結式與其應用

Timo Chang
timo65537@protonmail.com
譯者: 仙女國公主

最後編輯: 2026 年 1 月 19 日

本文介紹兩多項式的結式的概念, 並提供一些其在代數幾何學及數論上的應用.

1 結式

定義 1.1 (結式) 設 R 爲整環, $f,g\in R[x]$ 爲兩非零多項式, 設 $f(x)=\sum_{i=0}^{n}a_ix^i$, $g(x)=\sum_{j=0}^{m}b_jx^j$, $a_nb_m\neq 0$, 則將與 f 和 g 相關的西爾維斯特矩陣 $\mathrm{Syl}(f,g)$ 的行列式稱爲 f 和 g 的**結式**, 記作 $\mathcal{R}(f,g)$. 詳言之, 若 $n=m=0$, 則 $\mathcal{R}(f,g):=1$; 若 $n+m>0$, 則

$$\mathcal{R}(f,g):=\det\begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ \vdots & a_1 & & & \vdots & b_1 & & \\ a_n & \vdots & \ddots & & b_m & \vdots & \ddots & \\ & a_n & & a_0 & & b_m & & b_0 \\ & & & a_1 & & & & b_1 \\ & & (m\text{ 行}) & \vdots & & & (n\text{ 行}) & \vdots \\ & & & a_n & & & & b_m \end{pmatrix}_{(n+m)\times(n+m)}.$$

上述矩陣可如下理解: 設 F 爲 R 的分式體 (分式域), 將以 $\{1,x,\dots,x^n\}$ 爲有序基、含所有不超過 n 次的多項式的 F-線性空間記作 $P_n(F)$, 則對於如定義 1.1 所述的 f,g, 考慮線性映射

$$T_{f,g}:P_{m-1}(F)\times P_{n-1}(F)\longrightarrow P_{n+m-1}(F),\quad T_{f,g}(u,v):=fu+gv, \tag{1}$$

則不難看出 $T_{f,g}$ 的矩陣表示式恰為 $\mathrm{Syl}(f,g)$.

註記 1.2 定義 1.1 所述的結式可能和某些教材上不太一樣, 有的作者將多項式的各項係數以相反的順序來排列 (即降冪排列), 或者按列[1]排列, 而這些定義至多只有一個正負號之差.

[1]本講義中, 「 列 」是指橫排, 「 行 」是指縱排.

命題 1.3 設 $f, g \in R[x]$ 爲非零多項式, 又設 $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$, $g(x) = b\prod_{j=1}^{m}(x-\beta_j)$, 其中 α_i, β_j 分別爲 $f(x), g(x)$ 在 F 的某個代數閉包中的根 (不要求相異), 則

$$\mathcal{R}(f,g) = a^m b^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\beta_j - \alpha_i) = b^n f(\beta_1)\cdots f(\beta_m) = (-1)^{nm} a^m g(\alpha_1)\cdots g(\alpha_n).$$

證明 只需證明第一條等式. 設

$$\tilde{f} := a\prod_{i=1}^{n}(x - X_i) \quad 及 \quad \tilde{g} := b\prod_{j=1}^{m}(x - Y_j),$$

其中 X_i, Y_j 爲不定元. 視 $\tilde{f}, \tilde{g}$ 爲 $F\left[X_1, \ldots, X_n, Y_1, \ldots, Y_m\right][x]$ 的元素, 只要證明

$$\mathcal{R}_x(\tilde{f}, \tilde{g}) = a^m b^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (Y_j - X_i),$$

而結論可由下列賦值映射直接推得:

$$(X_1, \ldots, X_n, Y_1 \ldots, Y_m) \longmapsto (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m).$$

設 $K := F(X_1, \ldots, X_n, Y_1 \ldots, Y_m)$ 爲在 F 上加入這 $n+m$ 個變元的有理函數體, 並視 $\tilde{f}, \tilde{g} \in K[x]$. 考慮下述 K-線性映射:

$$T : P_{m-1}(K) \times P_{n-1}(K) \longrightarrow P_{n+m-1}(K) \longrightarrow K^{n+m},$$

