**理科专业基础课(71100201)**

# 《代 数 与 几 何》

**主讲人: 吕新民**

# 《代数与几何》(I)教学计划

| 章节 | 内容 | 主讲 | 测验 | 解析 |
|---|---|---|---|---|
| 第一章 | 多项式 | 12课时 | 3课时 | 3课时 |
| 第二章 | 行列式 | 6课时 | 3课时 | 3课时 |
| 第三章 | 矩阵 | 12课时 | 3课时 | 3课时 |
| 第四章 | 线性方程组 | 9课时 | 3课时 | 3课时 |
| 第五章 | 二次型 | 9课时 | 3课时 | 3课时 |

注：本学期总课时$5\times16=80$学时，课堂教学78学时，期末复习答疑2学时.

# 第一章 多项式

- 数域
- 一元多项式及其运算
- 最大公因式
- 因式分解
- 重因式
- 有理系数多项式

# 第1节　数　域

常用记号：$\mathbb{N}$表示自然数集，$\mathbb{Z}$表示整数集，$\mathbb{Q}$表示有理数集，$\mathbb{R}$表示实数集，$\mathbb{C}$表示复数集.

- **数域**

在整个高等代数的研究中，都是在一定的数域基础上展开的. 什么是数域?

**定义** 设$P \subseteq \mathbb{C}$，且满足条件：

(1) $0, 1 \in P$;

(2) $\forall\, a, b \in P$，$a+b, a-b, ab, \frac{a}{b}\,(b \neq 0) \in P$，

则称$P$是一个数域.

【例1】 记$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}|\ a, b \in \mathbb{Q}\}$. 证明：$\mathbb{Q}[\sqrt{2}]$是一个数域.

**证明：** 显然，$0, 1 \in \mathbb{Q}[\sqrt{2}]$，且$\mathbb{Q}[\sqrt{2}]$关于数的加、减及乘法运算封闭. 令$a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$，且$c + d\sqrt{2} \neq 0$，其中$a, b, c, d \in \mathbb{Q}$. 于是

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2} \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

故$\mathbb{Q}[\sqrt{2}]$是一个数域.

注: 对每一个素数$p$，$\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p}|\ a, b \in \mathbb{Q}\}$是两两互异的数域，且$\mathbb{Q} \subset \mathbb{Q}[\sqrt{p}] \subset \mathbb{R}$，即在$\mathbb{Q}$与$\mathbb{R}$之间存在无穷多个不同的数域. 但在$\mathbb{R}$与$\mathbb{C}$之间不存在任何真的数域

【例2】若$P$是一个数域，则$P\supseteq\mathbb{Q}$，即$\mathbb{Q}$是所有数域中最小的数域.

**证明：** 因为$P$是一个数域，则$1\in P$. 又$P$对加法运算的封闭，则

$$1+1=2, 2+1=3,\cdots,n+1=n+1$$

全在$P$中，因此，$\mathbb{N}\subseteq P$. 同时，$0\in P$，及$P$对减法运算的封闭性，$0-n=-n$也在$P$中，所以$\mathbb{Z}\subseteq P$. 又每一个有理数均可表为两个整数的商，由$P$对除法运算的封闭性知$\mathbb{Q}\subseteq P$.

- **《高等代数》研究中常用的方法**

方法1：直接法. 即利用相关的概念、性质及定理从正面证明问题的方法.

方法2：反证法. 基于一个命题的原命题与其逆否命题等价所建立的证明问题的方法. 一般地，欲证命题："已知条件$A$，则有结论$B$"，在无法直接证明的前提下，可采用假定结论$B$不成立，推出条件$A$不成立. 反证法在《高等代数》研究中经常使用.

方法3：数学归纳法. 数学归纳法主要证明涉及自然数$n$的命题$P(n)$. 数学归纳法主要有第一数学归纳法和第二数学归纳法两种形式.

为了给出数学归纳法的一个合理的解释，引入

**良序公理** $\mathbb{N}$的每个非空子集$S$均包含最小元. 特别地，$0$是$\mathbb{N}$的最小元.

下面我们将借助于良序公理来证明数学归纳法.

**数学归纳法** 设$S$是$\mathbb{N}$的一个子集，且$0 \in S$，如果$S$满足下面两个条件之任一：

(1) $\forall n \in \mathbb{N}$，若$n \in S$，则$n+1 \in S$.

(2) $\forall n \in \mathbb{N}$，若$m \in S$且$0 \leq m < n$，则$n \in S$.

则$S = \mathbb{N}$.

证明：假定$S \neq \mathbb{N}$，则$\emptyset \neq \mathbb{N} - S \subseteq \mathbb{N}$. 依据良序公理，$\mathbb{N} - S$必有最小元，记作$n$，则$n \notin S$. 因$n$是$\mathbb{N} - S$中的最小元，从而对于任意的$m \in \mathbb{N}$，若$m < n$，$m \notin \mathbb{N} - S$，即$m \in S$.

①若条件(1)成立，因$n-1 < n$，从而$n-1 \in S$，导致$n \in S$，矛盾.

②若条件(2)成立，对于任意的$0 \leq m < n$，必然$m \in S$，同样导致$n \in S$，矛盾.

满足条件(1)的称为第一数学归纳法，满足条件(2)的称为第二数学归纳法.

## 第2节 一元多项式及其运算

- **定义**

**定义** 设$P$是一个数域，$x$是一个符号，$n$是一个非负整数，形式表达式

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

其中每个$a_i \in P$，称$f(x)$为数域$P$上的一元多项式.

为理解方便，作如下说明:

(1) 若$a_n \neq 0$，称$f(x)$为$n$次多项式，我们用符号$\deg(f(x))$或$\partial(f(x))$表示$f(x)$的次数，即$\deg(f(x)) = n$或$\partial(f(x)) = n$.

