回忆：设 $(R,+,0,\cdot,1)$ 是交换环

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

也是交换环，称为 R 上关于 x 的一元多项式环，

其中 $f=\sum_{i=0}^{d} f_i x^i$

代表无穷序列

$(f_0,f_1,\cdots f_d\ 0,0\cdots\cdots)$

特别地：$R[x]$ 中的加法单位是

$(0,0,\cdots\cdots\cdots)$

乘法单位是

$(1,0,0,\cdots\cdots)$

x^i 是

$(0,\cdots 0,1,0\ 0\cdots\cdots)$

$\hookrightarrow i$ （从左到右从零数起）

定义：当 $0\le i\le d$ 时 我们称 f_i 是

f 中关于 x^i 的系数（coefficient）

当 $i>d$ 时，f 中关于 x^i 的系数是 0

命题 2.1 设 $f,g\in R[x]$

$f=g \iff \forall i\in\mathbb{N}$，$f$ 和 g 中关于 x^i 的系数都相同。特别地，

$f=0 \iff \forall i\in\mathbb{N}$，$f$ 关于 x^i 的系数为 0

证：设 f 和 g 关于 x^i 的系数分别是 f_i 和 g_i

则 $f=(f_0,f_1,\cdots\cdots)$，$g=(g_0,g_1,\cdots)$

$f=g \iff f_i=g_i,\ \forall i\in\mathbb{N}$. ☒

注：称 x 是未定元（indeterminate）

注：北大：x 是一个符号（或文字）

北航：x 是一个字母（或未定元）

科大：x 是未定元。

§2.2 多项式的计算

定义：设 $f=f_d x^d+f_{d-1}x^{d-1}+\cdots+f_0\in R[x]$

其中 $f_d,f_{d-1},\cdots f_0\in R$ 且 $f_d\neq 0$

则称 d 是 f 关于 x 的次数，记作 $\deg_x(f)$ 或

$\deg(f)$。f_d 是 f 的首项系数，记作

$\mathrm{lc}_x(f)$ 或 $\mathrm{lc}(f)$。

(deg = degree . lc = leading coefficient)

特别地. 0 的次数定义为 $-\infty$, 其首项系数

记为 0.

记 $\sigma: R \hookrightarrow R[x]$

$r \longmapsto (r, 0, 0 \cdots\cdots)$

σ 是单的环同态. 于是 R 可以理解为

$R[x]$ 的子集. 由沿用符号: 把 $(r, 0 \cdots 0)$

记 rx^0 记为 r. 特别地 0 记为 0, 单

记为 1.

命题2.2 设 $f, g \in R[x]$

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

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

证: 当 f 或 g 为零时. 命题显然成立

设 $f = f_d x^d + f_{d-1} x^{d-1} + \cdots + f_0$

$g = g_e x^e + g_{e-1} x^{e-1} + \cdots + g_0$

其中 $f_d \neq 0$, $g_e \neq 0$.

不妨设 $d \geq e$

则 当 $d > e$ 时 $\deg(f+g) = d$

当 $d = e$ 时

$f+g = (f_e + g_e) x^e + (f_{e-1} + g_{e-1}) x^{e-1} + \cdots + f_0 + g_0$

$\deg(f_e + g_e) \leq e = d$.

于是 $\deg(f, g) \leq \max(d, e)$

fg 的最高次项之多是 $f_d g_e x^{e+d}$.

于是 $\deg(fg) \leq d + e$ ☐

推论2.1 沿用命题2.2中的符号.

若 $lc(f)$ 或 $lc(g)$ 不是 R 中的零因子时

$\deg(fg) = \deg(f) \cdot \deg(g)$

$lc(fg) = lc(f)\, lc(g)$

证: 沿用命题2.2中证明的符号.

$lc(f) = f_d$, $lc(g) = g_e$.

