普通高等教育“十二五”规划教材
大学本科数学类专业基础课程系列丛书

高等代数教程

郭聿琦　岑嘉评　王正攀　编著

科学出版社

普通高等教育“十二五”规划教材

大学本科教学类专业基础课程系列丛书

高等代数教程

郭聿琦　岑嘉评　王正攀　编著

科学出版社

北京

内 容 简 介

本书除了第 0 章“整数, 数域与多项式”外, 将“线性代数” 内容分为上下两篇, 上篇以较为具体的“线性方程组的一般理论问题”的提出、分析、抽象、解决和引申为线索组织“线性空间理论”, 并在问题的讨论中充分使用它; 下篇以“实二次型的主轴问题”的提出、分析、抽象、解决和引申为线索组织“线性变换理论”, 并在问题的讨论中充分使用它, 这是宏观框架, 详见目录. 其微观处理, 则以“线性相关性” 这一“线性代数” 的核心概念贯穿始终, 且使用了许多独特的处理方法和技巧. 每章后的习题之外, 贯穿于各章节中的诸多“注” 提供了若干思考问题. 另外, 本书在“现代化处理上” 实现了内容上的诸多“更新”(语言上的, 开发路线上的, 证明方法上的, …), 也给出了内容上的适当的“增新” (诸如引进了出现于 28 年前的“关于多项式的 Fermat 大定理的初等证明”).

本教材为数学类各专业(特别地, 各类数学人才班) “高等代数” 课程所撰写, 供数学类各专业师生和有关数学工作者使用.

图书在版编目(CIP)数据

高等代数教程/郭晋云, 周建华, 韩青编著. —北京: 科学出版社, 2014.7

ISBN 978-7-03-040417-6

Ⅰ. ①高… Ⅱ. ①郭… ②周… ③韩… Ⅲ. ①高等代数-教材

Ⅳ. ① O15

中国版本图书馆 CIP 数据核字(2014)第 074002 号

责任编辑: 胡海霞 / 责任校对: 刘亚琦

责任印制: 阎 磊 / 封面设计: 迷底书装

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

北京市文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2014 年 7 月第 一 版 开本: 787 × 1092 1/16

2014 年 7 月第一次印刷 印张: 20 1/4

字数: 440 000

定价: 49.00 元

(如有印装质量问题, 我社负责调换)

序　言

“高等代数” 是数学类各专业乃至许多其他相关专业的一门主干基础课程. 最近高兴地看到郭聿琦、岑嘉评、王正攀三位教师为这门课程撰写的这本新教材，我非常乐于为它再作一序，这不仅是因为郭聿琦教授是我的学生，香港中文大学讲座教授岑嘉评博士是我们 20 余年来的学术研究合作者，更是因为这是他们的又一用功之作.

这一新教材，处处体现着作者对教材处理上的几个关键问题的理解和实践，诸如，现代化的问题、少而精的问题、经得住读者推敲的问题.

这里特别要提到的是，这一教材实现了在基础课程教材中当代新学术成果的展示 (关于多项式的 Fermat 大定理的一个初等证明，出现不到 30 年), 实现了在基础课程教材中公理化方法与非公理化方法的对比使用 (在行列式的定义中), 提炼出新概念，用以设置了矩阵秩概念的新开发, 给出了著名定理的简化证明 (关于 Cayley-Hamilton 定理).

这一新教材，在内容的宏观组织上, 除了从目录上一目了然的那一条明线, 更加突出了 “线性相关性” 在线性代数部分的暗中贯穿，诸如涉及内积的、涉及线性变换的、涉及矩阵秩的、涉及空间直和分解的以及涉及各种标准形的 “线性相关性”.

这一新教材，在理论开发上, 秉持 “几何观点” 与 “矩阵方法”, 扩充了矩阵分块运算和初等变换的使用范围；在不增加难度但增加深度的原则下, 在更一般原理的探讨中，揭示出事实的本质, 遵循了由浅入深、由易到难、由具体到抽象, 以及难点分散的认知规律；在注重理论背景和理论应用的过程中, 显示着抽象的必要和威力.

