高等代数简明教程

GAODENG DAISHU JIANMING JIAOCHENG

主　编◎阳庆节

中国人民大学出版社

高等代数简明教程

GAODENG DAISHU JIANMING JIAOCHENG

主　编◎阳庆节
编写者◎戚发全　孙大英　魏二玲

中国人民大学出版社
·北京·

图书在版编目（CIP）数据

高等代数简明教程/阳庆节主编.
北京：中国人民大学出版社，2010
ISBN 978-7-300-12671-5

Ⅰ. ①高…
Ⅱ. ①阳…
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（2010）第 174705 号

高等代数简明教程
主编　阳庆节
Gaodeng Daishu Jianming Jiaocheng

出版发行	中国人民大学出版社		
社　　址	北京中关村大街 31 号	**邮政编码**	100080
电　　话	010－62511242（总编室）	010－62511398（质管部）	
	010－82501766（邮购部）	010－62514148（门市部）	
	010－62515195（发行公司）	010－62515275（盗版举报）	
网　　址	http://www.crup.com.cn		
	http://www.ttrnet.com(人大教研网)		
经　　销	新华书店		
印　　刷	北京鑫丰华彩印有限公司		
规　　格	185 mm×260 mm　16 开本	**版　　次**	2010 年 9 月第 1 版
印　　张	18.75	**印　　次**	2010 年 9 月第 1 次印刷
字　　数	436 000	**定　　价**	28.00 元

前 言

高等代数是一门基础理论课。近年来，由于自然科学和工程技术的迅速发展，特别是由于电子计算机的普遍使用，使得代数学得到日益广泛的应用。这就要求计算机、信息、统计、经济学、金融工程等专业的学生不仅要了解代数学的一些计算问题，还应具备代数学的基础理论知识，以便融会贯通地运用代数学的工具去解决理论上和实践中遇到的各种问题。编者结合多年从事高等代数课程教学的体会和经验，编写了这本教材的讲义，目的是为计算机、信息、统计、经济学、金融工程等相关专业提供一本适用的高等代数教科书，试用多年，师生反应不错。我们根据这几年的教学过程师生提供的反馈信息，对讲义内容进行了修改，形成了今天呈现给读者的这一版本教材。

在编写过程中，我们借鉴了国内外一些优秀教材的思想、处理方法和编排体例，注重理论与应用相结合，叙述上由浅入深，使初学者能快速入门，进而深入掌握高等代数的基本理论和方法。本教材以线性方程组作为引子，以矩阵作为贯穿全书的主线，详细介绍了高等代数中的基本概念和基本思想。本书的前四章是高等代数的基础篇，内容包括一元多项式理论、线性方程组理论、矩阵代数和行列式；后四章则是高等代数的核心篇，主要介绍了线性空间、欧氏空间、矩阵可对角化问题及二次型化简等内容。本书渗透了现代数学的思想和观点，在概念引入、理论分析和例题演算等环节尽量体现代数和几何的联系，使学生能够通过几何背景理解代数概念的来龙去脉，并找到分析和解决代数问题的方法。本书还介绍了高等代数在其他学科中的一些应用。本书的每一节都配有一定的习题，书后附有习题提示与参考答案。同时，还将配套出版辅导教材《高等代数简明教程学习指导》。

全书共八章，各章之间既相对独立又紧密联系。前四章供第一学期使用，后四章供第二学期使用。根据高等代数课程的基本要求，全年共 108 学时加上 36 课时的习题课可以讲完全部内容。如果课时紧张，加 $*$ 号的章节可以作为选学内容。我们建议，具体的课时安排如下：第一章 10 学时，第二章 16 学时，第三章 16 学时，第四章 12 学时，第五章 12 学时，第六章 16 学时，第七章 12 学时，第八章 14 学时。实际使用时也可以根据需要进行调整。

本书由阳庆节主编，第一、五章由威发全撰写，第三章由魏二玲撰写，第四、六章由孙大英撰写，第二、七、八章由阳庆节撰写。中国人民大学数学系的许多老师对本书的初稿进行了讨论，提出了许多宝贵的建议。对此我们表示衷心感谢。

本书的正式出版得到了中国人民大学出版社编辑潘旭燕、刘冬的热情支持和帮助，在此一并表示感谢。

由于编者水平有限，书中内容结构可能会有不当之处，真诚欢迎读者批评指正。

编 者

2010 年 7 月

目 录

第一章　多项式

多项式是中学代数课程的一项主要内容, 也是代数学中一个最基本的对象, 在数学以及实际应用中都会碰到. 因此有必要比较系统地对其进行学习. 本章将介绍多项式的概念, 研究整除性理论和因式分解的问题, 对在中学所学的相关知识作加深和推广.

§1.1　数域

数是数学中一个最基本的概念. 数的发展, 大体上经历了从开始接触数时的自然数, 到整数, 再到有理数、实数、复数, 这样一个渐进的认识过程. 为方便起见, 我们一般用 $\mathbf{N}$ 表示所有自然数, $\mathbf{Z}$ 表示所有整数, $\mathbf{Q}$ 表示所有有理数, $\mathbf{R}$ 表示所有实数, $\mathbf{C}$ 表示所有复数.

