Cardano's Formulas & Field Theory Motivation

Skyler Hu

February 4, 2026

Contents

1 Introduction

We have seen by the introduction to Galois Theory that the general polynomial of degree 5 and above is not solvable by radicals. The other side ofof this theorem is that the general polynomials of degrees 1 through 4 are solvable by radicals. Solving the linear and quadratic equations have been a long-studied and solved problem since ancient times, and around the time of the Renaissance, Italian mathematicians extended the solution to cubics and quartics. Notably, the general solution for equations of degree 3 and 4 are first given by Gerolamo Cardano (1501-1576), marking a further step in solving polynomials and foreshadowing the question of whether the quintic could be solved.

In this handout we explain Cardano's formulas for the cubic as an example, shed light on the motivation behind it and its connection with Galois Theory. Through this handout, we hope to familiarize the reader with arithmetic methods of solving cubics, as well as provide further intuition on the structure behind polynomials and roots.

2 What is a Discriminant?

In this section we introduce the discriminant and its properties, including its connections to field theory, and explain the importance of the discriminant to solving a polynomial.

Definition 2.1. (Discriminant.) Define the discriminant D of $x_1, x_2, \ldots, x_n$ to be

$$D = \prod_{i<j} (x_i - x_j)^2.$$

The *discriminant of a polynomial* is defined as the discriminant of all the roots of the polynomial.

We can see the implication of the discriminant for the Galois group of a polynomial:

Proposition 2.1. The Galois group of $f(x) \in F[x]$ with degree n is a subgroup of A_n if and only if the discriminant D of $f(x)$ is a square in F.

Proof. Consider when two elements $x_j, x_k (j < k)$ are permuted. The only effect this has on $\sqrt{D} = \prod_{i<j}(x_i - x_j)$ is that the term $x_j - x_k$ becomes $x_k - x_j$, so $\sqrt{D}$ changes sign once. An additional permutation of 2 elements (i.e. a transposition) would change the sign of $\sqrt{D}$ again, so $\sqrt{D}$ is fixed. We know that the Galois group A_n consists of elements that are products of an even number of transpositions. Therefore $Gal(f(x)) \subseteq A_n$ if and only if every permutation of roots in the Galois group fixes

$$\sqrt{D} = \prod_{i<j}(x_i - x_j),$$

i.e. if and only if $\sqrt{D} \in F$, so $\sqrt{D}$ is a square in F. □

A good example of this is the following cubics:

Example 2.1.
1. $((f(x) = x^3 + 3x^2 + 3x + 1.))$ The discriminant of this polynomial is 0, which is a square in $\mathbb{Q}$. The Galois group of $f(x)$ is therefore contained in A_3. In fact, $Gal(f(x)) = 1$, the identity subgroup, since the splitting field of $f(x)$ over $\mathbb{Q}$ is exactly $\mathbb{Q}$.

2. $(g(x) = x^3 - 1.)$ The discriminant of this polynomial is -27, which is not a square in $\mathbb{Q}$. The Galois group of $g(x)$ is therefore not contained in A_3, and we know this is true because we have shown $Gal(g(x)) = S_3$.

Through the proposition and examples, you should get an understanding that the discriminant gives information on the Galois group of a polynomial. This idea is illustrated further in the rest of this section, which connects the discriminant to the specific roots of the polynomial.

Example 2.2. (Discriminant of a Quadratic.) The usual discriminant of a quadratic, $b^2 - 4ac$, is already well known from high school algebra. Here we shall investigate it further in a field-theoretic approach, and use this as a starting point for computing discriminants from coefficients of a polynomial.

Consider the monic quadratic polynomial $x^2 + ax + b$. If it has roots α and β, then the discriminant $D = (\alpha - \beta)^2$. We use Vieta's formulas to write this in a and b:

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = a^2 - 4b.$$

Then $Gal(x^2 + ax + b) \subseteq S_2 = \{1, (\alpha, \beta)\}$ and is trivial if and only if $a^2 - 4b$ is a square in the rationals, which corresponds to our existing knowledge of whether or not a quadratic has real roots.

Example 2.3. (Discriminant of a Cubic.) Before we start: the discriminant of a cubic $f(x) = x^3 + ax^2 + bx + c$ is

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

This is written conventionally as $D = -4p^3 - 27q^3$, where

$$p = \frac{1}{3}(3b - a^2) \text{ and } q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

The derivation of D is given on the following page. It's long, quite tedious and includes the use of derivatives in an algebraic sense, so feel free to skip it if you want.

