回忆：设 R 是交换环，R 上的一元多项式也是交换环

设 $f = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_0$

$g = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_0$

则 $fg = f_m g_n x^{m+n} + (f_m g_{n-1} + f_{m-1} g_n) x^{m+n-1} + \cdots$

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

且当 $f_m g_n \neq 0$ 时

$\deg(fg) = \deg(f) + \deg(g)$.

定理2.1 设 R 是整环，则 $R[x]$ 也是整环

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

$$fg = \big(lc(f)\,lc(g)\big)x^{\deg(f)+\deg(g)} + \text{低次项}$$

$\because lc(f) \neq 0$, $lc(g) \neq 0$, R 是整环

$\therefore lc(f)\,lc(g) \neq 0$

于是 ~~$\deg(fg) = \deg(f) + \deg(g)$~~ $fg \neq 0$.

注：由 (*) 和条件 R 是整环可得

$\forall f, g \in R[x] \setminus \{0\}$,

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

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

§2.2 赋值同态

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

$r \in \mathbb{R}$ $\quad f(r) = \sum_{i=0}^{d} f_i r^i$

设 $f(x) = (x-2)(x+2)$ 求 $f(15)$

法1 $f(x) = x^2 - 4$ $\quad f(15) = 15^2 - 4 = 221$

法2： $f(x) = (15-2)(15+2) = 13 \times 17 = 221$

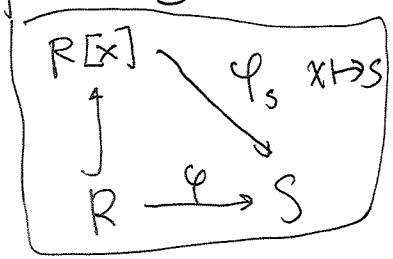
定理2.3 设 $(R, +, 0, \cdot, 1)$ 和 ~~$S \in R$~~ $(S, +, 0_S, \cdot, 1_S)$ 是两个交换环

$\varphi: R \to S$ 是环同态. 设 $s \in S$

则 $\exists!$ 环同态 $\varphi_s: R[x] \to S$ 满足

(i) $\varphi_s|_R = \varphi$

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



证： $\varphi_s: R[x] \to S$

$$f(x) = \sum_{i=0}^{d} f_i x^i \mapsto \sum_{i=0}^{d} \varphi(f_i) s^i$$

良定义验证：由引理2.2. $f(x)$ 可以唯一地写成 $\sum_{i=0}^{d} f_i x^i$. 于是 φ_s 是良定义的.

当 $f=f_0$ 时 $\varphi_S(f)=\varphi(f_0)$

$\Rightarrow \varphi_S|_R=\varphi$

当 $f=x$ 时 $\varphi_S(f)=\varphi(1)S=1_S S=S$

于是 φ_S 满足定理中的两个要求.

下面验证 φ_S 是环同态. $\varphi_S(0)=0_S$

设 $f(x)=f_m x^m+f_{m-1}x^{m-1}+\cdots+f_0$

$g(x)=g_n x^n+g_{n-1}x^{n-1}+\cdots+g_0$, $f_i, g_j\in R$

$f_m\neq 0$, $g_n\neq 0$ $\quad m\geq n$

$g(x)=g_m x^m+\cdots+g_{n+1}x^{n+1}+g_n x^n+\cdots+g_0$

其中 $g_m=\cdots=g_{n+1}=0$

$$\varphi_S(f+g)=\varphi_S\left(\sum_{i=0}^{m}(f_i+g_i)x^i\right)$$

$$=\sum_{i=0}^{m}\varphi(f_i+g_i)S^i \quad [\varphi_S\text{ 的定义}]$$

$$=\sum_{i=0}^{m}(\varphi(f_i)+\varphi(g_i))S^i \quad [\varphi\text{ 是同态}]$$

$$=\sum_{i=0}^{m}\varphi(f_i)S^i+\sum_{i=0}^{m}\varphi(g_i)S^i \quad [\text{分配}]$$

$$=\varphi_S(f)+\varphi_S(g) \quad [\varphi_S\text{ 的定义}]$$

验证: $\varphi_S(fg)=\varphi_S(f)\varphi_S(g)$

先证: $\varphi_S(f_i x^i g)=\varphi_S(f_i x^i)\varphi_S(g)$ (*)

$$\text{左}=\varphi_S\left(\sum_{j=0}^{n}f_i g_j x^{i+j}\right)$$

$$=\sum_{j=0}^{n}\varphi(f_i g_j)S^{i+j} \quad [\varphi_S\text{ 的定义}]$$

$$=\sum_{j=0}^{n}\varphi(f_i)\varphi(g_j)S^{i+j} \quad [\varphi\text{ 是同态}]$$

$$=\varphi(f_i)S^i\sum_{j=0}^{n}\varphi(g_j)S^j \quad [\text{分配律}]$$

$$=\varphi_S(f_i x^i)\varphi(g) \quad [\varphi_S\text{ 的定义}]$$

(*) 成立.

