THE CUBIC FORMULA AND GALOIS THEORY

NAT KUHN

1. Introduction

The method of solving quadratic equations—what we know as the quadratic formula—was know to the ancient Babylonians [4]. The discovery of the method of solving the cubic equations had to wait until the early 1500s, more than three millennia later; the quartic equation was solved shortly thereafter.

Gerolamo Cardano was the first to publish the solution to the cubic equation, in his 1545 *Ars Magna* [2]. While he credits Scipione del Ferro as its original discoverer, it generally goes by the name *Cardano's formula*, although Mazur [6] has attempted to violate Stigler's law of eponymy [7] by calling it "dal Ferro's formula." It states that the solutions of the cubic equation $x^3 + px + q = 0$ are given by

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \tag{1}$$

The history and characters behind this equation and its publication are colorfully recounted in [3, Chapter 6]. Cardano's formula, along with Ferrari's solution of the quartic, may well be the high point of Renaissance mathematics.

To be honest, though, my eyes would tend to glaze over whenever I would see this formula on a page. It looked unfriendly, unwieldly, and hard to grasp, a difficult equation to love. And it looked (in the pre-computer era) as though it would take an annoying amount of computation to apply it to any specific cubic polynomial given the difficulties of extracting cube roots. Another confusing issue is that to generate all the possible roots, the cube roots must be allowed to take multiple values; however, since each cube root has 3 possible values, this formula appears to give 9 possible solutions. In fact, the formula has a surprising amount of symmetry, and, as we shall see, the resolution of the 9-solutions problem also allows us to cut the computational work roughly in half.

Equations of degree 5 and higher resisted similar solutions for about another 300 years, until Niels Henrik Abel was able to complete Paolo Ruffini's proof that such attempts are futile: there is no general formula for solving polynomial equations of degree 5 and higher using only algebraic operations (addition, subtraction, multiplication, and division) and the extraction of roots.

The crowning achievement of this line of inquiry was Evariste Galois's theory of equations, now known as Galois theory, which is both a staple of introductory abstract algebra courses and the bedrock foundation of the entire field of algebraic number theory. Going beyond the work of Abel and Ruffini on the general equation

Date: January 14, 2019; edited Jan 15, 2019.

of degrees 5 and higher, Galois theory can also be applied to *specific* polynomials and gives an exact criterion for the existence of solutions by radicals.

On the other hand, courses in Galois theory rarely cover the explicit solutions of the cubic and quartic equations; in one of the rare cases where the cubic formula is covered, the solution is obtained by an ad hoc method that is essentially the same one that del Ferro employed [1, Section 14.2]. (See Exercise 15 for a version of this solution.)

It is the goal of this paper to show how the cubic formula can be derived in a relatively natural way in the context of Galois theory. The paper should be accessible to an undergraduate who has had a course in Galois theory; in any case, we review the necessary Galois theory in Section 3, and an adventuresome reader who has not had such a course but is familiar with the basics of groups, fields, and linear algebra might get enough out of this paper to want to study Galois theory in more depth.

The bulk of what is treated here—and quite a bit more—is covered in Janson's *Roots of Polynomials of Degrees 3 and 4* [5], using the "discrete Fourier transform." While following Janson's notation as much as possible, I have taken the mathematically equivalent approach of looking at eigenvectors of field automorphisms, which is naturally connected to the Galois theory of root extraction and which motivates further study of the representations of Galois groups. I also believe that the approach taken here ends up simplifying some of the caculations involved.

2. Background: Cubic Equations

The roots of a general cubic polynomial are the solutions of the equation

$$f(x) = ax^3 + bx^2 + cx + d = 0$$

where $a \neq 0$. Because we are going to transform this formula, let's write it again with primes after everything:

$$f(x') = a'x'^3 + b'x'^2 + c'x + d' = 0$$

Because $a' \neq 0$, we can divide through by a' without changing the roots, obtaining the equation

$$f(x') = x'^3 + bx'^2 + cx + d = 0$$

where $b = b'/a, c = c'/a$, and $d = d'/a$. At the price of belaboring the obvious, this has allowed us to "knock out" the leading coefficient a'.

The next trick is slightly less obvious, but it is essentially a reprise of "completing the square," which allows us to solve quadratic equtions. Letting $x' = x - b/3$, we can "knock out" b, transforming our equation to

$$g(x) = x^3 + px + q = 0 \tag{2}$$

If we use $\alpha_1, \alpha_2, \alpha_3$ to denote the roots of $f(x')$, then the roots of of $g(x)$ can be taken to be $\beta_i = \alpha_i + b/3$.

A cubic polynomial of this sort, without the x^2 term, is known as a *depressed* or *reduced* cubic. Interestingly, this is the sort of cubic that del Ferro learned how

to solve. Although it is a much simpler problem to modern eyes, it was only later that Cardano discovered how to reduce the general cubic to the depressed cubic.

