# 第一次习题课

## 一. 课程内容回顾与补充

### §5. 多元多项式环

5.1 多元多项式环的构造：这一小节需注意会计算未定元的次数 (eg 1.1)

以及对于单项式排序的补充 (eg 1.2).

5.2 齐次多项式：

在了解齐次多项式基础上，学会做齐次分解 (eg 1.3)，以及齐次的显示表达 (eg 1.4) → 对之后判断齐次出题很有用.

☆5.3 赋值同态及应用

重复定义

5.4 初等对称多项式与 Vieta 定理

eg 2.1.

### §6 一元多项式元素方幂方

注意：$lcm(m,n) = \dfrac{mn}{gcd(m,n)}$.

eg 3.1 + 3.2

### §7. 中国剩余定理.

了解原理，会做计算题

## 二. 拓展内容：对称多项式基本定理

eg 4.1 + 引理 4.2 + 引理 4.3.

eg 1.1 设 $f = x_1 - (x_3x_2)(x_2 + x_4^3)^2 - x_3 \in \mathbb{Z}_2[x_1, x_2, x_3, x_4]$. 计算 $\deg(f)$ 和 $\deg_{x_i}(f)$. $i = 1, 2, 3, 4$.

解: $f = x_1 - (x_3x_2)(x_2^2 + x_4^6) - x_3$

$= x_1 + (x_3 + x_3x_2^2 + x_3x_2x_4^6)$ (特征2时, $1 = -1$). (看成 $x_1$ 元多项式) $\deg_{x_1}(f) = 1$

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

$= x_2x_2^3 + x_3x_4^6x_2 + (x_1 + x_3)$ (看成 $x_2$ 元) $\deg_{x_2}(f) = 3$

$= (1 + x_2^3 + x_2x_4^6)x_3 + x_1$ (看成 $x_3$ 元) $\deg_{x_3}(f) = 1$

$= x_3x_2x_4^6 + (x_1 + x_3 + x_3x_2^2)$ (看成 $x_4$ 元) $\deg_{x_4}(f) = 6$.

$= x_3x_2x_4^6 + x_3x_2^2 + (x_1 + x_3)$ (看成分布形式) $\deg(f) = 8$.

单项式: 设 $M = x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ 和 $N = x_1^{j_1}\cdots x_n^{j_n}$ 是两个单项式. 显然

$$M \mid N \iff i_1 \le j_1, \cdots i_n \le j_n$$

eg 1.2 (i) 纯字典序. 我们说 $M$ 在纯字典序下低于 $N$, 如果存在 $k \in \{1, 2, \cdots, n\}$ s.t

$$i_1 = j_1, \cdots, i_{k-1} = j_{k-1}, \quad i_k < j_k.$$

(ii) 全次数+纯字典序. 我们说 $M$ 在全次数+纯字典序下低于 $N$, 如果或者 $\deg(M) < \deg(N)$. 或者 $\deg(M) = \deg(N)$ 且 $M$ 在纯字典序下低于 $N$.

从高到低:

纯字典 $f = x_1 + x_2^3x_3 + x_2x_3x_4^6 + x_3$

全+纯 $f = x_2x_3x_4^6 + x_2^3x_3 + x_1 + x_3$

eg 1.3. $f$ 的齐次分解得:

$$f = \underbrace{x_2x_3x_4^6}_{h_8} + \underbrace{x_2^3x_3x_2}_{h_5} + \underbrace{x_1 + x_3}_{h_1}$$

其他齐次分支都等于0.

eg1.4 设 $f\in R[x_1,\cdots x_n]$. 证明f是齐d次多项式当且仅当对于任意 $p\in R[x_1,\cdots x_n]$

$$f(px_1,\cdots,px_n)=p^d f(x_1,\cdots x_n).$$

proof: 设单项式 $M(x_1,\cdots,x_n)=x_1^{d_1}\cdots x_n^{d_n}$ 的次数是 $d$. 则

$$M(px_1,\cdots,px_n)=(px_1)^{d_1}\cdots(px_n)^{d_n}=p^{d_1+\cdots+d_n}x_1^{d_1}\cdots x_n^{d_n}=p^dM.$$

"$\Rightarrow$"

设f是齐d次. 则 $f=\sum_{i=1}^{k}a_iM_i$, 其中 $a_i\in F$, $M_i\in X_n$. 且 $\deg(M_i)=d$, $i=1,2\cdots n$.

