一元多项式的带余除法与根

F代表某个选定的域 $\therefore F$是整环，F是交换环 $\therefore F[X]$是交换环.

命题（多项式的带余除法）~~之前已证~~ 对$\forall a, d\in F[X]$，若$d\neq 0$，则存在唯一的$q, r\in F[X]$，使得 $\deg(r)<\deg(d)$ 而且

$a=dq+r$. 此处定义 $\deg(0):=-\infty$

Proof: 考虑集合 $A=\{a-dq : q\in F[X]\}\subseteq F[X]$

$\because a=a-d\cdot 0\in A \quad \therefore A\neq\emptyset$.

$\therefore \{\deg(a-dq) : q\in F[X]\}\subseteq\{-\infty\}\cup\mathbb{Z}_{\geq 0}$

且 $\{\deg(a-dq) : q\in F[X]\}\neq\emptyset$

$\therefore$由非负整数的良序原理，$\exists q\in F[X]$ s.t. $\deg(a-dq)$ 极小（容许为$-\infty$）

设 $r=a-dq\in F[X]$ $\therefore a=dq+r$.

若$r=0$，则 $\deg(r)=-\infty<\deg(d)$ （因为 $d\neq 0$. 所以 $\deg(d)\in\mathbb{Z}_{\geq 0}$）

若$r\neq 0$，则 设 $r=\alpha_n X^n+$低次项，$d=\beta_m X^m+$低次项

（$\because r\neq 0$. $\therefore \deg(r)\in\mathbb{Z}_{\geq 0}$ $\therefore \alpha_n\neq 0$，$n\in\mathbb{Z}_{\geq 0}$.

$\because d\neq 0$ $\therefore \deg(d)\in\mathbb{Z}_{\geq 0}$ $\therefore \beta_m\neq 0$，$m\in\mathbb{Z}_{\geq 0}$ ）

假设 $\deg(r)\geq\deg(d)$，则有 $n\geq m$

$\therefore$ ~~deg~~ $r-\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)d=(\alpha_n X^n+$低次项$)-(\beta_m X^m+$低次项$)\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)$

$=(\alpha_n X^n+$低次项$)-(\alpha_n X^n+$低次项$)=$ 次数$<n$的项.

$$\therefore \deg\left(r - d\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)\right) < n = \deg(r)$$

$$\because a - d\left(q + \frac{\alpha_n}{\beta_m}X^{n-m}\right) = a - \left(dq + d\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)\right)$$

$$= a - dq - d\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right) = r - d\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)$$

$$\therefore \deg\left(a - d\left(q + \frac{\alpha_n}{\beta_m}X^{n-m}\right)\right) = \deg\left(r - d\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)\right) < \deg(r)$$

$= \deg(a-dq)$. 与 $\deg(a-dq)$ 极小矛盾.

$\therefore \deg(r) < \deg(d)$ 存在性得证.

假设存在 $q_1, r_1, q_2, r_2 \in F[X]$, s.t.

$a = dq_1 + r_1$, $\deg(r_1) < \deg(d)$

$a = dq_2 + r_2$, $\deg(r_2) < \deg(d)$

$$\because dq_1 + r_1 = a = dq_2 + r_2$$

$$\therefore d(q_1 - q_2) = dq_1 - dq_2 = r_2 - r_1$$

$$\therefore \deg(r_2 - r_1) = \deg(d(q_1 - q_2))$$

~~假设 $q_1 - q_2 = 0$ 则有: $q_1 = q_2$ $\therefore r_2 - r_1 = d(q_1 - q_2) = d\cdot 0 = 0$ $\therefore r_1 = r_2$~~

假设 $q_1 - q_2 \neq 0$. 则 $\because d \neq 0$ 且 $q_1 - q_2 \neq 0$.

$$\therefore \deg(r_2 - r_1) = \deg(d(q_1 - q_2)) = \deg(d) + \deg(q_1 - q_2) \geq \deg(d)$$

$$\therefore \deg(d) \leq \deg(r_2 - r_1) = \deg(r_2 + (-r_1)) \leq \max\{\deg(r_2), \deg(-r_1)\}.$$

$= \max\{\deg(r_2), \deg(r_1)\} < \deg(d)$ 矛盾.

$\therefore q_1 - q_2 = 0 \quad \therefore q_1 = q_2 \quad \therefore r_2 - r_1 = d(q_1 - q_2) = d \cdot 0 = 0$

$\therefore r_1 = r_2$. 唯一性得证. $\square$

定义(多项式的整除). 设 $a, d \in F[X]$. 如果存在 $q \in F[X]$, s.t. $a = dq$, 则称 d 整除 a, 记作 $d \mid a$.

