高等学校教材

高等代数基础

（修订第二版）

周伯壎

高等教育出版社

高等学校教材

高等代数基础

（修订第二版）

周伯壎

高等教育出版社

内 容 提 要

本书主要由多项式的理论，矩阵的理论与线性空间的理论等三个部分所组成，又作了张量与外代数以及代数结构等方面的简单介绍．可作为综合大学与高等师范院校数学系高等代数课程的教科书与教学参考书。

高等学校教材

高等代数基础

（修订第二版）

周 伯 壎

高等教育出版社出版

新华书店上海发行所发行

商务印书馆上海印刷厂印装

开本 850×1168 1/32 印张 14 字数 336,000

1966 年 10 月第 1 版

1989 年 10 月第 2 版 1989 年 10 月第 1 次印刷

印数 00,001—1,730

ISBN 7-04-002331-8/O·794

定价 3.20 元

再 版 序

本书是笔者所编高等代数(高等教育出版社, 1964)一书的再版，事实上是在原有的基础上重写的. 一些概念的叙述与一些理论的推导都作了较大的修改，使之更加严格，能较好地起着承上启下与横向连系的作用. 内容上也作了不少的增删，例如，删去了实根的近似值与斯图姆定理，等等，同时又加了矩阵函数与辛空间等方面的理论. 第十一章张量与外代数全章都是新加的. 在《高等代数》的原稿中本拟写上这样一章，但在定稿时抽掉了. 现在看来，这种理论对于数学系的学生以及物理系某些专业的学生来说仍有必要. 本书所述的理论仅是初步的，起点是比较低的(从多重线性函数说起)，方法也是较初等的(未用到理想论与泛性质). 笔者认为，对于不是专攻代数学的学生来说，这里的张量与外代数的理论基本上是够用的，也不是很难接受的.

所有各章节都不分大小字，因为编者不想明确表示哪些是重要的，主要的，哪些是次要的，或不重要的. 任一位大学教师都应该有权决定他的教学大纲，不应局限于一本教科书. 事实上，大学课程的教科书应只是一本教学参考书，至多是一本主要的参考书，教师完全有权取舍其某些章节，或者作额外的补充.

本书将习题解法的建议与提示放在书的末尾，其用意是让读者首先独立思考，以培养其进行科研的能力，实在有困难，再参阅书末的建议与提示. 编者无意肯定所建议的方法是最好的，学生在独立思考以后完全有可能研究出更好的方法. 我们鼓励学生多用这种方式来学习.

本书不论是在取材方面或是在材料的处理方面都肯定尚存在

不少的问题，尚祈学者们指正。

石生明教授对本书的初稿提出了许多中肯有益的意见，笔者特表示衷心感谢。

编　者

1988年元月

目　录

第一章　数环，数域和一元多项式环

多项式是最初等也是最重要的函数之一．本章将在高中代数的基础上讨论一元多项式环的运算，因式，倍式以及其零点等基本理论．由于多项式的性质事实上取决于其系数，所以我们首先将讨论数环与数域等基本概念，由此来讨论数域上的一元多项式环．

§1　数环和数域

我们在处理一个数学问题时，总要用到一些数，而且也往往要对这些数作某些运算．一般说来，并不需要用到所有的复数，而是只需要或只允许使用其中的一部分的数，这些数与问题的本身有关，当然也与所要进行的运算有关．例如，在作自然数的加法时，用不到考虑分数，负数与其它的实数，因为自然数加自然数仍为自然数．在作自然数的减法时，不但需要自然数和0，而且也需要负整数．在解整数系数的一元一次方程时，需要有理数，而在解整系数的一元二次方程时，不但需要有理数，而且还需要某些无理数，甚至还需要一部分的虚数．从这些例子看来，一个代数问题能否解决，往往牵涉到数的范围，在数的小范围内不能解决的问题，可能在较大的范围得到解决．

在作代数问题时，不但要考虑一些数，而且要对于这些数作某一种或某几种运算，因此所考虑的数的集合就必需对所用到的运算是封闭的，就是说，此数集中任两个数作所述运算的结果仍然在这个数集内．数与数之间的运算是多种多样的，但是最基本的运算是加，减，乘，除这四种．我们就这四种基本运算来考虑两种重要

的数集.

我们将采用以下的记号. 如果 a 是集合 A 的一个元素, 就记成 $a\in A$, 读成"a 属于 A"; 如果 a 不是 A 的元素, 就记成 $a\overline{\in}A$, 读成"a 不属于 A". 如果 A 是 B 的子集, 就记成 $A\subseteq B$, 否则记成 $A\nsubseteq B$. 在 $A\subseteq B$ 但 $A\neq B$ 时, 记成 $A\subset B$.

