GALOIS THEORY: LECTURE 3

FEBRUARY 8, 2023

1. Insolvability of the quintic: Arnold vs. Galois

Recall that last lecture was devoted to the proof of

Theorem 1 (Arnold, 1963)**.** *There is no quintic formula built out of a finite combination of radicals, continuous functions, and the four field operations* $+, -, \times, \div$.

In particular, this implies there's no quintic formula one can write down using any finite combination of radicals, the functions $\exp()$, $\sin()$, and $\cos()$, and the field operations. It is instructive to compare this to what we'll be able to get from Galois theory:

Theorem 2 (Consequence of Galois theory)**.** *Given any polynomial* $f(x)$*, pick one of its roots* r_f*, and express it using only the coefficients of* f*, the four field operations, and radicals. There exists an algorithm which, given* f*, predicts the level of nesting of radicals in* r_f.

For example, we will be able to run this algorithm to deduce that the polynomial $x^5 - x - 1$ requires *infinite* nesting of radicals. This immediately implies that there's no general quintic formula (built solely out of a finite combination of the field operations and radicals).

Comparing Arnold's and Galois' conclusions, we see that each has an advantage over the other. Galois theory can be used to determine the solvability of a particular polynomial, which is stronger than Arnold's approach (which only deals with the solvability of a general quintic). On the other hand, the notion of 'formula' in Galois theory is more restrictive than in Arnold's approach, as the latter allows the use of arbitrary continuous functions in addition to radicals.

2. Solving the cubic

Arnold's proof of the nonexistence of a quintic formula motivates some of the key ideas we'll see later on as we develop Galois theory. It turns out that some other ideas of Galois theory stem from the derivation of the cubic formula. How do we solve a general cubic equation $x^3 + ax^2 + bx + c = 0$? This isn't obvious (to Leo, at any rate). For inspiration, we turn to what we know: the quadratic. For example, how do we solve the quadratic equation $x^2 - 4x + 6 = 0$? Of course we can do this using the quadratic formula, but suppose we didn't know that formula. How would we approach this? Tommy proposed the following computation:

$$\begin{aligned} & x^2 - 4x + 6 = 0 \\ \implies & x^2 - 4x + 4 + 2 = 0 \\ \implies & (x-2)^2 = -2 \\ \implies & x = 2 \pm \sqrt{-2} \end{aligned}$$

The key idea here was to *complete the square*: we found the perfect square which looks as much as possible like the given quadratic, and then rewrote the original in terms of that square.

Remark. We're happy to say at the end of the above calculation that we 'solved' the original, but what is $\sqrt{-2}$? It's a solution to $x^2 = -2$. (In fact, it's a solution *by definition* – we didn't actually have to do any work to solve $x^2 = -2$, which is suspicious!) Thus, all we did was to reduce solving the original equation to finding the roots of $x^2 + 2$.

Summary of a lecture by Leo Goldmakher; typed by Jacob Lehmann Duke from notes by Shaurya Taxali.

Armed with this intuition, let's return to the cubic. How do we find the roots of

$$f(x) := x^3 - 3x^2 - 3x + 7?$$

And what might we expect the answer to look like? We should certainly allow the field operations $+, -, \times$, and $\div$ as a start. Jamie suggested that square roots might also be involved, since we can factor f as a quadratic times a linear factor and roots of the quadratic should involve square roots. Inspired by the three solutions to the equation $x^3 - 2 = 0$, Jonathan observed that we'll likely require using a $\sqrt[3]{\cdot}$ somewhere, and Jenna added that we will probably need $\omega = e^{2\pi i/3}$.

OK, so how do we actually solve $f(x) = 0$? We pursued a number of suggestions (by Jamie, Alex, Felix, and Carlos), but couldn't seem to make much progress. However, building on some of these ideas and inspired by the quadratic case, Jake proposed that we attempt to 'complete the cube', whatever that means. With Alex's help, we realized this in the form

$$\begin{aligned} f(x) &= (x-1)^3 - 6x + 8 \\ &= (x-1)^3 - 6(x-1) + 2. \end{aligned}$$

Thus, to find the roots of $f(x)$ it suffices to find the roots of the simpler-looking cubic

$$g(x) := x^3 - 6x + 2.$$

Let's call these roots α, β, and γ. Observe that

$$\begin{aligned} g(x) &= (x-\alpha)(x-\beta)(x-\gamma) \\ &= x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma \qquad (\clubsuit) \\ &= x^3 + 0x^2 - 6x + 2, \end{aligned}$$

which implies that $\alpha + \beta + \gamma = 0$, $\alpha\beta + \alpha\gamma + \beta\gamma = -6$, and $\alpha\beta\gamma = -2$. Sadly, trying to solve this system of equations simply gives us back our original $g(x)$, so it seems we're stuck.

However, this does tell us something: that any cubic formula *must involve square-roots.* To see this, suppose Évariste Galois rose from the grave and magically brought us the value of α. Then finding the other roots would be easy: we have

$$\beta + \gamma = -\alpha \qquad \text{and} \qquad \beta\gamma = -\frac{2}{\alpha}$$

so defining the auxiliary quadratic

$$h(t) := (t-\beta)(t-\gamma) = t^2 + \alpha t - \frac{2}{\alpha}$$

and applying the quadratic formula yields

$$\beta, \gamma = \frac{1}{2}\left(-\alpha \pm \sqrt{\alpha^2 + \frac{8}{\alpha}}\right).$$

This validates Jamie's prediction that square roots should be involved in solving a cubic!

