一元多项式的无平方部分

设 F 是域，$f \in F[x]$ 的次数为正，则在 F 上两两互不相伴的不可约多项式 $p_1, \cdots, p_k \in F[x] \setminus F$ 和唯一的 $m_1, \cdots, m_k \in \mathbb{Z}^+$ 使得

$$f = p_1^{m_1} \cdots p_k^{m_k}. \tag{1}$$

（$F[x]$ 是 UFD + 注解 3.12（f 的一个标准不可约分解）

上述 p_i 称为 f 的 m_i 重因子，$i=1,2,\cdots,k$. 特别地，当 $m_i=1$ 时，p_i 称为单因子. 因子 $p_1 p_2 \cdots p_k$ 称为 f 的无平方部分，当 f 的不可约因子都是单因子时，f 称为无平方的.

计算无平方部分

设 $f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0 \in F[x]$. 定义 f 关于 x 的导数是

$$f' = n f_n x^{n-1} + (n-1) f_{n-1} x^{n-2} + \cdots + f_1$$

可验证：对 $\forall f, g \in F[x]$，

① $(f+g)' = f' + g'$

② $(fg)' = f'g + fg'$

验证第②条，$\forall f, g \in F[x]$，设 $n = \max(\deg(f), \deg(g))$，

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0.$$

$$g = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_1 x + g_0.$$

（对于未出现幂次的系数全为 0）

$$(f \cdot g)' = \left[\left(\sum_{i=0}^{n} f_i x^i\right) \cdot \left(\sum_{j=0}^{n} g_j x^j\right)\right]' = \left(\sum_{k=0}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} f_i g_j\right) x^k\right)' = \sum_{k=1}^{2n} \left(k \sum_{\substack{i+j=k \\ 0 \le i,j \le n}} f_i g_j\right) x^{k-1}$$

$$= \sum_{k=1}^{2n} \left((i+j) \sum_{\substack{i+j=k \\ 0 \le i,j \le n}} f_i g_j\right) x^{i+j-1} = \sum_{k=1}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} i f_i g_j\right) x^{i+j-1} + \sum_{k=1}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} j f_i g_j\right) x^{i+j-1}$$

$$= \sum_{k=1}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} i f_i x^{i-1} \cdot g_j x^j\right) + \sum_{k=1}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} j g_j x^{j-1} \cdot f_i x^i\right)$$

$$= f'g + fg'.$$

定理 设 F 是特征为 0 的域，$f \in F[x] \setminus F$，则 f 的无平方部分在 F 上与 $f / \gcd(f, f')$ 相伴.

pf：由(1)可知，

$$f' = m_1 p_1^{m_1-1} p_1' \cdots p_k^{m_k} + \cdots + m_k p_1^{m_1} \cdots p_k^{m_k-1} p_k'$$

$$= \sum_{i=1}^{k} m_i \left(p_1^{m_1} \cdots p_{i-1}^{m_{i-1}} p_i^{m_i-1} p_i' p_{i+1}^{m_{i+1}} \cdots p_k^{m_k}\right)$$

$$= \underbrace{\left(p_1^{m_1-1} \cdots p_k^{m_k-1}\right)}_{g} \cdot \underbrace{\sum_{i=1}^{k} m_i \left(p_1 \cdots p_{i-1} p_i' p_{i+1} \cdots p_k\right)}_{h}$$

于是 g 是 f 和 f' 的公因子，

下面证 $\gcd(f, h) = 1$

假设该结论不成立，则存在 $i \in \{1, \cdots, k\}$，使得 $p_i \mid h$. 不妨设 $p_1 \mid h$.

$$\Rightarrow p_1 \mid m_1 (p_1' p_2 \cdots p_k).$$

由于 $\gcd(p_1, p_i) = 1$，$i = 2, \cdots, k$. 且 m_1 在特征为 0 的域中非零，所有 $p_1 \mid p_1'$

$\Rightarrow \deg(P_i) \le \deg(P_i')$ $\rightarrow\leftarrow$

$\Rightarrow \gcd(f,h)=1$, i.e. $\gcd(f,f')=g$

$\Rightarrow \dfrac{f}{\gcd(f,f')} = P_1\cdots P_m$.

推论 设 F 是特征为0的域，$f\in F[x]\setminus F$，则 f 是无平方因式当且仅当 $\gcd(f,f')=1$

Pf: "$\Rightarrow$" 若 f 无平方，则 $m_1=\cdots=m_k=1$，于是 $\gcd(f,f')=P_1^{m_1-1}\cdots P_k^{m_k-1}=1$

"$\Leftarrow$" 若 $\gcd(f,f')=1$，则由上述定理知 f 与它的无平方部分在 F 上相伴，于是 f 是无平方的.