这一新教材，从宏观框架到微观处理, 处处凝聚着作者讲授 “高等代数” 多年来的心得体会, 使用了许多独特的处理方法和技巧, 不乏新颖之处.

总之, 这一教材, 内容紧凑, 系统性和节奏感都很强, 能很好地实现知识传授中的能力培养和素质提高, 因此，它是一本新的有特色的好教材.

许永华

2014 年 2 月于复旦大学

前　言

本教材是在我们的前一本 “高等代数” 教材《线性代数导引》(“教育部面向 21 世纪课程教材” 之一) 使用若干年的基础上形成的, 后者的第一版 (中文版) 于 2001 年在科学出版社出版, 2004 年再次印刷; 它的第二版《Linear Algebra》(英文版) 于 2007 年在科学出版社出版. 这一新教材的整部书稿曾在兰州大学数学与统计学院的 2012 级和 2013 级各班级, 特别是数学萃英班和数学基地班两个人才班, 试用了两届.

本教材沿用了原来的宏观框架 (囿于某些考虑, 作为附录的 “整数, 数域与多项式” 已改为第 0 章, 位居两篇之前). 相对于大家较熟悉的前一本书, 增加了 “行列式的 (某一种) 公理化定义” 一节, 在与行列式的其他定义的对照使用中, 显示了各种方法的优越性, 同时, 与行列式的归纳法定义等处理方法一起, 扩大了矩阵的初等变换方法的应用范围; 采用了关于 Cayley-Hamilton 定理的一个简化证明 (出现于 2013 年)(Gruenberg et al., 1977), 与矩阵的乘法结合律、Cramer 法则等其他内容的处理一起扩大了矩阵分块方法的应用范围; 对于多项式, 增加了 “关于多项式的 Fermat 大定理的一个初等证明” (出现于 1985 年, 我们将它收入本书时, 又对其作了进一步的简化) 一节, 实现了基础课教程内容上难得的 “增新” (对于教材编著中的现代化处理, 更多的是经典内容的 “更新”, 诸如, 语言上的更新、开发路线的更新、证明方法的更新等), 这一增新让低年级大学生感受到, 他们离数学前沿也并非想象得那么遥远, 同时, 借以实现了关于多项式基本内容的一个完美的总结; 关于矩阵秩概念的建立, 相对于 “n 维向量组涉及其向量的初等变换其秩不变”, 也平行地建立了 “n 维向量组涉及其分量的初等变换其秩不变” 的事实, 这不但简化了其后关于矩阵的三种秩相等的证明, 而且读者会觉得很直观, 很容易理解; 另外, 涉及开发路线的微观处理, 几乎在每一章节, 我们都在进一步完善着我们的一个初衷的实现 (例如, 线性变换理论从涉及线性变换的线性相关性的一个基本事实出发 — 它等价于 Sylvester 定理, 直到关于矩阵的一类相似标准型的几何形象的阐述), 这一初衷是, 将 “线性代数” 的基本内容 (“高等代数” 课程的主要内容), 处处围绕 “线性相关性” 这一核心概念展开.

本教材的撰写得到了兰州大学教务处、兰州大学萃英学院 (国家“基础学科拔尖学生培养试验计划”) 与兰州大学数学与统计学院的支持和鼓励, 得到了兰州大学教务处和兰州大学萃英学院 (国家“基础学科拔尖学生培养试验计划”) 对本教材撰写和出版的资助, 我们在此一并致谢; 也向承担过助教工作的博士研究生梁星亮、裴俊、乔丽、冯辛阳、唐剑、张佳等同学致谢, 感谢她 (他) 们提出了若干修订建议, 特别是各章后习题的设置, 并承担了全书的打字和校对工作; 更向西北师范大学数学与统计学院副教授杨晓燕博士致谢, 她仔细审阅了整本书稿, 提出了中肯的修订建议.

