目　录

第一章　多项式

§1　数域

关于数的加、减、乘、除等运算的性质通常称为数的代数性质.代数所研究的问题主要涉及数的代数性质,这方面的大部分性质是有理数、实数、复数所共有的.

定义 1　设 P 是由一些复数组成的集合,其中包括 0 与 1.如果 P 中任意两个数的和、差、积、商(除数不为零)仍然是 P 中的数,那么 P 就称为一个数域.

显然,全体有理数组成的集合、全体实数组成的集合、全体复数组成的集合都是数域.这三个数域分别用字母 Q 、R 、C 来代表.但是,全体整数组的集合不是数域,因为任意两个整数的商不一定是整数.

如果数的集合 P 中任意两个数作某一种运算的结果都仍在 P 中,就说数集 P 对这个运算是封闭的.因此数域的定义也可以说成,如果一个包含 0,1 在内的数集 P 对于加法、减法、乘法与除法(除数不为零)是封闭的,那么 P 就称为一个数域.

例 1　所有具有形式

$$a+\sqrt{2}b$$

的数(其中 a,b 是任意有理数),构成一个数域.通常用 $Q(\sqrt{2})$ 来表示这个数域.显然,数集 $Q(\sqrt{2})$ 包含 0 与 1,并且它对于加减法是封闭的.现在证明它对乘法也是封闭的.我们知道 $(a+\sqrt{2}b)(c+\sqrt{2}d)=(ac+2bd)+(ad+bc)\sqrt{2}$.

因为 a,b,c,d 都是有理数,所以 $ac+2bd$,$ad+bc$ 也是有理数.这就说明乘积 $(a+\sqrt{2}b)(c+\sqrt{2}d)$ 还在 $Q(\sqrt{2})$ 内,所以 $Q(\sqrt{2})$ 对于乘法是封闭的.

设 $a+\sqrt{2}b\neq 0$,于是 $a-\sqrt{2}b\neq 0$,而

$$\begin{aligned}\frac{c+\sqrt{2}d}{a+\sqrt{2}b}&=\frac{(c+\sqrt{2}d)(a-\sqrt{2}b)}{(a+\sqrt{2}b)(a-\sqrt{2}b)}\\&=\frac{ac-2bd}{a^2-2b^2}+\frac{ad-bc}{a^2-2b^2}\sqrt{2}.\end{aligned}$$

因为 a,b,c,d 是有理数,所以 $\frac{ac-2bd}{a^2-2b^2}$,$\frac{ad-bc}{a^2-2b^2}$ 也是有理数.所以 $Q(\sqrt{2})$ 对于除法也是封闭的.

例 2　所有可以表成形式

$\dfrac{a_0+a_1\pi+a_2\pi^2+\cdots a_n\pi^n}{b_0+b_1\pi+b_2\pi^2+\cdots b_m\pi^m}$ 的数组成一个数域,其中 m ,n 为任意非负整数,a_i ,b_j $(i=0,1\cdots n;j=0,1\cdots m)$ 是整数(自证).

例 3 所有奇数组成的数集,对于乘法是封闭的,但对于加、减法不是封闭的.

性质:任何的数域都包含有理数域作为它的一部分.

事实上,设 P 是一个数域,由定义可知,P 含有 1. 根据 P 对于加法的封闭性,$1+1=2,1+2=3,\cdots 1+n=1+n$ 全在 P 中,换句话说,P 包含全体自然数. 又因为数 0 在 P 中,再由 P 对减法的封闭性,$0-n=-n$ 也在 P 中,因而 P 包含全体整数. 任何一个有理数都可以表示成两个整数的商,由 P 对除法的封闭性即得上述结论. 换句话说,有理数是最小的数域.

§2 一元多项式

一、一元多项式

定义 2 设 n 是一非负整数,形式表达式

$$a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_0. \tag{1-2-1}$$

其中 $a_0,a_1,a_2\cdots a_n$ 全属于数域 P ,称为系数在数域 P 中的一元多项式,或者简称为数域 P 上的一元多项式.

在上述多项式(1-2-1)中,a_ix^i 称为 i 次项,a_i 称为 i 次项的系数. 以后用 $f(x)$,$g(x)$,… 或 $f,g,\cdots$ 等来表示多项式.

注意:这里定义的多项式是符号或文字的形式表达式. 当这个符号是未知数时,它就是我们中学数学中的代数多项式,根据应用需要,这个符号还可以代表其他应用事物.