按照所研究问题的不同, 我们常常需要界定数的不同范围. 在数的不同范围内对同一个问题的回答可能是不同的. 例如, 一个二次方程有没有解与所考虑的取值范围有关; 又如, 在整数范围内, 并不是总可以作除法的, 这是因为任意两个整数的商不一定是整数. 由一些数组成的集合称为数集. 我们知道, 不同的数集会具有一些不同的性质, 但在代数学中经常将有共同性质的对象进行统一的讨论. 加、减、乘、除四则运算是数与数之间的基本运算关系. 在一个数集中能否进行四则运算是我们要考虑的基本性质. 为此, 我们引入数域的概念.

定义 1.1　设 P 是一个由一些复数组成的集合, 其中包含 0 和 1. 如果 P 中的任意两个数作加、减、乘、除（除数不能为零）运算的结果仍在 P 中, 则称 P 是一个**数域(number field)**.

例如, 上面提到的有理数集 $\mathbf{Q}$, 实数集 $\mathbf{R}$, 复数集 $\mathbf{C}$ 都是数域. 而自然数集 $\mathbf{N}$ 和整数集 $\mathbf{Z}$ 不是数域.

如果数集 P 中任意两个数作某种运算的结果仍然在 P 中, 则称数集 P 对这种运算是**封闭的(closed)**. 例如, 自然数集 $\mathbf{N}$ 只对加法和乘法封闭, 整数集 $\mathbf{Z}$ 对加、减、乘封闭, 而我们常用的有理数域 $\mathbf{Q}$, 实数域 $\mathbf{R}$ 和复数域 $\mathbf{C}$ 对加、减、乘、除（除数不能为零）都是封闭的, 或者说对四则运算封闭. 根据定义, 一个数域就是一个复数集的子集, 它包含 $0, 1$, 且对四则运算封闭.

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

证明　显然, $0 = 0 + 0\sqrt{2}$, $1 = 1 + 0\sqrt{2} \in \mathbf{Q}(\sqrt{2})$.

现在来证明封闭性. 对任意 $a_1 + b_1\sqrt{2}$, $a_2 + b_2\sqrt{2} \in \mathbf{Q}(\sqrt{2})$, 由于 $a_1, a_2, b_1, b_2 \in \mathbf{Q}$, 我们有,

$$(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2} \in \mathbf{Q}(\sqrt{2}),$$
$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbf{Q}(\sqrt{2}),$$

所以 $\mathbf{Q}(\sqrt{2})$ 对加法、减法和乘法是封闭的.

再看除法. 设 $a_2+b_2\sqrt{2}\neq 0$, 由于 $\sqrt{2}\notin\mathbf{Q}$, $a_2-b_2\sqrt{2}\neq 0$, 所以

$$\frac{a_1+b_1\sqrt{2}}{a_2+b_2\sqrt{2}}=\frac{(a_1+b_1\sqrt{2})(a_2-b_2\sqrt{2})}{(a_2+b_2\sqrt{2})(a_2-b_2\sqrt{2})}=\frac{a_1a_2-2b_1b_2}{a_2^2-2b_2^2}+\frac{a_2b_1-a_1b_2}{a_2^2-2b_2^2}\sqrt{2}\in\mathbf{Q}(\sqrt{2}),$$

即 $\mathbf{Q}(\sqrt{2})$ 对除法也封闭.

这就证明了 $\mathbf{Q}(\sqrt{2})$ 是一个数域. □

例 1.2 设 F 是至少包含两个数的数集, 如果 F 对四则运算封闭, 证明 F 是一个数域.

证明 我们只要证明 F 中含有 0 和 1 就可以了.

因为 F 中至少含有两个数, 设这两数为 a, b, 其中必有一个不为 0, 不妨设 $a\neq 0$, 那么, 由于 F 对减法和除法封闭, $a-a=0$, $\frac{a}{a}=1\in F$, 故 F 是一个数域. □

命题 1.1 任意数域 P 都包含有理数域 $\mathbf{Q}$ 作为其子域, 即满足 $P\supset\mathbf{Q}$.

证明 首先由于 P 是数域, 故 $1\in P$. 而 P 对加法封闭, 于是任意正整数 $n=1+1+\cdots+1\in P$. 又因 $0\in P$, 由 P 对减法封闭, 得 $-n=0-n\in P$, 所以 $P\supset\mathbf{Z}$. 最后由于 P 对除法封闭, P 包含任意两个整数(除数不为零)的商. 因此 $P\supset\mathbf{Q}$. □

习题 1.1

1. 下列数集哪些是数域? 哪些不是?
   (1) $P_1=\{a+b\sqrt{3}\mathrm{i}\,|\,a,b\in\mathbf{Q}\}$;
   (2) $P_2=\{a+b\mathrm{i}\,|\,a,b\in\mathbf{Q}\}$;
   (3) $P_3=\{a+b\mathrm{i}\,|\,a\in\mathbf{Q},b\in\mathbf{R}\}$;
   (4) $P_4=\{a+b\sqrt{3}\mathrm{i}\,|\,a,b\in\mathbf{Z}\}$;
   (5) $P_5=\{a+b\sqrt[3]{2}\,|\,a,b\in\mathbf{Q}\}$.

§1.2 一元多项式

我们将在一个给定的数域 P 上来讨论多项式.

一、基本概念

设 P 是一个数域, x 是一个符号(或称文字).

定义 1.2 设 n 是一个非负整数, 形式表达式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \tag{1.1}$$

其中 $a_i\in P\,(i=0,1,\ldots,n)$, 称为**系数在数域 P 中的一元多项式(one variable polynomial)**, 简称为数域 P 上的多项式.

