Galois Theory, Galois Style

Ivan Aidun, 2/29/24

Solving Quadratics

If we have a quadratic polynomial $f = x^2 + a_1x + a_2$, and we know that the complex roots of f are r_1 and r_2, then we can write $x^2 + a_1x + a_2 = (x - r_1)(x - r_2)$. When we expand the right hand side, we get $x^2 - (r_1 + r_2)x + r_1r_2$. Since this must equal our original polynomial, we get the relations

$$\begin{aligned} -a_1 &= r_1 + r_2 \\ a_2 &= r_1r_2. \end{aligned}$$

Notice that the functions $r_1 + r_2$ and r_1r_2 are both symmetric in the roots. However, when we solve the quadratic formula we need to be able to write the non-symmetric functions r_1 and r_2 in terms of these symmetric functions. Let's see how this happens:

$$\begin{aligned} r_1, r_2 &= \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2} \\ &= \frac{r_1 + r_2 \pm \sqrt{(r_1 + r_2)^2 - 4r_1r_2}}{2} \\ &= \frac{r_1 + r_2 \pm \sqrt{r_1^2 - 2r_1r_2 + r_2^2}}{2}. \end{aligned}$$

Notice that all the functions inside are still symmetric, but the asymmetry is introduced by the square root. Notice that $r_1^2 - 2r_1r_2 + r_2^2 = (r_1 - r_2)^2 = (-r_1 + r_2)^2$. So, there are two functions, $r_1 - r_2$ and $-r_1 + r_2$, that we could choose for $\sqrt{r_1^2 - 2r_1r_2 + r_2^2}$, but these two functions are no longer symmetric, but instead when we switch r_1 and r_2, these two functions get multiplied by -1.

Solving Cubics

Completing the Cube

Moving up a degree, let's look at a cubic polynomial $x^3 + a_1x^2 + a_2x + a_3$. Similar to how when we derive the quadratic formula, we use the technique of "completing the square", there is a similar technique called "completing the cube".

For example, if we want to solve $x^3 - 6x^2 + 5x - 4 = 0$, we can subtract $5x - 4$ from both sides to get $x^3 - 6x^2 = -5x + 4$. Now, we can ask if there's a cube polynomial $(x + a)^3$ whose first two terms are $x^3 - 6x^2$. Since $(x + a)^3 = x^3 + 3ax^2 + 3a^2x + a^3$, if I want the first two terms to be $x^3 - 6x^2$, I should choose $a = -2$. Now, we can add $12x - 8$ to both sides of $x^3 - 6x^2 = -5x + 4$. When we do, we get

$$\underbrace{x^3 - 6x^2 + 12x - 8}_{=(x-2)^3} = 7x - 4.$$

Now, we can substitute in $X = x - 2$ (first rewriting $7x - 4$ as $7(x - 2) + 10$), and we find that solving our original cubic is the same as solving $X^3 - 7X + 10$. But we have made progress, because now we have no X^2 term to worry about! A cubic polynomial with no quadratic term is called a "depressed cubic", and below we will only work with such cubics.

Onward to Galois Theory

So, if we have a depressed cubic $x^3 + a_2x + a_3$, and its roots are r_1, r_2, r_3, then we get

$$\begin{aligned} 0 &= r_1 + r_2 + r_3 \\ a_2 &= r_1r_2 + r_1r_3 + r_2r_3 \\ -a_3 &= r_1r_2r_3. \end{aligned}$$

In order to pick out r_1, r_2, r_3, we again need to be able to solve for non-symmetric functions in terms of symmetric functions. This will be quite complicated, so let's start with an easier goal, let's consider this function:

$$\Delta(r_1, r_2, r_3) = r_1^2r_2 + r_2^2r_3 + r_3^2r_1 - r_2^2r_1 - r_3^2r_2 - r_1^2r_3.$$

This function has the properties that $\Delta(r_1, r_2, r_3) = -\Delta(r_2, r_1, r_3)$ and $\Delta(r_1, r_2, r_3) = \Delta(r_2, r_3, r_1)$. That is to say, Δ gets multiplied by -1 if two of the entries are swapped, but stays the same if all three entries get cyclically rotated. Functions like Δ, or like $r_1 - r_2$ from before, that have the property that swapping two roots multiplies them by -1 are called *alternating* functions.

