厦门大学新世纪教材大系

线性代数

卢琳璋 曾晓明 编
许传炬 林亚南

新世纪教材大系

科学出版社

厦门大学新世纪教材大系

线 性 代 数

卢琳璋　曾晓明
许传炬　林亚南　编

科 学 出 版 社
2001

内 容 简 介

本书是厦门大学组织编写的面向21世纪系列教材之一.

本书系统地介绍了线性代数的基本内容,主要包括:多项式、行列式、矩阵及其分解、线性方程组、线性空间与线性变换、Euclid空间、二次型与对称矩阵等.本书强调了矩阵理论的应用及矩阵简洁记号的使用,编写上考虑到了数学系不同专业的后续课程的需要.

本书也可作为物理、机电等理工科相应课程的教材或参考书.

图书在版编目(CIP)数据

线性代数/卢琳璋等编.-北京:科学出版社,2001.3
(厦门大学新世纪教材大系)
ISBN 7-03-009081-0

Ⅰ.线… Ⅱ.卢… Ⅲ.线性代数-高等学校-教材 Ⅳ.O151.2

中国版本图书馆CIP数据核字(2000)第84222号

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
漳浦印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2001年3月第 一 版 开本:710×1 000 1/16
2001年3月第一次印刷 印张:11 1/2
印数:1—3 000 字数:203 000

定价:16.00元

(如有印装质量问题,我社负责调换〈杨中〉)

前　言

线性代数或高等代数是数学学科的基础课之一，是所有理工科高等数学课程的重要组成部分．为了满足高等院校在21世纪进行教学、教材改革的需要，考虑到现在大多数高校数学学科不分专业统一开基础课的实际情况，也考虑到数学学科以外的其它理工科（特别是研究生）对本课程的更高要求，我们编写了这本教材．

本教材的内容包括了线性代数的古典理论：多项式、行列式、矩阵、线性代数方程组、线性空间和线性变换、Euclid空间和正交变换、二次型、对称矩阵和Jordan标准形理论等．也在这些古典内容中加入了一些更适用于现代需要的内容：如矩阵的QR分解、奇异值分解、特征值估计、Hermite阵的Rayleigh商和极大极小原理等等．作为一种尝试，我们还在给出线性空间的定义之前引入了群的概念；结合讨论线性方程组的解的结构简单介绍了矩阵广义逆；由于有些内容，如数域、等价关系等贯穿在整本教材，我们特地编写了一个“第零章”．本教材的编写参考并引用了多本国内外相关的教材和书，但有对其中被引用的有些内容进行了简化和改写．本书充分使用了简洁的矩阵记号，减少了一些篇幅．

全书共分十章，其中第零、六、七章由卢琳璋编写；第一、五章由曾晓明编写；第二、三、四章初稿由林亚南编写（后经卢琳璋改写）；第八、第九章由许传炬编写．卢琳璋对全书作了比较大的修改并统一了全书的格式．

一方面由于本书多数编者是初次编写教材，另一方面由于编者水平有限，本书的错误在所难免，欢迎读者批评指正．

编者

2000．12

目　录

第零章　基本概念 ……（1）
§1　集合、映照和数域……（1）
§2　二元关系与代数运算……（3）
习题零 ……（5）
第一章　多项式 ……（6）
§1　一元多项式……（6）
§2　整除性与最大公因式……（8）
§3　因式分解及其惟一性定理……（13）
§4　根与代数基本定理……（17）
§5　常见数域上多项式的可约性与分解……（20）
§6　多元多项式简介……（24）
习题一 ……（27）
第二章　行列式 ……（30）
§1　排列……（30）
§2　行列式的定义……（31）
§3　行列式的基本性质……（33）
§4　Laplace 定理、行列式按行（列）展开 ……（39）
§5　行列式的计算……（43）
习题二 ……（46）
第三章　矩阵 ……（49）
§1　矩阵及其运算……（49）
§2　可逆矩阵与分块矩阵……（53）
§3　初等变换与初等矩阵……（57）
§4　方阵的行列式……（63）
§5　矩阵的秩……（64）
习题三 ……（67）
第四章　线性方程组 ……（70）
§1　消元法与初等变换……（70）
§2　可解性问题……（73）