(2) 系数全为零的多项式称为零多项式，记作$0$，零多项式不定义次数.

数域$P$上的一元多项式全体记为$P[x]$.

(3) 设$f(x)=\sum\limits_{i=1}^{n} a_i x^i, g(x)=\sum\limits_{j=1}^{m} b_j x^j \in P[x]$，规定

$$f(x)=g(x) \Leftrightarrow m=n\text{，且}a_i=b_i \ \ (\forall\, i).$$

- **运算**

**定义** 设$f(x)=\sum\limits_{i=1}^{n} a_i x^i, g(x)=\sum\limits_{j=1}^{m} b_j x^j \in P[x]$.

(1) 加减法：不失一般性，令$n \geq m$，且补充$b_{m+1} = \cdots = b_n = 0$后可令$g(x) = \sum_{i=1}^{n} b_i x^i$，规定

$$f(x) \pm g(x) = \sum_{i=1}^{n} (a_i \pm b_i) x^i.$$

(2) 乘法：规定

$$f(x)g(x) = a_n b_m x^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0 = \sum_{s=0}^{n+m} (\sum_{i+j=s} a_i b_j) x^s.$$

显然，$P[x]$关于上述定义的加，减，乘三种运算封闭，且对任意的$f(x), g(x), h(x) \in P[x]$，有

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

(3) 次数公式：

①$\deg(f(x)\pm g(x))\le\max\{\deg(f(x)),\deg(g(x))\}$

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

**问题：** 在$P[x]$中，能否进行普通意义上的除法运算? 即

若$f(x),g(x)\in P[x]$，问是否$\frac{f(x)}{g(x)}\in P[x]$?

等价地，是否存在$h(x)\in P[x]$，使得$f(x)=g(x)h(x)$?

答案是否定的. 如取$f(x)=x^2+1, g(x)=x$，显然不存在$h(x)\in P[x]$，使得$f(x)=g(x)h(x)$.

- **带余除法**

**定理** 设$f(x), g(x) \in P[x]$，如果$g(x) \neq 0$，则必存在$q(x), r(x) \in P[x]$，使得$f(x) = q(x)g(x) + r(x)$，其中$r(x) = 0$或$\deg(r(x)) < \deg(g(x))$，且满足条件的$q(x), r(x)$是唯一的.

**证明：** 先证存在性. 若$f(x) = 0$，取$q(x) = r(x) = 0$即可. 若$f(x) \neq 0$，令$n, m$分别为多项式$f(x), g(x)$的首项次数，假定$n < m$，取$q(x) = 0, r(x) = f(x)$即可. 当$n \geq m$时，假设当次数小于$n$时，$q(x), r(x)$的存在性已证. 现考察次数为$n$的情形. 令$ax^n, bx^m$分别为$f(x), g(x)$的首项，则

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

的 次 数 小 于$n$或 为$0$. 对 于 后 者， 取$q(x) = b^{-1}ax^{n-m}, r(x) = 0$即可. 对于前者，由归纳假设，存在$q_1(x), r_1(x)$，使得

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

其中$r_1(x) = 0$或者$\deg(r_1(x)) < \deg(g(x))$. 于是

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

令$q(x) = q_1(x) + b^{-1}ax^{n-m}, r(x) = r_1(x)$，则$f(x) = q(x)g(x) + r(x)$. 由归纳原理，存在性得证.

再证唯一性. 假定还有$q'(x), r'(x)$使得

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

其中$\deg(r'(x)) < \deg(g(x))$或者$r'(x) = 0$. 于是

$$(q(x) - q'(x))g(x) = r'(x) - r(x).$$

假定$q'(x) \neq q(x)$，则$r'(x) \neq r(x)$，且有

$$\deg(q(x) - q'(x)) + \deg(g(x)) = \deg(r'(x) - r(x)).$$

但

$$\deg(g(x)) > \deg(r'(x) - r(x)),$$

即上式不成立，$q'(x) = q(x)$，进而$r'(x) = r(x)$.

通常，称满足定理条件的$q(x)$为$g(x)$除$f(x)$的商，而$r(x)$为$g(x)$除$f(x)$的余式.

注: 只有当$r(x)=0$或$\deg(r(x))<\deg(g(x))$时，$q(x),r(x)$才是唯一的. 如取$f(x)=x+1, g(x)=x$，则$f(x)=1\cdot g(x)+1=(-1)\cdot g(x)+(2x+1)$.

- **整除**

**定义** 设$f(x),g(x)\in P[x]$，$g(x)$称为整除$f(x)$，记作$g(x)|f(x)$，如果存在$h(x)\in P[x]$，使得$f(x)=g(x)h(x)$. 此时也称$g(x)$是$f(x)$的一个因式.

利用带余除法法则易知$g(x)|f(x)\Leftrightarrow r(x)=0$. 整除具有如下性质:

**定理** 设$f(x),g(x),h(x)\in P[x]$.

(1) 若$f(x),g(x)\neq 0$，且$f(x)|g(x)$，$g(x)|f(x)$，则$f(x)=cg(x)$，这里$c$是一个非零常数.

(2) 若$f(x),g(x)\neq 0$，且$f(x)|g(x)$，$g(x)|h(x)$，则$f(x)|h(x)$.

(3) 若$f(x)\neq 0$，且$f(x)|g(x),f(x)|h(x)$，则对任意的$u(x),v(x)\in P[x]$，$f(x)|(u(x)g(x)+v(x)h(x))$.

证明：直接验证即可.

