

Remark 1.2. The resultant defined in Definition 1.1 may not be exactly the same as in other references. Some authors put these coefficients in reverse order (i.e., with decreasing indices), or in rows. But these definitions are the same up to a sign multiple.

Proposition 1.3. *Let $f, g \in R[x]$ be non-zero polynomials. Suppose $f(x) = a \prod_{i=1}^n (x - \alpha_i)$ and $g(x) = b \prod_{j=1}^m (x - \beta_j)$ where α_i, β_j are the roots of $f(x), g(x)$ (not necessarily distinct), respectively, lying in a fixed algebraic closure of F . Then*

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

Proof. It suffices to prove the first equality. Set

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

where X_i, Y_j are indeterminates. Viewing \tilde{f}, \tilde{g} as elements in $F[X_1, \dots, X_n, Y_1, \dots, Y_m][x]$, we prove that

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

And the result will follow from the specialization

$$(X_1, \dots, X_n, Y_1, \dots, Y_m) \mapsto (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m).$$

Let $K := F(X_1, \dots, X_n, Y_1, \dots, Y_m)$ be the rational function field over F joining these $n + m$ variables. We view $\tilde{f}, \tilde{g} \in K[x]$. Consider the following K -linear transformation

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

where the first map is given by

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

and the second map is given by the evaluation map

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

Then with respect to the standard ordered basis of $P_n(K)$ and the canonical basis of K^{n+m} , we see that

- the first map is represented by the Sylvester matrix $\text{Syl}(\tilde{f}, \tilde{g})$ associated to \tilde{f} and \tilde{g} ;

- the second map is represented by the Vandermonde matrix

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

- the composite map T is represented by

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

where

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

Hence, we have

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

Taking determinants yields

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

So from the well known fact about the determinant of Vandermonde matrices, we have

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

Finally, we cancel out all the common terms and obtain

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

This completes the proof. □

There are some immediate consequences of Proposition 1.3.

Corollary 1.4. (1) $\mathcal{R}(f, g) = (-1)^{nm} \cdot \mathcal{R}(g, f)$ for every non-zero $f, g \in R[x]$, where $n = \deg f$ and $m = \deg g$.

2 Applications in Algebraic Geometry

2.1 Intersection of two Plane Curves

Given two polynomials $f(x, y), g(x, y) \in \mathbb{C}[x, y]$, we ask for a method to find their common roots. That is, we want to solve the system of equations

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

Geometrically speaking, we look for the intersections of any two plane curves.

We can reduce this problem by fixing any $y = y_0 \in \mathbb{C}$, and solve the one-variable system of equations

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

By Corollary 1.4(4), we know the solution exists if and only if $\mathcal{R}_x(f(x, y_0), g(x, y_0)) = 0$. Viewing $f(x, y), g(x, y) \in \mathbb{C}[y][x]$, this quantity can be thought of as $\mathcal{R}_x(f(x, y), g(x, y)) \in \mathbb{C}[y]$ specialized at $y = y_0$. This suggests a process of finding the intersection points:

- (1) Find the roots of $\mathcal{R}_x(f(x, y), g(x, y)) \in \mathbb{C}[y]$.
- (2) For each such root $y = y_0$, solve the one-variable system of equations

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

Of course, the role of x and y is interchangeable.

Example 2.1. Let us first consider a simple example. Say we want to solve the system of equations

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

Surely, this is simple enough to solve directly. But let us use the method described above. For step one, it seems easier to compute $\mathcal{R}_y(f(x, y), g(x, y))$. We find that

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

So $x = 0, \pm 2$.

For step two, we consider three one-variable systems of equations, which correspond respectively to $x = 0, \pm 2$.

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

So the solutions to the original system of equations (2) are $(0, 0), (2, 0), (-2, \pm 2\sqrt{2}i)$.

