高等代数

第二讲

暨巨大学数学系编

一九八二年一月

第七章　多项式

§1 集合、数环与数域

一、集合

集合是数学中常用的一个基本术语。集合（简称集）就是指一些事物的全体。例如，所有整数构成整数集；0，1这两个数也构成一个数集；所有n阶方阵构成一个方阵集合；线性方程组$Ax=b$的所有解构成它的解集合等等。集合通常以大写字母S、T、M、N…记之。构成集合的事物称为该集合的元素或元，通常以小写字母a，b，c…记之。

所谓给出一个集合，就是要指明它由那些元素构成。一般有以下两种表示法：其一，（如果可能的话）列出集合中所有的元素，例如整数集Z可表示为$Z=\{0,\pm1,\pm2\cdots\}$，其二，指出集合中元素所具有的特性。记号$S=\{x\mid x$所具有的性质$P\}$表明集合S由所有具有性质P的元素构成。例如$T=\{x\mid 2x^2+3x+1=0,x$为有理数$\}$代表方程$2x^2+3x+1=0$的解集合。

对于某个集合S来说，某一事物a或者是集合S的元素，或者不是，两者必居其一。若a是S的元素，记为$a\in S$，读作a属于S；否则，记为$a\notin S$，读作a不属于S。

为表达方便起见，称不含有任何元素的集合为空集，以Φ记之。例如$S=\{x\mid x>1\}$，则S是一个空集。T不是空集，记为$T\neq\Phi$，读作T非空。例如$T=\{0\}$不是空集。

设S、T是两个集合，称S为T的子集（记为$S\subseteq T$），如果S中任一元素都是T的元素；称S为T的真子集（记为$S\subset T$），如果S是T的子集，且T中至少有一个元素不属于S。记号

$S \subseteq T$（$S \subset T$），读作S包含（真包含）在T中。规定空集是任何集合的子集。今后恒以Z、Q表示整数集和有理数集，于是有$\emptyset \subset Z \subset Q$。

称集合S与T相等（记为$S=T$），如果$S \subseteq T$且$T \subseteq S$。例如$\{1, 2, 3\}=\{1, 2, 3, 1\}$。显然，相等的两个集合含有相同的元素。称集合为无限集，如果其中含有无限多个不同的元素。否则，称为有限集。

集合之间进一步的关系，将在第十一章中介绍。

二、数环与数域

数集是常见的一种集合。其中的自然数集N、整数集Z、有理数集Q、实数集R、复数集C已为大家所熟知。

在数集S中，任取两数作某种运算，若其结果仍在S中，则称数集S对于这种运算是封闭的。显然，Z、Q、R、C对于数的减法是封闭的，N却不然；Q、R、C对于数的除法（除数非零）是封闭的，Z却不然。

代数中讨论问题时，经常涉及某一数集中数的加、减、乘、除运算及其性质，为了统一处理具有共同性质的数集，引进数环与数域的概念。

定义　称非空数集S为数环，如果S对于数的加、减、乘运算是封闭的，（即$\forall a, b \in S \Rightarrow a \pm b, ab \in S$）①。称至少包含两个不同元素的数集Ω为数域，如果Ω对于数的加、减、乘、除（除数非零）运算是封闭的（即$\forall a, b \in S, \Rightarrow a \pm b, ab$，$\frac{a}{b}(b \neq 0) \in S$）。

由定义可知，若某一数集是数域，则必是数环。Q、R和C

是数域，分别称为有理数域、实数域和复数域；Z 是数环，但不是数域，称为整数环。N 不是数环，当然也不是数域。

例 1　验证数集 $Q(\sqrt{2})=\{x \mid x=a+b\sqrt{2}\ \forall\ a, b\in Q\}$ 为一数域。

〔证明〕　首先，$0,1\in Q(\sqrt{2})$。其次 $Q(\sqrt{2})$ 对数的加、减运算显然是封闭的。$\forall\ x, y\in Q(\sqrt{2})$，可设