通常，称表达式$u(x)g(x)+v(x)h(x)$为$g(x)$与$h(x)$的线性组合.

【例3】设$f(x)=x^2+mx+1, g(x)=x^3+px+q$，若$f(x)|g(x)$，求$p,q$满足的条件.

解：由带余除法有

$$g(x)=xf(x)+(m^2+p+1)x+q-m.$$

因$f(x)|g(x)$，于是

$$(m^2+p+1)x+q-m=0.$$

从而$p=-m^2-1, q=m$. 故$p,q$满足的条件是$p=-q^2-1$.

## 第3节 最大公因式

- **定义**

**定义** 设$f(x),g(x) \in P[x]$，$d(x) \in P[x]$称为$f(x),g(x)$的一个最大公因式，如果满足：

(1) $d(x)|f(x), d(x)|g(x)$；

(2) 若$k(x)|f(x), k(x)|g(x)$，则$k(x)|d(x)$.

显然，如果有等式$f(x) = q(x)g(x) + r(x)$，那么$f(x),g(x)$和$g(x),r(x)$有相同的公因式.

- **辗转相除法**

**辗转相除法：** 对于任意的$f(x),g(x) \in P[x]$，$f(x)$与$g(x)$的最大公因式$d(x)$存在，且$d(x) = u(x)f(x) + v(x)g(x)$，其中$u(x),v(x) \in P[x]$.

**证明：** 如果$f(x), g(x)$中有一个为零，如$g(x)=0$，则$d(x)=f(x)=1\cdot f(x)+0\cdot g(x)$，结论成立.

现设$g(x)\neq 0$，由带余除法法则，用$g(x)$除$f(x)$，得商$q_1(x)$，余式$r_1(x)$；如果$r_1(x)\neq 0$，用$r_1(x)$除$g(x)$，得商$q_2(x)$，余式$r_2(x)$；如果$r_2(x)\neq 0$，用$r_2(x)$除$r_1(x)$，得商$q_3(x)$，余式$r_3(x)$，如此辗转下去，所得余式的次数不断降低，即

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

注意$g(x)$的次数是有限的，因此，在有限次后，必然余式为零，于是有

$$f(x)=q_1(x)g(x)+r_1(x)$$
$$g(x)=q_2(x)r_1(x)+r_2(x)$$
$$\cdots\quad\cdots\quad\cdots\quad\cdots$$
$$r_{s-2}(x)=q_s(x)r_{s-1}(x)+r_s(x)$$
$$r_{s-1}(x)=q_{s+1}(x)r_s(x)$$

**$r_s(x)$必是$r_s(x)$与$r_{s-1}(x)$的最大公因式，依次倒推可知$r_s(x)$必是$f(x)$与$g(x)$的最大公因式.**

**由倒数第二式得**

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

**再依此上推，最终可得**

访问主页
标题页
目录页
◀◀ ▶▶
◀ ▶

返回
全屏显示
关闭
退出

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

上述法则通常称为辗转相除法. 由定义，两个多项式的最大公因式的表达形式不是唯一的，可以相差一个常数因子. 符号$(f(x), g(x))$表示$f(x)$与$g(x)$的首项系数为1的最大公因式.

【例 4】设$f(x) = x^4 + x^3 - 3x^2 - x + 2$，$g(x) = x^3 - 4x$，求$u(x), v(x)$，使得$u(x)f(x) + v(x)g(x) = (f(x), g(x))$.

**解**：由辗转相除法法，得

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

$$g(x)=(x^2+3x+2)(x-3)+(3x+6).$$
$$x^2+3x+2=(3x+6)(\tfrac{1}{3}x+\tfrac{1}{3}).$$

于是$(f(x),g(x))=x+2$. 又

$$\begin{aligned}(f(x),g(x))&=x+2\\&=\tfrac{1}{3}g(x)-\tfrac{1}{3}(x^2+3x+2)(x-3).\\&=\tfrac{1}{3}g(x)-\tfrac{1}{3}[f(x)-g(x)(x+1)](x-3).\\&=(-\tfrac{1}{3}x+1)f(x)+(\tfrac{1}{3}x^2-\tfrac{2}{3}x-\tfrac{2}{3})g(x).\end{aligned}$$

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

**【例5】**设$f(x)=x^3+(1+t)x^2+2x+2u$与$g(x)=$

$x^3+tx^2+u$的最大公因式是一个二次多项式，求$t,u$的值.

**解：** 由辗转相除法法得

$$f(x)=1\cdot g(x)+(x^2+2x+u)$$

$$g(x)=(x+(t-2))(x^2+2x+u)-(u+2t-4)x+u(3-t).$$

由题设，$-(u+2t-4)x+u(3-t)=0$，即

$$\begin{cases} u+2t-4=0 \\ u(3-t)=0 \end{cases},$$

解之得$\begin{cases} u=0 \\ t=2 \end{cases}$或$\begin{cases} u=-2 \\ t=3 \end{cases}.$

注: 由定理知，辗转相除法终止于一个二次多项式.

- **互素**

**定义** 设$f(x), g(x) \in P[x]$，$f(x), g(x)$称为互素，如果$(f(x), g(x)) = 1$.

关于互素的判定，有如下基本定理.

**定理** 设$f(x), g(x) \in P[x]$，则$(f(x), g(x)) = 1 \Leftrightarrow$存在$u(x), v(x) \in P[x]$，使得$u(x)f(x) + v(x)g(x) = 1$.

证明：必要性显然. 下证充分性. 因$(f(x), g(x))|f(x), (f(x), g(x))|g(x)$，于是

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

故$(f(x),g(x))=1.$

注: 若$(f(x),g(x))=1$，则必存在$u(x),v(x)$，使得$u(x)f(x)+v(x)g(x)=1$. 满足关系式的$u(x),v(x)$未必唯一. 如取$f(x)=x+1,g(x)=x$，则$(f(x),g(x))=1$，但同时有$1\cdot f(x)+(-1)\cdot g(x)=1$与$-(x-1)\cdot f(x)+x\cdot g(x)=1.$

互素具有如下性质.