定义 3 如果在多项式 $f(x)$ 与 $g(x)$ 中,除去系数为零的项外,同次项的系数全相等,那么 $f(x)$ 与 $g(x)$ 就称为相等,记为

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

系数全为零的多项式称为零多项式,记为 0.

在(1-2-1)中,如果 $a_n\neq 0$,那么 a_nx^n 称为多项式(1-2-1)的首项,a_n 称为首项系数,n 称为多项式(1-2-1)的次数. 零多项式是唯一不定义次数的多项式. 多项式 $f(x)$ 的次数记为

$$\partial(f(x)).$$

因为零多项式不定义次数,所以在用符号 $\partial(f(x))$ 时,总是假定 $f(x)\neq 0$.

二、多项式的运算

设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0,$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_1x+b_0$$

是数域 P 上两个多项式,那么可以写成

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

$$g(x)=\sum_{i=0}^{m}b_ix^i.$$

在表示多项式 $f(x)$ 与 $g(x)$ 的和时,如 $n\geqslant m$,为了方便起见,在 $g(x)$ 中令 $b_n=b_{n-1}=b_{n-2}=\cdots=b_{m+1}=0$,那么 $f(x)$ 与 $g(x)$ 的和为

$$\begin{aligned}f(x)+g(x)&=(a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\cdots+(a_1+b_1)x+(a_0+b_0)\\&=\sum_{i=0}^{n}(a_i+b_i)x^i,\end{aligned}$$

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 s 次项的系数是

$$a_sb_0+a_{s-1}b_1+a_{s-2}b_2+\cdots a_1b_{s-1}+a_0b_s=\sum_{i+j=s}a_ib_j,$$

所以 $f(x)g(x)$ 可表成

$$f(x)g(x)=\sum_{s=0}^{n+m}(\sum_{i+j=s}a_ib_j)x^s.$$

显然,数域 P 上的两个多项式经过加、减、乘运算后,所得结果仍然是数域 P 上的多项式.

对于多项式的加减法,不难看出

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

对于多项式的乘法,可以证明,若 $f(x)\neq 0$, $g(x)\neq 0$,则 $f(x)g(x)\neq 0$,且

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

由以上证明看出,多项式乘积的首项系数就等于因子首项系数的乘积.

和数的运算一样,多项式的运算满足以下的一些规律:

1. 加法交换律:$f(x)+g(x)=g(x)+f(x)$;
2. 加法结合律:$[f(x)+g(x)]+h(x)=f(x)+[g(x)+h(x)]$;
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:$f(x)[g(x)+h(x)]=f(x)g(x)+f(x)h(x)$;
6. 乘法消去律:若 $f(x)g(x)=f(x)h(x)$,且 $f(x)\neq 0$,则 $g(x)=h(x)$.

定义 4　所有系数在数域 P 中的一元多项式的全体,称为数域 P 上的一元多项式环,记为 $P[x]$,P 称为 $P[x]$ 的系数域.

§3　整除的概念

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——除法运

算，并不是普遍可以做的. 因此整除就成了两个多项式之间的一种特殊的关系.

一、整除的概念

和中学代数一样，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. 例如，设

$$f(x)=3x^3+4x^2-5x+6,$$
$$g(x)=x^2-3x+1.$$

我们可以按如下方法来做除法：

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

于是求得商为 $3x+13$，余式为 $31x-7$. 所得结果可以写成

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

这种求法实际上具有一般性.

带余除法：对于 $P[x]$ 中任意两个多项式 $f(x)$ 与 $g(x)$，其中 $g(x)\neq 0$，一定有 $P[x]$ 中的多项式存在，使得

$$f(x)=q(x)g(x)+r(x) \tag{1-3-1}$$

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

带余除法中所得的 $q(x)$ 通常称为 $g(x)$ 除 $f(x)$ 的商，$r(x)$ 称为 $g(x)$ 除 $f(x)$ 的余式.

定义 5 数域 P 上的多项式 $g(x)$ 称为整除 $f(x)$，如果有数域 P 上的多项式 $h(x)$ 使等式

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

成立. 用“$g(x)\mid f(x)$”表示 $g(x)$ 整除 $f(x)$，用“$g(x)\nmid f(x)$”表示 $g(x)$ 不能整除 $f(x)$.