其中第一個映射定義成

$$(u, v) \mapsto \tilde{f}u + \tilde{g}v,$$

第二個映射則定義成賦值映射

$$h(x) \mapsto (h(Y_1), \ldots, h(Y_m), h(X_1), \ldots, h(X_n)).$$

於是, 關於 $P_n(K)$ 的標準有序基及 K^{n+m} 的標準基, 可看出:

- 第一個映射的矩陣表示式爲與 $\tilde{f}$ 和 $\tilde{g}$ 相關的西爾維斯特矩陣 $\mathrm{Syl}(\tilde{f}, \tilde{g})$;
- 第二個映射的矩陣表示式爲范德蒙矩陣

$$V := \begin{pmatrix} 1 & Y_1 & \cdots & Y_1^{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & Y_m & \cdots & Y_m^{n+m-1} \\ 1 & X_1 & \cdots & X_1^{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & \cdots & X_n^{n+m-1} \end{pmatrix}_{(n+m)\times(n+m)} ;$$

- 合成映射 T 的矩陣表示式爲

$$\begin{pmatrix} B & O \\ O & A \end{pmatrix}_{(n+m)\times(n+m)},$$

其中,

$$B = \left(Y_i^{j-1}\tilde{f}(Y_i)\right)_{m\times m} \quad \text{及} \quad A = \left(X_i^{j-1}\tilde{g}(X_i)\right)_{n\times n}.$$

那麼, 我們有

$$V \cdot \mathrm{Syl}(\tilde{f},\tilde{g}) = \begin{pmatrix} B & O \\ O & A \end{pmatrix}.$$

取行列式, 可得

$$\det V \cdot \mathcal{R}_x(\tilde{f},\tilde{g}) = \det B \cdot \det A.$$

因此, 根據范德蒙行列式的一些基本事實, 有

$$\begin{aligned} &\left(\prod_{i<j} Y_j - Y_i\right)\left(\prod_{i<j} X_j - X_i\right)\left(\prod_{i,j} X_i - Y_j\right)\cdot \mathcal{R}_x(\tilde{f},\tilde{g}) \\ &= \tilde{f}(Y_1)\cdots\tilde{f}(Y_m)\tilde{g}(X_1)\cdots\tilde{g}(X_n)\cdot\left(\prod_{i<j} Y_j - Y_i\right)\left(\prod_{i<j} X_j - X_i\right). \end{aligned}$$

最後, 消去所有公因子, 即得

$$\mathcal{R}_x(\tilde{f},\tilde{g}) = a^m b^n \prod_{\substack{1\le i\le n \\ 1\le j\le m}} (Y_j - X_i),$$

證畢. □

從命題 1.3 立刻可推得一些結果.

系理 1.4 (1) 對所有非零多項式 $f, g \in R[x]$, 若 $n = \deg f$, $m = \deg g$, 則 $\mathcal{R}(f,g) = (-1)^{nm}\cdot\mathcal{R}(g,f)$.

(2) 對所有非零多項式 $f_1, f_2, g \in R[x]$, 有 $\mathcal{R}(f_1 f_2, g) = \mathcal{R}(f_1,g)\cdot\mathcal{R}(f_2,g)$.

(3) 對所有非零多項式 $f, g_1, g_2 \in R[x]$, 有 $\mathcal{R}(f, g_1 g_2) = \mathcal{R}(f,g_1)\cdot\mathcal{R}(f,g_2)$.

(4) 若且唯若 $\mathcal{R}(f,g) = 0$, 則 $f(x), g(x)$ 在 F 的代數閉包中有公共根.