**定理** 设$f(x),g(x),h(x)\in P[x]$，$(f(x),g(x))=1$，且$f(x)|g(x)h(x)$，则$f(x)|h(x)$.

**证明：** 因为$(f(x),g(x))=1$，存在$u(x),v(x)\in P[x]$，使得$u(x)f(x)+v(x)g(x)=1$. 于是

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

因 为$f(x)|g(x)h(x)$， 从 而$f(x)|[u(x)f(x)h(x)+v(x)g(x)h(x)]=h(x)$.

**推 论** 设$f_1(x),f_2(x),g(x)\in P[x]$，若$f_1(x)|g(x)$，$f_2(x)|g(x)$，且$(f_1(x),f_2(x))=1$，则$f_1(x)f_2(x)|g(x)$.

**证明：** 因为$f_1(x)|g(x)$，则$g(x)=f_1(x)h_1(x)$对某个$h_1(x)\in P[x]$. 又$f_2(x)|g(x)=f_1(x)h_1(x)$，而$(f_1(x),f_2(x))=1$，于是由定理知，$f_2(x)|h_1(x)$，即$h_1(x)=f_2(x)h_2(x)$对某个$h_2(x)\in P[x]$. 于是$g(x)=f_1(x)f_2(x)h_2(x)$，故$f_1(x)f_2(x)|g(x)$.

最大公因式与互素的概念可以推广到任意有限多个多项式的情形.

【例6】证明：若$f(x), g(x)$不全为零，且$u(x)f(x)+v(x)g(x)=(f(x), g(x))$，则$(u(x), v(x))=1$.

**证明：** 若$f(x), g(x)$不全为零，则$(f(x), g(x))\neq 0$. 由最大公因式定理，存在$u(x), v(x)\in P[x]$，使得

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

因为$(f(x), g(x))|f(x), (f(x), g(x))|g(x)$，所以$\frac{f(x)}{(f(x),g(x))}, \frac{g(x)}{(f(x),g(x))}\in P[x]$. 于是

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

故$(u(x),v(x))=1.$

注：对任意$f(x),g(x)\in P[x]$，在一般情况下，不要随意使用符号$\frac{f(x)}{g(x)}$，除非$g(x)|f(x)$.

## 第4节 因式分解

- **不可约多项式**

**定义** 设$p(x)\in P[x]$，且$\deg((p(x))\geq 1$，$p(x)$称为数域$P$上的不可约多项式，如果$p(x)$不能表示成数

域$P$上的两个次数比$p(x)$的次数低的多项式的乘积.

由定义知：若$p(x)$不可约，则

(1) $p(x)$的因式只有非零常数与它自身的非零常数倍;

(2) 对于任意的$f(x) \in P[x]$，$p(x)|f(x)$或者$(f(x), p(x)) = 1$.

**定理** 如果$p(x)$是数域$P$上的不可约多项式，则对任意的$f(x), g(x) \in P[x]$，若$p(x)|f(x)g(x)$，则$p(x)|f(x)$或者$p(x)|g(x)$.

**证明**：若$p(x) \nmid f(x)$，因$p(x)$是不可约多项式，

则$(f(x),p(x))=1$，由整除的性质知，$p(x)|g(x)$.

下列结论表明上述定理的逆命题也是成立的.

【例 7】 证明：设$p(x)$是次数大于零的多项式，如果对于任何多项式$f(x),g(x)$，由$p(x)|f(x)g(x)$可以推出$p(x)|f(x)$或者$p(x)|g(x)$，则$p(x)$是不可约多项式.

证明：假定$p(x)$可约，则$p(x)=p_1(x)p_2(x)$，这里$1\leq \deg(p_i(x))<\deg(p(x))$，$i=1,2$. 因为$p(x)|p_1(x)p_2(x)$，所以$p(x)|p_1(x)$或者$p(x)|p_2(x)$，这是不可能的. 故$p(x)$是不可约多项式.

- **因式分解定理**

对$\deg(f(x))$及$s$作数学归纳法，可得

**因式分解定理**：数域$P$上的每个次数$\geq 1$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. 所谓唯一性是指，如果$f(x)$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$s = t$，且适当排列因式的次序后有

$$p_1(x) = c_i q_i(x), \quad i = 1, 2, \cdots, s,$$

这里每个$c_i$都是一些非零常数.

**标准分解式**：若将分解式中每一个不可约因式的首项系数提出来成为首项系数为1的多项式，再把相同的不可约因式合并，则$f(x)$的分解式成为

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

其中$c$是$f(x)$的首项系数，$p_1(x),p_2(x),\cdots,p_s(x)$是不同的首项系数为1的不可约多项式，而$r_1,r_2,\cdots,r_s$是正整数，且满足

$$\deg(f(x))=r_1\deg(p_1(x))+\cdots+r_s\deg(p_s(x)),$$

这种分解称为标准分解式.

注: 事实上，对任意$f(x)\in P[x]$，我们无法获取$f(x)$的标准分解式，上述结果只是从理论上表明$f(x)$的标准分解式的存在性.

