UMSS

大学数学科学丛书 — 1

代数导引

万哲先 著

科学出版社
www.sciencep.com

大学数学科学丛书 1

代 数 导 引

万哲先 著

科 学 出 版 社

北 京

内 容 简 介

本书将抽象代数导引和线性代数初步揉合在一起，并详细地阐述了有限域的结构，有限域上二次型的合同标准形，以及有限域上多项式的因式分解．本书的编写贯穿了从具体到抽象及具体演算和严格推导并重这两个原则．

本书内容覆盖了大学及师范院校抽象代数和线性代数这两门课程的教学内容，可用作教材，亦可作自学之用．

图书在版编目(CIP)数据

代数导引／万哲先著．—北京：科学出版社，2004
(大学数学科学丛书；1)
ISBN 7-03-013406-0

Ⅰ.代… Ⅱ.万… Ⅲ.代数-高等学校-教材 Ⅳ.O15

中国版本图书馆 CIP 数据核字(2004)第 041648 号

责任编辑：吕 虹／责任校对：钟 洋
责任印制：钱玉芬／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
源海印刷有限责任公司印刷
科学出版社发行 各地新华书店经销
*
2004 年 8 月第 一 版 开本：B5(720×1000)
2004 年 8 月第一次印刷 印张：23 1/4
印数：1—3 000 字数：425 000

定价：38.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

《大学数学科学丛书》序

按照恩格斯的说法，数学是研究现实世界中数量关系和空间形式的科学. 从恩格斯那时到现在，尽管数学的内涵已经大大拓展了，人们对现实世界中的数量关系和空间形式的认识和理解已今非昔比，数学科学已构成包括纯粹数学及应用数学内含的众多分支学科和许多新兴交叉学科的庞大的科学体系，但恩格斯的这一说法仍然是对数学的一个中肯而又相对来说易于为公众了解和接受的概括，科学地反映了数学这一学科的内涵. 正由于忽略了物质的具体型态和属性、纯粹从数量关系和空间形式的角度来研究现实世界，数学表现出高度抽象性和应用广泛性的特点，具有特殊的公共基础地位，其重要性得到普遍的认同.

整个数学的发展史是同人类物质文明和精神文明的发展史交融在一起的. 作为一种先进的文化，数学不仅在人类文明的进程中一直起着积极的推动作用，而且是人类文明的一个重要的支柱. 数学教育对于启迪心智、增进素质、提高全人类文明程度的必要性和重要性已得到空前普遍的重视. 数学教育本质是一种素质教育；学习数学，不仅要学到许多重要的数学概念、方法和结论，更要着重领会到数学的精神实质和思想方法. 在大学学习高等数学的阶段，更应该自觉地去意识并努力体现这一点.

作为面向大学本科生和研究生以及有关教师的教材，教学参考书或课外读物的系列，本丛书将努力贯彻加强基础、面向前沿、突出思想、关注应用和方便阅读的原则，力求为各专业的大学本科生或研究生（包括硕士生及博士生）走近数学科学、理解数学科学以及应用数学科学提供必要的指引和有力的帮助，并欢迎其中相当一些能被广大学校选用为教材，相信并希望在各方面的支持及帮助下，本丛书将会愈出愈好.

李大潜

2003 年 12 月 27 日

序　言

本书是根据作者 1976 年 3 月出版的《代数和编码》一书中代数部分(即第一、二、五章)增补、改写而成. 该书曾于 1980 年出版修订版, 并多次重印, 现在已经绝版. 这次增补、改写, 主要是将原书第一章"抽象代数的基本概念和有限域的结构"拆成第一、三、四章并增写了第二章、第三章 3.4 节和第四章 4.4 节. 同时将原书第二章"线性代数初步"拆成第五、七、八章并增写了第六章、第七章 7.3 节和第九章. 其余章节也有一些小的增补和改动, 不再一一列举. 增补、改写的目的是希望这本书能成为大学和师范院校数学系抽象代数和线性代数(或高等代数)这两门课程的教材或教学参考书, 因此增补了这两门课程教学大纲中没有包括在《代数和编码》一书中的一些内容.