Example 2.2. We now consider a more complicated example. Say

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

We find that

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

And so $y = 0, (-1 \pm \sqrt{2})/2$. This gives three one-variable systems of equations. The next step is to find all of their solutions. We will leave this as an exercise. The solutions are

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

2.2 The Defining Equation of a Rational Parameterized Curve

The idea in the previous application can be used to find the defining equation of a rational parameterized plane curve. Given a curve C defined by the parametric equation

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

where $p, q, r, s \in \mathbb{C}[t]$ with $\gcd(p, q) = \gcd(r, s) = 1$. Note that a point $(x_0, y_0) \in C$ if and only if

$$\begin{cases} x_0q(t) - p(t) = 0, \\ y_0s(t) - r(t) = 0 \end{cases}$$

has a solution, except when t is one of the (finitely many) roots of $q(t)$ and $s(t)$. And by Corollary 1.4(4), this is equivalent to say that the resultant $\mathcal{R}_t(x_0q(t) - p(t), y_0s(t) - r(t)) = 0$. Hence, the curve C can be defined by the equation

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

Example 2.3. Consider a curve C with the parametric equation

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

Then

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

So C is defined by the equation $x^2 + y^2 - 1 = 0$, which is parameterized by the given $(x(t), y(t))$ (except for the point $(1, 0) \in C$).

2.3 Hilbert Nullstellensatz

Recall for a subset S in the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$, the corresponding *algebraic set* is defined as

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

Below we prove the important theorem in algebraic geometry, called Hilbert Nullstellensatz, with the help of resultant.

Theorem 2.4 (Hilbert Nullstellensatz (Weak Version)). *Given an ideal I in $\mathbb{C}[x_1, \dots, x_n]$, either $1 \in I$ or $V(I) \neq \emptyset$.*

Proof. We proceed by induction on n . When $n = 1$, we have $I = (f(x_1))$ is principal. Then $1 \in I$ if and only if $f \in \mathbb{C}^\times$ is a constant if and only if $V(f) = \emptyset$ by fundamental theorem of algebra. So the case $n = 1$ is true.

Suppose now $n > 1$ and assume $1 \notin I$. We may also assume $I \neq 0$ because otherwise, we have $V(I) = V(0) = \mathbb{C}^n \neq \emptyset$. Thus, I contains a non-constant polynomial g . Note by change of variables

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

where N is any natural number greater than the total degree of g , we obtain another ideal J so that it contains an element which is monic in x_n .¹ And note that we have $1 \in I \iff 1 \in J$ and $V(I) \neq \emptyset \iff V(J) \neq \emptyset$. So we may further assume g is monic in x_n .

Consider the ideal $I' := I \cap \mathbb{C}[x_1, \dots, x_{n-1}]$ in $\mathbb{C}[x_1, \dots, x_{n-1}]$. Note $1 \notin I'$, so by induction hypothesis, $V(I') \neq \emptyset$. Thus, there exists $(a_1, \dots, a_{n-1}) \in V(I')$. We will claim that the ideal

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

is proper in $\mathbb{C}[x_n]$. Assume this for a moment, then we have $1 \notin I''$. So by the $n = 1$ case, $V(I'') \neq \emptyset$. Say $a_n \in V(I'')$. Then we have $f(a_1, \dots, a_{n-1}, a_n) = 0$ for all $f \in I$. That is, $(a_1, \dots, a_{n-1}, a_n) \in V(I)$. So $V(I) \neq \emptyset$.

¹For each non-zero term $cx_1^{d_1} \dots x_n^{d_n}$ in g , the change of variables gives $c(x_1 + x_n^N)^{d_1} \dots (x_{n-1} + x_n^{N^{n-1}})^{d_{n-1}} x_n^{d_n}$. One sees that there is a unique term with largest degree, namely, $cx_n^{d_n + d_1 N + \dots + d_{n-1} N^{n-1}}$. Since each term of g produces different such term as $N > d_i$ for all possible i , there exists a unique term with largest degree after the change of variables. Now, adjust the coefficient so that it is monic in x_n .

