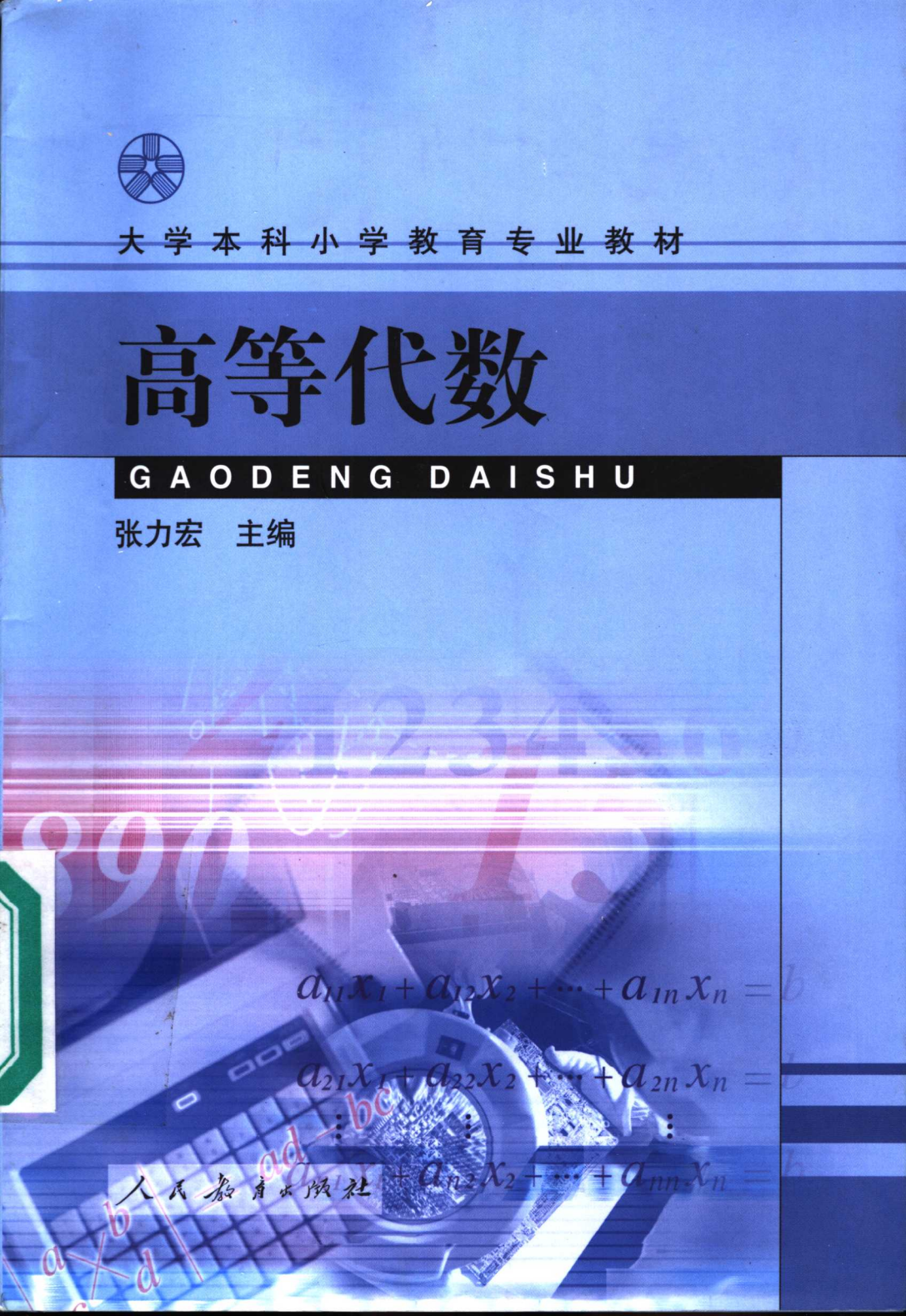
大学本科小学教育专业教材

高等代数

GAODENG DAISHU

张力宏　主编



大学本科小学教育专业教材

高等代数

主　编　张力宏
副主编　刘效丽
　　刘德鹏

人民教育出版社
·北京·

图书在版编目（CIP）数据

高等代数/张力宏主编. —北京：人民教育出版社，2002

大学本科小学教育专业教材

ISBN 7-107-15629-2

Ⅰ. 高…

Ⅱ. 张…

Ⅲ. 高等代数—高等学校—教材

Ⅳ. 015

中国版本图书馆 CIP 数据核字（2002）第 043647 号

人民教育出版社 出版发行

（北京沙滩后街 55 号　邮编：100009）

网址：http://www.pep.com.cn

人民教育出版社 印刷厂印装　　全国新华书店经销

2002 年 9 月第 1 版　2002 年 9 月第 1 次印刷

开本：890 毫米×1240 毫米　1/32　印张：12.25

字数：308 千字　　印数：0 001～2 000 册

定价：17.80 元

本书编者说明

本书是根据大学本科小学教育专业的培养需要而编写的《高等代数》课教材，供培养师范本科小学教师使用.

开设这门课程的目的主要是培养小学教师掌握基本的数学基础知识，训练小学教师的抽象思维能力，体会数学的思想方法，提高数学教学的专业素质.

本书在内容的选择和安排上，以有利于基本理论的掌握、巩固、提高，有利于基本方法的培养和应用为原则. 在编写过程中充分体现矩阵在线性代数中的工具作用，尽量做到通俗、易懂，力求与初等代数相衔接.

全书共分八章、三部分. 第一部分为多项式理论，主要研究多项式整除、因式分解等理论问题，以体现初等数学中多项式整除、最大公因数、因数分解等问题是多项式理论的特殊情况. 第二部分为行列式、矩阵、线性方程组. 在这部分中，注重突出矩阵的作用，特别是在线性方程组中的应用. 这样，既体现了高等代数的思想方法，又体现了中学数学的继续. 第三部分以向量空间、欧氏空间、线性变换和二次型等抽象的代数概念为主体揭示空间的结构. 从矩阵的角度体现线性变换在空间上的作用，利用矩阵有具体表现形式的优点尽量淡化线性变换等抽象概念，利用矩阵可以进行具体运算的优点来化简二次齐次多项式的形式以达到研究其几何性质的目的.