Derivation of Discriminant for a Cubic.
We start with the cubic $f(x) = x^3 + ax^2 + bx + c$. In order to simplify calculations, we take the substitution

$$y = x + \frac{a}{3} \text{ to get } f(x) = g(y) = y^3 + py + q$$

where

$$p = \frac{1}{3}(3b - a^2) \text{ and } q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

$g(y)$ is in the form of a cubic without a x^2 term, which is what we call a *depressed cubic*. Finding the discriminant of $f(x)$ is equivalent to finding the discriminant of $g(y)$ since the discriminant takes the difference of the roots, which cancels out the $-\frac{a}{3}$ part.
Let $g(y)$ have roots α, β, γ. Then $g(y) = (y - \alpha)(y - \beta)(y - \gamma)$. Our goal is to write the discriminant as a combination of elementary symmetric functions in α, β and γ, and $D = [(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)]^2$, so we can make use of the derivative of $g(y)$:

$$D_y g(y) = (y - \alpha)(y - \beta) + (y - \alpha)(y - \gamma) + (y - \beta)(y - \gamma).$$

Substitue the roots:

$$\begin{aligned} D_y g(\alpha) &= (\alpha - \beta)(\alpha - \gamma) \\ D_y g(\beta) &= (\beta - \alpha)(\beta - \gamma) \\ D_y g(\gamma) &= (\gamma - \alpha)(\gamma - \beta) \end{aligned}$$

Then $D = -D_y g(\alpha) D_y g(\beta) D_y g(\gamma)$. Using the definition of a derivative, we know that $D_y g(y) = 3y^2 + p$, so

$$\begin{aligned} -D &= (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3. \end{aligned}$$

We can see the elementary symmetric functions. Using the substituion by Vieta's theorem

$$\begin{aligned} \alpha\beta\gamma &= -q \\ \alpha\beta + \alpha\gamma + \beta\gamma &= p \\ \alpha + \beta + \gamma &= 0 \end{aligned}$$

we find

$$-D = 4p^3 + 27q^2, \text{ so } D = -4p^3 - 27q^2.$$

We can substitute a, b, c back to find $D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$. Please thank me for doing all the calculations for you, and don't even think about deriving the discriminant for the quartic. I'm not doing that.

2.1 Galois group & Discriminant

In this section we shall briefly see the interaction between the Galois group and discriminant of a polynomial. We investigate again with the example of a cubic.
Consider an irreducible cubic polynomial $f(x) \in F[x]$. Since any root extension over $F[x]$ gives an extension of degree 3 ($f(x)$ is irreducible), the Galois group has order divisible by 3 by FTGT. There are two possibilities: $Gal(f(x)) = A_3$ or S_3.

Proposition 2.2. $Gal(f(x)) = A_3$. $Gal(f(x)) = A_3$ if and only if the discriminant of $f(x)$ is a square in F.

Proof. See proposition 2.1. □

We can further analyze the two Galois groups:

1. ($Gal(f(x)) = A_3$.) If D is a square in F, then the splitting field of $f(x)$ over F is obtained by adjoining any root of $f(x)$ to F, and the Galois group is of order 3.
2. ($Gal(f(x)) = S_3$.) Then D is not a square in F, and the splitting field of $f(x)$ over F is obtained by adjoining $\sqrt{D}$ (a quadratic extension) and a root of f (an extension of degree 3) to F. The splitting field has degree 6 over F and the Galois group is S_3.

3 Cardano's Formulas

3.1 Exposition

Take a deep breath:

Theorem 3.1. (Cardano's Formulas for Cubic.) The roots of $x^3 + ax^2 + bx + c$ are:

$$x_1 = \frac{1}{3}(\sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}} + \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}})$$
$$x_2 = \frac{1}{3}(\rho\sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}} + \rho^2\sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}})$$
$$x_3 = \frac{1}{3}(\rho^2\sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}} + \rho\sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}})$$

where

$$D = -4p^3 - 27q^2$$
$$p = \frac{1}{3}(3b - a^2)$$
$$q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

Note: It is not advisable to use this formula to actually solve a cubic. Better options include sketching a graph, estimation using Newton's method, factoring (whenever possible), and TI-84. Unlike the formula for the quadratic, Cardano's formula for the cubic wouldn't make much sense in any context requiring specific solutions of a cubic.

