回忆: $\tilde{R} = \{ (a_0, a_1, \cdots) \mid \begin{matrix} a_0, a_1 \cdots \in R \\ \text{有限个非零} \end{matrix} \}$

$(\tilde{R}, +, \tilde{0})$ 是加法群

符号约定: 设 $\tilde{a} = (a_0, a_1, \cdots)$

$\tilde{a}$ 中第 k 个成员 记为 a_k 或 $\tilde{a}_k$

$$+: \tilde{R} \times \tilde{R} \longrightarrow \tilde{R}$$
$$(\tilde{a}, \tilde{b}) \longmapsto \tilde{c}, \text{ 其中 } c_k = a_k + b_k, k \in \mathbb{N}$$

定义 $\cdot : \tilde{R} \times \tilde{R} \longrightarrow \tilde{R}$

$$(\tilde{a}, \tilde{b}) \longmapsto \tilde{c}$$

其中 $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ (convolution)

背景: $\tilde{a} = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0$

$\tilde{b} = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$

$\tilde{a} \cdot \tilde{b}$ 中 x^k 的系数

是 $a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$

验证 良定义

设 $m \in \mathbb{N}$ 使得 $a_{m+1} = a_{m+2} = \cdots = 0$

$b_{m+1} = b_{m+2} = \cdots = 0$

$\forall k > 2m.$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0$$

$\Rightarrow \tilde{c} \in \tilde{R} \Rightarrow$ "$\cdot$" 良定义

验证 $(\tilde{R}, \cdot, \tilde{1})$ 是交换的含幺半群

其中 $\tilde{1} = (1, 0, 0, \cdots)$

交换: 设 $\tilde{c} = \tilde{a}\tilde{b}$, $\tilde{d} = \tilde{b}\tilde{a}$

$\forall k \in \mathbb{N}$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j \Rightarrow c_k = d_k$$

$(\because R \text{交换})$

$$d_k = \sum_{j=0}^{k} b_j a_{k-j} = \sum_{i+j=k} b_j a_i$$

结合: 设 $\tilde{a}, \tilde{b}, \tilde{c} \in \tilde{R}$

验证 $(\tilde{a}\tilde{b})\tilde{c} = \tilde{a}(\tilde{b}\tilde{c})$

设 $\tilde{p} = \tilde{a}\tilde{b}$, $\tilde{q} = \tilde{b}\tilde{c}$

则 $(\tilde{p}\tilde{c})_m = \sum_{k+l=m} p_k c_m = \sum_{k+l=m}\left(\sum_{i+j=k} a_i b_j\right) c_m$

$= \sum_{k+l=m}\sum_{i+j=k} a_i b_j c_m$ （分配律）

$= \sum_{i+j+l=m} a_i b_j c_m$ （加法交换）

类似 $(\tilde{a}\tilde{q})_m = \sum_{k+l=m} a_k q_l = \sum_{k+l=m} a_k \sum_{i+j=l} b_i c_j$

$= \sum_{i+j+k=m} a_k b_i c_j$

$\Rightarrow (\tilde{p}\tilde{c})_m = (\tilde{a}\tilde{q})_m \Rightarrow (\tilde{a}\tilde{b})\tilde{c} = \tilde{a}(\tilde{b}\tilde{c})$

乘法单位.

$\tilde{a}\cdot\tilde{1} = (a_0, a_1, \cdots)(1, 0, 0\cdots)$.

由 $(\tilde{a}\cdot\tilde{1})_k = \sum_{i+j=k} a_i 1_j$

故 $= a_k$

$\Rightarrow \tilde{a}\cdot\tilde{1} = \tilde{a}$.

分配律

$[\tilde{a}(\tilde{b}+\tilde{c})]_k = \sum_{i+j=k} a_i(b_j+c_j)$

$= \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j = [\tilde{a}\tilde{b}]_k + [\tilde{a}\tilde{c}]_k$

$\Rightarrow \tilde{a}(\tilde{b}+\tilde{c}) = \tilde{a}\tilde{b} + \tilde{a}\tilde{c}$.

