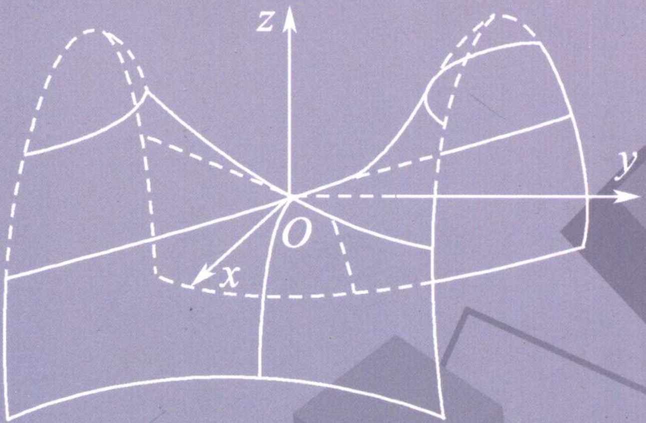
山东省高等学校精品课程
临沂大学优秀校本教材



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

姜同松　任庆军　等编

高等代数与解析几何

Higher Algebra and Analytic Geometry

山东人民出版社
Shandong People's Publishing House

山东省高等学校精品课程
临沂大学优秀校本教材

高等代数与解析几何

Higher Algebra and Analytic Geometry

姜同松 任庆军 等编

山东人民出版社
Shandong People's Publishing House

图书在版编目(CIP)数据

高等代数与解析几何/姜同松等编. —济南:山东人民出版社,2013.8
ISBN 978-7-209-07244-1

Ⅰ.①高… Ⅱ.①姜… Ⅲ.①高等代数-高等学校-教材 ②解析几何-高等学校-教材 Ⅳ.①O15 ②O182

中国版本图书馆 CIP 数据核字(2013)第 131898 号

责任编辑:王 晶
封面设计:彭 路

高等代数与解析几何
姜同松 任庆军 等编

山东出版集团
山东人民出版社出版发行
社 址:济南市经九路胜利大街 39 号 邮 编:250001
网 址:http://www.sd-book.com.cn
发行部:(0531)82098027 82098028
新华书店经销
山东省东营市新华印刷厂印装

规 格 16 开(184mm×260mm)
印 张 26.5
字 数 590 千字
版 次 2013 年 8 月第 1 版
印 次 2013 年 8 月第 1 次
ISBN 978-7-209-07244-1
定 价 46.00 元

临沂大学教材建设指导委员会

主　任：姜同松

成　员：（以姓氏笔画为序）

王统永　毛红旗　孔繁金　申洪源　任世忠　江兆林　全先庆

许汝贞　孙成通　孙成明　朱文玉　李洪忠　张立富　张问银

张根柱　陈学营　陈建国　林光哲　周光亮　郑秀文　赵　勇

赵光怀　徐东升　奚凤兰　谢　楠　彭文修

《高等代数与解析几何》　编写者

姜同松　任庆军　姚金江　孙洪春

周厚春　刁科凤　王建勇　王树艳

前言

《高等代数》与《解析几何》是高等学校数学专业课程中联系十分密切的两门专业基础课程.《高等代数》一般由线性代数和多项式理论组成. 作为《高等代数》的主要研究内容，线性代数理论是由二维、三维几何空间中的向量代数进一步抽象推广得来的，《高等代数》的多数概念和方法都有着很强的几何背景. 而《解析几何》的研究内容则是用代数的方法研究空间的几何问题. 因此，《高等代数》与《解析几何》有着紧密的联系，它们的关系可以归纳为“代数为几何提供研究方法，几何为代数提供直观背景”.

多年来，国内外《高等代数》和《解析几何》大多都是独立设置的两门课程，相应教科书一般都只重视和强调各自课程的独立性，两门课程在各自课程体系的设计和相应教学内容的编排上都普遍注重了各自的完整性、系统性，忽略了两门课程内容以及方法之间的内在联系等，结果导致两门课程在体系和内容上出现重复，在教学中出现了两门课程知识的分割和课程间方法上的隔离. 故传统意义上的课程体系没有能够很好地体现出两课程所共有的代数思维方法，对培养学生运用几何与代数相结合的方法分析问题和解决问题的能力不到位. 而且这种各自独立设置的课程体系和教学内容还导致了教学学时上的增加和重复.