例 计算 $\mathbb{Z}[x]$ 中多项式 $f=x^3-x^2-x+1$ 的无平方部分

解: $f=x^3-x^2-x+1$, $f'=3x^2-2x-1$ $\Rightarrow \gcd(f,f')=x-1$.

$$
\begin{array}{r|l|l|l}
 & 3x^2-2x-1 & x^3-x^2-x+1 & \frac{x}{3}-\frac{1}{9} \\
-\frac{27}{8}x-\frac{9}{8} & 3x^2-3x & x^3-\frac{3}{3}x^2-\frac{x}{3} & \\
\hline
 & x-1 & -\frac{x^2}{3}-\frac{2}{3}x+1 & \\
 & x-1 & -\frac{x^2}{3}+\frac{2}{9}x+\frac{1}{9} & \\
\hline
 & 0 & -\frac{8}{9}x+\frac{8}{9} &
\end{array}
$$

$\dfrac{f}{\gcd(f,f')} = x^2-1$.

例 设 F 是分式域 $\mathbb{Z}_2$，令 $P=x^2$，则 $P'=\bar{2}x=\bar{0}$，$\gcd(P,P')=P$. 但 P 的无平方部分显然不可能是.

例 设 $f=x^n+a\in\mathbb{Q}[x]$，其中 $n>1$，$a\in\mathbb{Q}$. 证明 f 是无平方因式当且仅当 $a\neq 0$.

Pf: $f'=nx^{n-1}$. 注意到

$$f+\frac{-x}{n}f'=a, \text{ i.e. } \frac{f}{a}+\frac{-x}{na}f'=1 \quad (a\neq 0)$$

当 $a\neq 0$ 时，由 Bezout 关系可知，$\gcd(f,f')=1$，于是 f 是无平方因式，反之，设 f 是无平方因式.

因为 $n>1$，所以 x^n 不是无平方因式，于是 $a\neq 0$.

无平方分解

定义 $f\in F[x]\setminus F$，f 的无平方分解表示为

$$f=P_1P_2^2\cdots P_k^k$$

其中 $P_1,\cdots,P_k$ 都是无平方多项式（可能某些 P_i 为1）而且两两互素

记 $f_0=f$, $f_1=\gcd(f,f')=P_2P_3^2\cdots P_k^{k-1}$

$$h_1=\frac{f_0}{f_1}=P_1P_2\cdots P_k.$$

$f_2=\gcd(f_1,f_1')=P_3P_4^2\cdots P_k^{k-2}$

$h_2 = \frac{f_1}{f_2} = \frac{P_2 P_3^2 \cdots P_k^{k-1}}{P_3 P_4^2 \cdots P_k^{k-2}} = P_2 P_3 P_4 \cdots P_k$

$\frac{h_1}{h_2} = \frac{P_1 P_2 \cdots P_k}{P_2 P_3 \cdots P_k} = P_1$

.....

$f_{k-2} = P_{k-1} P_k^2$

$f_{k-1} = gcd(f_{k-2}, f_{k-2}') = P_k$

$h_{k-1} = \frac{f_{k-2}}{f_{k-1}} = P_{k-1} P_k$

$f_k = gcd(f_{k-1}, f_{k-1}') = 1$

$h_k = \frac{f_{k-1}}{f_k} = f_{k-1} = P_k$

$\frac{h_{k-1}}{h_k} = P_{k-1}$

无平方分解算法

输入: $f \in F[x]$

输出: $P_1, \cdots, P_k$, 无平方多项式且两两互素

1. [初始化] 令 $g_1 := gcd(f, f')$;
   $h_1 := \frac{f}{g_1}$;
   $i := 1$;
2. [下循环] while $g_i \neq 1$ do
   $g_{i+1} := gcd(g_i, g_i')$;
   $h_{i+1} := \frac{g_i}{g_{i+1}}$;
   $P_i := \frac{h_i}{h_{i+1}}$;
   $i := i+1$;
   end do;
3. [处理最后一个因子] $k := i$; $P_k := h_k$;
4. [返回] return $P_1, \cdots, P_k$;

例 $f = x^3 - x^2 - x + 1$ 在 $Q[x]$ 中的无平方分解.

解: $f_0 = f$, $f' = 3x^2 - 2x - 1$

$g_1 = gcd(f, f') = x - 1$

$h_1 = \frac{f}{g_1} = x^2 - 1$

$i = 1$

$g_2 = gcd(g_1, g_1') = 1$

$h_2 = \frac{g_1}{g_2} = x - 1$

$P_1 = \frac{h_1}{h_2} = \frac{x^2-1}{x-1} = x + 1$

$i = 2$

$k = 2$, $P_2 = h_2 = x - 1$

$\Rightarrow f = (x+1)(x-1)^2$.

