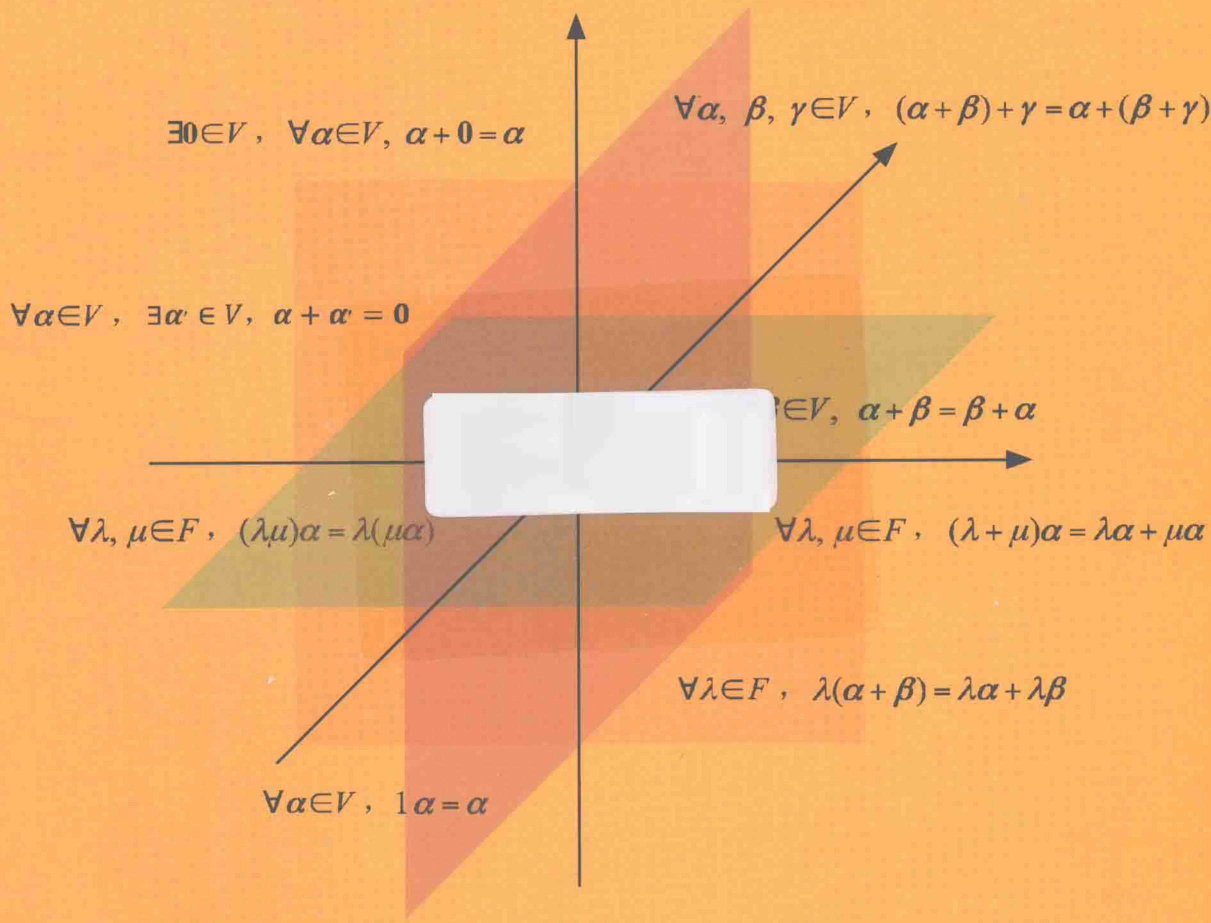
高等代数

陈小松　主编



清华大学出版社

高等代数

陈小松　主编
李俊平　刘金旺　刘庆平　王国富　参编

清华大学出版社
北　京

内 容 简 介

本书是为高等院校数学类专业编写的高等代数教材。包含多项式、行列式、线性方程组、矩阵、二次型、向量空间、线性变换、欧氏空间，双线性函数共9章内容。在注重强化基础知识及其训练的同时，兼顾应用以及与数学软件的结合，内容精炼，重点突出。每章最后一节也可以作为学生自主研学的内容，对培养学生主动学习的能力大有益处。