$$\varphi_S(fg)=\varphi_S\left(\sum_{i=0}^{m}(f_i x^i g)\right) \quad [\text{分配}]$$

$$=\sum_{i=0}^{m}\varphi_S(f_i x^i g) \quad [\varphi_S\text{ 保持加法}]$$

$$= \sum_{i=0}^{m} \varphi_S(f_i x^i)\,\varphi_S(g) \qquad [(*)]$$

$$= \left[\sum_{i=0}^{m} \varphi(f_i)\, s^i\right] \varphi_S(g) \qquad [\text{分配律和 } \varphi_S \text{ 定义}]$$

$$= \varphi_S(f)\,\varphi_S(g) \qquad [\varphi_S \text{ 定义}]$$

$\varphi_S(1) = \varphi(1) = 1_S$. φ 是同态

唯一性：设 $\psi: R[x] \to S$ 是环同态

满足上述条件. $\forall f \in R[x]$, $f = \sum_{i=0}^{m} f_i x^i$

$$\psi(f) = \sum_{i=0}^{m} \psi(f_i x^i) = \sum_{i=0}^{m} \psi(f_i)\psi(x^i)$$

$$= \sum_{i=0}^{m} \varphi(f_i)\, s^i = \varphi(f)$$

于是 $\psi = \varphi$ ▨

推论2.1 设 $n \in \mathbb{Z}^+$, $n > 1$. $\pi: \mathbb{Z} \to \mathbb{Z}_n$

是商映射, $\bar{m} \in \mathbb{Z}_n$

则 $\pi_{\bar{m}}: \mathbb{Z}[x] \to \mathbb{Z}_n$

$f(x) \mapsto f(\bar{m})$

是环同态

例：设 $f = x^2 - 4 \in \mathbb{Z}[x]$, $\bar{3} \in \mathbb{Z}_5$

求 $f(\bar{3})$

解：$f(\bar{3}) = \bar{3}^2 - \bar{4} = \bar{9} - \bar{4} = \bar{5} = \bar{0}$

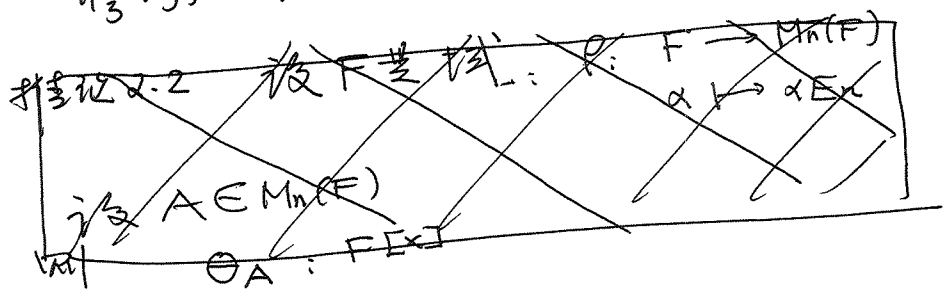
$f = (x-2)(x+2)$

$f(\bar{5}) = (\bar{3}-\bar{2})(\bar{3}+\bar{2}) = \bar{1}\cdot\bar{5} = \bar{0}$

设 $g = (179x - 286)(813x - 857)$

求 $g(\bar{3})$

$\pi_{\bar{3}}(g) = (\bar{4}\cdot\bar{3} - \bar{1})(\bar{3}\cdot\bar{3} - \bar{2}) = \bar{11}\cdot\bar{7} = \bar{4}\cdot\bar{2} = \bar{2}$



推论2.2 设 F 是域，$A \in M_n(F)$

$$\rho: F \to F[A], \quad \alpha \mapsto \alpha E_n$$

则 $\rho_A: F[x] \to F[A]$ 是环同态

$$\sum_{i=0}^{m} f_i x^i \mapsto \sum_{i=0}^{m} f_i A^i$$

证：由定理2.2 只需证 ρ 是环同态

$\forall \alpha, \beta \in F \quad \rho(\alpha+\beta) = (\alpha+\beta)E_n$

$= \alpha E_n + \beta E_n = \rho(\alpha) + \rho(\beta)$.

$\rho(\alpha\beta) = \alpha\beta E_n = \alpha E_n \beta E_n = \rho(\alpha)\rho(\beta)$

$\rho(1) = 1 \cdot E_n = E_n$. ☒

例：设 $x^2 - 4 \in \mathbb{R}[x]$. $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ 求 $f(A)$

解 $f(A) = A^2 - 4E_2 = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} - \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$

$= \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$

$f(x) = (x-2)(x+2) = (A-2E_2)(A+2E_2)$

$= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$

§2.3 一元多项式的除法

定理2.3 设 $f, g \in R[x]$, $g \neq 0$ 且 $lc(g)$ 可逆，则 $\exists!\ q, r \in R[x]$ 使得 $f = qg + r$ 且 $\deg(r) < \deg(g)$.

证：(存在性) 当 $\deg(f) < \deg(g)$ 时 $f = 0 \cdot g + f$ 存在性成立

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

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

$g = g_n x^n + g_{n-1}x^{n-1} + \cdots + g_0$

其中 $f_i, g_j \in R$, $f_{n+k} \neq 0$, g_n 可逆

对 k 归纳

$k=0$. $f = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0$

$f - (f_n g_n^{-1})g = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0$

$- (f_n x^n + (f_n g_n^{-1} g_{n-1})x^{n-1} + \cdots + f_n g_n^{-1} g_0)$

$= \underbrace{(f_{n-1} - f_n g_n^{-1} g_{n-1})x^{n-1} + \cdots + (f_0 - f_n g_n^{-1} g_0)}_{r}$.