“高等代数和解析几何两课程的整合”是2000年山东省省级立项课题，是山东省课程体系与教学内容试点改革课题，课题成果《高等代数与解析几何》获2004年山东省精品课程，该教改研究课题获2005年山东省优秀教学成果二等奖. 课题即是针对传统《高等代数》和《解析几何》两课程传统的课程体系和教学内容存在的弊端而提出的一个新颖的教学改革课题. 课题的鲜明特色是针对《高等代数》和《解析几何》两课程的基本内涵和方法，进行两课程整合的改革思想. 所谓《高等代数》与《解析几何》两课程的整合是指超越《高等代数》和《解析几何》两课程各自的知识体系，

而以关注《高等代数》和《解析几何》两课程的共同要素的方式来安排学习的课程开发活动. 整合的目的是减少两课程知识的分割和两课程间的隔离，把受教育者所需要的不同的知识体系统一联合起来，实现两课程的整体优化. 本书即是课题组在上述指导思想的指导下，用系统论的观点，从整体优化《高等代数》和《解析几何》的课程体系与教学内容入手，重构的一新型课程体系. 新课程体系较好地体现出鲜明的代数思想和代数方法，避免原两课程体系中无谓的重复，达到整体优化和融合的目的.

《高等代数与解析几何》是高等学校数学专业课程体系中的一门重要的专业基础课程，是数学专业高年级后继课程的重要基础，本课程对数学专业学生专业课程的学习来说具有承上启下的关键作用. 课程的特点是内容抽象，逻辑性强. 通过课程的教学，一方面培养学生运用代数与几何相结合的方法分析问题与解决问题的能力，实现由初等数学的思维方式向现代数学的思维方式的转变，培养学生的抽象思维和严密逻辑推理能力；另一方面为数学专业高年级后继课程的学习打下良好的基础. 课程教学的难点是培养学生掌握代数与几何的基本理论和基本方法，重要的是培养学生的高等代数与几何的思维方法，培养学生抽象思维能力、逻辑推理能力以及数学哲学思想素质，实现知识、能力和素质的协调全面发展.

《高等代数与解析几何》的基本内容由线性代数、多项式理论和解析几何三个基本模块组成. 全书共分十三章. 第一章是预备知识. 第二章引入 n 阶行列式的概念，研究了行列式的一系列性质. 第三章介绍几何空间中的向量代数，讨论了平面与直线问题. 矩阵是高等代数中最基本的工具，第四章介绍矩阵代数、可逆矩阵、矩阵的秩、矩阵的初等变换以及矩阵分块的技巧和应用，为以后进一步学习打好基础. 第五章利用矩阵的方法研究线性方程组解的理论，给出了线性方程组的解与矩阵的秩之间的关系. 第六章研究一元多项式的理论. 第七章引入一般向量空间的定义，讨论向量组的线性相关性，研究一般向量空间的一系列性质. 第八章引入并讨论线性变换，通过矩阵来描述线性变换，建立起线性变换与矩阵间的联系. 第九章通过引入 λ- 矩阵的概念，研究矩阵的若当标准形理论. 第十章引入一般向量空间上的内积，建立并研究一般欧氏空间的一系列理论. 第十一章讨论二次型的化简及正定二次型等理论. 第十二章讨论几何空间的常见曲面方程的建立与性质，通过二次型的主轴问题给出化一般二次曲面方程为

标准方程的方法. 最后在第十三章讨论二次曲线的一般理论.

本书第一版于 2005 年 8 月由石油大学出版社出版. 本次修订再版进一步优化了课程体系与教学内容，增加了二次曲线的一般理论一章，对各章节的习题也进行了修改和完善，增添了问答和判断题，在每一章的最后一节还增设了 Matlab 算例. 另外，作者还编写了《高等代数方法与技巧》一书，对高等代数的解题方法进行了认真系统地梳理和总结，必要时读者可以配套选用.