定义 1 假定 R 是一个至少含有一个数的数集. 如果在 $a\in R, b\in R$ 时, $a+b$, $a-b$ 与 ab 也都属于 R, 对称 R 为**一个数环**.

定义 2 假定 F 是一个至少含有两个数的数环. 如果在 $a\in F$, $b\in F$ 但 $b\neq 0$ 时, 商 a/b 也属于 F, 则 F 叫作**一个数域**.

最常见的数环是**整数环**, 它是由 0 及所有的正负整数所组成的. 整数环常以黑体的字母 $\boldsymbol{Z}$ 来表示. 它当然不是一个数域, 因为例如 1/2 就不属于 $\boldsymbol{Z}$.

所有的有理数(0 及正负有理数)组成**有理数域**, 这个域将表以 $\boldsymbol{Q}$. 所有的实数组成**实数域** $\boldsymbol{R}$, 所有的复数将组成**复数域** $\boldsymbol{C}$, 它是最大的数域, 当然也是最大的数环, 任何数域与数环都是 $\boldsymbol{C}$ 的子域(子环)(其元素属于某域(环), 且对于此域(环)的运算也成一域(环)).

容易看到, 任何数环 R 都必包含 0 这个数, 因为当 $a\in R$ 时, $a-a=0$ 必 $\in R$. 由此即得, 若 $a\in R$, 则 $-a=0-a\in R$, 而且对任何自然数 n, a^n 与 $\pm na$ 也都是 R 中的数. 类似地, 任何数域 F 都必然包含 1 这个数, 因为 F 既至少含两个数, 其中必有一个 $a\neq 0$, 因而 $1=\frac{a}{a}\in F$, 于是对任何自然数 n, 也必有 $a^{-n}\in F$. 但数环却不一定包含 1, 例如所有的偶数组成一个数环, 但 1 却不是它的一个元素. 如果 1 是数环 R 中的一个数, 我们常称 1 为 R 的**单位元**.

再举几个例子.

例 1 数 0 这一个数组成一个数环, 因为 $0\pm 0=0, 0\cdot 0=0$. 这

个环是最小的数环，也是唯一的一个只含有一个数的数环．它显然不能是一个域，因为一个域至少要含有两个数．

例 2 以 R 表示所有可表成 $a+b\sqrt{2}$ 形状的数的集合，这里的 a, b 只限定为整数，则 R 是一个有单位元（就是 1）的环，因为

$$(a+b\sqrt{2})\pm(c+d\sqrt{2})=a\pm c+(b\pm d)\sqrt{2},$$

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

这个 R 肯定不能是一个域，因为，例如 $\dfrac{1}{2+\sqrt{2}}=1-\dfrac{1}{2}\sqrt{2}$ 不能属于 R.

例 3 若在例 2 中，让 $a+b\sqrt{2}$ 中的 a 与 b 都可以是有理数，那么，这个数集就组成一个数域，因为在 $a+b\sqrt{2}\neq 0$ 时

$$\frac{1}{a+b\sqrt{2}}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2},$$

这里大家都知道，在 a 与 b 都是有理数时，a^2-2b^2 是不等于 0 的，因此 $\dfrac{1}{a+b\sqrt{2}}$ 也属于这个数集．

例 4 让 p 为一个素数，以 R 表示所有的整数以及分母不以 p 为因数的既约分数的集合，则 R 是一个数环，但不是数域，因为例如 $\dfrac{1}{p}\in R$，但 $p\in R$．这个数环显然是 $\boldsymbol{Q}$ 的子环．

设 R 是一个有单位元 1 的数环，而 $a\in R$．如果 a 的倒数 $\dfrac{1}{a}$ 也属于 R，则 a 叫做 R 中的一个**幺因子**，因为它是单位元 1 的因子，$a\cdot\dfrac{1}{a}=1$．显然，若数环 R 有单位元 1，则它是一个域当且仅当 R 中每一个不等于 0 的数都是幺因子．幺因子也称为环 R 的**可逆元**，又叫**单位**（注意，单位不是单位元，因为只有 1 这个数才是 R 的单位元 $1\cdot a=a$）．± 1 当然都是幺因子（如果 $1\in R$），而整数 $\boldsymbol{Z}$ 中也只有 ± 1 才是幺因子．但是在其它包含 1 的数环中，也可能有除 ± 1 以外的幺因子，例如在例 3 中，$1\pm\sqrt{2}$ 都是幺因子；在

例 4 中，如果整数 a 与 b 都不能被 p 所整除，则 $\frac{a}{b}$ 与 $\frac{b}{a}$ 都是幺因子. 幺因子的理论在代数数论这门学科中占有很重要的地位.

§ 2 整数环的有序性与单一分解性

整数环 $\boldsymbol{Z}$ 是一个我们比较熟悉的数环，它是数论这门学科的主要研究对象之一.

