

## 0.1 域上一元多项式

### 定义 0.1

设  $R[x]$  是交换整环  $R$  上的一元多项式环, 若  $f(x) \in R[x]$  且  $f(x) \neq 0$ , 有

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_n \neq 0.$$

则  $a_ix^i$  称为  $f(x)$  的  $i$  次项,  $a_i$  称为  $i$  次项的系数,  $a_0$  称为常数项,  $a_nx^n$  称为首项,  $n$  称为  $f(x)$  的次数, 记为  $\deg f(x) = n$ . 如果  $f(x) \neq 0$  且  $f(x)$  的首项系数为 1, 则称  $f(x)$  为首一多项式. 今后以  $(f(x), g(x))$  表示  $f(x), g(x)$  的最大公因式中的首一多项式.

若  $f(x) = a_0 \neq 0$ , 则记  $\deg f(x) = 0$ , 一般对零元素 0 是不规定次数的, 但规定 0 的次数为  $-\infty$ , 即  $\deg 0 = -\infty$  且规定

$$-\infty + (-\infty) = -\infty, \quad -\infty + n = -\infty, \quad -\infty < n, \quad 2^{-\infty} = 0.$$



### 定理 0.1

设  $R[x]$  是交换整环  $R$  上的一元多项式环,  $R^* = R \setminus \{0\}$ ,  $f(x), g(x) \in R[x]$ , 则

- (1)  $\deg f(x) = 0 \iff f(x) \in R^*$ .
- (2)  $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$ .
- (3)  $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ .
- (4) 令  $\delta(f(x)) = 2^{\deg f(x)}$ , 则有

$$\deg f(x) < \deg g(x) \iff \delta(f(x)) < \delta(g(x)),$$

$$\delta(f(x)g(x)) = \delta(f(x))\delta(g(x)).$$

- (5) 首一多项式的乘积仍为首一多项式.
- (6)  $R[x]$  也是交换整环且  $R[x]$  的单位就是  $R$  的单位.
- (7)  $R$  上  $n$  元多项式环  $R[x_1, x_2, \dots, x_n]$  也是交换整环且其单位就是  $R$  的单位.



### 证明

- (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- (7)



### 定理 0.2

设  $F$  是一个域,  $F[x]$  为  $F$  上一元多项式环, 则

- (1)  $\forall f(x), g(x) \in F[x], g(x) \neq 0$ , 存在唯一的一对多项式  $q(x), r(x)$ , 使得

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x);$$

分别称  $q(x), r(x)$  为  $f(x)$  除以  $g(x)$  的商、余式.

- (2)  $F[x]$  是 Euclid 环.



**注** 由定理 0.2(2) 知  $F[x]$  是 Euclid 环, 又由定理 ?? 知  $F[x]$  是主理想整环, 进而也是唯一析因环.

### 证明

- (1) 首先证明  $q(x), r(x)$  的存在性. 对  $\deg f(x)$  作归纳. 设  $\deg g(x) = m$ . 由假设知  $m \geq 0$ , 当  $\deg f(x) < m$  时可取  $q(x) = 0$ , 即  $r(x) = f(x)$ . 现设  $\deg f(x) < n$  时,  $q(x)$  与  $r(x)$  已存在. 设  $\deg f(x) = n$ . 不妨设  $n \geq m$ . 又设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0.$$

由  $b_m \neq 0$ , 取  $q_0(x) = a_n b_m^{-1} x^{n-m}$ . 令

$$f_1(x) = f(x) - q_0(x)g(x) = (a_{n-1} - a_n b_m^{-1} b_{m-1})x^{n-1} + \cdots,$$

故  $\deg f_1(x) \leq n-1 < n$ . 由归纳假设有  $q_1(x), r_1(x)$ , 使得

$$f_1(x) = q_1(x)g(x) + r_1(x), \quad \deg r_1(x) < \deg g(x),$$

因而有

$$f(x) = q_0(x)g(x) + q_1(x)g(x) + r_1(x) = (q_0(x) + q_1(x))g(x) + r_1(x).$$

取  $q(x) = q_0(x) + q_1(x), r(x) = r_1(x)$ , 它们满足定理条件.