考虑到读者对象，我们在每介绍一个新概念之后都引进一些简单例子以增加读者对所述知识点的理解. 在每章后面都有综合例题分析作为习题课内容，以便提高学生的综合分析能力和解题能力.

在部分内容后面简单介绍了该部分内容的历史起源和发展概况，希望读者对所学内容有一个比较全面系统的了解.

本书由张力宏主编，副主编是刘效丽、刘德鹏. 各部分执笔人是：第一、八章，赵国良；第二、三章，刘效丽；第四、六、七章，张力宏；第五章，周双苗；各章综合例题分析和发展简史，刘德鹏.

张力宏对全书的结构作了统一的设计构思，并最后承担了书稿的修订和统稿、定稿工作.

全书计划约 108 学时讲完，使用本书的教师可根据学时要求及学生的实际需要，在教学时可以对书中内容作适当的取舍.

北京师范大学数学系郝钢新教授认真审阅了本书的编写大纲和全部书稿. 担任本书责任编辑和审稿工作的，除了有人民教育出版社本身的编审人员外，还有中国科学院数学研究所燕敦验博士后和首都师范大学数学系华德康教授. 他们为本教材的修改、润色、完善，付出了艰辛的劳动和大量的心血. 在此，我们谨向以上各位老师表达由衷的谢意.

编　者

2002 年 6 月

目　录

第一章　多项式理论

初等代数课程的中心内容是关于解方程的问题. 方程的研究是从只含一个未知量的一个一次方程开始，然后向两个方向发展：一方面，讨论含两个未知量两个一次方程的所谓二元一次方程组以及三元一次方程组等；另一方面，研究一个只含一个未知量的二次方程及某些可化为二次方程的高次方程. 这些问题构成了初等代数的中心内容. 在高等代数课程中，这两个方面均得到进一步的发展，分成高等代数的两大组成部分：线性代数基础和多项式理论.

§1.1　数的基本知识

本节主要给出整数的整除性、最大公因数、因数分解定理及数环与数域等内容.