§3　齐次线性方程组……（77）
§4　Cramer 法则 ……（79）
习题四 ……（80）
第五章　线性空间 ……（82）
§1　线性空间的概念……（82）
§2　子空间……（84）
§3　线性相关与线性无关……（89）
§4　基、维数与坐标……（93）
§5　基变换与坐标变换……（98）
§6　线性方程组解的结构和矩阵广义逆……（100）
习题五 ……（104）
第六章　线性变换 ……（108）
§1　定义、实例及运算……（108）
§2　线性变换与矩阵……（111）
§3　值域与核……（116）
§4　不变子空间……（118）
习题六 ……（120）
第七章　矩阵特征与 Jordan 标准型 ……（123）
§1　特征值与特征多项式……（123）
§2　特征向量……（127）
§3　Jordan 标准型……（131）
§4　Hamilton-Caylay 定理与最小多项式 ……（137）
§5　λ 矩阵简介……（140）
习题七 ……（141）
第八章　Euclid 空间 ……（143）
§1　定义与基本性质……（143）
§2　标准正交基……（146）
§3　正交矩阵与正交变换……（148）
§4　正交子空间与正交补……（150）
§5　酉空间和酉变换……（151）
§6　*QR* 分解和 Schur 分解 ……（153）
习题八 ……（156）
第九章　二次型与对称矩阵 ……（158）
§1　二次型及其矩阵表示……（158）

§2 对称矩阵和二次型的标准型……（160）
§3 正定二次型……（166）
§4 Rayleigh 商与极大-极小原理 ……（170）
§5 奇异值……（172）
§6 线性和双线性函数……（173）
习题九 ……（174）

第零章　基本概念

§1　集合、映照和数域

为了便于本书后面的讨论，我们先引入一些基本的概念，如集合、映照、数域等. 集合是不易定义的，只能描述它. 简单地说，所谓**集合**(简称**集**)指的是由某些特定的事物组成的一个整体. 例如，“全体自然数的集合”，“某个学校全体学生的集合”. 组成集合的事物称为该集合的**元素**(简称**元**). 我们用大写字母 $A,B,C,\cdots$ 表示集合，用小写字母 $a,b,c,\cdots$ 表示集合的元素. 如果 a 是集合 A 的元素，称 a 属于 A，记作 $a\in A$. 如果 a 不是集合 A 的元素，称 a 不属于 A，记作 $a\notin A$.

只含有限多个元素的集合称做**有限集**. 含无限多个元素的集合称做**无限集**. 不含任何元素的集合称做**空集**，空集用符号$\varnothing$表示. 例如，由数 1,2,3 组成的集合是有限集，适合方程 $x^2+y^2=1$ 的平面上的点的集合是无限集，方程 $x^2+1=0$ 的实根构成的集合是空集.

所谓给出一个集合，就是规定这个集合是由哪些元素组成的. 给出一个集合通常有两种方法：一种是列举出它的全部元素，例如，$A=\{1,2,3\}$；另一种是给出该集合元素的特征性质. 例如，适合方程 $x^2+y^2=1$ 的全部点的集合写成

$$A=\{(x,y)\mid x^2+y^2=1\}$$

如果集合 A 的元素全是集合 B 的元素，那么 A 就称为 B 的子集，记为

$$A\subseteq B \qquad 或 \qquad B\supseteq A$$

例如，全体偶数组成的集合是全体整数组成的集合的子集. 按规定，每个集合都是它自身的子集. 我们约定，空集是任一集合的子集.

两个集合 A 和 B 如果同时满足 $A\subseteq B$ 和 $A\supseteq B$，即 A 和 B 有完全相同的元素，则称 A 和 B 相等，记作 $A=B$.

设 A,B 是两个集合，由 A 的所有元素和 B 的所有元素组成的集合叫做 A 与 B 的**并**(集)，记为 $A\cup B$，即

$$A\cup B=\{x\mid x\in A \text{ 或 } x\in B\}$$

由 A 和 B 所有的公共元素组成的集合称为 A 与 B 的**交**(集)，记为 $A\cap B$，即

$$A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}$$

例如，$\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}$，$\{1,2,3\} \cap \{2,3,4\} = \{2,3\}$.

由定义，显然有 $A \cap B \subseteq A$，$A \cap B \subseteq B$，$A \subseteq A \cup B$，$B \subseteq A \cup B$.