当 $g(x)\mid f(x)$ 时，$g(x)$ 就称为 $f(x)$ 的因式，$f(x)$ 称为 $g(x)$ 的倍式.

当 $g(x)\neq 0$ 时，带余除法给出了整除性的一个判别条件.

定理 1 对于数域 P 上的任意两个多项式 $f(x)$，$g(x)$，其中 $g(x)\neq 0$，$g(x)\mid f(x)$ 的充要条件是 $g(x)$ 除 $f(x)$ 的余式为零.

带余除法中 $g(x)$ 必须不为零. 但 $g(x)\mid f(x)$ 中，$g(x)$ 可以为零. 这时

$$f(x)=g(x)\cdot h(x)=0\cdot h(x)=0.$$

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

二、整除的性质

1. 任一多项式 $f(x)$ 一定整除它自身.

2. 任一多项式 $f(x)$ 都能整除零多项式.

3. 零次多项式，即非零常数，能整除任一个多项式.

4. 若 $f(x)\mid g(x)$，$g(x)\mid f(x)$，则 $f(x)=cg(x)$，其中 c 为非零常数.

5. 若 $f(x)\mid g(x)$，$g(x)\mid h(x)$，则 $f(x)\mid h(x)$（整除的传递性）.

6. 若 $f(x)\mid g_i(x)$，$i=1,2,3,\cdots r$ 则

$$f(x)\mid(u_1(x)g_1(x)+u_2(x)g_2(x)+u_3(x)g_3(x)+\cdots u_r(x)g_r(x)),$$

其中 $u_i(x)$ 是数域 P 上任意的多项式.

通常，$u_1(x)g_1(x)+u_2(x)g_2(x)+u_3(x)g_3(x)+\cdots u_r(x)g_r(x)$ 称为

$$g_1(x),g_2(x),g_3(x),\cdots,g_r(x)$$

的一个组合.

由以上性质可以看出，$f(x)$ 与它的任一个非零常数倍 $cf(x)$（$c\neq 0$）有相同的因式，也有相同的倍式. 因之，在多项式整除性的讨论中，$f(x)$ 常常可以用 $cf(x)$ 来代替.

最后，两个多项式之间的整除关系不因系数域的扩大而改变. 即若 $f(x)$，$g(x)$ 是 $P[x]$ 中两个多项式，$\bar{P}$ 是包含 P 的一个较大的数域，则 $f(x)$，$g(x)$ 也可以看成是 $\bar{P}[x]$ 中的多项式. 从带余除法可以看出，不论把 $f(x)$，$g(x)$ 看成是 $P[x]$ 中或者是 $\bar{P}[x]$ 中的多项式，用 $g(x)$ 去除 $f(x)$ 所得的商式及余式都是一样的.

因此，若在 $P[x]$ 中 $g(x)$ 不能整除 $f(x)$，则在 $\bar{P}[x]$ 中，$g(x)$ 也不能整除 $f(x)$.

§4 多项式的最大公因式

一、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，那么 $\varphi(x)$ 就称为 $f(x)$ 与 $g(x)$ 的一个公因式.

定义 6 设 $f(x)$ 与 $g(x)$ 是 $P[x]$ 中两个多项式. $P[x]$ 中多项式 $d(x)$ 称为 $f(x)$，$g(x)$ 的一个最大公因式，如果它满足下面两个条件：

1. $d(x)$ 是 $f(x)$ 与 $g(x)$ 的公因式；

2. $f(x)$，$g(x)$ 的公因式全是 $d(x)$ 的因式.

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. 特别地，根据定义，两个零多项式的最大公因式就是 0.

引理 如果有等式

$$f(x)=q(x)g(x)+r(x) \tag{1-4-1}$$

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

定理 2 对于 $P[x]$ 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 $d(x)$ 可以表成 $f(x)$，$g(x)$ 的一个组合，即有 $P[x]$ 中多项式 $u(x)$，$v(x)$ 使

$$d(x)=u(x)f(x)+v(x)g(x). \tag{1-4-2}$$

由最大公因式的定义不难看出，如果 $d_1(x)$，$d_2(x)$ 是 $f(x)$，$g(x)$ 的两个最大公因式，那么一定有 $d_1(x)\,|\,d_2(x)$ 与 $d_2(x)\,|\,d_1(x)$，也就是说 $d_1(x)=cd_2(x)$（$c\neq 0$）.