图书在版编目(CIP)数据

高等代数/陈小松主编.--北京：清华大学出版社，2014
ISBN 978-7-302-37096-3

Ⅰ. ①高…　Ⅱ. ①陈…　Ⅲ. ①高等代数—高等学校—教材　Ⅳ. ①O15

中国版本图书馆CIP数据核字(2014)第145984号

责任编辑：刘　颖
封面设计：傅瑞学
责任校对：赵丽敏
责任印制：王静怡

出版发行：清华大学出版社
　　网　　址：http://www.tup.com.cn，http://www.wqbook.com
　　地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
　　社 总 机：010-62770175　　**邮　　购**：010-62786544
　　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　　质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：河北新华第一印刷有限责任公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　张**：18　　**字　　数**：391千字
版　　次：2014年9月第1版　　**印　　次**：2014年9月第1次印刷
印　　数：1～3000
定　　价：35.00元

产品编号：060601-01

前言

FOREWORD

高等代数所包含的教学内容在大学数学专业、理科和工科专业都起着重要的作用. 在教与学的过程中教材起着重要的作用. 一本好的教材，我们认为要具有以下五个条件：一是要注意继承过去已列名优教材的优点，教学内容选择要恰当，内容安排顺序要自然，循序渐进，由浅入深；二是要注重教学内容的历史，问题的目的、来源和发展要简单扼要地交待清楚，强化“问题驱动”的教学思想；三是要与时俱进，注重教学内容的应用，要将数学应用和数学软件融入到教材里，注重将数学软件的应用编入到例题和习题中，可以作为学生自主研学的辅助材料；四是要适合专业的特点，要给教师根据教学对象和学时多少选择教学内容的余地，教材要包含大多数名优教材的基本内容，以便于教师和学生查阅；五是要以学生为中心，充分发挥学生的主体作用，将引导学生进行自主研究性学习内容选入教材. 我们根据多年的教学经验和体会，编写了这本教材. 我们注意继承过去名优教材的优点，同时具有如下特点：第一，注重了教学内容的历史；第二，注重了教学内容的应用；第三，注重了将数学软件 Maple 应用到习题中，可以作为学生自主研学的辅助素材；第四，我们也将习题单独装订为合页册，方便学生习题和交作业，也方便老师批改；第五，部分调整了教学体系的结构，使得教学内容由浅入深，注重启发性，避免教学内容单纯重复；第六，增加了中英文对照的名词索引.

李俊平教授、刘金旺教授、刘庆平教授、王国富副教授和我多次对该教材进行讨论、编写和修改，并为本套教材配备了习题. 教材由刘伟俊教授审稿. 该书适合数学、信息与计算科学及统计学专业作为教材使用，也适合一些理科专业的学生对其内容选择使用. 可以根据课程的学时，适当选择教学内容. 例如，教学计划为 128 学时的，可以选择除 9.3 节，9.4 节以外的所有内容，教学计划为 88 学时的，可以选择 1.1～1.4 节，第 2 章到第 6 章中非星号部分加上 7.1～7.8 节、8.1～8.6 节的内容. 整个教材中打星号的部分，可供教师教学时选

择. 每一章的最后一节可以作为学生自主研学、开展科研训练的内容. 教材可能还会存在一些问题,希望使用该教材的同学和老师将问题指出来,发送到我的邮箱:xschen@csu.edu.cn,以便今后重印或再版时修改.

陈小松

2014 年 5 月于中南大学

目 录

CONTENTS

第 1 章
CHAPTER 1

多　项　式

多项式是代数中的一个基本概念，求多项式方程的解是最古老的数学问题之一．多项式理论不仅对数学本身非常重要，而且它的重要性更体现在实际应用中．

1.1　数域　整数的整除性

集合的概念：若干事物的全体称为一个集合，组成集合的这些事物称为集合的元素．

集合的概念只是一个描述性的说明．集合中的元素具有：确定性、互异性和无序性．

常用大写字母 A,B,C 等表示集合，用小写字母 a,b,c 等表示集合的元素．当 a 是集合 A 的元素时，就称 a 属于 A，记作 $a\in A$；当 a 不是集合 A 的元素时，就称 a 不属于 A，记作$a\notin A$．