两个非负整数 a 与 b 可以比大小，例如 $3<5$, $22<38$, 等等. 这是自然界中客观事物在数量上的反映. 这种比大小的现象提供了正整数的一种排序方法，小的排在前，大的排在后. 这种排序方法也用于正有理数. 若 a, b, c 与 d 都是正整数，则 $\frac{a}{b}<\frac{c}{d}$ 当且仅当 $ad<bc$. 有理数的这种排序方法就是实数概念的理论基础. 再者，正数的大小也反映到负数，若 $0<a<b$，则必 $-b<-a<0$. 于是全体实数按照大小的顺序变成一个有序的集合：任给两个实数 a 与 b，必有 $a<b$，或 $a=b$，或 $a>b$，三者必居其一，且仅居其一；而且若 $a<b$，$b<c$，则必 $a<c$.

整数环 $\boldsymbol{Z}$ 的这种序有一个特性，就是，当 $a\in\boldsymbol{Z}$ 时，在 a 与 $a+1$ 之间不存在第三个整数，即，不存在 $b\in\boldsymbol{Z}$，使 $a<b<a+1$（有理数的集合没有这个性质，任两个有理数之间都可以插进无穷多个有理数）. 由此即得，若 a, $b\in\boldsymbol{Z}$，且 $b>a$，则在 a 与 b 之间恰有 $b-a-1$ 个整数，它们是 $a+1$, $a+2$, $\cdots$, $a+(b-a-1)$.

若 $a\in\boldsymbol{Z}$，以 $\boldsymbol{Z}^{(a)}$ 表示 $\boldsymbol{Z}$ 中所有不小于 a 的数的集合，即，$x\in\boldsymbol{Z}^{(a)}$ 当且仅当 $x\geqslant a$，则有

$\boldsymbol{Z}^{(a)}$ 的良序原理. 若 B 是 $\boldsymbol{Z}^{(a)}$ 的任一非空子集，$B\subseteq\boldsymbol{Z}^{(a)}$，则 B 中必有一个最小的元素 b，即，$b\in B$，而且在 $x\in B$ 时，必有 $b\leqslant x$.

证 B 既不是空集，必有 $b_1\in B$. 若 b_1 是 B 中的最小的数，

则 b_1 就是所要求的 b. 若 b_1 不是最小的数，那么必有 $b_2 \in B$, $a \leqslant b_2 < b_1$, 若 b_2 是 B 中最小的数，则 b_2 就是所要求的 b. 若 b_2 仍不是最小的，则有 $b_3 \in B$. 由于只有有限个数可供选择，所以最终必能找到最小的 b.

由上述的良序原理可推出下列的数学归纳原理.

数学归纳原理 设 P_n 是一系列的命题，其中 n 属于某一个 $\boldsymbol{Z}^{(a)}$，如果

(1) 于 $n=a$ 时，已证明 P_a 正确；

(2) 对于任何 $m>a$，在已假定 P_a, P_{a+1}, …, P_{m-1} 都正确的条件下，可证出 P_m 也正确；

则 P_n 对于任何 $n \in \boldsymbol{Z}^{(a)}$ 也必正确.

证 用反证法. 假定 P_n 并不是对所有 $n \in \boldsymbol{Z}^{(a)}$ 都正确，因此使 P_n 不正确的 n 组成 $\boldsymbol{Z}^{(a)}$ 的一个非空子集 B. 由良序原理，B 有一个最小的数，设为 b. 这个 b 不能等于 a, 因为由(1)，已知 P_a 正确，即，$a \overline{\in} B$. 由 B 及 b 的定义，a, $a+1$, …, $b-1$ 都不属于 B，因此，在 $a \leqslant m \leqslant b-1$ 时，P_m 正确. 但由(2)，P_b 也必然是正确的，于是 $b \overline{\in} B$. 这就引出了矛盾，所以 B 是空集，即，对所有的 $n \geqslant a$, P_n 都正确.

数学归纳原理又称为**一般数学归纳法**，它是数学中常用的一种方法. 我们将应用这种方法来证明整数环 $\boldsymbol{Z}$ 的一条重要的性质，即，单一因式分解性. 以下，所有的拉丁字母均表正整数.

先说明几个简单的事实.

(1) 若 $b>a$，以 a 除 b，得商 q，余数为 r，则有 $b=aq+r$，这里 $0 \leqslant r < a$. 若 $r=0$，称 a 为 b 的因数，或 a 可整除 b，记成 $a \mid b$. 若 $r \neq 0$，则 a 不能整除 b，记以 $a \nmid b$.

(2) 若 $a \mid b$，且 $a \mid c$，则 $a \mid (b+c)$.

事实上，从 $b=aq$, $c=aq_1$，得 $b+c=aq+aq_1=a(q+q_1)$.

(3) 若 $a|(b+c)$，且 $a|b$，则 $a|c$.