故 $f(px_1,\cdots,px_n)=\sum_{i=1}^{n}a_ip^dM_i=p^df$.

"$\Leftarrow$" 设 $f(px_1,\cdots,px_n)=p^df(x_1,\cdots x_n)$ 对任意 $p\in F[x_1,\cdots x_n]$ 成立. 假设 $f$ 不齐次.

$$f=h_k+h_m+h_{m-1}+\cdots+h_0. \qquad h_i\text{是}i\text{齐次的}.\ i=0,1,\cdots m-1$$

$$h_k\neq 0,\ h_m\neq 0$$

$$k>m.$$

令 $p=x_1$. 由上述证明 $f(x_1^2,x_1x_2,\cdots x_1x_n)$ 有两个齐次分解.

$$x_1^dh_k+x_1^dh_m+x_1^dh_{m-1}+\cdots+x_1^dh_0=x_1^kh_k+x_1^mh_m+x_1^{m-1}h_{m-1}+\cdots+x_1^0h_0$$

$x_1^dh_k=x_1^kh_k$ 和 $x_1^dh_m=x_1^mh_m$ 于是 $\deg(x_1^dh_k)=\deg(x_1^kh_k)$.

$d+k=2k$ 和 $d+m=2m$ $k=m$ 矛盾. □

eg2.1. 设 $A\in M_n(F)$, 其中F是域. 令 $f(t)=\det(tE-A)\in F[t]$.

(i) 证明: $\deg_t(f)=n$ 且首一.

设 $A=(a_{ij})_{n\times n}$ 则

$$f(t)=\begin{vmatrix} t-a_{11} & -a_{12} & \cdots & -a_{1n}\\ -a_{21} & t-a_{22} & \cdots & -a_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ -a_{n1} & -a_{n2} & \cdots & t-a_{nn}\end{vmatrix}$$

"不同行,不同列的元素乘积再求和"

由行列式定义可知, $f(t)$ 中关于t的最高次出现在 $(t-a_{11})\cdots(t-a_{nn})$, 而在其它乘积中t的最高次数至多是 $n-1$. 于是f是次数为n的首一多项式.

证明：$f(0)=(-1)^n\det(A)$.

由 $f(t)$ 的行列式表示和一元多项式赋值同态可知：$f(0)=\det(-A)$.

于是 $f(0)=(-1)^n\det(A)$.

由行列式性质也可得到：

$$f(0)=\begin{vmatrix} -a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & -a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & -a_{nn} \end{vmatrix}=(-1)^n\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

一元多项式赋值同态：

设 $S$ 是交换环，$\varphi: R\to S$ 是环同态，且 $s\in S$. 则存在唯一的环同态 $\varphi_s: R[x]\to S$ 满足

$$\varphi_s|_R=\varphi \quad 和 \quad \varphi_s(x)=s.$$

我们称上述定理中的环同态 $\varphi_s$ 关于 $\varphi$ 在 $s$ 处的赋值同态.

当 $S=R$ 且 $\varphi=\mathrm{id}_R$ 时，$\varphi_s$ 就是通常的从 $R[x]$ 到 $R$ 的在 $s$ 处的赋值映射

$f(x)\mapsto f(s)$.

故：$f(0)=\varphi_0(f)=\det(-A)$.

(iii) 设：$f$ 在下中有 $n$ 个根 $a_1,\cdots,a_n$. 证明：$a_1\cdots a_n=\det(A)$.

由 (i) 可设 $f(t)=t^n+\beta_{n-1}t^{n-1}+\cdots+\beta_0$. 其中 $\beta_{n-1},\beta_{n-2},\cdots\beta_0\in F$.

由 (ii) 知 $\beta_0=(-1)^n\det(A)$. 根据 Vieta 定理 $\left(\frac{a_i}{a_n}=(-1)^{n-i}\epsilon_{n-i}(a_1,\cdots,a_n)\right)$.

$$a_1\cdots a_n=(-1)^n\beta_0=\det(A).$$

eg3.1. 设 $f=x^n+a\in Q[x]$，其中 $n>1$，$a\in Q$. 证明 $f$ 是无平方的当且仅当 $a\neq 0$.