一般用 $f(x)$, $g(x)$, ... 或 f, g, ... 来表示多项式.

在多项式 (1.1) 中, a_0 称为**零次项或常数项(constant)**; a_ix^i 称为 **i 次项(ith term)**, 而 a_i 则称为 i 次项的**系数(coefficient)**; 如果最高次项系数 $a_n\neq 0$, 则 a_nx^n 称为多项式 (1.1) 的

首项(leading term)，a_n 称为**首项系数(leading coefficient)**，而 n 称为多项式 (1.1) 的**次数(degree)**. 首项系数为 1 的多项式称为**首一多项式(monic polynomial)**.

系数全部为零的多项式称为**零多项式(zero polynomial)**,记为 0. 零多项式没有次数. 当我们谈到多项式 $f(x)$ 的次数时, 总假定 $f(x)\neq 0$. 多项式 $f(x)$ 的次数记为 $\partial(f(x))$.

注记 这里多项式是符号 x 的形式表达式, x 是未知量只是一种特殊情形, x 还可以是在第三章将介绍的方阵（此时称为矩阵多项式）, 也可以是第五章要讲的线性变换（此时称为线性变换多项式）, 还可以是数学分析中的高阶导数. 我们抽象地定义多项式并引入运算, 以便统一地研究上述对象具有的普遍的公共性质.

思考题 零多项式与零次多项式有什么区别?

在介绍多项式的运算之前, 先定义多项式相等的概念.

定义 1.3 数域 P 上的两个多项式 $f(x)$ 与 $g(x)$, 如果它们的同次项系数都相等, 则称**两个多项式相等**, 记为 $f(x)=g(x)$.

二、多项式的运算

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 P 上的两个多项式, 简记为 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$, $g(x)=\sum\limits_{j=0}^{m}b_jx^j$.

1. 多项式的加法和减法

不妨设 $n\geq m$, 这时令 $b_n=b_{n-1}=\cdots=b_{m+1}=0$, 我们称多项式

$$(a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\cdots+(a_1+b_1)x+(a_0+b_0)=\sum_{i=0}^{n}(a_i+b_i)x^i$$

为 $f(x)$ 与 $g(x)$ 的**和**, 记为 $f(x)+g(x)$.

简单地说, 两个多项式作加法, 就是合并同次项.

例 1.3 设 $f(x)=2x^2+3x-1$, $g(x)=x^3+2x^2-3x+2$, 则

$$f(x)+g(x)=(0+1)x^3+(2+2)x^2+(3-3)x+(-1+2)=x^3+4x^2+1.$$

类似地, 不难给出多项式减法的定义: $f(x)$ 与 $g(x)$ 的**差**为

$$f(x)-g(x)=\sum_{i=0}^{n}(a_i-b_i)x^i.$$

2. 多项式的乘法

多项式 $f(x)$ 与 $g(x)$ 的**积** $f(x)g(x)$ 定义为多项式

$$a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}+\cdots+(a_1b_0+a_0b_1)x+a_0\,b_0=\sum_{k=0}^{n+m}c_kx^k,$$

其中 k 次项的系数 c_k 为下标之和为 k 的 a_i 与 b_j 的乘积之和, 即

$$c_k=a_kb_0+a_{k-1}b_1+\cdots+a_1b_{k-1}+a_0b_k=\sum_{i+j=k}a_ib_j.$$

例 1.4 设 $f(x)=2x^2+3x-1$, $g(x)=x^3+2x^2-3x+2$, 计算 $f(x)g(x)$.

解　对于具体的两个多项式的乘积, 我们可以用竖式计算:

$$\begin{array}{rl} & f(x)=2x^2+3x\ -1 \\ \times) & g(x)=\ x^3+2x^2-3x\ +2 \\ \hline & 2x^5+3x^4-\ x^3 \\ & \qquad 4x^4+6x^3-2x^2 \\ & \qquad\quad -6x^3-9x^2+3x \\ & \qquad\qquad\quad 4x^2+6x-2 \\ \hline & 2x^5+7x^4-\ x^3-7x^2+9x-2 \end{array}$$

所以 $f(x)g(x)=2x^5+7x^4-x^3-7x^2+9x-2$. □

可见, 这里多项式的加法、减法和乘法与中学里多项式的加法、减法和乘法是完全一致的. 显然, 数域 P 上两个多项式经过加、减、乘等运算后, 所得的多项式仍是数域 P 上的多项式.

不难证明, 运算后的次数满足如下结论.

命题 1.2　对于多项式的加减法,

$$\partial\big(f(x)\pm g(x)\big)\le\max\{\partial\big(f(x)\big),\partial\big(g(x)\big)\}. \tag{1.2}$$

如果 $f(x)\neq 0$, $g(x)\neq 0$, 那么, $f(x)g(x)\neq 0$, 且

$$\partial\big(f(x)g(x)\big)=\partial\big(f(x)\big)+\partial\big(g(x)\big). \tag{1.3}$$

三、多项式的运算规律

多项式的运算具有下列性质:

(1) 加法交换律: $f(x)+g(x)=g(x)+f(x)$.

(2) 加法结合律: $\big(f(x)+g(x)\big)+h(x)=f(x)+\big(g(x)+h(x)\big)$.