这就是说，**两个多项式的最大公因式在可以相差一个非零常数倍的意义下是唯一确定的**. 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. 在这个情形下，我们约定用

$$(f(x),g(x))$$

来表示首项系数是 1 的那个最大公因式.

用来求最大公因式的方法通常称为辗转相除法(Euclidean Algorithm).

例 1 设

$$f(x)=x^4+3x^3-x^2-4x-3,$$
$$g(x)=3x^3+10x^2+2x-3,$$

求 $(f(x),g(x))$，并求 $u(x)$ 和 $v(x)$，使

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

辗转相除法可按照以下格式来作：

	$g(x)$	$f(x)$	
$-\frac{27}{5}x+9$	$3x^3+10x^2+2x-3$	$x^4+3x^3-x^2-4x-3$	$\frac{1}{3}x-\frac{1}{9}$
$=q_2(x)$	$3x^3+15x^2+18x$	$x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x$	$=q_1(x)$
	$-5x^2-16x-3$	$-\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3$	
	$-5x^2-25x-30$	$-\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3}$	
	$r_2(x)=9x+27$	$r_1(x)=-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}$	$-\frac{5}{81}x-\frac{10}{81}$
		$-\frac{5}{9}x^2-\frac{5}{3}x$	$=q_3(x)$
		$-\frac{10}{9}x-\frac{10}{3}$	
		$-\frac{10}{9}x-\frac{10}{3}$	
		0	

用等式写出来，就是

$$f(x)=(\frac{1}{3}x-\frac{1}{9})g(x)+(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}),$$

$$g(x)=(-\frac{27}{5}x+9)(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3})+(9x+27),$$

$$-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}=(-\frac{5}{81}x-\frac{10}{81})(9x+27).$$

因之

$$(f(x),g(x))=x+3,$$

而

$$\begin{aligned}9x+27&=g(x)-(-\frac{27}{5}x+9)(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3})\\&=g(x)-(-\frac{27}{5}x+9)[f(x)-(\frac{1}{3}x-\frac{1}{9})g(x)]\\&=(\frac{27}{5}x-9)f(x)+[1-(\frac{27}{5}x-9)(\frac{1}{3}x-\frac{1}{9})]g(x)\\&=(\frac{27}{5}x-9)f(x)+(-\frac{9}{5}x^2+\frac{18}{5}x)g(x),\end{aligned}$$

于是

$$(f(x),g(x))=(\frac{3}{5}x-1)f(x)+(-\frac{1}{5}x^2+\frac{2}{5}x)g(x).$$

注:定理 2 的逆不成立.例如,令

$$f(x)=x,\ g(x)=x+1,$$

则

$$x(x+2)+(x+1)(x-1)=2x^2+2x-1.$$

但 $2x^2+2x-1$ 显然不是 $f(x)$ 与 $g(x)$ 的最大公因式.

但是当(1-4-2)式成立,而 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个公因式,则 $d(x)$ 一定是 $f(x)$ 与 $g(x)$ 的一个最大公因式.

二、多项式互素

定义 7　$P[x]$ 中两个多项式 $f(x)$,$g(x)$ 称为互素(也称为互质),如果

$$(f(x),g(x))=1.$$

显然,两个多项式互素,那么它们除去零次多项式外没有其他的公因式;反之亦然.

定理 3　$P[x]$ 中两个多项式 $f(x)$,$g(x)$ 互素的充分必要条件是有 $P[x]$ 中多项式 $u(x)$,$v(x)$ 使

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

定理 4　如果 $(f(x),g(x))=1$,且 $f(x)\mid g(x)h(x)$,那么

$$f(x)\mid h(x).$$

证明　由 $(f(x),g(x))=1$ 可知,有 $u(x)$,$v(x)$ 使

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

等式两边同乘 $h(x)$，得

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

因为 $f(x)\mid g(x)h(x)$，所以 $f(x)$ 整除等式左端，从而

$$f(x)\mid h(x).$$

推论 1　如果 $f_1(x)\mid g(x)$，$f_2(x)\mid g(x)$，且 $(f_1(x),f_2(x))=1$，那么

$$f_1(x)f_2(x)\mid g(x).$$

推论 2　如果 $(f_1(x),g(x))=1$，$(f_2(x),g(x))=1$，那么 $(f_1(x),f_2(x),g(x))=1$.

