# 多项式

问题: 分解因式$x^4-x^2-2$.

- 有理数范围: $(x^2+1)(x^2-2)$;
- 实数范围: $(x^2+1)(x+\sqrt{2})(x-\sqrt{2})$;
- 复数范围: $(x+\sqrt{-1})(x-\sqrt{-1})(x+\sqrt{2})(x-\sqrt{2})$.

有理数集$\mathbb{Q}$, 实数集$\mathbb{R}$, 复数集$\mathbb{C}$具有以下共同点:

- 都含有0, 1;
- 对四则运算封闭.

**定义**

设$\mathbb{P}$是复数集$\mathbb{C}$的子集, 如果它满足: (1) $0, 1 \in \mathbb{P}$; (2) 关于四则运算封闭(即$P$中任意两数相加、相减、相乘、相除(除数不为零), 结果仍在$\mathbb{P}$中), 则称$\mathbb{P}$为一个数域.

除了前面提到的有理数域$\mathbb{Q}$, 实数域$\mathbb{R}$和复数域$\mathbb{C}$之外, 还有很多其他的数域, 我们举一个简单的例子.

**例**

令$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, 则它是一个数域.

- 加、减法:
  $(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2}$;
- 乘法:
  $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$;
- 除法: $(a_1 + b_1\sqrt{2})/(a_2 + b_2\sqrt{2}) =$
  $\big((a_1a_2 - 2b_1b_2) + (a_2b_1 - a_1b_2)\sqrt{2}\big)/(a_2^2 - 2b_2^2)$.

**思考题**

(*) 证明$\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$是一个数域.

**命题1**

任何一个数域$P$都包含有理数域$\mathbb{Q}$, 因此$\mathbb{Q}$ 是最小的数域.

**证明**

由于$P$中包含0, 1, 利用加、减法的封闭性可知$P$中包含所有整数, 再用除法封闭性可知$P$中包含所有有理数.

**命题2**

若数域$P$包含实数域$\mathbb{R}$, 且$P \neq \mathbb{R}$, 则$P = \mathbb{C}$.

**证明**

由于$\mathbb{R} \subset P$且$P \neq \mathbb{R}$, 所以存在虚数$a + b\sqrt{-1} \in P$, $a, b \in \mathbb{R}$, $b \neq 0$. 再利用$a$, $b \in P$, 即得$\sqrt{-1} \in P$.

**定义**

设$P$是一个数域, $x$是一个变元(符号). 称形式表达式

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

为数域$P$上的一元多项式, 简称多项式. 称$a_ix^i$为这个多项式的$i$次项, $a_i$为$i$次项的系数; $a_0$也称为常数项. 若$a_n \neq 0$, 则称$a_nx^n$为首项, $a_n$为首项系数, $n$为该多项式的次数.

- 各项系数全为零的多项式, 称为零多项式, 记为0. 约定零多项式的次数为$-\infty$.
- 通常用$f$, $g$或$f(x)$, $g(x)$等等表示多项式. 将$f$的次数记作$\deg(f)$. 数域$P$上关于变元$x$的多项式的集合, 记作$P[x]$.
- 对于多项式$a_0 + a_1x + \cdots + a_nx^n$, 当$i > n$时, 约定它的$i$次项系数为0. 两个多项式相等, 是指它们的各项系数对应相等.

**定义**

两个多项式相加，就是把对应项的系数加起来；所得的多项式称为这两个多项式的和. 将多项式$f$与$g$的和记作$f+g$.

**例**

若$f=1-7x-4x^3+3x^5$, $g=12+3x+4x^2+5x^3$, 则

$$f+g=13-4x+4x^2+x^3+3x^5.$$

多项式的加法满足下述运算律:

- 交换律: $f+g=g+f$;
- 结合律: $(f+g)+h=f+(g+h)$;
- 零元素: $0+f=f$;
- 负元素: $f+(-f)=0$, 这里$-f$表示将$f$的各项系数变为其相反数之后所得的多项式, 称为$f$的相反多项式或负多项式.

**定义**

两个多项式相减，就是把对应项的系数相减；所得的多项式称为这两个多项式的差. 将多项式$f$与$g$的差记作$f - g$.

由定义可知，多项式$f$与$g$的差$f - g$，等于$f$与$-g$的和$f + (-g)$.

**例**

若$f = 1 - 7x - 4x^3 + 3x^5$，$g = 12 + 3x + 4x^2 + 5x^3$，则

$$f - g = -11 - 10x - 4x^2 - 9x^3 + 3x^5.$$

**思考题**

(**) 设$f, g \in P[x]$. 证明：$\deg(f \pm g) \leq \max(\deg(f), \deg(g))$.

**定义**

两个多项式相乘，就是把两者的各项分别相乘再加起来；所得多项式称为它们的积. 两个多项式$f$与$g$的积，记作$fg$.

