高等代数

张贤科 许甫华 编著

清华大学出版社

高等代数学

张贤科　许甫华　编著

清华大学出版社

(京)新登字 158 号

内 容 提 要

本书主要内容为线性代数，包括数与多项式，行列式，线性方程组，矩阵，线性空间，二次型，线性变换，空间分解，矩阵相似，欧空间和酉空间，双线性型，张量积与外积等。内容较深厚，便于打下优势基础；观点较新，便于适应现代数学。还有若干较深选读内容。可作为高校数学专业或计算机等专业的教材或供其它专业参阅。本书成书于作者长期在中国科学技术大学和清华大学讲授此课及从事代数学方面的研究工作，编写时参阅了国外若干著名教材。书中配有难易不等的丰富例题与习题，书后有答案与提示，附录，中英文名词索引，及参考书目。

图书在版编目(CIP)数据

高等代数学/张贤科，许甫华编著. —北京：清华大学出版社，1997
ISBN 7-302-02740-4

Ⅰ. 高… Ⅱ. ① 张… ② 许… Ⅲ. 高等代数 Ⅳ. 015

中国版本图书馆 CIP 数据核字(97)第 24847 号

出版者：清华大学出版社（北京清华大学校内，邮编 100084）
因特网地址：www. tup. tsinghua. edu. cn
印刷者：清华园胶印厂
发行者：新华书店总店北京科技发行所
开　本：787×1092 1/16　印张：23.25　字数：550 千字
版　次：1998 年 3 月第 1 版　1998 年 3 月第 1 次印刷
书　号：ISBN 7-302-02740-4/O・188
印　数：0001～4000
定　价：21.00 元

引　言

本书内容的主体也称为线性代数学，含数与多项式、线性代数常有内容，以及酉空间，张量积和外积等. 并配有大量例题、习题，及答案与提示. 书后有附录，中英文名词索引等. 本书内容较深厚，基础训练有所加强，以便使各专业的学习者都能在此重要课程中，为将来的发展打下牢固的根基. 书中也包含了一些进一步的内容，采用了较新的理论观点，以便于学习者日后适应现代科学的发展和应用. 此外，不少章节尽量独立，较难部分标以 * 号，便于使用时对内容作各种配置取舍，以适应不同的教学环境需要（如两学期或一学期），也便于参考.

作者较长期地在中国科学技术大学和清华大学讲授高等代数和从事代数学方面的研究工作，这是本书的基础. 以本书初稿印刷的讲义已在清华大学数学系，计算机系本科生教学中使用多次，也已在全校性实验班，辅修学位班等多次使用. 此次又作了系统的修改和补充. 在教学和编写本书过程中，参阅了国外一些著名大学新近的教材和研究生教材，及国内一些主要教材，并试图体现作者在多年学习、教学和研究工作中的一些感悟. 叙述上，力求由浅入深，简洁明确. 全书强调了基础训练和基本概念. 一方面，坐标和矩阵方法使用较多，因为有简洁直接性，可算性，也有助于对以后抽象概念的理解领悟. 另一方面，对于映射和变换等概念和方法，也有较充分论述，这是进一步学习和阅读现代文献的基础. 编写时，为了适应理论和应用两方面的新需求，采用了较新的理论角度，也写进了一些一般书中不常有的内容，一些地方试探了新的，可能更自然的发展脉路和证法. 例如全书以一般域为基域（特别可为有限域），而不只限于（实）数域. 这对以后的理论学习很有好处，而且对于越来越重要的计算机和通信应用十分必要. 又如新增“线性表示介绍”一节作为选读内容，不仅本身非常有趣味，而且是一门十分重要的现代数学分支的萌芽. 再如，书中少量使用了群、环等名词术语，有助于对内容提纲挈领地理解把握. 极力避免这些名词是不明智的，国外许多文献已经在大量使用，开始使用这些名词并不难，在不断的使用中其含义就逐渐具体明晰了. 还比如，对偶空间一节有对偶性，将来会遇到许多抽象的对偶性，例如阿贝尔群与其特征群的对偶，Galois 理论等. 而现在的对偶有直观的几何意义（正交补），较容易懂. 书中还定会有许多不足或错误之处，特别是有些处理上不太一般的地方，恳请读者和教师提出批评指正.

本书主要是为高等院校数学专业、计算机专业或信息等专业而编写的教材（周四学时两学期，另伴以习题课），讲授时，可略去部分内容（尤其是带 * 号部分）供将来参考. 对大学一年级学生可将较难的第 1 章放在第 6 章之后讲解或略去. 第 7 章中，1～6 节和 7～9 节是两种证明路线，可以只取其中一种，第二种较易接受且实用. 本书也可以作为其它专业学生的教材（只讲一学期），可只讲第 2～6 章及二次型（即第 8 章前 4 节），或再对某些内容作些介绍（如若当标准形和欧几里得空间）. 本书还可作为师范院校等的研究生教材.