由此可知

$(\tilde{R}, +, \tilde{0}, \cdot, \tilde{1})$ 是交换环

令 $x = (0, 1, 0, 0, \cdots)$

$x^0 = \tilde{0}$ [约定]

$x^1 = x$ [约定]

$x^2 = (0, 1, 0, \cdots 0)(0, 1, 0, \cdots 0, \cdots)$

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

设 $x^{n-1} = (\underset{0}{0}, \cdots \underset{n-2}{0}, \underset{n-1}{1}, 0, 0, \cdots)$

则 $x^n = x\,x^{n-1} = (0, 1, 0\cdots 0\cdots)(0, \cdots 0, 1, 0\cdots)$

$= (0, \cdots 0, \underset{n}{1}, 0\cdots)$

~~于是 $\forall \tilde{a} \in \tilde{R}$~~

命题2.1：$\varphi: R \to \tilde{R}$

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

是单的环同态

证：φ 是单射. ✓

设 $a, b \in R$

$\varphi(a+b) = (a+b, 0, 0, \cdots)$

$= (a, 0, 0, \cdots) + (b, 0, 0, \cdots)$

$= \varphi(a) + \varphi(b)$

$\varphi(ab) = (ab, 0, 0, \cdots)$ ~~$(b, 0, 0, \cdots 0)$~~

$= (a, 0, 0, \cdots)(b, 0, 0, \cdots 0)$

$= \varphi(a)\varphi(b)$

$\varphi(1) = (1, 0, 0, \cdots) = \tilde{1}$ 图

注：滥用符号，将

$(r, 0, 0, \cdots)$ 记为 r

则 $r\tilde{a} = (ra_1, ra_2, \cdots, ra_p, \cdots)$. ③

进一步：设 $a_{m+1} = a_{m+2} = \cdots = 0$

$\tilde{a} = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0$

验证：$a_m x^m = (0, \cdots 0, \overset{m}{a_m}, 0, 0, \cdots)$

$a_{m-1} x^{m-1} = (0, \cdots 0, \overset{m-1}{a_{m-1}}, 0, 0, \cdots)$

$\vdots$

$a_0 = (a_0, 0, \cdots 0, \cdots)$

它们之和是 $(a_0, a_1, \cdots a_m, 0, \cdots) = \tilde{a}$

于是 $\tilde{R} = \left\{ \sum_{i=0}^{m} a_i x^i \,\middle|\, m \in \mathbb{N}, a_0, a_1, \cdots a_m \in R \right\}$ 称为 R 上一元多项式环

记为 $R[x]$.

~~定理2.1~~

定理2.1(i) 设 $p \in R[x]$. ~~如果~~ $p = p_d x^d + \cdots + p_1 x + p_0$ $(p_i \in R)$

$p = 0 \iff p_d = \cdots = p_1 = p_0 = 0$

(ii) 设 $p, q \in R[x]$. $q = q_e x^e + \cdots + q_1 x + q_0$ $(q_j \in R)$

$p = q \iff p_{\max(d,e)} = q_{\max(d,e)}, \cdots$

$p_1 = q_1, \quad p_0 = q_0.$

其中 $p_k = 0\ (k > d)$, $q_k = 0, (k > e)$

证: (i) $p=0 \iff (p_0, p_1, \cdots p_d, 0, 0, \cdots)$

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

$$\iff p_0 = p_1 = \cdots = p_d = 0$$

(ii) $p = q \iff (p_0, p_1 \cdots p_d, 0, 0, \cdots)$

$$= (q_0, q_1 \cdots q_e, 0 \cdots 0)$$

$$\iff p_i = q_i, \quad i \in \mathbb{N}. \quad \square$$

定义: 设 $p \in R[x]$

$$p = p_d x^d + p_{d-1} x^{d-1} + \cdots + p_0, \quad p_i \in R$$

且 $p_d \neq 0$

则: d 称为 p 的次数. 记为 $\deg_x(p)$ 或 $\deg(p)$

p_i 称为 x^i 在 p 中的系数. 特别地

p_d 称为 p 的首项系数 记为

$lc_x(p)$ 或 $lc(p)$.