**例**

若$f = x^4 - 4x^3 + 8x^2 + 4x + 1$，$g = x^4 + 4x^3 + 8x^2 - 4x + 1$，则

$$fg = x^8 + 98x^4 + 1.$$

一般地，若$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$，则

$$fg = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \cdots + c_1 x + c_0,$$

其中

$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0, \quad 0 \le k \le n+m.$$

多项式的乘法满足如下运算律:

- 交换律: $fg = gf$;
- 结合律: $f(gh) = (fg)h$;
- 分配律: $(f+g)h = fh + gh$.

**思考题**

(**) 设 $f$, $g \in P[x]$. 证明: $\deg(fg) = \deg(f) + \deg(g)$.

**命题**

设$f$, $g$为$P[x]$中多项式, 且$g \neq 0$, 则存在唯一的一组多项式$q$, $r \in P[x]$, 使得

$$f = gq + r, \quad \deg(r) < \deg(g).$$

分别称$q$, $r$为$g$除$f$所得的商和余式.

## 证明

存在性: 我们对$\deg(f)$用数学归纳法.
当$\deg(f) < \deg(g)$时, $q = 0$, $r = f$符合要求.
假设当$\deg(f) < m$时(这里$m \geq \deg(g)$), 存在符合要求的多项式$q$, $r$. 那么, 当$\deg(f) = m$时, 设$f$, $g$的首项分别为$ax^m$, $bx^n$,
令$q_1 = a/bx^{m-n}$, $f_1 = f - gq_1$, 则$\deg(f_1) < m$, 由归纳假设可知, 存在多项式$q_2$, $r$ 使得

$$f_1 = gq_2 + r, \quad \deg(r) < \deg(g).$$

令$q = q_1 + q_2$, 则有$f = gq + r$.

## 证明(续)

唯一性: 若有多项式$q$, $r$和$\widetilde{q}$, $\widetilde{r}$使得

$$f = gq + r = g\widetilde{q} + \widetilde{r}, \quad \deg(q) < \deg(g), \quad \deg(\widetilde{q}) < \deg(g),$$

则$r - \widetilde{r} = (\widetilde{q} - q)g$, 我们有

$$\deg(\widetilde{q} - q) + \deg(g) = \deg(r - \widetilde{r}) < \deg(g),$$

因此$\widetilde{q} - q = 0$, $r - \widetilde{r} = 0$.

当$g = x - \alpha$为一次多项式时，$g$除$f$的余式$r$的次数$< 1$，所以$r$为常数．在等式$f = (x - \alpha)q + r$中取$x = \alpha$代入，就得到$r = f(\alpha)$．因此有

**余数定理**

一次多项式$x - \alpha$除$f(x)$所得的余式为$f(\alpha)$.

当$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$时，可以采用下面的方法计算$f(\alpha)$:

$$\begin{aligned} b_n &= a_n, \\ b_{n-1} &= \alpha b_n + a_{n-1}, \\ b_{n-2} &= \alpha b_{n-1} + a_{n-2}, \\ &\cdots\cdots \\ b_1 &= \alpha b_2 + a_1, \\ b_0 &= \alpha b_1 + a_0. \end{aligned}$$

容易看出, $b_k = a_n\alpha^{n-k} + a_{n-1}\alpha^{n-k-1} + \cdots + a_{k+1}\alpha + a_k$, $b_0 = f(\alpha)$.

计算$x-\alpha$除$f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$的过程可以采用下面的格式, 称为综合除法.

$$\begin{array}{c|cccccc} \alpha & a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ & & \alpha b_n & \alpha b_{n-1} & \cdots & \alpha b_2 & \alpha b_1 \\ \hline & b_n & b_{n-1} & b_{n-2} & \cdots & b_1 & b_0 \end{array}$$

## 例

计算$x-2$除$x^3-3x^2+3x-1$的商和余式.

## 解答

$$\begin{array}{c|cccc} 2 & 1 & -3 & 3 & -1 \\ & & 2 & -2 & 2 \\ \hline & 1 & -1 & 1 & 1 \end{array}$$

因此, 商为$x^2-x+1$, 余式为1.

**定义**

设$f$, $g \in P[x]$且$g \neq 0$. 如果$g$除$f$所得的余式为0, 则称$g$整除$f$, 记作$g|f$. 这时称$g$为$f$的因式, 称$f$为$g$的倍式.

**整除的性质**

设$a$, $b$, $c \in P[x]$.

(1) (传递性) 若$a|b$, $b|c$, 则$a|c$;

(2) (组合性) 若$a|b$, $a|c$, 则$a$整除$b$与$c$的一个组合, 即$a|bu+cv$, $\forall u$, $v \in P[x]$.