也可供数学工作者，科技工作人员，教师，研究生等参考. 事实上，在作者主持的一个讨论班上(椭圆曲线的数论)，常引用本书作参考(例如一族自伴变换的同时对角化和公共特征向量，不变因子，对偶等). 作者也遇到过一些非数学工作者询问外积(Grassmann 代数)，张量，及空间分解等本书可以解决的不少问题.

书中各章内容特点简述如下. 第 1 章 3～6 节讲述多项式(及整数)的唯一因子分解，以后是根与重根，整系数多项式的分解，和对称多项式. 本章还介绍了群和环的定义(可以先只作为名词使用). 选学内容有整数的同余，以及因子分解定理的推广. 本章内容不仅是代数的，也是整个数学的重要基础. 对实用也很重要.

第 2 章是行列式的丰富内容，也引入了矩阵及其简单运算.

第 3 章以线性方程组为线索，引入了矩阵的秩、行向量空间等线性代数最基础的内容.

第 4 章是矩阵方法的基础.

第 5～6 章是常规必学内容.

第 7 章，7.1～7.6 节和 7.7～7.9 节是两种路线，理论上都有重要前景，数学专业学生应都掌握(难点在 7.5 节). 非数学专业学生可只学后一种，便于计算应用.

第 8 章前 4 节很浅易，8.5～8.7 节是本书在第 7 章之后的第二个较难部分.

第 11 章 11.1 节是简介，其余各节对张量及外积的各方面论述甚详.

各章习题有基本的和较难的两种. 一般教学掌握基本习题和正文即可. 书末有答案与提示，但我们建议读者不要轻易去看. 因为无论在学习上，还是在心理上，独立攻克一个难题会受益良多.

初学代数学的人有的感到不能很快适应，会提出为何与别的学科感觉不同，有何用途等问题. 从数学结构来说，代数、分析、几何是数学的三要素，它们相互渗透化合，生发出数学的绚烂篇章. 如代数数论、代数几何、模形式(自守函数)、算术代数几何、代数 K-理论、同调代数、代数拓扑、泛函分析、范畴、格论、拓扑代数、Lie 群与 Lie 代数，等等，都是代数学起重要作用的充满生机的现代数学分支. 尤其近期以来，代数学在数学的现代发展中作用特别突出. 随着电子计算机和信息通信的革命性大潮，代数学(离散数学)的应用发展惊人.

代数学的历史当然可以追溯到人文之初. 它的西文名称(Algebra)源于阿拉伯数学和天文学家花拉子米(Alkwarizmi)公元 820 年的书名《Al gebr w'al muquabala》(移项与并项). 在中国 1835 年由李善兰译为代数学. 但从数学发展史意义上可以说，代数学的本意就是“用符号代替(未知)数”并参加运算得出解答，这源于印度. 后来发展到“用符号代替一般表达式”(法国 F. Viete，1540—1603). 现在可以说，代数学就是“用符号代替各种事物(称为元素)并研究其间关系”的学问，也就成为研究各种代数系统(即元素间有一定运算关系的集合，如群，环，域，线性空间，及各种推广)的一个数学分支. 这些代数系统是现实世界无数真实对象的高度抽象概括(符号“代替”).

代数学的这一高度抽象概括的特性，不同于其它数学学科. 这也是有些初学者感到不具体直观的原因. 从这种意义上说，高等代数正是代数学的大门和基础. 高等代数学的对象，如线性方程组、矩阵、多项式，还是比较具体的. 再如线性空间、内积、变换等与中学立

体几何中的空间、内积、旋转等也很相近. 人类的认识总是要经过具体——抽象——具体(思维中的具体)的过程. 只要不断努力,量变引发质变,抽象的理论是完全可以被掌握的. 在登山的征途上,没有平坦的大道可走,只有那在陡峭的山路攀登上能体味欢乐的人,有希望到达光辉的顶点. 只有山路的陡长,才有顶峰的辉煌. "会当凌绝顶,一览众山小". 愿以七绝逍遥游一首,赠给有志奋斗的青年:鲲鹏怒化垂天翼,海运扶摇九万击. 野马息吹搏视下,苍苍正色上至极.

编写过程中参阅了许多国内外文献(见参考文献),在此深表感谢.

林小雁同志在教学中多次使用本教材,给出许多习题的答案与提示. 深表感谢.

北京大学赵春来教授给本书提出了宝贵的意见,第 11 章就是听取他的意见增加的. 深表感谢. 作者也对中国科大和清华大学同仁们的热情支持深表感谢.