不妨设 $f_d \in R$ 不是零因子. 当 $g_e \neq 0$ 时

$f_d g_e \neq 0$. 则于是 fg 中的最高

项是 $f_d g_e x^{e+d}$. ~~命题成立~~ 推论成立

当 $g = 0$ 时. ~~命题~~ 推论由定义直接导出 ☐

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

计算 $f+g$. fg

$$f+g = 2x^2+1 + (-2x^2-x+1) = -x+2$$

$$fg = (2x^2+1)(-2x^2-x+1)$$

$$= -2x^2(2x^2+1) - x(2x^2+1) + (2x^2+1)$$

$$= -4x^4-2x^3-x+1.$$

例：设 $f=\bar{2}x+\bar{1} \in \mathbb{Z}_4[x]$. 计算 f^2

$$f^2=(\bar{2}x+\bar{1})^2 = (\bar{2}x)^2+2(\bar{2}x)\cdot\bar{1}+\bar{1}^2$$

$$=\bar{4}x^2+\bar{4}x+\bar{1} = \bar{1}.$$

定理 2.1 如果 R 是（交换的）整环，

则 $R[x]$ 也是整环

证：设 $f, g \in R[x]$. $f\neq 0$, $g\neq 0$

则 $lc(f), lc(g) \in R\setminus\{0\}$. 不是零因子

由推论 2.1 $\deg(fg)=\deg(f)+\deg(g)\geq 0$

于是 $fg\neq 0$. $\boxed{}$

§2.3 多项式赋值

例：设 $f(x)=\sum_{i=0}^{d} f_i x^i \in \mathbb{R}[x]$，$r\in\mathbb{R}$

定义：$f(r) = \sum_{i=0}^{d} f_i r^i$

$$f(x): \mathbb{R} \longrightarrow \mathbb{R}, \quad r \longmapsto f(r)$$

例：当 $x=15$ 时 计算 $(x-2)(x+2)$ 的值

方法1：$(x-2)(x+2)=x^2-4 \Rightarrow$ 值为 $15^2-4=221$

方法2：值 $=(15-2)(15+2)=13\times 17=221$.

定理 2.2 设 $(R,+,0\cdot 1)$ 和 $(T,+,0_T\cdot 1_T)$ 是两个交换环. $\varphi: R\longrightarrow T$ 是环同态.

设 $t\in T$. 则 $\exists!$ 环同态 $\varphi_t: R[x]\longrightarrow T$

满足 $\varphi_t|_R=\varphi$ 且 $\varphi_t(x)=t$.

例：设 $R=T=\mathbb{R}$ $\quad \varphi: \mathbb{R}\to\mathbb{R},\ a\mapsto a$

令 $t=r$. 由定理 2.2，$\exists$ 环同态

$\varphi_r: \mathbb{R}[x]\longrightarrow\mathbb{R}$ 满足 $\varphi_r|_{\mathbb{R}}$ 是恒同

映射，$\varphi_r(x)=r$.

$$\varphi_r(f)=\varphi_r\left(\sum_{i=0}^{d} f_i x^i\right)$$
$$=\left(\sum_{i=0}^{d}\varphi_r(f_i x^i)\right)=\sum_{i=0}^{d}\varphi_r(f_i)\varphi_r(x^i)$$
$$=\sum_{i=0}^{d} f_i r^i = f(r)$$

$\forall\, f.g \in \mathbb{R}[x]$，$\underset{\substack{\parallel \\ (f+g)(r)}}{\varphi_r(f+g)} = \varphi_r(f)+\varphi_r(g) = f(r)+g(r)$

同理 $\underset{\substack{\parallel \\ (fg)(r)}}{\varphi_r(fg)} = \varphi_r(f)\varphi_r(g) = f(r)\,g(r)$

定理2.2 的证明：

$$\varphi_t : R[x] \longrightarrow T$$
$$f=\sum_{i=0}^{d} f_i x^i \longmapsto \sum_{i=0}^{d}\varphi(f_i)t^i$$

由命题2.1 和同态φ，φ_t 是良定义的.

设 f 如上，$g=\sum_{j=0}^{e} g_j x^j \in R[x]$ 且 $d\geqslant e$

把 g 改写为 $g=\sum_{i=0}^{d} g_i x^i$，其中

$g_d=\cdots=g_{e+1}=0$

$$\varphi_t(f+g)=\varphi_t\left(\sum_{i=0}^{d}(f_i+g_i)x^i\right)$$
$$=\sum_{i=0}^{d}\varphi(f_i+g_i)t^i \qquad (\varphi_t \text{ 的定义})$$
$$=\sum_{i=0}^{d}[\varphi(f_i)+\varphi(g_i)]t^i \qquad (\varphi: R\to T \text{ 是同态})$$
$$=\sum_{i=0}^{d}\varphi(f_i)t^i+\sum_{i=0}^{d}\varphi(g_i)t^i$$
$$=\varphi_t(f)+\varphi_t(g). \qquad (*)$$

$\forall\, i\in\{0,1,\dots e\}$
$$\varphi_t(f_i x^i g)=\varphi_t\left(\sum_{j=0}^{e} f_i g_j x^{i+j}\right)$$
$$=\sum_{j=0}^{e}\varphi(f_i g_j)t^{i+j}$$
$$=\sum_{j=0}^{e}\varphi(f_i)\varphi(g_j)t^{i+j}$$
$$=\left[\sum_{j=0}^{e}\varphi(g_j)t^j\right]\varphi(f_i)t^i$$
$$=\varphi_t(f_i x^i)\ \varphi_t(g)$$

