回忆：在本周讲义中，R是一个交换环

例如：$\mathbb{Z}$，$\mathbb{Z}_m$，$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$

R上的一元多项式环

$$R[x]=\left\{\sum_{i=0}^{d}a_ix^i \,\middle|\, d\in\mathbb{N},\ a_i\in R\right\}.$$

x 是未定元 (indeterminate)

$$\sum_{i=0}^{d}a_ix^i=0 \iff a_0=\cdots=a_d=0.$$

上学期讲义16 (p15)

定理2.1 如果R是整环，则$R[x]$也是整环

定理2.2 设S是交换环，$s\in S$

$\varphi: R\to S$ 是环同态，则存在环

同态 $\varphi_s: R[x]\to S$

满足 (i) $\varphi_s|_R=\varphi$

(ii) $\varphi_s(x)=s$

事实上 $\varphi_s\left(\sum_{i=0}^{d}a_ix^i\right)=\sum_{i=0}^{d}\varphi(a_i)s^i$

§3 多元多项式

§3.1 多元多项式环

$$\begin{tikzcd}
R \arrow[r] \arrow[d, dash] & R[x_1] \arrow[r] \arrow[d, dash] & R[x_1][x_2] \arrow[r] \arrow[d, dash] & \cdots \arrow[r] & R[x_1][x_2]\cdots[x_n] \arrow[d, dash] \\
\text{交换环} \arrow[d, dash] & \text{交换环} \arrow[d, dashed, dash] & \text{交换环} \arrow[d, dashed, dash] & & \text{交换环} \arrow[d, dashed, dash] \\
\text{整环} & \text{整环} & \text{整环} & & \text{整环}
\end{tikzcd}$$

记 $R[x_1][x_2]\cdots[x_n]$ 为 $R[x_1,x_2,\ldots,x_n]$，称为R上关于未定元 $x_1,x_2,\ldots,x_n$ 的多元多项式环．

由定理2.1和数学归纳法可知

定理3.1 如果R是整环，则 $R[x_1,\ldots,x_n]$ 也是整环．

定理3.2 设 S 是交换环, $s_1,\dots,s_n\in S$

$\varphi: R\to S$ 是环同态. 则存在唯一的环同态 $\varphi_{s_1,\dots,s_n}$ 满足

(i) $\varphi_{s_1,\dots,s_n}\big|_R=\varphi$

(ii) $\forall i\in\{1,\dots,n\}$, $\varphi_{s_1,\dots,s_n}(x_i)=s_i$

证: $n=1$. 即是定理2.2

设 $n-1$ 时结论成立. 即存在唯一的环同态 $\varphi_{s_1,\dots,s_{n-1}}$ 满足

(i) $\varphi_{s_1,\dots,s_{n-1}}\big|_R=\varphi$

(ii) $\forall i\in\{1,\dots,n-1\}$, $\varphi_{s_1,\dots,s_{n-1}}(x_i)=s_i$

对 $R[x_1,\dots x_{n-1}]$, s_n, ~~和~~ $\varphi_{s_1,\dots,s_{n-1}}$ 应用定理2.2

可得唯一的环同态

$$\varphi_{s_1,\dots s_{n-1},s_n}: R[x_1,\dots x_{n-1}][x_n]\longrightarrow S$$

满足 (i) $\varphi_{s_1,\dots,s_{n-1},s_n}\big|_{R[x_1,\dots x_n]}=\varphi_{s_1,\dots,s_{n-1}}$

(ii) $\varphi_{s_1,\dots s_{n-1},s_n}(x_n)=s_n$

$\varphi_{s_1,\dots s_{n-1},s_n}\big|_R=\varphi_{s_1,\dots s_{n-1}}\big|_R=\varphi$

$\varphi(x_i)=s_i$, $i=1,2,\dots,n$ □

例: 设 $f=x^2+2y-1$, $g=xy+2\in\mathbb{Z}[x,y]$,

$h=fg$. 求 $h(2,5)$

解: $\varphi:\mathbb{Z}\to\mathbb{Z}$ 是恒同映射 是环同态. 故得

$\varphi_{2,5}\ \mathbb{Z}[x,y]\to\mathbb{Z}$ 是环同态.