设 M，N 是两个集合. 如果有某种规则，使得对于 M 中的每个元 a，都有 N 中一个且只有一个元 $\sigma(a)$ 与 a 对应，这样的对应关系称为 M 到 N 的**映照**. $\sigma(a)$ 称为 a 的像，M 称为 σ 的定义域，集合 $\{x \mid x = \sigma(a), a \in M\}$ 称为 σ 的值域，记为 $\sigma(M)$. 特别地，M 到 M 自身的映照，通常称为 M 的变换. 当值域在实数集 **R** 中时，映照 σ 就称为(实)函数，当值域在复数集 **C** 中时，σ 称为复函数.

在映照的定义中，要求一个元只对应一个像，并不要求不同的元对应不同的像，也不要求值域就是整个集合 N. 如果一个映照 σ，使得 M 中不同的元对应 N 中不同的元，则称 σ 是一一(**对应**)映照. 而如果，$\sigma(M) = N$，即 σ 的值域就是整个集合 N，则称 σ 是**到上映照**. 如果一个映照 σ 既是一一映照，又是到上映照，称 σ 是一个一一**到上映照**.

一个无限集 M 如果可以与自然数集 $N = \{1,2,3,\cdots\}$ 建立起一一到上映照，则称 M 是**可列集或可数集**. 例如所有的偶数所形成的集 $M = \{2,4,\cdots\}$，它与自然数集 N 可以建立起一个一一到上映照：M 中的 $2n$ 与 N 中的 n 相对应. 因此 M 是可列集. 由此可见，对于无限集来说，一个集可以与它的真子集建立起一一对应关系，这也是无限与有限的一个差别.

在中学代数里，我们知道，讨论问题时，常常需要明确规定所考虑的数的范围，即确定数集. 在不同数集中考虑同一个问题，答案可能是不一样的. 例如，方程 $x^2 + 1 = 0$. 在实数集中考虑，这个方程没有解；若在复数集中考虑，则这个方程有两个解 $x_1 = \mathrm{i}$，$x_2 = -\mathrm{i}$. 我们经常遇到的数集有复数集 **C**、实数集 **R**、有理数集 **Q**，它们显然是不同的集合. 但它们有一些共同的性质，比如集合 **Q**，**R**，**C** 中的元素都可以进行加、减、乘、除(除数不为 0)运算. 还有很多数集也具有与 **Q**，**R**，**C** 共有的这种代数性质，为把它们统一起来讨论，我们引入数域的定义.

定义 1　设 F 是含有非零数的一个数集. 如果 F 中任意两个数(这两个数可以相同)的和、差、积、商(除数不为 0)仍然是 F 中的数，则 F 就称为一个**数域**.

按此定义，数集 **Q**，**R**，**C** 均为数域，分别叫做有理数域、实数域、复数域. 因为任意两个整数的商未必是整数，所以整数集 **Z** 不是数域. 再看一个例子.

例 1　$A = \{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\}$ 是一个数域.

解　首先，$1 = 1 + 0\sqrt{3} \in A$，即 A 含有非零数.

又由 $a+b\sqrt{3}, c+d\sqrt{3}\in A$，可得

$$(a+b\sqrt{3})\pm(c+d\sqrt{3})=(a\pm c)+(b\pm d)\sqrt{3}\in A$$

$$(a+b\sqrt{3})(c+d\sqrt{3})=(ac+3bd)+(ad+bc)\sqrt{3}\in A$$

设 $c+d\sqrt{3}\neq 0$，则 c, d 不能同时为 0，所以 $c-d\sqrt{3}\neq 0$，而

$$\frac{a+b\sqrt{3}}{c+d\sqrt{3}}=\left(\frac{a+b\sqrt{3}}{c+d\sqrt{3}}\right)\left(\frac{c-d\sqrt{3}}{c-d\sqrt{3}}\right)=\frac{ac-3bd}{c^2-3d^2}+\frac{bc-ad}{c^2-3d^2}\sqrt{3}\in A$$

这说明了 A 是一个数域.

本节最后，我们给出数域的一个重要性质.

命题 1 任何数域都包含有理数域 $\mathbf{Q}$.

证 设 F 是一个数域，则有非零数 $a\in F$. 于是 $a/a=1\in F$，$a-a=0\in F$，从而 $1+1=2, 2+1=3, \cdots, n+1=n+1, \cdots$ 都在 F 中，即 F 包含全体正整数. 又 $0-n=-n$ 也属于 F，所以 F 包含全体整数. 对任意的 $b\in\mathbf{Q}$，b 可以表成两个整数的商，所以 $b\in F$.