在本书中，自然数集合、整数集合、有理数集合、实数集合、复数集合分别用 **N**、**Z**、**Q**、**R**、**C** 表示.

定义 1　设 a、$b\in\mathbf{Z}$. 若存在 $q\in\mathbf{Z}$，使等式

$$a=bq \tag{1}$$

成立，则称 b 整除 a，或 a 被 b 整除. 用记号 $b\mid a$ 表示；若满足 (1) 式的整数 q 不存在，则称 b 不整除 a 或 a 不能被 b 整除，用记号 $b\nmid a$ 表示.

如果 $b\mid a$，我们说 b 是 a 的因数或约数，而 a 是 b 的倍数.

由整除的定义，容易得出下述结果.

定理 1.1.1 若 $c \mid b$，$b \mid a$，则 $c \mid a$.

定理 1.1.2 若 $m \mid a$，$m \mid b$，则对任意的 p、$q \in \mathbf{Z}$ 有 $m \mid pa+qb$.

由于整数加法满足结合律，上述定理 1.1.2 中两个整数 a、b 可以推广到任意有限多个整数的情形.

定理 1.1.3 （带余除法）若 a、$b \in \mathbf{Z}$，$b \neq 0$，则存在惟一的 q、$r \in \mathbf{Z}$，使

$$a=bq+r,\ 0 \leqslant r < |b|. \tag{2}$$

证明：由于 $a=bq+r$ 成立当且仅当 $a=(-b)(-q)+r$ 成立，因此可设 $b>0$. 对于整数序列

$$\cdots -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b,\ \cdots$$

有两种情形：

1）a 恰好是该序列中某一项，此时有

$$a=bq+0,\ r=0;$$

2）a 介于该序列某相邻两项之间，此时有

$$bq<a<b(q+1),\quad q \in \mathbf{Z}.$$

或改写为

$$0<a-bq<b,\quad q \in \mathbf{Z}.$$

令 $r=a-bq$，则

$$a=bq+r\quad 0<r<b.$$

综合以上两种情形，有

$$a=bq+r\quad 0 \leqslant r < |b|.$$

如果还有 q_1，$r_1 \in \mathbf{Z}$，使

$$a=bq_1+r_1,\quad 0 \leqslant r_1 < |b|,$$

那么有

$$\begin{aligned} bq+r&=bq_1+r_1,\\ b(q-q_1)&=r_1-r,\\ |b|\ |q-q_1| &= |r_1-r|. \end{aligned} \tag{*}$$

由于分别有 $0\leqslant r<|b|$，$0\leqslant r_1<|b|$，$-|b|<-r\leqslant 0$，所以 $-|b|<r_1-r<|b|$，$|r_1-r|<|b|$. 若 $q\neq q_1$，(*)式左端大于或等于 $|b|$，矛盾. 所以 $q=q_1$，从而 $r=r_1$，即满足(2)式的 q、$r\in\mathbf{Z}$ 是惟一的.

定义 2　设 a、b、$d\in\mathbf{Z}$，如果满足 $d\mid a$，$d\mid b$，并且对任意的 $h\in\mathbf{Z}$，只要 $h\mid a$，$h\mid b$，就有 $h\mid d$，则称 d 是 a 和 b 的一个最大公因数.

应该注意到，定义 2 包含两层意思. 首先由 $d\mid a$，$d\mid b$ 说明 d 同时是 a 和 b 的因数，此时可称为 a 和 b 的公因数；其次由 $h\mid d$ 说明 d 是 a 和 b 的任意公因数的倍数，表明了 d 的最大性.

对任意的 $a\in\mathbf{Z}$，由于总有 $0=a0$，说明 a 是 a 和 0 的公因数. 很显然，a 是 a 和 0 的最大公因数. 设 a、$b\in\mathbf{Z}$，如果 $a\mid b$，则 a 是 a、b 的最大公因数.

定理 1.1.4　设 a、b、$c\in\mathbf{Z}$，满足 $a=bq+c$，其中 $q\in\mathbf{Z}$，则两组整数对 a、b 与 b、c 有相同的最大公因数.