$\deg r < n$.

则 $f = \underbrace{(f_n g_n^{-1})}_{q} g + r$.

设 $\deg(f) - \deg(g) < k$ 时对存在性成立.

当 $\deg(f) - \deg(g) = k$.

令 $h = f - (f_{n+k} g_n^{-1} x^k) g$

$= (f_{n+k-1} - f_{n+k} g_n^{-1} g_{n-1})x^{n+k-1} + \cdots + f_{n+k} g_n^{-1} g_0 x^k$

$\deg(h) < n+k$

由归纳假设和 $\deg(f) < \deg(g)$ 的结论

$\exists \tilde{q}, r \in R[x]$ 使得

$f = \tilde{q} g + r$ 且 $\deg(r) < \deg(g)$

$f = (f_{n+k} g_n^{-1} x^k + \tilde{q}) g + r$.

存在性成立

唯一性. 设 $f = q^* g + r^*$, 其中

$q^*, r^* \in R[x]$, $\deg r^* < \deg g$

则 $(q - q^*) g + r - r^* = 0$

$\Rightarrow (q - q^*) g = r^* - r$ (命题2.2)

$\because lc(g)$ 可逆 $\therefore \deg(q - q^*) + \deg(g) = \deg(r - r^*)$

$\Rightarrow \because \deg(g) = n$. $\deg(r - r^*) < n$

$\therefore q - q^* = 0$ $r - r^* = 0$ 证毕

例: 设 $f = x^3 + 2x + 1$, $g = 2x^2 + 1 \in \mathbb{Q}[x]$

求

定义: 设 f、g 如定理2.3.

则 q 称为 f 关于 g 的商

r ... f 关于 g 的余式

记为 $quo(f, g)$ 和 $rem(f, g)$

例: 设 $f = x^3 + 2x + 1$, $g = 2x^2 + 1$ 或 $\in \mathbb{Q}[x]$

求 $quo(f, g)$, $rem(f, g)$

解:

$$\begin{array}{r|l} & \frac{1}{2}x \\ \hline 2x^2+1 & x^3 + 2x + 1 \\ & x^3 + \frac{1}{2}x \\ \hline & \frac{3}{2}x + 1 \end{array}$$

$f = \frac{1}{2}x \cdot g + \frac{3}{2}x + 1$

$quo(f, g) = \frac{1}{2}x$

$rem(f, g) = \frac{3}{2}x + 1$.

结论2.3. 设 F 是域. $\forall f, g \in F[x]$ 且 $g \neq 0$. $quo(f, g)$, $rem(f, g)$ 存在且唯一

证: $\because g \neq 0 \therefore lc(g) \neq 0 \Rightarrow lc(g)$ 可逆 证毕

定理2.4 (余式定理)

设 $f \in R[x]$. $\alpha \in R$. $r = rem(f, x - \alpha)$

则 $r = f(\alpha)$.

证: 由多项式除法

$$f(x) = g(x)(x-\alpha) + r$$

其中 $g \in R[x]$, $r \in R$

由定理2.2 $f(\alpha) = g(\alpha)(\alpha-\alpha) + r = r$ 因

§2.4 多项式的根

定义: 设 F 和 E 是两个域, $F \subset E$

设 $f \in F[x]$, $\alpha \in E$. 如果 $f(\alpha)=0$

则称 α 是 f 在 E 中的一个根

例: $f = x^2 - 2 \in \mathbb{Q}[x]$. f 在 $\mathbb{Q}$ 中无根

f 在 $\mathbb{R}$ 中有两个根 $\pm\sqrt{2}$

定理2.5 设 F 是域, $f \in F[x] \setminus \{0\}$

(i) $\alpha \in F$ 是 f 的根 $\Leftrightarrow$ f 关于 $x-\alpha$ 的余式为0

(ii) 设 f 的次数为 d, 则 f 在域 F 中

至多有 d 个互不相同的根

证: (i) 定理2.4 (余式定理) 的直接

推论

(ii) 对 d 归纳 (20)

当 $d=1$ 时 $f = f_1 x + f_0$. $f_1 \neq 0$

则 f 的唯一根是 $-f_1^{-1} f_0$.