当 $p=0$ 时, $\deg(p) := -\infty$

$lc(p) := 0$.

注: x 在代数上通常称为未定元 (indeterminate) $p \in R[x]$ 称为关于未定元 x 的一元多项式

命题2.4 设 $p, q \in R[x]$

(i) $\deg(p+q) \leq \max(\deg(p), \deg(q))$

当 $\deg(p) \neq \deg(q)$ 时, 等号成立

(ii) $\deg(pq) \leq \deg(p) + \deg(q)$

当 $lc(p)lc(q) \neq 0$ 时, $\deg(pq) = \deg(p) + \deg(q)$

且 $lc(pq) = lc(p)lc(q)$

证: 设 $p = p_d x^d + p_{d-1} x^{d-1} + \cdots + p_0$

$$q = q_e x^e + q_{e-1} x^{e-1} + \cdots + q_0$$

其中 $p_i, q_j \in R$.

不妨设 $d>e$.

则：加法公式

$$p+q = p_d x^d + \cdots + p_{e+1} x^{e+1} + (p_e+q_e) x^e + \cdots + (p_0+q_0)$$

乘法公式

$$pq = (p_d q_e) x^{d+e} + (p_d q_{e-1} + q_e p_{d-1}) x^{d+e-1} + \cdots + \Big(\sum_{i+j=k} p_i q_j\Big) x^k + \cdots + p_0 q_0$$

当 $p=0$ 或 $q=0$ 时 结论(i),(ii) 显然成立.

设 $p\neq 0$, $q\neq 0$, $p_d\neq 0$, $q_e\neq 0$

(i) 由加法公式: $\deg(p+q)\leq d$

当 $d>e$ 时. $\deg(p+q)=e$

(ii) 由乘法公式: $\deg(p+q)\leq d+e$

当 $p_d q_e\neq 0$ 时 $\deg(pq)=d+e$

且 $lc(pq)=p_d q_e$ $\boxtimes$

例: 设 $f=\bar{2}x^2+\bar{3}x+\bar{1}$, $g=\bar{3}x+\bar{4}$ 是 $\mathbb{Z}_6[x]$ 中的多项式. 求 $f+g$ 和 fg

解: $f+g=(\bar{2}x^2+\bar{3}x+\bar{1})+(\bar{3}x+\bar{4})$

$=\bar{2}x^2+\bar{6}x+\bar{5}=\bar{2}x^2+\bar{5}$

$fg=(\bar{2}x^2+\bar{3}x+\bar{1})(\bar{3}x+\bar{4})$

$=(\bar{2}x^2+\bar{3}x+\bar{1})(\bar{3}x)+(\bar{2}x^2+\bar{3}x+\bar{1})\bar{4}$

$=\bar{6}x^3+\bar{9}x^2+\bar{3}x+\bar{8}x^2+\overline{12}x+\bar{4}$

$=\bar{3}x^2+\bar{3}x+\bar{2}x^2+\bar{4}=\bar{5}x^2+\bar{3}x+\bar{4}$

定理2.2 设D是整环，则D[x]也是整环

证: 设 $f, g\in D[x]$ 且 $f\neq 0$, $g\neq 0$

则 $lc(f)\neq 0$, $lc(g)\neq 0$

$\Rightarrow lc(f)lc(g)\neq 0$ [D是整环]

$\Rightarrow lc(fg)=lc(f)lc(g)\neq 0$ [命题2.2(ii)]

$\Rightarrow fg\neq 0$ $\boxtimes$

注：当 F 是域时，$F[x]$ 是整环，由第四章§4中分式域的结论

$F[x]$ 有分式域

$$F(x)=\left\{\frac{f(x)}{g(x)}\,\middle|\, f,g\in F[x],\ g\neq 0\right\}$$

称为 F 上关于 x 的有理分式域.

例 $\mathbb{R}(x)$，$\mathbb{Z}_p(x)$.