于是 $\varphi_t((f_i x^i)g)=\varphi_t(f_i x^i)\,\varphi_t(g)$ (**)

$$\varphi_t(fg)=\varphi_t\left(\sum_{i=0}^{d}(f_i x^i)g\right)$$
$$=\sum_{i=0}^{d}\varphi_t(f_i x^i g) \qquad [\ \varphi_t\ \text{~~保持~~}\ (*)\ ]$$

$$= \sum_{i=0}^{d} \varphi_t(\cancel{f_i} x^i)\varphi_t(g) \qquad (**)$$

$$= \left[\sum_{i=0}^{d} \varphi(f_i) t^i\right] \varphi_t(g) = \varphi_t(f)\ \varphi_t(g)$$

$$\varphi_t(1) = \varphi(1) = 1_T$$ 于是 φ_t 是同态

唯一性自己验证，~~一见~~最后一页 ☒

例：设 $f \in \mathbb{Z}[x]$, $n \in \mathbb{Z}^+ \setminus \{1\}$

$\forall m \in \mathbb{Z}$, $\overline{m}$ 代表 m 在 $\mathbb{Z}_n$ 中的同余类. 设 $f = \sum_{i=0}^{d} f_i x^i$.

~~$f: \mathbb{Z} \to \mathbb{Z}_n$, $m \mapsto \sum_i$~~

定义：$f(\overline{m}) = \sum_{i=0}^{d} \overline{f_i}\ \overline{m}^i$

证明 $\forall g \in \mathbb{Z}$. $f(\overline{m})\, g(\overline{m}) = (fg)(\overline{m})$

证：$\pi: \mathbb{Z} \to \mathbb{Z}_n$ 环同态
$a \mapsto \overline{a}$

$$\pi_{\overline{m}}: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_n$$
$$f \mapsto \sum_{i=0}^{d} \pi(f_i)\, \overline{m}^i = \sum_{i=0}^{d} \overline{f_i}\, \overline{m}^i = f(\overline{m})$$

是环同态

$$fg(\overline{m}) = \pi_{\overline{m}}(fg) = \pi_{\overline{m}}(f)\,\pi_{\overline{m}}(g)$$
$$= f(\overline{m})\, g(\overline{m})$$ ☒

引理2.1 设 F 是域. $A \in M_n(F)$.
定义：$F[A] = \left\{ \sum_{i=0}^{d} f_i A^i \,\middle|\, f_i \in F,\ d \in \mathbb{N} \right\}$
则 $F[A]$ 是 $M_n(F)$ 中的交换子环.
（注：$A^0 = E$. $M_n(F)$ 中的 n 阶单位阵）

证：$O_{n\times n}$, $E \in F[A]$
设 $U, V \in F[A]$. 可直接验证：
$U \pm V$, $UV \in F[A]$.
注意到 $\forall \alpha, \beta \in F$ $\quad \alpha A^i \beta A^j = \alpha\beta A^{i+j}$
$= \beta A^j \alpha A^i$.

由此可知 $F[A]$ 乘法交换.

命题2.3. 利用引理2.1中记号. 设 $f = \sum_{i=0}^{d} f_i x^i \in F[x]$
令 ~~$f(A)$~~ $f(A) = \sum_{i=0}^{d} f_i A^i$

证明 $\forall f, g \in F[x]$
$$f(A) + g(A) = (f+g)(A)$$
$$f(A)\, g(A) = fg(A).$$

证: $\theta: F \longrightarrow F[A]$

$\alpha \longmapsto \alpha E$

可直接验证. θ 是环同态.

由定理2.2 存在 θ_A 环同态

$\theta_A: F[x] \longrightarrow F[A]$ 满足 $\theta_A|_F=\theta$

且 $\theta_A(x)=A$

$$\theta_A(f) = \theta_A\left(\sum_{i=0}^{d} f_i x^i\right)$$

$$= \sum_{i=0}^{d} \theta_A(f_i)\theta_A(x^i) = \sum_{i=0}^{d} \theta(f_i)\theta_A(x)^i$$

$$= \sum_{i=0}^{d} f_i E A^i = \sum_{i=0}^{d} f_i A^i = f(A)$$

$$\theta_A(fg) = \theta_A(f)\theta_A(g) = f(A)g(A)$$

$\shortparallel$

$(fg)(A)$

同理 $(f+g)(A) = f(A)+g(A)$. □

例: $A=\begin{pmatrix}0&2\\2&0\end{pmatrix}$ ~~计算~~ $f=x^2$, $g=x^2-4$

计算 $f(A)$ 和 $g(A)$

$$f(A) = A^2 = \begin{pmatrix}0&2\\2&0\end{pmatrix}\begin{pmatrix}0&2\\2&0\end{pmatrix} = \begin{pmatrix}4&0\\0&4\end{pmatrix}$$

$$g(A) = A^2-4A^0 = A^2-4E = \begin{pmatrix}4&0\\0&4\end{pmatrix}-\begin{pmatrix}4&0\\0&4\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$$