- **复数域或实数域上多项式的因式分解**

复数域$\mathbb{C}$上的不可约多项式只有一次的. 于是有:

**定理** 每个次数$\geq 1$的复系数多项式$f(x)$在复数域上都可以唯一地分解成一次因式的乘积，即

$$f(x) = a_n(x-\alpha_1)^{\ell_1}(x-\alpha_2)^{\ell_2}\cdots(x-\alpha_s)^{\ell_s}$$

其中$a_n, \alpha_1, \cdots, \alpha_s \in \mathbb{C}$，而$\ell_1, \cdots, \ell_s$是正整数.

实数域$\mathbb{R}$上的不可约多项式只有一次或二次质因式(满足条件$\triangle = p^2 - 4q < 0$的二次式$x^2 + px + q$). 因此有:

**定理** 每个次数$\geq 1$的实系数多项式$f(x)$在实数域上都可以唯一地分解成一次因式与二次质因式的乘积，即

$$f(x) = a_n(x-\alpha_1)^{\ell_1}\cdots(x-\alpha_s)^{\ell_s}(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_rx+q_r)^{k_r}$$

其中$a_n, \alpha_1, \cdots, \alpha_s, p_1, \cdots, p_r, q_1, \cdots, q_r \in \mathbb{R}$，而$\ell_1, \cdots, \ell_s, k_1, \cdots, k_r$是正整数.

注: 判断一般数域$P$上的多项式$f(x)$是否不可约，有时可以直接判断. 如判断多项式$f(x) = x^4+4$在数域$P$上是否不可约? 因$f(x) = (x^2+2)^2 - 4x^2 = (x^2+2x+2)(x^2-2x+2)$，所以$f(x) = x^4+4$在数域$P$上可约；有时无法判断. 如判断多项式$f(x) = x^4+2$在数域$P$上是否不可约? 如不明确具体的数域$P$，判断将无法进行.

## 第5节 重因式

- **形式微商**

设$f(x)=\sum\limits_{i=0}^{n} a_i x^i \in P[x]$，定义

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$$

为$f(x)$的一阶形式微商. 由归纳法可定义$n$阶形式微商: $f^{(n)}(x)=[f^{(n-1)}(x)]'$. 由上述规定易得

**定理** 设$f(x), g(x) \in P[x]$.

(1) 若$\deg(f(x)) \geq 1$，则$\deg(f'(x))=\deg(f(x))-1$.

(2) $(f(x)\pm g(x))'=f'(x)\pm g'(x)$.

(3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$，特别地，$(cf(x))' = cf'(x)$.

(4) 若$p(x)$不可约，则$(p(x), p'(x)) = 1$.

- **重因式**

**定义** 不可约多项式$p(x)$称为多项式$f(x)$的$k$重因式，如果$p^k(x)|f(x)$，而$p^{k+1}(x) \nmid f(x)$.

当$k = 1$时，$p(x)$称为$f(x)$的单因式，当$k > 1$时，$p(x)$称为$f(x)$的$k$重因式. 今后除非具体指明$k$重因式时，$k$可以取1从而$p(x)$是单因式. 否则当提到重因式时，意味着$k \geq 2$.

以下将利用形式微商，建立一个多项式有重因式的条件.

**定理** 如果不可约多项式$p(x)$是$f(x)$的$k(k \geq 1)$重因式，则它必是$f'(x)$的$k-1$重因式.

**证明：** 由题设令$f(x) = p^k(x)g(x)$，这里$g(x) \in P[x]$，且$p(x) \nmid g(x)$. 于是有

$$f'(x) = p^{k-1}(x)(kg(x)p'(x) + p(x)g'(x)).$$

因此，$p^{k-1}(x)|f'(x)$. 但$p(x) \nmid (kg(x)p'(x) + p(x)g'(x))$. 故$p(x)$是$f'(x)$的$k-1$重因式.

通过对$k$作数学归纳法，易得

**推论** 如果不可约多项式$p(x)$是$f(x)$的$k$重因式($k \geq 1$)，则$p(x)$必是

$$f(x), f'(x), \cdots, f^{(k-1)}(x)$$

的因式，但不是$f^{(k)}(x)$的因式.

由此建立$f(x)$是否有重因式的判别方法.

**定理** 不可约多项式$p(x)$是$f(x)$的重因式$\Leftrightarrow p(x)$是$f(x)$与$f'(x)$的公因式.

**证明：** 必要性显然. 下证充分性. 假定$k = 1$，易知$p(x)$不是$f(x)$与$f'(x)$的公因式，从而$k > 1$. 故$p(x)$是$f(x)$的重因式.

**推论** $f(x)$没有重因式$\Leftrightarrow (f(x), f'(x)) = 1.$

**【例 8】**试确定$p$的值，使$f(x) = x^3 + 6x^2 + 3px + 8$有重因式.

**解：** $f'(x) = 3(x^2 + 4x + p)$. 由辗转相除法，得

$$f(x) = (x + 2)f'(x) + 2(p - 4)x + 2(4 - p).$$

①当$p = 4$时，$(f(x), f'(x)) = x^2 + 4x + 4$，$f(x)$有重因式；

②当$p \neq 4$时，继续由辗转相除法，得

$$f'(x) = (\frac{1}{p-4}x + \frac{5}{p-4})((p - 4)x + (4 - p)) + p + 5.$$

当$p=-5$时，$(f(x),f'(x))=x-1$，$f(x)$也有重因式.

综上所述，$p=4$或$-5$

- **多项式函数**

设$f(x)=\sum\limits_{i=0}^{n}a_ix^i$是数域$P$上的一元多项式. 对于任意的$\alpha\in P$，称$f(\alpha)=\sum\limits_{i=0}^{n}a_i\alpha^i$为$f(x)$在$x=\alpha$时的值. 由此多项式$f(x)$即是定义在$P$上的函数. 特别地，如果$f(\alpha)=0$，称$\alpha$是$f(x)$在$P$上的根.