集合的表示方法一般有两种：描述法、列举法．

描述法：给出这个集合的元素所具有的特征性质，即 $M=\{x\mid x$ 具有性质 $P\}$．

列举法：把构成集合的全部元素一一列举出来．

例如

$$M=\{(x,y)\mid x^2+y^2=4,x,y\in\mathbb{R}\},\quad N=\{1,2,3,\cdots\}.$$

不含任何元素的集合称为空集，记为$\varnothing$．

如果集合 B 中的每个元素都是集合 A 中的元素，则称 B 是 A 的子集合或 B 包含于 A，记作 $B\subseteq A$．空集是任意集合的子集合．

如果 A 与 B 两集合含有完全相同的元素，则称 A 与 B 相等，记作 $A=B$．$A=B$ 当且仅当 $A\subseteq B$ 且 $B\subseteq A$．

集合 $A\cap B=\{x\mid x\in A$ 且 $x\in B\}$称为 A 与 B 的交．

集合 $A\cup B=\{x\mid x\in A$ 或 $x\in B\}$称为 A 与 B 的并．

为了在下面课程里讨论起来严谨和方便，需要引入数域的概念．

数是数学中一个最基本的概念，随着人们对客观世界的认识的不断深入，使得数经历了由自然数到整数、有理数、实数，再到复数这样一个发展过程．通常我们用$\mathbb{N}$表示自然数集合，用$\mathbb{Z}^+$表示正整数集合，用$\mathbb{Z}$表示整数集合，用$\mathbb{Q}$表示有理数集合，用$\mathbb{R}$表示实数集合，用$\mathbb{C}$

表示复数集合.

若数集 S 中任意两个数作某一运算的结果仍在 S 中,则称数集 S 对这一运算是封闭的.

扩张数范围的主要原因是由于要求某些运算封闭或方程求解引起的.任意两个整数进行加、减、乘法运算后仍然是整数,但任意两个整数的商不一定是整数,这就是说,限制在整数的范围内,除法不是普遍可以做的,而在有理数范围、实数范围及复数范围,只要除数不为零,除法是可以做的,因此,在数的不同范围内,回答同一个问题的答案可能是不同的.例如,在解决一个实际问题中列出一个一元二次方程,这个方程有没有解与未知量所允许的取值范围有关.我们经常会遇到的数的范围有全体有理数、全体实数以及全体复数,它们显然具有一些不同的性质,它们也有很多共同的性质,为了在今后讨论中能够把它们关于加、减、乘、除运算的共同性质统一起来,我们引入一个一般的概念.

定义 1.1　设 S 是复数集的非空子集.如果对于 S 中的任意两个数的和、差、积仍属于 S,则称 S 是一个**数环**.

$\mathbb{Z}$对数的加法、减法和乘法作成一个数环,我们称它为整数环.

定义 1.2　设 F 是由一些复数组成的集合,其中包含 0 与 1.如果 F 中任意两个数的和、差、积、商(除数不为 0)仍是 F 中的数,则称 F 为一个**数域**.

容易验证,全体有理数的集合$\mathbb{Q}$对于通常的四则运算作成一个数域,称为有理数域.类似地,$\mathbb{R}$称为实数域,$\mathbb{C}$称为复数域.整数环$\mathbb{Z}$不是数域.

例 1.1　证明:数集 $Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$是一个数域.

证明　由于 $0=0+0\sqrt{2}$,$1=1+0\sqrt{2}$,故 $0,1\in Q(\sqrt{2})$.又对 $\forall x,y\in Q(\sqrt{2})$,设 $x=a+b\sqrt{2}$,$y=c+d\sqrt{2}$,$a,b,c,d\in\mathbb{Q}$,则有

$$x\pm y=(a\pm c)+(b\pm d)\sqrt{2}\in Q(\sqrt{2}),\quad x\cdot y=(ac+2bd)+(ad+bc)\sqrt{2}\in Q(\sqrt{2}).$$

设 $a+b\sqrt{2}\neq 0$,于是 $a-b\sqrt{2}$ 也不为 0.否则,若 $a-b\sqrt{2}=0$,则 $a=b\sqrt{2}$,于是 $a=0,b=0$,$a+b\sqrt{2}=0$.矛盾.

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

所以,$Q(\sqrt{2})$为数域.

例 1.2　任意数域 F 都包括有理数域$\mathbb{Q}$.即有理数域是最小数域.