§2 赋值同态

例：设 $f(x)=x^2-4\in\mathbb{Z}[x]$，求 $f(15)$

$f(15)=15^2-4=225-4=221$

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

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

$$\begin{tikzcd}
f(x)=(x-2)(x+2) \arrow[r, "\mathbb{Z}[x]\text{中乘法}"] \arrow[d, "\text{代入}x=15"'] & x^2-4 \arrow[d, "\text{代入}x=15"] \\
13\cdot 17 \arrow[r, "\mathbb{Z}\text{中乘法}"] & 221
\end{tikzcd}$$

定理2.3 设 $\varphi: R\to S$ 是两个交换环之间的同态，取定 $a\in S$

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

满足 (i) $\varphi_a|_R=\varphi$

(ii) $\varphi(x)=a$

证：存在性

$$\varphi_a: R[x]\longrightarrow S$$

$$f=\sum_{i=0}^{d} f_i x^i \longmapsto \sum_{i=0}^{d}\varphi(f_i)\,a^i$$

$(f_i\in R)$

由定理2.1 φ_a 是良定义的映射.

再设 $g=g_e x^e+g_{e-1}x^{e-1}+\cdots+g_0$，$g_j\in R$

且不妨设 $d\geq e$.

从而 $g=g_d x^d+\cdots+g_{e+1}x^{e+1}+g_e x^e$

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

其中 $g_d=\cdots=g_{e+1}=0$

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

$$= \sum_{i=0}^{d}\varphi(f_i+g_i)a^i \qquad [\varphi_a\text{的定义}]$$

$$= \sum_{i=0}^{d}(\varphi(f_i)+\varphi(g_i))a^i \qquad [\varphi: R\to S\text{ 环同态}]$$

$$= \sum_{i=0}^{d}\varphi(f_i)a^i + \sum_{i=0}^{d}\varphi(g_i)a^i \qquad [S\text{ 是环}]$$

$$= \varphi_a(f) + \varphi_a(g).$$

于是 $\varphi_a(f+g) = \varphi_a(f)+\varphi_a(g)$ $(*)$

设 $\alpha\in R$,

$$\varphi_a(f\alpha x^j) = \varphi_a\left(\sum_{i=0}^{d}(f_i\alpha)x^{i+j}\right)$$

$$= \sum_{i=0}^{d}\varphi(f_i\alpha)a^{i+j} \qquad [\varphi_a\text{的定义}]$$

$$= \sum_{i=0}^{d}\varphi(f_i)\varphi(\alpha)a^{i+j} \qquad [\varphi: R\to S\text{ 环同态}]$$

$$= \sum_{i=0}^{d}\left[\varphi(f_i)a^i(\varphi(\alpha)a^j)\right] \qquad [S\text{ 交换}]$$

$$= \left(\sum_{i=0}^{d}\varphi(f_i)a^i\right)\varphi(\alpha)a^j \qquad [S\text{ 中分配律}]$$

$$= \varphi_a(f)\varphi_a(\alpha x^j) \qquad [\varphi_a\text{的定义}]$$

$$\varphi_a(f\cdot(\alpha x^j)) = \varphi_a(f)\varphi_a(\alpha x^j) \qquad (**)$$

$$\varphi_a(fg) = \varphi_a\left(f\cdot\sum_{j=0}^{e}g_j x^j\right)$$

$$= \varphi_a\left(\sum_{j=0}^{e}(fg_jx^j)\right) \qquad [R\text{ 中分配律}]$$

$$= \sum_{j=0}^{e}\varphi_a(fg_jx^j) \qquad [(*)]$$

$$= \sum_{j=0}^{e}\varphi_a(f)\varphi_a(g_j)a^j \qquad [(**)]$$

$$= \varphi_a(f)\left[\sum_{j=0}^{e}\varphi_a(g_j)a^j\right] \qquad (S\text{ 中的分配律})$$

$$(\varphi_a\text{的定义})$$

$$= \varphi_a(f)\varphi_a(g)$$

$$\varphi_a(1_R) = \varphi(1_R)\cdot a^0 = 1_S\cdot 1_S = 1_S.$$

于是 φ_a 是环同态.