本书力求做到代数方法和几何方法的结合，突出矩阵方法这一主线，通过用矩阵代数的方法来研究和解决代数和几何中的一系列问题，使问题处理得更加简洁明了. 同时，使学生对代数方法的几何背景有更深入的了解，能够更好地培养和提高学生的抽象思维和逻辑推理能力.

作为山东省课程体系和教学内容改革课题成果以及山东省精品课程教材，本书是课程教学团队成员多年教学经验与成果的积累和总结，是在我校原《高等代数与解析几何》精品课程教材的基础上，由姜同松教授、任庆军教授、姚金江教授、孙洪春教授、周厚春教授、刁科凤教授、王建勇、王树艳等进一步修订优化编写而成，最后由姜同松博士定稿. 在修订编写过程中，山东大学数学系的博士生导师刘桂真教授、华东师范大学数学系的博士生导师魏木生教授对本书提出了许多宝贵意见和建议，在此表示诚挚的谢意！

本教材被学校评选确定为优秀立项建设教材，并得到学校出版资助.

水平所限，不妥之处在所难免，诚望读者批评指正！

编　者

2013 年 8 月

CONTENTS 目 录

第七章 向量空间 /190

第八章 线性变换 /225

第九章 若当（Jordan）标准形 /260

第十章 欧氏空间 /281

CHAPTER 1 第一章 预备知识

在这一章里，我们把本课程要用到的一些基本知识介绍一下，为今后的学习做必要的准备.

1.1 数环和数域

我们进行数的四则运算，总是要在一定的数的范围内进行. 最初接触的一个重要的数的范围可以认为是自然数集合，在自然数集合中，数的四则运算中的加法和乘法可以永远进行，但减法和除法却不能永远进行. 将自然数集合扩展到整数集合，则数的加法、减法、乘法可以永远进行. 但除法即使在除数不为零的情况下，仍不能永远进行. 再将整数集合扩展到有理数集合，则数的四则运算都能永远进行，只是除法有除数不为零的限制.

由此我们给出

定义 1.1 设 S 是复数集 $\mathbf{C}$ 的一个非空子集，如果对于 S 中任意两个数 a 和 b，$a-b$，$a+b$ 和 ab 都在 S 内，即 S 关于数的加法、减法、乘法封闭，则称 S 是一个**数环**.

定义 1.2 设 F 是一个数环且至少含有一个非零的数，若对 F 中任意两个数 a 和 $b(b\neq 0)$，$\dfrac{a}{b}$ 都在 F 内，即 F 关于数的除法封闭，则称 F 是一个**数域**.

由定义可知，数域一定是数环，但反之不然.

例如，有理数集 $\mathbf{Q}$，实数集 $\mathbf{R}$，复数集 $\mathbf{C}$ 都是数域，同时也是数环，整数集 $\mathbf{Z}$ 是数环，但不是数域.

我们再看几个例子.

例 1.1 取定一个整数 a，令

$$S=\{na\mid n\in\mathbf{Z}\}.$$

则 S 是一个数环，这是因为，设 $n_1,n_2\in\mathbf{Z}$，则

$$n_1a\pm n_2a=(n_1\pm n_2)a\in S,$$

$$(n_1a)(n_2a)=(n_1n_2a)a\in S.$$

但显然 S 不是数域. 当取 $a=2$ 时, S 就是全体偶数组成的数环, 通常称为偶数环. 当 $a=0$ 时, S 由单独一个数 0 组成, $\{0\}$ 可以说是最小的数环, 这是因为, 假设 S 是一个数环, 由于 S 非空, 因此可以在其中任取一个数 b, 则 $b-b=0\in S$, 即任意数环包含 $\{0\}$.