证明：设 d 是 a、b 的最大公因数，则 $d\mid a$，$d\mid b$，由 $a=bq+c$ 及定理 1.1.2，有 $d\mid c$，得 d 是 b、c 的公因数；设 h 是 b、c 的任意公因数，即有 $h\mid b$，$h\mid c$，再由 $a=bq+c$ 及定理 1.1.2 有 $h\mid a$，所以 h 是 a、b 的公因数，得 $h\mid d$，说明 d 是 b、c 的最大公因数.

反之，注意到 $c=b(-q)+a$，再重复上述证明可得 b、c 的最大公因数也是 a、b 的最大公因数.

有定理 1.1.4 之后，我们可以得到

定理 1.1.5　对任意 a、$b\in\mathbf{Z}$，都有最大公因数.

证明：如果 a、b 中有一个为 0，则另一个就是最大公因数；如果 a、b 都不为 0，由带余除法，有 q_1、$r_1\in\mathbf{Z}$，使

$$a=bq_1+r_1\qquad 0\leqslant r_1<|b|.$$

如果 $r_1=0$，显然 b 就是 a、b 的最大公因数. 否则，再由带余除

法，有 q_2、$r_2\in\mathbf{Z}$ 使

$$b=r_1q_2+r_2 \qquad 0\leqslant r_2<|r_1|=r_1.$$

如果 $r_2=0$，则 r_1 就是 b、r_1 的最大公因数，由定理 1.1.4，亦是 a、b 的最大公因数. 否则，再由带余除法，如此继续下去……由于每进行一次带余除法，余数 r_i 至少减 1，所以经过有限次带余除法之后，总有 q_n，q_{n+1}，$r_n\in\mathbf{Z}$，使

$$r_{n-2}=r_{n-1}q_n+r_n \quad 0\leqslant r_n<r_{n-1}$$

$$r_{n-1}=r_nq_{n+1}.$$

所以反复应用定理 1.1.4，可得 r_n 就是 a，b 的最大公因数.

这个定理的重要性在于证明过程给出了两个数的最大公因数的求法. 事实上最大公因数不惟一.

定理 1.1.6 设 d 是 a，b 的最大公因数，则 d' 也是 a，b 的最大公因数当且仅当 $d=\pm d'$.

证明：如果 d' 也是 a，b 的最大公因数，则由定义 2，有 $d\mid d'$，$d'\mid d$，即有 q，$q'\in\mathbf{Z}$，使

$$d'=dq, \quad d=d'q',$$

从而有 $1=qq'$，得 $q'=\pm1$，所以 $d=\pm d'$；

反之，因为 d 是 a，b 的最大公因数，显然 $-d$ 也是 a，b 的最大公因数.

定理 1.1.6 说明了虽然 a，b 的最大公因数不是惟一的，但是它们只相差一个符号. 通常用 (a, b) 表示 a，b 的正的最大公因数.

完全与定义 2 类似，可以给出任意有限多个整数的最大公因数的定义.

定义 3 设 $a_i\in\mathbf{Z}$，$i=1, 2, \cdots, n$，$d\in\mathbf{Z}$，如果 $d\mid a_i$，$i=1, 2, \cdots, n$，并且对 $h\in\mathbf{Z}$，只要 $h\mid a_i$，$i=1, 2, \cdots, n$，就有 $h\mid d$，则称 d 是 a_1，a_2，$\cdots$，a_n 的一个最大公因数. 用符号 $(a_1, a_2, \cdots, a_n)$ 表示 a_1，a_2，$\cdots$，a_n 的正的最大公因数. 如果 $(a_1, a_2, \cdots, a_n)=1$，则称 a_1，a_2，$\cdots$，a_n 互质或互素.