$\forall r\in R$

$$\varphi_a(r) = \varphi_a(rx^0) = \varphi(r)a^0 = \varphi(r)$$

$$\Rightarrow \varphi_a|_R = \varphi.$$

$\varphi_a(x) = \varphi(1_R)\, a = a$.

于是 φ_a 是满足定理要求的环同态.

唯一性 设 $\psi: R[x] \to S$ 是满足定理

要求的环同态.

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

$$= \sum_{i=0}^{d} \psi(f_i)\, \psi(x)^i \qquad [\psi \text{是环同态}]$$

$$= \sum_{i=0}^{d} \varphi(f_i)\, a^i \qquad [\psi \text{的性质}]$$

$$= \varphi_a(f)$$

□

注: 设 $\varphi: R \to S$ 是环同态. $a \in S$

$f \in R[x]$

$$f(a) := \varphi_a(f)$$

称为 f 关于 φ 在 a 处的赋值.

例: $\varphi: \mathbb{Z} \to \mathbb{Z}$ 恒同映射. $a = 15$

$f = x^2 - 4$

$f(15) = \varphi_a(f) = 15^2 - 4 = 221$

$$\varphi_a(f) = \varphi_a((x-2)(x+2)) = \varphi_a(x-2)\, \varphi_a(x+2)$$

$$= (15-2)(15+2) = 221$$

例: 设 $\varphi: \mathbb{Z} \to \mathbb{Z}_5$, 其中 $\varphi = \pi_5$

$a = \bar{3}$. $f = x^2 - 4 \in \mathbb{Z}$

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

$$\varphi_{\bar{3}}((x-2)(x+2)) = \varphi_{\bar{3}}(x-2)\, \varphi_{\bar{3}}(x+2)$$

$$= (\bar{3} - \bar{2})\underbrace{(\bar{3} + \bar{2})}_{=\bar{0}} = \bar{0}$$

设 $g = (179x - 286)(413x - 857)$

求 $g(\bar{3})$

$g(\bar{3}) = \varphi_{\bar{3}}(179x-286)\,\varphi_{\bar{3}}(413x-857)$

$=(\bar{4}\cdot\bar{3}-\bar{1})(\bar{3}\cdot\bar{3}-\bar{2})=\bar{1}\cdot\bar{2}=\bar{2}$ ∎

命题2.3 设F是域，$A\in M_n(F)$

$\rho: F\longrightarrow F[A]$

$\alpha\longmapsto \alpha E$

则：$\rho_A: F[x]\longrightarrow F[A]$ 是环同态

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

证：直接验证可得 ρ 是环同态

由第4章命题3.4. $F[A]$是交换环

$\rho_A(f)=\sum_{i=0}^{m} f_i A^i$

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

$=\sum_{i=0}^{m} \rho(f_i) A^i$

由定理2.3. ρ_A是环同态

注：记 $\rho_A(f)$ 为 $f(A)$.

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

求$f(A)$

解：$f(A)=\rho_A(f)=A^2-4E$

$=\begin{pmatrix}2&1\\0&2\end{pmatrix}\begin{pmatrix}2&1\\0&2\end{pmatrix}-4\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}0&4\\0&0\end{pmatrix}$

$f(A)=(A-2E)(A+2E)=\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}4&1\\0&4\end{pmatrix}$

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

§2.3 一元多项式的除法

命题2.4 设 $f, g\in R[x]$, $g\neq 0$

如果 $lc(g)$ 可逆，则$\exists!\ q, r\in R[x]$

满足 $f=qg+r$ 且

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

商

余式

证：存在性 若 $\deg(f) < \deg(g)$

则令 $q=0$，$r=f$ 即可

设 $\deg f = n+k$，$\deg g = n$，$lc(g)=g_n$，$lc(f)=f_{n+k}$

对 k 归纳. 当 $k=0$ 时

令 $r = f - f_n g_n^{-1} g$

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

k 存在性成立

设 $k>0$ 且 存在性对 次数低于 $n+k$ 的多项式成立

令 $h = f - f_{n+k} g_n^{-1} x^k g$

则 $\deg(h) < n+k$.