《代数和编码》一书是当时为工程技术人员编写的, 因此在编写时力求从具体实例出发, 引出抽象概念, 强调计算而不只偏重理论推导. 这次增补、改写也贯穿了上述两个原则. 因此本书仍适合工程技术人员阅读. 采用这两个原则来编书, 对于在学的大学生也是有益的, 他们不会认为代数只是抽象概念和理论推导的堆积, 通过具体实例引出代数概念, 可以深刻领会它们的涵义, 通过例题的演算也可以学会代数计算的技巧和明了理论推导的线索.

这本书的另一个特点是用较大的篇幅来讨论有限域和有限域上的多项式, 这主要是因为它们有许多重要的工程技术应用, 同时学习抽象代数一方面应该把它们落实到复数域、实数域、有理数域和整数环等这一些常见的代数结构, 另一方面也可以落实到有限域. 这对理解和掌握抽象代数是有帮助的.

这本书的第一、二、三、四、六章可以作为抽象代数的教材, 它的第五、七、八、九章可以作为线性代数的教材. 其实这两部分内容在本书中是有机地贯穿在一起的. 因此也可以把抽象代数和线性代数合并成一门代数课, 而连贯地采用这本书的前九章作为教材.

这本书前九章还包括了教学大纲以外的一些内容, 这些材料可以有选择地作为学生的课外阅读材料, 读了可以开宽眼界, 启发思路.

第十章(即原书第五章)应该是计算代数的内容之一, 为了工程技术人员的需要仍把它保留下来. 计算代数还应该包括 Gröbner 基、Sturm 定理、计算群论等内容. 计算代数的重要性日益明显, 希望不久的将来它能成为大专院校数学系的必修课.

这本书的增补、改写得到了河北北方学院霍元极、寇福来教授的大力帮助和推动. 他们花了不少精力、心血和时间, 积极地和作者讨论应该增添改写哪些内容并协助作者编写, 还将本书用CCT排版系统输入到计算机里. 没有他们的帮助和推动, 本书是很难完成的. 谨向他们致以衷心的感谢.

作者还要感谢山东理工大学和范跃进教授, 他们为作者提供了良好的生活环境和优越的工作条件, 使作者能在山东张店山东理工大学的校园里完成本书的编写. 张店是作者童年生活和学习的地方, 1932~1936年作者曾在张店生活了4年, 并就读于胶济铁路张店小学. 作者对张店和胶济铁路张店小学怀有深厚的感情, 每次乘火车路过张店都要下车在月台上漫步, 凝视张店的草木和建筑, 目睹张店的发展和进步, 并回忆过去在张店的生活和学习. 作者愿以此书来寄托对它们的怀念.

万哲先

2003年5月于山东张店

目　录

预 备 知 识

我们先介绍阅读本书所需要的一些预备知识：首先给出集合和映射这两个基本概念，然后介绍整数的因数分解.

0.1 集合和映射

集合和映射是近代数学中的两个基本概念，我们在下面对它们作一扼要的介绍.

所谓*集合* 就是指作为整体来考察的一堆东西. 例如，有理数的全体就组成一个集合，实数的全体也组成一个集合. 我们用 $\mathbb{Q}$ 表示全体有理数组成的集合，用 $\mathbb{R}$ 表示全体实数组成的集合，而用 $\mathbb{Z}_p$ 表示由 $0, 1, 2, \cdots, p-1$ 组成的集合. 组成集合的成员叫做这个集合的*元素*. 我们用

$$a \in M$$

表示 a 是集合 M 的元素，读作 *a属于M*; 用

$$a \notin M$$

表示 a 不是集合 M 的元素，读作 *a不属于M*.

通常有两种办法给出一个集合，一种是列举出它的全部元素，一种是给出这个集合的元素所具有的特征性质. 譬如，$\mathbb{Z}_p$ 是由 $0, 1, 2, \cdots, p-1$ 这 p 个元素组成的集合，记作

$$\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\},$$

这就是列举出 $\mathbb{Z}_p$ 的全部元素. 又如 $\mathbb{Q}[\sqrt{2}]$ 是由一切形如

$$a + b\sqrt{2}$$

的实数组成的集合，其中 a 和 b 是有理数，记作

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\},$$

这就是给出 $\mathbb{Q}[\sqrt{2}]$ 中元素的特征性质. 括号 $\{\cdots\}$ 中的符号 ":" 之前的 $a + b\sqrt{2}$ 表明 $\mathbb{Q}[\sqrt{2}]$ 中元素的形状，但 a, b 究竟是什么则由符号 " : " 之后的性质 $a, b \in \mathbb{Q}$ 来说明.