事实上，若 $b+c=aq$，$b=aq_1$，则 $c=aq-aq_1=a(q-q_1)$.

若 $p>1$，且除了 1 及 p 本身以外，p 没有其它的因数，则 p 叫做一个**素数**，例如 2, 3, 5, 7, 11, …都是素数.

我们需要一条引理.

引理 若 p 是素数，$p|bc$，但 $p\nmid b$，则 $p|c$.

证 先设 $b<p$，若 $b=1$，则已有 $p|c$. 设 $b>1$，作带余除法，$p=bq_1+r_1$. 因 p 是素数，$b\nmid p$，故 $1\leqslant r_1<b$. 于是从 $pc=bcq_1+r_1c$ 得 $p|r_1c$. 若 $r_1=1$，则 $p|c$. 若 $r_1>1$，再作带余除法 $p=r_1q_2+r_2$，于是又有 $p|r_2c$. 由此得到一系列的正整数 $p>b>r_1>r_2>\cdots$，都有 $p|r_ic$，$i=1, 2, \cdots$. 因 b 是有限数，这种作法不可能无限制地进行下去，故必到某一个 k，使 $r_k=1$，故 $p|c$.

再设 $b>p$. 让 $b=pq+r$，因 $p\nmid b$，故 $1\leqslant r<p$. 由 $bc=pqc+rc$ 得 $p|rc$. 现在 $r<p$，$p\nmid r$，故由上面的证明，得 $p|c$.

现在我们证明

整数环 Z 的单一素因数分解定理 若 n 为大于 1 的任一个整数，则 n 可唯一地表达成有限个素数 $p_1, p_2, \cdots, p_s$ 的乘积的形式.

$$n=p_1p_2\cdots p_s, \quad s\geqslant 1. \tag{2.1}$$

唯一性是指若 n 另有一个表达式

$$n=q_1q_2\cdots q_t, \quad t\geqslant 1 \tag{2.2}$$

诸 q_j 都是素数，则必 $s=t$，而且必要时重排一下次序以后，必有

$$p_1=q_1, \quad p_2=q_2, \cdots, p_s=q_s,$$

如果将(2.1)中相等的 p 合并成幂的形式，我们就得到 n 的**标准分解式**

$$n=p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}, \quad 在 i\neq j 时，\ p_i\neq p_j. \tag{2.3}$$

证 这条定理事实上是一系列命题 $P_2, P_3, \cdots, P_n, \cdots$，的无

穷集合，这里 P_n 的意思是说，n 这个具体的整数或本身是一个素数((2.1)中 $s=1$ 的情况)，或者可唯一地分解成 $s(>1)$ 个素数 $p_1, p_2, \cdots, p_s$ 的乘积 $p_1p_2\cdots p_s$.

现在应用归纳原理.

先设 $n=2$. 2 这个数本身就是一个素数，也就是(2.1)中 $s=1$ 的情况，而且 2 不可能分解成另外有限个素数的乘积，所以命题 P_2 是正确的.

现在假定 $n>2$，而且 $P_2, P_3, \cdots, P_{n-1}$ 都正确，就是说，于 $2\leqslant m\leqslant n-1$ 时，假定 m 可唯一地表达成素因子的乘积，我们要证明，n 也必有此性质.

如果 n 本身是一个素数，$n=p$，那么，它已是(2.1)的形式($s=1$ 的情况)，而且 p 不可能分解成另外一些素数的乘积.

如果 n 不是一个素数，则有因数 m 与 k，使 $n=mk$，$2\leqslant m<n$，$2\leqslant k<n$. 于是由归纳法的假定

$$m=p_1p_2\cdots p_{s'}, \quad k=p_{s'+1}p_{s'+2}\cdots p_s,$$

因此

$$n=mk=p_1p_2 \quad p_{s'}p_{s'+1}\cdots p_s.$$

故(2.1)对这个 n 成立. 如果又有

$$n=q_1q_2\cdots q_t,$$

诸 q_j 都是素数，那么，由于 $p_s\mid n$，故 $p_s\mid q_1q_2\cdots q_t$. 因此，由上述引理，p_s 必可整除诸 q_j 之一. 不失普遍性，可假定 $p_s\mid q_t$ 但 q_t 也是素数，所以 $p_s=q_t$. 于是有

$$p_1p_2\cdots p_{s-1}p_s=q_1q_2\cdots q_{t-1}p_s.$$

消去双方的 p_s，得

$$n'=p_1p_2\cdots p_{s-1}=q_1q_2\cdots q_{t-1}, \tag{2.4}$$

现在 $2\leqslant n'<n$，故由归纳法的假定，$P_{n'}$ 正确，(2.4)中 n' 的两个素数乘积的表达式应该是相同的. 所以 $s-1=t-1$，而且在重排次