设 $\deg f = d-1$ 时定理成立

$\alpha_1, \cdots \alpha_r$ 是 f 在 F 中 r 个互不相同的根

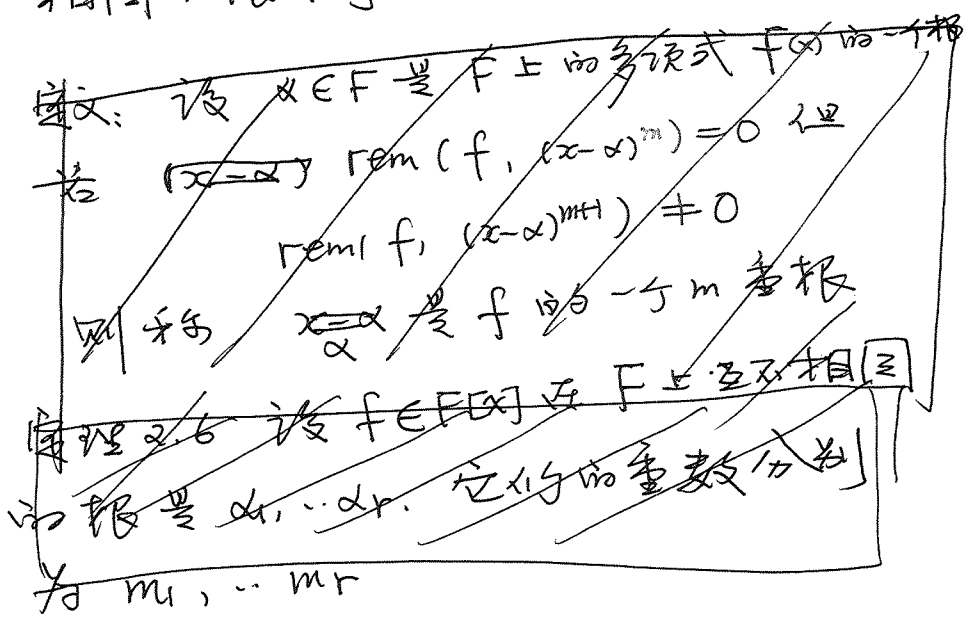
由 (i) $\exists g \in F[x]$ 使得

$$f(x) = g(x)(x-\alpha_r)$$

$\forall i \in \{1, 2, \cdots r-1\}$ $f(\alpha_i) = g(\alpha_i)(\alpha_i - \alpha_r)$

$\because \alpha_i - \alpha_r \neq 0$ 且 F 是域

$\therefore g(\alpha_i) = 0$ 即 $\alpha_1 \cdots \alpha_{r-1}$ 是 g 的互不相同的根, 于是 $r-1 \leq d-1 \Rightarrow r \leq d$. 因



§3 算术学基本定理

定理3.1 设 $n\in\mathbb{Z}^+$, $n>1$.

则 (i) 存在有限个素数 $p_1,\cdots p_k$ (不一定两两不同) 使得

$n=p_1\cdots p_k$ (称为 n 的一个不可约分解)

(ii) 如果 $n=q_1\cdots q_l$ 是另一个不可约分解

则 $k=l$ 且在适当调整顺序后有

$q_1=p_1,\ \cdots,\ p_k=q_k$

证: (i) 见第一章定理8.4

(ii) 设 ~~$p_1=q_1,q_2,\cdots$~~ $k\le l$

由 $p_1p_2\cdots p_k=q_1q_2\cdots q_l$

$p_1\mid q_1q_2\cdots q_l$

~~由~~ 反复应用引理8.2 (第一章)

$\exists j\in\{1,2,\cdots,l\}$.

$p_1\mid q_j$

因为 p_1,q_j 是两个素数. 所以 $p_1=q_j$

适当调整顺序后 可假设 $j=1$

于是 $q_1p_2\cdots p_k=q_1q_2\cdots q_l$

$\Rightarrow$ $p_2p_3\cdots p_k=q_2q_3\cdots q_l$

对 $q_2,q_3\cdots$ 依次运用同样推理可得

$q_2=p_2,\ \cdots\ p_k=q_k$

从而 $1=q_{k+1}\cdots q_l\Rightarrow l=k$ 证毕

推论3.1. 设 $n\in\mathbb{Z}\setminus\{0,1\}$. 则存在 ~~$p_1,\cdots p_s$~~ 互不相同的素数 ~~使得~~ 和 $m_1,\cdots m_s\in\mathbb{Z}^+$, 使得

$$n=p_1^{m_1}\cdots p_s^{m_s}\ \text{或}\ n=-p_1^{m_1}\cdots p_s^{m_s}$$

且 $p_1,\cdots p_s$ 和 $m_1,\cdots m_s$ 都唯一

证: 当 $n>0$ 时 由定理3.1直接可得

当 $n<0$ 时 对 $-n$ 用定理3.1. 证毕

例: $24=2^3\cdot 3$.

§4. 域上一元多项式的因式分解

在本节中，F 是域，特征不限

§4.1. 整除与相伴.

定义：设 $f, g \in F[x]$，$f \neq 0$. 如果存在 $h \in F[x]$ 使得 $g = hf$. 则称 f 是 g 的因子，g 是 f 的倍式，此时记 $f \mid g$.

例：设 $g \in \mathbb{Q}[x]$，$g = x^2 - 1$，$f = x - 1$. $f \mid g$. 注意到 $\forall g \in \mathbb{Q} \setminus \{0\}$，$(gf) \mid g$.

定义：设 $f, g \in F[x]$. 如果存在 $\alpha \in F \setminus \{0\}$ 使得 $f = \alpha g$. 则称 f 和 g 在 F 上相伴（associated），记为 $f \sim_F g$ 或 $f \sim g$.

