何适
hashi2020@amss.ac.cn

# §1. 一元多项式的无平方部分.

$F$ 域. $F[X]$ 为主理想整环.

回忆: $F[X]$ 为 UFD. i.e.

$\forall f \in F[X]$, $\exists p_1, \cdots, p_k \in F[X]$ 不可约, $m_1, \cdots, m_k \in \mathbb{N}^+$

s.t. $f = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$, 且这个分解是"唯一"的.

$f = p_1^{m_1} \cdots p_k^{m_k} = q_1^{n_1} \cdots q_l^{n_l}$

$\Rightarrow k = l$, 对应项有 $q_i = u_i p_i$, $u_i$ 为可逆单位.

定义: 若 $f \in F[X]$, $f = p_1^{m_1} \cdots p_k^{m_k}$ 如上. 因子 $p_1 \cdots p_k$ 称为 $f$ 的无平方部分. 简记为 SFP (square free part). 称 $f$ 是无平方的若 $m_1 = \cdots = m_k = 1$.

目标: 若 $\mathrm{char} F = 0$, 我们给出方法计算其 SFP.

定义: (Formal derivative) $\forall f \in F[X]$, $f = a_n x^n + \cdots + a_1 x + a_0$, 其形式导数 $f'$ 为 $f' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$.

性质: $(f+g)' = f' + g'$, $(f \cdot g)' = f'g + f \cdot g'$ 莱布尼兹法则.

命题: 若 $\mathrm{char} F = 0$, $f \in F[X] \setminus F$, 则其 SFP 为 $\dfrac{f}{\gcd(f, f')}$.

证明:

$f = p_1^{m_1} \cdots p_k^{m_k}$,

SFP 应该为: $p_1 \cdots p_k$

若 $p_1 \cdot p_2 \cdots p_k$ 是无平方部分, 则 $u p_1 \cdot p_2 \cdots p_k$ 也是无平方部分. 对于某些 $u \in F[X]^\times$

欲证此命题: $\gcd(f, f') = u p_1^{m_1 - 1} \cdots p_k^{m_k - 1}$

$$f' = \sum_{i=1}^{k} m_i p_1^{m_1} \cdots p_i^{m_i - 1} \cdot p_i' \cdots p_k^{m_k}$$

$$= p_1^{m_1 - 1} \cdots p_k^{m_k - 1} \left( \sum_{i=1}^{k} m_i p_1 \cdots p_i' \cdots p_k \right) \quad h.$$

$p_1^{m_1 - 1} \cdots p_k^{m_k - 1} \mid f'$, $p_1^{m_1 - 1} \cdots p_k^{m_k - 1} \mid f$

$\Rightarrow p_1^{m_1 - 1} \cdots p_k^{m_k - 1} \mid \gcd(f, f')$

下证 $\gcd(f,f') \mid p_1^{m_1-1}\cdots p_k^{m_k-1}$

证明 $\gcd(f,h)=1$ 即可. $f'=h\cdot p_1^{m_1-1}\cdots p_k^{m_k-1}$

$\gcd(f,h)=1 \Longrightarrow \gcd(f,f') \mid p_1^{m_1-1}\cdots p_k^{m_k-1}$

↑ 因式分解唯一性.

若 $\gcd(f,h)\neq 1$. 则 $\exists p_i$ 为 $f$ 的因子 $p_i \mid h$

$h=\sum_{j=1}^{k} m_j p_1\cdots p_j'\cdots p_k \Rightarrow p_i \mid m_i p_1\cdots p_i'\cdots p_k$

$\mathrm{char}F=0 \Rightarrow p_i \mid p_1\cdots p_i'\cdots p_k$

$p_1,\cdots,p_k$ 不相伴, 两两不同的. $\Rightarrow p_i \mid p_i'$

$\deg p_i \geq 1$, $\deg p_i' = \deg p_i - 1 < \deg p_i$ 矛盾. □

推论: 若 $\mathrm{char}F=0$, $f\in F[x]\setminus F$, $f$ 无平方 $\Leftrightarrow$ $f$ 与 $f'$ 互素.

证明: $\gcd(f,f')=1$. $f$ 的 $SPF=\dfrac{f}{\gcd(f,f')}=f$ □

例: $f=x^4-2x+1\in\mathbb{Q}[x]$ 无平方.