§2 二元关系与代数运算

设 M 是一个集合. 对任意的 $a, b\in M$，所有有序对 (a, b) 组成的集合称为 M 的乘积集，记为 $M\times M$，即

$$M\times M=\{(a,b)\mid a\in M, b\in M\}$$

例如 $M=\{1,2,3\}$，则

$$M\times M=\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$$

对于 M 中的元素 (a, b)，如果 a 与 b 具有某种关系 R，则记为 $R(a, b)$ 或者 aRb. 这种 M 上二个元素之间的关系称为**二元关系**. 如果 R 是 M 的一个二元关系，则集合：$\{(a,b)\mid aRb\}$ 构成 $M\times M$ 的一个子集. 例如 $M=\{1,2,3\}$，关系 R 是数的大于关系“$>$”. 则使这个关系 R 成立的 $M\times M$ 中的元素只有三个：$(2,1), (3,1), (3,2)$. 这三个元素构成 $M\times M$ 的一个子集. 所以一个二元关系确定了 $M\times M$ 的一个子集，反过来 $M\times M$ 的一个子集，也可以看作是由某种二元关系所确定的. 显然，同一个乘积集上，可以有很多不同的二元关系.

定义 2 如果集合 M 上的一个二元关系 R，具有下列三个性质：

(1)自反性：对所有 $a\in M$，有 aRa，

(2)传递性：若 aRb, bRc，则 aRc，

(3)对称性：若 aRb，则 bRa，

则称 R 为 M 上的一个**等价关系**.

例如 M 是平面上所有三角形的集合,关系 R 为几何上的相似,则 R 就是 M 上的一个等价关系.两个三角形的"全等关系"也是 M 上的一个等价关系.但是并不是所有的关系都能成为一个等价关系.例如,前面定义的集合 $M=\{1,2,3\}$ 和关系"$>$",就不是一个等价关系.

有了等价关系,我们可以引入等价类的概念.

如果 R 是 M 上的一个等价关系,对于 $a\in M$,可定义:$R_a=\{x\mid aRx, x\in M\}$,并且称这个集合为 a 的一个**等价类**.显然,$R_a\neq\varnothing$,因为 $a\in R_a$.

如果 a、$b\in M$,R_a 与 R_b 作为 M 的子集是不同的,我们称 R_a 与 R_b 不相同.

命题 2　不相同的等价类 R_a 与 R_b 是不相交的.

证　如果有 $c\in M$,而且 $c\in R_a\cap R_b$,则 aRc,bRc.根据 R 的对称性有 cRb,根据 R 的传递性有 aRb,再根据 R 的对称性有 bRa.

对任意的 $d\in R_a$,则 aRd.根据传递性有 bRd,即 $d\in R_b$.因此,$R_a\subseteq R_b$.同理可证,$R_b\subseteq R_a$.从而 $R_a=R_b$.这与假设矛盾.这样一来,$R_a\cap R_b=\varnothing$.

由于 M 中的每一个元素必定归属于一个等价类,因此有

命题 3　集合 M 是等价关系 R 的不同也不相交的等价类之和集.

设 R 是集 M 的一个等价关系,以它的所有等价类为元素(相同的等价类当作一个元素)的集合,称为 M 的**商集**,记作 M/R.

例 2　设 M 是正整数集.M 的任一个元素除以 5 的余数是 0,1,2,3,4 中的一个.考虑如下关系 R:对任意的 a,$b\in M$,如果它们除以 5 的余数相同,记为 aRb.这种关系称为同余关系,它是一个等价关系.于是,M 中除以 5 余数为 0,1,2,3,4 的元素构成等价类:R_0,R_1,R_2,R_3,R_4.商集 M/R 的元素就是这 5 个元素.

上述乘积集的概念可以进行推广.一般地,若 $M_1,M_2,\cdots,M_s$ 是 s 个集合,则可定义乘积集:

$$M_1\times M_2\times\cdots\times M_s=\{(a_1,a_2,\cdots,a_s)\mid a_i\in M_i,i=1,2,\cdots,s\}$$

下面介绍代数运算的概念.