**定义**

设$f_1$, $f_2$, $g \in P[x]$且$g \neq 0$. 如果$g$除$f_1$, $f_2$ 所得的余式相等, 则称$f_1$, $f_2$模$g$同余, 记作$f_1 \equiv f_2 \pmod{g}$.

显然$f_1 \equiv f_2 \pmod{g}$等价于$g | f_1 - f_2$.

**同余的可加性和可乘性**

如果$f_1 \equiv f_2 \pmod{g}$, $h_1 \equiv h_2 \pmod{g}$, 则有

$$f_1 + h_1 \equiv f_2 + h_2 \pmod{g},$$
$$f_1 h_1 \equiv f_2 h_2 \pmod{g}.$$

**定义**

设$f$, $g \in P[x]$. 如果存在$d \in P[x]$, 使得

(1) $d$是$f$与$g$的公因式, 即$d|f$, $d|g$;

(2) 对于$f$与$g$的任一公因式$h$, 有$h|d$;

则称$d$为$f$, $g$的一个最大公因式.

**引理**

设$f$, $g$, $q$, $r \in P[x]$满足$f = gq + r$. 如果$d$是$g$与$r$ 的最大公因式, 则$d$也是$f$与$g$的最大公因式.

**证明**

由$d|g$, $d|r$可知$d|gq + r$, 即$d|f$. 可见$d$是$f$与$g$的公因式. 对于$f$与$g$的任一公因式$h$, 由$h|f$, $h|g$可知$h|f - gq$, 即$h|r$. 因此$h$也是$g$与$r$的公因式, $h|d$.

# Bezout定理

**定理**

设$f, g \in P[x]$不同时为零，则$f$与$g$的最大公因式$d$存在，且能写为$f$与$g$的组合.

**证明**

不妨设$\deg(g) \le \deg(f)$. 若$g = 0$，则$f$是$f$与$g$的最大公因式. 因此以下设$\deg(g) \ge 0$.
我们对$\deg(g)$用数学归纳法.
当$\deg(g) = 0$时，$g$为非零常数，易知$g$是$f$与$g$的最大公因式.
假设当$\deg(g) < n$时(这里$n \ge 1$)，$f$与$g$的最大公因式存在且能表达为$f$与$g$的组合. 那么，当$\deg(g) = n$时，作带余除法$f = gq + r$，$\deg(r) < \deg(g)$. 则由归纳假设知$g$与$r$的最大公因式$d$存在，且能表达为$g, r$的组合. 再由引理，$d$也是$f$与$g$的最大公因式.

上述定理的证明过程就是计算最大公因式的辗转相除法：为了计算两个多项式的最大公因式，只需用其中次数较低的多项式去除另一个多项式，并将后者用余式代替. 如此反复作除法，则多项式的次数一直严格减小，直到其中一个多项式为零，这时另一个多项式就是要求的最大公因式.

**例**

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

**解答**

应用辗转相除法，依次得到$f = q_1 g + r_1$, $g = q_2 r_1 + r_2$, $r_1 = q_3 r_2 + r_3$, $r_2 = q_4 r_3 + r_4$, 其中$q_1 = x + 1$, $r_1 = x^3 + x^2 + 2$, $q_2 = x - 2$, $r_2 = x^2 - x + 1$, $q_3 = x + 2$, $r_3 = x$, $q_4 = x - 1$, $r_4 = 1$. 可见$(f, g) = (r_3, r_4) = 1$.

**定义**

设$f,\ g\in P[x]$. 如果$(f,g)=1$, 则称$f$与$g$互素.

**定理**

设$f,\ g\in P[x]$不全为 0, 则$f$与$g$互素的充要条件是存在$u,\ v\in P[x]$使得$uf+vg=1$.

**证明**

$\Longrightarrow$: Bezout定理.
$\Longleftarrow$: 由于$(f,g)$一定整除$uf+vg=1$, 所以$(f,g)=1$.

**命题**

设$f$, $g$, $h \in P[x]$.

(1) 若$(f, g) = 1$且$f \mid gh$, 则$f \mid h$;

(2) 若$(f, g) = 1$且$f \mid h$, $g \mid h$, 则$fg \mid h$.

**证明**

(1) 由$(f, g) = 1$可知存在$u$, $v \in P[x]$使得$uf + vg = 1$. 由$f \mid gh$可知存在$w \in P[x]$使得$gh = fw$. 由这两式消去$g$可得$h = (uh - vw)f$, 因此$f \mid h$.

(2) 由条件可知存在$u$, $v$, $p$, $q \in P[x]$, 使得$uf + vg = 1$, $fp = h$, $gq = h$. 消去$f$, $g$, 可得$(uq + vp)h = pq$. 因此$h = (uq + vp)(h/p)(h/q) = (uq + vp)fg$.