[自己验证 $\sim_F$ 是等价关系]

命题4.1 设 $f, g \in F[x]$，$f \neq 0$，$g \neq 0$

$r, u, v, w \in F[x]$

(i) $f \mid g$，$g \mid r \Rightarrow f \mid r$

(ii) $f \mid r$，$f \mid u \Rightarrow f \mid (vr + wu)$

证：(i) $f \mid g$，$g \mid r \Rightarrow g = sf$，$r = tg$，其中 $s, t \in F[x] \Rightarrow r = (st)f \Rightarrow f \mid r$

(ii) $r = sf$，$u = tf$，$s, t \in F[x]$

$\Rightarrow vr + wu = (vs + wt)f \Rightarrow f \mid (vr + wu)$.

命题4.2 设 $f, g \in F[x]$，$fg \neq 0$

则 $f \sim g \Leftrightarrow f \mid g$ 且 $g \mid f$

证："$\Rightarrow$" $f \sim g \Leftrightarrow f = \alpha g$，$\alpha \in F \setminus \{0\}$

$\Rightarrow f = \alpha g$ 且 $g = \alpha^{-1} f \Rightarrow f \mid g$ 且 $g \mid f$

"$\Leftarrow$" $f = ug$ 且 $g = vf$，$u, v \in F[x]$

$f = uvf \Rightarrow f(1 - uv) = 0$

$\Rightarrow uv = 1 \Rightarrow u, v \in F \setminus \{0\}$.

$\Rightarrow f \sim g$.

§4.2. 不可约多项式

定义：设 $f \in F[x] \setminus F$. 如果 f 不能写成 $F[x]$ 两个次数大于零的多项式之积，则称 f 是 F 上的不可约多项式.
(或 f 是 $F[x]$ 中 - - - - - -).

例：任何 $F[x]$ 中的一次多项式都是不可约的.

例：x^2-2 在 $\mathbb{Q}[x]$ 中是不可约的.
但在 $\mathbb{R}[x]$ 中是可约的.

$$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$$

例：$x^2+\bar{1}$ 在 $\mathbb{Z}_3[x]$ 中可约

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

命题4.3 设 $f, g \in F[x]$. $\deg(f)>0$, $\deg(g)>0$ 且 f 不可约

则 (i) $f \sim g \Rightarrow g$ 不可约

(ii) $g \mid f \Rightarrow f \sim g$. g 不可约

进而，

证：(i) 设 $f = \alpha g$，其中 $\alpha \in F \setminus \{0\}$

若 $g = g_1 g_2$. 其中 $g_1, g_2 \in F[x]$

则 $f = \alpha g_1 g_2$. 因为 f 不可约. 所以

$\deg(g_1)=0$ 或 $\deg(g_2)=0$

于是 g 不可约

(ii) 设 $f = ug$. 因为 f 不可约且 $\deg(g)>0$

所以 $u \in F^*$ $\Rightarrow f \sim g$ $\Rightarrow g$ 不可约. (由(i)易

定理4.1 设 $f \in F[x]$, $\deg(f)>0$

则存在不可约多项式 $p_1, p_2, \cdots p_s$ 使得

$$f = p_1 p_2 \cdots p_s$$

证：设 $n=\deg(f)$. 对 n 归纳证.

当 $n=1$ 时. f 不可约. 取 $s=1$, $p_1=f$ 即可

设 $\deg(f)<n$ 时定理成立. 当 n 时

若 f 不可约. 则取 $s=1$, $p_1=f$. 否则

$f = gh$. 其中 $\deg(g)>0$, $\deg(h)>0$

于是 $\deg(g)<n$. $\deg(h)<n$

由 - - - deg

由此和归纳假设可得 f 等于若干不可约多项式之积.

§4.3 $F[x]$ 中的最大公因子

定义. 设 $f, g \in F[x]$, $h \in F[x] \setminus \{0\}$

如果 $h \mid f$ 且 $h \mid g$, 则称 h 是 f 和 g 的公因子.

设 h 是 f 和 g 的公因子. 如果 f 和 g 的任何公因子 p, 都有 $p \mid h$, 则称 h 是 f 和 g 的最大公因子.

定理 4.2 设 $f, g \in F[x]$ 且 $g \neq 0$

(i) f 和 g 有最大公因子

(ii) 设 h_1, h_2 是 f 和 g 的两个最大公因子, 则 $h_1 \sim h_2$

(iii) 设 h 是 f 和 g 的最大公因子, 则存在 $u, v \in F[x]$, 使得

$$uf + vg = h.$$

证: 设 $I = \{ sf + tg \mid s, t \in F[x] \}$

令 h 为 I 中非零且次数最小的多项式, 则 $\exists u, v \in F[x]$ 使得

$$uf + vg = h \qquad (*)$$

(注: $\because g \in I$, $\therefore$ h 必然存在)

先证: h 是 f 和 g 的公因子

反设 $h \nmid f$. 则 $r = \mathrm{rem}(f, h) \neq 0$

假设 $f = qh + r$, $-\infty < \deg(r) < \deg(h)$

由 $(*)$, $quf + qvg = qh = f - r$

$$(qu - 1)f + qvg = -r.$$

$\Rightarrow -r \in I$ 但 $\deg(-r) < \deg(h)$ $\rightarrow\leftarrow$

于是 h 是 f, g 的公因子.