在算术中的 +,−,×,÷ 四则运算就是代数运算,用集合和映照的语言来说,就是实数集上的一个有序对 (a,b) 对应实数集上一个数.例如,通常的两个数的加法 $(x,y)\to x+y$ 和乘法 $(x,y)\to xy$ 就是两种不同的代数运算.推广到一般情况有

定义 3　设若 $M_1,M_2,\cdots,M_s$ 和 N 是 $s+1$ 个集合,G 是 $M_1\times M_2\times\cdots\times M_s$ 的一个非空子集,G 到 N 的一个映照 ω 称为 s **元代数运算**,简称 s 元运算

或代数运算.

例如 $M_1=M_2=N=R, G=\{(a,b)\mid a\in M_1,\in M_2, b\neq 0\}$, $\omega:(a,b)\to a/b$. 则 ω 是一个二元运算,也就是算术中的除法运算. 此外,算术中的开方运算就是正数集到正数集的一种映照,是一种一元运算.

通常二元运算用得比较多,此时,$G\subseteq M_1\times M_2$,对任一$(a,b)\in G$,由 ω 确定了一个对应的$c\in N$,可记作:$a\omega b=c$. 在 $M_1=M_2=M$ 的情况下,二元运算称为 M 上的**二元运算**或**代数运算**.

习 题 零

1. 验证下列数集是数域:
   $(1)F_1=\{a+b\sqrt{2}\mid \forall a,b\in\mathbf{Q}\}$;$(2)F_2=\{a+bi\mid \forall a,b\in\mathbf{Q}\}$.
2. 设 F_1 与 F_2 为两个数域,而 $F=\{a\mid a\in F_1$ 且 $a\in F_2\}$,试证 F 亦为一个数域.
3. 下面集合中,哪些是有限集? 哪些是无限集? 哪些是空集? 哪些集合相等? 哪些集合有包含关系?
   N(自然数集),**Z**(整数集),**Q**,**R**
   $A=\{2x\mid x\in Z\}, B=\{2\}$, $C=\{x\mid x\in A$ 且 $x^2=1\}$,
   $D=\{x\mid x\in A$ 且 x 为质数$\}$, $E=\{x\mid x\in\mathbf{Q}$ 且 $x^2=2\}$.
4. 设 A,B,C 为集合,证明:
   $A\cap(B\cup C)=(A\cap B)\cup(A\cap C), A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$
5. 设 M 是球面上去掉一点后的点的全体,N 是平面上点的全体,如何建立 M 和 N 之间的一个一一到上映照.

第一章 多 项 式

§1 一元多项式

多项式是高等代数课程基本的内容之一，并且在学习其它数学课程时也会经常涉及到.这章我们讨论多项式(主要是一元多项式)的一些基本性质.下面假定，我们总是在一个预先给定的数域 F 上讨论问题.

定义 1 设 x 是一个符号(或称文字)，形式表达式

$$a_nx^n + a_{n-1}x^{n-1}\cdots + a_1x + a_0 \tag{1}$$

称为数域 F 上的一元多项式，其中 n 为非负整数，$a_n, a_{n-1}, \cdots, a_0$ 是 F 中的数.记号 $F[x]$ 表示数域 F 上的全体一元多项式.

比如 $x^3 - \frac{1}{2}x + 6, \pi x + \mathrm{i}, 2, 0$ 都是 x 的多项式，而 $3x^{1/2} - x, x^2 - x + 2x^{-1}$ 都不是 x 的多项式.

在多项式(1)中，a_ix^i 称为 i 次项，a_i 称为 i 次项的系数，a_0 称为 0 次项或常数项.我们常用 $f(x), g(x), \cdots$ 等来表示多项式.在(1)中，如果 $a_n \neq 0$，那么 a_nx^n 称为多项式(1)的首项，a_n 称为首项系数，而 n 就称为多项式(1)的次数.如果在(1)中，$a_n = a_{n-1} = \cdots = a_0 = 0$，这种多项式称为零多项式，记为 0.零多项式不规定次数.因此，以后我们说到多项式 $f(x)$ 的次数时，总是假定 $f(x) \neq 0$，并用记号 $\partial(f(x))$ 表示多项式 $f(x)$ 的次数.

如果两个多项式 $f(x)$ 与 $g(x)$ 的次数相同，且同次项的系数完全相同，则称 $f(x)$ 与 $g(x)$ 相等，记作 $f(x) = g(x)$.一个多项式中可以任意加入或去掉一些系数是 0 的项.