## 定义

设$f_1, f_2, \cdots, f_n \in P[x]$. 如果$d \in P[x]$满足

(1) $d$是$f_1, f_2, \cdots, f_n$的一个公因式, 即$d|f_i$, $1 \leq i \leq n$;

(2) 对于$f_1, f_2, \cdots, f_n$的任一公因式$h$, 有$h|d$,

则称$d$为$f_1, f_2, \cdots, f_n$的一个**最大公因式**.

## 命题

设$f_1, f_2, \cdots, f_k \in P[x]$不全为零($k \geq 2$), 则它们的最大公因式存在, 并有

(1) 如果$f_1, f_2, \cdots, f_{k-1}$不全为零, 则$(f_1, f_2, \cdots, f_k) = ((f_1, f_2, \cdots, f_{k-1}), f_k)$;

(2) $(f_1, f_2, \cdots, f_k)$可写为$f_1, f_2, \cdots, f_k$的一个组合;

(3) $(f_1, f_2, \cdots, f_k) = 1$的充要条件是$f_1, f_2, \cdots, f_k$有某个组合等于1.

## 证明

对$k$用数学归纳法．当$k=2$时，前面已证．
假设当$k=n$时结论成立，那么，当$k=n+1$时，
记$d_1=(f_1,f_2,\cdots,f_n)$，$d=(d_1,f_{n+1})$，则有

(1) 由于$d|d_1|f_i$，$1\leq i\leq n$，且$d|f_{n+1}$，所以$d$是$f_1$，$f_2$，$\cdots$，$f_{n+1}$的公因式．进一步，对于$f_1$，$f_2$，$\cdots$，$f_{n+1}$的任一公因式$h$，它也是$f_1$，$f_2$，$\cdots$，$f_n$的公因式，所以$h|d_1$，结合$h|f_{n+1}$可知$h|(d_1,f_{n+1})=d$．
(2) 由前面已证的结果，$d$可写为$d_1$和$f_{n+1}$的组合．又由归纳假设，$d_1$可写为$f_1$，$\cdots$，$f_n$的组合，因而$d$可写为$f_1$，$\cdots$，$f_n$，$f_{n+1}$的组合．
(3) 与$k=2$时的证法一样．

本节开始我们来证明多项式环的因式分解定理. 我们先给出不可约多项式的概念.

**定义**

设$f \in P[x]$且$\deg(f) > 0$. 如果存在$g, h \in P[x]$, 使得$f = gh$, 且$\deg(g) < \deg(f)$, $\deg(h) < \deg(f)$, 则称$f$是可约的, 否则称$f$是不可约的.

**命题**

(1) 一次多项式是不可约的;

(2) 不可约多项式的因式只有非零常数及自身的非零常数倍;

(3) 若$p, f \in P[x]$且$p$为不可约多项式, 则要么$p|f$, 要么$(p, f) = 1$;

(4) 若$p$ 是不可约多项式, 且$p|fg$, 则$p|f$或$p|g$.

## 证明

(1) 一次多项式显然不能写为两个次数小于1的多项式之积.

(2) $n$次不可约多项式没有次数$\in (0, n)$的因式, 因此它的因式一定是0次或$n$次的.

(3) 注意$(p, f)$是$p$的因式, 所以$(p, f) = 1$或$(p, f) = cp$.

(4) 如果$p$不整除$f$, 则由(3)知$(p, f) = 1$. 结合$p|fg$可得$p|g$.

**定理**

设$f \in P[x]$的次数$> 0$, 则存在首一不可约多项式$p_1, p_2, \cdots, p_s$, 使得

$$f = cp_1p_2\cdots p_s,$$

其中$c$为$f$的首项系数. 进一步, 在不计次序的意义下, 这个分解是唯一的.

**证明**

存在性: 对$\deg(f)$用数学归纳法. 如果$f$不可约, 则结论已经得证; 如果$f$可约, $f = gh$, 其中$g$, $h$的次数更小, 则由归纳假设知$g$, $h$分别能写为首一不可约多项式与非零常数的乘积, 从而结论也得证.
唯一性: 设$f = cp_1p_2\cdots p_s$是一种分解方式, $f = cq_1q_2\cdots q_t$是另一种分解方式. 由$p_1|q_1q_2\cdots q_t$可知存在某个$q_j$使得$p_1|q_j$. 然而$p_1$与$q_j$都是首一不可约多项式, 只可能$p_1 = q_j$. 等式两端消去这个相等的因式, 再对剩下的因式用同样的方法就证明了唯一性.

在多项式$f$的分解式中，通常将重复出现的不可约因式写为乘方的形式，这样我们有

$$f = cp_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},$$

其中$c$为$f$的首项系数，$p_1, p_2, \cdots, p_k$为互不相同的首一不可约多项式，$e_1, e_2, \cdots, e_k$为正整数. 称这样的式子为$f$的标准分解式.