再证 h 是最大公因子

设 p 是 f, g 的公因子. 则

$p \mid f$ 且 $p \mid g \Rightarrow p \mid (uf + vg)$ (命题 4.1)

$\Rightarrow p \mid h$. (i) 成立

(ii) 由最大公因子的定义，

$h_1 \mid h_2$ 且 $h_2 \mid h_1$. 于是 $h_1 \sim h_2$ (允差1)

(iii) 由 (*) 直接可得. 证

注. 最大公因子的计算.

给定 $f, g \in F[x]$, $\deg(f) \geq 0$, $\deg(g) \geq 0$

求 f, g 的最大公因子，记为 $\gcd(f,g)$

设 $P_0 = f$, $P_1 = g$

由多项式带余

$P_0 = q_2 P_1 + P_2$, 其中 $q_2 = quo(P_0, P_1)$, $P_2 = rem(P_0, P_1)$

若 $P_2 \neq 0$ $P_1 = q_3 P_2 + P_3$ 其中 $q_3 = quo(P_1, P_2)$, $P_3 = rem(P_1, P_2)$

$\vdots$

$P_{k-2} = q_k P_{k-1} + P_k$ 其中 $q_k = quo(P_{k-2}, P_{k-1})$,

$P_k = rem(P_{k-2}, P_{k-1})$

$P_k \neq 0$

$\because \deg(P_1) > \deg(P_2) > \cdots > \deg(P_k) \geq 0$

又由于设

$$P_{k-1} = q_{k+1} P_k .$$

只证: $P_k = \gcd(f,g)$

$P_k \mid P_k$, $P_k \mid P_{k-1} \Rightarrow P_k \mid P_{k-2}$

$P_k \mid P_{k-1}$, $P_k \mid P_{k-2} \Rightarrow P_k \mid P_{k-3}$

$\cdots$

$P_k \mid P_3$, $P_k \mid P_2 \Rightarrow P_k \mid P_1 = g$

$P_k \mid P_2$, $P_k \mid P_1 \Rightarrow P_k \mid f$

于是 P_k 是 f 和 g 的公因子

设 h 是 f 和 g 的公因子 则

$h \mid P_1$, $h \mid P_2 \Rightarrow h \mid P_3$

$h \mid P_2$, $h \mid P_3 \Rightarrow h \mid P_4$

$\cdots$

$h \mid P_{k-2}$, $h \mid P_{k-1} \Rightarrow h \mid P_k$

于是 P_k 是 f 和 g 的最大公因子

有类似地扩展欧基里德算法计算 $u, v \in F[x]$

使得 $uf + vg = \gcd(f,g)$.

定义：设 $f, g \in F[x]$，$fg \neq 0$，如果 $\gcd(f,g)=1$

则称 f 和 g 互素。

定理 4.3. 设 $f, g \in F[x]$，$fg \neq 0$

则 f 和 g 互素 $\Leftrightarrow \exists u, v \in F[x]$ 使得

$$uf + vg = 1$$

证：由定理 4.2 和互素的定义直接可得

例：设 $f = x^4+\bar{1}$，$g = x^3+\bar{1}$ 是 $Z_2[x]$ 中的多项式，求 $\gcd(f,g)$

设 $p_0 = f$，$p_1 = g$

$$\begin{array}{r|l} x & \\ \hline x^3+\bar{1} & x^4+\bar{1} \\ & x^4+x \\ \hline & x+\bar{1} \end{array} \Rightarrow p_2 = \mathrm{rem}(p_0, p_1) = x+\bar{1}$$

$$\begin{array}{r|l} x^2+x+\bar{1} & \\ \hline x+\bar{1} & x^3+\bar{1} \\ & x^3+x^2 \\ \hline & x^2+\bar{1} \\ & x^2+x \\ \hline & x+\bar{1} \\ & x+\bar{1} \\ \hline & \bar{0} \end{array} \Rightarrow p_3 = \mathrm{rem}(p_1, p_2) = \bar{0}$$

$$\Rightarrow \gcd(f,g) = x+\bar{1}.$$

§4.4 $F[x]$ 中的因式分解（唯一性）

定理 4.4 设 $f \in F[x]$，$\deg(f) > 0$

则存在 α 不可约多项式 $p_1, \cdots p_m \in F[x] \setminus F$

$\alpha \in F \setminus \{0\}$ 使得

$$f = \alpha p_1 \cdots p_m$$

如果 $f = \beta q_1 \cdots q_n$，其中 $\beta \in F \setminus \{0\}$

$q_1, \cdots q_n \in F[x] \setminus F$ 不可约

则 $m=n$，且适当调整下标顺序后

有 $p_1 \sim q_1, \cdots p_m \sim q_m$

欲证该定理，需要

引理 4.1 设 $f \in F[x]$ 不可约，$g, h \in F[x]$

如果 $f \mid gh$，则 $f \mid g$ 或 $f \mid h$

证：设 $f \nmid g$，因为 f 不可约，所以

f 和 g 互素

$\exists u, v \in F[x]$ $uf + vg = 1$. （定理 4.3）

$ufh + vgh = h$，$\Rightarrow$ 由 $f \mid f$ 和 $f \mid gh$

$\Rightarrow f \mid h$（命题 4.1） ☒

定理4.4 的证明

(i) 见定理 4.2

(ii) 我们有

$$\alpha p_1 \cdots p_m = \beta q_1 \cdots q_n \quad (**)$$

不妨设 $m \le n$. 由 (**) 得到

$$p_1 \mid \beta q_1 \cdots q_n$$

反复应用引理 4.1 得到 $j \in \{1, \cdots n\}$ 使得 $p_1 \mid q_j$

不妨设 $j=1$. 由命题 4.3, $p_1 \sim q_1$

设 $p_1 = \beta_1 q_1$. 其中 $\beta_1 \in F$. 由 (**)

