高等代数

申富饶教授主讲

89686522(O)
frshen@nju.edu.cn
http://cs.nju.edu.cn/rinc

课程助教信息

安俊逸 sky771674990@qq.com

韩峰 robocoder@foxmail.com

梅鸿远 meihongyuan@smail.nju.edu.cn

http://cs.nju.edu.cn/rinc/index.html

校内论坛→课程论坛→高等代数

主要参考书目

高等代数, (第四版）,北京大学数学系前代数小组，王萼芳、石生明修订，高等教育出版社,2013年版。

高等代数， 林成森、盛松柏编，南京大学出版社，1993。

考核方式

考试方法:　平时成绩　　40%

　　　　闭卷考试　　60%

平时成绩含作业、出勤情况和期中考试。

作业、出勤缺 **三** 次以上者平时成绩 **0** 分

引言

简介

- 几何学：研究客观世界的空间形式
- **代数学：通过运算来研究客观世界的数量关系**
- 分析学：用变化的观点研究客观世界中数量之间的确定性依赖关系
- 概率统计：研究客观世界中的不确定现象（随机现象）

观察→抽象→探索→猜测→论证

融会贯通、认真听讲、多做习题

数

- 数的概念：是一个用作计数、标记或用作量度的抽象概念，是比较同质或同属性事物的等级的简单符号记录形式
  - 通过对现实事物数数这种方式得到了数
  - 数可以使用一定的方式进行运算
  - 数同空间事物相联系时，可表明这些事物的多少
- 数的发展史
  - 抽象的概念：“有”和“无”
  - “一、二、三、多”
  - 用一些符号代替数——进一步抽象（正的含义）
  - 自然数：数量、次序（基数、序数）
  - 0的出现、负数、整数
  - 有理数、无理数、实数、复数（狭义数）→？（广义数）
- 数集合是否对于运算是封闭发展出新的数的概念

随着对于“数”的概念的认知发展，人类的智力不断提高

代数

- 算术：数和数之间的四则运算——加、减、乘、除
- 代数：
  - 运算：加、减、乘、除扩展到包括乘方和开方
  - 研究对象：数扩展到矩阵、向量、向量空间及其变换
    - 研究未知数更多的一次方程组，引进矩阵、向量、空间等符号和概念，形成“线性代数”；
    - 研究未知数次数更高的高次方程，形成“多项式代数”（也叫“多项式理论”）
- 代数学的内容可以概括称为带有运算的一些代数结构的集合
  - 如群、环、域等
  - 包含抽象代数、布尔代数、关系代数、计算机代数等众多分支

高等代数

- 初等代数：研究实数和复数，以及以它们为系数的代数式的代数运算理论和方法的数学分支学科
  - 三种数——有理数、无理数、复数
  - 三种式——整式、分式、根式（统称代数式）
  - 三类方程——整式方程、分式方程、无理方程（统称代数方程）
  - 以及由有限多个代数方程联立而成的代数方程组
  - 从最简单的一元一次方程开始，一方面进而讨论二元及三元的一次方程组，另一方面研究二次以上及可以转化为二次的方程组
- 高等代数：初等代数在这两个方向的继续发展
  - 讨论任意多个未知数的一次方程组→线性代数
  - 研究次数更高的一元方程组→多项式代数
  - 是代数学发展到高级阶段的总称，包括许多分支

高等代数的重要性

- 高等代数课程中体现了近代数学的一个重要思想: 空间、结构、关联

- 诸多工程计算中涉及的矩阵、行列式和大规模线性方程组、代数特征值等都以该课程为主要基础

- 高等代数及其相关课程是现代信息科学与技术领域研究的重要工具和手段

高等代数

- 多项式
- 行列式
- 线性方程组
- 矩阵
- 二次型
- 线性空间
- 线性变换
- 欧几里得空间

第1章 多项式

§ 1 数域

- 对所要讨论的问题，通常要明确所考虑的数的范围，不同范围内同一问题的回答可能是不同的。例如，$x^2+1=0$在实数范围与复数范围内解的情形不同。
- 常遇到的数的范围：有理数集 、实数集、复数集

  共性（代数性质）：加、减、乘、除运算性质
- 有些其它数集也有与有理数集 、实数集、复数集相同的代数性质

  为在讨论中将其统一起来，引入一个一般的概念——数域。

数域的定义

- 数域的定义　设P是由一些数组成的集合，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）仍在P中，则称P为一个数域.
- 常用数域：有理数域**Q** 、实数域**R**、复数域**C**

- 数域定义的另一形式　包含0与1的数集P，如果对于加法、减法、乘法、除法（除数不为零）运算封闭，则称P为一个数域.

复数 $a+bi$; $i^2=-1$

数域

如果复数的一个非空集合 P 含有非零的数，且其中任意两数的和、差、积、商（除数不为零）仍属于该集合，则称数集 P 为一个数域.

- 自然数集合 N
- 整数集合 z
- 有理数集合 Q
- 实数集合 R
- 复数集合 c
- 集合 $A(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}$

是否构成数域?

- 自然数域 ✕
- 整数域 ✕
- 有理数域 √
- 实数域 √
- 复数域 √

注意：所有的数域都包含有理数域，且都包含整数 0 和 1

每个数的否（逆）也在同一数域中

例1　所有形如 $a+b\sqrt{2}$（a, b是有理数）的数集构成一个数域． $Q(\sqrt{2})$

解　(i)　$0,1\in Q(\sqrt{2})$;

(ii) 对四则运算封闭．事实上

$\forall\alpha,\beta\in Q(\sqrt{2})$, 设 $\alpha=a+b\sqrt{2}, \beta=c+d\sqrt{2}$, 有

$$\alpha\pm\beta=(a\pm c)+(b\pm d)\sqrt{2}\in Q(\sqrt{2})$$

$$\alpha\beta=(ac+2bd)+(ad+bc)\sqrt{2}\in Q(\sqrt{2})$$

设$\alpha = a + b\sqrt{2} \neq 0$，则$a - b\sqrt{2} \neq 0$,这是因为

若$a - b\sqrt{2} = 0$,则$a = b\sqrt{2}$，于是$\dfrac{a}{b} = \sqrt{2} \in Q$

或者$a = 0, b = 0$, $\Rightarrow a + b\sqrt{2} = 0$,矛盾.

$$\frac{\beta}{\alpha} = \frac{c + d\sqrt{2}}{a + b\sqrt{2}} = \frac{(c + d\sqrt{2})(a - b\sqrt{2})}{(a + b\sqrt{2})(a - b\sqrt{2})}$$

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

3. 有理数域是一个最小的数域

（任何数域都包含有理数域作为它的一部分）

证：设P为一个数域.