例 1.5 考慮 $\mathbb{Q}[x]$ 中的多項式 $f(x) = x^4 + 4x^2 + 3x + 4$ 及 $g(x) = 2x^3 - 3x^2 - 3x - 5$, 則

$$\mathcal{R}(f,g) = \det\begin{pmatrix} 4 & & & -5 & & & \\ 3 & 4 & & -3 & -5 & & \\ 4 & 3 & 4 & -3 & -3 & -5 & \\ 0 & 4 & 3 & 2 & -3 & -3 & -5 \\ 1 & 0 & 4 & & 2 & -3 & -3 \\ & 1 & 0 & & & 2 & -3 \\ & & 1 & & & & 2 \end{pmatrix} = 0.$$

故依系理 1.4(4), f, g 在 $\overline{\mathbb{Q}}$ 中有公共根. 事實上, 不難看出 $f(x) = (x^2 + x + 1)(x^2 - x + 4)$ 及 $g(x) = (x^2 + x + 1)(2x - 5)$, 所以它們的公共根爲 $\left(-1 \pm \sqrt{-3}\right)/2$.

命題 1.6 設 $f, g \in R[x]$ 分別爲次數爲 n, m 的兩非零多項式, 則存在 $u, v \in R[x]$, $\deg u < m$, $\deg v < n$, 使得

$$fu + gv = \mathcal{R}(f, g).$$

證明 考慮如 (1) 的線性映射 $T_{f,g}$, 其矩陣表示式爲西爾維斯特矩陣 $\mathrm{Syl}(f, g)$, 則需要證明 $\mathcal{R}(f, g) \in R \subseteq P_{n+m-1}(F)$ 作爲常值多項式在 $T_{f,g}$ 的像空間中. 等價地, 設

$$u(x) = u_0 + u_1 x + \cdots + u_{m-1} x^{m-1} \quad \text{及} \quad v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1},$$

則欲解線性方程組

$$\mathrm{Syl}(f, g) \begin{pmatrix} u_0 \\ \vdots \\ u_{m-1} \\ v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} = \begin{pmatrix} \mathcal{R}(f, g) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

根據定義 1.1, $\mathcal{R}(f, g) := \det \mathrm{Syl}(f, g)$, 所以只要 $\mathcal{R}(f, g) \neq 0$, 便由克拉瑪法則可知方程組有解, 其解向量的元均在 R 中. 另一方面, 若 $\mathcal{R}(f, g) = 0$, 則矩陣 $\mathrm{Syl}(f, g)$ 是奇異矩陣, 故有非平凡零空間, 也因此可取適合的解, 使得對每個 i, j, 均有 $u_i, v_j \in R$. □

2 應用於代數幾何學中

2.1 兩平面曲線的交點

給定兩多項式 $f(x, y), g(x, y) \in \mathbb{C}[x, y]$, 我們想要尋求一種方法來求它們的公共根, 即解方程組

$$\begin{cases} f(x, y) = 0, \\ g(x, y) = 0. \end{cases}$$

從幾何的觀點來看, 相當於在求兩平面曲線的交點.

我們可以透過固定任意 $y = y_0 \in \mathbb{C}$ 來將問題化約為求解一元方程組

$$\begin{cases} f(x, y_0) = 0, \\ g(x, y_0) = 0. \end{cases}$$

依系理 1.4(4), 可知上述方程組有解的充要條件為 $\mathcal{R}_x\left(f\left(x, y_0\right), g\left(x, y_0\right)\right) = 0$. 將 $f(x, y)$、$g(x, y)$ 視為屬於 $\mathbb{C}[y][x]$ 中的多項式時, 該量可理解為 $\mathcal{R}_x(f(x, y), g(x, y)) \in \mathbb{C}[y]$ 在 $y = y_0$ 處的值, 這啟發了一種求交點的方式:

(1) 求 $\mathcal{R}_x(f(x,y),g(x,y))\in\mathbb{C}[y]$ 的根.

(2) 對於上述求得的每一個根 $y=y_0$, 解一元方程組

$$\begin{cases} f(x,y_0)=0,\\ g(x,y_0)=0. \end{cases}$$

當然, x 和 y 的角色可對調.