清华大学教务处和清华大学出版社对本书的出版给予了大力支持,在此一并深表感谢.

最后,愿借此机会对 30 多年前大学的代数老师曾肯成教授致谢. 曾先生毕业于清华大学,工作于中国科大,以学问和师德闻名. 现将先生 66 岁时,作者书赠的七言一首录此以致作者的深深谢意:曾吟水木清华园,肯为英材倾玉泉. 成就文宣千代业,师法至圣一大贤.

作　者

1997 年 2 月于清华园

目　录

第1章

数与多项式

1.1 数的进化与代数系统

自然数 1,2,3,…的发现史可能与人类史同样古老. 自然数全体记为 **N**,其中有加法和乘法两种运算,但对二者的逆运算减法和除法均不封闭. 人类在实践中逐渐接受了零和负数为"数",于是由自然数发展出**整数**(即正负自然数和零). 整数全体记为 **Z**(源于德文 Zahl),对加法及其逆运算封闭. 人类又接受分数为数,发展出**有理数**. 全体有理数记为 **Q**(源于 quotient),对加法和乘法及它们的逆运算均封闭(0 不作除数). 在很长时期内,人们认为有理数就是世上仅可能有的数了,在实用中似乎也足够了. 后来为了极限的完备性(即 Cauchy 序列均有极限存在;直观上表现为任意线段都能有数表其长),人类终于承认无限不循环小数也是数,于是发展出**实数**. 实数全体记为 **R**(源于 real),对极限是完备的,对加、乘法及它们的逆运算也都是封闭的. 很久以后为了解代数方程的需要,例如解方程 $x^2+1=0$,人类终于承认 $\sqrt{-1}$ 等虚数为数,由此发展出**复数**. 复数全体记为 **C**(源于 complex),任意(复系数)代数方程在 **C** 中均有解(见图 1.1).

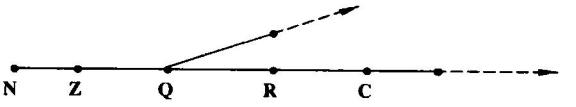

图 1.1

由此可见,数的概念随人类的进步是不断进化的. 人们后来又发展出其它许多"数". 而且,更重要的是,人们由这些数的发展得到启示,概括抽象出群、环、域等概念,使数学进入了新天地.

为了使用清楚方便,以下我们给出群、环、域的定义和术语,这对阅读本书已足够. 尽早熟悉这些定义和术语,对学习和应用近代数学甚有益处.

定义 1.1 一个**群**(group)即是一个非空集合 G,在其中定义了一个二元运算 $*$(即对 G 中任意元素 a,b,有 G 中唯一元素(记为 $a*b$)与之对应),且满足如下规律:

(1) **封闭性**:对任意 $a,b\in G$,总有 $a*b\in G$;

(2) **结合律**:$a*(b*c)=(a*b)*c$ (对任意 $a,b,c\in G$);

(3) **恒元**:存在 $e\in G$,使 $e*a=a$ 对所有 $a\in G$ 成立;

(4) **逆元**:对任意 $a\in G$,总存在 $b\in G$,使 $b*a=e$.

上述群常记为 $(G,*)$ 或 G,(4)中的 b 称为 a 的**逆**,记为 a^{-1},e 称为**恒元**,也称为**单位元**. 有时也称运算 $*$ 为"乘法",事实上它可以是满足上述四个条件的任意二元运算,并不

一定是普通数学的乘法意义. 此外注意,上述定义中的恒元和逆元都是乘在左边的,但可以证明乘在右边也具有同样的性质,也就是说,对任意 $a\in E$,有

$a*a^{-1}=e$ 及 $a*e=a$

事实上,由 $a^{-1}=e*a^{-1}=(a^{-1}*a)*a^{-1}=a^{-1}*(a*a^{-1})$,两边在左方均再乘以 $(a^{-1})^{-1}$即得 $e=a*a^{-1}$. 又显然有 $a*e=a*(a^{-1}*a)=(a*a^{-1})*a=e*a$.

如果群$(G,*)$还满足**交换律**,即 $a*b=b*a$ 对任意 $a,b\in G$ 成立,则该群称为**Abel群**或**交换群**. Abel 群的运算经常记为加法(用+代替 * 作为运算符),恒元常记为 0 称为**零元**. a 的逆元常记为 $-a$ 称为 a 的**负元**.

例 1.1 $(\mathbf{Z},+),(\mathbf{Q},+),(\mathbf{R},+),(\mathbf{C},+)$均为 Abel 群,这里加法(+)均指普通数的加法.