It remains to finish the claim. Suppose on the contrary that $I'' = \mathbb{C}[x_n]$. Then there exists $f \in I$ such that $f(a_1, \dots, a_{n-1}, x_n) = 1$. Now, recall that we chose a non-constant polynomial $g \in I$ which is monic in x_n . Viewing $f, g \in \mathbb{C}[x_1, \dots, x_{n-1}][x_n]$, we consider the resultant $\mathcal{R}_{x_n}(f, g)$. Then by Proposition 1.6, there exist $u, v \in \mathbb{C}[x_1, \dots, x_{n-1}][x_n]$ such that $\mathcal{R}_{x_n}(f, g) = fu + gv$.

- As $f, g \in I$, we have $\mathcal{R}_{x_n}(f, g) \in I$. Moreover, it is a polynomial in $\mathbb{C}[x_1, \dots, x_{n-1}]$. So $\mathcal{R}_{x_n}(f, g) \in I'$. And since $(a_1, \dots, a_{n-1}) \in V(I')$, we have $\mathcal{R}_{x_n}(f, g)(a_1, \dots, a_{n-1}) = 0$.
- On the other hand, write $f = \sum_{i=0}^r f_i x_n^i$ and $g = \sum_{j=0}^s g_j x_n^j$ as polynomials in x_n , where $f_i, g_j \in \mathbb{C}[x_1, \dots, x_{n-1}]$. Then by our assumptions on f and g , we have

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

So the matrix in $\mathcal{R}_{x_n}(f, g)$ specialized at (a_1, \dots, a_{n-1}) is upper triangular with 1 along the diagonal. In particular, $\mathcal{R}_{x_n}(f, g)(a_1, \dots, a_{n-1}) = 1$.

Hence, we are led to a contradiction. □

3 Applications in Number Theory

3.1 Discriminant of a Polynomial

In §3.1 only, we assume $\text{char}(F) = 0$. For a monic polynomial $f(x) \in F[x]$, write $f(x) = \prod_{i=1}^n (x - \alpha_i)$ where α_i lies in a fixed algebraic closure of F for all i . Recall the *discriminant* of f is defined as

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

The following proposition gives an equivalent definition of discriminant using resultant.

Proposition 3.1. *Let $f(x) \in F[x]$ be a monic polynomial. One has*

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

Proof. Note that

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

So

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

Thus, by Proposition 1.3, one sees that

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

□

Example 3.2. Consider the quadratic polynomial $f(x) = x^2 + bx + c \in \mathbb{C}[x]$ and its derivative $f'(x) = 2x + b$. By Proposition 3.1, the discriminant of f is

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

And by Corollary 1.4(4), $b^2 - 4c = 0$ if and only if f and f' share a common root in \mathbb{C} , i.e., f has multiple roots in \mathbb{C} .

Example 3.3. Now, consider the cubic polynomial $f(x) = x^3 + ax + b \in \mathbb{C}[x]$ and its derivative $f'(x) = 3x^2 + a$. By Proposition 3.1,

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

And by Corollary 1.4(4) again, we have $4a^3 + 27b^2 = 0$ if and only if f has multiple roots in \mathbb{C} .

3.2 The Field of Algebraic Elements

Let E/F be an arbitrary field extension. Define $F^{\text{alg}}(E) := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$, called the *algebraic closure of F in E* . Then it is a basic fact that $F^{\text{alg}}(E)$ is a field. That is, for any $\alpha, \beta \in E$ which are algebraic over F , we have $\alpha + \beta, \alpha\beta$, and $1/\alpha$ (when $\alpha \neq 0$) are all algebraic over F . A standard proof of this fact uses elementary field theory and is rather implicit in the sense that the polynomials satisfied by these values are not explicitly given. Using resultant, we give a constructive proof of this fact. Namely, we explicitly construct polynomials over F which are satisfied by $\alpha + \beta, \alpha\beta$, and $1/\alpha$.

Proposition 3.4. *Let E/F be a field extension and $\alpha, \beta \in F^{\text{alg}}(E)$ with $f(\alpha) = g(\beta) = 0$ for some non-zero $f(x), g(x) \in F[x]$. Put*

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

Then we have $h_1(\alpha + \beta) = h_2(\alpha\beta) = 0$. In particular, $\alpha + \beta, \alpha\beta \in F^{\text{alg}}(E)$. Moreover, if f, g are monic, then so are h_1, h_2 .