定理 1.1.7　设 a，$b\in\mathbf{Z}$，则 a，b 互质当且仅当有 u、$v\in\mathbf{Z}$，使

$$au+bv=1. \tag{3}$$

证明：如果（3）式成立，则对 a，b 的任一公因数 h，都有 $h\mid 1$，从而 $h=\pm 1$，得$(a,\ b)=1$；

反之，如果$(a,\ b)=1$，由定理 1.1.5 的证明过程，有等式组

$$\begin{aligned}
a-bq_1&=r_1\\
b-r_1q_2&=r_2\\
&\cdots\cdots\\
r_{n-3}-r_{n-2}q_{n-1}&=r_{n-1}\\
r_{n-2}-r_{n-1}q_n&=1\\
r_{n-1}-q_{n+1}&=0.
\end{aligned}$$

从倒数第二个等式开始，顺次将上一等式代入下一个等式，再整理就有（3）式.

定理 1.1.8　设 a，b，$c\in\mathbf{Z}$，

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

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

证明：1）根据定理 1.1.7，如果$(a,\ b)=1$，则（3）式成立，由 c 乘（3）式两端，有

$$acu+bcv=c.$$

显然 a 整除该式左端，从而 $a\mid c$.

2）由于 $a\mid c$，$b\mid c$，得 $ab\mid ac$，$ab\mid bc$，从而有

$$ab\mid acu+bcv=c.$$

定义 4　设 p 是大于 1 的整数. 如果 p 不能写成两个比 p 小的正整数的乘积，则称 p 为质数或素数.

显然，p 是质数当且仅当除了 1 和 p 之外 p 没有其他正因数. 关于质数有下面的结果.

定理 1.1.9　设 p 是质数，

1) 对任意 $a\in\mathbf{Z}$，有 $p\mid a$ 或 $(p,a)=1$；

2) 对 $a,b\in\mathbf{Z}$，由 $p\mid ab$，有 $p\mid a$ 或 $p\mid b$.

证明：1) 如果 $(p,a)\neq 1$，则由 $(p,a)\mid p$ 及 p 是质数，有 $(p,a)=p$，即 $p\mid a$；

2) 如果 $p\nmid a$，由 1)，$(p,a)=1$，再由定理 1.1.8 的 1)，得 $p\mid b$.

由归纳法不难证明，设 p 是质数，若 $p\mid a_1a_2\cdots a_n$，则必有某一 i，$1\leqslant i\leqslant n$，使得 $p\mid a_i$.

定理 1.1.10（算术基本定理） 任意一个大于 1 的整数 n 都能写成有限个质数的乘积，即

$$n=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}, \tag{4}$$

其中 p_1，p_2，…，p_s 是互不相同的质数，$r_i(i=1,2,\cdots,s)$是正整数；如果不考虑因数的次序，该分解式是惟一的.

证明：若 $n=2$，则（4）式显然成立.

假设对大于 2 小于 n 的整数结论成立，下面证明对于 n 结论也成立.

如果 n 是质数，定理成立. 如果 n 不是质数，则由定义 4，有大于 1 小于 n 的整数 a_1，a_2，使

$$n=a_1a_2.$$

由归纳假设，a_1，a_2 均能写成（4）式，所以对 n，（4）式成立.

现在证明分解的惟一性，如果还有

$$n=q_1^{l_1}q_2^{l_2}\cdots q_t^{l_t} \tag{4'}$$

其中 q_1，q_2，…，q_t 是互不相同的质数，$l_i(i=1,2,\cdots,t)$是正整数. 下面对 s 作归纳法.

当 $s=1$ 时，有

$$n=p_1^{r_1}=q_1^{l_1}q_2^{l_2}\cdots q_t^{l_t}.$$

根据定理 1.1.9，存在某个 $q_i(1\leqslant i\leqslant t)$，使 $p_1\mid q_i$，但 q_i 是质数，得 $p_1=q_i$，不妨设 $q_i=q_1$，有 $p_1=q_1$. 如果 $r_1\neq l_1$，不妨设 $r_1>l_1$，

则有

$$p_1^{r_1-l_1}=q_2^{l_2}\cdots q_t^{l_t}.$$

再根据定理 1.1.9，一定有某一 $q_j(2\leqslant j\leqslant t)$，使 $p_1=q_j$，这与 q_1，q_2，…，q_t 互不相同矛盾，所以 $r_1=l_1$，此时有

$$1=q_2^{l_2}\cdots q_t^{l_t}.$$

如果 $t>1$，显然是矛盾的. 所以 $s=1=t$.