由归纳假设. $\exists\, q_1, r \in R[x]$ 且 $\deg(r)<\deg(g)$

使得 $h = q_1 g + r$.

$$f = (\underbrace{f_{n+k} g_n^{-1} x^k + q_1}_{q}) g + r$$

存在性成立

唯一性：设 $f = \tilde{q} g + \tilde{r}$，其中 $\tilde{q}, \tilde{r} \in R[x]$，$\deg(\tilde{r}) < \deg(g)$

则 $q g + r = \tilde{q} g + \tilde{r}$

$(q - \tilde{q}) g = \tilde{r} - r$

由命题2.2 $\deg(\tilde{r} - r) < \deg(g)$

$\Rightarrow q - \tilde{q} = 0 \Rightarrow \tilde{r} - r = 0$ ∎

例：设 $f = x^3+2x+1$，$g = 2x^2+1$ 是 $\mathbb{Q}[x]$ 中的多项式. 求 f 关于 g 的余式和商

解

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

于是 $q=\frac{1}{2}x$，$r=\frac{3}{2}x+1$.

~~定义、证明：设 f~~

定理2.4 设 F 是域，$f, g \in F[x]$

且 $g \neq 0$. 则 $\exists!\ q, r \in F[x]$

使得 $f = qg + r$ 且 $\deg(r) < \deg(g)$

称 q, r 为 f 关于 g 的商和余式

注：称 q、r 为 f 关于 g 的商和余式

记为 $quo(f, g, x)$, $rem(f, g, x)$

证：$\because g \neq 0 \therefore lc(g) \in F \setminus \{0\}$ 可逆

由命题2.4，定理成立 ∎

例：设 $f = \bar{3}x^3 + \bar{2}x^2 + \bar{1}$, $g = \bar{2}x^2 + \bar{4}$

是 $\mathbb{Z}_5[x]$ 中的多项式. 求 f 关于 g 的余式和商

解：

$$
\begin{array}{r|l}
 & \bar{4}x + \bar{1} \\
\bar{2}x^2 + \bar{4} & \bar{3}x^3 + \bar{2}x^2 + \bar{1} \\
 & \bar{3}x^3 + x \\ \hline
 & \bar{2}x^2 + \bar{4}x + \bar{1} \\
 & \bar{2}x^2 + \bar{4} \\ \hline
 & \bar{4}x + \bar{2}
\end{array}
\qquad \bar{2} \cdot \bar{3} = \bar{1}
$$

$quo(f, g) = \bar{4}x + \bar{1}$, $rem(f, g) = \bar{4}x + \bar{2}$

定理2.5 设 F 是域，$f \in F[x]$, $\alpha \in F$

则 $f(\alpha) = rem(f, x - \alpha)$

证：设 $r = rem(f, x - \alpha)$, 则 $r \in F$

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

$f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r$ ∎

§2.4 多项式的根

设 F, K 是域且 $F \subset K$. 设 $f \in F[x]$

$\alpha \in K$. 如果 $f(\alpha) = 0$, 则称

α 是 f 在 K 中的一个根

其中 $f(\alpha)$ 是 f 关于 $F \hookrightarrow K$, $r \longmapsto r$ 在 α 处的赋值

例：$f = (x^2 - 2)(x^2 + 1) \in \mathbb{Q}[x]$

f 在 $\mathbb{Q}$ 中无根，在 $\mathbb{R}$ 中有两个根 $\pm\sqrt{2}$

在 $\mathbb{C}$ 中有四个根 $\pm\sqrt{2}$, $\pm\sqrt{-1}$.

定理2.6 设 $F \subset K$ 是两个域. $\alpha \in K$

$f \in F[x]$ 且 $d = \deg(f) > 0$

(i) $f(\alpha) = 0 \iff \mathrm{rem}(f, x-\alpha) = 0$

(ii) f 在 K 中至多有 d 个互不相同的根

证: (i) 由定理2.5直接可得 (把 f 看成 $K[x]$ 中的多项式)

(ii) 对 d 归纳. 当 $d=1$.