例 2.1 先來考慮一個簡單的例子, 比如說求解方程組

$$\begin{cases} x^3-x^2-2x-y^2=0,\\ x^2-2x+y^2=0. \end{cases} \tag{2}$$

當然, 這很容易可直接求解, 但我們使用上述方法來求解. 步驟一, 計算 $\mathcal{R}_y(f(x,y),g(x,y))$ 看起來比較簡單. 由於

$$\begin{aligned}\mathcal{R}_y(f(x,y),g(x,y)) &= \det\begin{pmatrix} x^3-x^2-2x & & x^2-2x & \\ 0 & x^3-x^2-2x & 0 & x^2-2x\\ -1 & 0 & 1 & 0\\ & -1 & & 1 \end{pmatrix}\\ &= x^2(x-2)^2(x+2)^2,\end{aligned}$$

故有 $x=0,\pm2$.

步驟二, 考慮三個分別對應 $x=0,\pm2$ 的一元方程組:

$$x=0\implies\begin{cases}-y^2=0,\\ y^2=0,\end{cases}\qquad x=2\implies\begin{cases}-y^2=0,\\ y^2=0,\end{cases}\qquad x=-2\implies\begin{cases}-8-y^2=0,\\ 8+y^2=0.\end{cases}$$

因此, 方程組 (2) 的解爲 $(0,0),(2,0),\left(-2,\pm2\sqrt{2}i\right)$.

例 2.2 現在來看看更複雜的例子, 如

$$\begin{cases} x^3-2x^2y^2+xy^4-y^5=0,\\ x^2-y^3-y^4=0. \end{cases}$$

不難算出

$$\mathcal{R}_x(f(x,y),g(x,y))=y^9(4y^2+4y-1),$$

故 $y=0,\left(-1\pm\sqrt{2}\right)/2$, 即得三個一元方程組. 下一步即求解該三個方程組, 具體過程留作習題, 最終可得解爲

$$(0,0),\left(\frac{-1+\sqrt{2}}{4},\frac{-1+\sqrt{2}}{2}\right),\left(\frac{-1-\sqrt{2}}{4},\frac{-1-\sqrt{2}}{2}\right).$$

2.2 有理參數曲線的直角坐標方程

上一個應用的想法亦可用於求有理參數平面曲線的直角座標方程. 設曲線 C 的參數方程式為

$$(x(t), y(t)) = \left(\frac{p(t)}{q(t)}, \frac{r(t)}{s(t)}\right),$$

其中, $p, q, r, s \in \mathbb{C}[t]$, $\gcd(p, q) = \gcd(r, s) = 1$. 注意到, 若且唯若 $(x_0, y_0) \in C$, 則

$$\begin{cases} x_0 q(t) - p(t) = 0, \\ y_0 s(t) - r(t) = 0 \end{cases}$$

有解, 除非 t 是 $q(t)$ 和 $s(t)$ 的 (有限多) 根的其中一者. 依系理 1.4(4), 這等價於結式 $\mathcal{R}_t(x_0 q(t) - p(t), y_0 s(t) - r(t)) = 0$. 因此, 曲線 C 可由方程

$$\mathcal{R}_t(xq(t) - p(t), ys(t) - r(t)) \in \mathbb{C}[x, y]$$

確定.

例 2.3 考慮曲線 C, 其參數方程爲

$$(x(t), y(t)) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1}\right),$$

則

$$\mathcal{R}_t(x(t^2 + 1) - (t^2 - 1), y(t^2 + 1) - (2t)) = 4x^2 + 4y^2 - 4,$$

故 C 由方程式 $x^2 + y^2 - 1 = 0$ 確定, 其可參數化爲上述給定的 $(x(t), y(t))$ (除了點 $(1, 0) \in C$).