回忆. 设 p 为素数, $\forall a \in \mathbb{Z}$, 有 $a^p \equiv a \bmod p$. (Fermat 小定理)

$\forall a, b \in \mathbb{Z}$, 有 $(a+b)^p \equiv a^p + b^p \bmod p$. (Freshmen's dream)

定理 如果 $\mathbb{Z}_p[x]$ 中的多项式 $f = a_0 + a_1 x + \cdots + a_m x^m$ 满足 $f' = 0$ 当且仅当存在 $g \in \mathbb{Z}_p[x]$ 使得 $f = g^p$.

Pf: $\Rightarrow$ 因为 $f' = a_1 + 2a_2 x + \cdots + m a_m x^{m-1} = 0$, 所以 $a_i \neq 0 \Rightarrow p \mid i$

$\Rightarrow f = a_{i_1} x^{j_1 p} + \cdots + a_{i_l} x^{j_l p}$, 其中 $a_{i_1}, \cdots, a_{i_l} \in \mathbb{Z}_p^*$ 且 $i_1 = j_1 p, \cdots, i_l = j_l p$.

$\Rightarrow f = (a_{i_1} x^{j_1})^p + \cdots + (a_{i_l} x^{j_l})^p$

令 $g = a_{i_1} x^{j_1} + \cdots + a_{i_l} x^{j_l}$, 则 $f = g^p$ (Freshmen's dream).

"⇐" $f=g^p$, $f'=pg^{p-1}g'=0$.

考虑 $\mathbb{Z}_p[x]$ 中的无平方因子解，设 $f\in\mathbb{Z}_p[x]$ 的无平方因子分解为

$$f=P_1P_2^2\cdots P_k^k.$$

如果 $f'\neq 0$，那么使用特征为0的情况下的方法可以得到 f 的所有 P_i 的因子 g_i，

如果 $f'=0$ 或对 P_i 的非平凡因子 g_i，我们可以利用上述思想将问题化为求更低次多项式的无平方因子分解.

例 求 $f=x^3-x^2-x+1\in\mathbb{Z}_2[x]$ 的无平方分解

$f_0=f$, $f'=3x^2-2x-1=x^2-1$

$g_1=\gcd(f,f')=\gcd(x^3-x^2-x+1,\ x^2-1)=x^2-1$

$h_1=\frac{f}{g_1}=\frac{x^3-x^2-x+1}{x^2-1}=x+1$.

对于 g_1, $g_1'=2x=0$.

$\Rightarrow g_1=(x-1)^2$.

$\Rightarrow f=h_1g_1=(x+1)(x-1)^2=(x-1)^3$.

中国剩余定理

整数版本

引理 设 $m_1,\cdots,m_k\in\mathbb{Z}^+\setminus\{1\}$ 两两互素，则

(i) $m_1\cdots m_{k-1}$ 与 m_k 互素

(ii) $\operatorname{lcm}(m_1,\cdots,m_k)=m_1\cdots m_k$.

Pf: (i) 因为 $\forall i\in\{1,\cdots,k-1\}$, $\gcd(m_i,m_k)=1$，所以 $\exists\, u_i,v_i\in\mathbb{Z}$, s.t.

$$u_im_i+v_im_k=1.$$

于是

$$1=\prod_{i=1}^{k-1}(u_im_i+v_im_k)=u(m_1\cdots m_{k-1})+vm_k,$$

其中 $u=u_1\cdots u_{k-1}$ 且 v 是整数. 从而 $m_1\cdots m_{k-1}$ 与 m_k 互素.

(ii) 对 k 归纳. 当 $k=2$ 时, $\operatorname{lcm}(m_1,m_2)=\dfrac{m_1m_2}{\gcd(m_1,m_2)}=m_1m_2$ (第五周讲义命题7.18)

假设 $k-1$ 时结论成立，令

$$l=\operatorname{lcm}(m_1,m_2,\cdots,m_k)$$

则 l 是 $m_1,\cdots,m_{k-1}$ 的公倍式，由归纳假设知 $\operatorname{lcm}(m_1,\cdots,m_{k-1})=m_1\cdots m_{k-1}\mid l$,

又因为 $m_k\mid l$，于是

$$\operatorname{lcm}(m_1\cdots m_{k-1},m_k)\mid l$$

由(i)可知, $\gcd(m_1\cdots m_{k-1},m_k)=1$. 从而

$$\operatorname{lcm}(m_1\cdots m_{k-1},m_k)=m_1\cdots m_{k-1}m_k\mid l.$$

显然 $m_1m_2\cdots m_k$ 是 $m_1,m_2,\cdots,m_k$ 的公倍式，从而 $l\mid m_1\cdots m_{k-1}m_k$. 故 $l=m_1\cdots m_k$.