$$x=a+b\sqrt{2},\qquad a, b\in Q,$$

$$y=c+d\sqrt{2},\qquad c, d\in Q.$$

于是，

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

而当 $y=c+d\sqrt{2}\neq 0$ 时，必有 $c-d\sqrt{2}\neq 0$，

且

$$\frac{x}{y}=\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{ac-2bd}{c^2-2d^2}+$$

$$+\frac{bc-ad}{c^2-2d^2}\sqrt{2}$$

因为 a，b，c，d∈Q，Q 为数域，所以 $ac+2bd\in Q$，$ad+bc\in Q$，即 $Q(\sqrt{2})$ 对于乘法是封闭的；注意到 $c^2-2d^2\neq 0$

所以 $\frac{ac-2bd}{c^2-2d^2}\in Q$，$\frac{bc-ad}{c^2-2d^2}\in Q$，即 $Q(\sqrt{2})$ 对于除法也封闭。这就验证了 $Q(\sqrt{2})$ 是一数域。

类似地，可以验证数集 $Z(\sqrt{2})=\{x \mid x=a+b\sqrt{2},\ \forall a, b\in Z\}$ 为一数环。必须注意 $Z(\sqrt{2})$ 不是数域，事实上，若在 $Z(\sqrt{2})$ 中特别取 $x=\sqrt{2}$，$y=2$，则 $x/y=\frac{1}{2}\sqrt{2}\notin Z(\sqrt{2})$，即 $Z(\sqrt{2})$ 对

上页(1)：记号“$\forall$ ……”的含义是“对所有的……”。

于除法运算不封闭。

由定义不难得到下列性质。

命题1　任一数环必包含0，任一数域必包含0与1。

命题2　有理数域是最小的数域。

命题1的证明留给读者。利用它的逆否命题立即可以断定奇数集不是一数环，偶数集不是一数域。

下面证明命题2。设Ω为任一数域，由命题1，$1\in\Omega$。利用Ω对于加法的封闭性可得任一整数$n\in\Omega$，注意到$0\in\Omega$并利用Ω对于减法的封闭性可得任一负整数$(-n)\in\Omega$。综合之，$Z\subseteq\Omega$，$\forall x\in Q$，可设$x=\frac{p}{q}$，其中$p、q\in Z$，$q\neq 0$。$\because Z\subseteq\Omega$

$\therefore p、q\in\Omega$，因数域Ω对于除法运算封闭，所以$x=p/q\in\Omega$。这就证明了$Q\subseteq\Omega$。　　证毕

设Ω_1，Ω_2为两个数域，若$\Omega_1\subset\Omega_2$，则称Ω_1为Ω_2的真子域，而称Ω_2为Ω_1的扩域。例如R是C的真子域，而C是R的扩域。

习　题

1，下列数集中，哪些是数域，哪些仅是数环，哪些不是数环？（说明理由）

(i)　非零数的有理数集合S；

(ii)　偶数与分子为偶数的既约数数集合T；

(iii)　$Q(\sqrt{-1})=\{x\mid x=a+b\sqrt{-1},\ \forall a、b\in Q\}$；

(iv)　$Q(\sqrt[3]{2})=\{x\mid x=a+b\sqrt[3]{2},\ \forall a、b\in Q\}$。

2，设M为至少包含一个非零元的数集。

(i) 证明，若M对于数的减法、除法（除数非零）封闭，则对于数的加法、乘法也封闭。

(ii) 举例说明(i)中结论之逆未必成立。

3，(i) 数域$Q(\sqrt{2})$是否为实数域R的真子域。

(ii) 数域$Q(\sqrt{-1})$是否为实数域R的扩域。

§2 一元多项式

一、定义 有关的约定及名词

定义 设Ω为一数域，x为一符号，若$a_i \in \Omega$ ($i=0, 1, 2, \cdots, n$) n为一非负整数，则称形式表达式

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \qquad (1)$$

为数域Ω上（关于x）的一个一元多项式。

一元多项式通常以f(x)、g(x)、h(x)或f、g、h…记之。规定a_0代表$a_0 x^0$，称(1)中的$a_i x^i$为i次项，i为它的次数，a_i为它的系数（$i=0, 1, 2, \cdots, n$）。我们将(1)与表达式$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$不加区别。习惯上，今后总采用降次标准式(1)，并常将它记为