注1: 代入矩阵时, 零次系数变为
该系数乘E

注2: $f_d A^d + \dots + f_1 A + f_0 E = O_{n\times n}$

$\not\Rightarrow f_d = \dots = f_1 = f_0 = 0$

§2.4 多项式的带余除法

引理2.2 设 $f, g \in R[x]$ 且 $g \neq 0$

如果 $lc(g)$ 可逆, 则存在唯一的

$q, r \in R[x]$ 使得

(i) $f = qg + r$

(ii) $\deg r < \deg g$.

证: 存在性. 当 $\deg(f) < \deg(g)$ 时

取 $q=0$, $r=f$ 即可

设 $\deg(g)=e$, $\deg(f)=e+k$, $k\geq 0$

令 $g = g_e x^e + g_{e-1}x^{e-1} + \dots + g_0$

其中 g_e 可逆

对 k 归纳：当 $k=0$ 时

$$f = f_e x^e + f_{e-1}x^{e-1} + \cdots + f_0$$

$$f - f_e g_e^{-1} g = f_e x^e + f_{e-1}x^{e-1} + \cdots + f_0 - (f_e x^e + f_e g_e^{-1} g_{e-1} x^{e-1} + \cdots + f_e g_e^{-1} g_0)$$

$$= (f_{e-1} - f_e g_e^{-1} g_{e-1}) x^{e-1} + \cdots + (f_0 - f_e g_e^{-1} f_0)$$

$=: r$

则 $\deg(r) < e$. 令 $q = f_e g_e^{-1}$ 则

$f = q g + r$. 引理成立.

设 $\deg(f) - \deg(g) < k$ 时 引理成立

考虑 $\deg(f) = e+k$ 的情形. 此时

$$f = f_{e+k} x^{e+k} + f_{e+k-1} x^{e+k-1} + \cdots + f_0$$

$$f - f_{e+k} g_e^{-1} x^k g = f - (f_{e+k} x^{e+k} + f_{e+k} g_e^{-1} g_{e-1} x^{e+k-1} + \cdots + f_{e+k} g_e^{-1} g_0 x^k) =: h$$

则 $\deg(h) < e+k$.

由归纳假设 $\exists\, p, r \in R[x]$ 使得

$h = pg + r$. 其中 $\deg(r) < \deg g$

于是

$$f = f_{e+k} g_e^{-1} x^k g + h$$
$$= f_{e+k} g_e^{-1} x^k g + pg + r$$
$$= (f_{e+k} g_e^{-1} x^k + p) g + r$$

令 $q = f_{e+k} g_e^{-1} x^k + p$ 即可. 存在性成立

设 $f = ug + v$, 其中 $u, v \in R[x]$

$\deg v < \deg g$.

则 $qg + r = ug + v$

$(q-u)g = v + r$

如果 $q - u \neq 0$. 则由推论2.1

$\deg((q-u)g) = \deg(q-u) + \deg(g) \geq e$

而 $\deg(v+r) < e$ 与 $(q-u)g = v+r$ 矛盾

于是 $q - u = 0 \Rightarrow v = r$. ∎

注 称 r 为 f 关于 g 的余式
q …… 商.

定理2.2 的唯一性验证：

设 $\psi: R[x] \longrightarrow T$ 满足

(i) $\psi|_R = \varphi$ (ii) $\psi(x) = t$

且 ψ 是环同态。

$\forall\ f = f_d x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in R[x],\ f_i \in R$

$$\psi(f) = \psi\left(\sum_{i=0}^{d} f_i x^i\right)$$

$$= \sum_{i=0}^{d} \psi(f_i)\psi(x^i) \quad (\because \psi \text{是同态})$$

$$= \sum_{i=0}^{d} \varphi(f_i)\, t^i \quad \left(\because \begin{array}{c}\psi(f_i)=\varphi(f_i)\\ \psi(x)=t\end{array}\right)$$

$$= \varphi_t(f)$$

于是 $\psi = \varphi_t$ 唯一性验证完