$\varphi_{2,5}(x)=2$, $\varphi_{2,5}(y)=5$

$h(2,5)=\varphi_{2,5}(h)=\varphi_{2,5}(f)\,\varphi_{2,5}(g)$

$=f(2,5)\times g(2,5)$

$=(4+10-1)(10+2)=13\times12=156$

回忆 §3.1 已讲内容

令 $X_n=\{x_1^{i_1}\cdots x_n^{i_n} \mid i_1,\cdots,i_n\in\mathbb{N}\}$

X_n 中的元素称为单项式 (monomial)

~~命题~~3.1 设 $f\in R[x_1,\cdots,x_n]\setminus\{0\}$. 则存在唯一的 $\alpha_1,\cdots,\alpha_k\in R\setminus\{0\}$, $M_1,\cdots,M_k\in X_n$ 两两不同 使得

$$f=\alpha_1M_1+\cdots+\alpha_kM_k \quad (*)$$

称 α_j 是 f 关于 M_j 的系数. (*) 称为 f 的分布式 (distributive form)

例: 设 $f=(x_1-1)(x_2-1)+x_1x_2^2+x_1x_2+x_1^2$ 把 f 写成关于 x_1, 关于 x_2 的多项式. 求 f 的分布式

解: $f=x_1^2+(x_2^2+2x_2-1)x_1-(x_2-1)\in\mathbb{Z}[x_2][x_1]$

$f=x_1x_2^2+(2x_1-1)x_2+x_1^2-x_1+1\in\mathbb{Z}[x_1][x_2]$

$f=x_1x_2^2+x_1^2+2x_1x_2-(x_1+x_2)+1$

~~定理~~ §3.2 多元多项式的总次数 (total degree)

定义: 设 $M=x_1^{i_1}\cdots x_n^{i_n}\in X_n$. M 的总次数是 $i_1+\cdots+i_n$ 记为 $\deg(M)$. 特别有 $\deg(1)=0$

再设 $N=x_1^{j_1}\cdots x_n^{j_n}\in X_n$

$$MN=x_1^{i_1+j_1}\cdots x_n^{i_n+j_n}$$

$$\deg(MN)=\deg(M)+\deg(N).$$

定义: 设 $f\in R[x_1,\cdots,x_n]\setminus\{0\}$ 的分布式是

$$f=\alpha_1M_1+\cdots+\alpha_kM_k$$

f 的总次数定义为 $\max\limits_{1\le j\le k}(\deg(M_j))$.

特别约定 $\deg(0)=-\infty$

把 f 看成关于 x_i 的多项式. 即 $f\in R[x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n][x_i]$

f 关于 x_i 的次数记为 $\deg_{x_i}(f)$

注. 在上例中 $\deg_{x_1}(f)=2$, $\deg_{x_2}(f)=2$

$$\deg(f)=3.$$

回忆：一元多项式运算与次数之间的关系

设 $f, g \in R[x]$

(i) $\deg(f+g) \leq \max(\deg(f), \deg(g))$

(ii) $\deg(fg) \leq \deg(f) + \deg(g)$.

当 R 是整环时 (ii) 中等号成立.

(见讲义15. P14).

下面我们把上述结论推广到 $R[x_1, \ldots, x_n]$

定义：设 $h \in R[x_1, \ldots, x_n] \setminus \{0\}$.

$$h = \alpha_1 M_1 + \cdots + \alpha_k M_k$$

是 h 的分布式. 如果 $\deg(M_1) = \cdots = \deg(M_k) =: d$ 则称 h 是齐 d 次的. 此外, 0 称为齐任何次的.

例：齐一次

$\alpha_1 x_1 + \cdots + \alpha_n x_n$

$\alpha_1, \ldots \alpha_n \in R$

一次

$\alpha_1 x_1 + \cdots + \alpha_n x_n + \beta$

$\alpha_1, \ldots \alpha_n \in R$ 不全为零

$\beta \in R$

齐二次

$\alpha_1 x_1^2 + \cdots + \alpha_n x_n^2 + \sum_{1 \leq i < j \leq n} \beta_{ij} x_i x_j$

$\alpha_1, \ldots \alpha_n, \beta_{ij} \in R$

二次

非零齐二次 + 一次

引理 3.1

(i) 任何两个齐 d 次多项式之和仍是齐 d 次的

(ii) 设 $u, v \in R[x_1, \ldots, x_n]$ 分别是齐 d 次和齐 e 次的 则 uv 是齐 $d+e$ 次的

证：设 $f = \alpha_1 M_1 + \cdots + \alpha_k M_k$

$g = \beta_1 N_1 + \cdots + \beta_l N_l$

其中 $\alpha_1, \ldots \alpha_k, \beta_1, \ldots \beta_l \in R$, $M_1, \ldots M_k, N_1, \ldots N_l \in X_n$

则 $f + g = \alpha_1 M_1 + \cdots + \alpha_k M_k + \beta_1 N_1 + \cdots + \beta_l N_l$

$$fg = \sum_{i=1}^{k} \sum_{j=1}^{l} \alpha_i \beta_j M_i N_j$$

(i) $\deg(M_i) = \deg(N_j) = d$, $i \in \{1, \ldots k\}$, $j \in \{1, \ldots l\}$

$\Rightarrow f+g$ 是齐 d 次的

(ii) 设 $L_{ij} = M_i N_j$. 则 $L_{ij} \in X_n$ 且 $\deg(L_{ij}) = d+e$. 于是 fg 是齐 $d+e$ 次的.