(3) 加法消去律: 若 $f(x)+g(x)=f(x)+h(x)$, 那么 $g(x)=h(x)$.

(4) 乘法交换律: $f(x)g(x)=g(x)f(x)$.

(5) 乘法结合律: $\big(f(x)g(x)\big)h(x)=f(x)\big(g(x)h(x)\big)$.

(6) 分配律: $f(x)\big(g(x)+h(x)\big)=f(x)g(x)+f(x)h(x)$.

(7) 乘法消去律: 若 $f(x)g(x)=f(x)h(x)$, 且 $f(x)\neq 0$, 那么 $g(x)=h(x)$.

以上运算规律不难直接用定义证明. 下面我们证明乘法消去律.

证明　因为 $f(x)g(x)=f(x)h(x)$, 有

$$f(x)(g(x)-h(x))=0.$$

而 $f(x)\neq 0$, 由命题 1.2, 得 $g(x)-h(x)=0$, 故 $g(x)=h(x)$. □

最后, 我们引入一个术语.

定义 1.4　系数在数域 P 中的一元多项式全体组成的集合称为数域 P 上的**一元多项式环(one variable polynomial ring)**, 记为 $P[x]$, P 称为 $P[x]$ 的**系数域(coefficient field)**.

习题 1.2

1. 计算 $(x^2+ax-b)(x^2-1)+(x^2-ax+b)(x^2+1)$.

2. 设 $f(x)=3x^2-5x+3$, $g(x)=ax(x-1)+b(x+2)(x-1)+cx(x+2)$, 确定 a, b, c 的值使 $f(x)=g(x)$.
3. 设 $f(x)$ 和 $g(x)$ 是两个非零多项式, $f(x),g(x)$ 的系数满足什么条件时, 次数不等式 $\partial(f(x)+g(x))\leq\max\{\partial(f(x)),\partial(g(x))\}$ 中的等号成立? 满足什么条件时, 小于号成立?
4. 设 $f(x),g(x)$ 和 $h(x)$ 都是实系数多项式, 如果 $f^2(x)=xg^2(x)+xh^2(x)$, 证明 $f(x)=g(x)=h(x)=0$.
5. 证明: 多项式

$$f(x)=(x^{50}-x^{49}+x^{48}-x^{47}+\cdots+x^2-x+1)(x^{50}+x^{49}+\cdots+x+1)$$

的展开式中没有奇数次项.

§1.3 整除性

一、带余除法

前面我们给出了一元多项式的加法、减法、乘法运算, 这些运算在一元多项式环 $P[x]$ 中是封闭的. 多项式之间有没有除法呢? 也就是当 $g(x)\neq 0$ 时, $\frac{f(x)}{g(x)}$ 还是不是多项式呢? 答案是否定的. 但是, 我们可以得到以下定理.

定理 1.1 [带余除法(division with remainder)] 对于 $P[x]$ 中的任意两个多项式 $f(x)$, $g(x)$, 其中 $g(x)\neq 0$, 一定存在 $P[x]$ 中的多项式 $q(x)$, $r(x)$ 使得

$$f(x)=g(x)q(x)+r(x), \tag{1.4}$$

其中 $\partial\big(r(x)\big)<\partial\big(g(x)\big)$ 或者 $r(x)=0$, 并且这样的 $q(x)$, $r(x)$ 是唯一确定的.

证明 *存在性* 若 $f(x)=0$ 或 $\partial\big(f(x)\big)<\partial\big(g(x)\big)$, 这时, 取 $q(x)=0$, $r(x)=f(x)$ 即可.

下面假设 $f(x)\neq 0$, $n\geq m$, 其中 $n=\partial\big(f(x)\big)$, $m=\partial\big(g(x)\big)$. 我们对 n 作第二数学归纳法.

当 $n=0$ 时, $m=0$, 存在性显然成立. 假设当 $f(x)$ 的次数小于 n 时存在性成立.

当次数为 n 时, 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, 记

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

则 $\partial\big(f_1(x)\big)<n$. 由归纳假设, 对 $f_1(x)$, $g(x)$ 来说, 存在 $q_1(x)$, $r_1(x)$ 使

$$f_1(x)=g(x)q_1(x)+r_1(x),$$

其中 $\partial\big(r_1(x)\big)<\partial\big(g(x)\big)$ 或者 $r_1(x)=0$, 所以

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

取 $q(x)=q_1(x)+b^{-1}ax^{n-m}$, $r(x)=r_1(x)$ 即满足

$$f(x)=g(x)q(x)+r(x).$$

所以根据数学归纳法原理, 存在性成立.

唯一性　设 $f(x)=g(x)q_1(x)+r_1(x)$，且 $\partial(r_1(x))<\partial(g(x))$ 或者 $r_1(x)=0$ 也成立. 这样有

$$g(x)q_1(x)+r_1(x)=g(x)q(x)+r(x),$$

所以 $(q(x)-q_1(x))g(x)=r_1(x)-r(x)$.

如果 $q(x)\neq q_1(x)$，由于 $g(x)\neq 0$，$r_1(x)-r(x)\neq 0$，得

$$\partial(q(x)-q_1(x))+\partial(g(x))=\partial(r_1(x)-r(x)),$$

与 $\partial(g(x))>\partial(r_1(x)-r(x))$ 矛盾. 所以 $q(x)=q_1(x)$，从而 $r(x)=r_1(x)$. □

在上面的带余除法中，$q(x)$ 称为 $g(x)$ 除 $f(x)$ 的**商式(quotient)**，$r(x)$ 称为 $g(x)$ 除 $f(x)$ 的**余式(remainder)**. 证明的过程提供了一个计算商和余式的方法. 我们举例说明.