证明　设 F 为任一数域.由定义可知,$0\in F$,$1\in F$.于是有

$$\forall m\in\mathbb{Z}^+,\quad m=1+1+\cdots+1\in F,$$

即 F 包含全体自然数.又

$$\forall m,\quad n\in\mathbb{Z}^+,\quad \frac{m}{n}\in F,\quad -\frac{m}{n}=0-\frac{m}{n}\in F.$$

而任意一个有理数可表成两个整数的商,所以,$\mathbb{Q}\subseteq F$.

定义 1.3 设 $a,b\in\mathbb{Z},b\neq0$,如果 $\exists q\in\mathbb{Z}$,使得 $a=bq$,则称 b **整除** a,记作 $b|a$,这时称 b 是 a 的**因数**,也称 a 是 b 的倍数;当 $q\neq\pm1,\pm a$ 时,称 b 是 a 的真因数.如果这样的 q 不存在,则称 b 不整除 a,记作 $b\nmid a$.

定理 1.1(基本性质) (1) 若 $c|b,b|a$,则 $c|a$;

(2) 若 $m|a,m|b$,则 $\forall p,q\in\mathbb{Z},m|pa+qb$;

(3) 若 $b|a,a\neq0$,则 $|b|\leqslant|a|$;

(4) 若 $b|a$ 当且仅当 $c\neq0,cb|ca$.

证明 (1) 由已知,$b=cs,a=bt$,故 $a=(cs)t=c(st)$,即 $c|a$;

(2) 由已知 $a=ms,b=mt$,故 $pa+qb=mps+mqt=m(ps+qt)$,即 $m|pa+qb$;

(3) 由已知 $a=bc$,故 $|a|=|b||c|$.而 $a\neq0$,故 $|a|\neq0$,因为 $|c|\geqslant1$,所以 $|b|\leqslant|a|$;

(4) 由已知 $a=bs$,故 $ca=cbs$,即 $cb|ca$.

定理 1.2(带余除法) 设 $a,b\in\mathbb{Z},b\neq0$,则存在唯一的 q,r,使得 $a=bq+r,0\leqslant r<|b|$.

证明 作数列$\cdots,-2|b|,-|b|,0,|b|,2|b|,\cdots,a$ 必落在此数列相邻两项所构成的某一区间且只能落在一个区间内,即存在 q,使得 $q|b|\leqslant a<(q+1)|b|$,减去 $q|b|$,得 $0\leqslant a-q|b|<|b|$.令 $r=a-q|b|$,则有 $a=q|b|+r,0\leqslant r<|b|$.由于只能在一个区间,所以 q 唯一,从而 r 唯一.

定理 1.2 中的 q 称为不完全商,r 称为余数.

定义 1.4 设 $a_1,a_2,\cdots,a_n\in\mathbb{Z},d|a_i,i=1,2,\cdots,n$,则称 d 是 $a_1,a_2,\cdots,a_n$ 的一个公因数,所有的公因数中最大的称为 $a_1,a_2,\cdots,a_n$ 的**最大公因数**,记作$(a_1,a_2,\cdots,a_n)$,如果$(a_1,a_2,\cdots,a_n)=1$,则称 $a_1,a_2,\cdots,a_n$ **互素**.

定理 1.3 如果 $a=bq+c$,则 $(a,b)=(b,c)$.

证明 若 $d|a,d|b$,则 $d|c=a-bq$.反过来,若 $d|b,d|c$,则 $d|a=bq+c$.所以 a,b 与 b,c 有相同的公因数集,最大者也就相同了.

定理 1.4(辗转相除法) 设 $a,b\in\mathbb{Z}^+$,则 (a,b)等于辗转相除的最后一个不等于 0 的余数 r_n.

证明 $a,b\in\mathbb{Z}^+$,则

$$\begin{aligned}
a\ &=bq_1+r_1,0<r_1<b,\\
b\ &=r_1q_2+r_2,0<r_2<r_1,\\
r_1&=r_2q_3+r_3,0<r_3<r_2,\\
&\vdots\\
r_{k-1}&=r_kq_{k+1}+r_{k+1},0<r_{k+1}<r_k,\\
&\vdots\\
r_{n-1}&=r_nq_{n+1},r_n\neq0,r_{n+1}=0.
\end{aligned}$$

由定理 1.3,得 $r_n=(0,r_n)=(r_n,r_{n-1})=\cdots=(r_2,r_1)=(r_1,b)=(b,a)=(a,b)$.

例 1.3　求(525,231).