2.3 希爾伯特零點定理

還記得以前學過, 對於多項式環 $\mathbb{C}[x_1, \ldots, x_n]$ 的某個子集 S, 其相應的**代數集**為

$$V(S) := \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid \forall f \in S, f(a_1, \ldots, a_n) = 0\},$$

下面我們藉助結式來證明代數幾何學中的重要定理, 稱為希爾伯特零點定理.

定理 2.4 (希爾伯特零點定理 (弱形式)) 給定 $\mathbb{C}[x_1, \ldots, x_n]$ 的理想 I, 或者 $1 \in I$, 或者 $V(I) \neq \varnothing$.

證明 對 n 作歸納法. 當 $n = 1$ 時, $I = (f(x_1))$ 是主理想. 於是, $1 \in I$ 等價於 $f \in \mathbb{C}^\times$ 爲常數, 而依代數學基本定理, 這又等價於 $V(f) = \varnothing$. 因此, 當 $n = 1$ 時, 命題成立.

現設 $n > 1$, 且假設 $1 \notin I$, 進一步可假設 $I \neq 0$, 否則就有 $V(I) = V(0) = \mathbb{C}^n \neq \varnothing$. 於是, I 含有非常數多項式 g. 透過變數變換

$$(x_1, \ldots, x_{n-1}, x_n) \longmapsto (x_1 + x_n^N, \ldots, x_{n-1} + x_n^{N^{n-1}}, x_n),$$

其中 N 是大於 g 的次數的任意正整數, 可得另一個含有關於 x_n 首一的多項式的理想 J.[2] 又注意到 $1 \in I \iff 1 \in J$, 以及 $V(I) \neq \varnothing \iff V(J) \neq \varnothing$, 故可進一步假設 g 是關於 x_n 首一的多項式.

考慮 $\mathbb{C}[x_1, \ldots, x_{n-1}]$ 中的理想 $I' := I \cap \mathbb{C}[x_1, \ldots, x_{n-1}]$, 注意到 $1 \notin I'$, 故依歸納假設, 有 $V(I') \neq \varnothing$, 因此存在 $(a_1, \ldots, a_{n-1}) \in V(I')$. 斷言: 理想

$$I'' := \{f(a_1, \ldots, a_{n-1}, x_n) \mid f \in I\}$$

是 $\mathbb{C}[x_n]$ 的眞理想. 如果已確定該斷言正確, 那麼就有 $1 \notin I''$, 從而由 $n = 1$ 的情形, 有 $V(I'') \neq \varnothing$, 不妨設 $a_n \in V(I'')$, 此時對所有 $f \in I$, $f(a_1, \ldots, a_{n-1}, a_n) = 0$ 均成立, 即 $(a_1, \ldots, a_{n-1}, a_n) \in V(I)$, 所以 $V(I) \neq \varnothing$.

現在只需要證出上述斷言. 假設 $I'' = \mathbb{C}[x_n]$, 則存在 $f \in I$ 使得 $f(a_1, \ldots, a_{n-1}, x_n) = 1$. 回顧一下, 我們當初取了關於 x_n 首一的非常數多項式 $g \in I$, 現將 f, g 視爲 $\mathbb{C}[x_1, \ldots, x_{n-1}][x_n]$ 的元素, 考察 $\mathcal{R}_{x_n}(f, g)$. 於是, 依命題 1.6, 存在 $u, v \in \mathbb{C}[x_1, \ldots, x_{n-1}][x_n]$ 使得 $\mathcal{R}_{x_n}(f, g) = fu + gv$.