Since $g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$, it follows that

$$0 = \beta_1 + \beta_2 + \beta_3 \tag{3a}$$

$$p = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 \tag{3b}$$

$$-q = \beta_1\beta_2\beta_3 \tag{3c}$$

Exercise 1. *With the notation as above, show that*

$$p = c - \frac{b^2}{3} \text{ and } q = d - \frac{bc}{3} + \frac{2b^3}{27}$$

3. Background: Galois Theory

In Galois theory, we consider a base field K, and some *field extension* E, that is, a field E with $K \subseteq E$. Then E is a vector space over the field K. For example, K might be the field $\mathbb{Q}$, the field of rational numbers. The field $\mathbb{C}$ of complex numbers is an extension field; as a vector space over $\mathbb{Q}$ it has infintely many dimensions. (Don't worry, the field extensions we will be working with are all finite-dimensional.) If you like, you can think of all our fields as containg $\mathbb{Q}$ and being contained in $\mathbb{C}$, but it is not necessary. In fact, our arguments will work over any base field as long as the characteristic of K is not 2 or 3.

The results we need from Galois theory are quite minimal. If f is a polynomial with coefficients in K, the *splitting field* (call it E) of f is the smallest field which contains all the roots of f, call them $\{\alpha_1, ..., \alpha_n\}$ with the α_i distinct. The splitting field is a finite-dimensional vector space over K, and its dimension as a vector space is called the *degree* of the field extension, denoted $[E : K]$. Degrees are multiplicative: if K' is a field with $K \subseteq K' \subseteq E$, then $[E : K] = [E : K'][K' : K]$.

The *Galois group* $G = \text{Gal}(E : K)$ is the group of field automorphsims σ of E which fix K, that is, with $\sigma(x) = x$ for all $x \in K$. (That is, K is contained in the 1-eigenspace of σ, considering σ as an operator on E—a K-linear transformation of E to itself.) In this situation, G is a finite group with $|G| = [E : K]$. The subfield of elements of E fixed by every $\sigma \in G$ contains K by definition, but it is a fundamental result of Galois theory that this "fixed field" of G is in fact equal to K.

Because the coefficients of our polynomial f are in K, $\sigma(f(x)) = f(\sigma(x))$ for all $x \in E$ and $\sigma \in G$. So if x is a root of f and $\sigma \in G$, then $f(\sigma(x)) = \sigma(f(x)) = \sigma(0) = 0$, so $\sigma(x)$ is also a root of f. Thus, σ permutes the roots of f, and there is a natural homomorphism mapping G to the group of permutations of the roots, which is isomorphic to S_n. Furthermore, since the α_i generate E, any automorphism which fixes them must fix all of E and therefore equal the identity element of G, so our homomorphism is injective. Thus we can indentify the Galois group with a subgroup of the permutations of the n roots. If f is an irreducible polynomial, G acts transitively on the roots of f, that is, there is an element of G which will take any individual root to any other specified root.

A central result of Galois theory is that there is a one-to-one correspondence between subgroups of G and fields which are intermediate between E and K. A subgroup $H \subseteq G$ corresponds to the subfield F of E consisting of all elements of E fixed by every element of H. (Thus, the trivial subgroup corresponds to the entire field E, while the entire Galois group G corresponds to the base field K.) H is the

Galois group $\mathrm{Gal}(E:F)$, so $|H| = [E:F]$. Finally, H is a normal subgroup if and only if F is a Galois extension of K (meaning that it is the splitting field of some polynomial), and in this case G/H is isomorphic to the Galois group $\mathrm{Gal}(F:K)$.

From the standpoint of Galois theory, extraction of roots is connected to eigenvectors of elements of our Galois group. Suppose $b \in E$ is an n-th root of a, that is, $b^n = a$, and that a and b are non-zero. Let us fix an element $\sigma \in G$ and suppose further that $\sigma(a) = a$—for example, any $a \in K$ would satisfy this condition. Then $(\sigma(b))^n$ is also equal to a, so if $\zeta = \sigma(b)/b$, $\zeta^n = 1$, that is, ζ is an n-th root of unity. Also, $\sigma(b) = \zeta b$, so b is a ζ-eigenvector of σ. We have proved one-half of the following proposition, which is the key element of Galois' criterion relating solvability of equations by radicals to "solvability" of the Galois group G.

Proposition 1. *Let $\sigma \in G$ with σ^n equal to the identity transformation. Then all eigenvalues of σ are n-th roots of unity. Furthermore, $b \in E$ is the n-th root of some a with $\sigma(a) = a$ if and only if b is an eigenvector of σ.*

Exercise 2. *Fill in any details of the above argument that are hazy, and prove the rest of Proposition 1.*

If $\sigma(a) = a$, then a is fixed by every power of σ, so a is in the fixed field of the cyclic subgroup generated by σ, which will be a proper subfield of our field extension (assuming σ is not the identity). Thus, eigenvectors are roots of elements of a smaller field.

The following exercise fleshes this situation out for the case $n = 2$, understanding that the "2-th roots of unity" are ± 1.

Exercise 3. *Let $f(x)$ be the quadratic polynomial $x^2 + bx + c$. When the equation's discriminant, $D = b^2 - 4c$, is a square in K show that the splitting field of f over K is simply K itself. Otherwise, show that the splitting field is an extension of degree 2; that its Galois group has one element other than the identity, call it σ; that $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$; and that the eigenspaces of σ consist of K itself (the 1-eigenspace), and the multiples of $\sqrt{D}$ (the -1-eigenspace).*

The next two exercises are a warm-up for the following section, where we will consider more general projections onto eigenspaces.