One can check that Δ and $-\Delta$ are the two functions we can choose for $\sqrt{-27a_3^2 - 4a_2^3}$ (and I do so in the last section). So, again here we see that when we start with functions that are symmetric, and we take a square root, we end up with functions that are "half as symmetric", in the sense that only half of the permutations of r_1, r_2, r_3 preserve Δ, and the other half negate it.

We want to go further, though, and find the roots r_1, r_2, r_3. In order to do this, we need to define $\omega = \frac{-1+i\sqrt{3}}{2}$. This number has the properties that $\omega^2 + \omega + 1 = 0$ and $\omega^3 = 1$. Let's now look at the function $S_1 = r_1 + \omega r_2 + \omega^2 r_3$. This function has the property that when you apply a permutation of the roots fixing Δ (that is, a cyclic permutation), S_1 gets multiplied by ω or ω^2, similarly to how swapping two roots multiplied Δ by -1. The function S_1 has a "twin", $S_2 = r_1 + \omega^2 r_2 + \omega r_3$, which gets multiplied by ω when you cycle it the opposite direction. Swapping any pair of roots swaps S_1 with S_2. Notice that if we knew S_1 and S_2, we could find r_1, r_2, r_3 by $r_1 = \frac{1}{3}(S_1 + S_2)$, $r_2 = \frac{1}{3}(\omega^2 S_1 + \omega S_2)$, $r_3 = \frac{1}{3}(\omega S_1 + \omega^2 S_2)$.

So, now we have S_1 and S_2, which both have the property that S_i^3 is invariant under cyclic permutations, which means $S_1^3 + S_2^3$ is completely symmetric, and $S_1^3 - S_2^3$ is alternating. This means we should be able to write $S_1^3 + S_2^3$ in terms of a_1, a_2, a_3, and $S_1^3 - S_2^3$ in terms of a_1, a_2, a_3, and Δ. It turns out that $S_1^3 + S_2^3 = -27a_3$ and $S_1^3 - S_2^3 = 3\sqrt{-3}\Delta$. So, we can write

$$S_1 = \sqrt[3]{\frac{1}{2}(-27a_3 + 3\sqrt{-3}\Delta)}, \qquad S_2 = \sqrt[3]{\frac{1}{2}(-27a_3 - 3\sqrt{-3}\Delta)}.$$

Once again, when we introduce the cube root, we break the remaining symmetries that Δ had, so that S_1 and S_2 are "1/3 as symmetric", in the sense that only one of the three symmetries of Δ is also a symmetry of S_1 and S_2. (And it's the "do nothing" symmetry!)

Galois' observation seems to have been that for a general polynomial of degree n, solving that polynomial using radicals depends on being able to carry out a strategy like this. First, you need to find a function $F_1(r_1, \ldots, r_n)$ so that some permutations of the roots fix F_1, and some multiply it by an kth root of unity, that is, by a number $\zeta \in \mathbb{C}$ so that $\zeta^k = 1$. Then F^k will be symmetric in the roots, and so can be expressed in terms of the coefficients of the polynomial. Then, you repeat, you try to find a function $F_2(r_1, \ldots, r_n)$ so that, of the permutations that fix F_1, some fix F_2, and some multiply F_2 by a ℓth root of unity, etc. If you are able to continue like this, eventually you reach functions like our S_1, S_2 above, which have no symmetries, and you can use them to write down the roots. However, you're not guaranteed to be able to do this, but saying why precisely would require more of a dive into group theory and field theory, so we'll leave it for another time.

