# 多元多项式

例 $f = x_1 - (x_3x_2)(x_2+x_4^3)^2 - x_3 \in \mathbb{Z}_2[x_1,x_2,x_3,x_4]$. 计算 $\deg(f)$ 和 $\deg_{x_i}(f)$　$i=1,2,3,4$.

解:
$$f = x_1 - (x_3x_2)(x_2^2+x_4^6) - x_3. \quad (\text{Freshmen's dream}).$$
$$= x_1 + x_3 + x_3x_2^3 + x_3x_2x_4^6 \quad \leftarrow \quad f\text{的分布式}$$

$\deg_{x_1}(f)=1$, $\deg_{x_2}(f)=3$, $\deg_{x_3}(f)=1$, $\deg_{x_4}(f)=6$

$\rightarrow$ 把 $f$ 看作关于 $x_i$ 的多项式

$\deg(f) = 8$.

Thm. 设 $P \in R[x_1,\dots,x_n]$ 且 $P \neq 0$，则存在唯一的 $k \in \mathbb{Z}^+$，$\alpha_1,\dots,\alpha_k \in R\setminus\{0\}$ 和两两不同的单项式 $M_1,\dots,M_k \in X_n$，使得

$$P = \alpha_1M_1 + \dots + \alpha_kM_k \quad \rightarrow P\text{的分布式}$$

$$\deg(P) := \max\{\deg(M_1),\dots,\deg(M_k)\}.$$

规定 0 的次数为 $-\infty$

齐次多项式

Def (齐次多项式) 设 $h \in R[x_1,\dots,x_n]$，如果存在 $\beta_1,\dots,\beta_l \in R$ 和 $d$ 次的单项式 $N_1,\dots,N_l \in X_n$，使得
$$h = \beta_1N_1 + \dots + \beta_lN_l.$$
则称 $h$ 为齐 $d$ 次的。

Thm 任意一个非零的 $d$ 次多项式 $P$ 都可以唯一地写成 $P = h_d + h_{d-1} + \dots + h_0$，其中 $h_i$ 是齐 $i$ 次的多项式且 $h_d \neq 0$.

例子中 $f$ 的齐次分解为
$$f = \underbrace{x_3x_2x_4^6}_{h_8} + \underbrace{x_3x_2^3}_{h_4} + \underbrace{x_1+x_3}_{h_1}，\text{其余齐次分支都等于}0$$

Def (对称多项式) 设 $P \in R[x_1,\dots,x_n]$. 如果对于任意的 $\sigma \in S_n$，$\boxed{\phi_\sigma}(P) = P$，则称 $P$ 是关于 $x_1,\dots,x_n$ 的对称多项式

$\sigma \in S_n$，$\phi_\sigma: R[x_1,\dots,x_n] \rightarrow R[x_1,\dots,x_n]$.

$\phi_\sigma(x_i) = x_{\sigma(i)}$，$i=1,\dots,n$ 且 $\phi_\sigma|_R = \mathrm{id}$

同构映射 $\rightarrow$ 自行验证　例: $\sigma=(12)$　$\phi_\sigma(x_1+2x_2^3) = x_2+2x_1^3$

判断: 设 $f \in R[x_1,\dots,x_n]$，$\forall i,j \in \{1,2,\dots,n\}$，

$$P(x_1,\dots,\underset{i}{x_i},\dots,\underset{j}{x_j},\dots,x_n) = P(x_1,\dots,\underset{i}{x_j},\dots,\underset{j}{x_i},\dots,x_n).$$

例 $\forall r\in R$，$r$是对称多项式

$\forall k\in \mathbb{Z}^+$，$x_1^k+x_2^k+\cdots+x_n^k$ 是对称多项式，称为 $k$次幂和多项式

Prop. 设$T$是$R[x_1,\cdots,x_n]$中的所有对称多项式构成的集合，则$T$是$R[x_1,\cdots,x_n]$中的子环

Pf: 设$f,g\in T$，则对任意$\sigma\in S_n$，

$\phi_\sigma(f-g)=\phi_\sigma(f)-\phi_\sigma(g)=f-g$

$\Rightarrow f-g\in T$

$\Rightarrow (T,+,0)$ 是 $(R[x_1,\cdots,x_n],+,0)$ 的加法子群.