推广：对于任意多个多项式 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)(s\geqslant 2)$，$d(x)$ 称为 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)(s\geqslant 2)$ 的一个最大公因式，如果 $d(x)$ 具有下面的性质：

1. $d(x)\mid f_i(x)$，$i=1,2,3,\cdots s$；

2. 如果 $\varphi(x)\mid f_i(x)$，$i=1,2,3,\cdots s$，那么 $\varphi(x)\mid d(x)$.

我们仍用符号 $(f_1(x),f_2(x),f_3(x),\cdots,f_s(x))$ 来表示首项系数为 1 的最大公因式. 不难证明 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 的最大公因式存在，而且当

$$f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$$

全不为零时，$((f_1(x),f_2(x),f_3(x)\cdots,f_{s-1}(x),f_s(x))$ 就是 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 的最大公因式，即

$$f_1(x),f_2(x),f_3(x)\cdots f_s(x)=(f_1(x),f_2(x),f_3(x)\cdots,f_{s-1}(x),f_s(x)).$$

同样，利用以上这个关系可以证明，存在多项式 $u_i(x)$，$i=1,2,3,\cdots s$，使

$$u_1(x)f_1(x)+u_2(x)f_2(x)+u_3(x)f_3(x)+\cdots u_s(x)f_s(x)$$
$$=(f_1(x),f_2(x),\cdots,f_{s-1}(x),f_s(x)).$$

如果 $(f_1(x),f_2(x),\cdots,f_{s-1}(x),f_s(x))=1$，那么 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 就称为互素的. 同样有类似定理 3 的结论.

注意：(1)当一个多项式整除两个多项式之积时，若没有互素的条件，这个多项式一般不能整除积的因式之一. 例如

$$x^2-1\mid(x+1)^2(x-1)^2\text{，但 }x^2-1\nmid(x+1)^2\text{，且 }x^2-1\nmid(x-1)^2.$$

(2)推论 1 中没有互素的条件，则不成立. 如

$$g(x)=x^2-1,\ f_1(x)=x+1,\ f_2(x)=(x+1)(x-1),$$

则 $f_1(x)\mid g(x)$，$f_2(x)\mid g(x)$，但 $f_1(x)f_2(x)\nmid g(x)$.

注意：s $(s\geqslant 2)$ 个多项式 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 互素时，它们并不一定两两互素. 例如，多项式

$$f_1(x)=x^2-3x+2,\ f_2(x)=x^2-5x+6,\ f_3(x)=x^2-4x+3$$

是互素的，但 $(f_1(x),f_2(x))=x-2$.

令 $\overline{P}$ 是含 P 的一个数域，$d(x)$ 是 $P[x]$ 的多项式 $f(x)$ 与 $g(x)$ 在 $P[x]$ 中的首

项系数为 1 的最大公因式，而 $\overline{d}(x)$ 是 $f(x)$ 与 $g(x)$ 在 $\overline{P}[x]$ 中首项系数为 1 的最大公因式，那么 $\overline{d}(x)=d(x)$. 即从数域 P 过渡到数域 $\overline{P}$ 时，$f(x)$ 与 $g(x)$ 的最大公因式本质上没有改变.

互素多项式的性质可以推广到多个多项式的情形：

1. 若多项式 $h(x)\mid f_1(x)f_2(x)f_3(x)\cdots f_s(x)$，并 $h(x)$ 与 $f_1(x),\cdots,f_{i-1}(x)$，$f_{i+1}(x),\cdots,f_s(x)$ 互素，则 $h(x)\mid f_i(x)$ ，$(1\leq i\leq s)$.

2. 若多项式 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 都整除 $h(x)$ ，且 $f_1(x),f_2(x)$，$f_3(x),\cdots,f_s(x)$ 两两互素，则 $f_1(x)f_2(x)f_3(x)\cdots f_s(x)\mid h(x)$.

3. 若多项式 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 都与 $h(x)$ 互素，则

$$(f_1(x)f_2(x)\cdots f_s(x),h(x))=1 .$$

§5　因式分解定理

在中学所学习的代数里，我们学过把一个多项式分解为不能再分解的因式的乘积，但那时所谓的不能再分解，常常只是我们看不出怎样分解下去. 所谓不能再分解，其实不是绝对的，而是相对于系数所在的数域而言的. 例如，在有理数域里，把 x^4-4 分解为

$$(x^2-2)(x^2+2)$$

的形式就不能再分解了，但在数域 $Q(\sqrt{2})$ 上，甚至扩大些，在实数域上，就可以进一步分解成为

$$(x-\sqrt{2})(x+\sqrt{2})(x^2+2),$$

而在复数域上，还可以进一步分解成为

$$(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i).$$

由此可见，所谓的不能再分解并不绝对，在明确系数域后，不能再分解才能有明确的涵义.

