Resultant and its Applications

Timo Chang
timo65537@protonmail.com

Last edited: January 5, 2025

In this essay, we introduce the notion of resultant of two polynomials, and give several applications in algebraic geometry and number theory.

1 Resultant

Definition 1.1 (Resultant)**.** Let R be an integral domain and $f, g \in R[x]$ be two non-zero polynomials. Write $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$ with $a_n b_m \neq 0$. The *resultant* of f and g, denoted as $\mathcal{R}(f, g)$, is the determinant of the Sylvester matrix $\operatorname{Syl}(f, g)$ associated to f and g. More precisely,

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

if $n + m > 0$ and $\mathcal{R}(f, g) := 1$ if $n = m = 0$.

The above matrix can be understood as follows: Let F be the field of fractions of R. Denote $P_n(F)$ the F-vector space consisting of all polynomials of degree not exceeding n and equip it with the standard ordered basis $\{1, x, \ldots, x^n\}$. Then for f, g as in the above definition, consider the linear transformation

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

Then one sees that the matrix representation of $T_{f,g}$ is precisely $\operatorname{Syl}(f, g)$.

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

Proposition 1.3. *With the notations as above. Suppose* $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ *and* $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$ *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*

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

Proof. It's sufficient to prove the first equality. Set

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

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

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

And the result will follow from the specialization

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

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

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

Finally, we cancel out all the common terms and obtain
$$\mathcal{R}_x(\tilde{f}, \tilde{g}) = a_n^m b_m^n \prod_{\substack{1\le i\le n \\ 1\le j\le m}} (Y_j - X_i).$$

This is exactly what we want. □

There are some immediate consequences of Proposition 1.3.

Corollary 1.4. *Let all notations be as above, then*
(1) $\mathcal{R}(f, g) = (-1)^{nm} \cdot \mathcal{R}(g, f)$.
(2) $\mathcal{R}(f_1 f_2, g) = \mathcal{R}(f_1, g) \cdot \mathcal{R}(f_2, g)$ *for non-zero* $f_1, f_2 \in R[x]$.
(3) $\mathcal{R}(f, g) = 0$ *if and only if* $f(x)$ *and* $g(x)$ *have a common root (in an algebraic closure of* F*).*

Example 1.5. Consider the polynomials $f(x) = x^4 + 4x^2 + 3x + 4$ and $g(x) = 2x^3 - 3x^2 - 3x - 5$ in $\mathbb{Q}[x]$. Note
$$\mathcal{R}(f, g) = \det \begin{pmatrix} 4 & & & -5 & & & \\ 3 & 4 & & -3 & -5 & & \\ 4 & 3 & 4 & -3 & -3 & -5 & \\ 0 & 4 & 3 & 2 & -3 & -3 & -5 \\ 1 & 0 & 4 & & 2 & -3 & -3 \\ & 1 & 0 & & & 2 & -3 \\ & & 1 & & & & 2 \end{pmatrix} = 0.$$

So they must share a common root in $\overline{\mathbb{Q}}$ by Corollary 1.4(3). In fact, one sees that $f(x) = (x^2+x+1)(x^2-x+4)$ and $g(x) = (x^2+x+1)(2x-5)$. So their common roots are $(-1 \pm \sqrt{-3})/2$.

Proposition 1.6. *Let $f, g \in R[x]$ be two non-zero polynomials of degree n, m, respectively. Then there exist $u, v \in R[x]$ with $\deg u < m$ and $\deg v < n$ such that*

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

Proof. Consider the linear transformation $T_{f,g}$ in (1), which is represented by the Sylvester matrix $\operatorname{Syl}(f, g)$. Then we are asked to show that $\mathcal{R}(f, g) \in R \subseteq P_{n+m-1}(F)$ (as constant polynomials) lies in the image of $T_{f,g}$. Equivalently, set

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

Then we want to solve the following system of linear equations:

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

Recall that by definition, $\mathcal{R}(f, g) := \det \operatorname{Syl}(f, g)$. So if $\mathcal{R}(f, g) \neq 0$, then by Cramer's rule we may obtain a solution, which can be seen to have all entries in R. On the other hand, if $\mathcal{R}(f, g) = 0$, then the matrix $\operatorname{Syl}(f, g)$ is singular. So it admits a non-trivial null space. Hence, we may choose a suitable solution so that $u_i, v_j \in R$ for all i, j. □

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, i.e., 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(3), 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 $y = y_0$, 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

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

Surely, this is simple enough to solve directly. Here we 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

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

So $x = 0, \pm 2$.

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

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

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 Implicit Function of a Rational Parameterized Curve

The idea in the previous application can be used to find an implicit function of a rational parameterized plane curve. Given a curve C defined by $f(x,y) = 0$ with a 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 $\gcd(p,q) = \gcd(r,s) = 1$. This means we have $f(x(t), y(t)) = 0$ for all t. Note that a point $(x_0, y_0) \in C$ if and only if

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

has a solution, except when t is one of the (finitely many) roots of $q(t)$ and $s(t)$. And by Corollary 1.4(3), this is equivalent to say that the resultant $\mathcal{R}_t(x_0 q(t) - p(t), y_0 s(t) - r(t)) = 0$. Hence, the curve C can be defined by the implicit function

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

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 $x^2 + y^2 - 1$, 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 $\mathbb{C}[x_1, \ldots, x_n]$, either $1 \in I$ or $V(I) \neq \varnothing$.*

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 $V(f) = \varnothing$ 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 $V(I) = V(0) = \mathbb{C}^n \neq \varnothing$. Thus, I contains a non-constant polynomial g. Note by change of variables

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

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 $V(I) \neq \varnothing \iff V(J) \neq \varnothing$. So we may further assume g is monic in x_n.