下面证明  $q(x)$  与  $r(x)$  的唯一性. 设有  $q_2(x), r_2(x)$  也满足

$$f(x) = q_2(x)g(x) + r_2(x), \quad \deg r_2(x) < \deg g(x),$$

于是有  $(q(x) - q_2(x))g(x) = r_2(x) - r(x)$ . 若  $q(x) - q_2(x) \neq 0$ , 则

$$\deg(r_2(x) - r(x)) \geq \deg g(x) > \max\{\deg r_2(x), \deg r(x)\}.$$

另一方面有

$$\deg(r_2(x) - r(x)) \leq \max\{\deg r_2(x), \deg r(x)\},$$

这就导出矛盾. 故  $q(x) = q_2(x), r_2(x) = r(x)$ .  $q(x)$  与  $r(x)$  的唯一性得证.

- (2) 令  $\delta(f(x)) = 2^{\deg f(x)}$ , 注意到  $\deg r(x) < \deg g(x)$ , 由定理 0.1(4) 得

$$\delta(r(x)) < \delta(g(x)),$$

故  $F[x]$  为 Euclid 环. □

### 定义 0.2

设  $F$  是一个域,  $F[x]$  为  $F$  上一元多项式环, 若  $f_1(x)$  与  $f_2(x)$  除以  $g(x)$  的余式相同, 则称  $f_1(x)$  与  $f_2(x)$  模  $g(x)$  同余. 记为  $f_1(x) \equiv f_2(x) \pmod{g(x)}$ . ♣

### 推论 0.1

设  $F[x]$  为域  $F$  上的一元多项式环,  $f_1(x), f_2(x), g(x) \in F[x]$  且  $g(x) \neq 0$ , 则

$$f_1(x) \equiv f_2(x) \pmod{g(x)} \iff g(x) \mid (f_1(x) - f_2(x)),$$

而且  $f_1(x) \equiv f_2(x) \pmod{g(x)}$  无论对  $F[x]$  的加法或乘法都是同余关系. ♥

**证明**  $f_1(x) \equiv f_2(x) \pmod{g(x)}$  当且仅当存在  $q_1(x), q_2(x), r(x) \in F[x]$ , 使

$$f_1(x) = q_1(x)g(x) + r(x), \quad f_2(x) = q_2(x)g(x) + r(x).$$

这也当且仅当

$$f_1(x) - f_2(x) = (q_1(x) - q_2(x))g(x) \iff g(x) \mid (f_1(x) - f_2(x)).$$

设  $f_1(x) \equiv f_2(x) \pmod{g(x)}, f_3(x) \equiv f_4(x) \pmod{g(x)}$ , 则存在  $q_1(x), q_2(x), q_3(x), q_4(x), r_1(x), r_2(x) \in F[x]$ , 使

$$f_1(x) = q_1(x)g(x) + r_1(x), \quad f_2(x) = q_2(x)g(x) + r_1(x),$$

$$f_3(x) = q_3(x)g(x) + r_2(x), \quad f_4(x) = q_4(x)g(x) + r_2(x).$$

于是

$$\begin{aligned} f_1(x) + f_3(x) &= (q_1(x) + q_3(x))g(x) + r_1(x) + r_2(x), \\ f_2(x) + f_4(x) &= (q_2(x) + q_4(x))g(x) + r_1(x) + r_2(x), \\ f_1(x)f_3(x) &= (q_1(x)q_3(x)g(x) + q_1(x)r_2(x) + q_3(x)r_1(x))g(x) + r_1(x)r_2(x), \\ f_2(x)f_4(x) &= (q_2(x)q_4(x)g(x) + q_2(x)r_2(x) + q_4(x)r_1(x))g(x) + r_1(x)r_2(x). \end{aligned}$$

故

$$\begin{aligned} f_1(x) + f_3(x) &\equiv f_2(x) + f_4(x) \pmod{g(x)}, \\ f_1(x)f_3(x) &\equiv f_2(x)f_4(x) \pmod{g(x)}. \end{aligned}$$

因此  $f_1(x) \equiv f_2(x) \pmod{g(x)}$  对  $F[x]$  的加法和乘法都是同余关系.