解　将 525 和 231 辗转相除

$$\begin{array}{r|rr|l} 2 & 525 & 231 & 3 \\ & 462 & 189 & \\ \hline 1 & 63 & 42 & 2 \\ & 42 & 42 & \\ \hline & 21 & 0 & \end{array}$$

所以 $(525,231)=21$.

定理 1.5　设 $a,b\in\mathbb{Z}$且不全为 0,则存在 $x,y\in\mathbb{Z}$,使得$(a,b)=xa+yb$. 特别地,当$(a,b)=1$时,存在 $s,t\in\mathbb{Z}$使得 $sa+tb=1$.

证明　由辗转相除法向上反推即可得所证结论.

定义 1.5　正因数只有 1 和其自身的大于 1 的正整数称为素数,正因数的个数大于等于 3 的正整数称为合数.

定理 1.6　设 $a\in\mathbb{Z}$,p 是素数,则必有 $p|a$ 或$(p,a)=1$.

证明　由 $(p,a)|p$,$(p,a)=p$ 或 1,若$(p,a)=p$,由$(p,a)|a$,即 $p|a$.

推论 1.1　设 p 是素数 $p|ab$,则 $p|a$ 或 $p|b$.

证明　若 $p\nmid a$,则 $(p,a)=1$. 由定理 1.5 知,存在 s,t 使得 $sp+ta=1$,两端同时乘以 b,则得 $spb+tab=b$,于是 $p|b$.

1.2　一元多项式

定义 1.6　设 n 是一个非负整数,$a_0,a_1,\cdots,a_n$ 属于数域 F,x 是一个符号(或称文字),形式表达式

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

称为数域 F 上的一元**多项式**. a_0 称为常数项或 0 次项,a_ix^i 称为 i 次项,a_i 称为 i 次项系数,若 $a_n\neq 0$,则称 a_nx^n 为 $f(x)$的首项,a_n 称为首项系数,n 称为多项式 $f(x)$的次数,记作$\partial(f(x))$. 系数全为零的多项式 0 称为零多项式. 零多项式是唯一不定义次数的多项式.

通常用 $f(x),g(x),h(x),\cdots$或 $f,g,h,\cdots$表示多项式,这种表示方法是瑞士数学家欧拉最先使用的.

设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=\sum_{i=0}^{n}a_ix^i,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0=\sum_{j=0}^{m}b_jx^j.$$

若 $n\geqslant m$,在 $g(x)$中令 $b_n=b_{n-1}=\cdots=b_{m+1}=0$,则

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0=\sum_{j=0}^{n}b_jx^j.$$

若 $a_i=b_i(i=0,1,2,\cdots,n)$，则称 $f(x)$ 与 $g(x)$ 相等，记作 $f(x)=g(x)$.

规定加法：$f(x)+g(x)=\sum\limits_{i=0}^{n}(a_i+b_i)x^i$.

规定乘法：
$$\begin{aligned}f(x)g(x)&=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\cdots+c_1x+c_0\\&=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}+\cdots+(a_1b_0+a_0b_1)x+a_0b_0\\&=\sum_{s=0}^{n+m}\sum_{i+j=s}(a_ib_j)x^s,\end{aligned}$$

其中 s 次项 x^s 的系数为

$$c_s=a_sb_0+a_{s-1}b_1+\cdots+a_1b_{s-1}+a_0b_s=\sum_{i+j=s}a_ib_j.$$

规定 $-f(x)=\sum\limits_{i=0}^{n}(-a_i)x^i$，由此可规定 $f(x)-g(x)=f(x)+(-g(x))$.

设 $f(x),g(x)$ 为数域 F 上的任意两个多项式，则 $f(x)\pm g(x),f(x)g(x)$ 仍为数域 F 上的多项式.

定义 1.7 所有数域 F 上的一元多项式的全体称为数域 F 上的**一元多项式环**，记作 $F[x]$.

多项式的加法和乘法满足以下运算律：

(1) 加法交换律 $f(x)+g(x)=g(x)+f(x)$；

(2) 加法结合律 $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$；

(3) 乘法交换律 $f(x)g(x)=g(x)f(x)$；

(4) 乘法结合律 $(f(x)g(x))h(x)=f(x)(g(x)h(x))$；

(5) 乘法对加法的分配律 $f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$.