例 1.5　$f(x)=3x^3+4x^2-5x+6, g(x)=x^2-3x+1$，求 $g(x)$ 除 $f(x)$ 的商式和余式.

解　我们把计算过程用竖式除法表示. 将被除式写在中间，除式写在左边，而商写在右边，最下面得到的就是余式:

x^2-3x+1	$3x^3$	$+4x^2$	$-5x$	$+6$	$3x+13$
	$3x^3$	$-9x^2$	$+3x$		
		$13x^2$	$-8x$	$+6$	
		$13x^2$	$-39x$	$+13$	
			$31x$	-7	

所以，商式为 $q(x)=3x+13$，余式为 $r(x)=31x-7$，即

$$3x^3+4x^2-5x+6=(3x+13)(x^2-3x+1)+31x-7.$$ □

二、整除

定义 1.5　对于数域 P 上的多项式 $f(x)$，$g(x)$，如果存在 P 上的多项式 $h(x)$ 使得

$$f(x)=g(x)h(x)$$

成立，则称 $g(x)$ **整除(divide exactly)** $f(x)$，记为 $g(x)\,|\,f(x)$；否则用 $g(x)\nmid f(x)$ 表示.

若 $g(x)\,|\,f(x)$，则 $g(x)$ 称为 $f(x)$ 的**因式(factor)**，而 $f(x)$ 称为 $g(x)$ 的**倍式(multiple)**.

当 $g(x)\neq 0$ 时，带余除法给出了整除性的一个判别法.

定理 1.2　对于多项式环 $P[x]$ 中的任意两个多项式 $f(x)$，$g(x)$，其中 $g(x)\neq 0$，则 $g(x)\,|\,f(x)$ 的充要条件为 $g(x)$ 除 $f(x)$ 的余式为零.

注记　(1) 在带余除法中 $g(x)$ 必须是非零多项式，而在整除概念中未作要求. 我们可以有 $0\,|\,f(x)$，但此时一定有 $f(x)=0\cdot h(x)=0$.

(2) 当 $g(x)\,|\,f(x)$ 时，若 $g(x)\neq 0$，那么 $g(x)$ 除 $f(x)$ 所得的商 $q(x)$ 也记为 $\dfrac{f(x)}{g(x)}$.

(3) 任意 $f(x)\,|\,f(x)$，因为 $f(x)=f(x)\cdot 1$.

(4) 任意 $f(x)\,|\,0$，因为 $0=f(x)\cdot 0$.

(5) 对 P 中任意 $a\neq 0$ 和任意 $f(x)\in P[x]$，有 $a\,|\,f(x)$. 事实上，$f(x)=a\big(a^{-1}f(x)\big)$.

下面介绍关于整除的几个性质.

性质 1 若 $g(x)\,|\,f(x)$, $f(x)\,|\,g(x)$, 则 $f(x)=cg(x)$, 其中 c 是一个非零常数, 即 $f(x)$ 与 $g(x)$ 至多相差一个非零常数倍.

证明 由于 $g(x)\,|\,f(x)$, 存在 $h_1(x)$ 使 $f(x)=g(x)h_1(x)$; 同理, $g(x)=f(x)h_2(x)$. 于是

$$f(x)=f(x)h_1(x)h_2(x).$$

若 $f(x)=0$, 则 $g(x)=0$, 结论成立; 若 $f(x)\neq 0$, 由消去律有

$$h_1(x)h_2(x)=1,$$

从而 $\partial\big(h_1(x)\big)+\partial\big(h_2(x)\big)=0$. 所以, $\partial\big(h_1(x)\big)=0$, 故 $h_1(x)=c$ 为非零常数. 结论亦成立. □

性质 2 （传递性） 若 $f(x)\,|\,g(x)$, $g(x)\,|\,h(x)$, 则 $f(x)\,|\,h(x)$.

证明 由假设, 有 $g(x)=f(x)g_1(x)$, $h(x)=g(x)h_1(x)$, 于是得 $h(x)=f(x)\big(g_1(x)h_1(x)\big)$. 故 $f(x)\,|\,h(x)$. □

性质 3 若 $f(x)\,|\,g_i(x)$, $i=1,2,\cdots,r$, 那么

$$f(x)\,|\,(u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x)),$$

其中 $u_i(x)(i=1,2,\cdots,r)$ 是数域 P 上的任意多项式, 右边的多项式

$$u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x)$$

称为 $g_1(x),g_2(x),\cdots g_r(x)$ 的一个**组合**.

证明留给读者完成.