3.2 Cardano's Formulas for the Cubic: Derivation

3.2.1 Cardano's Proof (Algebra)

Warning: skip the part after the depressed cubic if you're not a fan of calculations.
We begin with depressing the cubic, as it simplifies further calculations tremendously:

$$x^3 + ax^2 + bx + c = y^3 + py + q$$

where

$$\begin{aligned} y &= x + \frac{a}{3} \\ p &= \frac{1}{3}(3b - a^2) \\ q &= \frac{1}{27}(2a^3 - 9ab + 27c) \end{aligned}$$

Since we have already taken a lot of substitutions, it would not hurt to take one more: let $y = u + v$ where $uv = -\frac{p}{3}$. Substitute $y = u + v$ into $y^3 + py + q$ and collect like terms:

$$u^3 + v^3 + (3uv + p)(u + v) + q = u^3 + v^3 + q = 0.$$

So $u^3 + v^3 = -q$. Since we also know that $uv = -\frac{p}{3}$, Vieta's formulas say that u^3 and v^3 are the roots of the quadratic equation

$$\begin{aligned} (x - u^3)(x - v^3) &= x^2 - (u^3 + v^3)x + (uv)^3 \\ &= x^2 + qx + \frac{p^3}{27} \\ &= 0. \end{aligned}$$

Solving for the two roots of this equation gives us:

$$\begin{aligned} u &= \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ v &= \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \end{aligned}$$

Since $y = u + v$, we have

$$y = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

which is a root of the equation $y^3 + py + q = 0$. The other two roots are found by multiplying each cube root by one of the two cube roots of unity.

3.2.2 A litte history

If you skipped the algebraic derivation: welcome back.

The birth of Cardano's formulas occured during the Renaissance period, when a group of Italian math enthusiasts, thinkers and part-time mafia leaders (calling themselves the *Cossists*) decided to tackle the problem of finding general solutions to higher-degree equations. The first known Cossist to make progress towards solving the cubic was Scipione del Ferro (1465-1526), who was widely believed to have solved a single case of the problem. However, the most remembered mathematicians for this effort are Gerolamo Cardano (1501-1576) and Niccolo Tartaglia (1500-1557).

The story goes: Cardano took an interest in Tartaglia's solutions to the cubic and sought the mathematician out for a collaboration. Tartaglia, being more content with working alone, refused, but finally relented when Cardano promised wealthy acquaintances and to keep his solution secret. Years later, Cardano decided to forgo his promise and published a revised solution to both the cubic and quartic in his *Ars Magna* (The Major Arts). Needless to say, Tartaglia was outraged, but nothing could've changed the course of events that named the formula after Cardano and left him more well-known for his name, which meant 'stammerer'. (He was stabbed in the lip by French soldiers when he was a boy.)

A side note is about the use of complex numbers in such solutions. This was centuries before the formal definition and use of complex numbers by Euler, and Cossists didn't concern themselves with the square roots of negative numbers: they accepted that they often show up in solving polynomials (e.g. when the discriminant of a cubic is negative), but they didn't venture further on these complex solutions or the implications behind complex numbers. Rafael Bombelli, another major contributor to the solution of polynomials by radicals, noted in his publication that such roots exist, but dismissed them as 'surds' and therefore useless for their system of real numbers.

If you read Cardano's proof in 3.2.1, you might've noticed that it wasn't very satisfying to work through. In fact, Cardano's proof is viewed more as an algebra trick that happened to work on the cubic (and quartic as well), and it was purely based on the very algebraic substitution $y = u + v$. (Incidentally, this substitution is now called the *del Ferro-Cardano substitution.*) For this reason we will introduce in the next section another proof of Cardano's formula for the cubic, this one created by the great French mathematician Joseph-Louis Lagrange (1736-1813), with closer ties with Galois Theory and roots of unity.

3.3 Lagrange's Proof

In this section we look at the field theory behind Cardano's formula in more detail, featuring permuting roots (the core of Galois Theory) with roots of unity and Lagrange's innovative idea of applying permutations to solving polynomials. First, let's lay the groundwork by defining a Lagrange resolvent and some relevant theorems.

3.3.1 Lagrange Resolvent & Roots of unity

The following proposition is the motivation behind a Lagrange Resolvent:

Proposition 3.1. (Simple Radical Extensions are Cyclic) Let F be a field of characteristic not dividing n which contains an nth root of unity. Then the simple extension $F(\sqrt[n]{a})$ is cyclic over F (i.e. it has a cyclic Galois group) with a degree dividing n.

The proof uses roots of unity, feel free to skip to the end if you want:

Proof. Note that all roots of $x^n - a$ differ by a factor of the nth root of unity. The extension $K = F(\sqrt[n]{a})$ is Galois over F if F contains an nth root of unity (and therefore all the nth roots of unity), since K is the splitting field of $x^n - a$ over F. For any permutation $\sigma \in Gal(K/F)$, $\sigma(\sqrt[n]{a})$ is another root of this polynomial, so $\sigma(\sqrt[n]{a}) = \zeta_\sigma(\sqrt[n]{a})$ for some nth root of unity ζ_σ. This induces a homomorphism map

$$Gal(K/F) \mapsto \mu_n, \text{ the group of } n\text{th roots of unity} \tag{1}$$

$$\sigma \mapsto \mu_\sigma. \tag{2}$$

(See if you can prove that this is a homomorphism.) This homomorphism has kernel 1 since $\sqrt[n]{a}$ does not lie in F, and the only element fixing $\sqrt[n]{a}$ is the identity map. Therefore there exists an injective homomorphism $Gal(K/F) \mapsto \mu_n$, and μ_n is cyclic, so $Gal(K/F)$ is also cyclic with degree dividing $\mid \mu_n \mid = n$. □