引理3.2 设 $f\in R[x]\setminus\{0\}$，$\deg(f)=d$.

则存在唯一的齐 i 次多项式 h_i，$i=0,1,\dots,d$

使得 $f=h_d+h_{d-1}+\dots+h_0$ 且 $h_d\neq 0$.

证：~~设 $H=\{M_1,\dots,M_k\}$~~ 设

$f=\alpha_1M_1+\dots+\alpha_kM_k$ 是分布式

$H=\{M_1,\dots M_k\}$. $H_i=\{M\in H\mid \deg(M)=i\}$

其中 $i=0,1,\dots,d$. 令

$$h_i=\sum_{M_j\in H_i}\alpha_jM_j$$ 当 $H_i=\emptyset$，$h_i=0$

则 $f=h_d+h_{d-1}+\dots+h_0$ 且 $h_d\neq 0$

再设 $f=\tilde h_d+\tilde h_{d-1}+\dots+\tilde h_0$，~~其中~~ $\tilde h_i$ 是 i 齐次的，$i=0,1,\dots d$. 则

$$(h_d-\tilde h_d)+(h_{d-1}-\tilde h_{d-1})+\dots+(h_0-\tilde h_0)=0$$

因为次数不同的单项式不能彼此抵消，

所以 $h_i-\tilde h_i=0$ （引理3.1 (ii)）

$i=0,1,\dots,d$ □

定理3.3 设 $f,g\in R[x_1,\dots x_n]$

(i) $\deg(f+g)\le\max(\deg(f),\deg(g))$

(ii) $\deg(fg)\le\deg(f)+\deg(g)$. 当 R 的整环时

(ii) 中 ~~等~~ 号成立

证：当 $f=0$ 或 $g=0$ 时 定理显然成立

设 $f\neq0$，$g\neq0$. 由引理3.2

$f=u_d+u_{d-1}+\dots+u_0$，其中 u_i 是齐 i 次的

且 $u_d\neq0$，$i=0,1,\dots d$. 类似

$g=v_e+v_{e-1}+\dots+v_0$，其中 v_j 是齐 j 次的

且 $v_e\neq0$，$j=0,1,\dots e$. 不妨设 $d\ge e$

(i) $f+g=u_d+\dots+u_{e+1}+(u_e+v_e)+\dots+(u_0+v_0)$

则当 $d>e$ 时 $\deg(f+g)=d$ $\Rightarrow \deg(f+g)\le d$

当 $d=e$ 时 $\deg(f+g)\le d$

(ii) $fg=u_dv_e+\sum_{0\le i+j<d+e}u_iv_j$

由引理3.1 (ii) $\deg(fg)\le d+e$

当 R 是整环时，由定理3.1 (i) 得出，$u_dv_e\neq0$

$\deg(u_dv_e)=d+e$ □

§4 对称多项式简介

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

$$f(x_1,\cdots,\underset{i}{x_i},\cdots,\underset{j}{x_j},\cdots,x_n)=f(x_1,\cdots,\underset{i}{x_j},\cdots,\underset{j}{x_i}\cdots x_n)$$

则称 f 是对称多项式

注：$\forall\sigma\in S_n$，σ 是若干对换之积。

于是 $f(x_1,\cdots,x_n)$ 对称 $\Leftrightarrow\forall\sigma\in S_n$

$$f(x_1,\cdots x_n)=f(x_{\sigma(1)},\cdots,x_{\sigma(n)})$$

例：$\forall r\in R$，r 是对称多项式

$\forall k\in\mathbb{N}$ $x_1^k+x_2^k+\cdots+x_n^k$ 是对称的

称为 k 次幂和多项式。

例 $\varepsilon_k=\sum\limits_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}x_{i_1}x_{i_2}\cdots x_{i_k}$ $k\in\{1,2,\cdots n\}$

称为 k 次初等对称多项式

$k=1$，$\varepsilon_1=x_1+\cdots+x_n$

$k=2$ $\varepsilon_2=\sum\limits_{1\leqslant i<j\leqslant n}x_ix_j$

$k=n$ $\varepsilon_n=x_1x_2\cdots x_n$

特别地，定义 $\varepsilon_0=1$.

下面证明 $\forall k\in\{0,1,\cdots n\}$，$\varepsilon_k$ 是对称多项式。

设 $p=(x-x_1)\cdots(x-x_n)\in R[x_1,\cdots,x_n,x]$

$$=x^n+p_{n-1}x^{n-1}+\cdots+p_0,$$

其中 $p_{n-1},\cdots,p_0\in R[x_1,\cdots,x_n]$. 令 $p_n=1$

则 $p_{n-k}=(-1)^k\varepsilon_k$，$k=0,1,\cdots,n$.

