = qb + r. \tag{1.1.10}$$

其中 $r$ 或者为 0 或者满足 $v(r) < v(b)$. 定义了这种赋值的整环称为 Euclid **整环**.

整数环$\mathbb{Z}$在赋值 $v(a) = |a|$ 之下是一 Euclid 整环.

上述定义中的性质 $P_2$ 称为除法性质, 这种除法称为**带余除法**或 Euclid **除法**, 其中 $q$ 和 $r$ 分别称为$a$ 除以$b$ 的**商**和**余式**. 在一般的 Euclid 整环中, 商和余式未必是唯一确定的. 例如对 Euclid 整环$\mathbb{Z}$, 取 $a = -8$, $b = 3$, 则有

$$-8 = (-2)\times 3 - 2 \text{ 或者 } -8 = (-3)\times 3 + 1,$$

即两个数, 对 $q = -2$, $r = -2$ 和 $q = -3$, $r = 1$ 都满足性质 $P_2$. 对一些我们感兴趣的 Euclid 整环, 可以设法定义适当的赋值, 使得 Euclid 除法中的商和余式是唯一的. 比如对整数环$\mathbb{Z}$, 若要求 $r \geqslant 0$, 则 Euclid 除法中的商和余式就是唯一的.

在 Euclid 整环中, 利用带余除法, 可以计算两个元素的最大公因子(如果存在).

**定理 1.1.2** 设 $\boldsymbol{D}$ 为 Euclid 整环, $a$, $b \in \boldsymbol{D}$ 且$b \neq 0$. 又设 $q$, $r$ 为商和余式, 使得 $a = qb + r$, 且或有 $r = 0$ 或有 $v(r) < v(b)$, 则

$$\gcd(a, b) = \gcd(b, r). \tag{1.1.11}$$

**证明** 设 $g = \gcd(a, b)$, $h = \gcd(b, r)$, 则由 $a = qb + r$ 可知, $h$ 为$a$, $b$ 的公因子, 当然应该有 $h \mid g$. 同理, 再由 $r = a - qb$ 可知, $g$ 也为$b$, $r$ 的公因子, 故也有 $g \mid h$. 又因为 $g$ 和$h$ 都是规范元, 所以 $g = h$.

下面讨论如何利用带余除法来计算 Euclid 整环中两个元素的最大公因子.

设 $\boldsymbol{D}$ 为 Euclid 整环, $a$, $b \in \boldsymbol{D}$ 且$a$, $b$ 均不为零. 记 $r_0 = a$, $r_1 = b$, 则有 $q_1$, $r_2 \in \boldsymbol{D}$, 使得

$$r_0 = q_1 r_1 + r_2, \text{ 且或 } r_2 = 0 \text{ 或 } v(r_2) < v(r_1). \tag{1.1.12}$$

如果 $r_2 \neq 0$, 则又有 $q_2$, $r_3 \in \boldsymbol{D}$, 使得

$$r_1 = q_2 r_2 + r_3, \text{ 且或 } r_3 = 0 \text{ 或 } v(r_3) < v(r_2). \tag{1.1.13}$$

如此进行下去，则得一序列 $r_1, r_2, \cdots, r_k, \cdots$ 但是该序列的赋值满足

$$v(r_1) > v(r_2) > \cdots > v(r_k) > \cdots \tag{1.1.14}$$

这是一个严格单调下降的非负整数列，因此必有整数 $l$，使得 $r_l \neq 0$，$r_{l+1} = 0$. 倘若不然，则因 $v(r_k) - v(r_{k+1}) \geqslant 1$，$v(r_k) \geqslant 0$，必有 $l - 1 \leqslant v(r_1) - v(r_l) \leqslant v(r_1)$ 对任意 $l$ 成立，这显然是不可能的，于是

$$r_{l-1} = q_l r_l, \tag{1.1.15}$$

由定理 1.1.2，有

$$\begin{aligned} \mathrm{n}(r_l) &= \gcd(r_l, r_{l-1}) \\ &= \gcd(r_{l-1}, r_{l-2}) \\ &\quad \cdots\cdots \\ &= \gcd(r_1, r_0) \\ &= \gcd(a, b). \end{aligned} \tag{1.1.16}$$

利用上述推导，我们还得到如下定理.

**定理 1.1.3** 设 $\boldsymbol{D}$ 为 Euclid 整环，$a, b \in \boldsymbol{D}$，且 $c$ 为 $a$，$b$ 的最大公因子，则存在 $s$，$t \in \boldsymbol{D}$，使得

$$c = sa + tb. \tag{1.1.17}$$

**证明** 我们来证，对每个 $r_k$，有 $s_k$，$t_k \in \boldsymbol{D}$，使得

$$r_k = s_k a + t_k b, \tag{1.1.18}$$

对 $k = 0, 1, 2$，显然有 $s_0 = 1$，$t_0 = 0$，$s_1 = 0$，$t_1 = 1$，$s_2 = 1$，$t_2 = -q_1$. 假设当 $k \leqslant l - 1$ 时，有 $s_k$，$t_k \in \boldsymbol{D}$ 使得式(1.1.18)成立. 则当 $k = l$ 时，由 $r_{l-2} = q_{l-1} r_{l-1} + r_l$，得

$$\begin{aligned} r_l &= r_{l-2} - q_{l-1} r_{l-1} \\ &= (s_{l-2} a + t_{l-2} b) - (q_{l-1}(s_{l-1} a + t_{l-1} b)) \\ &= (s_{l-2} - q_{l-1} s_{l-1}) a + (t_{l-2} - q_{l-1} t_{l-1}) b. \end{aligned} \tag{1.1.19}$$

取

$$s_l = s_{l-2} - q_{l-1} s_{l-1}, \quad t_l = t_{l-2} - q_{l-1} t_{l-1},$$

可知结论对 $k = l$ 亦对. 最后注意到 $n(r_l) = \gcd(a, b)$，在式的两端同时乘以 $u(r_l)^{-1}$ 则得定理结论.

上述证明过程实际上也给出了计算 $s$，$t$ 的递推公式：

$$s_k = s_{k-2} - q_{k-1} s_{k-1}, \quad t_k = t_{k-2} - q_{k-1} t_{k-1}. \tag{1.1.20}$$

设 $a_1, \cdots, a_n \in \boldsymbol{D}$，$n > 2$，则 $n$ 个元素的最大公因子可以递归地定义为

$$\gcd(a_1, \cdots, a_n) = \gcd(\gcd(a_1, \cdots, a_{n-1}), a_n). \tag{1.1.21}$$

如果 $\gcd(a_1, \cdots, a_n) = 1$，则 $n$ 个元素 $a_1, \cdots, a_n \in \boldsymbol{D}$ 称为互素的.

由定理 1.1.3 可得：

**推论 1.1.1** 设 $c$ 为 $a_1, \cdots, a_n \in \boldsymbol{D}$ 的最大公因子，则存在 $s_1, \cdots, s_n \in \boldsymbol{D}$，使得

$$c = s_1 a_1 + s_2 a_2 + \cdots + s_n a_n. \tag{1.1.22}$$