浙江大学数学系列丛书

Advanced Algebra

高等代数（下册）

李 方 黄正达 汪国军 编著
李慧陵 主审

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

●浙江大学数学系列丛书

高等代数

（下　册）

编著　李　方　黄正达　汪国军
主审　李慧陵

浙江大學出版社

图书在版编目(CIP)数据

高等代数. 下册 / 李方，黄正达，汪国军编著 —杭州：浙江大学出版社，2009.4

（浙江大学数学系列丛书）

ISBN 978-7-308-06701-0

Ⅰ. 高… Ⅱ. ①李…②黄…③汪… Ⅲ. 高等代数—高等学校—教材 Ⅳ. 015

中国版本图书馆 CIP 数据核字(2009)第 054949 号

高等代数(下册)

李　方　黄正达　汪国军　编著

责任编辑　徐素君
封面设计　刘依群
出版发行　浙江大学出版社
（杭州天目山路 148 号　邮政编码 310028）
（网址：http://www.zjupress.com）
排　　版　杭州中大图文设计有限公司
印　　刷　浙江省良渚印刷厂
开　　本　787mm×1092mm　1/16
印　　张　10.5
字　　数　250 千
版 印 次　2009 年 4 月第 1 版　2009 年 4 月第 1 次印刷
书　　号　ISBN 978-7-308-06701-0
定　　价　23.00 元

序

为了弘扬浙江大学数学系的优良传统和学风，适应当代数学研究和教学的发展，2004年起浙江大学数学系组织力量对本科生课程设置和教材进行了重要改革，尤其是对数学系主干课程如数学分析、高等代数、解析几何、实变函数、常微分方程、科学计算、概率论等的教材进行了重新编写，并在浙江大学出版社出版浙江大学数学系列丛书。这是本套系列丛书的第一部分。

丛书的主要特点：

一、加强基础，突出普适性。丛书在内容取舍上，对数学核心内容不仅不削弱，反而有所加强，尤其注重数学基本理论、基本方法的训练。同时，为了适应浙江大学“宽口径”的学生培养制度，对数学应用、数学试验等内容也给予了高度关注。

二、关注前沿理论，强调创新。丛书试图从现代数学的观点审视和选择经典的内容，以新的视角来处理传统的数学内容，使丛书更加适合浙江大学教学改革的需要，适合通才教育的培养目标。

三、注重实践，突出适用性。丛书出版以前，有的作为讲义或正式出版物在浙江大学数学系试用过多次，使丛书的内容和框架、结构比较完善。同时，为了适合不同层次的学生合理取舍，丛书在内容选取上，为学生进一步学习准备了丰富的材料。

在编写过程中，数学系教授们征求了许多学生的意见，并希望能够在教学使用过程中对这套教材作进一步完善。今后我们还会对其他课程的教材进行相应的改革。

为了这套丛书的编写和发行，浙江大学数学系的许多教授和出版社的编辑投入了巨大的精力，我在此对他们表示衷心的感谢。

刘克峰

浙江大学数学系主任

2008年2月

前　言

高等代数课程是数学学科的主要基础课程之一，它和数学分析、空间解析几何组成数学专业大一学生的三门重要基础课程(俗称老三高)。该课程主要由多项式因式理论和线性代数两个部分组成。线性代数部分不仅仅对于数学学科非常重要，它也构成了非数学专业类学生的一门重要的基础课程。高等代数内容中的这两个部分都和方程求解这样一个既古老又具现实意义的问题有着千丝万缕的联系，其历史一直可追溯到《九章算术》时代。

正是因为课程的基础性和重要性，在共和国成立至今的半个多世纪里，出版了不少高等代数教材，其间闪烁着许多专家的真知灼见。传统意义下的以先多项式因式理论后线性代数内容为次序的教材以及将代数和解析几何内容合为一体的教材是其中的代表。这些教材已建立相对严密的理论体系，而后一种教材组织方法更多的是强调代数的几何本质。但这些模式的局限是它们把数学专业的该课程和非数学专业对该课程的需要完全分割开来。

浙江大学于2007年开始实施大类招生和大类培养的模式，它要求一年级新生不分专业，以便学生高年级时可以在一定范围之内选择合适的专业，使本科学生在确定自己最后主修专业前多了一次宝贵的选择机会。这就要求我们建立高等代数课程新的教学模式，使之既要满足以后不选数学学科的学生的对完整的线性代数的教学内容的需要，同时又要符合以后选择数学学科作为专业的学生对该课程的高要求。因此，更新传统教材中的体系使之符合我们新的教学模式，势在必行。这正是本书的出版目的。