这里只证明乘法结合律. 设 $h(x)=\sum\limits_{k=0}^{l}c_kx^k$，则

$f(x)g(x)$ 中 s 次项的系数为 $\sum\limits_{i+j=s}a_ib_j$，

$(f(x)g(x))h(x)$ 中 t 次项的系数为 $\sum\limits_{s+k=t}\Big(\sum\limits_{i+j=s}a_ib_j\Big)c_k=\sum\limits_{i+j+k=t}a_ib_jc_k$，

$g(x)h(x)$ 中 r 次项的系数为 $\sum\limits_{j+k=r}b_jc_k$.

$f(x)(g(x)h(x))$ 中 t 次项的系数为 $\sum\limits_{i+r=t}a_i\Big(\sum\limits_{j+k=r}b_jc_k\Big)=\sum\limits_{i+j+k=t}a_ib_jc_k$，从而得证.

多项式的加法和乘法关于次数有下面的结论.

定理 1.7 若 $f(x)\neq0,g(x)\neq0$，则：

(1) $f(x)g(x)\neq0$，且 $\partial(f(x)g(x))=\partial(f(x))+\partial(g(x))$；

(2) 当 $f(x)+g(x)\neq0$，$\partial(f(x)+g(x))\leqslant\max\{\partial(f(x)),\partial(g(x))\}$.

证明 (1) 设 $\partial(f(x))=n,\partial(g(x))=m$，$f(x)$ 的首项系数 $a_n\neq0$，$g(x)$ 的首项系数

$b_m \neq 0$，则 $f(x)g(x)$ 的首项系数 $a_n b_m \neq 0$，所以

$$\partial(f(x)g(x)) = \partial(f(x)) + \partial(g(x)).$$

(2) 不妨设 $m \leqslant n$，则 $f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i$. 当 x^n 项系数 $a_n+b_n=0$ 时，$\partial(f(x)+g(x))<\max\{\partial(f(x)),\partial(g(x))\}$；当 x^n 项系数 $a_n+b_n\neq 0$ 时，$\partial(f(x)+g(x))=\max\{\partial(f(x)),\partial(g(x))\}$.

推论 1.2　$f(x)g(x)=0$ 的充要条件是 $f(x)=0$ 或 $g(x)=0$.

推论 1.3　若 $f(x)g(x)=f(x)h(x)$，$f(x)\neq 0$，则 $g(x)=h(x)$.

证明　由 $f(x)g(x)=f(x)h(x)$，得 $f(x)(g(x)-h(x))=0$. 而 $f(x)\neq 0$，由推论 1.2 得 $g(x)-h(x)=0$，从而 $g(x)=h(x)$，这说明数域上多项式乘法适合消去律.

例 2.1　设 $f(x),g(x),h(x)\in\mathbb{R}[x]$. 证明：若 $f^2(x)=xg^2(x)+xh^2(x)$，则 $f(x)=g(x)=h(x)=0$.

证明　若 $f(x)\neq 0$，则 $x(g^2(x)+h^2(x))=f^2(x)\neq 0$，从而 $g^2(x)+h^2(x)\neq 0$. 于是 $\partial(xg^2(x)+xh^2(x))=\partial(x(g^2(x)+h^2(x)))$ 为奇数. 但 $\partial(f^2(x))$ 为偶数. 所以 $x(g^2(x)+h^2(x))\neq f^2(x)$，这与已知矛盾. 故 $f(x)=0$，从而 $g^2(x)+h^2(x)=0$. 又 $f(x),g(x)$ 均为实系数多项式，必有 $g(x)=h(x)=0$. 从而 $f(x)=g(x)=h(x)=0$.

该结论在复数域$\mathbb{C}$上不成立. 如取 $f(x)=0,g(x)=\mathrm{i}x,h(x)=x$，即有 $f^2(x)=xg^2(x)+xh^2(x)$.

1.3　整除的概念

这一节以后的讨论都是在某一固定的数域 F 上的一元多项式环 $F[x]$ 中进行的，在一元多项式环中，可以作加、减、乘三种运算，但是乘法的逆运算除法并不是普遍可以做的，因此多项式的整除理论就成了多项式理论的一个重要内容.

定义 1.8　设 $f(x),g(x)\in F[x]$，若存在 $h(x)\in F[x]$ 使 $f(x)=g(x)h(x)$，则称 $g(x)$ **整除** $f(x)$，记作 $g(x)\mid f(x)$，这时，$g(x)$ 称为 $f(x)$ 的**因式**，$f(x)$ 称为 $g(x)$ 的倍式.