教材建设中的教材处理, 从原则到实践, 充满着见仁见智的问题. 大家从我们的这本教材中便能窥视出我们的诸多观点之一斑, 例如, 我们认为, 教材的语言固然严忌艰涩, 也切忌所谓 “通俗易懂, 便于自学” (这绝不利于学生学会读书). 当然, 我们的观点和做法难免有不妥之处, 欢迎批评指正.

郭聿琦 (兰州大学, 西南大学)
岑嘉评 (香港中文大学)
王正攀 (西南大学)
2013 年 9 月 10 日

目　录

下篇　实二次型的主轴问题

第 0 章　整数, 数域与多项式

线性代数 (或称一次代数) 的讨论必然要使用多项式的一些基本概念, 这是本书要介绍一点多项式的基本概念的直接缘由. 另外, 多项式作为代数学中最基本的对象之一, 在代数学的各个分支以及其他数学学科中, 或者构成其基本内容, 或者多多少少要被涉及, 所以本书作为一本基础教程对它作一点起码的介绍, 也有更广泛的意义.

这里要介绍的多项式的一些最基本的事项与整数的许多基本事项是平行的, 两相对照十分有趣, 这又是要先讲一点整数的原因.

数量领域内的代数学, 问题的讨论常常需要事先明确解决问题的数量范围. 数量的加、减、乘、除等合成的性质通常称为数量的代数性质, 而数量的代数学所研究的问题基本上涉及的就是数量的代数性质, 它们是有理数全体、实数全体和复数全体所共有的, 为此, 我们要引入数域这一基本概念, 作为我们讨论数量领域内代数学的一个基础.

本章乃至全书的讨论要使用一些集合论的语言, 因此, 我们的 0.1 节先用于回顾集合及其相关概念, 并尽量将它们精确化.

0.1　集合, 映射与运算

集合是数学中少数不加定义的概念 (称为元概念) 之一, 它被界定为具备某种性质的对象的全体. 关于整数, 依我们的经验, 它们是

$$0, \pm 1, \pm 2, \cdots, \pm n, \cdots.$$

而整数的全体 $\mathbb{Z}$ 就是一个集合, 称 $\mathbb{Z}$ 为**整数集**. 构成一个集合 A 的每一个对象称为这一集合的一个**元素**, 这一关系, 记为 $x \in A$, 称为 "$\boldsymbol{x}$ **属于** $\boldsymbol{A}$"; 否则记为 $x \notin A$, 称为 "$\boldsymbol{x}$ **不属于** $\boldsymbol{A}$". 例如, $-2 \in \mathbb{Z}$, $\dfrac{1}{2} \notin \mathbb{Z}$.

不含任何元素的集合称为**空集**, 记为 $\varnothing$. 所谓一个集合是已知的, 指的是构成 A 的全体对象是已知的. 因此, 刻画一个集合, 就是阐述这个集合是由哪些元素构成的. 要阐述这一点, 一个直截了当的方法就是将这个集合的全部对象罗列出来, 这对于由有限个元素组成的集合 (称为**有限集**, 否则称为**无限集**, 通常用 $|A|$ 表示集合 A 含元素的个数), 都是行得通的, 例如, 由 $1, 2, 3$ 组成的集合 A, 我们就可以用这一罗列法将 A 表示为

$$A = \{1, 2, 3\}; \tag{0.1}$$

这一方法对于某些无限集也可以使用, 例如, 整数集 $\mathbb{Z}$ 可表示为

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots, \pm n, \cdots\}.$$

但是, 更一般的阐述方法是使用定义这一集合的性质. 于是, 如果集合 A 是由具有性质 P 的所有对象构成的, 那么我们就可以表示 A 为

$$A = \{x \mid x \text{ 具有性质 } P\}.$$

例如, 平面上落在双曲线 $x^2 - y^2 = 1$ 上的点 (x, y) 的全体 M, 就可写为

$$M = \{(x, y) \mid x^2 - y^2 = 1\};$$

又如, $\mathbb{Z}$ 可以写为

$$\mathbb{Z} = \{x \mid x \text{ 是整数}\}.$$

前面的罗列法也可归为后面的这一阐述方法, 例如, 式 (0.1) 中的 A 可以写为

$$A = \{x \mid x = 1, 2, 3\},$$

此时, 所使用的性质 P 是

$$P = \text{“}x \text{ 是 1, 或者 2, 或者 3”}.$$

任给两个集合 A, B, 我们可以使用下述各种合成的方法构造一些新的集合:

$$\begin{aligned} C_1 &= \{x \mid x \in A, \text{ 或 } x \in B\}, \\ C_2 &= \{x \mid x \in A, \text{ 且 } x \in B\}, \\ C_3 &= \{x \mid x \in A, \text{ 且 } x \notin B\}, \\ C_4 &= \{(x, y) \mid x \in A, y \in B\}, \end{aligned}$$

分别记它们为

$$\begin{aligned} C_1 &= A \cup B, \\ C_2 &= A \cap B, \\ C_3 &= A - B, \\ C_4 &= A \times B, \end{aligned}$$

且分别称 C_1, C_2, C_3 和 C_4 为集合 A 与 B 的**并**, **交**, **差**和 **Descartes 积**.

除了集合之间的上述基本合成 (它们原则上都可以由两个集合推广到多个集合) 外, 集合间还有一种基本关系, 称为包含 (或包含关系).

令 A, B 为两个集合. 称 A **包含在集合** B 中 (或称 B **包含** A, 也称 A 为 B 的**子集**), 记为 $A \subseteq B$, 即如果 $x \in A$ 意味着 $x \in B$. 例如, 对于式 (0.1) 中的 A, 有 $A \subseteq \mathbb{Z}$; 称 A 与 B **相等**, 记为 $A = B$, 如果 $A \subseteq B$, 且 $B \subseteq A$, 即 A 与 B 是同一个集合; 称 A **真包含在** B 中 (或称 B **真包含** A, 也称 A 是 B 的**真子集**), 即如果 $A \subseteq B$, 但 $A \neq B$. 任何集合 A 以自身 A 和空集 $\varnothing$ 为自己的子集, 这两个子集称为**平凡子集**. 若 $A = \{1, 2, 3\}$, 则 A 的所有子集为

$$\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A,$$

其中前 7 个子集是真子集, 中间 6 个子集是非平凡子集.

读者可以取 A 为式 (0.1) 中的 A 和 B 为 $\mathbb{Z}$ 来考查一下 A 与 B 的包含关系以及 A 与 B 的并, 交, 差和 Descartes 积.

现在, 我们可以再介绍集合的另外两种合成了.

令 S 为一集合, S_1 为它的子集, 即 $S_1 \subseteq S$. 分别称

$$C_5 \overset{\mathrm{d}}{=} \{x \mid x \in S | \ x \notin S_1\} \ (\overset{\mathrm{d}}{=} \text{表示用右边定义左边})$$

和

$$C_6 \overset{\mathrm{d}}{=} \{A \mid A \subseteq S\}$$

为 S_1 在 S 中的**补集**和 S 的**幂集**, 分别记 C_5 为 $\overline{S_1}$, C_6 为 $\mathcal{P}(S)$ (后者也记为 2^S); 与两集合的差相联系, $\overline{S_1} = S - S_1$.

下面我们要回顾的是作为函数推广的所谓集合间的映射的概念.

定义 0.1.1 令 A, B 为两个集合. A 到 B 的一个映射 f 是一个法则, 使得 A 中的每一个元素 a 按照这一法则都唯一确定 B 中的一个元素 b 与 a 对应, 此时, 记 $b = f(a)$, 称 b 为 a 在 f 下的**象**, a 为 b 在 f 下的一个**原象**.

我们表示 A 到 B 的一个映射 f 通常用下面的方式:

$$\begin{aligned} f : A &\longrightarrow B \\ a &\longmapsto b = f(a). \end{aligned}$$

称 $A(B)$ 为 f 的**定义域** (**值域**), 记 $A = D(f), B = R(f)$. 又令

$$\begin{aligned} \mathrm{Im}f &= \{b \in B \mid (\exists a \in A)\ f(a) = b\}, \\ f^{-1}(b) &= \{a \in A \mid f(a) = b\}, \quad b \in B. \end{aligned}$$

分别称它们为 f 的**象**和 $b \in B$ 在 f 下的**完全原象**.