由定义知$1\in P$，又P对加法封闭知：1+1=2，1+2=3，…P包含所有自然数；

由$0\in P$及P对减法的封闭性知：P包含所有负整数，因而P包含所有整数；

任何一个有理数都可以表为两个整数的商，由P对除法的封闭性知：P包含所有有理数. 即

任何数域都包含有理数域作为它的一部分.

§ 2 一元多项式（以固定数域P为基础）

定义 设x是一个符号，n为非负整数。形式表达式

i 次项

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0$$

首项($a_n \neq 0$)　　i 次项系数　　$a_i (i = 0,1,2,\cdots,n) \in P$

称为系数在数域P中的一元多项式，简称为数域P上的一元多项式.

符号x 可以是为未知数，
也可以是其它待定事物.

习惯上记为$f(x)$，$g(x)$……或f, g……上述形式表达式可写为

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

几个概念

- 零多项式 ——系数全为0的多项式
- 零次多项式 ——仅含常数项
- 多项式相等 ——$f(x)=g(x)$当且仅当同次项的系数全相等（系数为零的项除外）
- 多项式$f(x)$的次数 ——$f(x)$的最高次项对应的幂次，记作$\partial(f(x))$ 或$deg(f(x))$.

如：$f(x)=3x^3+4x^2-5x+6$的次数为3，即 $\partial(f(x))=3$

2. 多项式的运算

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

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

$$f(x)-g(x)=(2x^2+3x-1)-(x^3+2x^2-3x+2)=-x^3+6x-3$$

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

$$=2x^5+7x^4-x^3-7x^2+9x-2$$

乘法较为复杂，应用竖式方便、明了：

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

- $f(x)\,g(x)=2x^5+7x^4-x^3-7x^2+9x-2$

或为更简明，应用分离系数法进行：

设$f(x)$，$g(x)$为数域P上的一元多项式，不妨令

$$f(x)=\sum_{i=0}^{n}a_ix^i,\quad g(x)=\sum_{j=0}^{m}b_jx^j$$

加法：$f(x)\pm g(x)$ $=\sum_{i=0}^{n}(a_i\pm b_i)x^i$，当$n\geq m$

乘法：$f(x)g(x)$ $=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}+\cdots+a_0b_0$

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

结论: (1) $\partial(f(x)\pm g(x))\le max(\partial(f(x)), \partial(g(x))$

(2) $\partial(f(x)g(x))=\partial(f(x))+\partial(g(x))$,当 $f(x)\neq 0, g(x)\neq 0$

且乘积的首项系数等于因子首项系数的乘积

(3) 数域P上的两个多项式经过加、减、乘等运算后，

所得结果仍然是数域P上的多项式

运算律 设$f(x),g(x),h(x)$为数域P上的一元多项式,则

（1）$f(x)+g(x)=g(x)+f(x)$

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

（3）$f(x)g(x)=g(x)f(x)$

（4）$(f(x)g(x))h(x)=f(x)(g(x)h(x))$

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

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

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

证（4）$(f(x)g(x))h(x)=f(x)\,(g(x)\,h(x))$

设 $f(x)=\sum_{i=0}^{n}a_i x^i, g(x)=\sum_{j=0}^{m}b_j x^j$， $h(x)=\sum_{k=0}^{l}c_k x^k$

考虑等式两端 t次项的系数.

左边：$f(x)g(x)$中s次项的系数为 $\sum_{i+j=s}a_i b_j$

故t次项的系数 $\sum_{s+k=t}(\sum_{i+j=s}a_i b_j)c_k = \sum_{i+j+k=t}a_i b_j c_k$

右边：$g(x)\,h(x)$中r次项的系数为 $\sum_{j+k=r}b_j c_k$

故t次项的系数 $\sum_{i+r=t}a_i(\sum_{j+k=r}b_j c_k)= \sum_{i+j+k=t}a_i b_j c_k$ $\|$

证毕.

例1 当a,b,c取何制值时，多项式$f(x)=x-5$与$g(x)=a(x-2)^2+b(x+1)+c(x^2-x+2)$相等？

解 由于

$$g(x)=(a+c)x^2+(-4a+b-c)x+(4a+b+2c)$$

根据多项式相等的定义，得

$$\begin{cases} a+c=0 \\ -4a+b-c=1 \\ 4a+b+2c=-5 \end{cases}$$

解之得 $a=-\dfrac{6}{5}, b=-\dfrac{13}{5}, c=\dfrac{6}{5}.$

例2 设 $f(x)$, $g(x)$与$h(x)$为实数域上多项式. 证明：如果

$$f^2(x)= x\,g^2(x)+ x\,h^2(x)$$

则 $f(x)=g(x)=h(x)=0$

…$\neq 0$，则$f^2(x)\neq 0$.由

…$x) = x\,g^2(x)+ x\,h^2(x) = x(g^2(x)+h^2(x))$

$\neq 0$.因此

…$)) =\partial(x(g^2(x)+h^2(x)))$

…偶数,而$\partial(x(g^2(x)+x\,h^2(x)))$为奇数,因此

$$f^2(x)\neq x\,g^2(x)+ x\,h^2(x)$$

故$f(x)=0$.此时 $x(g^2(x)+ h^2(x))=0$.但 x 为一非

…有 $g^2(x)+ h^2(x)=0$

为什么？

…$x)$为实系数多项式，必有$g(x)=h(x)=0$.于是

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

> 若$g(x)\neq 0$，由于实数域内，非0数的平方为正数,所以$f^2(x)$的最高次项系数为正数.当
>
> $g^2(x)+ h^2(x)=0$
>
> 时, $h^2(x)$的最高次项系数必为负数.这是不可能的！所以$g(x)=0$.同理$h(x)=0$.

3.多项式环

环：设R是一个非空集合，如果它有两个代数运算（加法a+b，乘法ab）；并且这两个运算满足下列6条运算法则（$\forall a,b,c \in R$）：

① 加法结合律 $(a+b)+c=a+(b+c)$

② 加法交换律 $a+b=b+a$

③ 在R中有元素0，使得$a+0=a$，称0是R的零元

④ 对于a，在R中有元素d，使得$a+d=0$，称d是a的负元，记为$-a$

⑤ 乘法结合律 $(ab)c=a(bc)$

⑥ 乘法对于加法的左、右分配率

$a(b+c)=ab+ac$

$(b+c)a=ba+ca$

数域P上的一元多项式的全体，称为数域P上的**一元多项式环**，记作$P[x]$.