**定理** (余数定理)用一次多项式$x-\alpha$去除多项式$f(x)$，所得余式是一个常数，这个常数等于$f(\alpha)$.

**证明**：用$x-\alpha$去除$f(x)$，设商为$q(x)$，余式为一个常数$c$. 于是有

$$f(x)=(x-\alpha)q(x)+c.$$

令$x=\alpha$，得$c=f(\alpha)$.

**推论** $\alpha$是$f(x)$的根$\Leftrightarrow(x-\alpha)|f(x)$.

**定理** $P[x]$中$n$次多项式($n\geq 0$) 在数域$P$中的根不可能多于$n$个，重根按重数计算.

证明：设$f(x)\in P[x]$，若$\deg(f(x))=0$，结论显然成立. 若$\deg(f(x))>0$，将$f(x)$分解成不可约多项式的乘积，则在数域$P$中$f(x)$的根的个数等于分解式中一次因式的个数，这个数目自然不超过$n$.

【例9】如果$(x-1)^2|(ax^4+bx^2+1)$，求$a,b$.

解：$x-1$是$f(x)=ax^4+bx^2+1$的重因式，必是$f'(x)=4ax^3+2bx$的因式，于是

$$\begin{cases} f(1)=a+b+1=0 \\ f'(1)=4a+2b=0 \end{cases}，解之得\begin{cases} a=1 \\ b=-2 \end{cases}.$$

注: 一般地，$x_0$是$f(x)$的$n$重根$\Leftrightarrow f(x_0)=f'(x_0)=\cdots=f^{(n-1)}(x_0)=0$，但$f^{(n)}(x_0)\neq 0$.

## 第6节 有理系数多项式

- **本原多项式**

对任意$f(x) \in \mathbb{Q}[x]$，存在$c \in \mathbb{Z}$及$g(x) \in \mathbb{Z}[x]$，使得$g(x) = cf(x)$. 因此，任何一个有理系数多项式是否有根或是否可约的问题完全可以归结为一个整系数多项式是否有根或是否有可约的问题.

**定义** 如果一个非零的整系数多项式

$$f(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

的系数$b_n, b_{n-1}, \cdots, b_1, b_0$没有异于$\pm 1$的公因子，称它为一个本原多项式.

显然，任何一个有理系数多项式都可以表为一个有理数与一个本原多项式的乘积. 特别地，若$f(x)\in\mathbb{Q}[x]$，且

$$f(x)=rg(x)=sh(x),$$

$r,s\in\mathbb{Q}$，且$g(x)$与$h(x)$均是本原的，则$r=\pm s$.

**Gauss引理：** 两个本原多项式的乘积还是本原多项式.

**证明：** 设

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

是两个本原多项式，而

$$h(x)=f(x)g(x)=d_{n+m}x^{n+m}+d_{n+m-1}x^{n+m-1}+\cdots+d_1x+d_0$$

是它们的积.

假定$h(x)$不是本原的，则存在素数$p$整除$h(x)$的所有系数. 因$f(x)$是本原的，$p$不能整除$f(x)$的所有系数. 令$a_i$是第一个不能被$p$整除的数，即

$$p|a_0,\cdots,p|a_{i-1},p\nmid a_i.$$

同样地，$g(x)$是本原的，$p$不能整除$g(x)$的所有系数. 令$b_j$是第一个不能被$p$整除的数，即

$$p|b_0,\cdots,p|b_{j-1},p\nmid b_j.$$

考察$h(x)$的系数$d_{i+j}$，由乘积的定义，有

$$d_{i+j} = a_ib_j + a_{i+1}b_{j-1} + \cdots$$

因为$p|d_{i+j}$，且$p$能整除等式左端除$a_ib_j$以外的所有项，所以$p|a_ib_j$，从而$p|a_i$，或$p|b_j$，这与$a_i$及$b_j$的选取矛盾. 故$h(x)$是本原的.

利用Gauss引理，易得如下两个推论.

**推论 1** 如果一个非零的整系数多项式能够分解成两个次数较低的有理系数多项式的乘积，那么它一定能分解成两个次数较低的整系数多项式的乘积.

**推论 2** 设$f(x), g(x)$是整系数多项式，且$g(x)$是本

原的. 如果$f(x)=g(x)h(x)$，其中$h(x)$是有理系数多项式，那么$h(x)$一定是整系数多项式.

- **整系数多项式的有理根**

**定理** 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

是一个整系数多项式，而$\frac{r}{s}$是它的一个有理根，其中$r,s$互素，那么必有$s|a_n, r|a_0$. 特别地，如果$a_n=1$，那么$f(x)$ 的有理根都是整根.

**证明**：因为$\frac{r}{s}$是$f(x)$的有理根，因此，在有理数域$\mathbb{Q}$上，$(x-\frac{r}{s})|f(x)$，从而$(sx-r)|f(x)$. 因为$r,s$互素，所以$sx-r$是一个本原多项式，由推论2知

$$f(x)=(sx-r)(b_{n-1}x^{n-1}+\cdots+b_0)$$

式中$b_{n-1},\cdots,b_0$都是整数，比较两边的系数可得：

$$a_n=sb_{n-1},\ a_0=-rb_0.$$

故$s|a_n,\ r|a_0$.

**【例 10】**求方程$2x^4-x^3+2x-3=0$的有理根.

**解：** 这里$a_n=2, a_0=-3$，令方程的有理根为$\frac{r}{s}$，于是$s|2, r|3$. 故所有可能的有理根是$\pm1,\ \pm3,\ \pm\frac{1}{2},\ \pm\frac{3}{2}$. 直接验证(代入方程或通过带余除法法则)可知：除去1外，其余均不是方程的根，故原方程的有理根只有$x=1$.