为了处理问题的方便，我们引进*空集合* 的概念. 我们把空集合看作是不包含任何元素的集合，并记作 $\emptyset$. 其他的集合叫做*非空集合*. 因此，非空集合就是确实包含元素的集合.

我们用 $|M|$ 表示集合 M 所包含元素的个数，称之为集合 M 的*基数*. 如果 $|M|$ 是一个有限数，我们就说 M 是一个*有限集*. 我们把空集合看作是含 0 个元素的有限集，即 $|\emptyset| = 0$. 如果 M 不是有限集，我们就把它叫做*无限集*.

如果两个集合 M 与 N 含有完全相同的元素，即 $a \in M$ 当且仅当 $a \in N$, 那么就说这两个集合 **相等**, 记作

$$M = N.$$

如果集合 M 的元素都是集合 N 的元素，即从 $a \in M$ 可以推出 $a \in N$, 那么就说 M 是 N 的 **子集合**(简称 **子集**), 记作

$$M \subset N \quad 或 \quad N \supset M.$$

例如，设 $\mathbb{Q}, \mathbb{R}$ 和 $\mathbb{C}$ 分别是有理数集、实数集和复数集. 那么 $\mathbb{Q} \subset \mathbb{R}, \mathbb{R} \subset \mathbb{C}$. 根据定义，每个集合都是它自己的子集合. 我们还规定，空集是任一集合的子集合.

设 M 是一个集合， N 是 M 的一个子集合. 我们用 $M \setminus N$ 表示由 M 中不属于 N 的那些元素所组成的集合，即

$$M \setminus N = \{a : a \in M \text{ 而 } a \notin N\}.$$

$M \setminus N$ 称为集合 N 在 M 中的 **余集**. 例如，如果 $\mathbb{Z}$ 是全体整数所组成的集合，$2\mathbb{Z}$ 是全体偶数 (包含 0) 组成的集合，那么 $\mathbb{Z} \supset 2\mathbb{Z}$, 并且 $\mathbb{Z} \setminus 2\mathbb{Z}$ 是由全体奇数组成的集合.

设 M 和 N 是两个集合. 由既属于 M 又属于 N 的全体元素所组成的集合叫做 M 和 N 的 **交**, 记作

$$M \cap N,$$

即

$$M \cap N = \{a : a \in M \text{ 且 } a \in N\}.$$

例如，当 M 是全体偶数组成的集合，而 N 是全体小于 7 的正整数所组成的集合时，

$$M \cap N = \{2, 4, 6\}.$$

对于任意两个集合，显然有

$$M \cap N \subset M, \quad M \cap N \subset N.$$

仍设 M 和 N 是两个集合. 由属于集合 M 或属于集合 N 的全体元素所组成的集合叫做 M 和 N 的 **并**, 记作

$$M \cup N.$$

例如，

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

显然有

$$M \cup N \supset M, \quad M \cup N \supset N.$$

集合的交和并这两个概念可以推广到任意多个 (有限多个或无限多个) 集合的情形. 设 I 是一个足码集合. 又设对于每个 $\alpha \in I$, 都有一个集合 M_α. 那么，由属于每一个 $M_\alpha (\alpha \in I)$ 的元素的全体所组成的集合叫做这些 M_α 的 **交**, 记作

$$\cap_{\alpha\in I}M_\alpha.$$

同样，由属于任何一个 $M_\alpha(\alpha\in I)$ 的元素的全体组成的集合叫做这些 M_α 的**并**，记作

$$\cup_{\alpha\in I}M_\alpha.$$

显然有

$$\cap_{\alpha\in I}M_\alpha\subset M_\alpha,\quad \text{对任一}\ \alpha\in I,$$

$$\cup_{\alpha\in I}M_\alpha\supset M_\alpha,\quad \text{对任一}\ \alpha\in I.$$

下面再介绍映射的概念.