$f = f_1 x + f_0$, $f_1, f_0 \in F$, $f_1 \neq 0$

则 f 的唯一根是 $-f_1^{-1} f_0$.

设 $d > 1$ 且定理对 $\deg(f) = d-1$ 成立

设 $\deg(f) = d$. 且它在 K 中互不相同的根是 $\{\alpha_1, \cdots, \alpha_m\}$

由(i) $f(x) = g(x)(x - \alpha_m)$, 其中 $g \in F[x]$

$\deg g = d-1$

$\forall i \in \{1, 2, \cdots m-1\}$

$f(\alpha_i) = g(\alpha_i)(\alpha_i - \alpha_m) = 0$

$\because \alpha_i - \alpha_m \neq 0$ $\therefore g(\alpha_i) = 0$. 于是

$\alpha_1, \cdots \alpha_{m-1}$ 是 g 在 K 中互不相同的根

$m-1 \leq d-1$ (归纳假设) $\Rightarrow m \leq d$ ☐

§2.5 整除与相伴

在本节中 D 是整环, $D^* = D \setminus \{0\}$

定义: 设 $a, b \in D$ 且 $a \neq 0$. 如果存在 $c \in D$ 使得 $b = ca$. 则称 a 是 b 的因子. 记为 $a \mid b$. b 是 a 的倍式.

例: 在 $\mathbb{Z}$ 中 $2 \mid 4$. $2 \nmid 5$

在 $\mathbb{Q}[x]$ 中 $(x+1) \mid (x^2-1)$

$(x+1) \nmid (x^2+1)$

在 $\mathbb{Z}_2[x]$ 中 $(x+\bar{1}) \mid (x^2+\bar{1}) = (x+\bar{1})^2$

定义：设 $a, b \in D$，如果存在 $u \in U_D$ 使得 $a = ub$ 则称 a 与 b 相伴，记为 $a \approx b$.

注 U_D 是 D 中所有可逆元的集合 $(U_D, \cdot, 1)$ 是群. [见第四章定理3.3]

"$\approx$" 是等价关系

自反：$\forall a \in D$ $a = 1 \cdot a$.

对称：设 $a \approx b$. 则 $\exists u \in U_D$ 使得 $a = ub \Rightarrow u^{-1}a = b \Rightarrow b \approx a$

传递：设 $a \approx b$, $b \approx c$, 则 $\exists\, u, v \in U_D$ 使得 $a = ub$, $b = vc \Rightarrow a = uvc$ $\Rightarrow a \approx c$ $(\because uv \in U_D)$

例：$U_{\mathbb{Z}} = \{1, -1\}$，则 $\forall n \in \mathbb{Z}$ $n \approx n$, $n \approx -n$ 且只有这两种可能

例：设 F 是域，$U_{F[x]} = F^* := F \setminus \{0\}$

于是 $\forall f, g \in F[x]$ $f \approx g \Leftrightarrow \exists\, \alpha \in F^*$，使得 $f = \alpha g$

定义：设 $f \in F[x] \setminus \{0\}$，如果 $lc(f) = 1$. 则称 f 是首一的

注：$\forall f \in F[x] \setminus \{0\}$ $f \approx \underbrace{lc(f)^{-1} f}_{g}$. 而 g 是首一的