- **整系数多项式的不可约性**

Eisenstein 判别法：设

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

是一个整系数多项式. 如果存在一个素数$p$，使得

(1) $p \nmid a_n$;

(2) $p | a_{n-1}, a_{n-2}, \cdots, a_0$;

(3) $p^2 \nmid a_0$.

那么$f(x)$在有理数域上是不可约的.

**证明：**假定$f(x)$在有理数域上可约，则$f(x)$可分解成两个次数较低的整系数多项式的乘积，令

$$f(x)=(b_\ell x^\ell+b_{\ell-1}x^{\ell-1}+\cdots+b_0)(c_m x^m+c_{m-1}x^{m-1}+\cdots+c_0)$$

这里$0<\ell,m<n$，且$\ell+m=n$. 比较等式两端系数可得

$$a_n=b_\ell c_m,\quad a_0=b_0c_0$$

因为$p|a_0$，所以$p|b_0$或$p|c_0$，但$p^2\nmid a_0$，所以$p$不能同时整除$b_0$及$c_0$. 不失一般性，令$p|b_0$，但$p\nmid c_0$. 另一方面，因为$p\nmid a_n$，所以$p\nmid b_\ell$. 假设$b_0,b_1,\cdots,b_\ell$中第一个不能被$p$整除的是$b_k$，$p|b_0,\cdots,p|b_{k-1},p\nmid b_k$. 比较$f(x)$中$x^k$的系数可得：

$$a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k$$

式中$a_k, b_{k-1}, \cdots, b_0$都能被$p$整除，所以$b_k c_0$也必能被$p$整除. 但$p$是一个素数，所以$b_k$与$c_0$中至少有一个能被$p$整除，这是一个矛盾.

**【例 11】** 设$f(x) \in \mathbb{Z}[x]$ (整系数多项式).

(1) 令$x = y \pm 1$，$g(y) = f(y \pm 1)$，证明：$f(x)$与$g(y)$同时可约或同时不可约.

(2) 利用上述结果判断多项式$f(x) = x^6 + x^3 + 1$是否可约?

**证明：**(1) 假定$f(x)$可约，则$f(x) = f_1(x)f_2(x)$. 从而$g(y) = f(y \pm 1) = f_1(y \pm 1)f_2(y \pm 1)$，这即说

明$g(y)$可约，反之亦然. 故$f(x)$与$g(y)$同时可约或同时不可约.

(2) 令$x=y+1$，则

$$
\begin{aligned}
&(y+1)^6+(y+1)^3+1\\
&=y^6+6y^5+15y^4+21y^3+18y^2+9y+3
\end{aligned}
$$

现取$p=3$. 利用Eisenstein判别法知$f(x)$不可约.

注: 在利用Eisenstein判别法判别整系数多项式的不可约性时，注意这一条件只是充分条件. 因此当一个整系数多项式的常数项为1时，这一判别法失效. 此时需要对多项式形式作进一步变形(如【例11】)或采用其它方法，如反证法.

# 习题讨论课一

## 一、填空题

1. 若$(x^2+x-1)|(x^3+px+q)$，则$p, q$的值分别为______.

2. 已知用$x-1, x-2$除$f(x)$的余式分别为$1, 2$，则用$g(x)=(x-1)(x-2)$除$f(x)$的余式为______.

3. 设$f(x)=x^4-4x^3+1$，$g(x)=x^3-3x^2+1$，则$(f(x), g(x))=$______.

4. 设$k\in\mathbb{Z}$，若$x^3+kx+1$在$\mathbb{Q}[x]$上可约，则$k$应满足的条件是______.

5. 若多项式$f(x)=x^3+3x^2+tx+1$仅有$2$重根，则$t=$______.

## 二、解答与证明题.

6. 设$f(x)=x^3+(1+t)x^2+4x+2u$，$g(x)=x^3+tx^2+2u$的最大公因式是一个二次多项式，求$t, u$的值.

7. 若$(f(x),g(x))=1$，证明：$(f(x)+g(x),f(x)g(x))=1$.

8. 设

$$f(x)=6x^4+3x^3+ax^2+bx-1,$$
$$g(x)=4x^4-8ax^3+3x^2-20bx-16,$$

其中$a,b$是整数，试求出使$f(x),g(x)$有公共有理根的全部$a,b$.

9. 问多项式

$$f(x)=(x-1)(x-2)\cdots(x-n)-1$$

在有理数域$\mathbb{Q}$上是否不可约? 为什么?

10. 设$p$是一个素数. 证明: 多项式

$$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

在有理数域$\mathbb{Q}$上不可约.

# 习题讨论课一参考解答

1. **解**： 由带余除法，得$x^3+px+q=(x-1)(x^2+x-1)+(p+2)x+q-1$. 因为$(x^2+x-1)|(x^3+px+q)$，所以$(p+2)x+q-1=0$，从而$p=-2,q=1$.

2. **解**： 依题意，$f(1)=1,f(2)=2$. 由带余除法法则，令$f(x)=(x-1)(x-2)q(x)+r(x)$，其中$r(x)=0$或$\partial(f(x))\leq 1$. 显然$r(x)\neq 0$，令$r(x)=ax+b$，则

$$\begin{cases} r(1)=a+b=f(1)=1 \\ r(2)=2a+b=f(2)=2 \end{cases}，\text{解之得}\begin{cases} a=1 \\ b=0 \end{cases}.$$

故$r(x)=x$.

3. **解**： 利用辗转相除法，得$(f(x),g(x))=1$.