Writing Δ^2 in terms of a_2, a_3

Because of the relations we had before, we can see that Δ^2 is actually completely symmetric in r_1, r_2, r_3, and it is actually a fact that any symmetric function can be written in terms of the three we already have. Writing out all of Δ^2 in terms of r_1, r_2, r_3 would take a while, and it would be uninformative anyway. Instead, let's just think about the kinds of terms that will show up in Δ^2. We can get:

- terms that look like $r_i^4 r_j^2$,
- terms that look like $2r_i^3 r_j^2 r_k$,
- terms that look like $-2r_i^3 r_j^3$,

- terms that look like $-2r_i^4 r_j r_k$, and
- one term that looks like $-6r_i^2 r_j^2 r_k^2$.

This is a lot to keep track of. To simplify our lives a bit, let's introduce the notation

$$m_{n,m,o} = \sum_{i \neq j \neq k} r_i^n r_j^m r_k^o.$$

We will drop final 0s, so $m_{1,1}$ means the same thing as $m_{1,1,0}$. Then our accounting above tells us $\Delta^2 = m_{4,2} + 2m_{3,2,1} - 2m_{3,3} - 2m_{4,1,1} - 6m_{2,2,2}$. Moreover, we know $m_1 = 0$, $m_{1,1} = a_2$, and $m_{1,1,1} = -a_3$.

To write Δ^2 in terms of a_2 and a_3, first notice that Δ *almost* looks like $m_{2,1}$, except that half the coefficients are negative. In fact, we have that

$$\Delta^2 = m_{2,1}^2 - 4m_{3,3} - 4m_{4,1,1} - 12m_{2,2,2}.$$

Let's figure out these terms one at a time.

- To start off, it's easy to see that $m_{2,2,2} = m_{1,1,1}^2 = a_3^2$.
- After a little thinking, we can also see that when we multiply out $(r_1 + r_2 + r_3)(r_1 r_2 + r_2 r_3 + r_1 r_3)$, we get a term $r_i^2 r_j$ whenever the root from the left term is included in the product of two roots from the right term. We also get a term $r_1 r_2 r_3$, and we can get it in 3 different ways. So, this means $m_1 m_{1,1} = m_{2,1} + 3m_{1,1,1}$, which we can rewrite as $m_{2,1} = m_1 m_{1,1} - 3m_{1,1,1} = 3a_3$.
- For $m_{4,1,1}$, we have $m_{4,1,1} = m_{1,1,1} m_3$. Similar to the previous bullet point, we can think about the terms we get when we multiply out $(r_1 + r_2 + r_3)^3$. If you do, you will find that $m_1^3 = m_3 + 3m_{2,1} + 6m_{1,1,1}$. Rewriting, we get $m_3 = m_1^3 - 3m_{2,1} - 6m_{1,1,1} = -3a_3$. Thus, $m_{4,1,1} = 3a_3^2$.
- Finally, similar thinking to the last bullet point will show that $m_{1,1}^3 = m_{3,3} + 3m_{3,2,1} + 6m_{2,2,2} = m_{3,3} + 3m_{2,1} m_{1,1,1} + 6m_{2,2,2}$. Rewriting that, we get

$$\begin{aligned} m_{3,3} &= m_{1,1}^3 - 3m_{2,1} m_{1,1,1} - 6m_{2,2,2} \\ &= a_2^3 + 9a_3^2 - 6a_3^2 \\ &= a_2^3 + 3a_3^2. \end{aligned}$$

Putting it all together, we have found that

$$\begin{aligned}\Delta^2 &= m_{2,1}^2 - 4m_{3,3} - 4m_{4,1,1} - 12m_{2,2,2} \\ &= 9a_3^2 - 4(a_2^3 + 3a_3^2) - 4(3a_3^2) - 12a_3^2 \\ &= -27a_3^2 - 4a_2^3.\end{aligned}$$