例如, 若记

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\},$$

则让 $4 \mid n \mid$ 对应于 $n \in \mathbb{Z}$ 时, 我们有一映射

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow 2\mathbb{Z} \\ n &\longmapsto 4 \mid n \mid = f(n), \end{aligned} \tag{0.2}$$

其中 $|n|$ 表示 $n \in \mathbb{Z}$ 的绝对值. 此时,

$$\mathrm{Im}f = \{4 \mid n \mid \mid \ n \in \mathbb{Z}\} = \{0, 4, 8, 12, \cdots\}.$$

对于任意 $m \in 2\mathbb{Z}$,

$$f^{-1}(m) = \begin{cases} \{0\}, & \text{当 } m = 0 \text{ 时}, \\ \left\{\dfrac{m}{4}, -\dfrac{m}{4}\right\}, & \text{当 } m > 0, \text{ 且 } m \text{ 为 } 4 \text{ 的倍数时}, \\ \varnothing, & \text{其他情况}. \end{cases}$$

映射 $f: A \longrightarrow B$ 和 $g: A \longrightarrow B$ 称为**相等**的, 如果

$$(\forall a \in A) \quad f(a) = g(a).$$

称映射 $f: A \longrightarrow B$ 是一个**单射**, 或 **1 − 1 映射** (**满射**, 或**到上的映射**), 如果

$$(\forall b \in B) \quad |\, f^{-1}(b) \,| \leqslant 1 \quad (\mathrm{Im} f = B),$$

或者说,

$$(\forall a_1, a_2 \in A) \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2) \quad ((\forall b \in B) |\, f^{-1}(b) \,| \geqslant 1),$$

即 A 中不同的元素在 f 下的象也不同 (B 中的每一个元素都是 A 中的某一个元素在 f 下的象), 其中 $|\, D \,|$ 表示集合 D 中含元素的个数.

称映射 $f: A \longrightarrow B$ 是一个**双射**, 或**一一对应**, 如果 f 既是一个单射, 又是一个满射. 式 (0.2) 中的映射显然既不是单射, 也不是满射. 下面的映射

$$\begin{aligned} f_1 &: \mathbb{Z} \longrightarrow \mathbb{Z} \\ & \quad n \longmapsto 2n, \\ f_2 &: \mathbb{Z} \longrightarrow \{1, 2\} \\ & \quad n \longmapsto \begin{cases} 1, & \text{当 } 2 \nmid n \text{ 时}, \\ 2, & \text{当 } 2 \mid n \text{ 时}, \end{cases} \\ f_3 &: \mathbb{Z} \longrightarrow 2\mathbb{Z} \\ & \quad n \longmapsto 2n, \end{aligned}$$

显然, f_1, f_2, f_3 分别是一个单射但非满射、满射但非单射、双射的例子.

我们可以借助已知的映射

$$f: A \longrightarrow B, \quad g: B \longrightarrow C,$$

用下面的方法定义一个新的映射

$$\begin{aligned} h &: A \longrightarrow C \\ & \quad a \longmapsto g(f(a)), \end{aligned}$$

记 $h = g \circ f$, 称为 f 与 g 的**合成**. 显然, 这一合成是满足结合律的, 即对于任何映射

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

有

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

定理 0.1.1　映射 $f: A \longrightarrow B$ 是一个**单射** (**满射**) 当且仅当存在 $g: B \longrightarrow A$, 使得

$$g \circ f = i_A \quad (f \circ g = i_B),$$

其中 i_A 为 A 到自身的所谓**恒等映射**, 即对于任何 $a \in A$, $i_A(a) = a$.