设 M 和 M' 是两个集合. 所谓从集合 M 到集合 M' 的一个**映射**，是指一个对应规则，它使 M 中每一个元素 a 都有 M' 中一个确定的元素 a' 与它对应. 有时我们也把从集合 M 到 M' 的一个映射叫做定义在 M 上而在 M' 中取值的一个**函数**.

我们用记号

$$\sigma: M\longrightarrow M'$$

表示 σ 是从集合 M 到 M' 的一个**映射**. 如果在映射 σ 下，元素 $a'\in M'$ 与元素 $a\in M$ 对应，就记作

$$\sigma: a\longmapsto a'$$

或

$$\sigma(a)=a'.$$

我们把 a' 叫做 a 在映射 σ 之下的**像**，而 a 叫做 a' 在映射 σ 之下的一个**原像**. a' 在 σ 之下的全体原像的集合记作 $\sigma^{-1}(a')$，即

$$\sigma^{-1}(a')=\{a\in M:\sigma(a)=a'\},$$

并称之为 a' 在映射 σ 之下的**完全原像**. 更一般地，设 N' 是 M' 的一个子集合，我们用 $\sigma^{-1}(N')$ 来表示由 M 中的那些在 σ 之下的像为 N' 的元素的全体元素所组成的集合，即

$$\sigma^{-1}(N')=\{a\in M:\sigma(a)\in N'\},$$

并称之为 N' 在映射 σ 之下的**完全原像**.

设 σ 是从集合 M 到 M' 的一个映射. 我们用 $\sigma(M)$ 表示在映射 σ 之下，M 中所有元素的像组成的集合，即

$$\sigma(M)=\{\sigma(a):a\epsilon M\}.$$

显然

$$\sigma(M)\subset M'.$$

如果 $\sigma(M)=M'$, 映射 σ 就叫做是一个*满射*. 如果在映射 σ 之下, M 中不同元素的像也一定不同, 即由 $a_1,a_2\in M$ 而 $a_1\neq a_2$ 一定有 $\sigma(a_1)\neq\sigma(a_2)$, 我们就说 σ 是一个*单射*. 既是单射又是满射的映射叫做*双射*.

设 M 是一个集合. 将 M 的每一个元素都映到它自身的映射

$$a\longmapsto a,\quad a\in M$$

叫做集合 M 的*恒等映射*, 记作 1_M, 在不致引起混淆的情况下, 也可以简单地记作 1. 显然, 恒等映射是一个双射.

我们举几个例子来说明上面的概念.

例0.1 $M=\{1,2,3,4\}, M'=\{1',2',3'\}$. 定义 $\sigma(1)=\sigma(2)=1'$, $\sigma(3)=\sigma(4)=3'$. 映射 σ 不是满射, 因为 $2'$ 没有原像. σ 也不是单射, 因为 1 和 2 的像相同, 3 和 4 的像相同. 此外, $\sigma^{-1}(1')=\{1,2\}$, $\sigma^{-1}(\{1',2'\})=\{1,2\}$, 并且 $\sigma^{-1}(\{1',3'\})=\sigma^{-1}(M')=M$. □

例0.2 M 是全体整数的集合 $\mathbb{Z}$, 而 M' 是全体非负整数的集合. 定义从 M 到 M' 的一个映射 σ:

$$\sigma(a)=|a|,\quad a\in M.$$

那么 σ 是满射, 但不是单射. □

例0.3 设 M 是全体正整数的集合 $\mathbb{N}$, 而

$$M'=\{x,x^2,x^3,\cdots\},$$

即 M' 是未定元 x 的全体正幂次的集合. 定义从 M 到 M' 的一个映射 σ:

$$\sigma(n)=x^n,\quad n\in M.$$

那么 σ 既是满射又是单射, 因而是一个双射. □

现在, 设 σ 是从集合 M 到集合 M' 的一个映射, 而 σ' 是从 M' 到集合 M'' 的一个映射. 我们定义 σ 和 σ' 的*合成映射*, 记作 $\sigma'\circ\sigma$, 它是从 M 到 M'' 的一个映射, 其对应规则是

$$\begin{aligned}\sigma'\circ\sigma: M &\longrightarrow M''\\ a &\longmapsto \sigma'(\sigma(a)).\end{aligned}$$