习题 1.3

1. 用 $g(x)$ 去除 $f(x)$, 求商式 $q(x)$ 和 $r(x)$:
   (1) $f(x)=x^4+4x^2-x+6$, $g(x)=x^2+x+1$;
   (2) $f(x)=x^3+3x^2-x-1$, $g(x)=3x^2-2x+1$.
2. m, p, q 满足什么条件时, 有
   (1) $(x^2+mx+1)\,|\,x^3+px+q$; (2) $(x^2+mx+1)\,|\,x^4+px^2+q$.
3. 设 $f_1(x),f_2(x),g_1(x),g_2(x)$ 是四个多项式, 并且

   $$g_1(x)g_2(x)\,|\,f_1(x)f_2(x),\qquad f_1(x)\neq 0.$$

   试证: 若 $f_1(x)\,|\,g_1(x)$, 则 $g_2(x)\,|\,f_2(x)$.
4. 证明: $(x^d-1)\,|\,(x^n-1)$ 的充分必要条件是 $d\,|\,n$.
5. 证明: 多项式 $g(x)=1+x^2+x^4+\cdots+x^{2n}$ 能整除

   $$f(x)=1+x^4+x^8+\cdots+x^{4n}$$

   的充分必要条件是 n 为偶数.

§1.4 多项式的分解

我们在中学就学习过因式分解, 但没有深入地讨论这个问题. 在这一节, 我们将介绍不可约多项式的概念, 并证明多项式因式分解的存在及唯一性定理. 为叙述不可约多项式的性质, 我们需要先讨论最大公因式与互素的概念和性质.

一、最大公因式

与整数有最大公因数的情形一样, 我们可以讨论多项式的最大公因式.

如果多项式 $\varphi(x)$ 既是 $f(x)$ 的因式, 又是 $g(x)$ 的因式, 则 $\varphi(x)$ 称为 $f(x)$ 与 $g(x)$ 的一个**公因式(common divisor)**. 我们重点讨论所谓最大公因式.

定义 1.6 设 $f(x)$, $g(x)$ 是 $P[x]$ 中的两个多项式, $P[x]$ 中的多项式 $d(x)$ 如果满足

(1) $d(x)|f(x)$, $d(x)|g(x)$;

(2) 若 $\varphi(x)|f(x)$, $\varphi(x)|g(x)$, 必有 $\varphi(x)|d(x)$,

则称 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个**最大公因式(greatest common divisor)**.

例如, 任意多项式 $f(x)$ 与 0 的最大公因式是 $f(x)$; 特别地, 0 与 0 的最大公因式为 0.

由于零次多项式是任何多项式的因式, 可知任意两个多项式 $f(x)$ 与 $g(x)$ 的公因式总是存在的. 有了上面的定义以后, 一个自然的问题就是, 任意两个多项式是否存在最大公因式? 要解决这个问题, 主要依赖于带余除法. 关于带余除法我们给出下面的引理.

引理 1.1 如果 $f(x)=g(x)q(x)+r(x)$, 那么 $f(x)$, $g(x)$ 和 $g(x)$, $r(x)$ 有相同的公因式; 从而有相同的最大公因式.

证明 我们先证明引理的第一部分. 根据整除的性质3, 若 $\varphi(x)\,|\,g(x)$, $\varphi(x)\,|\,r(x)$, 那么 $\varphi(x)\,|\,f(x)$; 反之, 若 $\varphi(x)\,|\,g(x)$, $\varphi(x)\,|\,f(x)$, 则由于 $r(x)=f(x)-g(x)q(x)$, 有 $\varphi(x)\,|\,r(x)$. 引理的第一部分得证.

由此可见, 若 $d(x)$ 是 $f(x)$, $g(x)$ 的一个最大公因式, 那么 $d(x)$ 也是 $g(x)$, $r(x)$ 的一个最大公因式, 反之亦然. 引理的第二部分得证. □

定理 1.3 $P[x]$ 中的任意两个多项式 $f(x)$, $g(x)$ 在 $P[x]$ 中存在一个最大公因式 $d(x)$, 且 $d(x)$ 可以表示为 $f(x)$, $g(x)$ 的一个组合, 即存在 $P[x]$ 中的多项式 $u(x)$, $v(x)$ 使得

$$d(x)=u(x)f(x)+v(x)g(x). \tag{1.5}$$

证明 如果 $f(x)$, $g(x)$ 其中一个为零, 不妨设 $g(x)=0$, 则 $f(x)$ 就是 $f(x)$ 和 0 的最大公因式, 且

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

下设 $f(x)$, $g(x)$ 均不为零, 不妨设 $\partial(f(x))\geq\partial(g(x))$, 利用带余除法有

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

其中 $r_1(x)$ 是余式. 若 $r_1(x)=0$, 则 $g(x)$ 即为最大公因式; 否则用 $r_1(x)$ 去除 $g(x)$, 得

$$g(x)=r_1(x)q_2(x)+r_2(x),$$

此时如果余式 $r_2(x)=0$, 则 $r_1(x)$ 即为最大公因式; 否则再用 $r_2(x)$ 去除 $r_1(x)$, 得

$$r_1(x)=r_2(x)q_3(x)+r_3(x),$$

其中 $r_3(x)$ 是余式. 这样辗转相除下去, 在除尽之前, 所得余式的次数不断降低, 即

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

因为多项式的次数是有限的, 所以在若干次以后必有余式为零, 于是有等式组

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

$$
\begin{aligned}
g(x) &= r_1(x)q_2(x) + r_2(x),\\
r_1(x) &= r_2(x)q_3(x) + r_3(x),\\
&\cdots\cdots\\
r_{i-2}(x) &= r_{i-1}(x)q_i(x) + r_i(x),\\
&\cdots\cdots\\
r_{s-3}(x) &= r_{s-2}(x)q_{s-1}(x) + r_{s-1}(x),\\
r_{s-2}(x) &= r_{s-1}(x)q_s(x) + r_s(x),\\
r_{s-1}(x) &= r_s(x)q_{s+1}(x).
\end{aligned}
\tag{1.6}
$$

利用引理 1.1 可知 $r_s(x)$ 就是 $f(x)$ 与 $g(x)$ 的一个最大公因式.