**命题**

设$f, g$的标准分解式中出现的所有不可约因式为$p_1, p_2, \cdots, p_r$，即$f = ap_1^{i_1}\cdots p_r^{i_r}$，$g = bp_1^{j_1}\cdots p_r^{j_r}$，其中$i_1, \cdots, i_r, j_1, \cdots, j_r$为非负整数，那么

$$(f,g) = p_1^{\min(i_1,j_1)}\cdots p_r^{\min(i_r,j_r)}.$$

**定义**

设$p$, $f \in P[x]$且$p$为不可约多项式. 如果$p^k|f$, 但$p^{k+1} \nmid f$, 则称$p$为$f$的$k$重因式, 也称$p^k$恰整除$f$, 记作$p^k||f$. 特别地, 1重因式也称为单因式.

**例**

若$f = x^7 + x^6 - 3x^5 - 3x^4 + 3x^3 + 3x^2 - x - 1$, 则$x+1$是$f$的4重因式, $x-1$是$f$的3重因式.

如果能把$f$分解因式, 则可直接看出它的重因式以及相应的重数. 但这一般是做不到的, 实践中通常借助导数来进行判断.

### 定义

对于$P[x]$中的多项式$f=\sum_{k=0}^{n}a_kx^k$，称多项式$\sum_{k=1}^{n}ka_kx^{k-1}$为$f$的导数或形式微商，记作$f'$.

### 导数的性质

(1) 当$\deg(f)\geq 1$时，$\deg(f')=\deg(f)-1$;
(2) $f'=0$的充要条件是$f$为常数;
(3) $(f+g)'=f'+g'$;
(4) $(c\cdot f)'=c\cdot f'$, $\forall c\in P$;
(5) $(fg)'=f'g+fg'$;
(6) $(f^m)'=mf^{m-1}f'$;
(7) 当$p$为不可约多项式时，$(p,p')=1$.

**定理**

设不可约多项式$p$是$f$的因式. 那么, $p$是$f$的$k$重因式, 当且仅当$p$是$f'$的$k-1$重因式.

**证明**

先证$p^k || f \Longrightarrow p^{k-1} || f'$. 事实上, 若$f = p^k g$, 其中$p \nmid g$, 那么

$$f' = kp^{k-1}p'g + p^k g' = p^{k-1} \cdot (kp'g + pg'),$$

利用$(p, p') = 1$及$(p, g) = 1$即可说明$p \nmid kp'g + pg'$, 因此$p^{k-1} || f'$.
再证$p^{k-1} || f' \Longrightarrow p^k || f$. 事实上, 设$p$是$f$ 的$m$重因式, 则由前面的证明可知$p$是$f'$的$m-1$重因式, 与当前的条件比较就得到$m = k$.

我们把$f$的二阶导数记作$f''$, $k$阶导数记作$f^{(k)}$.

## 重因式判别法

设$p$, $f \in P[x]$且$p$为不可约多项式. 那么, $p$是$f$的$k$重因式, 当且仅当$p$是$f$, $f'$, $\cdots$, $f^{(k-1)}$的因式, 但不是$f^{(k)}$ 的因式.

## 推论1

不可约多项式$p$是$f$的$(\geq 2)$重因式, 当且仅当$p$ 是$f$, $f'$的公因式, 即$p|(f, f')$.

## 推论2

设$f \in P[x]$且$\deg(f) > 0$. 那么, $f$无重因式的充要条件是$(f, f') = 1$.

**命题**

设$f \in P[x]$且$\deg(f) > 0$. 令$g = f/(f, f')$, 则$g$与$f$的不可约因式相同, 但$g$无重因式.

**证明**

设$f$的标准分解式为

$$f = cp_1^{e_1} \cdots p_s^{e_s},$$

其中$p_1, \cdots, p_s$为首一不可约多项式, $e_1, \cdots, e_s$为正整数.
由于$(f, f')$是$f$的因式, 所以它一定形如$p_1^{i_1} \cdots p_s^{i_s}$. 由前述定理可知$i_1 = e_1 - 1, \cdots, i_s = e_s - 1$. 这样我们就得到

$$g = f/(f, f') = cp_1 \cdots p_s.$$

从而命题得证.

**定义**

设$f\in P[x]$. 如果$\alpha\in P$满足$f(\alpha)=0$, 则称$\alpha$为$f$的一个零点或根.

作为余数定理的推论, 我们有

**因式定理**

$\alpha$是$f\in P[x]$的根, 当且仅当$(x-\alpha)$是$f$的因式.

**例**

设$f=x^3-3x+2$, 由于$f(1)=0$, 所以$(x-1)$是$f$的因式.