$$\sum_{i=0}^{n} a_i x^i$$

在多项式中不出现的次数，认为其系数为零；对x^i，则认为其系数为1。

称多项式中系数非零的最高次项为它的首项，首项的次数称为多项式的次数。即若

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_n \neq 0,$$

则 $f(x)$ 的次数为 n，记为 $\deg(f(x))=n$。特别地，非零常数是零次多项式。称各次项系数均为零的多项式为零多项式，以 0 记之。对于零多项式，无次数可言。因此，今后当且仅当 $f(x)\neq 0$ 时才书写记号 $\deg(f(x))$，显然 $\deg(f(x))\geqslant 0$。

二、运算及其性质

数域 Ω 上一元多项式全体所成的集合记为 $\Omega[x]$，即

$$\Omega[x]=\{f(x)=\sum_{i=0}^{n}a_ix^i,\ \forall a_i\in\Omega(i=0,1,\cdots,n)\},$$

n 为任一非负整数，

定义 设 $f(x)$，$g(x)\in\Omega[x]$，称 $f(x)$ 与 $g(x)$ 相等（记为 $f(x)=g(x)$），如果它们同次项的系数全都对应相等。

由定义可知，次数不相同的多项式一定不相等，与零多项式相等的多项式只能是零多项式，即若

$$f(x)=\sum_{i=0}^{n}a_ix^i,$$

则 $f(x)=0 <=> a_i=0\ (i=0,1,2,\cdots,n)$

定义 $\forall f(x)$，$g(x)\in\Omega[x]$，在其中适当补上一些系数为零的项，总可设

$$f(x)=\sum_{i=0}^{n}a_ix^i \tag{2}$$

$$g(x)=\sum_{i=0}^{n}b_ix^i \tag{3}$$

令 $h(x)=\sum_{i=0}^{n}(a_i+b_i)x^i$，显然 $h(x)\in\Omega[x]$。称 $h(x)$ 为 $f(x)$ 与 $g(x)$ 相加所得的和，记为

$$f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i \tag{4}$$

令 $-g(x)=\sum_{i=0}^{n}(-b_i)x^i$，显然，$-g(x)\in\Omega[x]$，称$-g(x)$为$g(x)$的负元素，且称$f(x)+(-g(x))$为$f(x)$减去$g(x)$所得的差，记为

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

这里，减法是由加法来定义的。因此，对减法的讨论将归并在对加法的讨论之中，而不另外列出。不难验证，对于多项式的加法，有下列运算规则：

(i) $f(x)+g(x)=g(x)+f(x)$;

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

(iii) $0+f(x)=f(x)+0=f(x)$;

(iv) $f(x)+(-f(x)=0$

下面仅证明第(i)式，其余留给读者作为练习。事实上，若$f(x)$，$g(x)$如(2)、(3)所设，据加法定义，$f(x)+g(x)$的第i次项系数为a_i+b_i；$g(x)+f(x)$的第i次项系数为b_i+a_i，注意到数的加法可交换，即有$a_i+b_i=b_i+a_i$，再由多项式相等的定义，可得$f(x)+g(x)=g(x)+f(x)$。

除此之外，下列结论在多项式的运算中亦是常用的。

命题1 设$f(x)$，$g(x)\in\Omega[x]$，则

(i) $f(x)-g(x)=0 \Leftrightarrow f(x)=g(x)$;