□

### 定义 0.3

设  $F$  是一个域,  $F[x]$  为  $F$  上一元多项式环, 若  $c \in F$  且使  $f(c) = 0$ , 则称  $c$  是  $f(x)$  的一个根.

♣

### 推论 0.2

设  $F[x]$  为域  $F$  上的一元多项式环且  $f(x) \in F[x], c \in F$ , 则

$$f(x) \equiv f(c) \pmod{(x - c)} \quad (1)$$

且  $(x - c) \mid f(x) \iff f(c) = 0 \iff c$  是  $f(x)$  的根.

♡

**证明** 事实上, 由定理??,  $F$  的恒等映射  $\text{id}_F$  可开拓为  $F[x]$  到  $F$  的同态  $\eta$ , 使得

$$\eta_F = \text{id}_F, \quad \eta(x) = c.$$

从而

$$\eta(f(x)) = f(c), \quad \forall f(x) \in F[x].$$

现因  $\deg(x - c) = 1$ , 故  $\exists q(x) \in F[x], r \in F$ , 使得

$$f(x) = (x - c)q(x) + r.$$

两边作用以  $\eta$ , 则有

$$f(c) = (c - c)q(c) + r = r,$$

因而式(1)成立. 特别地,  $(x - c) \mid f(x) \iff f(x) \equiv 0 \pmod{(x - c)} \iff f(c) = 0$ .

□

### 推论 0.3

设  $F$  是一个域,  $F[x]$  为  $F$  上一元多项式环,  $f(x) \in F[x], c_i \in F (i = 1, 2, \dots, k)$ , 若  $c_1, c_2, \dots, c_k$  是  $f(x)$  的互不相同的根, 则有  $\prod_{i=1}^k (x - c_i) \mid f(x)$ , 从而  $k \leq \deg f(x)$ .

♡

**证明** 显然  $x - c_i$  是  $F[x]$  中不可约元素, 由定理 0.2(2) 知  $F[x]$  是 Euclid 环, 又由定理?? 知  $F[x]$  是唯一析因环. 再由定理?? 知  $F[x]$  满足素性条件. 因而  $x - c_i$  是素元素. 又由  $c_i \neq c_j (i \neq j, 1 \leq i, j \leq k)$ . 由

$$\frac{1}{c_i - c_j}(x - c_j) - \frac{1}{c_i - c_j}(x - c_i) = 1$$

及定理?? 知  $(x - c_i, x - c_j) = 1$ . 又由推论?? 知  $(x - c_i) \mid f(x)$ , 故由定理?? 知  $\prod_{i=1}^k (x - c_i) \mid f(x)$ , 从而  $k \leq \deg f(x)$ .

□

## 命题 0.1

设  $S$  为交换整环,  $R$  为  $S$  的子环且  $1 \in R$ , 则  $f(x) \in R[x]$  在  $S$  中不同根的个数不超过  $\deg f(x)$ .



**注** 设  $R$  为交换环,  $S$  为  $R$  的扩环,  $f(x) \in R[x], \deg f(x) > 0$ , 那么  $f(x)$  在  $S$  中不同根的数目是否超过  $\deg f(x)$ ? 如果  $S$  为交换整环, 则回答是肯定的. 若  $S$  非交换或有零因子则不然.

**证明** 事实上, 设  $F$  为  $S$  的分式域. 于是  $R[x] \subseteq S[x] \subseteq F[x]$ , 即  $f(x) \in F[x]$ . 由推论 0.3 知结论成立.

□

**例题 0.1** 设  $\mathbf{H}$  为四元数体 (见定理 ??), 由命题 ?? 知

$$\mathbf{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\},$$

因而  $\{a + 0 \cdot i + 0 \cdot j + 0 \cdot k \mid a \in \mathbf{R}\} \cong \mathbf{R}$  是  $\mathbf{H}$  的一个子环. 由命题 ?? 知  $i^2 = j^2 = k^2 = -1$ , 故  $i, j, k$  都是  $\mathbf{R}$  上的多项式  $x^2 + 1$  的根, 从而  $bi + cj + dk$  都是  $x^2 + 1$  的根, 因此  $x^2 + 1$  在  $\mathbf{H}$  中有无穷多个根.