In Proposition 3.1 we have seen that we can permute roots of a polynomial $x^n - a$ by multiplying the nth roots of unity to a root. This is the idea behind the Lagrange resolvent:

Definition 3.1. (Lagrange Resolvent.) Let K be any cyclic extension of degree n over F, with F containing the nth roots of unity. Let σ be a generator for cyclic $Gal(K/F)$.
For $\alpha \in K$ and any nth root of unity ζ, define the Lagrange resolvent $(\alpha, \zeta) \in K$ by

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

In case you're interested, the Lagrange Resolvent can be used to prove the other direction of Proposition 3.1: Cyclic extensions can be expressed in the form of a simple radical extension. But now we'll move on to a more elegant proof of Cardano's formula for the cubic.

3.3.2 Cubic formula derivation

Suppose we have the general cubic $f(x) = x^3 + ax^2 + bx + c$. $f(x)$ has Galois group S_3 over $\mathbb{Q}$. First depress the cubic, as we have done in 3.2.1:

$$f(x) = g(y) = y^3 + py + q \text{ where}$$

$$y = x + \frac{a}{3}$$
$$p = \frac{1}{3}(3b - a^2)$$
$$q = \frac{1}{27}(2a^3 - 9ab + 27c)$$

Root of Unity & Lagrange Resolvent.
Let the roots of $g(y)$ be α, β, γ, so that $\alpha + \beta + \gamma = 0$. We will show that $Gal(g(y))$, the Galois group taken over $\mathbb{Q}(\sqrt{D})$, is precisely A_3:

Proof. We begin with the fact that $Gal(g(y)) = A_3$ or S_3. Since the Galois group is taken over $\mathbb{Q}(\sqrt{D})$, every $\sigma \in Gal(g(y))$ has to fix $D = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$, so $Gal(g(y)) \leq A_3$, and $Gal(g(y)) = A_3$. □

Note. This provides some insight on why the depressed cubic 'simplifies' the process: we reduce the Galois group of the general cubic over $\mathbb{Q}$, which is S_3, into the Galois group of the depressed cubic over $\mathbb{Q}(\sqrt{D})$, which is A_3. This operation reduces the problem at hand in the sense that cubics with Galois group A_3 over a base field is easier to handle than cubics with Galois group S_3.

Adjoining a primitive cube root of unity ρ to $\mathbb{Q}(\sqrt{D})$ gives us a field extension containing all the roots of $g(y)$, since the generator of this extension is a Lagrange Resolvent (α, ρ). We can find all the Lagrange Resolvents of this form:

$$(\alpha, 1) = \alpha + \beta + \gamma = 0$$
$$\theta_1 = (\alpha, \rho) = \alpha + \rho\beta + \rho^2\gamma$$
$$\theta_2 = (\alpha, \rho^2) = \alpha + \rho^2\beta + \rho\gamma$$

With the Lagrange resolvents, we can come up with formulas to solve for α, β and γ individually, which would be useful in the final step of the derivation:

$$3\alpha = \theta_1 + \theta_2$$
$$3\beta = \rho^2\theta_1 + \rho\theta_2$$
$$3\gamma = \rho\theta_1 + \rho^2\theta_2$$

We know that θ_1 and θ_2 are in $\mathbb{Q}(\sqrt{D}, \rho)$. Solving for θ_1 and θ_2 with the help of elementary symmetric functions (purely computational, no algebra included) gives us

$$\theta_1^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D} \text{ and } \theta_2^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}.$$

We can now solve for the roots of $g(y)$: if we define for simplicity $A = \sqrt[3]{\theta_1}$ and $B = \sqrt[3]{\theta_2}$, then we have

$$\alpha = \frac{A + B}{3}, \beta = \frac{\rho^2 A + \rho B}{3}, \gamma = \frac{\rho A + \rho^2 B}{3}.$$

Conclusion. The roots of $g(y)$ are:

$$\alpha = \frac{1}{3}(\sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} + \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}})$$
$$\beta = \frac{1}{3}(\rho^2\sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} + \rho\sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}})$$
$$\gamma = \frac{1}{3}(\rho\sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} + \rho^2\sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}})$$

where

$$D = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = -4p^3 - 27q^2$$
$$p = \frac{1}{3}(3b - a^2)$$
$$q = \frac{1}{27}(2a^3 - 9ab + 27c)$$

and we can find the roots of $f(x)$ accordingly.