(ii) $f(x)+h(x)=g(x)+h(x)\Leftrightarrow f(x)=g(x)$。

〔证明〕 利用相等及减法的定义，(i)立即可得。现证(ii)，充分性是显然的；又若$f(x)+h(x)=g(x)+h(x)$，

则

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

利用加法运算规则（ii）、（iv）、（iii）即可得到$f(x)=g(x)$。

证毕

定义　　$\forall f(x), g(x)\in\Omega[x]$，设

$$f(x)=\sum_{i=0}^{n} a_i x^i, \qquad g(x)=\sum_{i=0}^{m} b_i x^i$$

令 $h(x)=\sum_{r=0}^{n+m}(a_r b_0+a_{r-1}b_1+\cdots+a_0 b_r)x^r$，显然

$h(x)\in\Omega[x]$。称$h(x)$为$f(x)$与$g(x)$相乘所得的积，为

$$f(x)g(x)=\sum_{r=0}^{n+m}\Big(\sum_{i+j=r} a_i b_j\Big)x^r \tag{5}$$

例如，若$f(x)=x^2+ax+b$，$g(x)x^2+cx+d$，则

$f(x)g(x)=x^4+(c+a)x^3+(d+ac+b)x^2+(ad+bc)x+bd$,

又如，$\forall f(x)\in\Omega[x]$，有$0\cdot f(x)=0$。

不难验证，对于多项式的乘法，有下列运算规则：

（i）　$f(x)g(x)=g(x)f(x)$;

（ii）　$(f(x)g(x)h(x)=f(x)(g(x)h(x))$;

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

$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$。

以上诸式的证明与加法交换律（i）的证明类似，其主要一步是考察有关多项式的同次项系数是否全都对应相等，从而便问题转化为对于数来证明相应的交涉规则。以（ii）式为例证之：若以a_i，b_i，c_i分别代表$f(x)$、$g(x)$、$h(x)$的i次项系数，

由乘法定义，$f(x)g(x)$中r次项的系数应为

$$\sum_{i+j=r} a_i b_j$$

$(f(x)q(x))h(x)$中S次项的系数应为

$$\sum_{r+k=s} \left(\sum_{i+j=r} a_i b_j \right) c_k ;$$

同理，$g(x)h(x)$中t次项的系数应为

$$\sum_{j+k=t} b_j c_k$$

$f(x)(g(x)h(x))$中S次项的系数应为

$$\sum_{i+t=s} a_i \left(\sum_{j+k=t} b_j c_k \right),$$

利用数的运算规则（用了哪几条？）可得

$$\sum_{r+k=s} \left(\sum_{i+j=k} a_i b_j \right) c_k = \sum_{i+j+k=s} a_i b_j c_k ,$$

$$\sum_{i+t=s} a_i \left(\sum_{j+k=t} b_j c_k \right) = \sum_{i+j+k=s} a_i b_j c_k ,$$

即（ii）式两边多项式的同次项系数全都对应相等，故（ii）式成立。

与数的乘法相似，多项式的乘法无零因子，从而消去律成立。此即

命题2 若$f(x)$、$g(x) \in \Omega[x]$，且$f(x)$、$g(x) \neq 0$，则

$$f(x) \cdot g(x) \neq 0$$

〔证明〕 因$f(x)$、$g(x) \neq 0$，不妨设$f(x)$、$g(x)$的首项分别为$a_n x^n$，$b_m x^m$。由乘法定义，$f(x) \cdot g(x)$的最高次项为$a_n b_m x^{n+m}$，注意到$a_n \neq 0$，$b_m \neq 0$，故$a_n b_m \neq 0$，

即可得 $f(x)g(x)\neq 0$。

推论 若 $f(x)h(x)=g(x)h(x)$，且 $h(x)\neq 0$，

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

〔证明〕 因 $f(x)h(x)=g(x)h(x)$，利用命题1及乘法运算规则（iii）可得

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

又因 $h(x)\neq 0$，由命题2即得 $f(x)-g(x)=0$，从而

$$f(x)=g(x)$$ 证毕。

前已约定，任一非零常数可代表零次多项式。在(5)式中令 $f(x)=c$（$c\neq 0$），可得

$$cg(x)=\sum_{i=0}(cb_i)x^i$$

称 $cg(x)$ 为 c 与 $g(x)$ 相乘（数乘）所得的积。

多项式的数乘，作为其乘法的特款，有下列运算规则：

(i) $(k\ell)f(x)=k(\ell f(x))$;

(ii) $(k+\ell)f(x)=kf(x)+\ell f(x)$;