类似地，$\phi_\sigma(fg)=\phi_\sigma(f)\,\phi_\sigma(g)=fg$

且 $1\in T$.

$\Rightarrow (T,\cdot,1)$是含幺半群.

$\Rightarrow T$ 是$R[x_1,\cdots,x_n]$ 中的子环

特殊的对称多项式 —— 初等对称多项式

设 $P=(x_{n+1}-x_1)\cdots(x_{n+1}-x_n)\in R[x_1,\cdots,x_n,x_{n+1}]$ ①，把它看成关于$x_{n+1}$的一元多项式，则

$$P=x_{n+1}^n-\epsilon_1x_{n+1}^{n-1}+\cdots+(-1)^{n-1}\epsilon_{n-1}x_{n+1}+(-1)^n\epsilon_n. \quad ②$$

其中 $\epsilon_1,\cdots,\epsilon_{n-1},\epsilon_n\in R[x_1,\cdots,x_n]$.

比较①和②两边对应的幂次项的系数，可得：

$\epsilon_1=x_1+\cdots+x_n$.

$\epsilon_n=x_1\cdots x_n$.

易验证 $\epsilon_1,\epsilon_n$ 都是关于$x_1,\cdots,x_n$的对称多项式.

claim: $\forall i\in\{1,2,\cdots,n\}$，$\epsilon_i$ 均为对称多项式

设 $\sigma\in S_n$，$\sigma$可看做 $S_{n+1}$中满足 $\sigma(n+1)=n+1$ 的元素.

定义 $\phi_\sigma: R[x_1,\cdots,x_n,x_{n+1}]\longrightarrow R[x_1,\cdots,x_n,x_{n+1}]$.

$\phi_\sigma(x_i)=x_{\sigma(i)}$，$i=1,2,\cdots,n$.

$\phi_\sigma(x_{n+1})=x_{n+1}$.

则 $\phi_\sigma(P)=(x_{n+1}-x_{\sigma(1)})\cdots(x_{n+1}-x_{\sigma(n)})=P$.

另一方面，$\phi_\sigma(P) = x_{n+1}^{n} - \phi_\sigma(\epsilon_1)x_{n+1}^{n-1} + \cdots + (-1)^{n-1}\phi_\sigma(\epsilon_{n-1})x_{n+1} + (-1)^n\phi_\sigma(\epsilon_n)$.

$= P$

$\Rightarrow \phi_\sigma(\epsilon_i) = \epsilon_i$，$i = 1, 2, \ldots, n$.

$\Rightarrow \epsilon_1, \epsilon_2, \ldots, \epsilon_n$ 是对称多项式

再设 $\epsilon_0 = 1$. 我们称 $\epsilon_0, \epsilon_1, \ldots, \epsilon_n$ 是关于 $x_1, \ldots, x_n$ 的初等对称多项式

例. $n=2$，$(x_3-x_1)(x_3-x_2)$.

$\epsilon_1 = x_1+x_2$

$\epsilon_2 = x_1x_2$.

$n=3$，$(x_4-x_1)(x_4-x_2)(x_4-x_3)$

$\Rightarrow \epsilon_1 = x_1+x_2+x_3$.

$\epsilon_2 = x_1x_2+x_2x_3+x_1x_3$.

$\epsilon_3 = x_1x_2x_3$.

对于一般：$(x_{n+1}-x_1)(x_{n+1}-x_2)\cdots(x_{n+1}-x_n)$

$\epsilon_1 = x_1+x_2+\cdots+x_n$.

$\epsilon_2 = \sum\limits_{1\le i_1<i_2\le n} x_{i_1}x_{i_2}$

$\vdots$

$\epsilon_k = \sum\limits_{1\le i_1<i_2<\cdots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k}$.

$\vdots$

$\epsilon_n = x_1x_2\cdots x_n$.

根与系数的关系.