为了适应体系的改变，我们对高等代数课程重新组织、融合内容上下了些工夫，这样的重组融合既要在理论逻辑上自然，也要让不同需求的学生分别在上册和下册的学习中达到自己的要求。无论是上册还是下册的内容，在学习标准和严密性的要求上，我们都力争做到不低于传统数学专业的高标准。我们在本课程上的这些创新尝试是否成功，还有待读者的检验。

本书分两册，上册涵盖了公共线性代数课程的内容，下册为给选择数学作为主修专业的学生传授进一步的内容。两册的内容包含数学专业高等代数课程的所有内容。

下册的指导思想决定了实际组织材料的困难所在，即：由于线性代数大纲要求的内容穿插在高等代数课程中除多项式理论外的所有章节中，因此抽出这些内容后的余下的高等代数课程内容在通常体系下是零散的，要把这些零散的内容组织为一个逻辑上自然、由浅入深的课程体系，是有一定难度的。本册目前的授课体系就是为了克服这一难点所作的尝试。

我们以直和理论为线索，研究从线性空间（包括欧氏空间）的子空间出发刻画整体空间的方法，并且进一步用广义逆矩阵理论对方程组通解给出另一种解释。在线性映射的进一步研究中，我们抓住值域与核的关系，来统一理解空间的同构关系及商空间等等。在 Jordan 标准形理论中，我们强调标准形的具体计算方法及该理论与多项式理论之间的有机联系。最后，我们从将欧氏空间思想用于各类非实域上线性空间的角度，介绍了准欧氏空间、正交空间、辛空间、酉空间等，并尝试性地提出准酉空间、酉辛空间的概念作为这些理论的统一与发展，使读者能在较高的观点上来理解各类线性空间的几何意义及方法上的相互联系。

本书在撰写和出版过程中，得到了学校、理学院、数学系同仁的大力支持，特别是理学院副院长陈杰诚教授和数学系副主任李胜宏教授的关心和帮助，葛根年教授、董烈钊副教授、吴志祥副教授、温道伟博士、乔虎生博士、朱海燕博士为本书提出了宝贵的建议，数学系部分研究生在内容校对和文字打印上提供了帮助，更有理学院近几届学生所给予的大力协助和对讲义初稿中不可避免的错误给予的理解。借此一角，谨向他们表示衷心的感谢。本书难免会出现疏漏之处，谨请各位专家、读者指正。

作 者

2009 年初春

目录

说明: 上述目录中打星号*的章节可以作为选读内容.

第 1 章　一元多项式理论

“高等代数”是中国大陆对本课程的一种称谓, 通常理解为线性代数和多项式两部分. 他们都是代数学的最基本对象和工具之一, 方法上不同但相互联系.

多项式这个词, 我们是不陌生的, 中学里就有了, 并已知道有关多项式因式分解的一些基本方法. 比如x^3+x^2-x-1, 它可分解为$(x+1)^2(x-1)$.

但我们现在要上升到一般的多项式理论来讨论, 对于多项式所处的数域也不再限于实数域或有理数域.

从方法上来说, 多项式理论可类比于整数理论. 这其实不是偶然的, 读者若学过近世代数, 就会发现它们是统一在所谓的唯一分解整环下的.

解多项式方程是数学中最基本的课题之一. 自17世纪以来, 对它的研究几乎未曾中断. 要想获得解任意次多项式方程的较好方法, 就需要建立完整的关于多项式的理论, 比如证明复数域上每个多项式方程必有根, 实数域上怎样的多项式才是不可分解的, 等等. 本章将逐次展开这些相关内容的讨论.

§1.1　一元多项式

首先给出一元多项式的抽象定义.

给定一个数域$\mathbb{P}$, x为一符号(或称文字), 形如

$$f(x)\triangleq a_0+a_1x+\cdots+a_nx^n+a_{n+1}x^{n+1}+\cdots \tag{1.1.1}$$

的形式表达式称为**系数在数域$\mathbb{P}$上的一元多项式**(或简称: **$\mathbb{P}$上的一元多项式**), 其中对$i=0,1,\cdots,n,\cdots$, 所有$a_i\in\mathbb{P}$至多有限个不等于0. 我们把a_ix^i称为$f(x)$的**i次单项**(或**i次项**), a_i称为i次项的**系数**. 用连加符号可表为

$$f(x)\triangleq\sum_{i=0}^{+\infty}a_ix^i.$$

在上式中, 若$a_n\neq 0$但是对所有$s>n$有$a_s=0$, 就称a_nx^n为**首项**, 称a_n为**首项系数**, 称n为$f(x)$的**次数**, 并表为$\partial(f(x))$. 若一个多项式的所有系数全为 0, 则称之为**零多项式**, 并记作0. 零多项式的次数规定为$-\infty$.