(iii) $k(f(x)+g(x))=kf(x)+kg(x)$;

(iv) $1\cdot f(x)=f(x)$

命题3 设 $f(x), g(x)\in\Omega[x]$，则

(i) $\deg(f(x)\pm g(x))\leqslant \max(\deg(f(x)), \deg(g(x)))$[①];

(ii) $\deg(f(x)\cdot g(x))=\deg(f(x))+\deg(g(x))$。

事实上，由加减法定义立即可得(i)，(ii)的证明已包含

---

①记号 $\max(a, b)$ 表示 a, b 之中较大的一个数。

Ch.5, §3, 习题10中已用max，但未说明。

在命题2的证明之中。

最后，我们指出，$\Omega[x]$中按(4)、(5)定义了加法、乘法之后，称为一元多项式环，读者稍加注意就会发现，若将Ω改为包含1的数环，本节所有的讨论结果仍然成立。

习　　题

1。证明多项式的下列运算规则

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

(ii) $(f(x)+g(x))\cdot h(x)=f(x)h(x)+g(x)h(x)$;

(iii) $(k\ell)f(x)=k(\ell f(x))$, $(k, \ell$为数$)$

2。由等式$(1+x)^m(1+x)^n=(1+x)^{m+n}$证明

$$C_m^k+C_m^{k-1}C_n^1+\cdots C_m^1C_n^{k-1}+C_n^k=C_{m+n}^k$$

3。设多项式$f(x)=q(x)g(x)+r(x)$，且$\deg(f)\geqslant\deg(g)>\deg(r)$，证明，$\deg(q)=\deg(f)-\deg(g)$。

§3 整除性

以Ω代表某一数域，下面的讨论在多项式环$\Omega[x]$中进行。

一。整除性及其性质

两个多项式相除未必都能除尽，于是有如下关于整除的定义。

定义　设$f(x)$、$g(x)\in\Omega[x]$，称$g(x)$能整除$f(x)$(记为g/f)，如果$\exists g(x)\in\Omega[x]$①，使得

$$f(x)=q(x)g(x),$$

---

①记号“$\exists$”的含义是“存在”。

否则，称$g(x)$不能整除$f(x)$（记为$g\nmid f$）。

当$g|f$时，也称$f(x)$能被$g(x)$整除。此时称$g(x)$为$f(x)$的因式，$f(x)$为$g(x)$的倍式。

由定义可得下列性质：

(i) 零多项式的因式可以是任一多项式，但其倍式只能是零多项式。

(ii) 任一多项式$f(x)$必以c，$cf(x)$为因式，其中c为任一个非零常数。

(iii) 若$f(x)|g(x)$，$g(x)|h(x)$，则$f(x)|h(x)$。

(iv) 若$f(x)|g_i(x)$ $(i=1, 2, \cdots, s)$，则$\forall u_i(x)$ $(i=1, 2, \cdots, 3)$成立 $f(x)|\sum_{i=1}^{s} u_i(x)g_i(x)$

(v) $f(x)|g(x)$且$g(x)|f(x) \Longleftrightarrow f(x)=cg(x)$，$c\neq 0$，它们的证明是容易的，下面仅证明性质(v)的必要性。由条件可设 $f(x)=h_1(x)g(x)$，$g(x)=h_2(x)f(x)$，于是

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

若$f(x)=0$，则$g(x)=h_2(x)f(x)=0$，从而$f(x)=g(x)$，结论成立；若$f(x)\neq 0$，由消去律可得

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

上式蕴含$h_1(x)\neq 0$，$h_2(x)\neq 0$，据§2命题3应有

$$deg(h_1(x))+deg(h_2(x))=0$$

从而 $deg(h_1(x))=deg(h_2(x))=0$。故可设$h_1(x)=c$，$c\neq 0$，必要性得证。

二、带余除法与整除判别法。

定理[1] $\forall f(x), g(x)\in\Omega[x]$，$g(x)\neq 0$，必存在

$g(x)$, $r(x)\in\Omega[x]$, 使得

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

其中, $r(x)=0$, 或者 $\deg(r(x))<\deg(g(x))$; 且这样的 $g(x)$, $r(x)$ 由 $f(x)$, $g(x)$ 唯一确定, 分别称它们为 $g(x)$ 除 $f(x)$ 的商式与余式。