引理2.1 设 $a, b \in D^*$, $c \in D$

(i) $a|b$, $b|c \Rightarrow a|c$

(ii) $a|b$, $a|c \Rightarrow \forall f, g \in D$ $a|(fb+gc)$

证：(i) 设 $b = pa$, $c = qb$, $p, q \in D$ $\Rightarrow c = (pq)a \Rightarrow a|c$

(ii) 设 $b = pa$, $c = qa$

$fb + gc = fpa + gqa = (fp + gq)a$

故 $a|(fb+gc)$ ☐

引理2.2. 设 $a, b \in D^*$. 则

$$a \approx b \iff a|b \text{ 且 } b|a$$

证: "⇒" $a \approx b \Rightarrow \exists u \in U_D$. $a = ub$, $u^{-1}a = b$

$\Rightarrow a|b$ 且 $b|a$

"⇐" 设 $a = pb$, $b = qa$, $p, q \in D^*$

则 $a = pqa \Rightarrow (1-pq)a = 0$

$\because a \neq 0$ $\therefore$ $1 - pq = 0$ {整环消去律

$pq = 1 \Rightarrow p, q \in U_D$

$\Rightarrow a \approx b$ ☐

定义: 设 $a, b \in D^*$. 如果 $c \in D^*$ 使得 $c|a$, $c|b$. 则称 c 是 a 和 b 的公因子.

设 g 是 a, b 的公因子. 如果对于 ~~$\forall a,b|c$~~ a, b 的公因子 c 都有 $c|g$. 则称 g 是 a, b 的最大公因子.

命题2.5 设 $a, b \in D^*$. g, h 是 a, b 的两个最大公因子. 则 $g \approx h$.

证: 由最大公因子的定义可知. $g|h$ 且 $h|g$. $\Rightarrow g \approx h$ (引理2.2)

例: $\mathbb{Z}$ 中 $\gcd(21, 35) = 7$ 或 -7

通常 $\gcd(m, n) > 0$

§2.6. 一元多项式环中的最大公因子

定理2.7 若 F 是域, 则 $\forall p, q \in F[x] \setminus \{0\}$ $\gcd(p, q)$ 存在. 且 $\exists u, v \in F[x]$ 使得 $up + vq = \gcd(p, q)$.

证：设 $I=\{ap+bq \mid a,b\in F[x]\}$

g 是 I 中次数最小的非零多项式

则 $\exists u,v\in F[x]$ 使得

$$up+vq=g \quad (*)$$

由多项式除法 $p=hg+r$

其中 $h,r\in F[x]$，$\deg(r)<\deg(g)$

于是由$(*)$，$p=h(up+vq)+r$

$$(1-hu)p+(-hv)q=r$$

$\Rightarrow r\in I$ [由 $\deg(g)$ 的极小性]

于是 $r=0$

$\Rightarrow g\mid p$，同理 $g\mid q$

设 c 是 p,q 的公因子.

由引理2.1和$(*)$ $c\mid g$ 于是 g 的最大公因子 $\square$

最大公因子的计算

设 $f,g\in F[x]\setminus\{0\}$，求 $\gcd(f,g)$

令 $r_0=f$，$r_1=g$.

$r_0=q_2r_1+r_2$，　$r_2=\mathrm{rem}(r_0,r_1)$

$r_1=q_3r_2+r_3$，　$r_3=\mathrm{rem}(r_1,r_2)$

$\vdots$

$r_{k-2}=q_kr_{k-1}+r_k$　$r_k=\mathrm{rem}(r_{k-2},r_{k-1})$

$\deg(r_2)>\deg(r_3)>\cdots>\deg(r_k)$

不妨设 $r_{k-1}=q_{k+1}r_k$

则类似第一章第6节（辗转相除）

可知 $\gcd(f,g)=r_k$ [见讲义1-4 pages]

例：设 $f=x^4+\bar{1}$，$g=x^3+\bar{1}$ ~~多项式~~ 是 $\mathbb{Z}_2[x]$ 中的 $\gcd(f,g)$.

解: $r_0 = x^4+\bar{1}$, $r_1 = x^3+\bar{1}$

$$
\begin{array}{r|l}
 & x \\
\hline
x^3+\bar{1} & x^4+\bar{1} \\
 & x^4+x \\
\hline
 & x+\bar{1}
\end{array}
$$

$r_2 = x+\bar{1}$

$$
\begin{array}{r|l}
 & x^2+\bar{1} \\
\hline
x+\bar{1} & x^3+\bar{1} \\
 & x^3+x \\
\hline
 & x+\bar{1} \\
 & x+\bar{1} \\
\hline
 & \bar{0}
\end{array}
$$

$r_3 = 0$

$\gcd(f, g) = r_2 = x+\bar{1}$.