注意: (1) 这里的运算“+”仅是一个“形式加法”, 只是将不同单项“连结”在一起;

(2) 系数a_i与x^i之间的关系a_ix^i仅表示“形式数乘”, 只是说明将两者“放在一起”;

(3) 我们约定, 一个多项式$f(x)$中系数为0的单项可以写出来, 也可以不写出来. 比如, 设$\partial(f(x))=n$, 我们可以写

$$f(x)=a_0+a_1x+\cdots+a_nx^n+0x^{n+1}+0x^{n+2}+\cdots,$$

也可以写

$$f(x)=a_0+a_1x+\cdots+a_nx^n.$$

设

$$f(x)=a_0+a_1x+\cdots+a_nx^n+\cdots,$$
$$g(x)=b_0+b_1x+\cdots+b_nx^n+\cdots$$

是数域$\mathbb{P}$上的两个多项式.

(1) 若对$i=0,1,\cdots$, 有$a_i=b_i$, 则称$f(x)$与$g(x)$是**相等**的, 表为$f(x)=g(x)$.
由于零多项式的系数全为零, 因此它不与任何一个非零多项式相等.

(2) 定义$f(x)$与$g(x)$的**和**为如下的一个新的多项式:

$$f(x)+g(x)\triangleq(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+\cdots;$$

(3) $f(x)$与$g(x)$的**乘积**为如下的一个新的多项式:

$$f(x)g(x)\triangleq c_0+c_1x+\cdots+c_sx^s+\cdots,$$

其中s次单项的系数是

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

因此, 当$f(x)\neq 0$, $g(x)\neq 0$时, 令$\partial(f(x))=n$, $\partial(g(x))=m$, 那么$f(x)=g(x)$ 当且仅当$n=m$ 且对$i=0,1,\cdots,n$, 有$a_i=b_i$. 若$n\geqslant m$, 则有

$$\begin{aligned}&f(x)+g(x)\\&=(a_0+a_1x+\cdots+a_mx^m+a_{m+1}x^{m+1}+\cdots+a_nx^n)\\&\quad+(b_0+b_1x+\cdots+b_mx^m+0x^{m+1}+\cdots+0x^n)\\&=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+(a_{m+1}+0)x^{m+1}+\cdots+(a_n+0)x^n.\end{aligned}$$

这时, 由上面多项式乘积的定义, 对$t>n+m$, 易见$c_t=0$. 因而,

$$f(x)g(x)=c_0+c_1x+\cdots+c_sx^s,$$

其中$s=n+m$. 对$0\leq i\leq s$, i次项的系数是

$$c_i=a_ib_0+a_{i-1}b_1+\cdots+a_1b_{i-1}+a_0b_i.$$

特别地, $c_s=a_nb_m$.

零多项式0起到的作用就是线性空间中零元的作用, 这是因为:

(1) $0+f(x)=f(x)$. 事实上,

$$\begin{aligned}0+f(x)&=(0+0x+\cdots+0x^n)+(a_0+a_1x+\cdots+a_nx^n)\\&=(0+a_0)+(0+a_1)x+\cdots+(0+a_n)x^n\\&=a_0+a_1x+\cdots+a_nx^n\\&=f(x);\end{aligned}$$

(2) 同理, $f(x)+0=f(x)$;

(3) 再由乘法定义可证, $f(x)0=0f(x)=0$.

定义$f(x)$的**负多项式**为:

$$-f(x)\triangleq(-a_0)+(-a_1)x+\cdots+(-a_n)x^n.$$

定义$f(x)$与$g(x)$的**减法**为:

$$f(x)-g(x)\triangleq f(x)+(-g(x)).$$

那么,

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

定义数c在多项式$f(x)$上的**数乘**为

$$cf(x)=ca_0+ca_1x+\cdots+ca_nx^n,$$

这也就是把c看作常数项多项式时与$f(x)$的多项式乘法得到的结果.