P——$P[x]$的系数域.

思考与练习

1.计算$f(x)+g(x), f(x)g(x)$,其中

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

2.求k,l,m,使

$$(2x^2+lx-1)(x^2-kx+1)=2x^4+5x^3+mx^2-x-1.$$

3. 例2中，若$f(x), g(x)$为复数域上多项式. 能否由

$$f^2(x)+g^2(x)=0 \Rightarrow f(x)=g(x)=0 \text{ ?}$$

考虑$f(x)=ix, g(x)=x$. 显然 $f^2(x)+g^2(x)=0$ 但 $f(x)\neq 0, g(x)\neq 0$.

§ 3 整除的概念（在$P[x]$ 中进行）

· 引言 在一元多项式环$P[x]$中,有$f(x)\pm g(x)$, $f(x)g(x)$. 是否有除法？应该如何描述$P[x]$中两个多项式相除的关系？两个多项式除法的一般结果是什么？

· 引例 （以中学代数多项式除法为基础）考虑

$$f(x)=3x^3+4x^2-5x+6$$

$$g(x)=x^2-3x+1$$

求出$f(x)$除以$g(x)$的商和余式.

采用长除法

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

商$q(x)$

$f(x)$

$g(x)$

余式 $r(x)$

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

结果： $f(x)=q(x)\,g(x)+r(x)$

采用竖式除法

$$
\begin{array}{r|l|l}
g(x) & \qquad f(x) & q(x) \\
x^2-3x+1 & 3x^3+4x^2-5x+6 & 3x+13 \\
 & 3x^3-9x^2+3x & \\
\hline
 & \qquad 13x^2-8x+6 & \\
 & \qquad 13x^2-39x+13 & \\
\hline
 & \qquad\qquad 31x-7 & \\
\end{array}
$$

商

余式

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

结果：$f(x)=q(x)\,g(x)+r(x)$

带余除法

定理　设$f(x)$, $g(x)\in P[x]$, $g(x)\neq 0$，则存在唯一的多项式$q(x)$, $r(x)\in P[x]$, 使

商

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

余式

其中$r(x)=0$或 $\partial(r(x))<\partial(g(x))$.

称上式中的$q(x)$ 为$g(x)$ 除$f(x)$的商， $r(x)$为$g(x)$除$f(x)$的余式.

（带余除法）定理证明

存在性　若$f(x)=0$，取$q(x)=r(x)=0$即可.以下设$f(x)\neq 0$. $\partial(f(x))=n$,$\partial(g(x))=m$. 对$f(x)$的次数n作数学归纳法.

当$n<m$时,取$q(x)=0$, $r(x)=f(x)$，有

$$f(x)=q(x)g(x)+r(x)\text{，结论成立.}$$

当$n\geq m$时,假设次数小于n时结论成立，即存在多项式$q(x)$, $r(x)\in P[x]$, 使$f(x)=q(x)g(x)+r(x)$.以下证明次数为n时结论也成立.

设$f(x)$、$g(x)$的首项分别为ax^n及bx^m.令

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

注意到$b^{-1}ax^{n-m}g(x)$与$f(x)$有相同的首项,知$\partial(f_1(x))<n$或为$f_1(x)=0$.

（带余除法）定理证明（续1）

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

$$f(x) = q(x)\, g(x) + r(x)\ ;$$

若$\partial(f_1(x)) < n$，由归纳法假设，有$q_1(x)$, $r_1(x) \in P[x]$,使

$$f_1(x) = q_1(x)\, g(x) + r_1(x) \qquad (**)$$

其中$\partial(r_1(x))<\partial(\, g(x)\,)$或$r_1(x) =0$. 于是由式 (*)、(**)有

$$f(x) = \underbrace{(q_1(x)+ b^{-1}a\, x^{n-m})}_{q(x)}\, g(x) + \underbrace{r_1(x)}_{r(x)}$$

由归纳法原理，对任意的$f(x)$, $g(x)\neq 0$， $q(x)$, $r(x)$的

存在性证毕.

（带余除法）定理证明（续2）

唯一性 若还有$q^*(x)$, $r^*(x) \in P[x]$,使

$$f(x) = q^*(x)\, g(x) + r^*(x)$$

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$q(x) \neq q^*(x)$，由假设 $g(x)\neq 0 \Rightarrow r^*(x)- r(x) \neq 0$且

$$\partial\, (q(x) - q^*(x)) +\partial\, (\, g(x)) = \partial\, (r^*(x)- r(x))$$

但$\partial(g(x)\,)>\partial(r^*(x)- r(x))$,矛盾.

因此$q(x) =q^*(x)$, $r^*(x)= r(x)$. $\|$

例1 求$g(x)$除$f(x)$所得的商$q(x)$和余式$r(x)$，这里
$f(x)=x^5+3x^4+x^3+x^2+3x+1,\ g(x)=x^4+2x^3+x+2.$

商

解：

$$
\begin{array}{c|rrrrrr|l}
g(x) & & & f(x) & & & & q(x) \\
x^4+2x^3+x+2 & x^5 & +3x^4 & +x^3 & +x^2 & +3x & +1 & x+1 \\
 & x^5 & +2x^4 & & +x^2 & +2x & & \\
\cline{2-7}
 & & x^4 & +x^3 & & +x & +1 & \\
 & & x^4 & +2x^3 & & +x & +2 & \\
\cline{2-7}
 & & & -x^3 & & & -1 &
\end{array}
$$

余式

即有 $x^5+3x^4+x^3+x^2+3x+1=(x+1)(x^4+2x^3+x+2)+(-x^3-1)$
所求商$q(x)=x+1$，余式$r(x)=-x^3-1.$

带余除法表明： $f(x) = q(x)\,g(x) + r(x)$

用多项式$g(x) \neq 0$去除多项式$f(x)$，可以得到一个商$q(x)$及余式$r(x)$，余式一般不为零.当余式等于0时，得到两个多项式之间的一种关系——整除.

整除的概念

(1)定义 设$f(x)$, $g(x) \in P[x]$, 如果存在多项式$h(x) \in P[x]$, 使

g(x)的倍式

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

称$g(x)$ 整除$f(x)$(或$f(x)$能被$g(x)$整除)，记为$g(x) \mid f(x)$.