例 1.2 令 $S=\{a+bi\mid a,b\in\mathbf{Z},i^2=-1\}$, 则对于 S 中任意元素 $a+bi$ 与 $c+di$ 有

$$(a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i\in S,$$
$$(a+bi)(c+di)=(ac-bd)+(bc+ad)i\in S.$$

所以 S 是一个数环, 但 S 显然不是数域, 这是因为 $2\in S, 3\in S$, 而 $\frac{2}{3}\notin S$.

例 1.3 令 $F=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$, 则 F 是一个数域.

这是因为对任意 $a+b\sqrt{2}, c+d\sqrt{2}\in F$, 有

$$(a+b\sqrt{2})\pm(c+d\sqrt{2})=(a\pm c)+(b\pm d)\sqrt{2}\in F,$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in F.$$

因此 F 是数环.

又 $1+0\sqrt{2}=1\neq 0$, 所以 F 中含有非零数.

现在设 $c+d\sqrt{2}\neq 0$, 则 $c-d\sqrt{2}\neq 0$, 否则, 在 $d=0$ 的情况下将得出 $c=0$, 这与 $c+d\sqrt{2}\neq 0$ 的假设矛盾, 在 $d\neq 0$ 的情况下得出 $\sqrt{2}=\frac{c}{d}\in\mathbf{Q}$, 这与 $\sqrt{2}$ 是无理数矛盾. 因此,

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}$$
$$=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}\in F.$$

这就证明了 F 是一个数域.

最后我们证明数域的一个重要性质, 即

定理 1.1 任何数域都包含有理数域 $\mathbf{Q}$.

证明 设 F 是任意一个数域, 由数域定义知 F 含有不为零的数, 任取 $a\neq 0$, 则由数域关于除法的封闭性知 $1=\frac{a}{a}\in F$, 由数域关于加法的封闭性知 $1+1, 1+1+1,\cdots$ 即全体正整数属于 F, 由数域关于减法的封闭性知 $0=1-1\in F$, 且任意负整数 $-n=0-n\in F$, 这样 F 含有全体整数. 又因为任意一个有理数可以表示为除数不为零的两个整数之商, 所以由数域关于除法的封闭性知 F 含有全体有理数.

在这个定理的意义之下, 我们常说有理数域是最小的数域.

习 题 1.1

1. 证明: 如果一个数环 $S\neq\{0\}$, 那么 S 含有无限多个数.
2. 证明: $F=\{a+bi\mid a,b\in\mathbf{Q}\}$ 是数域.
3. 证明: $S=\{\frac{m}{2^n}\mid m,n\in\mathbf{Z}\}$ 是一个数环. S 是不是数域?

4. 证明：两个数环的交是一个数环. 两个数域的交是一个数域. 两个数环的并是不是数环？

1.2 数学归纳法

数学归纳法是进行数学证明的有力工具之一. 数学归纳法所依据的原理是自然数集的一个最基本的性质 —— 最小数原理.

最小数原理 自然数集 $\mathbf{N}$ 的任意一个非空子集 S 必含有一个最小数，也就是存在一个数 $a \in S$，对于 $\forall c \in S$ 都有 $a \leqslant c$.

注意 1° 最小数原理并不是对任意数集都成立的. 例如，整数集 $\mathbf{Z}$ 就没有最小数.

2° 设 c 是任意一个整数，令

$$Mc = \{x \in \mathbf{Z} \mid x \geqslant c\},$$

那么以 Mc 代替自然数集 $\mathbf{N}$，最小数原理对于 Mc 仍然成立，也就是说，Mc 的任意一个非空子集必含有一个最小数. 特别地，当 $c = 0$ 时，可得一切非负整数所成的集合 $M_0 = \{0, 1, 2, 3, \cdots\}$ 的任一非空子集必含有一个最小数.

由最小数原理可得出以下的数学归纳法原理.

第一数学归纳法原理 设有一个与自然数 n 有关的命题，如果

1° 当 $n = 1$ 时，命题成立；

2° 假设 $n = k$ 时命题成立，则 $n = k + 1$ 时，命题也成立.

那么这个命题对于一切自然数 n 都成立.