Exercise 4. *Let V be a vector space, and let T be an operator on V (that is, a linear map $T : V \to V$) with T^2 equal to the identity map I. Show that any eigenvalue of T is either 1 or -1. Let Π_+ be the operator $\frac{1}{2}(T + I)$ and Π_- be the operator $\frac{1}{2}(T - I)$. Show that for any vector $v \in V$, $v = \Pi_+(v) + \Pi_-(v)$ and that Π_+ and Π_- are projections onto the 1 and -1 eigenspaces of T, respectively. Show that T is diagonalizable. If V is the vector space of $n \times n$ matrices and T is the transpose operator, show that Π_+ and Π_- decompose a matrix into a symmetic and an skew-symmetric part, so that Π_+ can be thought of as a "symmetrizer" and Π_- can be thought of as an "skew-symmetrizer."*

Exercise 5. *With the notation as in Exercise 4, show that if $V = \mathbb{C}$ considered as a two-dimensional vector space over $\mathbb{R}$ with T the complex conjugation operator, we have decomposed a complex number as the sum of its real and imaginary components. As a generalization of this situation, take V to be the splitting field of an irreducible quadratic polynomial f over the base field K, as in Exercise 3. Show that this process decomposes elements of V into a part that is in the base field plus a part that is a base-field multiple of $\sqrt{D}$.*

4. Galois Theory of the Cubic Equation

Let us return to our depressed cubic $g(x)$, given in Equation 2, with roots β_1, β_2, and β_3. As noted above, the Galois group G of $E = K(\beta_1, \beta_2, \beta_3)$ over K can be identified with a subgroup of S_3. Let us also assume that g is irreducible, in which case G acts transitively on the β_i, which are distinct.

S_3 has 6 subgroups. Visualizing S_3 as the dihedral group of symmetries of an equilateral triangle (with the β_i as vertices, if you like), these subgroups can be described as follows: S_3 itself; the trivial subgroup, consisting only of the identity; a subgroup (A_3) of order 3 consisting of rotations, or cyclic permutations of the β_i; and 3 subgroups of order 2, each generated by a reflection, which fixes one of the β_i and interchanges the other two. Only two of these subgroups operate transitively: A_3 and S_3; G must be one these two possibilities. The degree of the extension $[E : K] = |G|$ is either 3 or 6, correspondingly. In either case, A_3 is a (normal) subgroup of G, and we can let σ be an element of order 3 which generates A_3. We can number the β_i (or alternatively choose σ) such that $\sigma(\beta_1) = \beta_2$, $\sigma(\beta_2) = \beta_3$, and $\sigma(\beta_3) = \beta_1$.

Let let K' be the subfield of E fixed by A_3. (If $G = A_3$, K' is simply K.) We have a "tower" of field extensions $K \subseteq K' \subset E$ which corresponds in Galois theory to the contracting tower of subgroups $G \supseteq A_3 \supset \{1\}$, where 1 denotes the identity element of G. If $G = S_3$, Galois theory tells us that $[K' : K] = |\operatorname{Gal}(K' : K)| = |S_3/A_3| = 2$. So K' is either K itself, or a quadratic extension of K.

Exercise 6. *Prove anything in the previous two paragraphs that you are unsure of.*

Proposition 1 tells us that any eigenvector of σ is the cube root of an element of K'. The next section will be devoted to proving Proposition 3, which says that under an appropriate condition every element of E—including the solutions of our cubic—can be decomposed as sum of eigenvectors of σ. Let's look at what that will do for us.

In the case $G = A_3$, the fixed field of A_3 is simply K itself, and $K' = K$. If we can write our solution as a sum of eigenvectors of σ, we will have shown that it is a sum of cube roots of elements of our ground field K.

If $G = S_3$, K' is a quadratic extension of K, and so by Exercise 3, we will have shown that we can express the solutions of the cubic as a sum of cube roots of algebraic expressions that can the involve the square root of some $D \in K$. In either case, our solutions can be expressed in terms of algebraic operations and radicals. Essentially, we have reprised the proof that a polynomial with a solvable Galois group can be solved by radicals. However, it's a long way from there to an explicit formula; that is the problem we will take up in Section 6.

5. Eigenspaces of σ

In this section, we will examine σ as a linear operator on E, considered as K-vector space of dimension $|G|$. Our goal is to prove Proposition 3, which shows that any element of E, can be expressed as as sum of eigenvectors of σ. Our shorthand for this will be the equivalent condition that σ is diagonalizable.

In what follows, we make repeated implicit use of the following fact; if it is not obvious to you, you should prove it as an exercise.

Proposition 2. *Let V be a vector space, T be an operator on V, $f(x)$ be a polynomial with scalar coefficients, and let v be a λ-eigenvector of T. Then $p(T)v = p(\lambda)v$.*

Because σ^3 is the identity, any eigenvalue of σ must be a cube root of unity. To be able to diagonalize σ, we need our ground field K to include all the cube roots of unity. The "appropriate condition" referred to in the previous section is that K contain a primitive cube root of unity, which we will call ω. If our fields are contained in $\mathbb{C}$, we can take