此时称$g(x)$ 为$f(x)$ 的因式， $f(x)$为 $g(x)$的倍式.

f(x)的因式

特别地， 当$g(x)$ 不能整除$f(x)$时， 记为$g(x) \nmid f(x)$.

例如， $f(x)=3x^3+4x^2-x$, $g(x)=5x$,有$g(x)|f(x)$.

因 $3x^3+4x^2-x=\underbrace{\left(\frac{3}{5}x^2+\frac{4}{5}x-\frac{1}{5}\right)}_{h(x)}5x$

(2)整除性判别

定理 设$f(x), g(x)\in P[x]$, $g(x)\neq 0$, $g(x)|f(x)$

$\Leftrightarrow g(x)$ 除$f(x)$的余式为零.

证 $(\Leftarrow)$ 若余式$r(x)=0$，则$f(x)=q(x)g(x)$,即$g(x)\mid f(x)$;

$(\Rightarrow)$若$g(x)\mid f(x)$，则

$$f(x)=q(x)g(x)=q(x)g(x)+0$$

即$r(x)=0$. ||

例2 设$f(x)=2x^4-3x^3+5x^2-6$, $g(x)=x^2-x-1$,判断$g(x)$能否整除$f(x)$.

解 由

$$
\begin{array}{c|c|c}
g(x) & f(x) & q(x) \\
x^2-x-1 & 2x^4-3x^3+5x^2-6 & 2x^2-x+6 \\
 & 2x^4-2x^3-2x^2 & \\
\cline{2-2}
 & -x^3+7x^2-6 & \\
 & -x^3+x^2+x & \\
\cline{2-2}
 & 6x^2-x-6 & \\
 & 6x^2-6x-6 & \\
\cline{2-2}
 & 5x & \\
\end{array}
$$

$r(x)\neq 0$

因此 $g(x)\nmid f(x)$.

例3 m,p,q 满足什么条件， $g(x)=x^2+mx-1$能整除$f(x)=x^3+px+q$？

方法1

解 由带余除法，得

$$x^3+px+q=(x-m)(x^2+mx-1)+[(m^2+p+1)x+(q-m)]$$

$$g(x)|f(x) \Leftrightarrow (m^2+p+1)x+(q-m)=0$$

$$\Leftrightarrow m^2+p+1=0 \text{且} q-m=0$$

$$\Leftrightarrow p=-1-m^2 \text{且} q=m.$$

方法2

利用整除的定义，比较 $g(x)$与 $f(x)$的次数及首项系数.

$g(x)|f(x) \Leftrightarrow$ 存在$h(x)=x+a$ 使 $x^3+px+q=(x+a)(x^2+mx-1)$

比较等式两边同次项的系数，得

$$\begin{cases} m+a=0 \\ ma-1=p \\ -a=q \end{cases} \overset{\text{消去}a}{\Rightarrow} \begin{cases} m^2+p+1=0, \\ q-m=0. \end{cases}$$

例4 证明：如果$g(x)|f_1(x)+f_2(x)$，$g(x)|f_1(x)-f_2(x)$，则$g(x)|f_1(x)$，$g(x)|f_2(x)$.

证 由假设，有$h_1(x), h_2(x)$使

$$f_1(x)+f_2(x)=h_1(x)g(x)$$

$$f_1(x)-f_2(x)=h_2(x)g(x)$$

因此

$$f_1(x)=[\frac{1}{2}h_1(x)+\frac{1}{2}h_2(x)]g(x)$$

$$f_2(x)=[\frac{1}{2}h_1(x)-\frac{1}{2}h_2(x)]g(x)$$

由整除的定义，知$g(x)|f_1(x)$，$g(x)|f_2(x)$.

(3)整除的性质

- $f(x)|f(x)$ ——任意一个多项式可整除其自身；
- $f(x)|0$ ——任意一个多项式可整除零多项式；
- $c|f(x)$ ——零次多项式可整除任一多项式；
- 若$f(x)|g(x)$， $g(x)|f(x)$，则 $f(x)=cg(x)$；
- 若$f(x)|g(x)$， $g(x)|h(x)$，则 $f(x)|h(x)$；（传递性）
- 若$f(x)|g(x)$，则 $\forall c\neq 0, cf(x)|g(x)$；
- 若$f(x)|g_i(x)$ ($i=1,2,\ldots,r$) ,则$\forall u_i(x)\in P[x]$

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

$g_i(x)$的组合
$i=1,2,\ldots,r$

整除性质的证明

- $f(x)=1 \cdot f(x)$ ；
- $0 = 0 \cdot f(x)$；
- $f(x)= c[c^{-1}f(x)]$；
- 设$f(x) \mid g(x)$ ， $g(x) \mid f(x)$. 有

$$f(x)= h_1(x)\, g(x)\ ,\quad g(x)= h_2(x)\, f(x);$$

若$f(x)$， $g(x)$ 有一个是0多项式，则另一个必为0，因此任取非零常数c，即有$f(x)= c\, g(x)$.

若$f(x)$、 $g(x)$均不为0 ，有

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

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

$\Rightarrow \deg(h_1(x)\, h_2(x)\ )=\deg(h_1(x))+\deg(h_2(x)\ )=0$

$\Rightarrow \deg(h_1(x))=\deg(h_2(x)\ )=0$.即$h_1(x)$为非0常数.

整除性质的证明

- 传递性（略）；
- 显然；
- 由$f(x)|\ g_i(x)$ (i=1,2,…,r) ,有$h_i(x)$ (i=1,2,…,r) $\in P[x]$ 使

$$g_i(x) = h_i(x)\, f(x) \quad i=1,2,\ldots,r$$

而$\forall u_i(x) \in P[x]$，有

$$u_1(x)g_1(x)+ u_2(x)g_2(x)+\cdots+ u_r(x)g_r(x)$$
$$= [u_1(x)h_1(x)+ u_2(x)h_2(x)+\cdots+ u_r(x)h_r(x)\ ]f(x)$$

由整除的定义，知

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

作业与练习

- 习题1

1 . 1），2. 2），3.

- 证明：$g(x) \mid f_1(x)+2f_2(x)$，$g(x) \mid 3f_1(x)-4f_2(x)$，则$g(x) \mid f_1(x)$，$g(x) \mid f_2(x)$.
- 证明：

(1)$f(x) \mid g_1(x)$，$f(x) \mid g_2(x)$，则$f(x) \mid g_1(x)+g_2(x)$;

(2)若$f(x) \nmid g_1(x)$，$f(x) \nmid g_2(x)$，$f(x)$能否整除$g_1(x)+g_2(x)$？举例说明.