显然, 数域$\mathbb{P}$上两个多项式经加、减、乘运算后, 所得结果仍是$\mathbb{P}$上的多项式.

由多项式的次数定义, 我们有如下性质:

性质 1 对于任意两个非零多项式$f(x)=\sum a_ix^i$, $g(x)=\sum b_jx^j$, 若$\partial(f(x))=n$和$\partial(g(x))=m$, 那么,

(1) $\partial(f(x)+g(x))\leqslant\max\{\partial(f(x)),\ \partial(g(x))\}$;

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

证明 (1) 不妨设$n\geqslant m$, 即$\partial(f(x))\geqslant\partial(g(x))$. 则由前面给出的两个多项式和的公式, 当$n>m$时, $f(x)+g(x)$ 的首项是$(a_n+0)x^n=a_nx^n\neq0$, 故这时

$$\partial(f(x)+g(x))=n=\partial(f(x))=\max\{\partial(f(x)),\ \partial(g(x))\};$$

当$n=m$时, 若$a_n+b_n\neq0$, 则$f(x)+g(x)$ 的首项是$(a_n+b_n)x^n$且

$$\partial(f(x)+g(x))=n=\partial(f(x))=\partial(g(x))=n;$$

若$a_n+b_n=0$, 则$\partial(f(x)+g(x))\leqslant n-1$.

因此总有$\partial(f(x)+g(x))\leqslant\max\{\partial(f(x)),\ \partial(g(x))\}$.

(2) 由多项式乘积的定义可得

$$f(x)g(x)=\sum_{t=0}^{m+n}\left(\sum_{i+j=t}a_ib_j\right)x^t,$$

其中$a_nb_m\neq0$. 所以它的首项是$a_nb_mx^{n+m}$, 因此

$$\partial(f(x)g(x))=n+m=\partial(f(x))+\partial(g(x)).$$ □

不难将上面的结论推广到多个多项式的情形.

多项式的运算与数的运算有类似的规律, 即:

性质 2 对数域$\mathbb{P}$上的多项式$f(x)$, $g(x)$, $h(x)$, 有:

(i) 加法交换律: $f(x)+g(x)=g(x)+f(x)$;

(ii) 乘法交换律: $f(x)g(x)=g(x)f(x)$;

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

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

(v) 乘法对加法的(左、右)分配律:

$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x),$$
$$(g(x)+h(x))f(x)=g(x)f(x)+h(x)f(x);$$

(vi) 乘法的(左、右)消去律:

若$f(x)g(x)=f(x)h(x)$ (或$g(x)f(x)=h(x)f(x)$) 且$f(x)\neq0$, 则$g(x)=h(x)$.

证明 (i) 对$f(x)=\sum_{i=0}^{n}a_ix^i$, $g(x)=\sum_{i=0}^{m}b_ix^i$, 设$n\geqslant m$. 那么, 由加法定义可得:

$$\begin{aligned}
&f(x)+g(x)\\
&=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+(a_{m+1}+0)x^{m+1}+\cdots+(a_n+0)x^n\\
&=(b_0+a_0)+(b_1+a_1)x+\cdots+(b_m+a_m)x^m+(0+a_{m+1})x^{m+1}+\cdots+(0+a_n)x^n\\
&=g(x)+f(x).
\end{aligned}$$

(ii) 对$0 \le i \le n+m$, 有

$$c_i \triangleq a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i = b_ia_0 + b_{i-1}a_1 + \cdots + b_1a_{i-1} + b_0a_i.$$

于是,

$$f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m} = g(x)f(x).$$

(iii) 由加法定义即可得.

(iv) 对$f(x) = \sum_{i=0}^{n} a_ix^i$, $g(x) = \sum_{i=0}^{m} b_ix^i$, $h(x) = \sum_{i=0}^{l} c_ix^i$, 依乘法定义,

$$\begin{aligned}(f(x)g(x))h(x) &= \left(\sum_{s=0}^{n+m}\left(\sum_{i+j=s} a_ib_j\right)x^s\right)\left(\sum_{i=0}^{l} c_ix^i\right)\\ &= \sum_{t=0}^{n+m+l}\left(\sum_{s+k=t}\left(\sum_{i+j=s} a_ib_j\right)c_k\right)x_t\\ &= \sum_{t=0}^{n+m+l}\left(\sum_{i+j+k=t} a_ib_jc_k\right)x^t\\ &= \sum_{t=0}^{n+m+l}\left(\sum_{i+p=t} a_i\left(\sum_{j+k=p} b_jc_k\right)\right)x^t\\ &= f(x)(g(x)h(x)).\end{aligned}$$

(v) 由加法定义和乘法定义可证得, 请读者自证.