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \text{ so that } \omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

which are complex conjugates of each other. In the general case, since $x^3 - 1 = (x-1)(x^2+x+1)$, it follows that ω satisfies the polynomial x^2+x+1. From the quadratic formula,

$$\omega = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$$

in which case

$$\omega^2 = -\frac{1}{2} \mp \frac{\sqrt{-3}}{2}$$

and the two are interchanged by a different choice of $\sqrt{-3}$. In what follows, we will fix a particular choice of $\sqrt{-3}$ (just as the symbol i "fixes" a particular choice of $\sqrt{-1}$), and we will take

$$\begin{aligned} \omega &= -\frac{1}{2} + \frac{\sqrt{-3}}{2} \text{ so that} \\ \omega^2 &= -\frac{1}{2} - \frac{\sqrt{-3}}{2} \text{ and} \\ \omega - \omega^2 &= \sqrt{-3} \end{aligned} \tag{4}$$

Quantities such as $\sqrt{-27} = 3\sqrt{-3}$ and $\sqrt{-108} = 6\sqrt{-3}$ will be understood to be relative to our fixed choice of $\sqrt{-3}$. (Of course an alternative to this "fixed choice of $\sqrt{-3}$" approach would be to consider $K = K_0(\omega)$ as a Galois extension of a ground field K_0. This would add a possible extra layer of confusion without a lot of immediate benefit.)

We will express elements of E in terms of eigenvectors by projecting them onto the eigenspaces of σ, just as we did for operators of order 2 in Exercise 4. Our projections will be (quadratic) polynomials in our operator σ, analogous to the "linear polynomials" in T in Exercise 4.

As a motivating example, suppose that σ has the matrix representation

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$$

We can find a polynomial $p_1(x)$ with $p_1(1) = 1$, $p_1(\omega) = 0$, and $p_1(\omega^2) = 0$ by taking an appropriate scalar multiple of

$$(x-\omega)(x-\omega^2) = \frac{x^3-1}{x-1} = x^2+x+1$$

The "appropriate scalar multiple" is obviously $1/3$, because x^2+x+1 takes the value 3 at $x = 1$. (Readers who understand Lagrange interpolation will recognize

this procedure.) Then $p_1(\sigma)$ is represented by the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

which is the desired projection onto the 1-eigenspace of σ. In other words, the polynomial p_1 was cooked up to be in the identity on the 1-eigenspace and to "kill off" the other eigenspaces: $p_1(\lambda') = \delta_{1\lambda'}$ where δ is the Kronecker δ ($\delta_{\lambda\lambda'} = 1$ if $\lambda = \lambda'$ and 0 otherwise).

To complete the argument, we need these polynomials:

$$p_1(x) = \frac{(x-\omega)(x-\omega^2)}{3} = \frac{1}{3}(x^2 + x + 1)$$
$$p_\omega(x) = \frac{(x-1)(x-\omega^2)}{3\omega^2} = \frac{1}{3}(\omega x^2 + \omega^2 x + 1)$$
$$p_{\omega^2}(x) = \frac{(x-1)(x-\omega)}{3\omega} = \frac{1}{3}(\omega^2 x^2 + \omega x + 1)$$

Exercise 7. *Verify the equations above. With $\lambda, \lambda' \in \{1, \omega, \omega^2\}$, show that*

$$p_\lambda(\lambda') = \delta_{\lambda\lambda'}$$

(We have already done the case $\lambda = 1$.)

Now we can form the operators:

$$\Pi_1 = p_1(\sigma) = \frac{1}{3}(1 + \sigma + \sigma^2) \tag{5a}$$
$$\Pi_\omega = p_\omega(\sigma) = \frac{1}{3}(1 + \omega^2\sigma + \omega\sigma^2) \tag{5b}$$
$$\Pi_{\omega^2} = p_{\omega^2}(\sigma) = \frac{1}{3}(1 + \omega\sigma + \omega^2\sigma^2) \tag{5c}$$

where 1 denotes the identity operator. The operator Π_1 can be thought of as a "symmetrizer," while Π_ω and Π_{ω^2} can be thought of as "skew-symmetrizers" or "symmetrizers with a twist."

Proposition 3. *The operators Π_λ are projections of E onto the λ-eigenspace of σ. $\Pi_\lambda\Pi_{\lambda'} = 0$ if $\lambda \neq \lambda'$. Finally, if $r \in E$,*

$$r = \Pi_1(r) + \Pi_\omega(r) + \Pi_{\omega^2}(r) \tag{6}$$

Readers with some knowledge of group representations will see that this is equivalent to decomposing the representation of the cyclic group of order 3 generated by σ into irreducible representations.

If we already know σ is diagonalizable, the proof of Proposition 3 is simply an expanded version of our example above. It follows directly from Jordan canonical form that an operator like σ which satisfies a polynomial with distinct roots is diagonalizable. Readers who are willing to accept this proof may wish to proceed directly to the next section. The remainder of this section is a series of exercises giving a direct proof of Proposition 3. It is a special case of an argument that does not depend on Jordan canonical form and works for any operator which satifies a polynomial factoring into distinct linear factors; enterprising readers should be able to produce the general argument without much difficulty.

Exercise 8. *Show that* $p_1(x)+p_\omega(x)+p_{\omega^2}(x) = 1$. Hint: either calculate explicitly, or note that the sum, minus 1, is a quadratic polynomial with 3 zeros, and is therefore identically 0. *Use this result to prove Equation 6.*

Exercise 9. *Show that the image of* Π_λ *is contained in the* λ*-eigenspace of* σ. Hint: use the fact that that the polynomial $(x-\lambda)p_\lambda(x)$ is a scalar multiple of x^3-1.