- 因爲 $f, g \in I$, 所以 $\mathcal{R}_{x_n}(f, g) \in I$, 而且是 $\mathbb{C}[x_1, \ldots, x_{n-1}]$ 中的多項式, 故 $\mathcal{R}_{x_n}(f, g) \in I'$. 又 $(a_1, \ldots, a_{n-1}) \in V(I')$, 因此 $\mathcal{R}_{x_m}(f, g)(a_1, \ldots, a_{n-1}) = 0$.
- 另一方面, 記 $f = \sum_{i=0}^{r} f_i x_n^i$, $g = \sum_{j=0}^{s} g_j x_n^j$ 爲 x_n 的多項式, 其中 $f_i, g_j \in \mathbb{C}[x_1, \ldots, x_{n-1}]$, 則根據我們對 f 和 g 的假設, 有

$$\begin{cases} f_0(a_1, \ldots, a_{n-1}) = 1, \\ f_i(a_1, \ldots, a_{n-1}) = 0, \quad i = 1, \ldots, r, \\ g_s(x_1, \ldots, x_{n-1}) = 1. \end{cases}$$

  因此, 在代入 $(a_1, \ldots, a_{n-1})$ 後, $\mathcal{R}_{x_n}(f, g)$ 對應的矩陣是上三角矩陣, 其對角元全爲 1. 特別地, $\mathcal{R}_{x_n}(f, g)(a_1, \ldots, a_{n-1}) = 1$.

因此得到了矛盾. □

3 應用於數論中

3.1 多項式的判別式

在 §3.1 中, 我們總假定 $\mathrm{char}(F) = 0$. 對於首一多項式 $f(x) \in F[x]$, 將其表示為 $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$, 其中對所有 i, α_i 屬於 F 的某個固定的代數閉包. 回顧一下, f 的**判別式**為

$$\mathrm{disc}(f) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in F.$$

下述命題用結式來給出判別式的等價定義.

[2] 對 g 中每個非零的項 $cx_1^{d_1} \cdots x_n^{d_n}$ 作變數變換後可得 $c(x_1 + x_n^N)^{d_1} \cdots (x_{n-1} + x_n^{N^{n-1}})^{d_{n-1}} x_n^{d_n}$, 可見有唯一的最高次項, 爲 $cx_n^{d_n + d_1 N + \cdots + d_{n-1} N^{n-1}}$. 由於在每個可能 i 都滿足 $N > d_i$ 的條件之下, g 的各項均產生不同的該項, 在作變數變換後必存在唯一的最高次項. 現調整係數使之關於 x_n 是首一的多項式.

命題 3.1 設 $f(x) \in F[x]$ 爲首一多項式, 則

$$\operatorname{disc}(f) = (-1)^{n(n-1)/2}\mathcal{R}(f, f').$$

證明 注意到

$$f'(x) = \sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j),$$

所以

$$f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j).$$

因此, 依命題 1.3, 可得

$$\mathcal{R}(f,f') = (-1)^{n(n-1)}\prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n}\prod_{j\neq i}(\alpha_i-\alpha_j) = (-1)^{n(n-1)/2}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2.$$

□

例 3.2 考慮二次多項式 $f(x) = x^2 + bx + c \in \mathbb{C}[x]$ 及其導數 $f'(x) = 2x + b$. 依命題 3.1, f 的判別式爲

$$\operatorname{disc}(f) = -\mathcal{R}(f, f') = b^2 - 4c,$$

且依系理 1.4(4), 若且唯若 f 和 f' 在 $\mathbb{C}$ 中有公共根, 則 $b^2 - 4c = 0$, 即 f 在 $\mathbb{C}$ 中有重根.

例 3.3 現考慮三次多項式 $f(x) = x^3 + ax + b \in \mathbb{C}[x]$ 及其導數 $f'(x) = 3x^2 + a$. 依命題 3.1,

$$\operatorname{disc}(f) = (-1)^3\mathcal{R}(f, f') = -4a^3 - 27b^2,$$

且依系理 1.4(4), 若且唯若 f 在 $\mathbb{C}$ 中有重根, 則 $4a^3 + 27b^2 = 0$.