**例题 0.2** 设  $R = S = \mathbf{Z}_8$ . 不难看出  $x^2 - 1 \in R[x]$  有 4 个不同的根  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ , 其中  $\bar{n}$  表示  $n + 8\mathbf{Z}$ .

## 命题 0.2

设  $a, b \in \mathbf{N}$ , 若  $a \nmid b$ , 则存在素数  $p$ , 使得

$$a = p^r l, \quad b = p^s k, \quad (p, l) = (p, k) = (p, lk) = 1, \quad r > s.$$



**证明** 由算术基本定理知, 存在  $n \in \mathbf{N}$  以及互不相同的素数  $p_1, p_2, \dots, p_n$ , 使得

$$a = \prod_{i=1}^n p_i^{k_i}, \quad b = \prod_{i=1}^n p_i^{k'_i},$$

其中  $k_i, k'_i \in \mathbf{N}$ . 因为  $a \nmid b$  当且仅当  $k_i \leq k'_i, i = 1, 2, \dots, n$ , 所以由  $a \nmid b$  可得, 存在  $i_0 \in \{1, 2, \dots, n\}$ , 使得  $k_{i_0} > k'_{i_0}$ . 于是记  $p = p_{i_0}, r = k_{i_0}, s = k'_{i_0}, l = \prod_{i \neq i_0} p_i^{k_i}, k = \prod_{i \neq i_0} p_i^{k'_i}$ , 则  $r > s$  且

$$a = p_{i_0}^{k_{i_0}} \prod_{i \neq i_0} p_i^{k_i} = p^r l, \quad b = p_{i_0}^{k'_{i_0}} \prod_{i \neq i_0} p_i^{k'_i} = p^s k.$$

由  $p_1, p_2, \dots, p_n$  是互不相同的素数可知  $(p, l) = (p, k) = 1$ , 故  $(p, lk) = 1$ .

□

## 定理 0.3

设  $F$  是一个域,  $G$  是  $F^* = F \setminus \{0\}$  的一个有限的乘法子群, 则  $G$  为循环群.



**证明** 设  $|G| = n, g$  是  $G$  中最大阶的元素且其阶为  $m$ , 因而  $\langle g \rangle = \{1, g, g^2, \dots, g^{m-1}\} \subseteq G$ , 由 Lagrange 定理知  $m \mid n$ . 任取  $h \in G$ , 设  $h$  的阶为  $m_1$ , 如果  $m_1 \nmid m$ , 则由命题 0.2 知有素数  $p$ , 使得

$$m_1 = p^r l, \quad m = p^s k, \quad (p, l) = (p, k) = (p, lk) = 1, \quad r > s.$$

由  $h$  的阶为  $m_1$ , 故  $h^l$  的阶为  $p^r, g^{p^s}$  的阶为  $k$ , 由于  $G$  为 Abel 群, 故  $h^l g^{p^s} = g^{p^s} h^l, (p^r, k) = 1$ , 由推论 ?? 知  $h^l g^{p^s}$  的阶为  $p^r k$ , 但  $p^r k > p^s k = m$ . 这与  $m$  的选取矛盾, 故  $m_1 \mid m$ .

由此得  $\forall h \in G, h$  都是  $x^m - 1$  的根, 即  $G \subseteq \{x \mid x^m - 1 = 0\}$ . 由命题 0.1 知  $x^m - 1$  至多有  $m$  个根, 又  $\langle g \rangle$  中  $m$  个元素都是  $x^m - 1$  的根, 故  $\langle g \rangle \subseteq \{x \mid x^m - 1 = 0\}$  且  $|\{x \mid x^m - 1 = 0\}| = m = |\langle g \rangle|$ , 因此  $\langle g \rangle = \{x \mid x^m - 1 = 0\}$ . 于是  $G \subseteq \langle g \rangle$ . 故  $G = \langle g \rangle$ , 这就证明了  $G$  是循环群.

□

## 推论 0.4

有限域  $F$  的非零元素集  $F^*$  对乘法为循环群.