定义 1.2 一个**环**(ring)是一个集合 R,其中定义了两个二元运算,分别记为加法(−)和乘法(·),且满足:

(1) $(R,+)$是 Abel 群;

(2) $(R,\cdot)$是半群,即满足封闭性和结合律;

(3) **分配律** $a\cdot(b+c)=a\cdot b+a\cdot c$, $(a+b)\cdot c=a\cdot c+b\cdot c$

对任意 $a,b,c\in R$ 成立.

上述环记为$(R,+,\cdot)$或 R,乘号 · 常省去而记 $a\cdot b$ 为 ab,加法零元常记为 0. 注意 $0\cdot a=a\cdot 0=0$ 对任意 $a\in R$ 成立,事实上, $0a=(0+0)a=0a+0a$, 即得 $0a=0$.

如果环 R 对乘法有恒元 e,则称 R 为**含幺环**. 在含幺环 R 中,对 $c\in R$,若存在 $x\in R$ 使得 $xc=cx=e$,则称 x 为 c 的**逆**元,称 c 是**可逆的**(或称 c 为 R 的**单位**). 如果一个环 R 中乘法满足交换律,则称 R 为**交换环**.

定义 1.3 一个**域**(field)即是一个环$(F,+,\cdot)$,且要求 F 的非 0 元全体 F^* 对乘法是 Abel 群. 详言之,域即是有两个二元运算(+)和(·)的集合 F,且满足

(1) $(F,+)$是 Abel 群;

(2) $(F^*,\cdot)$是 Abel 群;

(3) 分配律.

例 1.2 $(\mathbf{Z},+,\cdot)$是环,称为**整数环**,这是很重要的一个环(这里运算是普通加法和乘法).

例 1.3 $\mathbf{Q},\mathbf{R},\mathbf{C}$ 对通常加法和乘法均是域,分别称为**有理数域**,**实数域**,和**复数域**. 这是常用到的也是最重要的域.

例 1.4 $\mathbf{Q}(\sqrt{5})=\{a+b\sqrt{5}\mid a,b\in\mathbf{Q}\}$是域.

若域 F 的子集合 K 对于 F 中的原运算仍是一个域,则称 K 是 F 的**子域**,F 是 K 的**扩域**. 类似有**子群**、**子环**的定义.

复数域 $\mathbf{C}$ 的子域被称作**数域**,上述三例中的域均是数域. 数域有很多(无穷多个),是重要的域. 注意任一数域中总含有自然数 1,从而含有 $\mathbf{Z}$,从而含有 $\mathbf{Q}$. 故有理数域 $\mathbf{Q}$ 是最小的数域,是任一数域的子域. 数域以外的域也有很多(无穷多个),且很重要. 下例即是信息编码中很重要的"**二元域**":

例 1.5 $F_2=\{\bar{0},\bar{1}\}$对于如下定义的加法和乘法是域: $\bar{0}+\bar{0}=\bar{0}$, $\bar{0}+\bar{1}=\bar{1}+\bar{0}=\bar{1}$,

$\bar{1}+\bar{1}=\bar{0}$, $\bar{0}\cdot\bar{0}=\bar{0}$, $\bar{0}\cdot\bar{1}=\bar{1}\cdot\bar{0}=0$, $\bar{1}\cdot\bar{1}=\bar{1}$.

今后常以 0 和 1 分别记一个域 F 中的加法和乘法单位元. 高等代数学中要经常以一个域 F 为基础，研究 F 上的函数、多项式、向量等. 比较早期的初等教程中常设基础域 F 为实数域 **R**. 本书的大部分论述是在一般的基础域 F 上展开，以适应数学进一步发展的理论需要和计算机信息通信等多方面的实际应用需求. 对一般的域 F，我们常常把其中的元素称为数(虽然并不一定是复数或实数)，这是相对于 F 上的多项式和向量等而言的.

*1.2 整数的同余与同余类

整数环 **Z** 的一个重要性质是可进行带余除法，即若 $m,n\in\mathbf{Z}$ 且 $m\neq 0$，则必存在 $q,r\in\mathbf{Z}$ 使得

$$n=mq+r,\qquad \text{且}\ 0\leqslant r<|m|;$$

这里 q 称为 n 除以 m 的**商**，r 称为**余数**. 若 $r=0$，则称 m **整除** n，记为 $m|n$. 由 **Z** 的带余除法性质可导出 **Z** 的许多其它性质，例如算术基本定理(即任一整数可唯一分解为素数之积，将在 1.6 节中证明，本节利用此性质讨论整数的同余).