对于二次多项式，设 $f = ax^2+bx+c \in \mathbb{R}[x]$ 且 $a\neq 0$. $\alpha, \beta \in \mathbb{C}$ 是 $f$ 的两个根.

由韦达定理可知，

$\alpha+\beta = -\frac{b}{a}$ 且 $\alpha\beta = \frac{c}{a}$.

$\downarrow$. 保证来自于代数学基本定理.

设 $f \in \mathbb{C}[x]\setminus\mathbb{C}$，则 $f$ 在 $\mathbb{C}$ 中有根

Thm. 设 $f\in\mathbb{C}[x]$，$\deg(f) = n > 0$，$lc(f) = a_n$，令

$f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = a_n(x-\alpha_1)\cdots(x-\alpha_n)$

其中 $\alpha_1, \ldots, \alpha_n \in F$，不必两两不同，则

$\frac{a_i}{a_n}=(-1)^{n-i}\epsilon_{n-i}(\alpha_1,\cdots,\alpha_n)$；其中 $\epsilon_{n-i}$ 是第 $n-i$ 个 $n$ 元初等对称多项式，$i=0,1,\cdots,n$.

回忆：赋值同态.

Thm 设 $R$ 和 $S$ 是两个交换环；$\phi: R\to S$ 是环同态。对任意的 $s_1,\cdots,s_n\in S$，存在唯一的环同态 $\phi_{s_1,\cdots,s_n}: R[x_1,\cdots,x_n]\to S$ 使得.

$$\phi_{s_1,\cdots,s_n}(x_i)=s_i,\ i=1,\cdots,n.\ \text{且}\ \phi_{s_1,\cdots,s_n}|_R=\phi.$$

Pf 由上述定理可知，存在赋值同态，

$$\phi: \mathbb{C}[x_1,\cdots,x_n,x_{n+1}]\to\mathbb{C}[x].$$

满足：$\phi|_F$ 是恒同映射，$\phi(x_i)=\alpha_i$，$i=1,2,\cdots,n$. 和 $\phi(x_{n+1})=x$.

令

$$g=a_n(x_{n+1}-x_1)\cdots(x_{n+1}-x_n)$$

$$\phi(g)=a_n(x-\alpha_1)\cdots(x-\alpha_n)=f$$

另一方面，$g=a_n(x_{n+1}^n-\epsilon_1x_{n+1}^{n-1}+\cdots+(-1)^n\epsilon_n)$.

$$\phi(g)=a_n(x^n-\phi(\epsilon_1)x^{n-1}+\cdots+(-1)^n\phi(\epsilon_n))$$
$$=\cancel{f_n}=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0.$$

$$\Rightarrow a_n(-1)^{n-i}\epsilon_{n-i}(\alpha_1,\cdots,\alpha_n)=a_i,\quad i=0,1,\cdots,n.$$

$$\Rightarrow \frac{a_i}{a_n}=(-1)^{n-i}\epsilon_{n-i}(\alpha_1,\cdots,\alpha_n)$$

例 设 $f=ax^3+bx^2+cx+d$ 且 $a\neq0$，$\alpha,\beta,\gamma\in\mathbb{C}$ 是 $f$ 的三个根. 则

$$\alpha+\beta+\gamma=-\frac{b}{a},\quad \alpha\beta+\beta\gamma+\gamma\alpha=\frac{c}{a},\quad \alpha\beta\gamma=-\frac{d}{a}$$

(对称多项式基本定理) 设 $\epsilon_1,\cdots,\epsilon_n$ 是关于 $x_1,\cdots,x_n$ 的初等对称多项式，$f\in R[x_1,\cdots,x_n]$. 则 $f$ 关于 $x_1,\cdots,x_n$ 是对称的当且仅当存在唯一的多项式 $p\in R[y_1,\cdots,y_n]$，使得.

$$f=(x_1,\cdots,x_n)=p(\epsilon_1,\cdots,\epsilon_n)$$

(证明细节，感兴趣的同学可参见：李老师个人网站 2019-2020 第二学期 [习题课讲义 0])

## 一元多项式的无平方部分

设F是域，$P\in F[x]$的次数为正，则存在$c\in F$，F上两两互不相伴的不可约多项式$P_1,\dots,P_k\in F[x]$和唯一的$m_1,\dots,m_k\in\mathbb{Z}^+$，使得

$$P=cP_1^{m_1}\cdots P_k^{m_k}.$$

称$P_i$是$P$的$m_i$重因子，$i=1,2,\dots,k$.