设 $i,j\in\{1,2,\cdots,n\}$

$$\varphi_{ij}:R[x_1,\cdots,x_n]\longrightarrow R[x_1,\cdots x_n]$$

$$f(x_1,\cdots,\underset{i}{x_i}\cdots,\underset{j}{x_j}\cdots x_n)\longmapsto f(x_1\cdots,\underset{i}{x_j},\cdots\underset{j}{x_i}\cdots x_n)$$

由定理3.2. φ_{ij} 是环同态

由定理3.2. φ_{ij} 可以扩充为环同态

$$\varphi_{ij,x}: R[x_1,\dots x_n][x] \longrightarrow R[x_1\dots x_n][x]$$

满足 $\varphi_{ij,x}\big|_{R[x_1,\dots,x_n]} = \varphi_{ij}$

$$\varphi_{ij,x}(x) = x$$

则

$$\varphi_{ij,x}(p) = \varphi_{ij,x}\big((x-x_1)\cdots(x-x_n)\big)$$

$$= \varphi_{ij,x}(x-x_1)\cdots\varphi_{ij,x}(x-x_n)$$

$$= \big(\varphi_{ij,x}(x)-\varphi_{ij,x}(x_1)\big)\cdots\big(\varphi_{ij,x}(x)-\varphi_{ij,x}(x_n)\big)$$

$$= (x-\varphi_{ij}(x_1))\cdots(x-\varphi_{ij}(x_n))$$

$$= (x-x_1)\cdots\underset{i}{(x-x_j)}\cdots\underset{j}{(x-x_i)}\cdots(x-x_n)$$

$$= p$$

另一方面

$$\varphi_{ij,x}(p) = \varphi_{ij,x}(x^n+p_{n-1}x^{n-1}+\dots+p_0)$$

$$= \varphi_{ij,x}(x^n)+\varphi_{ij,x}(p_{n-1})\varphi_{ij}(x^{n-1})+\dots+\varphi_{ij,x}(p_0)$$

$$= x^n+\varphi_{ij}(p_{n-1})x^{n-1}+\dots+\varphi_{ij}(p_0)$$

$\Rightarrow p_k = \varphi_{ij}(p_k)$, $k=0,1,\dots,n-1$.

$\Rightarrow p_k$ 是对称的 $\Rightarrow \varepsilon_k$ 是对称的 ▨

定理4.1 (Vieta 定理)

设F是域. $f(x)\in F[x]\setminus F$ 且

$f = f_n x^n + f_{n-1}x^{n-1}+\dots+f_0$, $f_i \in F$, f_n

$= f_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $\alpha_i \in F$

~~则 $\frac{f_{n-k}}{f_n} = (-1)^k \varepsilon_k(\alpha_1,\alpha_2,\dots,\alpha_n)$, $k=0,1,\dots$~~

~~$k=0,1,\dots n$~~

则 $f_{n-k}f_n^{-1} = (-1)^k\varepsilon_k(\alpha_1,\dots\alpha_n)$,

$k=0,1,\dots n$

证: 设同态 $\varphi: F[x_1,\dots,x_n][x] \longrightarrow F[x]$

$\varphi|_F = \mathrm{id}_F$. $\varphi(x_i) = \alpha_i$, $i=1,2,\dots n$

$\varphi(x) = x$.

由定理3.1, 这样的 φ 存在.

令 $p(x) = f_n(x-x_1)\cdots(x-x_n)$

$$\varphi(p) = \varphi(f_n)(\varphi(x)-\varphi(x_1))\cdots(\varphi(x)-\varphi(x_n))$$

$$= f_n(x-\alpha_1)\cdots(x-\alpha_n)$$

$$= f$$

另一方面

$$p = f_n x^n - f_n\varepsilon_1 x^{n-1} + \cdots + (-1)^{n-1} f_n\varepsilon_{n-1}x + (-1)^n f_n\varepsilon_n$$

$$\varphi(p) = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$$

$$= f_n x^n - f_n\varepsilon_1(\alpha_1,\ldots,\alpha_n)x^{n-1} + \cdots + (-1)^{n-1} f_n\varepsilon_{n-1}(\alpha_1,\ldots,\alpha_n)$$

$$+ (-1)^n f_n\varepsilon_n(\alpha_1,\ldots,\alpha_n)$$

于是 $f_{n-k} = (-1)^k f_n \varepsilon_k(\alpha_1,\ldots,\alpha_n)$

$$\Rightarrow f_{n-k} f_n^{-1} = (-1)^k \varepsilon_k(\alpha_1,\ldots,\alpha_n) \quad \square$$