一、不可约多项式

定义 8　数域 P 上次数大于等于 1 的多项式 $p(x)$ 称为域 P 上的不可约多项式 (Irreducible Polynomial)，如果它不能表成数域 P 上两个次数比 $p(x)$ 的次数低的多项式的乘积.

根据定义，一次多项式总是不可约多项式.

一个多项式是否可约是依赖于系数域的.

显然，不可约多项式 $p(x)$ 的因式只有非零常数与它自身的非零常数倍 $cp(x)$ ，$c\neq 0$ 这两种，此外就没有了. 反过来，具有这个性质的次数大于等于 1 的多项式一定是不可约的. 由此可知，不可约多项式 $p(x)$ 与任一多项式 $f(x)$ 之间只可能有两种关系，或者 $p(x)\mid f(x)$ 或者 $(p(x),f(x))=1$.

定理 5　如果 $p(x)$ 是不可约多项式，那么对于任意的两个多项式 $f(x)$ 与

$g(x)$，由 $p(x)\mid f(x)g(x)$ 一定能推出 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$.

推广　如果不可约多项式 $p(x)$ 整除一些多项式 $f_1(x),f_2(x),f_3(x),\cdots,f_s(x)$ 的乘积 $f_1(x)f_2(x)f_3(x)\cdots f_s(x)$，那么 $p(x)$ 一定整除这些多项式之中的一个.

二、因式分解定理

数域 P 上次数大于等于1的多项式 $f(x)$ 都可以唯一地分解成数域 P 上一些不可约多项式的乘积，此为因式分解及唯一性定理.

所谓唯一性是说，如果有两个分解式

$$f(x)=p_1(x)p_2(x)p_3(x)\cdots p_s(x)=q_1(x)q_2(x)q_3(x)\cdots q_t(x),$$

那么必有 $s=t$，并且适当排列因式的次序后有

$$p_i(x)=c_iq_i(x),$$

其中 $i=1,2,3,\cdots s$ 是一些非零常数.

应该指出，因式分解定理虽然在理论上有其基本重要性，但是它并没有给出一个具体的分解多项式的方法. 实际上，对于一般的情形，普遍可行的分解多项式的方法是不存在的.

在多项式 $f(x)$ 的分解式中，可以把每一个不可约因式的首项系数提出来，使它们成为首项系数为 1 的多项式，再把相同的不可约因式合并. 于是 $f(x)$ 的分解式成为

$$f(x)=cp_1^{r_1}(x)cp_2^{r_2}(x)cp_3^{r_3}(x)\cdots cp_s^{r_s}(x),$$

其中 c 是 $f(x)$ 的首项系数，$p_1(x),p_2(x),p_3(x),\cdots,p_s(x)$ 是不同的首项系数为 1 的不可约多项式，而 $r_1,r_2,r_3,\cdots,r_s$ 是正整数. 这种分解式称为标准分解式.

如果已经有了两个多项式的标准分解，就可以直接写出两个多项式的最大公因式. 多项式 $f(x)$ 与 $g(x)$ 的最大公因式 $d(x)$ 就是那些同时在 $f(x)$ 与 $g(x)$ 的标准分解式中出现的不可约多项式方幂的乘积，所带的方幂的指数等于它在 $f(x)$ 与 $g(x)$ 中所带的方幂中较小的一个.

由以上讨论可以看出，带余除法是一元多项式因式分解理论的基础.

若 $f(x)$ 与 $g(x)$ 的标准分解式中没有共同的不可约多项式，则 $f(x)$ 与 $g(x)$ 互素.

注意：上述求最大公因式的方法不能代替辗转相除法，因为在一般情况下，没有实际分解多项式为不可约多项式的乘积的方法，即使要判断数域 P 上一个多项式是否可约一般都是很困难的.

例如多项式 $f(x)=x^3+x^2-2x-2$，在有理数域上就可以分解为不可约多项式的乘积.