由等式组 (1.6) 中倒数第二个等式得

$$r_s(x) = r_{s-2}(x) - r_{s-1}(x)q_s(x). \tag{1.7}$$

将等式组 (1.6) 中的倒数第三个等式 $r_{s-1}(x) = r_{s-3}(x) - r_{s-2}(x)q_{s-1}(x)$ 代入式 (1.7), 消去 $r_{s-1}(x)$, 得

$$r_s(x) = [1 + q_s(x)q_{s-1}(x)]r_{s-2}(x) - q_s(x)r_{s-3}(x). \tag{1.8}$$

同理再消去式 (1.8) 中的 $r_{s-2}(x)$, 依次下去, 直到最终用第一个等式消去 $r_1(x)$, 合并可得

$$d(x) = r_s(x) = u(x)f(x) + v(x)g(x). \qquad \square$$

定理 1.3 的证明中给出了计算两个多项式的最大公因式的一种方法, 称为**辗转相除法(division algorithm for polynomial)**.

由整除的性质 1 可知, 两个多项式的最大公因式最多相差一个常数倍, 即若 $d_1(x)$, $d_2(x)$ 都是 $f(x)$, $g(x)$ 的最大公因式, 则 $d_1(x) = cd_2(x)$, 其中 $c \neq 0$.

两个不全为零的多项式的最大公因式总是一个非零多项式, 我们用 $\big(f(x), g(x)\big)$ 表示首项系数为 1 的最大公因式. 首一最大公因式是唯一确定的.

现在我们对多项式引入互素的概念.

定义 1.7 多项式环 $P[x]$ 中的任意两个多项式 $f(x)$, $g(x)$ 称为是**互素的(coprime)**, 如果满足 $\big(f(x), g(x)\big) = 1$.

可见, 如果两个多项式 $f(x)$, $g(x)$ 的最大公因式只有非零常数（即零次多项式）, 则它们是互素的; 反之亦然.

下面的定理给出了两个多项式互素的一个等价条件.

定理 1.4 $P[x]$ 中的两个多项式 $f(x)$, $g(x)$ 互素的充要条件是存在 $P[x]$ 中的多项式 $u(x)$, $v(x)$, 使得

$$u(x)f(x) + v(x)g(x) = 1. \tag{1.9}$$

证明 *必要性* 由定理 1.3 即得.

充分性 假设式 (1.9) 成立. 设 $\big(f(x), g(x)\big) = d(x)$, 则 $d(x) \mid f(x)$, $d(x) \mid g(x)$. 从而由整除的性质 3 可知, $d(x) \mid 1$, 即证. $\square$

定理 1.5 如果 $\big(f(x), g(x)\big) = 1$, 且 $f(x) \mid g(x)h(x)$, 那么 $f(x) \mid h(x)$.

证明　由 $(f(x),g(x))=1$, 存在 $u(x)$, $v(x)$ 使得

$$u(x)f(x)+v(x)g(x)=1.$$

两边同时乘以 $h(x)$, 得

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

因为 $f(x)\mid g(x)h(x)$, 故由整除的性质 3 可知, 有 $f(x)\mid h(x)$. □

由定理 1.5 不难得出如下推论.

推论 1.1　如果 $f(x)\mid h(x)$, $g(x)\mid h(x)$, 且 $(f(x),g(x))=1$, 那么 $f(x)g(x)\mid h(x)$.

例 1.6　设多项式 $f(x)$, $g(x)$ 和 $d(x)$ 满足 $d(x)=u(x)f(x)+v(x)g(x)$, 举例说明, $d(x)$ 不一定是 $f(x)$, $g(x)$ 的最大公因式. 若要 $d(x)$ 是 $f(x)$, $g(x)$ 的最大公因式, 需要加什么条件?

解　反例. $f(x)=x+1$, $g(x)=x^2+1$, 令

$$d(x)=(x+2)(x+1)+(x-1)(x^2+1),$$

显然 $d(x)$ 不会是 $f(x)$, $g(x)$ 的最大公因式, 甚至连因式都不是.

若要 $d(x)$ 是 $f(x)$, $g(x)$ 的最大公因式, 需要加的条件为: $d(x)$ 是 $f(x)$, $g(x)$ 的因式. 事实上, 此时只需要再证明 $d(x)$ 最大即可. 若 $\varphi(x)$ 是 $f(x)$, $g(x)$ 的公因式, 则易见 $\varphi(x)\mid d(x)$, 从而 $d(x)$ 是 $f(x)$, $g(x)$ 的最大公因式. □

例 1.7　设 $f(x)$, $g(x)$ 不全为零, 且

$$f(x)=d(x)f_1(x),\quad g(x)=d(x)g_1(x).$$

证明: $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式的充分必要条件是 $(f_1(x),g_1(x))=1$.