证明 若映射 $f:A\longrightarrow B$ 是一个单射, 则对于任何 $b\in B$, $|f^{-1}(b)|\leqslant 1$. 任意取定 A 中一元素 a_0, 当 $|f^{-1}(b)|=0$ (即 $f^{-1}(b)=\varnothing$) 时, 让 a_0 与 b 对应; 当 $|f^{-1}(b)|=1$ 时, 令 $f^{-1}(b)=\{a\}$, 则让 a 与 b 对应. 这一对应就确定一映射 $g:B\longrightarrow A$. 显然, 对于任意 $a\in A$,

$$(g\circ f)(a)=g(f(a))=a,$$

即 $g\circ f=i_A$. 反之, 若存在 $g:B\longrightarrow A$, 使得

$$g\circ f=i_A,$$

则对于任意 $a,a'\in A$, 由 $f(a)=f(a')$, 有

$$\begin{aligned}a=&i_A(a)=(g\circ f)(a)=g(f(a))\\=&g(f(a'))=(g\circ f)(a')\\=&i_A(a')=a'.\end{aligned}$$

因此, f 是单射.

若 f 是一个满射, 则 $\mathrm{Im}f=B$, 即对于任一 $b\in B$, $f^{-1}(b)\neq\varnothing$. 现对于任一 $b\in B$, 在 $f^{-1}(b)$ 中取一 a, 作

$$\begin{aligned}g:B&\longrightarrow A\\b&\longmapsto a.\end{aligned}$$

于是, 对于任意 $b\in B$,

$$(f\circ g)(b)=f(g(b))=f(a)=b,$$

即 $f\circ g=i_B$. 反之, 若存在 $g:B\longrightarrow A$, 使得

$$f\circ g=i_B,$$

则对于任一 $b\in B$,

$$b=i_B(b)=(f\circ g)(b)=f(g(b))\in\mathrm{Im}f,$$

因此, $\mathrm{Im}f=B$, 即 f 是一个满射. □

由定理 0.1.1 及其证明 (当 f 既是一个单射又是一个满射的时候, 证明中所作出的两个 $g:B\longrightarrow A$ 实际上是同一个), 我们有如下推论.

推论 0.1.1 映射 $f:A\longrightarrow B$ 是一个**双射**当且仅当存在 $g:B\longrightarrow A$, 使得

$$g\circ f=i_A,\quad f\circ g=i_B.$$

定义 0.1.2 当推论 0.1.1 的充要条件成立时, 称 f 为**可逆映射**, 显然, g 由 f 唯一确定, 记 $g=f^{-1}$, 称为 f 的**逆映射**.

于是, 推论 0.1.1 又可陈述为

推论 0.1.2 映射 f 为双射当且仅当 f 为一可逆映射.

在这一节的最后, 我们给出两类特殊的映射.

一类映射是 $f: A \longrightarrow A$, 我们称此类映射 f 为集合 A 上的**变换**, 也称它们为 A 上的**一元运算**. 例如, 取 $A=\{1,2,3\}$, A 上的变换可以写成

$$f=\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix},$$

其中 $i_j=f(j)$. 而每一 i_j 都有三种选择 (1, 或 2, 或 3), 因此, $A=\{1,2,3\}$ 上的变换恰有 27 个.

另一类映射是, $f: A\times A \longrightarrow A$, 我们称此类映射 f 为 A 上的**二元运算**.

例如, 通常的加法 "+" 就是 $\mathbb{Z}$ 上的一个二元运算.

$$\begin{aligned} +:\mathbb{Z}\times\mathbb{Z} &\longrightarrow \mathbb{Z} \\ (n,m) &\longmapsto n+m. \end{aligned}$$

通常的减法 "−", 乘法 "×" 也一样. 但通常的除法 "÷" 则不是 $\mathbb{Z}$ 上的一个二元运算, 即

$$(n,m)\longmapsto n\div m, \quad n,m\in\mathbb{Z}$$

不是 $\mathbb{Z}\times\mathbb{Z}$ 到 $\mathbb{Z}$ 的一个映射.