(vi) 由$f(x)g(x) = f(x)h(x)$, 得$f(x)(g(x) - h(x)) = 0$.

由$f(x) \neq 0$得$\partial(f(x)) \ge 0$.

若$g(x) - h(x) \neq 0$, 则$\partial(g(x) - h(x)) \ge 0$, 进而

$$\partial(f(x)(g(x) - h(x))) = \partial(f(x)) + \partial(g(x) - h(x)) \ge 0 \neq -\infty.$$

但$\partial(0) = -\infty$, 这与$f(x)(g(x) - h(x)) = 0$矛盾. 所以$g(x) - h(x) = 0$, 即$g(x) = h(x)$.□

由上面(i), 当$i \neq j$时, $a_ix^i + b_jx^j = b_jx^j + a_ix^i$, 因而, 对任一多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

我们可以有另一表达式

$$f(x) = a_nx^n + \cdots + a_1x + a_0.$$

更多地, 我们会用这一降次排序写法, 这也就是为何称a_nx^n ($a_n \neq 0$) 是$f(x)$的首项的原因.

数域$\mathbb{P}$上的所有一元多项式全体我们表示为集合$\mathbb{P}[x]$. 由上, $\mathbb{P}[x]$中已有加法、乘法和数乘, 由它们的定义和多项式相等的条件, 以及上面的讨论, 特别是性质2 (i) (iii), 可知, $\mathbb{P}[x]$是$\mathbb{P}$上无限维线性空间, 且若令

$$\mathbb{P}[x]_n = \{f(x) \in \mathbb{P}[x] : \partial(f(x)) < n\},$$

则$\mathbb{P}[x]_n$是一个以$1, x, \cdots, x^{n-1}$为基的$\mathbb{P}$上n维线性空间. 由此, 有子空间链:

$$\{0\} \subset \mathbb{P}[x]_0 \subset \mathbb{P}[x]_1 \subset \cdots \subset \mathbb{P}[x]_n \subset \mathbb{P}[x]_{n+1} \subset \cdots \subset \mathbb{P}[x].$$

又由性质2 (iv) (v), 我们将这个$\mathbb{P}$上线性空间$\mathbb{P}[x]$称为$\mathbb{P}$**上的一元多项式代数**. 一般的代数概念来自于近世代数课程, 它是一个有乘法的线性空间, 我们这里不再涉及.

我们在这里定义多项式的抽象概念, 目的是为了统一不同现实情况下出现的多项

式的共性. 比如, 当符号x具体到中学数学里的未知数时, $f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0$就代表一个未知数$x$的数字表达式, 加法和数乘就恢复到数的加、乘; 当x可以在数的一定范围内变动, 那么$f(x)$就成为x上的一个函数, 称为**多项式函数**. 当符号x具体到一个方阵$\boldsymbol{A}$时, $f(x)$就变成$f(\boldsymbol{A})=a_n\boldsymbol{A}^n+\cdots+a_2\boldsymbol{A}^2+a_1\boldsymbol{A}+a_0\boldsymbol{E}$, 这是一个矩阵表达式, 加法和数乘就具体到矩阵的加法和数乘. 看实际需要, 这个符号x还可以表示其他待定事物. 进一步, 我们就引入了形式化的多项式的运算来统一研究各类待定事物所满足的运算规律, 以得到它们普遍的共同的性质.

§1.2 整除理论

在一元多项式代数$\mathbb{P}[x]$中, 上节已定义了加减乘三种运算, 但乘法的逆运算—除法—通常是不可行的. 因为, 对某个多项式$f(x)\in\mathbb{P}[x]$, 若$\partial(f(x))\geq 1$, 则对任一非零多项式$g(x)\in\mathbb{P}[x]$, 必有

$$\partial(f(x)g(x))=\partial(f(x))+\partial(g(x)\geq\partial(f(x))\geq 1.$$

因此$f(x)g(x)\neq 1$, 故$\mathbb{P}[x]$中不存在$f(x)^{-1}$. 这说明除法是不可行的. 因此, 整除就成了某些多项式之间的特殊的重要关系.