**思考题**

若$f(x)$是$\mathbb{Q}[x]$中的不可约多项式, $\alpha$是它的一个复数根. 证明$\mathbb{Q}(\alpha)=\{g(\alpha)\,|\,g(x)\in\mathbb{Q}[x]\}$ 是一个数域.

**定义**

若$x-\alpha$是$f$的$k$重因式, 则称$\alpha$为$f$的$k$重根. 1重根也称为单根.

利用重因式判别法, 我们有

**重根判别法**

$\alpha$是$f$的$k$重根, 当且仅当

$$f(\alpha)=f'(\alpha)=\cdots=f^{(k-1)}(\alpha)=0, \quad f^{(k)}(\alpha)\neq 0.$$

**定理**

$P[x]$中$n\geq 0$次多项式至多有$n$个根, 其中$k$重根算$k$个根.

**证明**

对$n$用数学归纳法. $n=0$时结论是显然的. 假设$m-1$次多项式至多有$m-1$个根, 那么, 对于$m$次多项式$f$, 如果它有根$\alpha$, 则有一次因式$(x-\alpha)$, 从而有$m-1$次多项式$g$使得$f=(x-\alpha)\cdot g$. 由归纳假设知$g$至多有$m-1$个根, 从而$f$至多有$m$个根.

上述定理的一个有用推论是: $n$次多项式由它在$n+1$个点的值唯一决定.

**推论**

若$f,\ g\in P[x]$且它们的次数$\leq n$, 如果它们在$n+1$个不同的数$c_0$, $c_1,\cdots,c_n\in P$处的值都对应相等, 即$f(c_i)=g(c_i)$, $0\leq i\leq n$, 那么$f=g$.

**证明**

令$h=f-g$. 如果$h\neq 0$, 则$h$的根的个数$\leq\deg(h)\leq n$. 然而由条件知$h(c_i)=0$, $0\leq i\leq n$, 即$h$至少有$n+1$个根, 矛盾.

### 定理

设$f\in\mathbb{C}[x]$的次数大于0, 则$f$一定有复数根.

### 证明

不妨设$f$的首项系数为1且常数项不为零, 即

$$f=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_0\neq 0.$$

易知映射$f:\mathbb{C}\to\mathbb{C}$是连续的. 考虑以原点0为圆心, $r$为半径的圆, 它在映射$f$下的像是一条闭曲线, 记作$\Gamma_r$. 易知$\Gamma_r$随着$r$连续变化. 当$r\to 0$时, $\Gamma_r\to$点$a_0$, 这时原点0在$\Gamma_r$的外部. 下面的引理说明, 当$R$足够大时, 原点0在$\Gamma_R$的内部. 这样, 一定存在某个$r$, 使得$\Gamma_r$经过原点, 从而定理得证.

## 引理

设$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$且$a_0 \neq 0$.
记$R = 1 + |a_{n-1}| + \cdots + |a_1| + |a_0|$, 则当复数$\xi$满足$|\xi| = R$时,
有$|f(\xi) - \xi^n| < R^n$.

## 证明

注意$R > 1$, 我们有

$$
\begin{aligned}
|f(\xi) - \xi^n| &= |a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0| \\
&\leq |a_{n-1}\xi^{n-1}| + \cdots + |a_1\xi| + |a_0| \\
&= |a_{n-1}|R^{n-1} + \cdots + |a_1|R + |a_0| \\
&< |a_{n-1}|R^{n-1} + \cdots + |a_1|R^{n-1} + |a_0|R^{n-1} < R^n.
\end{aligned}
$$

引理的直观意义: 想象在0处有一棵树, $\xi^n$是一个人, $f(\xi)$ 是一个宠物. 人绕着树转圈(注意人到树的距离为$R^n$), 宠物在人附近运动, 且它到人的距离比人绕圈的半径要小. 这样, $f(\xi)$的轨迹$\Gamma_R$一定把原点0包含在内部.

**推论**

若$f \in \mathbb{C}[x]$的次数为$n \geq 0$, 则$f$恰有$n$个根( 重根按重数计).

利用因式定理, 可将上述结论重新叙述为

**复系数多项式的因式分解定理**

若$f \in \mathbb{C}[x]$的次数为$n > 0$, 则$f$可分解为$n$个一次因式的乘积, 即有分解

$$f = c \cdot (x - \alpha_1)^{r_1} \cdots (x - \alpha_s)^{r_s},$$

其中$\alpha_1, \cdots, \alpha_s$互不相同.

**推论**

$\mathbb{C}[x]$中的不可约多项式只有一次多项式.

下面讨论实系数多项式的因式分解.