Exercise 10. *Show that* Π_λ *is the identity on any* λ*-eigenvector of* σ*, implying that the image of* Π_λ *is the entire* λ*-eigenspace.* Hint: use Proposition 2 and Exercise 7. *Prove that* $\Pi_\lambda^2 = \Pi_\lambda$*, that is,* Π_λ *is a projection.* Hint: use Exercise 9.

Exercise 11. *Show that* $\Pi_\lambda\Pi_{\lambda'} = 0$ *if* $\lambda \neq \lambda'$. Hint: use the hints from the previous exercise.

That completes the proof of Proposition 3

Exercise 12. *Show that* E *is a direct sum of the eigenspaces of* σ*, which is equivalent to saying that* σ *is diagonalizable.*

6. Back to Our Roots

Returning to the specific situation of our depressed cubic in Equation 2, recall that its roots β_i satisfy $\sigma(\beta_1) = \beta_2$ and $\sigma(\beta_2) = \beta_3$; hence $\sigma^2(\beta_1) = \beta_3$.

As a result Equation 5a gives us:

$$\Pi_1(\beta_1) = \frac{1}{3}(\beta_1+\beta_2+\beta_3)$$

which is 0 by Equation 3a.

Applying Proposition 3, we see that

$$\beta_1 = \Pi_\omega(\beta_1) + \Pi_{\omega^2}(\beta_1)$$

We give these two eigenvectors of σ the names u and v. Applying Equations 5b and 5c we have

$$u = \Pi_\omega(\beta_1) = \frac{1}{3}(\beta_1+\omega^2\beta_2+\omega\beta_3) \tag{7a}$$

$$v = \Pi_{\omega^2}(\beta_1) = \frac{1}{3}(\beta_1+\omega\beta_2+\omega^2\beta_3) \tag{7b}$$

u and v are known as *Lagrange resolvents*, after Lagrange's work on roots of polynomials which laid the foundation for the work of Ruffini, Abel, and Galois. Since

$$\beta_1 = u+v \tag{8a}$$

we can see that

$$\beta_2 = \sigma(\beta_1) = \omega u+\omega^2 v = \omega(u+\omega v) \tag{8b}$$

$$\beta_3 = \sigma(\beta_2) = \omega^2 u+\omega v = \omega^2(u+\omega^2 v) \tag{8c}$$

Because u and v are eigenvectors of σ, we know from Proposition 1 that u^3 and v^3 lie in our smaller field K'. If we can develop formulas for u^3 and v^3, then β_1 is the sum of their cube roots. In fact, we can see from the above that β_2 and β_3 are the sums of *other* cube roots of u^3 and v^3. And we can see a hint of the resolution of our 9-solutions problem because while the choice of cube root may vary, in all three cases the product of the cube roots is equal to uv. We shall return to this point in Section 9. Meanwhile, let's work on our formulas for u^3 and v^3 by exploiting more symmetry.

Although u and v are not fixed by σ, $\beta_1\beta_2\beta_3$ lies in our base field K; in fact, it is equal to $-q$ (Equation 3c). Thus, combining Equations 8a–8c,

$$-q = \beta_1\beta_2\beta_3 = (u+v)(u+\omega v)(u+\omega^2 v)$$

By a fairly well-known identity, this last product is simply u^3+v^3!

Exercise 13. *If the fairly well-known identity is not known to you, prove that*

$$s^3 - t^3 = (s-t)(s-\omega t)(s-\omega^2 t)$$

starting from

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$$

Our result follows, taking $s = u$ and $t = -v$.

As a result, we have established that

$$u^3 + v^3 = -q \tag{9}$$

Since we have a formula for u^3+v^3, a formula for u^3-v^3 would get us formulas for u^3 and v^3, and hence the cubic formula. To try the same trick from Exercise 13, let's start with $u-v$. Combining Equations 7a and 7b,

$$u - v = \frac{(\omega^2-\omega)\beta_2 + (\omega-\omega^2)\beta_3}{3} = \frac{1}{3}(\omega^2-\omega)(\beta_2-\beta_3)$$

We can simplify this by recalling from Equation 4 that $\omega - \omega^2 = \sqrt{-3}$. Thus we see that

$$u - v = -\frac{1}{\sqrt{-3}}(\beta_2-\beta_3) \tag{10}$$

This looks promising! It is possible to do the same computation to get $(u-\omega v)$ and $(u-\omega^2 v)$, but it is less tedious to let to let the Galois group do the work for us. Applying σ to Equation 10, we get

$$\omega u - \omega^2 v = -\frac{1}{\sqrt{-3}}(\beta_3-\beta_1) \text{ which simplifies to } \omega(u-\omega v) \tag{11}$$

One more application of σ yields

$$\omega^2 u - \omega v = -\frac{1}{\sqrt{-3}}(\beta_1-\beta_2) \text{ which simplifies to } \omega^2(u-\omega^2 v) \tag{12}$$

Taking the product of Equations 10–12 and using Exercise 13 with $s = u, t = v$ yields

$$u^3 - v^3 = (u-v)(u-\omega v)(u-\omega^2 v) = -\frac{1}{\sqrt{-27}}(\beta_1-\beta_2)(\beta_2-\beta_3)(\beta_3-\beta_1) \tag{13}$$

Defining

$$\delta = (\beta_1-\beta_2)(\beta_2-\beta_3)(\beta_1-\beta_3) \tag{14}$$

and noting the order change in the last term, we have

$$u^3 - v^3 = \frac{\delta}{\sqrt{-27}} \tag{15}$$

Combining Equations 9 and 15 yields

$$u^3 = \frac{-q + \delta/\sqrt{-27}}{2} \tag{16}$$

$$v^3 = \frac{-q - \delta/\sqrt{-27}}{2} \tag{17}$$

We're almost there! If we can compute δ, we can compute u^3 and v^3, and, extracting cube roots, $\beta_1 = u + v$.