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

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

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

It remains to finish the claim. Suppose on the contrary that $I'' = \mathbb{C}[x_n]$. Then there exists $f \in I$ such that $f(a_1, \ldots, a_{n-1}, x_n) = 1$. Now, recall that we chose a non-constant polynomial $g \in I$ which is monic in x_n. Viewing $f, g \in \mathbb{C}[x_1, \ldots, x_{n-1}][x_n]$, we consider the resultant $\mathcal{R}_{x_n}(f, g)$. Then by Proposition 1.6, there exist $u, v \in \mathbb{C}[x_1, \ldots, x_{n-1}][x_n]$ 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 $\mathbb{C}[x_1, \ldots, x_{n-1}]$. So $\mathcal{R}_{x_n}(f, g) \in I'$. And since $(a_1, \ldots, a_{n-1}) \in V(I')$, we have $\mathcal{R}_{x_n}(f, g)(a_1, \ldots, a_{n-1}) = 0$.
- 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 $f_i, g_j \in \mathbb{C}[x_1, \ldots, x_{n-1}]$. Then by our assumptions on f and g, we have
$$\begin{cases} f_0(a_1, \ldots, a_{n-1}) = 1 \\ f_i(a_1, \ldots, a_{n-1}) = 0, \forall\, i = 1, \ldots, r \\ g_s(x_1, \ldots, x_{n-1}) = 1. \end{cases}$$

[1] For each non-zero term $cx_1^{d_1} \cdots x_n^{d_n}$ in g, the change of variables gives $c(x_1 + x_n^N)^{d_1} \cdots (x_{n-1} + x_n^{N^{n-1}})^{d_{n-1}} x_n^{d_n}$. One sees that there is a unique term with largest degree, namely, $cx_n^{d_n + d_1 N + \cdots + d_{n-1} N^{n-1}}$. 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.

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

For a monic polynomial $f(x)\in F[x]$ ($\mathrm{char}(F)=0$ for simplicity), 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

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

It turns out that there's an equivalent definition of discriminant using resultant.

Proposition 3.1. *Setting as above, one has*

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

Proof. Note that

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

So

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

By Proposition 1.3, one sees that

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

□

Example 3.2. Consider a quadratic polynomial $f(x)=x^2+bx+c\in\mathbb{C}[x]$ and its derivative $f'(x)=2x+b$. Note that $\mathcal{R}(f,f')=-(b^2-4c)$. So by Corollary 1.4(3), $-(b^2-4c)=0$ if and only if f and f' share a common root in $\mathbb{C}$ (i.e., f has multiple roots in $\mathbb{C}$). And by Proposition 3.1, one sees that the discriminant $\mathrm{disc}(f)=-\mathcal{R}(f,f')=b^2-4c$.

Example 3.3. Now, consider a cubic polynomial $f(x)=x^3+ax+b\in\mathbb{C}[x]$ and its derivative $f'(x)=3x^2+a$. In this case one finds that $\mathcal{R}(f,f')=4a^3+27b^2$. So by Corollary 1.4(3) again, $4a^3+27b^2=0$ if and only if f has multiple roots in $\mathbb{C}$. And by Proposition 3.1, $\mathrm{disc}(f)=(-1)^3\mathcal{R}(f,f')=-4a^3-27b^2$.

3.2 The Field of Algebraic Elements

Let E/F be a field extension. Define $F^{\mathrm{alg}}(E) := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$, called the *algebraic closure of F in E*. Then it is a basic fact that $F^{\mathrm{alg}}(E)$ is a field. That is, for any $\alpha, \beta \in E$ which are algebraic over F, the same is true for $\alpha+\beta, \alpha\beta$ and $1/\alpha$ (when $\alpha \neq 0$). One may recall a standard proof of this fact using elementary field theory is rather implicit. As an application of resultant, we give a *constructive proof* of it. 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 $\alpha, \beta \in F^{\mathrm{alg}}(E)$ with $f(\alpha) = g(\beta) = 0$ for some non-zero $f(x), g(x) \in F[x]$. Put*

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

Then we have $h_1(\alpha+\beta) = h_2(\alpha\beta) = 0$. In particular, $\alpha+\beta, \alpha\beta \in F^{\mathrm{alg}}(E)$.

Proof. These two can be easily deduced from Proposition 1.6. First, choose $u_1(x,y), v_1(x,y) \in F[y][x]$ such that

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

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

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

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

Remark 3.5. Alternatively, one may also use Proposition 1.3 to prove Proposition 3.4. This will be left as an exercise.

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 $g(x) = x^3-2$. We find $h_1(y)$ and $h_2(y)$.

First, we see that

$$g(y-x) = (y-x)^3 - 2 = -x^3 + 3yx^2 - 3y^2x + y^3 - 2.$$

So

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

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

$$x^{\deg g} g(y/x) = x^3\left(\left(\frac{y}{x}\right)^3 - 2\right) = -2x^3 + y^3.$$

So

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

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 $0 \neq \alpha$ satisfies $f(x) \in F[x]$ with $\deg f = n > 0$, then $1/\alpha$ satisfies $x^n f(1/x) \in F[x]$. □

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

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

Alternatively, given $\alpha \in F^{\text{alg}}(E)$, there's another way to construct a polynomial satisfied by $\beta := g(\alpha)$ for any given $g(x) \in F[x]$. (Hence, every element in $F(\alpha)$ can be considered.)

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, choose $u(x,y), v(x,y) \in F[y][x]$ such that

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

The result now follows from substituting $(x,y) = (\alpha, \beta)$. □

Example 3.10. Consider a 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 $f(x)$. (One may recall that the sum of two roots of $f(x)$ is $-b$.)