〔证明〕将中学代数课程中的长除法一般化, 即可获得存在性的证明。下面用第二数学归纳法来表达。

若 $f(x)=0$ 或 $\deg(f)<\deg(g)$, 则取 $q(x)=0$, $r(x)=f(x)$ 即可,

若 $\deg(f)\geq\deg(g)$, 则对 $\deg(f)$ 作归纳。设

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

当 $\deg(f)=0$ 时, 设 $f(x)=a_0$ $(a_0\neq 0)$, 此时 $g(x)=b_0$ $(b_0\neq 0)$, 注意到

$$f(x)=(a_0b_0^{-1})b_0,$$

取 $q(x)=a_0b_0^{-1}$, $r(x)=0$ 即可, 当 $\deg(f)=n$ 时, 设

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

因 $n\geq m$ 且 $b_m\neq 0$, 所以 $a_nb_m^{-1}x^{n-m}\in\Omega[x]$, 令

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

显然, $f_1(x)\in\Omega[x]$ 且 $f_1(x)=0$ 或者 $\deg(f_1)<\deg(f)=\Omega$。若 $f_1(x)=0$ 或 $\deg(f_1)<\deg(g)$, 则取 $q(x)=a_nb_m^{-1}x^{n-m}$, $r(x)=f_1(x)$ 即可; 若 $\deg(f_1)\geq\deg(g)$, 注意到 $\deg(f_1)<\Omega$, 由归纳假设, 必存在 $q_1(x)$, $r_1(x)\in\Omega[x]$, 使得

$$f_1(x)=g_1(x)g(x)+r_1(x)$$

其中 $r_1(x)=0$ 或者 $\deg(r_1)<\deg(g)$, 取 $q(x)=a_nb_mx^{n-m}$

$+q_1(x)$，$r(x)=r_1(x)$即可。

再证唯一性。设另有$\tilde{q}(x)$，$\tilde{r}(x)\in\Omega[x]$，使得

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

其中$\tilde{r}(x)=0$，或者$\deg(\tilde{r})<\deg(g)$。由

$$q(x)g(x)+r(x)=\tilde{q}(x)g(x)+\tilde{r}(x),$$

得$r(x)-\tilde{r}(x)=(\tilde{q}(x)-q(x))g(x)$，
下面证明$r(x)=\tilde{r}(x)$；若不然，因$g(x)\neq 0$，故$q(x)-\tilde{q}(x)\neq 0$，由§2命题3得到

$$\deg(\tilde{r}-r)=\deg(q-\tilde{q})+\deg(g)\geqslant\deg(g)$$

但此时$r(x)$，$\tilde{r}(x)$不全为零，只可能有

$$\deg(\tilde{r}-r)=\deg(\tilde{r})<\partial(g)\quad(\text{当}r(x)=0,\ \tilde{r}(x)\neq 0\text{时}),$$

或者

$$\deg(\tilde{r}-r)\leqslant\max(\deg(\tilde{r}),\deg(r))<\partial(g)$$

于是产生了矛盾，从而必有$r(x)=\tilde{r}(x)$，因$g(x)=0$，所

---

①：第二数学归纳法原理即若要证明一有关自然数n的命题$P(n)$对自n_0始的一切自然数n成立，只要

1°证明$P(n_0)$成立；

2°在$P(k)$对一切适合$n_0\leqslant k<n$的自然数k都成立的假设之下，证明$P(n)$成立。

此外，易以上一段文字中的“自然数”为“整数”，亦可将此归纳法应用于证明与整数有关的命题。

以 $q(x)=\tilde{q}(x)$。 证毕

定理 3·1 是一元多项式环中一个基本的性质，通常称之为一元多项式环中有带余除法。下面关于最大公因式、分解因式的讨论将以它为基础。定理 3·1 的证明给出了求 $q(x)$，$r(x)$ 的具体方法，进一步，便可获得一个判别整除的方法。