数域$\mathbb{P}$上的多项式$g(x)$称为**整除**$f(x)$的, 若存在$\mathbb{P}$上的多项式$h(x)$使得

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

成立. 我们用$g(x)\mid f(x)$表示$g(x)$整除$f(x)$. 当$g(x)$不能整除$f(x)$时, 用$g(x)\nmid f(x)$表示. 当$g(x)\mid f(x)$时, 称$g(x)$是$f(x)$的**因式**, $f(x)$是$g(x)$的**倍式**.

由中学代数我们已经知道, 对两个具体的多项式, 可用一个去除另一个, 求得商和余式. 例如, 设$f(x)=3x^3+4x^2-5x+6$, $g(x)=x^2-3x+1$, 可以按下面的格式来作除法:

$$\begin{array}{r|l}
 & 3x\ +13 \\
\cline{2-2}
x^2-3x+1 & 3x^3+4x^2-5x+6 \\
 & \underline{3x^3-9x^2+3x} \\
 & \quad 13x^2-\ 8x+6 \\
 & \underline{13x^2-39x+13} \\
 & \quad\quad 31x-7
\end{array}$$

即, 所得商为$3x+13$, 余式为$31x-7$. 上述竖式也可写为如下表达式:

$$f(x)=(3x+13)g(x)+(31x-7).$$

显然上述算式是对数字运算下的数字多项式进行的, 但不难看出, 事实上, 把上述多项式看作第一节中定义的"形式"多项式时, 算式一样成立. 也就是说, 我们可将此求商式和除式的方法用到"形式"多项式上. 这不是偶然的, 它建立在如下的结论上:

定理 1 (带余除法) 对于$\mathbb{P}[x]$中的任意两个多项式$f(x)$与$g(x)$, 其中$g(x)\neq 0$, 必存在唯一的$q(x)$, $r(x)\in\mathbb{P}[x]$使得

$$f(x)=q(x)g(x)+r(x) \tag{1.2.1}$$

成立, 且或者$r(x)=0$或者$\partial(r(x))<\partial(g(x))$.

证明 先证$q(x)$, $r(x)$的存在性.

当$f(x)=0$时, 取$q(x)=r(x)=0$即可.

当$f(x)\neq 0$时, 对$\partial(f(x))=n$用归纳法.

当$\partial(f(x))=0$, 若$\partial(g(x))=0$, 令$g(x)=c\in\mathbb{P}$, 取$q(x)=c^{-1}f(x)$, $r(x)=0$即可. 若$\partial(g(x))>0$, 取$q(x)=0$, $r(x)=f(x)$即可.

假设$\partial(f(x))<n$时结论成立, 考虑$\partial(f(x))=n$时的情况.

事实上, 当$\partial(g(x))>n$时, 取$q(x)=0$, $r(x)=f(x)$即可.

当$\partial(g(x))=m\leq n$时, 令$f(x)$和$g(x)$的首项分别是ax^n和bx^m, 则$b^{-1}ag(x)x^{n-m}$的首项也是ax^n, 故多项式$f_1(x)=f(x)-b^{-1}ax^{n-m}g(x)$的次数小于$f(x)$的次数$n$或$f_1(x)=0$.

若$f_1(x)=0$, 取$q(x)=b^{-1}a^{n-m}$, $r(x)=0$即可;

若$f_1(x)\neq 0$, 则$\partial(f_1(x))<n$. 由归纳假设, 对$f_1(x)$和$g(x)$, 存在$q_1(x)$, $r_1(x)$使得

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

成立, 其中$\partial(r_1(x))<\partial(g(x))$或$r_1(x)=0$. 于是,

$$\begin{aligned}f(x)&=f_1(x)+b^{-1}ax^{n-m}g(x)\\&=(q_1(x)+b^{-1}ax^{n-m})g(x)+r_1(x)\\&=q(x)g(x)+r(x),\end{aligned}$$

其中$q(x)=q_1(x)+b^{-1}ax^{n-m}$, $r(x)=r_1(x)$. 自然地, $\partial(r(x))<\partial(g(x))$.

由归纳法知, $q(x)$, $r(x)$的存在性成立.

再证上述$q(x)$, $r(x)$的唯一性.

若存在另一组$q^o(x)$, $r^o(x)$使得

$$f(x)=q^o(x)g(x)+r^o(x)\tag{1.2.2}$$

成立, 且$\partial(r^o(x))<\partial(g(x))$或$r^o(x)=0$. 将(1.2.1)与(1.2.2)两式相减, 得

$$(q(x)-q^o(x))g(x)=r^o(x)-r(x).$$

若$q(x)\neq q^o(x)$, 则

$$\partial((q(x)-q^o(x))g(x))\geq\partial(g(x))>\partial(r^o(x)-r(x)).$$

这与上述等式矛盾.