如果 $g(x)\neq 0$，则 $g(x)$ 除 $f(x)$ 所得的商可表示成 $\frac{f(x)}{g(x)}$.

定义中允许 $g(x)=0$，此时有 $0=0h(x)$，$\forall h(x)\in F[x]$. $g(x)$ 不能整除 $f(x)$ 时记作 $g(x)\nmid f(x)$.

和中学所学代数一样，作为形式表达式，也能用一个多项式去除另一个多项式，求得商和余式，即有带余除法.

定理 1.8　对 $\forall f(x),g(x)\in F[x]$，$g(x)\neq 0$，存在 $q(x),r(x)\in F[x]$，使

$$f(x)=q(x)g(x)+r(x)，其中\partial(r(x))<\partial(g(x))或 r(x)=0，$$

并且这样的 $q(x),r(x)$ 是唯一的.

证明 若 $f(x)=0$ 或 $\partial(f(x))<\partial(g(x))$，则令 $q(x)=0, r(x)=f(x)$，结论成立.

若 $f(x)\neq 0$ 或 $\partial(f(x))=n\geqslant\partial(g(x))=m$，设

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0=\sum_{i=0}^{n}a_i x^i,$$

$$g(x)=b_m x^m+b_{m-1}x^{m-1}+\cdots+b_1 x+b_0=\sum_{j=0}^{m}b_j x^j.$$

对 $f(x)$ 的次数 n 作数学归纳法. 若 $n=0$，则 $m=0$ 且 $b_0\neq 0$，$f(x)=a_0=\dfrac{a_0}{b_0}\cdot b_0+0$，结论成立.

假设当次数小于 n 时，结论成立.

现在来看 $f(x)$ 次数为 n 的情形. 这时 $f(x)$ 的首项为 ax^n，$g(x)$ 的首项为 $bx^m(n\geqslant m)$，则 $b^{-1}ax^{n-m}g(x)$ 与 $f(x)$ 有相同的首项，因而，多项式 $f_1(x)=f(x)-b^{-1}ax^{n-m}g(x)$ 的次数小于 n 或 $f_1(x)$ 为 0. 若 $f_1(x)=0$，令 $q(x)=b^{-1}ax^{n-m}$，$r(x)=0$ 即可；若 $\partial(f_1(x))<n$，由归纳假设，存在 $q_1(x), r_1(x)$ 使得 $f_1(x)=q_1(x)g(x)+r_1(x)$，其中 $\partial(r_1(x))<\partial(g(x))$ 或者 $r_1(x)=0$，于是

$$f(x)=b^{-1}ax^{n-m}g(x)+f_1(x)=(b^{-1}ax^{n-m}+q_1(x))g(x)+r_1(x),$$

即有

$$q(x)=b^{-1}ax^{n-m}+q_1(x), r(x)=r_1(x) \quad \text{使} \quad f(x)=q(x)g(x)+r(x).$$

由数学归纳法原理，存在性成立.

再证唯一性.

若还有 $f(x)=q'(x)g(x)+r'(x)$，其中 $\partial(r'(x))<\partial(g(x))$ 或 $r'(x)=0$，则

$q(x)g(x)+r(x)=q'(x)g(x)+r'(x)$，即 $(q(x)-q'(x))g(x)=r'(x)-r(x)$.

若 $r'(x)-r(x)\neq 0$，则 $q(x)-q'(x)\neq 0$，

$\partial(q(x)-q'(x))+\partial(g(x))\geqslant\partial(g(x))>\max\{\partial(r'(x)),\partial(r(x))\}\geqslant\partial(r'(x)-r(x))$，

矛盾. 所以 $r'(x)=r(x)$，从而 $q(x)=q'(x)$. 唯一性得证.

$q(x)$ 称为 $g(x)$ 除 $f(x)$ 的商式，$r(x)$ 称为余式.

例 3.1 设 $f(x)=3x^3+4x^2-5x+6$， $g(x)=x^2-3x+1$，求 $g(x)$ 除 $f(x)$ 的商式和余式.

解 用普通除法 $f(x)=(3x+13)g(x)+(31x-7)$，从而得 $q(x)=3x+13$，$r(x)=31x-7$.

定理 1.9 当 $g(x)\neq 0$ 时，$g(x)\mid f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式 $r(x)=0$.