现在来规定多项式的加法、减法与乘法运算.设

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

是数域 F 上两个多项式，不妨假定 $m \leqslant n$.那么 $f(x)$ 与 $g(x)$ 的和为

$$f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

其中 $b_{m+1} = \cdots = b_n = 0$.

而 $f(x)$ 与 $g(x)$ 的乘积为

$$f(x)g(x) = a_nb_mx^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + (a_1b_0 + a_0b_1)x + a_0b_0$$

其中 i 次项的系数为 $a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i$.

将 $g(x)$的所有系数变号所得到的多项式记为 $-g(x)$,利用多项式的加法运算可以定义 $f(x)$与 $g(x)$的差(减法):

$$f(x) - g(x) = f(x) + (-g(x)).$$

显然,数域 F 上的两个多项式经过加、减、乘运算后,所得结果仍然是数域 F 上的多项式.多项式的加法与乘法满足以下规律:

1. 加法交换律:$f(x)+g(x)=g(x)+f(x)$,

2. 加法结合律:$(f(x)+g(x))+b(x)=f(x)+(g(x)+b(x))$,

3. 乘法交换律:$f(x)g(x)=g(x)f(x)$,

4. 乘法结合律:$(f(x)g(x))b(x)=f(x)(g(x)b(x))$,

5. 乘法对加法的分配律:$f(x)(g(x)+b(x))=f(x)g(x)+f(x)\cdot b(x)$.

这些规律都可以由定义直接验证,我们这里就省略了.

关于多项式运算后的次数,我们还可以证明:

命题 1 设 $f(x)$与 $g(x)$是 F 上两个多项式,并且 $f(x)\neq 0, g(x)\neq 0$,则

1. 当 $f(x)+g(x)\neq 0$ 时,$\partial(f(x)\pm g(x))\leqslant \max(\partial(f(x)),\partial(g(x)))$①,

2. $f(x)g(x)\neq 0$,并且 $\partial(f(x)g(x))=\partial(f(x))+\partial(g(x))$.

证 设 $\partial(f(x))=n$,$\partial(g(x))=m$,并且 $m\leqslant n$,

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad (a_n \neq 0)$$

$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \quad (b_m \neq 0)$$

则

1. $f(x)+g(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0)$

其中 $b_{m+1}=\cdots=b_n=0$,当 $f(x)+g(x)\neq 0$ 时,显然和的次数不超过 n;

2. $f(x)g(x)=a_nb_mx^{n+m}+\cdots+(a_1b_0+a_0b_1)x+a_0b_0$

因为 $a_nb_m\neq 0$,所以 $f(x)g(x)\neq 0$,且 $\partial(f(x)g(x))=n+m$.

从命题 1 可得如下乘法消去律:

若 $f(x)\neq 0$ 且 $f(x)g(x)=f(x)b(x)$,则 $g(x)=b(x)$.

① $\max(n,m)$代表 n,m 中较大的一个数.

§2　整除性与最大公因式

从上一节知道，在多项式集合里，可以做加、减、乘三种运算，但是乘法的逆运算——除法，并不是普遍可以进行的，例如 $x \div x^2 = \frac{x}{x^2}$ 并不是一个多项式，即 x^2 不能除尽 x. 因而整除(除尽)就成了两个多项式之间的一种特殊关系.

定义 2　设 $f(x)$ 与 $g(x)$ 是 $F[x]$ 中的两个多项式，若存在 $F[x]$ 中的多项式 $b(x)$，使得 $f(x)=g(x)b(x)$，则称 $g(x)$ **整除** $f(x)$，记作 $g(x)|f(x)$，否则，称 $g(x)$ 不能整除 $f(x)$，记作 $g(x)\nmid f(x)$. 当 $g(x)|f(x)$ 时，则称 $g(x)$ 为 $f(x)$ 的一个因式，而称 $f(x)$ 为 $g(x)$ 的一个**倍式**.

下面是有关多项式整除的一些简单性质.

1. 当 $a\neq 0$ 时，由 $f(x)=a(a^{-1}f(x))$ 知道非零常数能整除任一多项式 $f(x)$;

2. 如果 $f(x)|g(x)$，$g(x)|b(x)$，则 $f(x)|b(x)$;

事实上，由条件 $g(x)=f(x)g_1(x)$，$b(x)=g(x)b_1(x)$，即可得 $b(x)=f(x)(g_1(x)b_1(x))$.