证：注意到 $f'=nx^{n-1}$. 于是 $f+\frac{-x}{n}f'=a$.

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

因为 $n>1$. $\therefore x^n$ 不是无平方的. 于是 $a\neq 0$.

□

eg 3.2 设 $p$ 是素数，$f \in \mathbb{Z}_p[x]$. 证明 $f' = 0$ 当且仅当存在 $g \in \mathbb{Z}_p[x]$ 使得 $f = g^p$.

证明："$\Leftarrow$" 如果 $f = g^p$，则 $f' = p g^{p-1} g' = 0$. 这是因为 $\mathbb{Z}_p$ 的特征等于 $p$.

"$\Rightarrow$"

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

其中 $f_n, f_{n-1}, \cdots f_1, f_0 \in \mathbb{Z}_p$. 由

$$f' = n f_n x^{n-1} + (n-1) f_{n-1} x^{n-2} + \cdots + f_1 = 0.$$

于是，我们有 $k f_k = 0$, $k = 1, 2, \cdots, n$ 如果 $f_k \neq 0$，则 $p \mid k$. 由此可知

$$f = f_{i_1} x^{j_1 p} + \cdots + f_{i_e} x^{j_e p},$$

其中 $f_{i_1}, \cdots, f_{i_e} \in \mathbb{Z}_p \setminus \{0\}$ 且 $i_1 = j_1 p, \cdots, i_e = j_e p$. 由 Fermat 小定理，

$a^p \equiv 1 \pmod p$. $a^p = a$

□.

重点补解 freshmen's dream：

二. 对称多项式基本定理：

$hm(f)$.

$\forall f, g \in R[x_1, \cdots, x_n] \setminus 0$, $hm(fg) = hm(f)\, hm(g)$.

eg 4.1 设 $\varepsilon_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}$. 则 $hm(\varepsilon_k) = x_1 x_2 \cdots x_k$.

引理 4.2. 设 $\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n$ 是关于 $x_1, \cdots x_n$ 的初等对称多项式. 则

$$hm(\varepsilon_1^{d_1} \varepsilon_2^{d_2} \cdots \varepsilon_n^{d_n}) = x_1^{d_1 + \cdots + d_n} x_2^{d_2 + \cdots + d_n} \cdots x_n^{d_n}$$

证：由 eg 4.1 可知，$hm(\varepsilon_k^{d_k}) = x_1^{d_k} \cdots x_k^{d_k}$. 而

$$hm(\varepsilon_1^{d_1} \varepsilon_2^{d_2} \cdots \varepsilon_n^{d_n}) = hm(\varepsilon_1^{d_1})\, hm(\varepsilon_2^{d_2}) \cdots hm(\varepsilon_n^{d_n}) = x_1^{d_1 + d_2 \cdots + d_n} x_2^{d_2 + \cdots + d_n} \cdots x_n^{d_n}$$ □

在设 $f$ 的齐次分解为 $f = h_d + h_{d-1} + \cdots + h_0$

对 $\forall \sigma \in S_n$，设 $\phi_\sigma : R[x_1, \cdots, x_n] \to R[x_1, \cdots, x_n]$ s.t. $\phi_\sigma(x_i) = x_{\sigma(i)}$, $i = 1, \cdots, n$ $\phi_\sigma(r) = r$ $\forall r \in R$. 则

$$\phi_\sigma(f) = \phi_\sigma(h_d) + \cdots + \phi_\sigma(h_0)$$

引理4.3：设 $f \in R[x_1, \cdots, x_n]$ 1的对称 $hm(f) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$.

如果f对称，则 $k_1 \geq k_2 \geq \cdots \geq k_n$.

证：设 $\sigma \in S_n$. 因为 $\phi_\sigma(f) = f$, $\therefore x_{\sigma(1)}^{k_1} \cdots x_{\sigma(n)}^{k_n}$ 出现在f分布式表示中且不高于 $hm(f)$.

由$\sigma$任意性可知 $k_1 \geq \max(k_2, \cdots, k_n)$. 否则会存在 $\tau \in S_n$ s.t $\phi_\tau(f)$ 的头项与f的头项不同，与f对称性矛盾. 同理可证.

$k_i \geq \max(k_{i+1}, \cdots, k_n)$, $i = 2, 3, \cdots, n-1$