例 $n=2$

$$f_1 f_2^{-1} = -\alpha_1+\alpha_2$$

$$f_0 f_2 = \alpha_1\alpha_2$$

即二次方程的韦达定理

例 设 $f(x) = x^3-2x^2+3x+1 \in \mathbb{C}[x]$ 的三个根是 $\alpha_1, \alpha_2, \alpha_3$. 求 $\alpha_1^2+\alpha_2^2+\alpha_3^2$

解: $\alpha_1^2+\alpha_2^2+\alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_1\alpha_3)$

$$= \varepsilon_1(\alpha_1,\alpha_2,\alpha_3)^2 - 2\varepsilon_2(\alpha_1,\alpha_2,\alpha_3)$$

注 $\varepsilon_1(x_1,x_2,x_3) = x_1+x_2+x_3$

$\varepsilon_2(x_1,x_2,x_3) = x_1x_2+x_2x_3+x_3x_1$

设 $f(x) = f_3x^3+f_2x^2+f_1x+f_0$

由 Vieta 定理

$$f_2 f_3^{-1} = -(\alpha_1+\alpha_2+\alpha_3) \Rightarrow \alpha_1+\alpha_2+\alpha_3 = 2$$

$$f_1 f_3^{-1} = \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 \Rightarrow \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 = 3$$

$$\Rightarrow \alpha_1^2+\alpha_2^2+\alpha_3^2 = 4-6 = -2$$

定理 4.2 设 $S = \{f \in R[x_1,\ldots,x_n] \mid f \text{ 对称}\}$

则 (i) S 是 $R[x_1,\ldots,x_n]$ 的子环

(ii) $\forall f \in S \ \exists!\, P \in R[y_1,\ldots,y_n]$

使得 $f(x_1,\ldots,x_n) = P(\varepsilon_1,\ldots,\varepsilon_n)$

证：(i) 可直接验证：$0, 1 \in S$，

$\forall f, g \in S$，$fg \in S$. 于是 S 是子环

(ii) 见书 P190-P191 定理1 及其证明

例*：求 $p \in \mathbb{Z}[y_1, y_2, y_3]$ 使得对称多项式

$$f = x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_1 + x_2^2 x_3 + x_3^2 x_1 + x_3^2 x_2 = p(\varepsilon_1, \varepsilon_2, \varepsilon_3)$$

$$f - \varepsilon_1\varepsilon_2 = f - (x_1+x_2+x_3)(x_1x_2+x_2x_3+x_1x_3)$$

$$= f - (f + 3x_1x_2x_3) = -3x_1x_2x_3 = -3\varepsilon_3$$

$$f = \varepsilon_1\varepsilon_2 - 3\varepsilon_3$$

即 $p = y_1y_2 - 3y_3$

例：展开

$$W = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ x_1^3 & x_2^3 & \cdots & x_n^3 \\ \vdots & & & \\ x_1^n & x_2^n & \cdots & x_n^n \end{vmatrix}$$

解：考虑

$$\widetilde{W} = \begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_2 & \cdots & x_n & y \\ x_1^2 & x_2^2 & \cdots & x_n^2 & y^2 \\ & \cdots & & & \\ x_1^n & x_2^n & \cdots & x_n^n & y^n \end{vmatrix}$$

$$= (y-x_1)\cdots(y-x_n)\prod_{1\le i<j\le n}(x_j - x_i)$$

把 $\widetilde{W}$ 看成关于 y 的多项式

则 $\widetilde{W}$ 关于 y 的系数是

$$(-1)^{n-1} W = (-1)^{n-1}\varepsilon_{n-1}(x_1 \cdots x_n)\prod_{1\le i<j\le n}(x_j - x_i)$$

$$\Rightarrow W = \left[\prod_{1\le i<j\le n}(x_j - x_i)\right]\left(\sum_{1\le k_1<k_2<\cdots<k_{n-1}\le n} x_{k_1}x_{k_2}\cdots x_{k_{n-1}}\right)$$

§5 补充内容

§5.1 中国剩余定理

引理5.1 设 $m_1, \cdots, m_k \in \mathbb{Z}^+$，两两互素

则 (i) $m_1 \cdots m_{k-1}$ 与 m_k 互素

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

证：(i) 因为 $\forall i \in \{1, \cdots, k-1\}$，$\gcd(m_i, m_k) = 1$

所以 $\exists u_i, v_i \in \mathbb{Z}$ 使得

$$u_i m_i + v_i m_k = 1$$

（Bezout关系，上学期讲义4，定理8.2）

于是 $\prod_{i=1}^{k-1} (u_i m_i + v_i m_k) = 1$

$\Rightarrow \exists u, v \in \mathbb{Z}$ 使得 $u(m_1 \cdots m_{k-1}) + v m_k = 1$

由同样的定理，$m_1 \cdots m_{k-1}$ 和 m_k 互素

(ii) 对 k 归纳，当 $k=2$ 时，由上述讲义中

定理8.3得：$\operatorname{lcm}(m_1, m_2) = \dfrac{m_1 m_2}{\gcd(m_1, m_2)} = m_1 m_2$