3.2 代數元所構成的體

設 E/F 為任意體擴張, 定義 $F^{\mathrm{alg}}(E) := \{\alpha \in E \mid \alpha \text{ 在 } F \text{ 上是代數元}\}$, 稱為 F 在 E 中的**代數閉包**, 則有基本事實指出 $F^{\mathrm{alg}}(E)$ 是體, 即: 對於 F 上的一切代數元 $\alpha, \beta \in E$, $\alpha + \beta$, $\alpha\beta$, 及 $1/\alpha$ ($\alpha \neq 0$) 均為 F 上的代數元. 該事實之標準的證明使用了基本的體論, 但其證明較為隱晦, 因為並未明示這些值所滿足的多項式. 使用結式可以得到該事實的建構式證明, 亦即, 我們可具體地構造出 $\alpha + \beta$, $\alpha\beta$, 及 $1/\alpha$ 在 F 上滿足的多項式.

命題 3.4 設 E/F 爲體擴張, $\alpha, \beta \in F^{\mathrm{alg}}(E)$, 且對於某兩非零多項式 $f(x), g(x) \in F[x]$, 有 $f(\alpha) = g(\beta) = 0$. 設

$$h_1(y) := \mathcal{R}_x(f(y-x), g(x)) \quad \text{及} \quad h_2(y) := \mathcal{R}_x(x^{\deg f} f(y/x), g(x)),$$

則有 $h_1(\alpha + \beta) = h_2(\alpha\beta) = 0$. 特別地, $\alpha + \beta, \alpha\beta \in F^{\mathrm{alg}}(E)$, 而且只要 f, g 是首一多項式, h_1, h_2 便也是首一多項式.

證明　因 $f(\alpha)=g(\beta)=0$, 可記

$$f(x)=a\prod_{i=1}^{n}(x-\alpha_i)\quad 及\quad g(x)=b\prod_{j=1}^{m}(x-\beta_j),$$

其中 α_i,β_j 分別是 $f(x),g(x)$ 的根, $\alpha_1=\alpha$, $\beta_1=\beta$. 先計算 $h_1(y)$. 注意到

$$f(y-x)=a\prod_{i=1}^{n}(y-x-\alpha_i)=a(-1)^n\prod_{i=1}^{n}(x-(y-\alpha_i)),$$

依命題 1.3, 有

$$h_1(y)=(a(-1)^n)^m b^n\prod_{\substack{1\le i\le n\\1\le j\le m}}(\beta_j-(y-\alpha_i))=a^m b^n\prod_{\substack{1\le i\le n\\1\le j\le m}}(y-(\alpha_i+\beta_j)).$$

因此, $h_1(\alpha+\beta)=h_1(\alpha_1+\beta_1)=0$, 並且只要 f,g 爲首一多項式 (即 $a=b=1$), $h_1(y)$ 便亦是首一多項式.

接著, 計算 $h_2(y)$. 不失一般性, 假設沒有任何 α_i 爲零, 則

$$x^{\deg f}f(y/x)=x^n a\prod_{i=1}^{n}\left(\frac{y}{x}-\alpha_i\right)=a\prod_{i=1}^{n}(y-\alpha_i x)=a\prod_{i=1}^{n}(-\alpha_i)\cdot\prod_{i=1}^{n}\left(x-\frac{y}{\alpha_i}\right),$$

故依命題 1.3, 有

$$h_2(y)=\left(a\prod_{i=1}^{n}(-\alpha_i)\right)^m b^n\prod_{\substack{1\le i\le n\\1\le j\le m}}\left(\beta_j-\frac{y}{\alpha_i}\right)=a^m b^n\prod_{\substack{1\le i\le n\\1\le j\le m}}(y-\alpha_i\beta_j).$$

因此, $h_2(\alpha\beta)=h_2(\alpha_1\beta_1)=0$, 且當 f,g 爲首一多項式時, $h_2(y)$ 是首一多項式. □

註記 3.5　命題 3.4 的另證如下: 依命題 1.6, 存在 $u_1(x,y),v_1(x,y)\in F[y][x]$ 滿足

$$h_1(y)=f(y-x)u_1(x,y)+g(x)v_1(x,y).$$

將 $(x,y)=(\beta,\alpha+\beta)$ 代入即得第一個結果. 類似地, 存在 $u_2(x,y),v_2(x,y)\in F[y][x]$ 使得

$$h_2(y)=x^{\deg f}f(y/x)u_2(x,y)+g(x)v_2(x,y).$$

此時, 將 $(x,y)=(\beta,\alpha\beta)$ 代入 (不妨假設 $\beta\neq 0$).