**注** 这个推论对有限域理论是很重要的.

**证明** 由定理 0.3 立得.

□

**定理 0.4**

设  $F$  为域,  $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$ , 则  $f(x), g(x)$  非互素的充分必要条件为  $\exists f_0(x), g_0(x) \in F[x]^*$ , 使得

$$g_0(x)f(x) = f_0(x)g(x),$$

其中,

$$0 \leq \deg f_0(x) < \deg f(x), \quad 0 \leq \deg g_0(x) < \deg g(x).$$

♡

**证明** 显然这样的最大公因式是唯一的. 设  $d(x) = (f(x), g(x))$ , 于是有  $f(x) = d(x)f_0(x), g(x) = d(x)g_0(x)$ . 由  $f(x), g(x)$  非互素, 故  $\deg d(x) > 0$ , 因而

$$0 \leq \deg f_0(x) < \deg f(x), \quad 0 \leq \deg g_0(x) < \deg g(x)$$

且有

$$g_0(x)f(x) = d(x)f_0(x)g_0(x) = f_0(x)g(x).$$

由此知必要性成立.

反之, 假设  $(f(x), g(x)) = 1$ , 于是  $\exists u(x), v(x) \in F[x]$ , 使  $u(x)f(x) + v(x)g(x) = 1$ , 因而有

$$\begin{aligned} f_0(x) &= f_0(x) \cdot 1 = f_0(x)u(x)f(x) + v(x)f_0(x)g(x) \\ &= f(x)(f_0(x)u(x) + v(x)g_0(x)), \end{aligned}$$

即得  $\deg f_0(x) \geq \deg f(x)$ . 这与条件矛盾, 故  $(f(x), g(x)) \neq 1$ .

□

**推论 0.5**

设  $F$  为域,  $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$ , 记

$$\begin{aligned} f(x) &= \sum_{k=0}^n a_k x^{n-k}, \quad a_0 \neq 0, n \in \mathbf{N}, \\ g(x) &= \sum_{k=0}^m b_k x^{m-k}, \quad b_0 \neq 0, m \in \mathbf{N}. \end{aligned}$$

再记

$$f_0(x) = \sum_{k=1}^n x_k x^{n-k}, \quad g_0(x) = \sum_{k=1}^m x_{n+k} x^{m-k},$$

则  $(f(x), g(x)) \neq 1$  当且仅当存在  $(x_1, x_2, \dots, x_{m+n}) \neq 0$ , 使  $f(x)g_0(x) = g(x)f_0(x)$ ,

♡

**证明** 由定理 0.4 立得.

□

**定义 0.4 (结式/Sylvester 行列式)**

设  $F$  是一个域,  $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$ , 则称

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & \cdots & a_n & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & \cdots & b_m & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix},$$

为  $f(x)$  与  $g(x)$  的**结式**或**Sylvester 行列式**. 显然有

$$\begin{cases} \text{ent}_{i+j}(R(f, g)) = a_j, & 1 \leq i \leq m, 0 \leq j \leq n, \\ \text{ent}_{n+i+j}(R(f, g)) = b_j, & 1 \leq i \leq n, 0 \leq j \leq m, \\ \text{ent}_j(R(f, g)) = 0, & \text{其他}. \end{cases}$$

**定理 0.5**

设  $F$  是一个域,  $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$  非互素的充分必要条件是  $f(x)$  与  $g(x)$  的结式  $R(f, g) = 0$ .

**证明** 记

$$\begin{aligned} f(x) &= \sum_{k=0}^n a_k x^{n-k}, \quad a_0 \neq 0, n \in \mathbf{N}, \\ g(x) &= \sum_{k=0}^m b_k x^{m-k}, \quad b_0 \neq 0, m \in \mathbf{N}. \end{aligned}$$

再记

$$f_0(x) = \sum_{k=1}^n x_k x^{n-k}, \quad g_0(x) = \sum_{k=1}^m x_{n+k} x^{m-k},$$

由**推论 0.5**知  $(f(x), g(x)) \neq 1$  当且仅当存在  $(x_1, x_2, \dots, x_{m+n}) \neq 0$ , 使  $f(x)g_0(x) = g(x)f_0(x)$ , 所以有

$$\sum_{l=0}^{n+m-1} \left( \sum_{\substack{j+k=l \\ 0 \leq k \leq m-1}} a_j x_{k+n+1} \right) x^{n+m-1-l} = \sum_{r=0}^{n+m-1} \left( \sum_{\substack{p+q=r \\ 0 \leq q \leq n-1}} b_p x_{q+1} \right) x^{n+m-1-r}.$$