因此必有$q(x)=q^o(x)$. 由此, 又得$r(x)=r^o(x)$. □

由此, 把定理1前面的具体例子中的$f(x)$和$g(x)$代入公式(1.2.1), 那么它们计算后的表达式恰符合由形式多项式获得的公式(1.2.1). 这说明我们由抽象多项式的方法导出的结论能覆盖非抽象定义的多项式的相应结论.

上述定理中所得到的$q(x)$称为$g(x)$除$f(x)$的**商**, $r(x)$称为$g(x)$除$f(x)$的**余式**. 由定理1和整除的定义我们不难得出下面的引理.

引理 1 当$g(x)\neq 0$时, $g(x)\mid f(x)$当且仅当$g(x)$除$f(x)$时的余式为0.

当$g(x)|f(x)$, 且$g(x)\neq 0$时, $g(x)$除$f(x)$所得的商$q(x)$有时也用$\dfrac{f(x)}{g(x)}$来表示.

对任一个$\mathbb{P}$上多项式$f(x)$和$0\neq a\in\mathbb{P}$, 必有$f(x)=1\cdot f(x)$, $0=0\cdot f(x)$, $f(x)=a(a^{-1}f(x))$, 因此总有:

$$f(x)|f(x),\quad f(x)|0,\quad a|f(x)\,.$$

下面介绍整除性的几个常用性质:

性质 3 若$f(x)|g(x)$, $g(x)|f(x)$, 则存在非零常数c使得$f(x)=cg(x)$成立.

证明 由$f(x)|g(x)$, $g(x)|f(x)$知, 分别存在$h_1(x)$, $h_2(x)$使得

$$g(x)=h_1(x)f(x),\ \text{且}f(x)=h_2(x)g(x)$$

成立. 于是

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

如果$f(x)=0$, 则$g(x)=0$, 结论显然成立.

如果$f(x)\neq 0$, 则由性质2 (vi)得$h_1(x)h_2(x)=1$, 从而$\partial(h_1(x))+\partial(h_2(x))=0$. 特别地,

$$\partial(h_2(x))=0,$$

故$h_2(x)=c$, 其中$c\in\mathbb{P}$是一个非零常数. □

性质 4 (整除的传递性) 若$f(x)|g(x)$, $g(x)|h(x)$, 则$f(x)|h(x)$.

证明 存在$g_1(x)$, $h_1(x)$, 使得

$$g(x)=g_1(x)f(x),\ h(x)=h_1(x)g(x)$$

成立, 从而$h(x)=h_1(x)g_1(x)f(x)$, 即$f(x)|h(x)$. □

性质 5 若$f(x)|g_i(x)(i=1,2,\cdots,r)$, 则对任意多项式$u_i(x)(i=1,2,\cdots,r)$, 有$f(x)|(u_1(x)g_1(x)+\cdots+u_r(x)g_r(x))$.

证明 由题设, 存在$h_i(x)(i=1,2,\cdots,r)$使得$g_i(x)=h_i(x)f(x)$成立. 从而

$$\sum_{i=1}^{r}u_i(x)g_i(x)=\left(\sum_{i=1}^{r}u_i(x)h_i(x)\right)f(x),$$

故

$$f(x)|(u_1(x)g_1(x)+\cdots+u_r(x)g_r(x)).$$ □

推论 1 任一多项式$f(x)$与它的任一非零常数倍$cf(x)(c\neq 0)$有相同的因式和倍式.

因此, 在多项式整除性讨论中, 不妨假设$f(x)$的首项系数为1.

最后指出, 两个多项式之间的整除性不会因为系数域的扩大而改变. 即:

定理 2 设$\mathbb{P}$, $\bar{\mathbb{P}}$是两个数域, 且$\mathbb{P}\subseteq\bar{\mathbb{P}}$. 设$f(x)$, $g(x)\in\mathbb{P}[x]$, 那么在$\mathbb{P}$中$g(x)|f(x)$当且仅当在$\bar{\mathbb{P}}$中$g(x)|f(x)$.

证明 若$g(x)=0$, 则在$\mathbb{P}$中$g(x)|f(x)$当且仅当$f(x)=0$, 从而当且仅当在$\bar{\mathbb{P}}$中$g(x)|f(x)$.