$$\alpha \beta_1 q_1 p_2 \cdots p_m = \beta q_1 q_2 \cdots q_n$$

$$\Rightarrow \alpha \beta_1 p_2 \cdots p_m = \beta q_2 \cdots q_n$$

对 $p_2, \cdots p_m$ 依次应用同样的理由得到

$$p_2 \sim q_2, \ \cdots, \ p_m \sim q_m$$

且 $\alpha \beta_1 \cdots \beta_m = \beta q_{m+1} \cdots q_n$

$\because \deg(\alpha \beta_1 \cdots \beta_m) = 0 \ \therefore \deg(q_{m+1} \cdots q_n) \to$

于是 $m = n$. ▨

§4.5 $\mathbb{Q}[x]$ 中的因式分解 (27)

定义: 设 $a \in \mathbb{Z}$ 则定义

$$\gcd(a) = |a|$$

设 $a_1, \cdots a_m \in \mathbb{Z} \setminus \{0\}$

$$\gcd(a_1, a_2, \cdots a_m) := \gcd(a_1, \gcd(a_2 \cdots a_m))$$

引理 4.2: 设 $a_1, a_2, \cdots a_m \in \mathbb{Z} \setminus \{0\}$

$d = \gcd(a_1, a_2 \cdots a_m)$.

则 (i) d 是 $a_1, a_2, \cdots a_m$ 的公因子

(ii) 设 k 是 $a_1, a_2, \cdots a_m$ 的公因子

则 $k \mid d$

证: 当 $m = 1, 2$ 时显然成立. 设 $m-1$ 时成立

$d = \gcd(a_1, \gcd(a_2, \cdots a_m))$

$\Rightarrow d \mid a_1$ 且 $d \mid \gcd(a_2, \cdots a_m)$

$\Rightarrow d \mid a_1$ 且 $d \mid a_i$, $i = 2, \cdots m$ (引理 4.1 的推论)

(ii) 设 $m = 1, 2$ 时成立 设 $m-1$ 时成立

则 $k \mid a_1$, $k \mid \gcd(a_2, \cdots a_m)$

$\Rightarrow k \mid \gcd(a_1, \gcd(a_2, \cdots a_m))$

$\Rightarrow k \mid d$ ▨

即 $\gcd(a_1, \cdots a_m)$ 是 $a_1, \cdots a_m$ 的最大公因子.

定义：设 $a_1, \cdots, a_m \in \mathbb{Z}$，不全为零 则 $\gcd(a_1, \cdots, a_m)$ 是指 $a_1, \cdots a_m$ 中非零整数的(正的)最大公因子.

定义：设 $f \in \mathbb{Z}[x] \setminus \{0\}$，是

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

其中 $f_0, f_1, \cdots f_d \in \mathbb{Z}$，$f_d \neq 0$. 称 $\gcd(f_d, f_{d-1}, \cdots f_0)$ 为 f 的容度. 记为 $\mathrm{cont}(f)$. 当 $\mathrm{cont}(f) = 1$ 时，f 称为本原的.

例：设 $f = 2x^2 + 3x - 2$，$g = 24x^2 + 3x^2 - 12$

$\mathrm{cont}(f) = \gcd(2, 3, -2) = 1$. $\mathrm{cont}(g) = 3$.

引理 4.3 设 p 是素数.

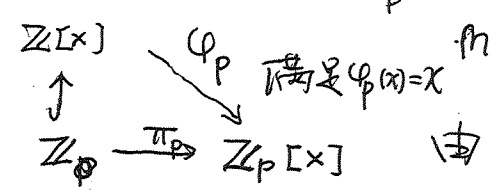
(i) $\varphi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$

$$\sum_{i=0}^{d} f_i x^i \mapsto \sum_{i=0}^{d} \overline{f_i} x^i$$

是环同态，其中 $\overline{f_i}$ 代表 f_i 在 $\mathbb{Z}_p$ 中的等价类

(ii) 若 $g \in \mathbb{Z}[x]$ 本原，则 $\varphi_p(g) \neq \overline{0}$

证：(i)



由赋值同态定理

φ_p 是环同态

(ii) 设 $g = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_0$

$\because \mathrm{cont}(g) = 1 \therefore$ p 不是 $g_0, g_1, \cdots g_n$ 的公因子. 于是 $\exists\, i \in \{0, 1, \cdots n-1\}$ 使得

$p \nmid g_i \Rightarrow \overline{g_i} \neq \overline{0}$

$$\varphi_p(g) = \overline{g}_n x^n + \cdots + \overline{g}_i x^i + \cdots + \overline{g}_0 \neq 0$$

Gauss 引理：设 $f, g \in \mathbb{Z}[x]$. 本原 则 fg 也本原

证：设 fg 不本原. 则 $\mathrm{cont}(fg) > 1$

$\exists$ 素数 p 使得 $p \mid \mathrm{cont}(fg)$. 于是

$\varphi_p(fg) = \overline{0}$. 另一方面

$\varphi_p(fg) = \varphi_p(f)\varphi_p(g) \neq 0$ (引理 4.3)

$\to\leftarrow$ ∎

定义：设 $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$. 如果 f 不能写成两个次数小于 f 的多项式之积，则称 f 在 $\mathbb{Z}$ 上不可约（或在 $\mathbb{Z}[x]$ 中不可约）

定理 4.5 设 $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$. 如果 f 在 $\mathbb{Z}$ 上不可约，则 f 在 $\mathbb{Q}$ 上也不可约.