**定理**

设$f \in \mathbb{R}[x]$且$\deg(f) > 0$. 若把$f$看作$\mathbb{C}[x]$ 中多项式时, $\alpha \in \mathbb{C}$是$f$的$k$重根, 那么, $\bar{\alpha}$也是$f$的$k$重根.

**证明**

$\alpha$是$f$的$k$重根, 则$f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0$, $f^{(k)}(\alpha) \neq 0$. 取共轭就得到$f(\bar{\alpha}) = f'(\bar{\alpha}) = \cdots = f^{(k-1)}(\bar{\alpha}) = 0$, $f^{(k)}(\bar{\alpha}) \neq 0$. 因此$\bar{\alpha}$也是$f$的$k$重根.

**定理**

若$f\in\mathbb{R}[x]$且$\deg(f)>0$, 则$f$有分解

$$f=c\cdot(x-\alpha_1)^{l_1}\cdots(x-\alpha_s)^{l_s}(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_rx+q_r)^{k_r},$$

其中$c$为首项系数, $\alpha_1,\cdots,\alpha_s\in\mathbb{R}$互不相同, $(p_1,q_1),\cdots,(p_r,q_r)$互不相同且$p_i^2-4q_i<0$, $1\le i\le r$.

**证明**

对$\deg(f)$用数学归纳法. 任取$f$的一个复数根$\alpha$. 如果$\alpha$ 为实数, 则$f$有一次因式$(x-\alpha)$; 如果$\alpha$为虚数, 则由虚根成对定理, $\bar{\alpha}$也是一个根, 这时$f$有二次因式$(x-\alpha)(x-\bar{\alpha})$.

现在着手讨论有理系数多项式. 对每个有理系数多项式$f$, 只要取各个系数的分母的最小公倍数$c$, 则$cf$是一个整系数多项式, 再取$cf$的各项系数的最大公约数$d$, 则$\frac{c}{d}f$的各项系数互素.

**定义**

若$f \in \mathbb{Z}[x]$的各项系数互素, 则称$f$为本原多项式.

**引理**

设$f \in \mathbb{Q}[x]$, 则存在唯一的正有理数$r$和本原多项式$g$, 使得$f = r \cdot g$.

**证明**

存在性已证. 现在证明唯一性. 若有另一正有理数$\tilde{r}$和本原多项式$\tilde{g}$使得$f = r \cdot g = \tilde{r} \cdot \tilde{g}$, 设$r = d/c$, $\tilde{r} = \tilde{d}/\tilde{c}$, 则有$d\tilde{c} \cdot g = \tilde{d}c \cdot \tilde{g}$. 注意左端多项式各项系数的最大公约数为$d\tilde{c}$, 右端各项系数的最大公约数为$\tilde{d}c$, 所以$d\tilde{c} = \tilde{d}c$, 即$r = \tilde{r}$.

## Gauss 引理

本原多项式的积仍是本原的.

## 证明

设$f = \sum a_i x^i$和$g = \sum b_j x^j$是本原多项式, 则

$$fg = \sum c_k x^k, \quad c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k.$$

若$fg$不是本原多项式, 则存在素数$p | c_0, c_1, c_2, \cdots$.
设$a_0, a_1, \cdots$中, 第一个不被$p$整除的是$a_r$; 在$b_0, b_1, \cdots$中, 第一个不被$p$整除的是$b_s$. 那么,

$$c_{r+s} = (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0)$$

不被$p$整除, 矛盾.

**定理**

设$f \in \mathbb{Q}[x]$可写为$r \cdot g$, 其中$r \in \mathbb{Q}^+$, $g$为本原多项式. 那么, $f$在$\mathbb{Q}[x]$中是可约的, 当且仅当$g$在$\mathbb{Z}[x]$中可分解.

**证明**

设$f = f_1 f_2$, 其中$f_i \in \mathbb{Q}[x]$. 设$f_i = r_i \cdot g_i$, 其中$r_i$为正有理数, $g_i$为本原多项式. 那么$f = (r_1 r_2) \cdot (g_1 g_2)$, 其中$r_1 r_2$为正有理数, $g_1 g_2$为本原多项式. 由唯一性可知$r = r_1 r_2$, $g = g_1 g_2$.

这个结论告诉我们, 要判断一个有理系数多项式是否可约, 只要看相应的本原多项式是否可分解就可以了.

为了判断一个整系数多项式是否可分解，我们先看它是否有一次因式，即是否有有理根.

**命题**

设$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$，$a_n \neq 0$. 如果$p/q$是$f$的有理根(其中$p$，$q$为互素的整数且$pq \neq 0$)，则$p|a_0$，$q|a_n$.

**证明**

由$f(p/q) = 0$可得

$$\begin{aligned} & a_n p^n/q^n + \cdots + a_1 p/q + a_0 = 0 \\ \Longrightarrow & a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n = 0. \end{aligned}$$

由此可知$p|a_0 q^n$，$q|a_n p^n$. 由于$p$，$q$互素，所以$p|a_0$，$q|a_n$.