δ, along with its generalization to polynomials of higher degree, plays a starring role in the theory of equations. It is not quite invariant under an arbitrary permutation of the β_i—it can change sign. As a result, its square

$$\Delta = \delta^2 = (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_1 - \beta_3)^2 \tag{18}$$

is invariant under under all permutations of the β_i, and it therefore lies in our ground field K. Δ known as the *discriminant* of our polynomial g from Equation 2.

We have arrived at a formula for our root:

$$\beta_1 = u + v = \sqrt[3]{\frac{-q + \sqrt{-\Delta/27}}{2}} + \sqrt[3]{\frac{-q - \sqrt{-\Delta/27}}{2}} \tag{19}$$

$$= \sqrt[3]{-q/2 + \sqrt{-\Delta/108}} + \sqrt[3]{-q/2 - \sqrt{-\Delta/108}} \tag{20}$$

There is a somewhat subtle point here. We cannot quite say $\delta = \sqrt{\Delta}$, because there are two possible choices for the square root. However, Equation 19 involves $\sqrt{-\Delta/27}$ and $-\sqrt{-\Delta/27}$ symmetrically, so that either choice of square root will yield the same result. We will return to this additional symmetry in the next section.

We still need to be able to compute Δ. As a symmetric polynomial in the β_i, it is in fact a polynomial in the elementary symmetric functions of the β_i, which are, up to sign, the coefficients of g: $0, p$, and q. A rather tedious calculation tells us that

$$\Delta = -4p^3 - 27q^2 \tag{21}$$

We will actually find an alternate route to this formula in Exercise 18. In the meantime, using Equation 21 in conjunction with Equation 20 finally brings us to Cardano's formula, Equation 1.

Before turning to the resolution of our 9-solutions problem, let's deal with the additional symmetry that has been lurking in the background.

7. The Galois Group and the Discriminant

Recall from Section 4 that for an irreducible cubic $G = \mathrm{Gal}(E : K)$ is either S_3 or A_3. In this section, we will distinguish these two cases by looking more closely at δ. Note that nothing in this section depends on having a cube root of unity (ω) in our base field K.

Recall Equation 14:

$$\delta = (\beta_1 - \beta_2)(\beta_2 - \beta_3)(\beta_1 - \beta_3)$$

Any permutation of the β_i will simply permute these terms, with some number of sign changes. In fact, for any $\gamma \in G$,

$$\gamma(\delta) = \operatorname{sgn}(\gamma)\delta \tag{22}$$

where $\operatorname{sgn}(\gamma)$ is the sign of γ considered as a permutation of the roots $\beta_1, \beta_2, \beta_3$. For many people, this is essentially the definition of the sign of a permutation; if that doesn't convince you, note that the number of terms of δ which change sign under the application of γ is the number of order-inversions by the permutation γ.

In any case: even permutations of our roots fix δ, while odd permutations carry δ to $-\delta$. Since A_3 is the group of even permutations, δ is in K', the fixed field of A_3.

If $\Delta = \delta^2$ is a square in K, then both of its square roots will lie in K (note that for higher powers this is not necessarily true—one n-th root lying in K does not mean that they all do). As a result, $\delta \in K$, which means that δ must be fixed by *every* element of G. It follows from equation 22 that every element of G is in A_3, and hence that $G = A_3$. (In fact, this argument works more generally: if the discriminant of a polynomial is a square in the ground field, then the Galois group of the polynomial is contained in A_n.)

On the other hand, if Δ is not a square in K, then $\delta \in K'$ but $\delta \notin K$. Therefore, $[K' : K] > 1$ and by the discussion in Section 4, $G = S_3$. To sum up, $G = A_3$ if Δ is a square in K, and $G = S_3$ otherwise.

Since $\delta \in K'$, $K \subset K(\delta) \subset K'$. When Δ is a square in K, $G = A_3$ and $K' = K$, hence $K' = K(\delta)$. When Δ is not a square in K, $\delta \notin K$, and $K(\delta)$ must be all of K' since $[K' : K] = 2$. In either case, $K' = K(\delta)$.

Let's look at the second case, $G = S_3$, in more detail.

8. When $G = S_3$

Throughout this section, we will assume that $G = S_3$.

The normal subgroup A_3 fixes $K' = K(\delta)$. Any $\gamma \in G$ will carry K' to itself; even permutations will fix K', while odd permutations carry δ to $-\delta$, by equation 22. The Galois group $\operatorname{Gal}(K' : K) = S_3/A_2$ has order 2, and its non-trivial element carries δ to $-\delta$, just as in Exercise 3.

Let τ be the element of S_3 which fixes β_1 but interchanges β_2 and β_3. Since τ is an odd permutation, we know that $\tau(\delta) = -\delta$ by Equation 22, and so τ interchanges u^3 and v^3 by Equations 16 and 17.