证明 假设命题不是对于一切自然数都成立，令 S 表示使命题不成立的自然数所成的集合，那么 $S \neq \varnothing$，于是由最小数原理，S 中有最小数 h，因为命题对于 $n = 1$ 成立，所以 $h \neq 1$，从而 $h - 1$ 是一个自然数，因为 h 是 S 中的最小数，所以 $h - 1 \notin S$. 这就是说，当 $n = h - 1$ 时，命题成立. 于是由 2°，当 $n = h$ 时命题也成立，因此 $h \notin S$，这就导致了矛盾.

注意 根据最小数原理的 2°，我们可以取 Mc 来代替自然数集 $\mathbf{N}$. 也就是说，如果要证明某一命题从某个整数 c 开始成立，这时仍然可以利用数学归纳法来证明，只要把第一数学归纳法原理中条件 1° 的 $n = 1$ 换成 $n = c$ 就行了.

我们看一个例子.

例 1.4 证明：当 $n \geqslant 3$ 时，n 边形的内角和等于 $(n-2)\pi$.

证明 1° 当 $n = 3$ 时，命题成立，因为三角形内角和等于 $\pi = (3-2)\pi$.

2° 假设 $n = k(k \geqslant 3)$ 时命题成立，对于任意一个 $k+1$ 边形 $A_1A_2\cdots A_kA_{k+1}$，连接 A_1A_3，那么 $A_1A_2\cdots A_kA_{k+1}$ 的内角和等于三角形 $A_1A_2A_3$ 的内角和再加上 k 边形 $A_1A_3\cdots A_kA_{k+1}$ 的内角和. 前者等于 π，后者由归纳假设，等于 $(k-2)\pi$，因此 $k+1$ 边形 $A_1A_2\cdots A_kA_{k+1}$ 的内角和等于

$$\pi + (k-2)\pi = (k-1)\pi = ((k+1)-2)\pi.$$

命题得证.

在有些情况下，归纳假定"命题对于 $n = k$ 成立"还不够，而需要较强的假定. 我们有

第二数学归纳法原理　设有一个与自然数 n 有关的命题,如果

1°　当 $n=1$ 时命题成立;

2°　假设命题对于一切小于 k 的自然数来说成立,则命题对于 k 也成立.

那么命题对于一切自然数 n 都成立.

可依照第一数学归纳法原理进行证明.

当然,在这个原理中,条件 1° 也可以换成 n 等于某一个整数 c.

例 1.5　设 $a_1=3, a_2=7, a_n=3a_{n-1}-2a_{n-2}(n=3,4,\cdots)$,试证:对任意自然数 n 都有 $a_n=2^{n+1}-1$.

证明　1° 当 $n=1$ 时,$a_1=3=2^{1+1}-1$.

当 $n=2$ 时,$a_2=7=2^{2+1}-1$.

所以对于 $n=1,2$,命题成立.

2° 假设 $n<k$ 时命题成立,要证 $a_k=2^{k+1}-1$,其中 $k\geqslant 3$.

因为$a_k=3a_{k-1}-2a_{k-2}$,由归纳假设有

$$a_{k-1}=2^{(k-1)+1}-1, a_{k-2}=2^{(k-2)+1}-1,$$

所以$a_k=3(2^k-1)-2(2^{k-1}-1)$

$=2^{k+1}-1$.

这就是说,$n=k$ 时命题也成立.

习　题 1.2

1. 证明:$1\cdot 1!+2\cdot 2!+\cdots+n\cdot n!=(n+1)!-1$.
2. 设 h 是一个正整数,证明:$(1+h)^n\geqslant 1+nh$,h 是任意自然数.
3. 证明二项式定理:
$(a+b)^n=a^n+C_n^1a^{n-1}b+\cdots+C_n^ra^{n-r}b^r+\cdots+b^n$.
4. 证明第二数学归纳法原理.

1.3　整数的整除性

在中小学数学里,我们已经接触过与整数的整除有关的性质,但缺少严格的证明,这一节里,我们将对这方面的问题做较为深入的讨论.