**例1**

求$4x^4-4x^3+5x^2-8x-6$的有理根.

**解答**

上述多项式的有理根$\in\{\pm 6,\pm 3,\pm 2,\pm 1,\pm 3/2,\pm 1/2,\pm 3/4,\pm 1/4\}$. 逐个检验知只有$-1/2$, $3/2$是根.

**例2**

设$k\in\mathbb{Z}$, 判断$x^3+kx+1$在$\mathbb{Q}[x]$中是否可约.

**解答**

这个3次多项式若可约, 则有1次因式, 从而有有理根. 根据有理根的判别法, 上述多项式的有理根只能是$\pm 1$. 相应$k=0$或$-2$. 其他情形该多项式不可约.

如果没有一次因式, 就需要考虑其他的辅助手段, 例如取一个素数$p$, 考虑在模$p$ 意义下的分解. 如果$f$在$\mathbb{Z}[x]$中可分解, 则它在模$p$的意义下也可以分解; 如果$f$在模$p$的意义下不能分解, 则它在$\mathbb{Z}[x]$中不能分解, 从而是不可约的.

**定义**

设$p$为素数, $f \in \mathbb{Z}[x]$且$\deg(f) > 0$. 如果$f$在模$p$意义下可分解为两个次数$< \deg(f)$的多项式的乘积, 则称$f$在$\mathbb{Z}_p[x]$中可分解, 否则称$f$在$\mathbb{Z}_p[x]$中不可分解.

**例1**

作为整系数多项式, $x^3 - 3x - 4$没有有理根, 所以没有一次因式, 因而不可分解. 但在模3的意义下, 它可以分解为$(x-1)(x^2+x+1)$; 在模7的意义下, 它可以分解为$(x-3)(x^2+3x-1)$.

### 例2

证明$f=x^4+x^2+x-1$在$\mathbb{Z}[x]$中不可分解, 因而是$\mathbb{Q}[x]$中的不可约多项式.

### 解答

首先容易看出, $f$没有有理根, 因而它没有1次因式.
为了证明$f$没有2次因式, 我们考虑模3. 在模3的意义下, 2次的首一不可约多项式只有$x^2+1$, $x^2+x-1$和$x^2-x-1$, 它们都不整除$f$, 所以$f$在模3的意义下没有2次因式, 因而它在$\mathbb{Z}[x]$中也没有2次因式.

### 思考题

- (***) 证明对任意素数$p$, 多项式$x^4+1$在模$p$的意义下可分解, 但它在$\mathbb{Z}[x]$中不可分解.
- (***) 证明对任意素数$p$, 多项式$x^8-16$在模$p$的意义下有根(即存在整数$t$使得$t^8-16\equiv 0 \pmod p$), 但它没有有理根.
- (****) 在$\mathbb{Z}_p[x]$中, 首项系数为1的$n$次不可约多项式有多少个?

类似于$P[x]$中多项式的因式分解，我们可证明(关键在于，$\mathbb{Z}_p$是一个域，它与数域是类似的).

**唯一分解定理**

设$f \in \mathbb{Z}[x]$的次数$> 0$，且首项系数$c$不被$p$整除．那么，$f$在$\mathbb{Z}_p[x]$中可分解为$c \cdot q_1 \cdots q_s$，其中$q_1, \cdots, q_s$是$\mathbb{Z}_p[x]$中的首一不可约多项式．进一步，在不计次序的意义下，这个分解是唯一的．

**Eisenstein判别法**

设$p$为素数，$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$．如果$p \nmid a_n$，$p | a_{n-1}, \cdots, p | a_1$，$p | a_0$，但$p^2 \nmid a_0$，则$f$在$\mathbb{Z}[x]$中不可分解．

**证明**

如果$f$能分解为两个次数$< n$的多项式$g$和$h$的乘积，则在模$p$的意义下它也能分解．在模$p$的意义下，$f \equiv a_n x^n$，由唯一分解定理可知，一定有$g \equiv b_k x^k$，$h \equiv c_m x^m$．因此$g$和$h$的常数项都模$p$余0，这就与$p^2 \nmid a_0$矛盾．

**例**

设$p$为素数，证明：$x^{p-1} + x^{p-2} + \cdots + x + 1$在$\mathbb{Q}[x]$中不可约．

**证明**

将$x$替换为$y+1$．则原多项式变为$(x^p - 1)/(x - 1) = ((y+1)^p - 1)/y = y^{p-1} + C_p^1 y^{p-2} + C_p^2 y^{p-3} + \cdots + C_p^{p-1}$．
由Eisenstein判别法知，这个多项式在$\mathbb{Q}[x]$中不可约．