The fact that τ interchanges u^3 and v^3 captures the symmetry between the two cube roots in Cardano's formula. In fact, it tells us that u^3 and v^3 are roots of a single quadratic equation with coefficients in K. The expressions under the cube roots in Cardano's formula are the two roots of that quadratic, as given by the quadratic formula. The action of τ corresponds to a different choice of $\sqrt{-\Delta/27}$, interchanging the cube roots of u^3 and v^3 in Equations 19, 20 and 1.

We know that u^3 and v^3 lie in K'; since $\tau(u^3v^3) = v^3u^3 = u^3v^3$, it follows that $u^3v^3 \in K$. Actually, we can already see this explicitly from Equations 16 and 17; multiplying them tells us that

$$u^3v^3 = \frac{q^2 + \Delta/27}{4} \tag{23}$$

which is an algebraic combination of elements of K, hence in K.

Exercise 14. *Use Equation 21 and Equation 23 to prove that*

$$u^3v^3 = -p^3/27$$

In fact, we shall see in the next section (Exercise 27) that $uv = -p/3$. Taking that as a given for the moment, we can look at the standard derivation of the cubic formula and see how it relates to the approach we have taken.

Exercise 15. *Using the identity $(u+v)^3 = u^3+v^3+3uv(u+v)$, show that when $uv = -p/3$ a marvelous cancelation occurs and the depressed cubic $g(x) = x^3+px+q$ (Equation 2) becomes $g(u+v) = u^3+v^3+q$. Roots of $g(x)$ correspond to solutions of $u^3+v^3 = -q$ (which is identical to Equation 9). Knowing u^3+v^3 and u^3v^3, find a quadratic equation that has u^3 and v^3 as solutions. (Alternatively, take $v = -p/(3u)$ and find a quadratic equation that has u^3 as a root; show that v^3 is also a root.) Use this quadratic equation to derive Cardano's fomula (Equation 1). Show that the discriminant of the quadratic equation is $\sqrt{-\Delta/27}$, and that its splitting field is $K(\delta)$.*

We also have the following:

Exercise 16. *Show that τ not only interchanges u^3 and v^3, it interchanges u and v.* Hint: $\tau(u)+\tau(v) = \tau(u+v) = \tau(\beta_1) = \beta_1 = u+v$. Use Equation 10 to show that $\tau(u)-\tau(v) = v-u$.

We can now diagram Cardano's formula (Equation 1) indicating how the Galois group acts on each part of it:

(24)
$$\overbrace{\sqrt[3]{\underbrace{-\frac{q}{2}+\overbrace{\underbrace{\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}_{\tau \text{ multiplies by } -1}}^{\text{in } K'=K(\delta)}}_{\sigma \text{ multiplies by } \omega}}+\sqrt[3]{\underbrace{-\frac{q}{2}-\overbrace{\underbrace{\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}_{\tau \text{ multiplies by } -1}}^{\text{in } K'=K(\delta)}}_{\sigma \text{ multiplies by } \omega^2}}}^{\text{exchanged by } \tau}$$

Let's complete our understanding of the Galois correspondence between subgroups of G and intermediate fields between E and K. We have seen above that, as always, the full Galois group G corresponds to the ground field K and the trivial subgroup of G corresponds to the full field E. The normal subgroup A_3 of order 3 corresponds to the Galois extension $K' = K(\delta)$ of K of degree 2. This leaves us with 3 subgroups of order 2, each generated by a transposition.

The transposition τ fixes β_1, so $K(\beta_1)$ is contained in its fixed field. $K(\beta_1)$ is an extension of K of degree 3, and so it must be equal to the fixed field of τ. In a similar way, $K(\beta_2)$ corresponds to the subgroup of order 2 fixing β_2 and $K(\beta_3)$ corresponds to the subgroup of order 2 fixing β_3.

Exercise 17. *When $G = S_3$, show that $E = K(\beta_i, \delta)$. When $G = A_3$, show that $E = K(\beta_1) = K(\beta_2) = K(\beta_3)$.*

9. The Product uv, and Conclusion

It is possible compute uv with a somewhat laborious computation, but we can also let symmetry do the heavy lifting. From Equation 8a,

(25)
$$\beta_1{}^2 = (u+v)^2 = u^2+2uv+v^2$$

Now uv satisfies $\sigma(uv) = (\omega u)(\omega^2 v) = uv$, so uv is a 1-eigenvector of σ, and $\Pi_1(uv) = uv$. On the other hand, $\sigma(u) = \omega u$, so $\sigma(u^2) = \omega^2 u^2$, that is, u^2 is an ω^2-eigenvector of σ. As a result $\Pi_1(u^2) = 0$. A similar argument shows that v^2 is an ω-eigenvector of σ, and hence $\Pi_1(v^2) = 0$. Applying Π_1 to Equation 25 and then applying Equation 5a gives us

$$2uv = \Pi_1({\beta_1}^2) = \frac{1}{3}({\beta_1}^2 + {\beta_2}^2 + {\beta_3}^2) \tag{26}$$

${\beta_1}^2 + {\beta_2}^2 + {\beta_3}^2$ is a symmetric polynomial in the roots, so as before it will be a polynomial in p and q. Using the identity

$$(\beta_1 + \beta_2 + \beta_3)^2 = {\beta_1}^2 + {\beta_2}^2 + {\beta_3}^2 + 2(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)$$

and applying Equations 3a and 3b, we obtain

$$0 = {\beta_1}^2 + {\beta_2}^2 + {\beta_3}^2 + 2p$$

Combining this result with Equation 26 gives us the promised result that

$$uv = -p/3 \tag{27}$$

In the previous section, we showed that $u^3v^3 = -p^3/27$ by using the formula for the discriminant. As promised earlier, we do not need to rely on an independent derivation of the discriminant formula.