定理 设 $m_1,\cdots,m_k\in\mathbb{Z}^+\setminus\{1\}$，两两互素，$r_1,\cdots,r_k\in\mathbb{Z}$. 则存在唯一的 $r\in\mathbb{N}$ 满足

$$\begin{cases} r\equiv r_1 \mod m_1\\ r\equiv r_2 \mod m_2\\ \quad\vdots\\ r\equiv r_k \mod m_k\end{cases}\qquad (*)$$

且 $r<m_1\cdots m_k$.

证明:(存在性) 对 k 归纳. 当 $k=1$ 时, 取 $r=\operatorname{rem}(r_1,m_1)$ 即可.

设 x' 满足 $x'\equiv r_1 \mod m_1,\ \cdots,\ x'\equiv r_{k-1}\mod m_{k-1}$.

由引理知, $\exists\, u,v\in\mathbb{Z}$, 使得

$$u(m_1\cdots m_{k-1})+vm_k=1\qquad (**)$$

令 $\boxed{x=x'+u(m_1\cdots m_{k-1})(r_k-x')}$

则 $x\equiv r_i \mod m_i$, $i=1,2,\cdots,k-1$

由(**)可知, $x=x'+(1-vm_k)(r_k-x')=r_k-vm_k(r_k-x')$.

$$\Rightarrow\quad x\equiv r_k \mod m_k$$

再令 $r=\operatorname{rem}(x,m_1\cdots m_k)$, 则 $0\le r<m_1\cdots m_{k-1}m_k$ 且 r 满足定理中的同余关系. 我们证明了存在性

(唯一性) 设 $\tilde{r}$ 也满足定理中同余关系且 $0 \le \tilde{r} < m_1 \cdots m_{k-1} m_k$. 不妨设 $r \ge \tilde{r}$, 则 $r - \tilde{r} \equiv 0 \bmod m_i$, $i = 1, \cdots, k-1, k$. 于是, $r - \tilde{r}$ 是 $m_1, \cdots, m_{k-1}, m_k$ 的公倍式且 $0 \le r - \tilde{r} < m_1 \cdots m_{k-1} m_k$.

由引理(ii)可知 $r = \tilde{r}$.

例 有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二. 问物几何.

解: 求解同余方程组
$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

$m_1 = 3$. $m_2 = 5$. $m_3 = 7$. $r_1 = 2$, $r_2 = 3$, $r_3 = 2$

$x_1 = r_1 = 2$. $2 \cdot 3 - 5 = 1$. $u_1 = 2$.

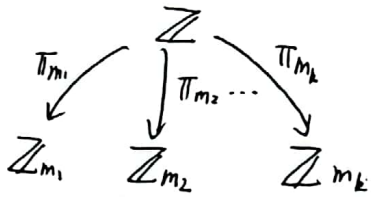
$x_2 = r_1 + u_1 m_1 (r_2 - x_1) = 2 + 2 \cdot 3 \cdot (3-2) = 8$

$1 \cdot (3 \cdot 5) - 2 \cdot 7 = 1$, $u_2 = 1$

$x_3 = x_2 + u_2 \cdot (m_1 \cdot m_2)(r_3 - x_2) = 8 + 1 \cdot (3 \cdot 5)(2 - 8) = 8 - 90 = -82$

$r = \text{rem}(-82, 105) = 23$

环同态的观点.



当 $m_1, m_2, \cdots, m_k$ 互素时, $\forall \bar{r}_1 \in \mathbb{Z}_{m_1}, \cdots, \bar{r}_k \in \mathbb{Z}_{m_k}$, $\exists x \in \mathbb{Z}$ 是 $\bar{r}_1 \in \mathbb{Z}_{m_1}, \cdots, \bar{r}_k \in \mathbb{Z}_{m_k}$ 关于自然投影 $\pi_{m_1}, \cdots, \pi_{m_k}$ 的公共原像.

多项式版本.

定义同余关系: 设 F 是域, $p \in F[x] \setminus F$, 设 $a, b \in F[x]$, 如果 $p \mid a - b$, 则称 a 和 b 关于 p 同余, 记为 $a \equiv b \bmod p$.

引理 设 $f_1, \cdots, f_k \in F[x]^*$, 两两互素.

(i) $f_1 \cdots f_{k-1}$ 和 f_k 互素

(ii) $\text{lcm}(f_1, \cdots, f_{k-1}, f_k) = f_1 \cdots f_{k-1} f_k$.

定理 设 $f_1, \cdots, f_k \in F[x] \setminus F$, 两两互素, $r_1, \cdots, r_k \in F[x]$, 则存在唯一的 $r \in F[x]$ 满足
$$\begin{cases} r \equiv r_1 \bmod f_1 \\ \quad \vdots \\ r \equiv r_k \bmod f_k \end{cases}$$
且 $\deg(r) < \deg(f_1) + \cdots + \deg(f_k)$.