1.3.1　整除

定义 1.3　设 a,b 是两个整数,如果存在一个整数 q,使得 $b=aq$,则称 a 整除 b(或说 b 被 a 整除),记作 $a\mid b$,这时 a 称为 b 的因数或约数,而 b 称为 a 的倍数,否则称 a 不整除 b,记作 $a\nmid b$.

容易推出下列关于整除的基本性质:

1) $a\mid b, b\mid c\Rightarrow a\mid c$.

2) $a \mid b, a \mid c \Rightarrow a \mid (b+c)$.

3) $a \mid b, c \in \mathbf{Z} \Rightarrow a \mid bc$.

4) $a \mid b_i, c_i \in \mathbf{Z}, i = 1,2,\cdots,t \Rightarrow a \mid (b_1c_1 + b_2c_2 + \cdots + b_tc_t)$.

5) 每一个整数都被1和-1整除.

6) 每一个整数a都被它自身和它的相反数$-a$整除.

7) $a \mid b$且$b \mid a \Rightarrow b = a$或$b = -a$.

这些性质都是明显的,我们只证明最后一个.

由$a \mid b$且$b \mid a$,我们有$b = ac, a = bd$,这里$c, d \in \mathbf{Z}$,于是$a = acd$,如果$a = 0$,那么$b = ac = 0 = a$;如果$a \neq 0$,那么$cd = 1$,从而$c = d = 1$或$c = d = -1$,于是$b = a$或$b = -a$.

下面我们给出整数的带余除法定理,它在整数的整除性理论中占有重要的地位.

定理 1.2 (带余除法定理) 设a, b是整数且$a \neq 0$,则存在唯一的一对整数q和r,使

$$b = aq + r \text{ 且 } 0 \leqslant r < |a|.$$

证明 令$S = \{b - ax \mid x \in \mathbf{Z}, b - ax \geqslant 0\}$,因为$a \neq 0$,所以$S$是非负整数集$M_0$的非空子集,根据最小数原理(对于$M_0$),$S$含有一个最小数,也就是说,存在$q \in \mathbf{Z}$,使得$r = b - aq$是$S$中的最小数,于是$b = aq + r$,并且$r \geqslant 0$.如果$r \geqslant |a|$,那么$r = |a| + r', r' \geqslant 0$,而

$$r' = \begin{cases} b - a(q+1), \text{若 } a > 0; \\ b - a(q-1), \text{若 } a < 0. \end{cases}$$

所以$r' \in S$且$r' < r$,这与r是S中的最小数矛盾,因此$r < |a|$.

假设还有$q', r' \in \mathbf{Z}$,使得

$$b = aq' + r' \text{ 且 } 0 \leqslant r' < |a|.$$

于是就有$a(q - q') = r' - r$,如果$q - q' \neq 0$,那么

$$|r' - r| = |a(q - q')| \geqslant |a|.$$

由此或者$r' \geqslant |a| + r \geqslant |a|$,或者$r \geqslant |a| + r' \geqslant |a|$,不论是哪一种情形,都导致矛盾.这样,必须$q - q' = 0$,从而$r' - r = 0$,也就是说$q' = q, r' = r$.

定理1.2中唯一确定的整数q和r分别叫做a除b所得的商和余数.

例如,$a = -5, b = 18$,则$q = -3, r = 3$;

$a = -5, b = -18$,则$q = 4, r = 2$.

根据带余除法,给出一对整数a, b,我们可以判断a能否整除b.如果$a \neq 0$,那么$a \mid b$当且仅当a除b所得的余数$r = 0$,如果$a = 0$,那么a只能整除0.

1.3.2 最大公因数

定义 1.4 若a, b是两个整数,满足下列条件的整数d叫做a与b的一个**最大公因数**:

1) $d \mid a$且$d \mid b$;

2) 如果$c \in \mathbf{Z}$,且$c \mid a, c \mid b$,那么$c \mid d$.