Exercise 18. *Prove Equation 21 by combining Equations 27 and 23.*

Equation 27 also allows us to resolve the mystery of the 9 potential solutions of Cardano's formula, Equation 1. The chosen cube roots must be such that their product is $-p/3$. In fact, mindlessly applying Cardano's formula is a terrible way to solve a cubic equation: it is far more computationally efficient to take one of the cube roots, divide it into $-p/3$ to obtain the other cube root, and then add them to get the solution to our polynomial equation.

Having resolved the 9-solutions issue, we close with a few exercises.

Exercise 19. *In the reducible case, show that a depressed cubic with a double root must have the form $(x - r)^2(x + 2r)$. Show that Cardano's formula, along with the requirement that the cube roots multiply out to $-p/3$, gives r (twice) and $-2r$ (once) as roots.*

As a parting exercise, the reader may wish to wrestle with what happens when our ground field K does not contain a primitive cube root of unity.

Exercise 20. *Let K_0 be a field (such as $\mathbb{Q}$) which does not contain a primitive cube root of unity, and let $K = K_0(\omega)$ be the quadratic extension of K_0 with $\omega^2 + \omega + 1 = 0$. Show that a square in K is either a square in K_0 or a square in K_0 multiplied by -3.*

Exercise 21. *Let g be an irreducible cubic polynomial with coefficients in K_0, and let E_0 be the splitting field of g over K_0, and suppose that K_0 does not contain a primitive cube root of unity. Let $K = K_0(\omega)$ and $E = E_0(\omega)$, and let $\Delta \in K_0$ be the discriminant of g (See Figure 1). Show that there are three mutually exclusive possibilities:*

(a) Δ is a square in K_0; $\mathrm{Gal}(E : K) = \mathrm{Gal}(E_0 : K_0) = A_3$.
(b) Neither Δ nor -3Δ is a square in K_0; $\mathrm{Gal}(E : K) = \mathrm{Gal}(E_0 : K_0) = S_3$.

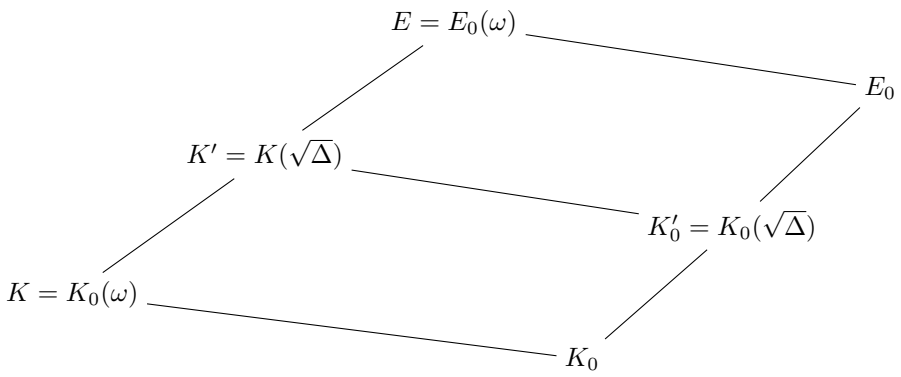

FIGURE 1. Diagram for Exercise 21.
Note that the diagram collapses in case (c)

(c) -3Δ *is a square in* K_0*;* $\mathrm{Gal}(E_0 : K_0) = S_3$*,* $\mathrm{Gal}(E : K) = A_3$*,* $K = K_0(\omega) = K_0(\sqrt{\Delta})$*,* $E = E_0$*, and if* $\tau \in \mathrm{Gal}(E_0 : K_0)$ *has* $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$*, then* $\tau(\omega) = \omega^2$*.*

REFERENCES

[1] Michael Artin. *Algebra*. Englewood Cliffs, N.J.: Prentice Hall, 1991. ISBN: 0130047635.

[2] Girolamo Cardano. *The Great Art; or, The Rules of Algebra*. eng. Cambridge, Mass.: M.I.T. Press, 1968.

[3] William Dunham. *Journey through Genius : The Great Theorems of Mathematics*. Wiley science editions. New York: Wiley, 1990. ISBN: 0471500305.

[4] Ron Irving. *Beyond the Quadratic Formula*. Mathematical Association of America, 2013. ISBN: 9780883857830.

[5] Svante Janson. *Roots of polynomials of degrees 3 and 4*. 2010. arXiv: 1009.2373.

[6] Barry Mazur. *Imagining Numbers : (particularly the square root of minus fifteen)*. 1st ed. New York: Farrar, Straus, and Giroux, 2003. ISBN: 0374174695.

[7] Alasdair Wilkins. *Stigler's Law: Why nothing in science is ever named after its actual discoverer*. 2011 (accessed January 9, 2018). URL: https://io9.gizmodo.com/5820736/.