$(\because \gcd(m_1, m_2) = 1)$

设 $k-1$ 时结论成立

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

则 l 是 $m_1 \cdots m_{k-1}$ 的公倍式，于是

$$\operatorname{lcm}(m_1, \cdots m_{k-1}) \underset{\text{归纳假设}}{=} (m_1 \cdots m_{k-1}) \mid l$$

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 $m_1 \cdots m_{k-1}$，m_k 互素，由 $k=2$ 的推理

可知：$\operatorname{lcm}(m_1 \cdots m_{k-1}, m_k) = m_1 m_2 \cdots m_k \mid l$

$\Rightarrow l = m_1 m_2 \cdots m_k$. ▨

定理5.1（Chinese Remainder Theorem）

设 $m_1, \cdots, m_k \in \mathbb{Z}$ 且大于1，两两互素

$r_1, \cdots r_k \in \mathbb{Z}$，使得

(i) $\exists x \in \mathbb{Z}$

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

(ii) 设 $x\in\mathbb{Z}$ 是上述~~方程~~同余~~方~~程组 (*) 的解

则 (*) 的所有整数解构成的集合是

$$\{x+l\,m_1\cdots m_k \mid l\in\mathbb{Z}\}$$

特别地 (*) 在 $[0, m_1\cdots m_k)$ 中有唯一的整数解

证：(i) 对 k 归纳。当 $k=1$ 时，取 $x=r_1$ 即可。设 x' 满足

$x'\equiv r_1 \bmod m_1, \cdots\cdots x'\equiv r_{k-1} \bmod m_{k-1}$

由引理 5.1 (i) $\exists\, u,v\in\mathbb{Z}$ 使得

$$u(m_1\cdots m_{k-1})+v\,m_k=1 \quad (**)$$

令 $x=x'+u(m_1\cdots m_{k-1})(r_k-x')$

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

由 (**)

$x=x'+(1-vm_k)(r_k-x')=r_k-vm_k(r_k-x')$

$$x\equiv r_k \bmod m_k$$

结论 (i) 成立

(ii) 若 $y=x+l(m_1\cdots m_k)$

则 $y\equiv x \bmod (m_i)$，$i=1,2,\cdots k$

$\Rightarrow y\equiv r_k \bmod m_i$.

反之：设 y 是 (*) 的解

则 $y\equiv x \bmod m_i$，$i=1,2,\cdots k$

$\Rightarrow m_i\mid(y-x) \Rightarrow (m_1\cdots m_k)\mid(y-x)$. [引理5.1(ii)]

$\Rightarrow \exists\, l\in\mathbb{Z}$ 使得 $y-x=l(m_1\cdots m_k)$.

设 $x_0=\mathrm{rem}(x, m_1\cdots m_k)$ 且 $x_0=x-q\,m_1\cdots m_k$

则 $x_0\in[0, m_1\cdots m_k)$ 其中 $q\in\mathbb{Z}$. 于是 x_0 是 (*) 的解。而其它解为 $x_0+l\,m_1\cdots m_k$，$l\in\mathbb{Z}\setminus\{0\}$

都在 $[0, m_1\cdots m_k)$ 中 ▨

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

求解同余方程组

$$\begin{cases} x\equiv 2 \mod 3\\ x\equiv 3 \mod 5\\ x\equiv 2 \mod 7\end{cases}$$

解：$x_1=2$　　$2\cdot 3-5=1$

$x_2=2+2\cdot 3\,(3-2)=8$，　$15-2\cdot 7=1$

$x_3=8+15\,(2-8)=-82$　　$3\times 5\times 7=105$

最小正整数解：$-82=-105+23$　　$x=23$

所有解　$\{\,23+k\times 105 \mid k\in\mathbb{Z}\,\}$

环同态的观点

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, "\pi_{m_1}"'] \arrow[d, "\pi_{m_2}"] \arrow[drr, bend left, "\pi_{m_k}"] & & \\ \mathbb{Z}_{m_1} & \mathbb{Z}_{m_2} & \cdots & \mathbb{Z}_{m_k} \end{tikzcd}$$

当 $m_1, m_2, \dots m_k$ 互素时，$\forall\, \bar{r}_1\in\mathbb{Z}_{m_1},\dots \bar{r}_k\in\mathbb{Z}_{m_k}$

$\exists\, x\in\mathbb{Z}$ 是 $\bar{r}_1\in\mathbb{Z}_{m_1},\dots,\bar{r}_k\in\mathbb{Z}_{m_k}$ 关于自然投影 $\pi_{m_1},\dots,\pi_{m_k}$ 的公共原像

定义：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 $a\equiv b \mod p$

引理5.2　设 $p_1,\dots p_k\in F[x]\setminus\{0\}$ 两两互素

(i) $p_1\cdots p_{k-1}$ 和 p_k 互素

(ii) $\mathrm{lcm}(p_1,\dots p_{k-1},p_k)=p_1\cdots p_{k-1}p_k$.