例0.4 设 $M=M'=M''=\mathbb{Z}$, σ 是映射

$$\begin{aligned}\sigma:\ \mathbb{Z} &\longrightarrow \mathbb{Z}\\ a &\longmapsto a^3,\end{aligned}$$

σ' 是映射

$$\begin{aligned}\sigma':\ \mathbb{Z} &\longrightarrow \mathbb{Z}\\ a &\longmapsto a^2.\end{aligned}$$

那么

$$\begin{aligned}\sigma' \circ \sigma : \quad \mathbb{Z} &\longrightarrow \mathbb{Z} \\ a &\longmapsto a^6.\end{aligned}$$

□

另外，如果 σ'' 是从 M'' 集合 M''' 的一个映射，那么

$$\sigma'' \circ (\sigma' \circ \sigma) = (\sigma'' \circ \sigma') \circ \sigma.$$

事实上，对任 $a \in M$, 我们有

$$(\sigma'' \circ (\sigma' \circ \sigma))(a) = \sigma''((\sigma' \circ \sigma)(a)) = \sigma''(\sigma'(\sigma(a))),$$

$$((\sigma'' \circ \sigma') \circ \sigma)(a) = (\sigma'' \circ \sigma')(\sigma(a)) = \sigma''(\sigma'(\sigma(a))).$$

设 S 是一非空集合. 用 $S \times S$ 来表示 S 中元素的有序对 $(a,b), a,b \in S$, 组成的集合，即

$$S \times S = \{(a,b) : a,b \in S\},$$

并把 $S \times S$ 叫做 S 与它自身的 笛卡儿积. 再设 $R = \{0,1\}$. 从 $S \times S$ 到 R 的一个映射

$$\begin{aligned}\sim : \quad S \times S &\longrightarrow R \\ (a,b) &\longmapsto \ \sim (a,b)\end{aligned}$$

也叫做 S 上的一个 关系. 当 $\sim (a,b) = 1$ 时，就说 a 和 b 有关系 $\sim$, 并记作 $a \sim b$; 当 $\sim (a,b) = 0$ 时，就说 a 和 b 没有关系 $\sim$, 并记作 $a \not\sim b$. 例如，设 $S = \mathbb{R}$, 在 $\mathbb{R}$ 上如下定义一个关系 $<$:

$$< (a,b) = 1 \quad \text{当且仅当} \quad a < b,$$

$$< (a,b) = 0 \quad \text{当且仅当} \quad a \geqslant b.$$

设 $\sim$ 是 S 上的一个关系. $\sim$ 叫做 S 上的一个 等价关系, 如果它适合下面三个条件：

1. $a \sim a$ 对所有 $a \in S$. (自反性)
2. 从 $a \sim b$ 推出 $b \sim a$. (对称性)
3. 从 $a \sim b$ 和 $b \sim c$ 推出 $a \sim c$. (传递性)

例0.5 设 $S = \mathbb{Z}$. 对于任意两个整数 a 和 b, 定义

$$a \sim b \text{ 当且仅当 } a,b \text{ 有相同的奇偶性.}$$

显然这样定义的 $a \sim b$ 是 $\mathbb{Z}$ 上的一个等价关系. □

设 $\sim$ 是非空集 S 上的一个等价关系. S 的非空子集 T 叫做一个 等价类, 如果对 T 中任意两个元素 a,b 都有 $a \sim b$, 而且对任意 $c \in S$, 如果 $c \sim a$ 对某个 $a \in T$ 就有 $c \in T$.

设 S 是一个非空集，而 I 是一个足码集. S 的一组非空子集 $S_\alpha(\alpha \in I)$ 叫 S 的一个 分拆，如果 $\cup_{\alpha\in I}S_\alpha = S$ 而且当 $\alpha \neq \beta$ 时 $S_\alpha \cap S_\beta = \emptyset$.

现在我们要证明非空集上的任一等价关系都给出这个集合分成等价类的一个分拆，而且非空集的任一分拆都可定义这个集合上的一个等价关系，如果当 a, b 属于这分拆的同一个子集时就定义 $a \sim b$.