不一定.

§ 3 整除的概念（小结）

- 带余除法 设$f(x)$, $g(x)\in P[x]$, $g(x)\neq 0$,则存在唯一的多项式

$q(x)$, $r(x)\in P[x]$, 使

$$f(x)=q(x)\,g(x)+r(x) \quad （*）$$

其中$r(x)=0$或 $\partial(r(x))<\partial(g(x))$.

- 整除性

1.定义 设$f(x),g(x)\in P[x]$, 如果存在多项式$h(x)\in P[x]$, 使

$f(x)=h(x)\,g(x)$， 称$g(x)\mid f(x)$.

2.整除性判别 $g(x)\mid f(x)$ $(g\neq 0)\Leftrightarrow$ （*）式中$r(x)=0$.

3.整除的性质 （略）

特别提醒: 整除性不是多项式之间的运算,它是$P[x]$中元素间的一种关系,即任给$f(x)$, $g(x)\in P[x]$， 可以判断 $g(x)$ 可以整除 $f(x)$ 或者 $g(x)$不能整除 $f(x)$.

§ 4　最大公因式

- $f(x)$ 与 $g(x)$ 的最大公因式

  定义、存在性与唯一性及其性质、最大公因式的求法（辗转相除法）

- 互素

  定义、判定定理、性质

- n个多项式的最大公因式

1. $f(x)$与$g(x)$的最大公因式

(1)公因式　设$f(x), g(x) \in P[x]$, 若有$\varphi(x) \in P[x]$,
使 $\varphi(x) \mid f(x)$, $\varphi(x) \mid g(x)$, 则称$\varphi(x)$为$f(x)$与$g(x)$的一 个公因式.

由于任意两个多项式总有公因式(非0常数),
因此公因式中占有重要地位的——最大公因式.

(2)最大公因式

定义　设$f(x), g(x) \in P[x]$. 若有$d(x) \in P[x]$满足

(i) $d(x)$是$f(x)$, $g(x)$的公因式;

(ii) $f(x)$, $g(x)$的公因式全是$d(x)$的因式.

则称$d(x)$为$f(x)$与$g(x)$的一个**最大公因式**.

说明:

①最大公因式在相差一个非零常数的意义下是唯一确定的.

事实上,若$d_1(x)$、$d_2(x)$是$f(x)$, $g(x)$的最大公因式, 由最大公因式定义, 知$d_1(x)$为$d_2(x)$的因式,$d_2(x)$也为$d_1(x)$的因式, 即

$$d_1(x)\mid d_2(x),\ d_2(x)\mid d_1(x)$$

由整除的性质知:

$$d_1(x)=c\ d_2(x).$$

②$(f(x), g(x))$——$f(x)$与$g(x)$首项系数为1的最大公因式.

最大公因式的存在性及其求法

- 引理 设$f(x), g(x) \in P[x]$. 如果等式

$$f(x) = q(x)\, g(x) + r(x) \qquad (*)$$

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

证明 由(*)知, $f(x)$是$g(x)$与$r(x)$的一个组合,故若 $\varphi(x) \mid g(x)$,$\varphi(x) \mid r(x)$,必有$\varphi(x) \mid f(x)$，此即$g(x), r(x)$的公因式都是$f(x), g(x)$的公因式;

又由(*)，有 $r(x) = f(x) - q(x)\, g(x)$

故若 $\varphi(x) \mid f(x)$, $\varphi(x) \mid g(x)$,必有$\varphi(x)$ 整除 $f(x)$与 $g(x)$的组合$r(x)$，此即$f(x), g(x)$的公因式都是$g(x), r(x)$的公因式.

综上所述，$f(x), g(x)$ 和$g(x), r(x)$有相同的公因式.

例1 求$f(x)=x^5+3x^4+x^3+x^2+3x+1$与$g(x)=x^4+2x^3+x+2$的最大公因式.

解 先用$g(x)$除$f(x)$:

$g(x)$	$f(x)$	$q(x)$
x^4+2x^3+x+2	$x^5+3x^4+x^3+x^2+3x+1$	$x+1$
	$x^5+2x^4+x^2+2x$	
	x^4+x^3+x+1	
	x^4+2x^3+x+2	
	$-x^3-1$	

得商$q(x)=x+1$，余式$r(x)=-x^3-1$.即

$$f(x)=(x+1)\,g(x)+(-x^3-1)$$

解(续)

但由引理，知 $(f(x),g(x))=(g(x),r(x))$，因此求 $(f(x),g(x))$可用$r(x)$除$g(x)$：

$$
\begin{array}{r|l|l}
r(x) & \qquad g(x) & q_1(x) \\
-x^3-1 & x^4+2x^3+x+2 & -x-2 \\
 & x^4 \qquad\quad +x & \\
\cline{2-2}
 & \qquad 2x^3 \quad +2 & \\
 & \qquad 2x^3 \quad +2 & \\
\cline{2-2}
 & \qquad\qquad\quad 0 &
\end{array}
$$

由于$r(x)\mid g(x)$，知$r(x)$是$g(x)$与$r(x)$的一个最大公因式，因此

$$(f(x),g(x))=(g(x),r(x))=x^3+1.$$

例1 求$f(x)=x^5+3x^4+x^3+x^2+3x+1$与 $g(x)=x^4+2x^3+x+2$ 的最大公因式.（解法小结）

(1)先用$g(x)$ 除$f(x)$,得

$$f(x)=q(x)\,g(x)+r(x)=(x+1)\,g(x)+(-x^3-1)$$

$r(x)\neq 0$， $\partial(r(x))<\partial(g(x))$

(2)用$r(x)$除$g(x)$,得

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

=0

因此 $(f(x),g(x))=(g(x),r(x))=(r(x),r_1(x))$

$$=(r(x),0)=x^3+1.$$

辗转相除而得

最大公因式的存在性及其求法

- **定理** $\forall f(x),g(x)\in P[x]$, 在$P[x]$中存在一个最大公因式$d(x)$, 且$d(x)$可以表达成$f(x),g(x)$的一个组合, 即有$u(x),v(x)\in P[x]$使

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

注意：等式 $d(x)=u(x)f(x)+v(x)g(x)$ 成立, $d(x)$未必就是$f(x)$与$g(x)$的最大公因式.

例如, $f(x)=x^2+1$, $g(x)=x$, $u(x)=x$,

$$v(x)=x^2+1$$

$d(x)=2x(x^2+1)$. 显然有

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

但$d(x)$不是$f(x)$与$g(x)$的最大公因式.