证：反证：设 设 $f = gh$，其中 $g, h \in \mathbb{Q}[x]$ $\deg(g) < \deg(f)$, $\deg(h) < \deg(f)$

设 $g = \frac{k}{m}\tilde{g}$, $h = \frac{l}{n}\tilde{h}$

其中 $m, n, k, l \in \mathbb{Z}$, $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ 本原

则 $$mnf = kl\tilde{g}\tilde{h}$$

$\Rightarrow \exists u, v \in \mathbb{Z}$, 互素，以使得

$$uf = v\tilde{g}\tilde{h}$$

若 $u > 1$. 则 $\exists$ 素数 p 使得 $p \mid u$

$$\varphi_p(uf) = \varphi_p(u)\varphi_p(f) = \bar{u}\varphi_p(f) = \bar{0}$$

$$\varphi_p(v\tilde{g}\tilde{h}) = \varphi_p(v)\varphi_p(\tilde{g}\tilde{h}) = \bar{v}\varphi_p(\tilde{g}\tilde{h}) \neq \bar{0}$$

（$\varphi_p(v) \neq \bar{0}$ 当因为 $\gcd(p, v) = 1$ $p \nmid v$

$\varphi_p(\tilde{g}\tilde{h})$ 当因为 $\tilde{g}\tilde{h}$ 当本原的 和习题4.3.）矛盾. 图

Eisenstein 判别法 设 $n \geq 1$

设 $f = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \in \mathbb{Z}[x]$ 其中 $f_{n-1}, \cdots, f_1, f_0 \in \mathbb{Z}$. 设 p 为素数，如果 $p \mid f_{n-1}, \cdots, p \mid f_1, p \mid f_0$ 但 $p^2 \nmid f_0$. 则 f 在 $\mathbb{Q}[x]$ 中不可约

证：由假设 f 在 $\mathbb{Q}$ 上可约，由上述定理. $\exists\ g, h \in \mathbb{Z}[x]$ 使得

$$f = gh. \quad (*)$$

不妨设 $lc(g) = lc(h) = 1$. 于是可写为

$$g = x^d + g_{d-1}x^{d-1} + \cdots + g_1 x + g_0$$

$$h = x^e + h_{e-1}x^{e-1} + \cdots + h_1 x + h_0$$

$$\varphi_p(f) = x^n \underset{(*)}{\Rightarrow} x^n = \left(x^d + \bar{g}_{d-1}x^{d-1} + \cdots + \bar{g}_1 x + \bar{g}_0\right)\left(x^e + \bar{h}_{e-1}x^{e-1} + \cdots + \bar{h}_1 x + \bar{h}_0\right)$$

$\Rightarrow$ ~~$\bar{g}_0 \bar{h}_0 = \bar{0}$~~ ⇏

由定理 4.4 $\bar{g}_0 = \bar{0}$ 且 $\bar{h}_0 = \bar{0}$ $\Rightarrow p \mid g_0, p \mid h_0$

矛

由此可知 $g_0 = ap$, $h_0 = bp$, $a, b \in \mathbb{Z}$

$\therefore f_0 = g_0 h_0$ (根据(*))

$\therefore f_0 = ab p^2 \Rightarrow p^2 \nmid f_0$ →←.

例: $\forall n \in \mathbb{Z}^+$, $n > 1$

$x^n + 2x + 2$ 在 $\mathbb{Q}[x]$ 中不可约

证: $2 \mid 2$ 但 $2 \nmid 2^2$

例: 设 p 是素数. 证明

$f(x) = x^p + x^{p-1} + \cdots + 1$ 在 $\mathbb{Q}[x]$ 中不可约

证: $\psi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]$

$g(x) \longmapsto g(x+1)$.

是环同态. 且令

$\theta: \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]$

$g(x) \mapsto g(x-1)$

则 $\psi \circ \theta = \theta \circ \psi = id_{\mathbb{Q}[x]}$ $\Rightarrow$ ψ 是同构

$\because f(x) = \dfrac{x^p - 1}{x - 1}$

$\therefore f(x+1) = \dfrac{(x+1)^p - 1}{x+1-1} = \dfrac{1}{x}\left[(x+1)^p - 1\right]$

$= \cancel{1} x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1}$

$p \mid \binom{p}{1}, \cdots p \mid \binom{p}{p-2}, p \mid \binom{p}{p-1}$

但 $p^2 \nmid \binom{p}{p-1}$.

$\Rightarrow f(x+1)$ 不可约.

$\Rightarrow f(x)$ 不可约 ▨