3. 如果 $f(x)|g(x)$，且 $g(x)|f(x)$，则 $f(x)=cg(x)(c\neq 0)$;反之亦然;

实际上，若 $f(x)=0$，由条件需 $g(x)=0$，结论成立. 因此可设 $f(x)\neq 0$，由条件有

$$g(x)=f(x)g_1(x) \quad 和 \quad f(x)=g(x)f_1(x)$$

即 $f(x)=f(x)g_1(x)f_1(x)$，因此 $1=g_1(x)f_1(x)$，所以 $f_1(x)$ 和 $g_1(x)$ 皆为非零常数;反之，若 $f(x)=cg(x)$，$c\neq 0$，则 $g(x)=c^{-1}f(x)$. 所以 $f(x)|g(x)$ 且 $g(x)|f(x)$.

4. 如果 $f(x)|g_i(x)$，$i=1,2,\cdots,s$，则对 F 上任意 s 个多项式 $u_i(x)$，$i=1,2,\cdots,s$，有

$$f(x)\mid \sum_{i=1}^{s} u_i(x)g_i(x) \ ①$$

事实上，由条件可设 $g_i(x)=f(x)b_i(x)$，$i=1,2,\cdots,s$，所以

① "$\sum$"称为连加号，$\sum_{i=1}^{s}a_i$ 表示 $a_1+a_2+\cdots+a_s$.

$$\sum_{i=1}^{s} u_i(x)g_i(x) = f(x)\sum_{i=1}^{s} u_i(x)b_i(x)$$

从上面的讨论知道,对任意两个多项式 $f(x)$ 与 $g(x)$,并不一定总是有整除关系,但我们有下面的

带余除法 设 $f(x)$ 与 $g(x)$ 是数域 F 上的任意两个多项式,并且 $g(x)\neq 0$,则存在 F 上惟一的两个多项式 $q(x)$ 与 $r(x)$,使得

$$f(x) = g(x)q(x) + r(x) \tag{2}$$

其中 $r(x)=0$ 或者 $\partial(r(x))<\partial(g(x))$.

证 如果 $f(x)=0$,取 $q(x)=r(x)=0$ 即可.下面设 $f(x)\neq 0$,而且 $\partial(f(x))=n$,$\partial(g(x))=m$.我们对 $f(x)$ 的次数 n 用(第二)数学归纳法.

当 $n<m$ 时,取 $q(x)=0$,$r(x)=f(x)$,(2)成立.因此只要讨论 $n\geqslant m$ 的情形.假设当 $f(x)$ 的次数小于 n 时,$q(x)$,$r(x)$ 的存在性已证.现在证明 $f(x)$ 的次数等于 n 时,$q(x)$,$r(x)$ 的存在性.

设 ax^n,bx^m 分别是 $f(x)$,$g(x)$ 的首项,显然 $b^{-1}ax^{n-m}g(x)$ 与 $f(x)$ 有相同的首项,因而多项式:$b(x)=f(x)-b^{-1}ax^{n-m}g(x)$ 的次数小于 n(或 $b(x)=0$,此时,命题显然成立).由归纳法的假设,对 $b(x)$,$g(x)$ 存在 $q_1(x)$,$r_1(x)$ 使得:

$$b(x) = g(x)q_1(x) + r_1(x)$$

其中 $\partial(r_1(x))<\partial(g(x))$ 或者 $r_1(x)=0$.这样,

$$f(x) = (q_1(x) + b^{-1}ax^{n-m})g(x) + r_1(x)$$

即有 $q(x)=q_1(x)+b^{-1}ax^{n-m}$,$r(x)=r_1(x)$ 使得(2)成立.由归纳法原理,$q(x)$,$r(x)$ 的存在性得证.

下面证明惟一性.设另有 $p(x)$,$t(x)$ 使得

$$f(x) = g(x)p(x) + t(x)$$

其中 $t(x)=0$ 或者 $\partial(t(x))<\partial(g(x))$.那么就有

$$g(x)p(x) + t(x) = g(x)q(x) + r(x)$$

或

$$g(x)(p(x) - q(x)) = r(x) - t(x)$$

若 $p(x)\neq q(x)$,又 $g(x)\neq 0$,那么就有 $r(x)-t(x)\neq 0$,从而

$$\partial(g(x)) + \partial(p(x) - q(x)) = \partial(r(x) - t(x))$$

但是由于 $\partial(g(x))>\partial(r(x)-t(x))$,因此上式不可能成立.这说明 $p(x)=q(x)$,进而有 $r(x)=t(x)$.