现在假设（4）式中质数个数为 $s-1$ 时惟一性成立.

由（4）和（4′）式有

$$n=p_1^{r_1}\cdots p_s^{r_s}=q_1^{l_1}\cdots q_t^{l_t},$$

根据定理 1.1.9. p_1 整除某个 $q_i(1\leqslant i\leqslant t)$，不妨设 $p_1\mid q_1$，但 q_1 是质数，得 $p_1=q_1$. 如果 $r_1\neq l_1$，不妨设 $r_1>l_1$，则有

$$p_1^{r_1-l_1}p_2^{r_2}\cdots p_s^{r_s}=q_2^{l_2}\cdots q_t^{l_t},$$

因此必然还有某个 $q_i(2\leqslant i\leqslant t)$，使 $p_1=q_i$，这与 $q_1\neq q_i$ 矛盾.
所以有 $r_1=l_1$. 从而可得

$$p_2^{r_2}\cdots p_s^{r_s}=q_2^{l_2}\cdots q_t^{l_t},$$

由归纳假设，有

$$s-1=t-1,\ s=t,\ r_i=l_i.\ (i=2,\ 3,\ \cdots,\ s)$$

说明分解式（4）式是惟一的.

由于任意两个整数的加、减、乘的结果还是整数. 这说明在整数集 **Z** 中可以进行加、减、乘运算. 其结果还在 **Z** 中. 这种特性我们称为 **Z** 关于加、减、乘三种运算封闭. 一般地，我们有

定义 5　设 S 是一个非空的数集，如果 S 关于数的加、减、乘三种运算封闭，则称 S 为一个数环.

显然，**Z**、**Q**、**R**、**C** 均是数环，但是 **N** 不是数环. 通常称 **Z** 为整数环.

例 1　由数字 0 组成的单元素集 $S=\{0\}$是一个数环.

例 2　设 m 是正整数，则集合

$$S=\{km\mid k\in\mathbf{Z}\}$$

是一个数环.

显而易见，**Z** 关于除法是不封闭的，但是 **Q**、**R**、**C** 关于除法均封闭. 一般地，我们有

定义 6 设 F 是一个含有非零元素的数环，如果 F 关于数的除法运算（除数不为 0）封闭，则称 F 为一个数域.

显然数域是特殊的数环. 数环 **Q**、**R**、**C** 均是数域，分别称为有理数域、实数域、复数域，而 **Z** 只是数环，不是数域.

例 3 设 $F=\{a+b\sqrt{5} \mid a、b\in\mathbf{Q}\}$，则 F 是一个数域.

证明：F 显然是一个数环.

设 $\alpha=a+b\sqrt{5}$，$\beta=c+d\sqrt{5}\in F$，且 $\beta\neq 0$，则有

$$\frac{\alpha}{\beta}=\frac{ac-5bd}{c^2-5d^2}+\frac{bc-ad}{c^2-5d^2}\sqrt{5}.$$

由于 $\beta\neq 0$，所以 c、d 不同时为零. 得 $c^2-5d^2\neq 0$. 从而

$$\frac{ac-5bd}{c^2-5d^2}\in\mathbf{Q},\ \frac{bc-ad}{c^2-5d^2}\in\mathbf{Q},$$

即 $\frac{\alpha}{\beta}\in F$，得 F 是数域.

设 F 是任意的数域，$0\neq a\in F$，由定义 6，$a-a=0\in F$，$\frac{a}{a}=1\in F$，$1+1=2\in F$，$1+2=3\in F\cdots$得所有正整数 $m\in\boldsymbol{F}$，又由于 $0-m=-m\in F$，得 $\mathbf{Z}\subseteq F$. 因为任意一个有理数都可以写成两个整数的商，所以有 $\mathbf{Q}\subseteq F$. 由此有

定理 1.1.11 任何数域都包含有理数域.

因此我们可以认为有理数域是所有数域之中的最小者.

习　题

1. 求 9405 与 5313 的最大公因数.

2. 设 a_1，a_2，…，$a_n\in\mathbf{Z}$，证明：$(a_1,a_2,\cdots,a_n)=((a_1,a_2,\cdots,a_{n-1}),a_n)$.