例 3.6　作爲例子, 在 $\mathbb{C}$ 中取 $\alpha=\left(-1+\sqrt{-3}\right)/2$ 及 $\beta=\sqrt[3]{2}$, 則 α 滿足 $f(x)=x^2+x+1$, 且 β 滿足 $g(x)=x^3-2$. 讓我們來計算 $h_1(y)$ 及 $h_2(y)$.

首先, 觀察出

$$f(y-x)=x^2+(-2y-1)x+(y^2+y+1),$$

於是

$$h_1(y)=\mathcal{R}_x(f(y-x),g(x))=y^6+3y^5+6y^4+3y^3+9y+9.$$

並且命題 3.4 告訴我們, $\alpha+\beta$ 是 $h_1(y)$ 的一根. 另一方面, 還有

$$x^{\deg f} f(y/x) = x^2 + yx + y^2,$$

於是

$$h_2(y) = \mathcal{R}_x(x^{\deg f} f(y/x), g(x)) = (y^3-2)^2,$$

並且命題 3.4 告訴我們, $\alpha\beta$ 是 $h_2(y)$ 的一根 (其實我們有點像是殺雞用牛刀, 注意到 $\alpha^3=1$, 即 α 是三次單位根, 故顯而易見 $\alpha\beta$ 滿足多項式 y^3-2).

系理 3.7 $F^{\mathrm{alg}}(E)$ 是體.

證明 依命題 3.4, 可知 $F^{\mathrm{alg}}(E)$ 在加法及乘法運算之下封閉. 爲了完成證明, 僅需要證明 $F^{\mathrm{alg}}(E)$ 在取乘法逆運算之下是封閉的. 不過容易看出, 只要 $\alpha\neq 0$ 滿足 $f(x)\in F[x]$, $\deg f = n > 0$, 那麼 $1/\alpha$ 便會滿足 $x^n f(1/x)\in F[x]$. □

系理 3.8 代數數集 $\overline{\mathbb{Q}}$ 是體.

證明 依定義, $\overline{\mathbb{Q}} := \mathbb{Q}^{\mathrm{alg}}(\mathbb{C})$. □

設 $\alpha\in F^{\mathrm{alg}}(E)$, 用歸納法以及命題 3.4, 對所有 $n\in\mathbb{N}$, 均可求出 α^n 所滿足的多項式, 也因此可求出 $F(\alpha)$ 的任一元素所滿足的多項式. 下一個命題提供了另一種建構該多項式的方法.

命題 3.9 設 E/F 爲體擴張, 且 $\alpha\in F^{\mathrm{alg}}(E)$ 滿足某非零多項式 $f(x)\in F[x]$. 對任何 $\beta := g(\alpha)$, 其中 $g(x)\in F[x]$, 令

$$h(y) := \mathcal{R}_x(f(x), y-g(x)),$$

則有 $h(\beta)=0$.

證明 依命題 1.6, 存在 $u(x,y), v(x,y)\in F[y][x]$ 使得

$$h(y) = f(x)u(x,y) + (y-g(x))v(x,y).$$

將 $(x,y)=(\alpha,\beta)$ 代入即得結論. □

例 3.10 考慮二次多項式 $f(x)=x^2+bx+c\in\mathbb{Q}[x]$, α 是其一根. 取 $g(x) := -x-b$ 及 $\beta := g(\alpha) = -\alpha - b$, 則依命題 3.9, β 滿足

$$h(y) = \mathcal{R}_x(f(x), y-g(x)) = y^2+by+c = f(y),$$

故 β 其實是 $f(x)$ 的另一根 (注意到 $f(x)$ 的兩根之和爲 $-b$).