特别地，$m_i=1$时，$P_i$称为单因子.

$P_1P_2\cdots P_k$称为$P$的无平方部分

Def 若多项式$P\in F[x]$的不可约因子都是单因子，则$P$称为无平方的.

计算无平方部分

工具：辗转相除法.

首先定义形式导数.

设$f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0\in F[x]$.定义$f$关于$x$的导数是

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

自行验证：对$\forall f,g\in F[x]$

① $(f+g)'=f'+g'$

② $(fg)'=f'g+fg'$

对于第②条验证：$\forall f,g\in F[x]$，设$n=\max(\deg(f),\deg(g))$.

$f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0$,

$g=g_nx^n+g_{n-1}x^{n-1}+\cdots+g_1x+g_0$. (注：未出现的幂次用0补齐).

$$(f\cdot g)'=\Big[\big(\sum_{i=0}^{n}f_ix^i\big)\big(\sum_{j=0}^{n}g_jx^j\big)\Big]'=\Big(\sum_{k=0}^{2n}\big(\sum_{\substack{i+j=k\\0\le i,j\le n}}f_ig_j\big)x^k\Big)'$$

$$\overset{①}{=}\sum_{k=0}^{2n}\Big(\big(\sum_{\substack{i+j=k\\0\le i,j\le n}}f_ig_j\big)x^k\Big)'=\sum_{k=1}^{2n}\Big(k\sum_{\substack{i+j=k\\0\le i,j\le n}}f_ig_j\Big)x^{k-1}$$

$$=\sum_{k=1}^{2n}\Big(\sum_{\substack{i+j=k\\0\le i,j\le n}}(i+j)f_ig_j\Big)x^{i+j-1}=\sum_{k=1}^{2n}\Big(\sum_{\substack{i+j=k\\0\le i,j\le n}}if_ig_j\Big)x^{i+j-1}+\sum_{k=1}^{2n}\Big(\sum_{\substack{i+j=k\\0\le i,j\le n}}jf_ig_j\Big)x^{i+j-1}$$

$$=\sum_{k=1}^{2n}\Big(\sum_{\substack{i+j=k\\0\le i,j\le n}}if_ix^{i-1}g_jx^j\Big)+\sum_{k=1}^{2n}\Big(\sum_{\substack{i+j=k\\0\le i,j\le n}}jg_jx^{j-1}\cdot f_ix^i\Big)$$

$=f'g+fg'$.

Thm. 设 $F$ 是特征为 0 的域，$f \in F[x] \backslash F$，则 $f$ 的无平方部分在 $F$ 上与 $\frac{f}{\gcd(f,f')}$ 相伴.

Pf: 不妨设 $f = p_1^{m_1} \cdots p_k^{m_k}$.

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

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

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

$\Rightarrow$ $g$ 是 $f$ 和 $f'$ 的公因子.

下证 $\gcd(f,h)=1$.

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

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

$\gcd(p_i,p_j)=1, i \neq j$ $\Rightarrow$ $p_1 \mid p_1'$

且 $m_1 \neq 0$ (∵特征为0).

$\Rightarrow$ $\deg(p_1') \geq \deg(p_1)$. $\rightarrow \Leftarrow$.

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

$\Rightarrow$ $\frac{f}{\gcd(f,f')} = p_1 \cdots p_k$.

Cor. 设 $F$ 是特征为 0 的域，$f \in F[x] \backslash F$，则 $f$ 是无平方的当且仅当 $\gcd(f,f')=1$.

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 $\gcd(f,f')=1$，由上述定理可知，$f$ 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 $f = x^3-x^2-x+1$  $f' = 3x^2-2x-1$  $\Rightarrow$ $\gcd(f,f') = x-1$.

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

无平方部分: $\frac{f}{\gcd(f,f')} = x^2-1$