一般地,设$a_1, a_2, \cdots, a_n$是n个整数,满足下列条件的整数d称为$a_1, a_2, \cdots, a_n$的一个最大公因数:

1) $d \mid a_i, i=1,2,\cdots,n$;

2) 如果 $c \in \mathbf{Z}$ 且 $c \mid a_i, i=1,2,\cdots,n$,那么 $c \mid d$.

关于任意 n 个整数的最大公因数,我们有

定理 1.3 任意 $n(n \geqslant 2)$ 个整数 $a_1,a_2,\cdots,a_n$ 都有最大公因数.如果 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因数,那么 $-d$ 也是一个最大公因数,且 $a_1,a_2,\cdots,a_n$ 的两个最大公因数最多相差一个符号.

证明 先证明任意 n 个整数 $a_1,a_2,\cdots,a_n$ 有最大公因数.

如果 $a_1=a_2=\cdots=a_n=0$,那么 0 显然是 $a_1,a_2,\cdots,a_n$ 的最大公因数.

设 $a_1,a_2,\cdots,a_n$ 不全为零,我们考虑 $\mathbf{Z}$ 的子集

$$I=\{t_1a_1+t_2a_2+\cdots+t_na_n \mid t_i \in \mathbf{Z}, 1 \leqslant i \leqslant n\}.$$

I 显然不是空集,因为对于每一个 i,都有

$$a_i=0 \cdot a_1+\cdots+0 \cdot a_{i-1}+1 \cdot a_i+0 \cdot a_i+\cdots+0 \cdot a_n \in I.$$

又因为 $a_1,a_2,\cdots,a_n$ 不全为零,所以 I 含有正整数.因此

$$I^+=\{s \mid s \in I \text{ 且 } s>0\}$$

是自然数集的一个非空子集.于是由最小数原理,I^+ 有一个最小数 d,我们说 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因数.

首先,因为 $d \in I^+$,所以 $d>0$ 并且 d 有形式

$$d=t_1a_1+t_2a_2+\cdots+t_na_n \in \mathbf{Z} \quad (1 \leqslant i \leqslant n).$$

又由带余除法,我们有

$$a_i=dq_i+r_i, 0 \leqslant r_i<d \quad (1 \leqslant i \leqslant n).$$

如果某一 $r_i>0$,比方说 $r_1>0$,那么

$r_1=a_1-dq_1=(1-t_1q_1)a_1-t_2q_1a_2-\cdots-t_nq_1a_n \in I^+$,

而 $r_1<d$,这与 d 是 I^+ 中的最小数的事实矛盾.这样,必须所有 $r_i=0$,即 $d \mid a_i, i=1,2,\cdots,n$.另一方面,如果 $c \in \mathbf{Z}, c \mid a_i, i=1,2,\cdots,n$,则 $c \mid (t_1a_1+\cdots+t_na_n)$,即 $c \mid d$.这就证明了 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因数.

由最大公因数的定义和整除的基本性质,定理后一部分的正确性是明显的.

这个定理告诉我们,任意 n 个整数的最大公因数一定存在,并且除相差一个符号外,是由这 n 个整数唯一确定的,我们把 n 个整数 $a_1,a_2,\cdots,a_n$ 的非负的最大公因数记作 $(a_1,a_2,\cdots,a_n)$.

由定理 1.3 的证明,我们还可得出关于最大公因数的一个重要性质,这就是

定理 1.4 设 d 是整数 $a_1,a_2,\cdots,a_n$ 的一个最大公因数,那么存在整数 $t_1,t_2,\cdots,t_n$,使得

$$t_1a_1+t_2a_2+\cdots+t_na_n=d.$$

证明 如果 $a_1=a_2=\cdots=a_n=0$,那么 $d=0$,定理显然成立.设 $a_1,a_2,\cdots,a_n$ 不全为零,由定理 1.3 的证明,我们知道 $d \in I$,因而存在 $t_1,t_2,\cdots,t_n \in \mathbf{Z}$,使得 $d=t_1a_1+\cdots+t_na_n$.

1.3.3 互素

定义 1.5 设 a,b 是两个整数,如果 $(a,b)=1$,那么就说 a 与 b **互素**.