整除具有以下性质：

(1) 若 $g(x)\mid f(x)$，$f(x)\mid g(x)$，则 $f(x)=cg(x)$，$c\neq 0$.

事实上，若 $f(x)=0$，则 $g(x)=0$，$f(x)=g(x)$；若 $f(x)\neq 0$，由 $f(x)\mid g(x)$，$\exists h_1(x)$ 使得 $g(x)=f(x)h_1(x)$；由 $g(x)\mid f(x)$，$\exists h_2(x)$ 使得 $f(x)=g(x)h_2(x)$. 于是 $f(x)=$

$h_1(x)h_2(x)f(x)$，从而 $h_1(x)h_2(x)=1$，故 $\partial(h_1(x))+\partial(h_2(x))=0$，即 $\partial(h_1(x))=\partial(h_2(x))=0$，因此 $h_1(x)$，$h_2(x)$皆为非零常数，故有 $f(x)=cg(x)$，$c\neq 0$.

(2) 若 $f(x)\mid g(x)$，$g(x)\mid h(x)$，则 $f(x)\mid h(x)$.

事实上，由 $g(x)=f(x)u(x)$，$h(x)=g(x)v(x)$，得

$$h(x)=(f(x)u(x))v(x)=f(x)(u(x)v(x)).$$

(3) 若 $f(x)\mid g_i(x)(i=1,2,\cdots,k)$，则对 $\forall\, u_i(x)\in F[x](i=1,2,\cdots,k)$，有

$$f(x)\mid(u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_k(x)g_k(x)).$$

(4) 若 $0\neq c\in F$，$\forall\, f(x)\in F[x]$，$c\mid f(x)$.

两个多项式的整除关系不会因系数域的扩大而改变. 但这个论断在数环上的多项式不一定成立，例如，在$\mathbb{Z}[x]$中，$2x$ 不整除 x^2.

1.4　最大公因式

设 F 是数域，$F[x]$是 F 上的一元多项式环，$f(x)$，$g(x)$，$h(x)\in F[x]$，若 $h(x)\mid f(x)$ 且 $h(x)\mid g(x)$，则称 $h(x)$是 $f(x)$，$g(x)$的一个公因式.

任意非零常数是 $f(x)$，$g(x)$的一个公因式，因此公因式是存在的.

定义 1.9　称 $d(x)$是 $f(x)$与 $g(x)$的一个**最大公因式**，如果

(1) $d(x)\mid f(x)$，$d(x)\mid g(x)$；

(2) 若 $h(x)\mid f(x)$，$h(x)\mid g(x)$，则 $h(x)\mid d(x)$.

$f(x)$与 $g(x)$的首项系数为 1 的最大公因式记作 $(f(x),g(x))$.

下面的讨论将证明最大公因式的存在性并给出求法. 我们还将看到最大公因式不是唯一的，任意两个多项式 $f(x)$与 $g(x)$的最大公因式相差一个非零常数倍，但首项系数为 1 的最大公因式是唯一的.

引理 1.1　设 $f(x)=q(x)g(x)+r(x)$，则 $f(x)$，$g(x)$与 $g(x)$，$r(x)$有相同的公因式，从而 $(f(x),g(x))=(g(x),r(x))$.

证明　如果 $d(x)\mid f(x)$，$d(x)\mid g(x)$，则 $d(x)\mid r(x)=f(x)-q(x)g(x)$，这就是说，$f(x)$，$g(x)$的公因式一定是 $g(x)$，$r(x)$的公因式.

如果 $d(x)\mid g(x)$，$d(x)\mid r(x)$，则 $d(x)\mid f(x)=q(x)g(x)+r(x)$，这就是说，$g(x)$，$r(x)$的公因式一定是 $f(x)$，$g(x)$的公因式.

再由最大公因式定义知，$f(x)$，$g(x)$的最大公因式与 $g(x)$，$r(x)$的最大公因式相互整除，因此$(f(x),g(x))=(g(x),r(x))$.

定理 1.10　对于 $F[x]$中任意两个多项式 $f(x)$与 $g(x)$，一定存在最大公因式 $d(x)$，且 $\exists\, u(x)$，$v(x)\in F[x]$ 使得 $d(x)=u(x)f(x)+v(x)g(x)$.

证明　如果 $g(x)=0$，则 $f(x)$就是 $f(x)$与 $g(x)$一个最大公因式，且

$$f(x)=1\cdot f(x)+0\cdot g(x).$$