证: $f, f'$ $f'=4x^3-2$

利用辗转相除计算 $\gcd(f,f')$

$f=\frac{1}{4}x(4x^3-2x)+r_1(x)$

$4x^3-2x=q(x)r_1(x)+r_2(x)$

$\cdots\cdots$

$\Rightarrow \gcd(f,f')=1$

$x=1$ 为 $f$ 的根.

$f(x)=(x-1)(\quad)$

例: $F=\mathbb{C}[x]$. $\forall f\in\mathbb{C}[x]$, $f=(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}$

↪ 代数闭域.

$f'=(x-\alpha_1)^{m_1-1}\cdots(x-\alpha_k)^{m_k-1}\left(\sum_{i=1}^{k} m_i(x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_k)\right)$

$\gcd(f,f')=(x-\alpha_1)^{m_1-1}\cdots(x-\alpha_k)^{m_k-1}$

$h$ 没有根, 所以进不了 $f$ 的因子. □

注：若 $\mathrm{char}F=p>0$ 则此命题不成立.

eg: 设 $g\in\mathbb{Z}_p[x]$ 为一不可约多项式. $f=g^{p^m}$.

f 无平方因子为 g.

$f'=p^m\cdot g^{p^m-1}\cdot g'=0$ , $\gcd(f,f')=f$.

$\gcd(f,0)$

## §2. 一些 UFD 的例子. $\mathbb{Z}$, $F[x]$, R是UFD, $R[x]$.

为简便：我们假定R为交换整环.

定义：$I\subset R$，称I为一个 理想(ideal) 若 I 满足

① I 为 R 的加法子群.

② $\forall r\in R$, $i\in I$ $r\cdot i\in I$. i.e. $R\cdot I\subset I$.


eg1. ⓪ $\{0\}\subset R$, $R\subset R$ 为理想，称为平凡理想. ($r\cdot 0=0\in\{0\}$, trivial)

① $R=F[x]$ $I_0=\{f(x)\mid f(0)=0\}$ 为 R 的理想. ($f=x\cdot g$)

$I_1=\{f(x)\mid f=x^2\cdot g(x) \text{ for some } g\in F[x]\}$ ($r\in F[x]$, $f=x^2g\in I$, $r\cdot f=x^2\cdot(rg)\in I$.)

② $R=F[x,y]$ $I_2=\{f(x,y)\mid f=xh(x,y)+yl(x,y) \text{ for some } h,l\in R\}$ ($R=F[x,y]$)

$\{f(x,y)=\sum_{\#\{(i,j)\mid ij>0\}} x^iy^j\cdot a_{ij}\}$

命题+定义：若 $r\in R$ 则 $(r)=\{r_0\cdot r\mid r_0\in R\}$ 为一个理想.

形如这样的理想，称为主理想.

pf: $r_0\cdot r$, $r_1\cdot r\in(r)$ $r_0\cdot r-r_1\cdot r=(r_0-r_1)\cdot r\in(r)$

$\forall r_0\cdot r\in(r)$, $\forall r_1\in R$ $r_1\cdot(r_0\cdot r)=(r_1\cdot r_0)\cdot r\in(r)$ □

一般整环中，与整环不有关相关概念可用理想表述.

eg: $a, b \in R$

$a \mid b \Leftrightarrow \exists c$ s.t. $b = ac \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$

($= c \cdot a$; $(a) = \{r \cdot a \mid r \in R\}$)

pf:

$b \in (a) \Leftrightarrow (b) \subseteq (a)$

"$\Rightarrow$" $b \in (a)$ $b = a \cdot c$ for some $c \in R$.

$\forall\, r \cdot b \in (b)$, $r \cdot b = r \cdot a \cdot c = (r \cdot c) \cdot a \Rightarrow (b) \subseteq (a)$

"$\Leftarrow$" $b \in (b)$ 因为 $b = 1 \cdot b \Rightarrow b \in (a)$. □

eg2: eg1 中. ① $(0) = \{0\}$, $R = (1)$.

② $I_0 = (x)$, $I_1 = (x^2)$

③ 尝试证明 $I_2$ 不是主理想.