若整数 a 与 b 除以 m 的余数相同，则称 a 与 b 对模 m **同余**(congruent modulo m)，记为

$$a\equiv b\ (\mathrm{mod}\ m),$$

这恰相当于 $m|a-b$，也恰相当于 $a=b+mk$ 对某 $k\in\mathbf{Z}$ 成立. 符号"$\equiv$"称为**同余号**，读为"同余于"，上面的表达式称为**同余式**(congruence). 同余与相等有如下类似性质(对任意 $a,b,c,d\in\mathbf{Z}$)：

1. (**传递性**) 若 $a\equiv b\ (\mathrm{mod}\ m)$，$b\equiv c\ (\mathrm{mod}\ m)$，则 $a\equiv c\ (\mathrm{mod}\ m)$.
2. (**对称性**) 若 $a\equiv b\ (\mathrm{mod}\ m)$，则 $b\equiv a\ (\mathrm{mod}\ m)$.
3. (**反身性**) 总有 $a\equiv a\ (\mathrm{mod}\ m)$.
4. (**同余式相加**) 若 $a\equiv b\ (\mathrm{mod}\ m)$，$c\equiv d\ (\mathrm{mod}\ m)$，则 $a+c\equiv b+d\ (\mathrm{mod}\ m)$.
5. (**同余式相乘**) 若 $a\equiv b\ (\mathrm{mod}\ m)$，$c\equiv d\ (\mathrm{mod}\ m)$，则 $ac\equiv bd\ (\mathrm{mod}\ m)$.
6. (**同余式约化**) (1) 若 $a\equiv b\ (\mathrm{mod}\ m)$，且 $d|a$，$d|b$，d 与 m 互素则

$$\frac{a}{d}\equiv\frac{b}{d}\ (\mathrm{mod}\ m).$$

(2) 若 $a\equiv b\ (\mathrm{mod}\ m)$且 d 为 a,b,m 的公因子，则

$$a/d\equiv b/d\ (\mathrm{mod}\ m/d).$$

同余概念首先由高斯(Gauss)引入，有重要的意义. 模数 m 通常取为正整数.

例 1.6(弃九法)　记正整数 a 的十进位表示的各位数字之和除以 9 的余数为 $\bar{a}$. 例如 $\overline{72982}=1$. 则"弃九法"断言，若 $a\times b=c$ 则 $\overline{\bar{a}\times\bar{b}}=\bar{c}$；若 $a+b=c$ 则 $\overline{\bar{a}+\bar{b}}=\bar{c}$. 这可用来初检运算的正确性. 例如对 $72982^2=5326372334$，因右方弃九后为 2，可知等式有误. 为了证明弃九法，只需注意 $10\equiv 1(\mathrm{mod}\ 9)$，故若 a 的十进位表示为 $a=a_n10^n+\cdots+a_110+a_0$，则 $a\equiv a_n+\cdots+a_1+a_0\equiv\bar{a}\ (\mathrm{mod}\ 9)$. 故若 $ab=c$，则应有 $\overline{\bar{a}\bar{b}}\equiv\bar{c}(\mathrm{mod}\ 9)$，此即弃九法.

练习 1　(用 9 整除判则)9 整除整数 a，当且仅当 9 整除 a 的数字和.

练习 2 找出用 3,5,4,8,7,11 等整除的判则，并证明之.

记集合 $m\mathbf{Z}=\{mk\mid k\in\mathbf{Z}\}$，整数全体可以分成 m 个类：$l+m\mathbf{Z}=\{l+mk\mid k\in\mathbf{Z}\}(l=0,1,\cdots,m-1)$，即

$$\mathbf{Z}=m\mathbf{Z}\cup(1+m\mathbf{Z})\cup\cdots\cup(m-1+m\mathbf{Z})$$

每一个类 $l+m\mathbf{Z}$ 中的数对模 m 均同余于 l，称为一个**同余类**，我们记

$$\bar{l}=l+m\mathbf{Z}=\{l+mk\mid k\in\mathbf{Z}\}.$$

定理 1.1 *整数对模 m 的 m 个同余类构成的集合记为*

$$\mathbf{Z}/m\mathbf{Z}=\{l+m\mathbf{Z}\mid l=0,1,\cdots,m-1\}=\{\bar{0},\bar{1},\cdots,\overline{m-1}\},$$

它对如下定义的加法和乘法是一个交换环：

$$\bar{l}_1+\bar{l}_2=\overline{l_1+l_2}\qquad(\text{或即}(l_1+m\mathbf{Z})+(l_2+m\mathbf{Z})=l_1+l_2+\mathbf{Z}m)$$

$$\bar{l}_1\cdot\bar{l}_2=\overline{l_1l_2}\qquad(\text{或即}(l_1+m\mathbf{Z})\cdot(l_2+m\mathbf{Z})=l_1l_2+\mathbf{Z}m)$$