0.2　整　　数

对于整数

$$0,\pm1,\pm2,\cdots,\pm n,\cdots$$

以及整数集 $\mathbb{Z}$ 关于加、减、乘运算和关系 "$\leqslant$" 的基本事项, 我们都使用读者至今积累起来的经验. 在这里我们对整数的讨论就从这些经验和下面的一个公理出发.

良序公理　令

$$S\subseteq\{n \mid n\in\mathbb{Z}, n\geqslant 0\}. \tag{0.3}$$

若 $S\neq\varnothing$, 则 S 中有最小元素 (即

$$\exists\, n_0\in S, \forall n\in S, \quad n_0\leqslant n).$$

注 0.1　式 (0.3) 中的 0 可以被任何整数替代.

应用非负整数的良序公理, 我们可以证明非负整数的另一个称为数学归纳法的性质. 我们在此陈述这一性质的两种基本形式, 但只证第二个, 另一个的证明读者自行作出.

第一数学归纳法　令 P_n 是以非负整数 $0,1,2,\cdots$ 为下标的一列命题. 若

(1) P_0 为真,

(2) 对于任意 $k\geqslant 0$, "P_k 为真" 意味着 "P_{k+1} 为真",

则对于任意 $n\geqslant 0$, P_n 为真.

第二数学归纳法　令 P_n 是以非负整数 $0,1,2,\cdots$ 为下标的一列命题. 若

(1) P_0 为真,

(2) 对于任意 $k\geqslant 1$, "P_ℓ 为真, $\ell=0,1,\cdots,k-1$" 意味着 "P_k 为真",

则对于任意 $n\geqslant 0$, P_n 为真.

证明　令

$$F=\{n\mid n\in\mathbb{Z},n\geqslant 0,P_n\text{ 不真}\}.$$

我们只需证明 $F=\varnothing$. 若 $F\neq\varnothing$, 则由良序公理, F 中有最小元素, 记其为 n_0. 由 (1) 知 $n_0>0$. 由于 n_0 的最小性, 对于任意 $\ell=0,1,2,\cdots,n_0-1$, P_ℓ 为真, 由 (2) 知 P_{n_0} 为真, 这导致一个矛盾. 于是, 第二数学归纳法得证. □

$\mathbb{Z}$ 上的加法在 $\mathbb{Z}$ 上有逆运算 (减法). 但 $\mathbb{Z}$ 上的乘法在 $\mathbb{Z}$ 上没有逆运算, 即使将 $\mathbb{Z}$ 换为 $\mathbb{Z}-\{0\}$ 也一样, 因为 $ax=b$ 在 $\mathbb{Z}$ 上并非都有解. 今借助乘法在 $\mathbb{Z}$ 上定义整除关系如下.

令 $a,b\in\mathbb{Z}$. 称 ***a* 整除 *b*** (***b* 被 *a* 整除**), 或称为 a 为 b 的**因子** (b 为 a 的**倍数**), 如果

$$\exists\, d\in\mathbb{Z},\quad b=ad.$$

此时, 记为 $a\mid b$, 否则记为 $a\nmid b$.

容易得到整除的下列基本性质.

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

(2) 令 $a,b_i\in\mathbb{Z}$, $i=1,2,\cdots,n,n\in\mathbb{Z}^+$. 则对于任意 $c_i\in\mathbb{Z}$, $i=1,2,\cdots,n$,

$$a\mid\sum_{i=1}^{n}b_ic_i$$

当且仅当 $a\mid b_i$, $i=1,2,\cdots,n$;

(3) 对于任意 $a\in\mathbb{Z}$, 有

$$(\pm1)\mid a,\quad(\pm a)\mid a,$$

±1 和 $\pm a$ 称为 a 的**平凡因子**;

(4) 若 $a\mid b$, 且 $b\mid a$, 则 $b=\pm a$, 反之亦然.

我们将用第二数学归纳法证明 $\mathbb{Z}$ 上的所谓带余除法.