定义：若 $R$ 的任一理想均为主理想，则称 $R$ 为主理想整环 (PID).

i.e. $\forall I \subset R$. $I$ 是理想 $\Rightarrow I = (a)$.

eg: $\mathbb{Z}$ 为主理想整环.

pf: $I \subset \mathbb{Z}$, 理想, i.e. $\begin{cases} I \text{ 是加法子群} \\ R \cdot I \subset I \end{cases}$.

$I \subset \mathbb{Z}$, $I \neq \{0\} = (0)$, $n$ 为 $I$ 中最小正整数.

$\forall\, m \in I$, 由带余除法 $m = q \cdot n + r$ $0 \le r \le n-1$.

$I$ 是理想, $q \cdot n \in I$, $m \in I \Rightarrow r = m - qn \in I$. $0 \le r < n$

$n$ 最小 $\Rightarrow r = 0$. i.e. $\forall m \in I$ $m = q \cdot n$.

i.e. $I = (n)$. □

目标：主理想整环是唯一分解整环.

命题：若 $R$ 是主理想整环，则 $R$ 中不可约元为素元.

即：若 $r\in R$ 为不可约元（$r\neq 0$），$r\mid bc$.

想证 $r\mid b$ or $r\mid c$ i.e. $b\in(r)$ or $c\in(r)$

若 $b\notin(r)$ 则 $I=(r)+(b)=\{\lambda r+\mu b\mid \lambda,\mu\in R\}$ 为理想

$R$ 为PID $\Rightarrow I=(r)+(b)=(t)$，$t\in R$.

$(r)\subsetneq I=(t)\Rightarrow t\mid r$，$r$ 不可约 $\Rightarrow t=u_0 r$ 或 $t=u_1$

$u_0,u_1$ 为单位.

若 $t=u r\Rightarrow b\in I=(t)=(u\cdot r)=(r)$，矛盾.（验证）

若 $t=u_1\Rightarrow I=(u_1)=R\Rightarrow 1\in I\Rightarrow$（验证；$u_1$ 单位）

$1=\lambda_0 r+\mu_0 b$

$\Rightarrow c=c\cdot 1=\lambda_0 rc+\mu_0 bc=\lambda_0 c r+\mu_0 bc\in(r)$

$\Rightarrow c\in(r)$. □

命题：PID 为 UFD.

对：若 R 为 PID，已知其不可约元必为素元.

我们只需证明 $\forall 0\neq r\in R$，$r$ 可写为有限不可约元（$r$ 不可逆）的乘积.

利用反证法. 若不成立 则 $a$ 一定不可约.

$a=a_1^{(1)}\cdot a_2^{(1)}$　　$a_1^{(1)}, a_2^{(1)}$ 不可逆.

且其中必有一个不能写为有限不可约元乘积，不妨设其为 $a_1^{(1)}$.

$a_1^{(1)}=a_1^{(2)}\cdot a_2^{(2)}$，$a_1^{(2)}, a_2^{(2)}$ 不可逆.

且其中必有一个不能写为有限不可约元乘积，不妨设其为 $a_1^{(2)}$

重复下去，得到序列 $a, a_1^{(1)}, a_1^{(2)}, a_1^{(3)}, \cdots$

满足 $a_1^{(i+1)} \mid a_1^{(i)}$ i.e. $(a_1^{(i)}) \subsetneq (a_1^{(i+1)})$.

我们得到理想序列

$(a)\subsetneq (a_1^{(1)})\subsetneq (a_1^{(2)})\subsetneq \cdots$

令 $I=\bigcup_{i=1}^{\infty}(a_1^{(i)})$，验证 $I$ 仍为理想.

$R$ 为 PID $\Rightarrow I=(r)$，$r\in R$.

$\Rightarrow r\in I \Rightarrow r\in (a_1^{(i)})$ for some $i\in\mathbb{N}$.

$\Rightarrow I=(r)\subset (a_1^{(i)})\subsetneq (a_1^{(i+1)})\subset I$.

矛盾.

$I\subsetneq I$

□

注：$\{\text{PIDs}\}\subsetneq\{\text{UFDs}\}$.

$R=F[x,y]$ 为 UFD 但非 PID.