证明：与引理5.1类似，把整数的Bezout关系用讲义16中定理4.3替代即可

定理5.2　(多项式版的CRT)

设 $p_1,\dots p_k\in F[x]\setminus F$ 两两互素，$r_1,\dots r_k\in F[x]$

则 (i) 存在 $f\in F[x]$ 满足

$$\begin{cases} f\equiv r_1 \mod p_1\\ \quad\vdots\\ f\equiv r_k \mod p_k\end{cases}\qquad (**)$$

(ii) $g\in F[x]$ 满足 (**) $\Leftrightarrow$ $\exists\, h\in F[x]$ 使得

$$g=f+hp_1\cdots p_k.$$

特别地 $\exists!\ r\in F[x]$ 满足(**)且

$$\deg(r)<\deg(p_1\cdots p_k)$$

证：与定理5.1类似，只需把~~整数~~整数除法和Bezout关系，换为多项式除法和Bezout关系即可.

§5.2 多项式插值

定理5.3 设 $\alpha_1,\cdots\alpha_n\in F$ ~~两~~两两不同 $\beta_1,\cdots\beta_n\in F$. 则存在唯一的多项式 $f\in F[x]$ 满足

(i) $f(\alpha_i)=\beta_i,\quad i=1,2,\cdots n$

(ii) $\deg f<n$.

证法1 (线性代数)

设 $f(x)=f_{n-1}x^{n-1}+f_{n-2}x^{n-2}+\cdots+f_0$，其中 $f_{n-1},f_{n-2},\cdots f_0\in F$ 待定

由 $f(\alpha_i)=\beta_i,\quad i=1,\cdots n$ 可得

~~$f_{n-1}\alpha_1^{n-1}+f_{n-2}\alpha$~~

$$f_0+f_1\alpha_i+\cdots+f_{n-1}\alpha_i^{n-1}=\beta_i$$

即

$$\underbrace{\begin{pmatrix}1&\alpha_1&\cdots&\alpha_1^{n-1}\\1&\alpha_2&\cdots&\alpha_2^{n-1}\\&&\cdots&\\1&\alpha_n&\cdots&\alpha_n^{n-1}\end{pmatrix}}_{A}\begin{pmatrix}f_0\\f_1\\\vdots\\f_{n-1}\end{pmatrix}=\begin{pmatrix}\beta_1\\\beta_2\\\vdots\\\beta_n\end{pmatrix}\quad(\star\star)$$

由范德蒙行列式可知 $\det(A)\neq0$

$\Rightarrow(\star\star)$ 有唯一解

证法2 (CRT). ~~由多项式除法~~

~~$f(x)=q_i(x)(x-\alpha_i)+\beta_i.$~~

由余式定理 (讲义16 定理2.4)

$$f(\alpha_i)=\beta_i\Leftrightarrow \mathrm{rem}(f,x-\alpha_i)=\beta_i$$

$$f\equiv\beta_i \mod x-\alpha_i$$

于是 $f(\alpha_i)=\beta_i\Leftrightarrow f\equiv\beta_i$

即：f 满足

$$\begin{cases} f \equiv \beta_1 \mod x-\alpha_1 \\ \quad\vdots \\ f \equiv \beta_n \mod x-\alpha_n \end{cases}$$ 即可

∵ $\alpha_1, \cdots, \alpha_n$ 两两不同 ∴ $x-\alpha_1, \cdots, x-\alpha_n$ 两两互素，由定理 5.2，结论成立 □

例：令 $f \in \mathbb{C}[x]$ 是三次多项式且满足

$$f(0)=9, \quad f(1)=12, \quad f(-1)=6, \quad f(2)=27$$

记 $\alpha_1, \alpha_2, \alpha_3$ 是 $f(x)$ 的三个根，

$$S = \alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_2^2\alpha_1 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 + \alpha_3^2\alpha_2$$