定理 0.2.1(带余除法)　令 $n,m\in\mathbb{Z}$, $m>0$. 则存在唯一的 q, $r\in\mathbb{Z}$, 使得

$$\begin{cases}n=qm+r,\\0\leqslant r<m.\end{cases}\tag{0.4}$$

证明　当 $n\geqslant 0$ 时, 如果 $n<m$, 那么取 $q=0,r=n$, 就有式 (0.4) 成立; 如果 $n\geqslant m$, 且假设对于任意 k, $0\leqslant k<n$, 存在 $q_1,r_1\in\mathbb{Z}$ (q_1,r_1 依赖于 k), 使得

$$\begin{cases}k=q_1m+r_1,\\0\leqslant r_1<m,\end{cases}$$

那么, 考虑上式中 $k=n-m$ 的情形, 并取 $q=q_1+1,r=r_1$, 即知式 (0.4) 成立. 由第二数学归纳法, 定理的存在性对于任意 $n\geqslant 0$ 成立.

当 $n<0$ 时, 由上述证明知, 存在 $q_1, r_1 \in \mathbb{Z}$, 使得

$$\begin{cases} \mid n \mid = q_1 m + r_1, \\ 0 \leqslant r_1 < m, \end{cases}$$

于是, 若 $r_1 = 0$, 则取 $q = -q_1, r = 0$, 就有式 (0.4) 成立; 若 $r_1 > 0$, 则

$$n = (-q_1)m - r_1 = -(q_1+1)m + (m - r_1),$$

此时, 取 $q = -(q_1+1), r = m - r_1$, 就有式 (0.4) 成立. 这又证明了对于 $n<0$ 定理的存在性也成立.

若存在 $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, 使得

$$\begin{cases} n = q_1 m + r_1, \\ 0 \leqslant r_1 < m, \end{cases} \qquad \begin{cases} n = q_2 m + r_2, \\ 0 \leqslant r_2 < m, \end{cases}$$

则

$$(q_1 - q_2)m = r_2 - r_1.$$

如果 $r_2 - r_1 \neq 0$, 不妨设 $r_2 - r_1 > 0$, 那么由上式, $r_2 - r_1 \geqslant m$, 但注意到有 $r_2 - r_1 < m$, 矛盾. 因此, $r_2 = r_1$, 从而, $q_2 = q_1$. 这又证明了定理的唯一性. □

式 (0.4) 中的 q, r 分别称为 m 除 n 的**商**和**余数**.

推论 0.2.1　令 $a, b \in \mathbb{Z}$. 则

(1) $a = 0$ 时, $a \mid b$ 当且仅当 $b = 0$;

(2) $a \neq 0$ 时, $a \mid b$ 当且仅当 $\mid a \mid$ 除 b 的余数为 0.

下面我们应用整数的带余除法讨论两个整数的最大公因数.

令 $a, b \in \mathbb{Z}$. $d \in \mathbb{Z}$ 称为 a 与 b 的一个**最大公因数**, 如果

(1) $d \mid a$, 且 $d \mid b$ (d 为 a 与 b 的公因数);

(2) 对于任意 $c \in \mathbb{Z}$, 若 $c \mid a$, 且 $c \mid b$, 则 $c \mid d$.

定理 0.2.2　任意整数 a 与 b 都有最大公因数, 且精确到正负号是唯一的.

证明　由最大公因数的定义和整除的基本性质 (4), 定理的上述意义上的唯一性是显然的. 下证任意两个整数的最大公因数的存在性.

若 $a = b = 0$, 则显然 0 就是 a 与 b 的最大公因数. 若 a, b 不全为零, 则

$$S = \{sa + tb \mid s, t \in \mathbb{Z}\} \cap \mathbb{Z}^+ \neq \varnothing,$$

其中 $\mathbb{Z}^+$ 为正整数全体, 即

$$\mathbb{Z}^+ = \{1, 2, \cdots, n, \cdots\}.$$

根据非负整数的良序公理, S 含最小元素, 令它为 d. 显然, $d > 0$, 且 d 为 a 与 b 的线性组合, 即对于某些 $s, t \in \mathbb{Z}$, d 可以表示为

$$d = sa + tb.$$