最大公因式存在性定理证明

- 证 (i)如果$f(x)$, $g(x)$有一个为零多项式，比如$g(x)=0$，则$f(x)$就是$f(x)$, $g(x)$一个最大公因式，即$d(x)=f(x)$，且

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

(ii)一般情形:不妨设$g(x)\neq 0$. 由带余除法, 用$g(x)$除$f(x)$, 得到商$q_1(x)$, 余式$r_1(x)$；即

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

若$r_1(x)=0$,则$r_1(x)$, $g(x)$的最大公因式为$g(x)$,从而$f(x)$, $g(x)$最大公因式$d(x)$仅与$g(x)$相差一个非0常数因子，此时

$$d(x)=cg(x)=0\cdot f(x)+cg(x)$$

最大公因式存在性定理证明（续1）

若$r_1(x)\neq 0$, 再用$r_1(x)$除$g(x)$,得到商$q_2(x)$,余式$r_2(x)$;又若$r_2(x)\neq 0$, 就用$r_2(x)$除$r_1(x)$, 得出商$q_3(x)$, 余式$r_3(x)$; 如此辗转相除下去 ……, 所得余式的次数不断降低，即 $\partial(g(x)) > \partial(r_1(x)) > \partial(r_2(x))$ > …… 经有限次之后, 必有余式为零(因次数有限). 即

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

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

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

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{i-2}(x) = q_i(x)\, r_{i-1}(x) + r_i(x)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

最大公因式存在性定理证明（续2）

…………………………

$$r_{s-3}(x) = q_{s-1}(x)\, r_{s-2}(x) + r_{s-1}(x)$$
$$r_{s-2}(x) = q_s(x)\, r_{s-1}(x) + r_s(x)$$
$$r_{s-1}(x) = q_{s+1}(x)\, r_s(x) + 0$$

$r_s(x)$与0的最大公因式是$r_s(x)$,由引理知,$r_s(x)$也是$r_s(x)$与$r_{s-1}(x)$的一个最大公因式;也是$r_{s-1}(x)$与$r_{s-2}(x)$的一个最大公因式,以此逐步上推……,$r_s(x)$就是$f(x)$与$g(x)$的一个最大公因式.

为得到定理结论中的等式，由上面的倒数第二个等式，我们有

$$r_s(x) = r_{s-2}(x) - q_s(x) r_{s-1}(x)$$

最大公因式存在性定理证明（续3）

而由倒数第三式, 有

$$r_{s-1}(x)=r_{s-3}(x) - q_{s-1}(x)r_{s-2}(x)$$

带入上式, 消去$r_{s-1}(x)$，得到

$$r_s(x) = (1+q_s(x)q_{s-1}(x))r_{s-2}(x)-q_s(x)r_{s-3}(x)$$

以同样的方法逐个消去$r_{s-2}(x)$， ……, $r_1(x)$,

并项后，得到

$$r_s(x) = u(x)f(x) + v(x)g(x)$$

综上所述，证毕.

定理中求最大公因式的方法称为辗转相除法.

例2 设$f(x)=4x^4-2x^3-16x^2+5x+9$, $g(x)=2x^3-x^2-5x+4$
求$(g(x),f(x))$,并求$u(x),v(x)$使

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

解 利用辗转相除法

$q_2(x)=$	$g(x)$	$f(x)$	$q_1(x)=$
$-\frac{1}{3}x+\frac{1}{3}$	$2x^3-x^2-5x+4$	$4x^4-2x^3-16x^2+5x+9$	$2x$
	$2x^3+x^2-3x$	$4x^4-2x^3-10x^2+8x$	
	$-2x^2-2x+4$	$r_1(x)=-6x^2-3x+9$	$6x+9$
	$-2x^2-x+3$	$-6x^2+6x$	$=q_3(x)$
	$r_2(x)=-x+1$	$-9x+9$	
		$-9x+9$	
		$r_3(x)=0$	

解（续1） 上述辗转相除过程为：

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

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

=0

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

因此，$r_2(x)$=-x+1为$f(x)$与$g(x)$的一个最大公因式,而首项系数为1的最大公因式为

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

以下求$u(x)$,$v(x)$. 由前式，得

$$r_2(x)=g(x)-q_2(x)r_1(x)=g(x)-q_2(x)[f(x)-q_1(x)g(x)]$$

$$=(1+q_1(x)q_2(x))\, g(x) - q_2(x)\, f(x)$$

解（续2） 即

$$-x+1=[1+2x(-\frac{1}{3}x+\frac{1}{3})]g(x)-(-\frac{1}{3}x+\frac{1}{3})f(x)$$

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

两端同乘以−1，得

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

因此，有

$$u(x)=-\frac{1}{3}x+\frac{1}{3},\quad v(x)=\frac{2}{3}x^2-\frac{2}{3}x-1.$$

2. 互素多项式

(1)定义 设$f(x),g(x)\in P[x]$, 如果$(f(x), g(x))=1$,称$f(x)$与$g(x)$互素（也称互质）.

易知，两个互素多项式的公因式只有零次多项式.

(2)互素的充分必要条件

定理 $P[x]$中多项式$f(x), g(x)$互素$\Leftrightarrow$存在有$u(x)$, $v(x)\in P[x]$，使 $u(x)f(x)+v(x)g(x)=1$。

证明 ($\Rightarrow$)因$(f(x), g(x))=1$，由最大公因式存在定理，有$u(x), v(x)\in P[x]$，使 $1=u(x)f(x)+v(x)g(x)$.

证明(续)

($\Leftarrow$)设有$u(x), v(x)\in P[x]$使

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

若$\varphi(x)$是$f(x)$与$g(x)$的一个最大公因式, 则

$\varphi(x)\mid f(x)$, $\varphi(x)\mid g(x)$, 从而$\varphi(x)\mid u(x)f(x)+v(x)g(x)$

即$\varphi(x)\mid 1\Rightarrow \varphi(x)=c$.

因此，$(f(x), g(x))=1$.

综上所述，证毕.

(3) 互素多项式的性质

定理 若$(f(x), g(x))=1$,且$f(x)\mid g(x)h(x)$,则$f(x)\mid h(x)$.

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

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

等式两边乘$h(x)$,得

$$u(x)f(x)h(x)+v(x)g(x)h(x)=h(x) \quad (*)$$

因$f(x)\mid g(x)h(x)$，$f(x)\mid f(x)$，有

(*)左端

$$f(x)\mid u(x)f(x)h(x)+v(x)g(x)h(x)$$

即$f(x)\mid h(x)$. 证毕.