证明　由于 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的公因式, 得 $d(x)$ 为最大公因式当且仅当存在 $u(x)$, $v(x)$ 使

$$d(x)=u(x)f(x)+v(x)g(x). \tag{1.10}$$

将 $f(x)=d(x)f_1(x)$, $g(x)=d(x)g_1(x)$ 代入式 (1.10), 得

$$d(x)=u(x)d(x)f_1(x)+v(x)d(x)g_1(x). \tag{1.11}$$

所以我们只需证明式 (1.11) 等价于

$$u(x)f_1(x)+v(x)g_1(x)=1. \tag{1.12}$$

若式 (1.11) 成立, 由于 $f(x)$ 与 $g(x)$ 不全为零, 故 $d(x)$ 不会为零, 利用消去律, 即得式 (1.12); 反之, 用 $d(x)$ 乘以等式 (1.12) 的两边, 即得式 (1.11). 故结论成立. □

最大公因式的概念可以推广到任意多个多项式.

对任意多个多项式 $f_1(x),f_2(x),\cdots,f_s(x)$ $(s>2)$, $d(x)$ 称为 $f_1(x),f_2(x),\cdots,f_s(x)$ 的一个**最大公因式**, 如果满足

(1) $d(x)\mid f_i(x)$, $i=1,2,\cdots,s$;

(2) 若 $\varphi(x)\mid f_i(x)$, $i=1,2,\cdots,s$, 那么 $\varphi(x)\mid d(x)$.

我们仍然用 $(f_1(x),f_2(x),\cdots,f_s(x))$ 表示首一最大公因式.

不难证明, $f_1(x),f_2(x),\cdots,f_s(x)$ 的最大公因式存在. 当 $f_1(x),f_2(x),\cdots,f_s(x)$ 全不为零时,

$$(f_1(x),f_2(x),\cdots,f_s(x))=\big((f_1(x),f_2(x),\cdots,f_{s-1}(x)),f_s(x)\big).$$

利用这个关系可以证明, 存在多项式 $u_i(x)$ $(i=1,2,\cdots,s)$ 使得

$$\big(f_1(x),f_2(x),\cdots,f_s(x)\big)=f_1(x)u_1(x)+f_2(x)u_2(x)+\cdots+f_s(x)u_s(x).$$

若 $\big(f_1(x),f_2(x),\cdots,f_s(x)\big)=1$, 则称 $f_1(x),f_2(x),\cdots,f_s(x)$ **互素**. 关于互素, 有类似于定理 1.4 的结论.

这些证明全部留给读者完成.

二、因式分解定理

在中学学习因式分解时, 我们把多项式分解为一些不能再分解的多项式的乘积, 但是所谓不能再分解其实不是绝对的, 它依赖于多项式所在的数域. 例如

$$\begin{aligned}x^4-4&=(x^2+2)(x^2-2) && \text{(在有理数域 } \mathbf{Q} \text{ 上不能再分解)}\\&=(x-\sqrt{2})(x+\sqrt{2})(x^2+2) && \text{(在实数域 } \mathbf{R} \text{ 上不能再分解)}\\&=(x-\sqrt{2})(x+\sqrt{2})(x+\sqrt{2}\,\mathrm{i})(x-\sqrt{2}\,\mathrm{i}). && \text{(在复数域 } \mathbf{C} \text{ 上不能再分解)}\end{aligned}$$

下面我们就来讨论数域 P 上的多项式的因式分解. 我们必须先明确不能再分解的意思是什么, 为此引入如下定义.

定义 1.8 数域 P 上的非常数多项式 $p(x)$ 称为 P 上的**不可约多项式(irreducible polynomial)**, 如果 $p(x)$ 不能写成 P 中两个次数比 $p(x)$ 次数低的多项式的乘积; 否则称为**可约的**.

注记 易见, 一次多项式在任何数域上都是不可约的; 若不可约多项式 $p(x)=f(x)g(x)$, 则必有 $f(x)=c$ 或者 $g(x)=c$; 并且一个多项式是否不可约依赖于所讨论的系数域.

不可约多项式具有下列性质.

性质 1 不可约多项式 $p(x)$ 与任意多项式 $f(x)$ 之间的关系只有两种可能: 或者 $p(x)\mid f(x)$, 或者 $p(x)$ 与 $f(x)$ 互素.

性质 2 设 $p(x)$ 是不可约多项式, 对任意两个多项式 $f(x)$, $g(x)$, 如果 $p(x)\mid f(x)g(x)$, 则一定有 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$.

性质 2 可以推广到多个多项式的情形. 设 $p(x)$ 是不可约多项式, 如果

$$p(x)\mid f_1(x)f_2(x)\cdots f_s(x),$$

则一定有某个 i $(1\leq i\leq s)$ 使得 $p(x)\mid f_i(x)$.

现在我们提出并证明多项式因式分解的存在及唯一性定理.

定理 1.6 **[因式分解的存在及唯一性定理]** 数域 P 上次数大于零的多项式 $f(x)$ 都可以唯一分解成数域 P 上的一些不可约多项式的乘积. 所谓唯一性是指, 如果有两种分解式

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x),$$

其中 $p_1(x),p_2(x),\cdots,p_s(x),q_1(x),q_2(x),\cdots,q_t(x)$ 都是 P 上的不可约多项式, 则 $s=t$, 且适当调整顺序后 $p_i(x)=c_iq_i(x)$, c_i 是非零常数 $(i=1,2,\cdots,s)$.

证明 *存在性* 对 $f(x)$ 的次数 $\partial\big(f(x)\big)=n$ 作第二数学归纳法.

当 $n=1$ 时, 结论自然成立. 假设对于次数低于 n 的多项式存在性成立.