推论: 对 $\forall a, d \in F[X]$, $d \neq 0$, $\exists$ 唯一的 $q, r \in F[X]$ 使得 $\deg(r) < \deg(d)$ 而且 $a = dq + r$. 则有:

$$d \mid a \iff r = 0$$

Proof: $(\Leftarrow)$: $\because r = 0 \quad \therefore a = dq \quad \because q \in F[X] \quad \therefore d \mid a$

$(\Rightarrow)$: $\because d \mid a \quad \therefore \exists \lambda \in F[X]$, s.t. $a = d\lambda$

$\therefore a = d\lambda + 0$, $\lambda \in F[X]$, $0 \in F[X]$, $\deg(0) = -\infty < \deg(d)$

$\because a = dq + r$, $q, r \in F[X]$, $\deg(r) < \deg(d)$

$\therefore$ 由唯一性知: $q = \lambda$, $r = 0 \quad \therefore r = 0$ $\square$

命题(整环 R 上的一元多项式环 $R[X]$ 上的带余除法) R 是一个整环, 对 $\forall a, d \in R[X]$, $d \neq 0$, d 的最高次项系数属于 $R^\times$, 则存在唯一的 $q, r \in R[X]$, 使得 $\deg(r) < \deg(d)$ 且 $a = dq + r$.

Proof: ~~考虑集~~ $\because R$是整环 $\therefore R$是非零交换环 $\therefore R[X]$是交换环.

考虑集合 $A=\{a-dq \mid q\in R[X]\}\subseteq R[X]$.

$\because 0\in R[X]$ $\therefore a-d\cdot 0\in A$ $\because a-d\cdot 0=a-0=a$

$\therefore a\in A$ $\therefore A\neq\emptyset$

$\therefore \{\deg(a-dq) \mid q\in R[X]\}\subseteq\{-\infty\}\cup\mathbb{Z}_{\geqslant 0}$

且 $\{\deg(a-dq) \mid q\in R[X]\}\neq\emptyset$.

$\therefore$由非负整数的良序原理，$\exists q\in R[X]$, s.t. $\deg(a-dq)$极小(容许为$-\infty$)

设 $r=a-dq$. $\because a,d\in R[X]$, $q\in R[X]$ $\therefore r\in R[X]$.

$\therefore q,r\in R[X]$，且有 $dq+r=dq+(a-dq)=dq+(a+(-dq))=a$

$\therefore a=dq+r$

若 $r=0$，则有 $\deg(r)=-\infty<\deg(d)$

若 $r\neq 0$，则有 $\deg(d)\in\mathbb{Z}_{\geqslant 0}$, $\deg(r)\in\mathbb{Z}_{\geqslant 0}$

$\therefore$设 $r=\alpha_n X^n+$低次项 (其中 $\alpha_n\neq 0$, $n\in\mathbb{Z}_{\geqslant 0}$)

$d=\beta_m X^m+$低次项 (其中 $\beta_m\neq 0$, $m\in\mathbb{Z}_{\geqslant 0}$) (已知 $\beta_m\in R^\times$)

假设 $\deg(r)\geqslant\deg(d)$，则有 $n\geqslant m$ $\therefore n-m\in\mathbb{Z}_{\geqslant 0}$

$\therefore r-d\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)=(\alpha_n X^n+\text{低次项})-(\beta_m X^m+\text{低次项})\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)$

$=(\alpha_n X^n+\text{低次项})-(\alpha_n X^n+\text{低次项})=$次数$<n$的项.

$\because q \in R[X]$, $\frac{\alpha_n}{\beta_m}X^{n-m} \in R[X]$ $\quad \therefore q + \frac{\alpha_n}{\beta_m}X^{n-m} \in R[X]$

$\therefore a - d\left(q + \frac{\alpha_n}{\beta_m}X^{n-m}\right) = a - \left(dq + d\cdot\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right)\right)$

$= a - dq - d\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right) = r - d\left(\frac{\alpha_n}{\beta_m}X^{n-m}\right) =$ 次数 $< n$ 的项.

$\therefore \deg\left(a - d\left(q + \frac{\alpha_n}{\beta_m}X^{n-m}\right)\right) < n = \deg(r) = \deg(a - dq)$

与 $\deg(a-dq)$ 极小矛盾.

$\therefore \deg(r) < \deg(d)$ $\quad\therefore$ 存在性得证.

唯一性的证明与之前的完全一样. $\square$