定理0.1 设 $\sim$ 是非空集 S 上的一个等价关系. 对任意 $a \in S$ 定义 $S_a = \{x \in S : a \sim x\}$. 那么 S_a 是一个等价类而且对任意两个元素 $a, b \in S$ 或者 $S_a \cap S_b = \emptyset$ 或者 $S_a = S_b$. 进一步 S 有一个子集 I 使得 $S_a \cap S_b = \emptyset$ 对 I 中任意两个不同的元素 a, b 而且 $\cup_{a\in I}S_a = S$, 即 $\{S_a : a \in I\}$ 是 S 分成等价类的一个分拆而且对任意两个元素 $a, b \in S$, $a \sim b$ 当且仅当 $a, b \in S_c$ 对某个 $c \in I$.

证明 首先对任意 $a \in S$ 都有 $a \sim a$, 因此 $a \in S_a, S_a$ 非空. 其次我们证明对 S_a 中任意两个不同的元素 b, c 都有 $b \sim c$. 根据 S_a 的定义，有 $a \sim b$ 和 $a \sim c$. 根据 $\sim$ 的对称性，从 $a \sim b$ 推出 $b \sim a$. 根据传递性，从 $b \sim a$ 和 $a \sim c$ 推出 $b \sim c$. 我们再证明对任意 $d \in S$, 从 $d \sim b$ 对某个 $b \in S_a$ 推出实 $d \in S_a$. 实际上，从 $d \sim b$ 推出 $b \sim d$ 而 $b \in S_a$ 的意思是 $a \sim b$. 根据传递性，从 $a \sim b$ 和 $b \sim d$ 推出 $a \sim d$. 因此 $d \in S_a$. 这证明了 S_a 是一个等价类.

假定 $S_a \cap S_b \neq \emptyset$. 我们先证明 $a \sim b$. 设 $c \in S_a \cap S_b$. 那么 $a \sim c$ 和 $b \sim c$. 但是从 $b \sim c$ 推出 $c \sim b$, 而从 $a \sim c$ 和 $c \sim b$ 推出 $a \sim b$. 对任意 $x \in S_b$ 有 $b \sim x$, 那么从 $a \sim b$ 和 $b \sim x$ 推出 $a \sim x$, 于是 $x \in S_a$. 类似地，从 $x \in S_a$ 推出 $x \in S_b$. 这证明了 $S_a = S_b$.

任选 $a \in S$, 都有一个等价类 S_a. 如果 $S_a = S$, 就令 $I = \{a\}$. 如果 $S_a \neq S$, 就有 $b \in S \setminus S_a$ 而 $S_a \cap S_b = \emptyset$. 令 I 是 S 的一个子集使得 $S_a \cap S_b = \emptyset$ 对 I 中任意两个不同的元素 a, b, 而且是具有此性质的最大的一个子集. 显然 $\cup_{a\in I}S_a = S$. 于是 $\{S_a : a \in I\}$ 是 S 分成等价类的一个分拆. 进一步，不难证明，对任意两个不同的元素 $a, b \in S$, $a \sim b$ 当且仅当 $a, b \in S_c$ 对某个 $c \in I$. □

反过来，我们有

定理0.2 设 S 是一个非空集，而 $\{S_\alpha : \alpha \in I\}$ 是 S 的一个分拆，这里 I 是一个足码集. 对任意 $a, b \in S$ 定义 $a \sim b$ 当且仅当 a 和 b 属于同一个 S_γ 对某个 $\gamma \in I$. 那么 $\sim$ 是 S 上的一个等价关系而对任意 $\alpha \in I$, 从 $a \in S_\alpha$ 推出 $S_\alpha = S_a = \{x \in S : a \sim x\}$.

证明留作习题.

0.2 整数的分解

用 $\mathbb{Z}$ 表示全体整数 (正整数、负整数和 0) 的集合. 我们知道在 $\mathbb{Z}$ 中可以进行加法和乘法运算，并且 $\mathbb{Z}$ 对于这两种运算是封闭的.

我们先来复习一下 $\mathbb{Z}$ 中的带余除法.

定理0.3 设 a 和 b 是两个整数，而 $b \neq 0$. 那么存在唯一的一对整数 q 和 r，使得

$$a = qb + r, \quad 0 \leqslant r < |b|, \tag{0.1}$$

式中 $|b|$ 表示 b 的绝对值.