由对应项系数相等, 即得

$$\sum_{\substack{j+k=l \\ 0 \leq k \leq m-1}} a_j x_{k+n+1} = \sum_{\substack{p+q=r \\ 0 \leq q \leq n-1}} b_p x_{q+1}, \quad l = r = 0, 1, \dots, n+m-1.$$

这样得到一个齐次线性方程组

$$A^T \mathbf{X} = \mathbf{0},$$

其中,  $\mathbf{X} = (x_1, x_2, \dots, x_{m+n})'$ ,

$$\begin{cases} \text{ent}_{i,i+j}(A) = b_j, & 1 \leq i \leq n, 0 \leq j \leq m, \\ \text{ent}_{n+i,i+j}(A) = -a_j, & 1 \leq i \leq m, 0 \leq j \leq n, \\ \text{ent}_{i,j}(A) = 0, & \text{其他}. \end{cases}$$

显然当且仅当  $\det A = 0$  时才能找到**定理 0.4**中的  $f_0(x)$  与  $g_0(x)$ . 又注意到  $R(f, g) = \pm \det A$ , 故  $(f(x), g(x)) \neq 1$  当

且仅当  $R(f, g) = 0$ .

□

**例题 0.3** 设  $f(x) = x^2 + x + 1, g(x) = x^3 - 1 \in \mathbf{Q}[x]$ . 证明  $f(x), g(x)$  不互素并求  $f_0(x), g_0(x)$ , 使得  $f(x)g_0(x) = g(x)f_0(x)$ .  
解

$$R(f, g) = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{vmatrix} = 0.$$

故由定理 0.5 知  $f(x), g(x)$  不互素. 令  $f_0(x) = 1, g_0(x) = x - 1$ , 则  $f(x)g_0(x) = g(x)f_0(x)$ .

□

### 命题 0.3

设

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

$$g(x) = (x - y_1)(x - y_2) \cdots (x - y_m) = x^m + b_1 x^{m-1} + \cdots + b_m,$$

证明

$$R(f, g) = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j).$$

**证明** 注意  $(-1)^i a_i, (-1)^j b_j$  分别是  $x_1, x_2, \dots, x_n$  的  $i$  次初等对称多项式,  $y_1, y_2, \dots, y_m$  的  $j$  次初等对称多项式.

在行列式  $R(f, g)$  按组合求和定义的完全展开式中任一非零项

$$\prod_{i=1}^{m+n} \text{ent}_i \sigma(i) R(f, g), \quad \sigma \in S_{m+n}$$

是  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$  的齐次多项式, 其次数为

$$\sum_{i=1}^m (\sigma(i) - i) + \sum_{i=m+1}^{m+n} (\sigma(i) - (i - m)) = \sum_{i=1}^{m+n} \sigma(i) - \sum_{i=1}^{m+n} i + mn = mn.$$

因此,  $R(f, g)$  是  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$  的  $mn$  次齐次多项式.

当  $x_i = y_j$  时, 此时  $f(x), g(x)$  有公共根, 从而  $f(x), g(x)$  不互素, 故由定理 0.5 知  $R(f, g) = 0$ . 将  $R(f, g)$  视为关于  $x_i$  的一元多项式, 则  $y_j$  为其根. 于是  $(x_i - y_j) \mid R(f, g)$ , 所以

$$\prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j) \mid R(f, g).$$

又  $\deg \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j) = mn = \deg R(f, g)$ , 于是

$$\prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j) = \pm R(f, g).$$

注意

$$\prod_{i=1}^{m+n} \text{ent}_i R(f, g) = a_0^m b_m^n = (-1)^{mn} (y_1 y_2 \cdots y_m)^n,$$

$\prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j)$  中  $(y_1 y_2 \cdots y_m)^n$  的系数亦为  $(-1)^{mn}$ , 因此有

$$R(f, g) = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j).$$

□