求 S 的值

解 设 $f = f_3x^3 + f_2x^2 + f_1x + f_0$

则 $$\begin{cases} f_0 = 9 \\ f_0 + f_1 + f_2 + f_3 = 12 \\ f_0 - f_1 + f_2 - f_3 = 6 \\ f_0 + 2f_1 + 4f_2 + 8f_3 = 27 \end{cases} \Rightarrow \begin{cases} f_0 = 9 \\ f_1 = 1 \\ f_2 = 0 \\ f_3 = 2 \end{cases}$$

即 $f = 2x^3 + x + 9$

由 §4 例*

$$S = \varepsilon_1(\alpha_1, \alpha_2, \alpha_3)\, \varepsilon_2(\alpha_1, \alpha_2, \alpha_3) - 3\alpha_1\alpha_2\alpha_3$$

$$= \left(-\frac{f_2}{f_3}\right)\left(\frac{f_1}{f_3}\right) + 3\frac{f_0}{f_3} = 3\frac{f_0}{f_3} = \frac{27}{2}$$

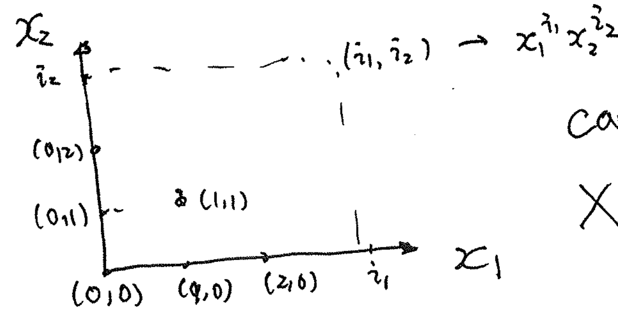
§5.3 关于单项式的计数

问题：设 $X_n^{(m)} = \{ M \in X_n \mid \deg(M) < m \}$

计算 $\mathrm{card}(X_n^{(m)})$

例 $n=1$, $X_1^{(0)} = \emptyset$, $X_1^{(m)} = \{1, x_1, \cdots, x_1^{m-1}\}$

$$\mathrm{card}(X_1^{(m)}) = m$$



$$\mathrm{card}(X_2^{(0)}) = 0$$

$$X_2^{(1)} = \{1\}$$

$X_2^{(2)}=\{1, x_1, x_2\}$ card$(X_2^{(2)})=0+1+2=3$

$X_2^{(3)}=\{1, x_1, x_2, x_1^2, x_1x_2, x_2^2\}$, card$(X_2^{(3)})$

$=0+1+2+3=6$

注意 次数为d的二元单项式是

$x_1^d,\ x_1^{d-1}x_2,\ \dots,\ x_1x_2^{d-1},\ x_2^d$

共 d+1个

card$(X_2^{(m)})=0+1+2+\dots+m-1=\frac{m(m+1)}{2}$

引理5.3 设S是方程

$$z_0+z_1+\dots+z_n=m+n \quad (*)$$

的正整数解的集合，则 card$(S)=$card$(X_n^{(m)})$

证: 当 $m=0$ 时, $S=\emptyset$, $X_n^{(m)}=\emptyset$.

引理成立

设 $m>0$

$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\in X_n^{(m)} \iff i_1+i_2+\dots+i_n<m$

且 $i_1, i_2, \dots, i_n\in\mathbb{N}$

$\iff (i_1+1)+\dots+(i_n+1)<m+n$, $i_1,\dots,i_n\in\mathbb{N}$

$\iff \exists\, i_0\in\mathbb{N}$, $(i_0+1)+(i_1+1)+\dots+(i_n+1)=m+n$ 且

$i_1,\dots,i_n\in\mathbb{N}$

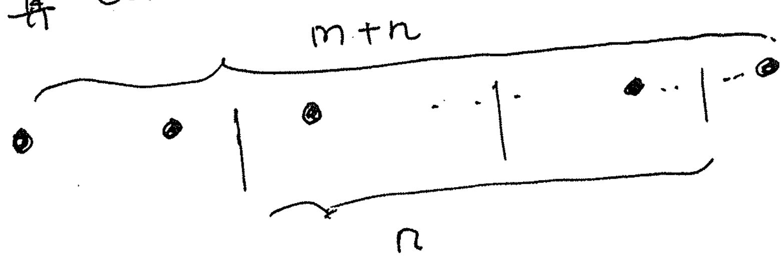
即 $x_1^{i_1}\cdots x_n^{i_n}\in X_n^{(m)} \iff$ ~~$\exists i_0\in\mathbb{N}$ 使得~~

$(i_0+1, i_1+1, \dots, i_n+1)\in S$

其中 $i_0=m-(i_1+\dots+i_n)-1$

于是 card$(X_n^{(m)})=$card(S). ▨

计算 card(S)



$$\text{card}(S)=\binom{m+n-1}{n}$$

例. $n=2$ 时 card$(S)=\binom{m+1}{2}=\frac{m(m+1)}{2}$