(*)右端

推论 若$f_1(x)\mid g(x)$, $f_2(x)\mid g(x)$且$(f_1(x), f_2(x))=1$，则$f_1(x)f_2(x)\mid g(x)$. （证明略）

· 习题1

10.若$f(x)$, $g(x)$不全为0，则 $\left(\dfrac{f(x)}{(f(x),g(x))},\dfrac{g(x)}{(f(x),g(x))}\right)=1.$

■ 证 若$f(x)$, $g(x)$不全为0，则$(f(x), g(x))= d(x)\neq 0$.由最大公因式存在定理，有$u(x)$, $v(x)$使

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

所以

$$u(x)\frac{f(x)}{d(x)}+v(x)\frac{g(x)}{d(x)}=u(x)\frac{f(x)}{(f(x),g(x))}+v(x)\frac{g(x)}{(f(x),g(x))}=1.$$

由互素的充要条件，有 $\left(\dfrac{f(x)}{(f(x),g(x))},\dfrac{g(x)}{(f(x),g(x))}\right)=1.$

12.若$(f(x), g(x))=1$, $(f(x), h(x))=1$,则$(f(x), g(x)h(x))=1$.

证明 因为（$f(x)$，$g(x))=1,(f(x),h(x))=1$,由多项式互素的充要条件，总存在$u_1(x),v_1(x)$和$u_2(x),v_2(x)$使得

$$u_1(x)f(x)+v_1(x)g(x)=1,$$

$$u_2(x)f(x)+v_2(x)h(x)=1,$$

两式相乘得

$$[u_1(x)u_2(x)f(x)+u_1(x)v_2(x)h(x)+u_2(x)v_1(x)g(x)]f(x)+$$

$$+(v_1(x)v_2(x))g(x)h(x)=1$$

因此由多项式互素的充要条件得，（$f(x),g(x)h(x))=1$

3. n个多项式的最大公因式

(1)定义　已知$f_i(x)$ $(i=1,2,\ldots,s\geq 2)\in P[x]$. 若有$d(x)\in P[x]$满足

(i) $d(x)$是$f_i(x)$ $(i=1,2,\ldots,s)$的公因式；

(ii) $f_i(x)$ $(i=1,2,\ldots,s)$的公因式全是$d(x)$的因式.

则称$d(x)$为$f_i(x)$ $(i=1,2,\ldots,s)$的一个**最大公因式**.

(2)求法

$(f_1(x), f_2(x),\ldots, f_s(x))=((f_1(x), f_2(x),\ldots, f_{s-1}(x)), f_s(x))$且$\exists u_i(x)$ $(i=1,2,\ldots,s)\in P[x]$使

$u_1(x)f_1(x)+\cdots+u_s(x)f_s(x)=(f_1(x), f_2(x),\ldots, f_s(x))$

例3 设$f_1(x)=x^6-7x^4+8x^3-7x+7$, $f_2(x)=3x^5-7x^3+3x^2-7$

$f_3(x)=x^4+x^3-7x^2-8x-1$， $f_4(x)=x^3+x^2-x-1$

求$(f_1(x), f_2(x), f_3(x), f_4(x))$.

解 利用

$(f_1(x), f_2(x), f_3(x), f_4(x))=(((f_1(x), f_2(x)), f_3(x)), f_4(x))$

逐步计算.

$$(f_1(x), f_2(x))=x^3+1$$

$$(x^3+1, f_3(x))=x+1$$

$$(x+1, f_4(x))=x+1$$

所以$(f_1(x), f_2(x), f_3(x), f_4(x))=x+1$.

(3)互素 如果$(f_1(x), f_2(x),\dots, f_s(x))=1$，称$f_1(x), f_2(x),\dots, f_s(x)$ 互素.

(4)两两互素 如果 $f_1(x), f_2(x),\dots, f_s(x)$ 中任意两个都互素，称$f_1(x), f_2(x),\dots, f_s(x)$两两互素.

例 $f_1(x)=x+1, f_2(x)= x-1, f_3(x)=x^2+1$ 互素且两两互素.

$f_1(x)=x+1, f_2(x)= x-1, f_3(x)=x^2-1$ 互素但不两两互素.

作业与练习

- 习题1

5 . 2),6. 2),7~9,11.,13.,14.

最大公约式 （Review1.1）

(1)公因式：$\varphi(x)\mid f(x),\varphi(x)\mid g(x)$,则称$\varphi(x)$为$f(x),g(x)$的公约式;

(2)最大公因式:(1)$d(x)$是$f(x),g(x)$的公约式；（2）$d(x)$的因式全由$f(x)$、$g(x)$的公约式所组成.则称$d(x)$是$f(x)$、$g(x)$的最大公因式.

约定（$f(x),g(x)$)表示$f(x)$与$g(x)$首项系数为1的最大公因式.

(3)对于任意多项式$f(x)\in P[x]$, $f(x)$与0的最大公因式是$f(x)$;

(4)引理 若有带余除法$f(x)=q(x)g(x)+r(x)$,则

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

(review1.2)

定理 对于$P[x]$中任意两个多项式$f(x),g(x)$，总存在一个最大公因式$d(x)$,且在$P[x]$总存在多项式$u(x),v(x)$使得
$d(x)=u(x)f(x)+v(x)g(x)$.

$d(x)$的存在性是利用辗转相除法，其原理有两条：一是根据（$(f(x),g(x))=(g(x),r_1(x))=(r_1(x),r_2(x))=\cdots(r_{s-1}(x),r_s(x))$
$=(r_s(x),0) \qquad \Rightarrow r_s(x)$就是$f(x),g(x)$的最大公约式.二是由于
$\partial(g(x))>\partial(r_1(x))>\partial(r_2(x))>\cdots>\partial(r_{s+1})=0$,因此在有限次之后，必然有余式为0.

因此辗转相除法同时提供了计算最大公因式的方法.

（Review1.3）

(5)如果$(f(x),g(x))=1$,则称$f(x),g(x)$互素；$f(x),g(x)$互素的充要条件是存在$u(x),v(x)\in P[x]$,使得

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

(6)互素多项式的性质：如果$(f(x),g(x))=1$,

且$f(x)\mid g(x)h(x)$,那么$f(x)\mid h(x)$.