定理 3·2 设 $f(x)$，$g(x)\in\Omega[x]$，$g(x)\neq 0$，则 $g(x)$ 能整除 $f(x)$ 的充分必要条件是 $g(x)$ 除 $f(x)$ 的余式为零。

〔证明〕 充分性是显然的。仅证必要性：若 $g(x)\mid f(x)$，则 $\exists\, h(x)\in\Omega[x]$，使得 $f(x)=h(x)g(x)=h(x)g(x)+0$。因 $h(x)$ 及 0 适合定理 3·1 对商式 $q(x)$、余式 $r(x)$ 的要求，由由 $q(x)$，$r(x)$ 的唯一性可得 $r(x)=0$

定理 3·2 还给出了“不能整除”的一种表述，下面用它来证明一个命题。

命题 1 设数域 $\bar{\Omega}$ 为 Ω 的扩域，$f(x)$，$g(x)\in\Omega[x]$，若在 $\Omega[x]$ 中，$g\nmid f(g/f)$，则在 $\bar{\Omega}[x]$ 中 $g\nmid f(g/f)$。

〔证明〕 仅就不能整除的情形证之。事实上，若 $g(x)=0$，因 $g\nmid f$，必有 $f(x)\neq 0$，这在 $\bar{\Omega}[x]$ 中仍有 $g\nmid f$；若 $g(x)\neq 0$，因 $g\nmid f$ 在 $\Omega[x]$ 中必 $\exists\, g(x)$，$r(x)\in\Omega[x]$，$r(x)\neq 0$ 使得

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

注意到 $\Omega\subset\bar{\Omega}$，可知 $\Omega[x]\subset\bar{\Omega}[x]$，上式亦可看作在 $\bar{\Omega}[x]$ 中成立。由定理 3·2 即得 $g\nmid f$（在 $\bar{\Omega}[x]$ 中）。

命题 1 表明，多项式的整除性不因其系数域的扩大而改变。

习　题

1，设$f_i(x)$，$g_i(x)\in\Omega[x]$，$(i=1,2)$，且$f_1(x)\neq 0$，又$f_1(x)f_2(x)$能整除$g_1(x)g_2(x)$整除，$f_1(x)$能整除，证明，$f_2(x)$能被$g_2(x)$整除。

2，设$f(x)$，$g_1(x)$，$g_2(x)\in\Omega[x]$，证明

$$(g_1(x)-g_2(x))\mid(f(g_1)-f(g_2))$$

3，求$g(x)$除$f(x)$所得的商式及余式

(i)　$f(x)=2x^3+x+1$，$g(x)=3x^3+x-4$

(ii)　$f(x)=x^4+x^3+2x^2+x-2$，$g(x)=x^2+3x+1$

4，m，p，q适合什么条件时，$g(x)$整除$f(x)$

(i)　$f(x)=x^3+px+q$，$g(x)=x^2+mx-1$

(ii)　$f(x)=x^4+px^2+q$，$g(x)=x^2+mx+1$

5，设$f(x)$，$q(x)\in\Omega[x]$，且不全为零。集合

$$P(f,g)=\{\varphi(x)\mid\varphi(x)=u(x)f(x)+v(x)g(x),\ \forall u(x),v(x)\in\Omega[x]\},$$

$\varphi_0(x)$为$P(f,g)$中次数最低者。证明：

(i)　$\varphi_0(x)$恒存在；

(ii)　$\forall\varphi(x)\in P(f,g)$，必成立$\varphi_0(x)\mid\varphi(x)$；

(iii)　$P(f,g)$中所有次数最低的多项式之间最多相差一个非零常数因子。

*6，设$f(x)$，$\varphi(x)\in\Omega[x]$，且$\deg(\varphi)>0$。证明，存在$c_i(x)\in\Omega[x]$，$(i=0,1,2,\cdots,k)$，使得

$$f(x)=C_k(x)\varphi^k(x)+C_{k-1}(x)\varphi^{k-1}(x)+\cdots+C_1(x)\varphi(x)+C_0(x),$$