证明 首先验证运算定义的合理性，若取 $l_1'\in\bar{l}_1$，$l_2'\in\bar{l}_2$，则 $l_1'=l_1+k_1m$，$l_2'=l_2+k_2m$ $(k_1,k_2\in\mathbf{Z})$，于是 $l_1'+l_2'=l_1+l_2+m(k_1+k_2)$ 与 l_1+l_2 同在一类. $l_1'l_2'=l_1l_2+l_1k_2m+l_2k_1m+k_1k_2m^2$ 也与 l_1l_2 同余. 这就证明了运算结果不依赖于代表元的选取(一个同余类 $l+m\mathbf{Z}$ 中的任一元 l' 都称为该类的代表元，此类也可写为 $l'+m\mathbf{Z}$)，其余关于环的条件容易验证. ■

例 1.7 $\mathbf{Z}/2\mathbf{Z}=\{\bar{0},\bar{1}\}$ 不仅是交换环，而且是域(即上节的二元域). 可以验证 $\mathbf{Z}/7\mathbf{Z}$ 也是域. 而 $\mathbf{Z}/8\mathbf{Z}$ 不是域，例如 $\bar{2}$ 不可逆，否则若 $\overline{2x}=\bar{1}$ 乘以 $\bar{4}$，知 $\bar{4}\cdot\overline{2x}=\bar{4}$，即得 $\bar{0}=\bar{4}$，矛盾. 有趣的是 $\mathbf{Z}/8\mathbf{Z}$ 中的可逆元全体

$$(\mathbf{Z}/8\mathbf{Z})^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$$

是一个乘法群，且 $\bar{3}\cdot\bar{3}=\bar{1}$，$\bar{3}\cdot\bar{7}=\bar{5}$，等等.

定理 1.2 *(1) 当 $m=p$ 为素数时，$\mathbf{Z}/p\mathbf{Z}=\mathbf{F}_p$ 是域.*

(2) 当 m 不是素数时，$\mathbf{Z}/m\mathbf{Z}$ 不是域. 此时 $\bar{l}$ 可逆，当且仅当 l 与 m 互素.

证明 首先设 m 不是素数，l 与 m 不互素，设 $d>1$ 为 l 与 m 的公因子，于是

$$\bar{l}\overline{\left(\frac{m}{d}\right)}=\overline{\left(\frac{l}{d}\right)}\bar{m}=\bar{0},$$

故 $\bar{l}$ 是零因子（若 a,b 均非 0 而 $ab=0$，则称 a 和 b 为**零因子**). 此时 $\bar{l}$ 必不可逆，否则，由 $\overline{lk}=\bar{0}$ 两边同乘以 $\bar{l}$ 的逆，则得 $\bar{k}=\bar{0}$，矛盾. 定理的其余部分依赖于下述引理，其证明将在不久给出. ■

引理 1.1 若整数 l 与 m 互素，则存在 $s,t\in\mathbf{Z}$ 使得

$$sl+tm=1.$$

由此引理可知，$\bar{1}=\overline{sl+tm}=\overline{sl}+\overline{tm}=\overline{sl}$，即 $\bar{l}$ 可逆. 当 m 为素数时，小于 m 的正整数均与 m 互素，故 $\mathbf{Z}/m\mathbf{Z}$ 的非 0 元均可逆，故 $\mathbf{Z}/m\mathbf{Z}$ 是域. ■

因此对每个素数 p 均有一个域

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\},$$

称为 **p 元(有限)域**. 这是一种很重要的域. 与数域不同的是,对 $\mathbf{F}_p$ 中任一元 $\bar{a}$,自身相加 p 次(或称 p 倍)总为 0 元: $\bar{a}+\cdots+\bar{a}=\overline{pa}=\overline{pa}=\bar{0}$. 这样的域称为**特征是 p 的域**.

定理 1.3 (Fermat) *$\mathbf{F}_p$ 的元素 x 均满足*

$$x^p = x.$$

证明 当 $x=\bar{1}$ 时命题显然. 现设 $x=\bar{l}$ 时命题成立,则

$$(l+1)^p = l^p + pl^{p-1} + \cdots + \frac{p(p-1)\cdots(p-k+1)}{k!}l^{p-k} + \cdots + pl + 1,$$

注意当 $k\neq 1$ 和 p 时,$p \mid C_p^k$(因为分子中的 p 不可能被分母约去),故

$$(l+1)^p \equiv p^p + 1 \pmod{p}, \text{即} (\overline{l+1})^p = \bar{l}^p + \bar{1} = \bar{l} + \bar{1} = \overline{l+1}.$$