证明 先证明存在性. 如果 $a = 0$, 就取 $q = r = 0$. 对于 $a > 0$, 我们对 a 作数学归纳法来证明. 如果 $a < |b|$, 就取 $q = 0$, $r = a$; 如果 $a \geqslant |b|$, 令 $a_1 = a - |b|$. 那么 $0 \leqslant a_1 < a$. 根据归纳法假设，有整数 q_1 和 r_1 存在，使得

$$a_1 = q_1 b + r_1, \quad 0 \leqslant r_1 < |b|.$$

把 a_1 代入前一个等式后再进行变换，我们得到

$$a = q_1 b + |b| + r_1, \quad 0 \leqslant r_1 < |b|.$$

如果 $b > 0$, 就令 $q = q_1 + 1$; 如果 $b < 0$, 就令 $q = q_1 - 1$. 在这两种情形我们取 $r = r_1$, 那么 (0.1) 成立.

剩下要考虑 $a < 0$ 的情形. 这时 $-a > 0$. 由上面的讨论，存在 q_1 和 r_1

$$-a = q_1 b + r_1, \quad 0 \leqslant r_1 < |b|.$$

那么 $a = -q_1 b - r_1$. 当 $r_1 = 0$ 时，取 $q = -q_1$, $r = 0$, 那么 (0.1) 成立. 下设 $r_1 \neq 0$. 如果 $b > 0$, 就令 $q = -(q_1 + 1)$ 和 $r = b - r_1$; 如果 $b < 0$, 就令 $q = -(q_1 - 1)$ 和 $r = -b - r_1$. 在这两种情形，都有 (0.1) 成立.

再证明唯一性. 假定存在 q, r 使得 (0.1) 成立，并且存在 q', r' 使得

$$a = q'b + r', \quad 0 \leqslant r' < |b|. \tag{0.2}$$

不妨设 $r' \geqslant r$, 由 (0.1) 减去 (0.2), 我们得

$$(q - q')b + r - r' = 0,$$

或等价地，

$$(q - q')b = r' - r \geqslant 0.$$

但 $r' - r \leqslant r' < |b|$. 于是 $|q - q'| \cdot |b| = r' - r < |b|$. 这就推出 $q = q'$, 因而 $r = r'$. □

(0.1) 式叫做用 b 去除 a 的**带余除法算式**. 由于 q 和 r 由 a 和 b 唯一确定，因此可以记

$$r = (a)_b.$$

当 $r = 0$ 时，我们就说 b 是 a 的**因数**，或 a 是 b 的**倍数**，也说 a 被 b **所整除**，或 b**整除** a，并用符号

$$b|a$$

来表示. 我们还用符号 $b \nmid a$ 表示 b 不整除 a. 显然，如果 b 是 a 的因数，而 $a \neq 0$，那么有

$$|b| \leqslant |a|.$$

设 a, b, c 都是整数，而 $c \neq 0$. 如果 c 既是 a 的因数，又是 b 的因数，我们就说 c 是 a 和 b 的公因数. 当 a 和 b 不全等于 0 时，a 和 b 的公因数中就有一个最大的；我们把 a 和 b 的公因数中最大的那一个叫做 a 和 b 的**最大公因数**，并用符号

$$\gcd(a, b)$$

来表示. 显然，$\gcd(a, b) > 0$. 当 a 和 b 都等于 0 时，那么任何一个整数都是它们的公因数，这时 a 和 b 没有最大公因数，因此符号 $\gcd(0, 0)$ 没有意义.

设 a 和 b 都是不等于 0 的整数. 我们来复习一下求 $\gcd(a, b)$ 的**辗转相除法**. 假定 $|a| > |b|$. 根据带余除法算式，依次有

$$a = q_1 b + r_1, \quad 0 < r_1 < |b|, \tag{0.3}$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1, \tag{0.4}$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2, \tag{0.5}$$

$$\cdots\cdots\cdots\cdots$$

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2}, \tag{0.6}$$

$$r_{n-2} = q_n r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1}, \tag{0.7}$$