Proof. Since $f(\alpha) = g(\beta) = 0$, we can write

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

where α_i, β_j are the roots of $f(x), g(x)$, respectively, with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. We first calculate $h_1(y)$. Note that

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

So by Proposition 1.3, we have

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

It follows that $h_1(\alpha + \beta) = h_1(\alpha_1 + \beta_1) = 0$, and $h_1(y)$ is monic if f, g are monic as well (i.e., if $a = b = 1$).

Next, we calculate $h_2(y)$. Without loss of generality, we assume none of the α_i is zero. Then we see that

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

So by Proposition 1.3 again, we have

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

It follows that $h_2(\alpha\beta) = h_2(\alpha_1\beta_1) = 0$, and $h_2(y)$ is monic if f, g are monic as well. \square

Remark 3.5. An alternate proof for the first part of Proposition 3.4 goes as follows. By Proposition 1.6, we choose $u_1(x, y), v_1(x, y) \in F[y][x]$ such that

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

Plugging in $(x, y) = (\beta, \alpha + \beta)$ yields the first result. Similarly, choose $u_2(x, y), v_2(x, y) \in F[y][x]$ such that

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

This time, plug in $(x, y) = (\beta, \alpha\beta)$. (Note we may assume $\beta \neq 0$.)

Example 3.6. As an example, take $\alpha = (-1 + \sqrt{-3})/2$ and $\beta = \sqrt[3]{2}$ in \mathbb{C} . Then we know α satisfies $f(x) = x^2 + x + 1$ and β satisfies $g(x) = x^3 - 2$. Let us find $h_1(y)$ and $h_2(y)$.

First, we see that

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

So

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

And Proposition 3.4 says that $\alpha + \beta$ is a root of $h_1(y)$. On the other hand, we see that

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

So

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

And Proposition 3.4 says that $\alpha\beta$ is a root of $h_2(y)$. (Actually, what we did is quite overkill. Note that α is a roots of unity with $\alpha^3 = 1$, so clearly $\alpha\beta$ satisfies the polynomial $y^3 - 2$.)

Corollary 3.7. $F^{\text{alg}}(E)$ is a field.

Proof. By Proposition 3.4 we know $F^{\text{alg}}(E)$ is closed under addition and multiplication. To complete the proof, it remains to show that $F^{\text{alg}}(E)$ is closed under taking multiplicative inverse. But one sees that if $\alpha \neq 0$ satisfies $f(x) \in F[x]$ with $\deg f = n > 0$, then $1/\alpha$ satisfies $x^n f(1/x) \in F[x]$. \square

Corollary 3.8. The set of all algebraic numbers $\overline{\mathbb{Q}}$ is a field.

Proof. By definition, $\overline{\mathbb{Q}} := \mathbb{Q}^{\text{alg}}(\mathbb{C})$. \square

Let $\alpha \in F^{\text{alg}}(E)$. Using induction argument and Proposition 3.4, one can find polynomials satisfied by α^n for all $n \in \mathbb{N}$, and thus, by any element in $F(\alpha)$. The next proposition gives another way to construct such polynomials.

Proposition 3.9. Let E/F be a field extension and $\alpha \in F^{\text{alg}}(E)$ with $f(\alpha) = 0$ for some non-zero $f(x) \in F[x]$. For any $\beta := g(\alpha)$ where $g(x) \in F[x]$, put

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

Then we have $h(\beta) = 0$.

Proof. By Proposition 1.6, there exist $u(x, y), v(x, y) \in F[y][x]$ such that

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

The result now follows from plugging in $(x, y) = (\alpha, \beta)$. \square

Example 3.10. Consider the quadratic polynomial $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$ with a root α . Take $g(x) := -x - b$ and $\beta := g(\alpha) = -\alpha - b$. Then by Proposition 3.9, β satisfies

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

So β is actually another root of $f(x)$. (Recall also the fact that the sum of two roots of $f(x)$ is $-b$.)