■

同余式 $a \equiv b \pmod{m}$ 与环 $\mathbf{Z}/m\mathbf{Z}$ 中的等式 $\bar{a}=\bar{b}$ 是同一事实的两种表述方法. 因此定理 1.3 也可表述为

$$a^p \equiv a \pmod{p}$$

对任意 $a \in \mathbf{Z}$ 成立. 当 $p \mid a$ 时,此式显然. 当 $p \nmid a$ 时, a 与 p 互素,两边同乘 $x=\bar{a}$ 的逆,即知定理 1.3 相当于

$$a^{p-1} \equiv 1 \pmod{p}.$$

1.3 多项式形式环

定义 1.4 (1) 设 F 为域(乘法单位元记为 1),X 为不属于 F 的任一个符号. 则形如

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \qquad (a_i \in F(i=0,\cdots,n),\ 0 \leqslant n \in \mathbf{Z},\ a_n \neq 0)$$

的表达式称为域 F 上 X 的一个**多项式形式**(polynomial form in X over **F**). 整数 n 称为其次数, a_i 称为其 i 次系数, a_iX^i 称为其 i 次项.

(2) 两个多项式形式相等规定为二者的次数和各同次系数均相等. 系数为 0 的项可以不写出,因此每个多项式形式也可以写为

$$a_0 + a_1X + a_2X^2 + \cdots$$

或

$$\sum_{i=0}^{\infty} a_iX^i,$$

其中只有有限个系数 a_i 非 0. 多项式形式也常称为**多项式**.

由上述定义可知,字母 X 只是一个符号,它与域 F 中元素的积与和都是形式的. 故 X 称为**不定元**(indeterminate).

注记 1 字母 X 的意义在数学中是不断进化的. 在初等代数中,X 作为"未知数"被首先引入,这时它虽是待求的,但其实是一个很具体的数. 后来在函数中,X 表示变量,但取值范围还是较确定的(如在实轴上). 在上述定义 1.4 中,X 已不被附加任何限定,成为不定元.

多项式形式 f 的次数(*degree*)记为 $\deg f$，域 F 的零元 0 也视为多项式，常设 $\deg 0=-\infty$. 多项式形式 f 的最高次非 0 项称为**首项**(leading term). 若首项系数为 1，则称为首一多项式. 多项式形式 f 也记为 $f(X)$，以指明不定元是 X.

定理 1.4 *域 F 上 X 的多项式形式全体 $F[X]$按如下运算成为交换环(称为多项式形式环)；*

$$\sum_{i=0}^{\infty}a_iX^i+\sum_{i=0}^{\infty}b_iX^i=\sum_{i=0}^{\infty}(a_i+b_i)X^i,$$

$$\Big(\sum_{i=0}^{\infty}a_iX^i\Big)\Big(\sum_{i=0}^{\infty}b_iX^i\Big)=\sum_{k=0}^{\infty}\Big(\sum_{i+j=k}a_ib_j\Big)X^k.$$

证明 按定义要验证以下各项：(1) $F[X]$对加法是 Abel 群，即满足封闭性，结合律，有零元，有负元，有交换律. (2) $F[X]$对乘法是交换半群，即满足封闭性，结合律，交换律，(3) 乘法对加法满足分配律. 这些都易验证，例如乘法结合律的验证

$$\Big(\Big(\sum a_iX^i\Big)\Big(\sum b_jX^j\Big)\Big)\Big(\sum c_kX^k\Big)$$

$$=\Big(\sum_{s=0}^{\infty}\Big(\sum_{i+j=s}a_ib_j\Big)X^s\Big)\Big(\sum c_kX^k\Big)$$

$$=\sum_{m=0}^{\infty}\Big(\sum_{s+k=m}\Big(\sum_{i+j=s}a_ib_j\Big)c_k\Big)X^m$$

$$=\sum_{m=0}^{\infty}\Big(\sum_{i+j+k=m}a_ib_jc_k\Big)X^m.$$

注意最后一个式子中 i,j,k 地位平等，故同理可知

$$\Big(\sum a_iX^i\Big)\Big(\Big(\sum b_jX^j\Big)\Big(\sum c_kX^k\Big)\Big)$$

也等于上式. 结合律得证. ■

对于多项式形式 f,g，注意 fg 的首项恰为 f 与 g 的首项之积. 所以总有

$$\deg(fg)=\deg(f)+\deg(g).$$

系 多项式形式环 $F[X]$中**消去律**成立，即若 $fg=fh$ 且 $f\neq 0$，则 $g=h$ (对任意 $f,g,h\in F[X]$).