$$r_{n-1} = q_{n+1} r_n, \tag{0.8}$$

那么

$$\gcd(a, b) = r_n.$$

事实上，由 (0.8) 式知 $r_n | r_{n-1}$，再由 (0.7) 式知 $r_n | r_{n-2}$，再由 (0.6) 式知 $r_n | r_{n-3}, \cdots$，如此继续下去，最后由 $r_n | r_1$ 和 $r_n | b$ 及 (0.3) 式知 $r_n | a$. 因此 r_n 是 a 和 b 的一个公因数. 反过来，假设 d 是 a 和 b 的一个公因数，即 $d | a$, $d | b$. 那么由 (0.3) 式知 $d | r_1$. 再由 (0.4) 式知 $d | r_2$，再由 (0.5) 式知 $d | r_3, \cdots\cdots$，如此继续下去，最后由 $d | r_{n-2}$ 和 $d | r_{n-1}$ 及 (0.7) 式知 $d | r_n$. 因此 $r_n = \gcd(a, b)$.

进一步，可将 (0.3) 至 (0.7) 式改写成

$$r_1 = a + (-q_1) b, \tag{0.9}$$

$$r_2 = b + (-q_2) r_1, \tag{0.10}$$

$$r_3 = r_1 + (-q_3) r_2, \tag{0.11}$$

$$\cdots\cdots\cdots\cdots$$

$$r_{n-1} = r_{n-3} + (-q_{n-1}) r_{n-2}, \tag{0.12}$$

$$r_n = r_{n-2} + (-q_n) r_{n-1}. \tag{0.13}$$

(0.13) 式是说 r_n 是 r_{n-2} 和 r_{n-1} 的整数系数的线性组合. 将 (0.12) 式代入 (0.13) 式，得

$$r_n = (-q_n)r_{n-3} + (1 + q_n q_{n-1})r_{n-2}.$$

这就是说， r_n 是 r_{n-3} 和 r_{n-2} 的整数系数的线性组合. 如此继续下去，就可以将 a 和 b 的最大公因数 r_n 表示成 a 和 b 的整数系数的线性组合，即

$$r_n = ca + db,$$

其中 c 和 d 都是整数. 从上面这个式子立刻推出 a 和 b 的任一公因数都是 r_n 的因数. 我们证明了

定理0.4 设 a 和 b 都是不等于 0 的整数. 那么 a 和 b 的最大公因数 $\gcd(a, b)$ 可以表示成 a 和 b 的整数系数的线性组合，而且 a 和 b 的任一公因数都是 $\gcd(a, b)$ 的因数. □

对于不全等于 0 的两个整数，定理 0.4 显然也成立. 譬如，设 $a = 0, b \neq 0$，那么 $\gcd(a, b) = |b| = 0 \cdot a + (|b|/b)b$ 而 $|b|/b = \pm 1$.

例0.6 设 $|a| = 49, |b| = 36$. 由带余除法，依次得到下面的一系列算式

$$\begin{aligned} 49 &= 1 \cdot 36 + 13, \quad 13 < 36, \\ 36 &= 2 \cdot 13 + 10, \quad 10 < 13, \\ 13 &= 1 \cdot 10 + 3, \quad 3 < 10, \\ 10 &= 3 \cdot 3 + 1, \quad 1 < 3, \\ 3 &= 3 \cdot 1. \end{aligned}$$

这表明

$$\gcd(49, 36) = 1.$$

将前四个式子改写成

$$\begin{aligned} 13 &= 49 - 1 \cdot 36, \\ 10 &= 36 - 2 \cdot 13, \\ 3 &= 13 - 1 \cdot 10, \\ 1 &= 10 - 3 \cdot 3. \end{aligned}$$

将第三式右方代入第四式中的后一个 3，再将所得算式中的 10 用第二式右方代入，最后将所得算式中的 13 用第一式右方代入，得

$$\begin{aligned} 1 &= 10 - 3 \cdot (13 - 1 \cdot 10) \\ &= (-3) \cdot 13 + 4 \cdot 10 \\ &= (-3) \cdot 13 + 4 \cdot (36 - 2 \cdot 13) \\ &= 4 \cdot 36 + (-11) \cdot 13 \\ &= 4 \cdot 36 + (-11) \cdot (49 - 1 \cdot 36) \\ &= (-11) \cdot 49 + 15 \cdot 36, \end{aligned}$$

即

$$1 = (-11) \cdot 49 + 15 \cdot 36.$$ □