通常称(2)中的 $q(x)$ 为 $g(x)$ 除 $f(x)$ 的商,$r(x)$ 为 $g(x)$ 除 $f(x)$ 的余式.从带余除法很容易得到整除性的一个判别法.

命题 2　对数域 F 上的任意两个多项式 $f(x)$ 与 $g(x)$，其中 $g(x)\neq 0$，则 $g(x)$ 整除 $f(x)$ 的充分必要条件是(2)式中 $r(x)=0$.

接下来我们讨论多项式的最大公因式. 如果 $b(x)$ 既是 $f(x)$ 的因式，又是 $g(x)$ 的因式，则称 $b(x)$ 是 $f(x)$ 与 $g(x)$ 的一个**公因式**. 两个多项式 $f(x)$ 与 $g(x)$ 的公因式总是存在的. 例如，零次多项式就是它们的公因式. 一般地，它们还有其他公因式，其中特别重要的就是所谓的最大公因式.

定义 3　设 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个公因式，又是 $f(x)$ 与 $g(x)$ 的任一个公因式的倍式，则称 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个**最大公因式**.

例如，对于任意多项式 $f(x)$，$f(x)$ 就是 $f(x)$ 与 0 的一个最大公因式. 又如果 $f(x)\mid g(x)$，那么 $f(x)$ 就是 $f(x)$ 与 $g(x)$ 的一个最大公因式. 任意两个多项式的最大公因式是否一定存在呢？答案是肯定的. 利用带余除法我们可以解决这个问题，先证一个命题.

命题 3　如果等式

$$f(x)=g(x)q(x)+r(x) \tag{3}$$

成立，那么 $f(x)$，$g(x)$ 与 $g(x)$，$r(x)$ 有相同的公因式.

证　若 $d(x)$ 是 $g(x)$ 与 $r(x)$ 的公因式，即 $d(x)\mid g(x)$ 且 $d(x)\mid r(x)$，由(3)得 $d(x)\mid f(x)$，因此 $d(x)$ 也是 $f(x)$ 与 $g(x)$ 的公因式. 反之由(3)得

$$r(x)=f(x)-g(x)q(x) \tag{4}$$

由(4)即得 $f(x)$，$g(x)$ 的公因式也都是 $g(x)$，$r(x)$ 的公因式.

事实上，可进一步推出：若(3)成立，则 $f(x)$，$g(x)$ 与 $g(x)$，$r(x)$ 有相同的最大公因式(看习题).

定理 1　数域 F 上任意两个多项式 $f(x)$ 与 $g(x)$ 必存在一个最大公因式 $d(x)$，且可以找到 F 上的多项式 $u(x)$，$v(x)$ 使得

$$u(x)f(x)+v(x)g(x)=d(x) \tag{5}$$

证　如果 $g(x)=0$，则 $f(x)$ 就是一个最大公因式，且 $f(x)=1\cdot f(x)+1\cdot 0$，这时定理成立.

因此可设 $g(x)\neq 0$，按带余除法，用 $g(x)$ 除 $f(x)$，得到商 $q_1(x)$ 和余式 $r_1(x)$. 如果 $r_1(x)=0$，那么，$g(x)$ 就是 $f(x)$，$g(x)$ 的最大公因式. 否则，再用 $r_1(x)$ 除 $g(x)$，得到商 $q_2(x)$ 和余式 $r_2(x)$. 如果 $r_2(x)=0$，则 $r_1(x)$ 就是 $f(x)$、$g(x)$ 的最大公因式. 否则，就用 $r_2(x)$ 除 $r_1(x)$，得到商 $q_3(x)$ 和余式 $r_3(x)$；如此辗转相除下去，显然，所得余式的次数不断降低，即

$$\partial(g(x))>\partial(r_1(x))>\partial(r_2(x))>\cdots$$

因此，在有限次除法之后，必然会有余式为零，于是我们有一串等式：

$$f(x)=g(x)q_1(x)+r_1(x)$$