上面最大公因式和互素的概念都是对两个多项式的，其中有些概念可以推广到多个多项式.(PPT63、64）

§ 5　因式分解定理（在$P[x]$ 中进行）

- 不可约多项式概念、性质

- 因式分解及唯一性定理

- 多项式因式分解的标准形式

1. 不可约多项式

(1)定义 如果数域P上次数≥1的多项式$p(x)$不能表成数域P上的两个次数比$p(x)$的次数低的多项式的乘积, 称其为域P上的不可约多项式.

按照定义:

①一次多项式总是不可约多项式;

②多项式是否可约依赖于数域;

如 $f(x)=x^2+2$在实数域上不可约, 在复数域上可约.

③不可约多项式$p(x)$的因式只有c及$cp(x)(c\neq 0)$.

③的证明

设$\varphi(x)$为$p(x)$的因式，则$\varphi(x)\mid p(x)$，即有$h(x)$使

$$p(x)=h(x)\varphi(x).$$

因$p(x)$ 不可约，即它不能表为两个次数比它低的多项式的乘积，因此

$$\partial(h(x))=0\text{或}\partial(\varphi(x))=0$$

若$\partial(h(x))=0$, 有 $h(x)=a\neq 0,\varphi(x)=a^{-1}p(x)=cp(x)$;

若$\partial(\varphi(x))=0$, 有 $\varphi(x)=c$.

即：不可约多项式$p(x)$的因式只有c及$cp(x)$ $(c\neq 0)$.

(2)不可约多项式的性质

- **定理** 如果$p(x)$是不可约多项式，则

(i) $\forall f(x)\in P[x]$,或者$p(x)\mid f(x)$;或者 $f(x)$与$p(x)$互素；

(ii)$\forall f(x),g(x)\in P[x]$, 由$p(x)\mid f(x)g(x)$一定推出

$p(x)\mid f(x)$或者$p(x)\mid g(x)$.

证明 (i)设$(f(x), p(x))=d(x)$，则$d(x)\mid p(x)$,但$p(x)$是不可约多项式$\Rightarrow d(x)=1$或$d(x)=cp(x)$（$c\neq 0$, $cp(x)$ 首项系数为1）.

若$d(x)=1$,则$f(x)$与$p(x)$互素；

若$d(x)=cp(x)$,则$p(x)\mid f(x)$.

(ii)分两种情况，若 $p(x)\mid f(x)$结论成立.

证明（续）

(ii) 若$p(x)\nmid f(x)$, 由(i)必有$(p(x),f(x))=1$.再由互素多项式互素的性质:$(p(x), f(x))=1$, 且 $p(x)\mid f(x)g(x)$,
$p(x)\mid g(x)$.

这就是说当p(x)是不可约多项式时，对$\forall f(x), g(x)\in P[x]$，由$p(x)\mid f(x)g(x)$ 一定推出 $p(x)\mid f(x)$或者 $p(x)\mid g(x)$.
这是两个函数的情况，而对于多个函数时由结果

一般地，有如下结论：

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

（用数学归纳法证明）略.

2. 因式分解及唯一性定理

定理 数域P上每一个次数≥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. 唯一性指：若有两个分解式

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

则必有s=t，且适当排列因式的次序后有

$$p_i(x)=c_iq_i(x)，\quad i=1, 2, \cdots, s$$

其中，c_i (i=1, 2, ⋯, s)是一些非零常数.

证明 (存在性)对$f(x)$的次数做数学归纳法.

由于一次多项式都是不可约的, 所以n=1时结论成立.

证明(续1)

设$\partial(f(x))=n$,并设结论对于次数低于n的多项式已经成立.

若$f(x)$是不可约多项式, 结论显然.

不妨设$f(x)$不是不可约的, 即有

$$f(x)=f_1(x)f_2(x)$$

其中$f_1(x)$, $f_2(x)$的次数都低于n. 由归纳法假定$f_1(x)$和$f_2(x)$都可以分解成数域P上一些不可约多项式的乘积. 把$f_1(x)$, $f_2(x)$的分解式合起来得到$f(x)$的一个分解式.

由归纳法原理, 结论普遍成立.

证明(续2)(唯一性)

设$f(x)$可以分解成不可约多项式的乘积

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)$$

若$f(x)$还有另一分解式

$$f(x)=q_1(x)q_2(x)\cdots q_t(x)$$

其中$q_i(x)(i=1,2,\cdots,t)$都是不可约多项式.于是

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x) \qquad ①$$

我们对s做归纳法. 当$s=1$时, $f(x)$是不可约多项式. 由定义必有 $s=t=1$,且

$$f(x)=p_1(x)=q_1(x).$$

假设不可约因式的个数为$s-1$时唯一性已证.由①有: $p_1(x)|q_1(x)q_2(x)\cdots q_t(x)$

证明(续3)

因此, $p_1(x)$必能整除其中某一个(PPT74). 不妨设 $p_1(x)|q_1(x)$.

由于$q_1(x)$也是不可约多项式，故有

$$p_1(x)=c_1q_1(x) \qquad ②$$

在①式两边消去$q_1(x)$，就有

$$p_2(x)\cdots p_s(x)=c_1^{-1}q_2(x)\cdots q_t(x)$$

由归纳法假定，有

$$s-1=t-1\text{，即}s=t, \qquad ③$$

且适当排列次序后，有

$$p_2(x)=c_2'c_1^{-1}q_2(x)=c_2q_2(x), p_i(x)=c_iq_i(x)\ (i=3, \cdots, s) \qquad ④$$

综合②、③ 、④分解的唯一性证毕.

3.标准分解式

在$f(x)$的分解式中，可以把每一个不可约因式的首项系数提出来, 使其成为首项系数为1的多项式，再将相同的不可约因式合并，于是有

(1)标准分解式

$$f(x)=cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x)$$

其中c为$f(x)$的首项系数, $p_i(x)$ (i=1, 2, …, s) 是不同的首项系数为1的不可约多项式, r_i (i=1, 2, …, s) 为正整数.

(2) 标准分解式的用途

①求两个多项式的最大公因式： $f(x)$与$g(x)$的最大公因式$d(x)$等于那些同时在$f(x)$与$g(x)$的标准分解式中出现的不可约多项式的方幂的乘积，所带方幂等于它在$f(x)$与$g(x)$标准分解式中所带方幂的较小的一个.

②讨论整除的关系：

$g(x) | f(x) \Leftrightarrow g(x)$的不可约因式$p(x)$都是$f(x)$的因式，且$p(x)$在$g(x)$中的幂次小于或等于在$f(x)$中的幂次.