若$g(x)\neq 0$, 则由定理1 的带余除法, 存在唯一的$q(x)$, $r(x)\in\mathbb{P}[x]$, 使得

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

(即定理1中的(1.2.1)式)成立, 且$\partial(r(x))<\partial(g(x))$或$r(x)=0$.

显然上述等式在$\bar{\mathbb{P}}[x]$中也成立.

因此, 在$\mathbb{P}[x]$中$g(x)|f(x)$当且仅当$r(x)=0$, 从而当且仅当在$\bar{\mathbb{P}}[x]$中$g(x)|f(x)$. □

例 1 设$g(x)=ax+b, a,b\in\mathbb{P}, a\neq 0, f(x)\in\mathbb{P}[x]$, 求证: $g(x)|f(x)^2$的充要条件

是$g(x)|f(x)$.

证明 充分性显然成立, 只需证明必要性也成立.

由带余除法, 存在$r \in \mathbb{P}$, 使得$f(x) = g(x)q(x) + r$成立. 所以

$$f(x)^2 = g(x)^2 q(x)^2 + 2rg(x)q(x) + r^2.$$

由$g(x)|f(x)^2$得$g(x)|r^2$, 故$r^2 = 0$, $r = 0$, 即$g(x)|f(x)$. □

例 2 设$f(x), g(x)$及$h(x) \neq 0$为三个多项式. 证明: $h(x)|(f(x) - g(x))$当且仅当$f(x)$与$g(x)$除以$h(x)$所得的余式相等.

证明 由带余除法, 可设

$$f(x) = h(x)q_1(x) + r_1(x),\ g(x) = h(x)q_2(x) + r_2(x),$$

其中$r_i(x) = 0$或$\partial(r_i(x)) < \partial(h(x)), i = 1, 2$. 上面二式相减, 得

$$f(x) - g(x) = h(x)[q_1(x) - q_2(x)] + r_1(x) - r_2(x). \tag{1.2.3}$$

由于$\partial(r_i(x)) < \partial(h(x))$, 故$\partial(r_1(x) - r_2(x)) < \partial(h(x))$. 所以$h(x)$除$f(x) - g(x)$的商为$q_1(x) - q_2(x)$, 余式为$r_1(x) - r_2(x)$.

若$r_1(x) = r_2(x)$, 则由上述(1.2.3)式得

$$f(x) - g(x) = h(x)[q_1(x) - q_2(x)],$$

从而

$$h(x)|(f(x) - g(x)).$$

反之, 若$h(x)|(f(x) - g(x))$, 则由引理1知 $r_1(x) - r_2(x) = 0$, 即$r_1(x) = r_2(x)$. □

§1.3 最大公因式

定义 1 设$f(x)$, $g(x)$, $\varphi(x)$, $d(x) \in \mathbb{P}[x]$.

i) 若$\varphi(x)|f(x)$且$\varphi(x)|g(x)$, 则称$\varphi(x)$是$f(x)$, $g(x)$的一个**公因式**;

ii) 若$d(x)$是$f(x)$, $g(x)$的一个公因式, 且对$f(x)$, $g(x)$的任一公因式$\varphi(x)$均有$\varphi(x)|d(x)$, 则称$d(x)$是$f(x)$, $g(x)$的一个**最大公因式**.

例 3 (1) 设$f(x) = 2(x-1)^3(x^2+1)$, $g(x) = 4(x-1)^2(x+1)$. 则$f(x)$和$g(x)$的首项系数为1的公因式有1, $x-1$, $(x-1)^2$, 其中$(x-1)^2$是一个最大公因式.

(2) 任一多项式$f(x)$总是它自身和零多项式0的一个最大公因式.

(3) 两个零多项式的最大公因式就是0, 但任一非零多项式都是这两个零多项式的公因式.

注意: 通常, 最大公因式是不唯一的, 比如上述(1)中, 最大公因式可以是$(x-1)^2$, 也可以是$2(x-1)^2$, 这两个最大公因式相差一个常数倍. 这不是偶然的, 事实上, 我们有:

命题 1 (唯一性) 两个多项式的最大公因式在可以相差非零常数倍的意义下是唯一确定的.

证明 设$f(x)$, $g(x)$有两个最大公因式$d_1(x)$和$d_2(x)$, 由最大公因式定义知

$$d_1(x)|d_2(x),\quad d_2(x)|d_1(x).$$