4. **解**：因为$x^3+kx+1$在$\mathbb{Q}[x]$上可约，所以$x^3+kx+1$必有一次因式，因而必有有理根. 又因其常数项为1，从而有理根为1或$-1$，于是必有

$1^3+k\cdot1+1=0$或$(-1)^3+k\cdot(-1)+1=0$，故$k=-2$或$0$.

5. **解：** 依题意，$(f(x),f'(x))\neq1$. $f'(x)=3x^2+6x+t$，用$f'(x)$除$f(x)$得余式

$$r_1(x)=\tfrac{2t-6}{3}x+\tfrac{3-t}{3}.$$

再用$r_1(x)$除$f'(x)$得余式

$$r_2(x)=t+\tfrac{15}{4}.$$

因多项式$f(x)$有重根，所以$(f(x),f'(x))\neq1$，从而$r_1(x)=0$或$r_2(x)=0$，解之得$t=3$或$t=-\frac{15}{4}$. 注意到当$t=3$时，$f(x)=x^3+3x^2+3x+1=(x+1)^3$有3重根，不合题意舍去，故$t=-\frac{15}{4}$.

6. **解：** 由辗转相除法法得

$$f(x)=1\cdot g(x)+(tx^2+4x)$$
$$g(x)=(x+t-4)(tx^2+4x)-4(t-4)x+2u.$$

依题意，$-4(t-4)x+2u=0$，从而

$$\begin{cases} -4(t-4)=0 \\ 2u=0 \end{cases}，解之得 \begin{cases} t=4 \\ u=0 \end{cases}.$$

7. **证明：** 假定$(f(x)+g(x), f(x)g(x)) \neq 1$，令$(f(x)+g(x), f(x)g(x)) = d(x)$，则$\partial(d(x)) \geq 1$. 取$d(x)$的一个不可约因式$p(x)$. 因为$p(x)|f(x)g(x)$，而$p(x)$是不可约的，所以$p(x)|f(x)$或$p(x)|g(x)$. 不失一般性，设$p(x)|f(x)$. 又$p(x)|f(x)+g(x)$，且$p(x)|f(x)$，则$p(x)|g(x)$，显然与$(f(x), g(x)) = 1$矛盾. 故结论成立.

8. **解：** $f(x)$可能的有理根为$\pm1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{6}$，而$g(x)$可能的有理根为$\pm1, \pm2, \pm4, \pm8, \pm16, \pm\frac{1}{2}, \pm\frac{1}{4}$，因此它们公共有理根的可能范围是$\pm1, \pm\frac{1}{2}$.

①若$f(1)=0, g(1)=0$时，有

$$\begin{cases} a+b=-8 \\ 8a+20b=-9 \end{cases}，解之得 \begin{cases} a=-\frac{151}{12} \\ b=\frac{55}{12} \end{cases}.$$

因为$a,b$不是整数，所以1不是$f(x)$与$g(x)$的公共有理根.

②若$f(-1)=0, g(-1)=0$时，有

$$\begin{cases} a-b=-2 \\ 8a+20b=9 \end{cases}，解之得\begin{cases} a=-\frac{31}{28} \\ b=\frac{35}{28} \end{cases}.$$

所以$-1$也不是$f(x)$与$g(x)$的公共有理根.

③若$f(-\frac{1}{2})=0, g(-\frac{1}{2})=0$时，有

$$\begin{cases} a-2b=4 \\ a+10b=15 \end{cases}，解之得\begin{cases} a=\frac{35}{6} \\ b=\frac{11}{12} \end{cases}.$$

所以$-\frac{1}{2}$也不是$f(x)$与$g(x)$的公共有理根.

④若$f(\frac{1}{2})=0, g(\frac{1}{2})=0$时，有

$$\begin{cases} a+2b=1 \\ a+10b=-15 \end{cases}，\text{解之得}\begin{cases} a=5 \\ b=-2 \end{cases}.$$

所以仅有$\frac{1}{2}$是$f(x)$与$g(x)$的公共有理根，此时$a=5, b=-2$.

9. **解**：不可约. 当$n=1$时，$f(x)=x-2$，结论成立. 当$n\geq 2$时，采用反证法证明. 假定$\exists g(x), h(x)\in\mathbb{Z}[x]$，使得

$$f(x)=g(x)h(x)，\text{其中}1\leq\partial(g(x)),\partial(h(x))<n.$$

则

$$f(i)=g(i)h(i)=-1\ (i=1,2,\cdots,n).$$

因为$g(i)$与$h(i)$均为整数，则$g(i)$与$h(i)$必符号相反，从而

$$g(i)+h(i)=0\ (i=1,2,\cdots,n).$$

这表明多项式$g(x)+h(x)$至少有$n$个不同的根$1,2,\cdots,n$，但由于多项式$g(x)+h(x)$的次数小于$n$，这显然是不可能的. 假定不成立，从而多项式$f(x)$不可约.

10. **解：** 令$x=y+1$，由$(x-1)f(x)=x^p-1$，可得

$$yf(y+1)=(y+1)^p-1=y^p+C_p^1y^{p-1}+\cdots+C_p^{p-1}y.$$

所以

$$g(y):=f(y+1)=y^{p-1}+C_p^1y^{p-2}+\cdots+C_p^{p-1}.$$

$g(y)$的最高次项系数1不能被$p$整除，其余任一项系数

$$C_p^k=\frac{p(p-1)\cdots(p-k+1)}{k!}$$

是一整数，但$(k!,p)=1$，所以$k!|(p-1)\cdots(p-k+1)$，从而$p|C_p^k$，但$p^2\nmid C_p^{p-1}=p$. 由Eisenstein判别法，$g(y)$在$\mathbb{Q}$上不可约. 从而$f(x)$在$\mathbb{Q}$上不可约.