证明 由 $f(g-h)=0$，故其首项为 0. 其首项是 f 的首项与 $g-h$ 的首项之积，而 f 的首项非 0，故 $g-h$ 的首项为 0，即 $g-h=0$. ■

有消去律的含幺交换环称为**整环**或**整区**(domain). 故 $\mathbf{Z}$ 和 $F[X]$均为整环. 注意 $F[X]$中的可逆元集为 F^*(即 F 中的非 0 元). F 中的元素也称为常数或数值.

正像由整环 $\mathbf{Z}$ 发展出有理数域 $\mathbf{Q}$ 一样，也可由整环 $F[X]$发展出一个域. 对任意 $f(X),g(X)\in F[X]$，$g(X)\neq 0$，称如下的表达式为一个**有理式形式**：

$$\frac{f(X)}{g(X)}.$$

两有理式形式 $\frac{f(X)}{g(X)}$ 与 $\frac{f_1(X)}{g_1(X)}$ 相等，定义为 $f(X)g_1(X)=f_1(X)g(X)$ (作为多项式形式相等). 又定义二者的和及积为

$$\frac{f(X)}{g(X)}+\frac{f_1(X)}{g_1(X)}=\frac{f(X)g_1(X)+f_1(X)g_1(X)}{g(X)g_1(X)}$$

$$\frac{f(X)}{g(X)}\frac{f_1(X)}{g_1(X)}=\frac{f(X)f_1(X)}{g(X)g_1(X)}$$

定理 1.5 域 F 上有理式形式全体 $F(X)$ 是一个域(称为以 X 为不定元的**有理式形式域**或**有理函数域**).

注记 2 注意多项式形式与多项式函数有本质的不同. 例如多项式形式 X^2 和 X 是不相等的. 但 x^2 与 x 作为定义在二元域 F_2 上的函数却是相等的(因为 F_2 中只有两个元素 0 和 1, 而 x 取 0 或 1 时, 总有 $x^2=x$). 不过以后会看到, 无限域(例如数域)上的多项式函数与多项式形式的区别不是本质的.

注记 3 在定义 1.4 中, 也可以用一个交换环 R 取代域 F, 其余规定均不变. 这样得到的多项式形式全体 $R[X]$ 也是一个交换环. 不过 $R[X]$ 将不具有 $F[X]$ 的许多性质.

注记 4 若 $ab=0$ 而 $a\neq0, b\neq0$, 则称 a 和 b 为**零因子**(zero divisor). 若环 R 中不含零因子, 则称 R 为**无零因子环**. 例如在 $\mathbf{Z}/8\mathbf{Z}$ 中, $\bar{2}\cdot\bar{4}=\bar{0}$, 故 $\bar{2}$ 和 $\bar{4}$ 均为零因子. 域 F 中总是无零因子的. 环 $\mathbf{Z}$ 中无零因子. 容易证明: 环 R 中**无零因子**当且仅当 R 中**消去律**成立. 事实上, 若 R 中有零因子, 比如说 $ab=0$ 而 a 和 b 均非 0, 如果消去律成立, 则由 $ab=a0$ 中消去 a, 得到 $b=0$, 矛盾. 反之, 设 R 中无零因子, 若 $ab=ab_1$ 而 $a\neq0$, 则因 $a(b-b_1)=0$, 故必然 $b-b_1=0$, $b=b_1$.

所以**整环**也可定义为**无零因子的含幺交换环**.

1.4 带余除法与整除性

整环 $\mathbf{Z}$ 和 $F[X]$ 有许多相似之处, 比如二者中均可作带余除法.

定理 1.6(带余除法) 对域 F 上任两多项式形式 $f, g\in F[X]$, 若 $g\neq0$, 则总存在多项式形式 $q, r\in F[X]$ 使

$$f=gq+r,\qquad \deg r<\deg g \text{ 或 } r=0,$$

且 q 和 r 由 f, g 唯一地决定.

证明 先证 q 和 r 的存在性. 若 $\deg f<\deg g$ 则令 $q=0$, $r=f$ 即可. 否则设 $f=a_mX^m+\cdots+a_0$, $g=b_nX^n+\cdots+b_0$, $m\geqslant n$, 且 a_m 与 b_n 非 0. 令

$$q_1=\frac{a_m}{b_n}X^{m-n},$$

则 q_1g 与 f 有相同的首项, 故 $f-q_1g=f_1$ 的次数比 f 低. 再对 f_1 作同样讨论可知, 存在 $q_1,\cdots,q_s$ 使 $f-q_1g-q_2g-\cdots-q_sg=f_s$ 的次数比 g 低. 令 $f_s=r$, $q_1+\cdots+q_s=q$ 即可.

现证唯一性, 设 $f=gq+r=gq_1+r_1$, $\deg r_1<\deg g$ 或 $r_1=0$. 于是 $g(q-q_1)=r_1-r$. 若两边均非 0, 则由