This insight is nice, but brings us no closer to actually finding the roots of $g(x)$. To understand the situation better, let's temporarily return to the familiar case of the quadratic. Suppose that we didn't know the quadratic formula, but somehow guessed that the roots of $x^2 - 4x + 6$ should take the form $r \pm \sqrt{s}$. Then

$$(r + \sqrt{s}) + (r - \sqrt{s}) = 4 \qquad \text{and} \qquad (r + \sqrt{s})(r - \sqrt{s}) = 6,$$

which immediately implies $r = 2$ and $s = -2$. The take-away here is that *if we can guess the correct shape of the roots, then it's easy to actually find them.* In fact, even if we'd made a more primitive guess that the roots should be of the form $r \pm s$, we would have been able to solve the quadratic with ease!

Let's try this approach to cubics. To inspire our guessing, we first wrote down an explicit comparison between the quadratic and cubic cases. (Recall that ω denotes the cube-root of unity $e^{2\pi i/3}$.)

Quadratic		Cubic	
equation	solution	equation	solution
$x^2 - 1 = 0$	$x = \pm 1$	$x^3 - 1 = 0$	$x = 1, \omega, \omega^2$
$x^2 - a = 0$	$x = \pm\sqrt{a}$	$x^3 - a = 0$	$x = \sqrt[3]{a}, \omega\sqrt[3]{a}, \omega^2\sqrt[3]{a}$
$x^2 + bx + c = 0$	$x = r \pm \sqrt{s}$	$x^3 - 6x + 2 = 0$	???

Inspired by some nice initial guesses by Molly and Eli, Tommy proposed that the three roots of $g(x)$ might be of the form

$$r + \sqrt[3]{s}, r + \omega\sqrt[3]{s}, r + \omega^2\sqrt[3]{s}.$$

From (♣), we deduce

$$\begin{aligned}(r + \sqrt[3]{s}) + (r + \omega\sqrt[3]{s}) + (r + \omega^2\sqrt[3]{s}) &= 0\\ (r + \sqrt[3]{s})(r + \omega\sqrt[3]{s})(r + \omega^2\sqrt[3]{s}) &= -2.\end{aligned} \tag{♡}$$

Eli observed that the former equation simplifies considerably, thanks to

Lemma 1. $1 + \omega + \omega^2 = 0$.

Proof. We saw three proofs of this:

- (Eli) Using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$, we find $1+\omega+\omega^2 = 1+(-\frac{1}{2}+\frac{\sqrt{3}}{2}i)+(-\frac{1}{2}-\frac{\sqrt{3}}{2}i) = 0$.
- (Friedrich) $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$.
- (Leo) We have $\omega(1 + \omega + \omega^2) = \omega + \omega^2 + \omega^3 = 1 + \omega + \omega^2$. □

The first equation of (♡) now implies $r = 0$, whence the second implies $s = -2$. But this is clearly wrong! In hindsight, we should have known this plan wouldn't work, since we were trying to use two indeterminates to satisfy three conditions (imposed by the coefficients of g). Oops.

Undeterred, we look back at the table comparing quadratic and cubics and try to make a better guess for what form the roots of the cubic should take. We tried to express the three roots of g using three linear combinations of indeterminates r, s, t, using $1, \omega$, and ω^2 as coefficients. Our first attempt led to a system with no solution, which led Jonathan to propose

$$\begin{aligned}\alpha &= r + s + t\\ \beta &= r + \omega^2 s + \omega t\\ \gamma &= r + \omega s + \omega^2 t.\end{aligned}$$

Note that we are *not* writing any cube roots down, because it's not clear where they should go! Instead, we focus on the use of permutations of the cube roots of unity as coefficients—by analogy with ± 1 being the coefficients for the two roots of a quadratic.

Going back to (♣), we deduce

$$(r + s + t) + (r + \omega^2 s + \omega t) + (r + \omega s + \omega^2 t) = 0,$$

instantly implying $r = 0$ via Lemma 1. (This step simplifies the rest of our computation dramatically, and vindicates Jake's decision to complete the cube!) Plugging $r = 0$ into (♣), we deduce

$$\begin{aligned}(s + t)(\omega^2 s + \omega t) + (s + t)(\omega s + \omega^2 t) + (\omega^2 s + \omega t)(\omega s + \omega^2 t) &= -6\\ (s + t)(\omega^2 s + \omega t)(\omega s + \omega^2 t) &= -2.\end{aligned} \tag{♠}$$

The latter equation is relatively straightforward to simplify: pulling ω's out of the factors we find

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

Next we turn to the first equation of (♠). Expanding the products, we see that there are just three types of terms: s^2, t^2, and st. Lemma 1 shows that the terms with s^2 and t^2 both vanish, and that the st term has coefficient -3. Thus, we see that (♠) reduces down to

$$\begin{aligned}-3st &= -6\\ s^3 + t^3 &= -2.\end{aligned}$$

Now we proceed in a familiar way: we define an auxiliary quadratic

$$h(x) := (x - s^3)(x - t^3) = x^2 + 2x + 8.$$

The quadratic formula implies $s^3, t^3 = -1 \pm \sqrt{-7}$, whence $s, t = \sqrt[3]{-1 \pm \sqrt{-7}}$. We've found a root of g:

$$\alpha = r + s + t = \sqrt[3]{-1 + \sqrt{-7}} + \sqrt[3]{-1 - \sqrt{-7}}.$$

Now that we have one root, it's straightforward to determine the other two (as discussed above).

Remark. Given an arbitrary cubic polynomial, the process above works! More precisely, one can complete the cube to eliminate the quadratic term, then guess the form of the solutions (namely, the form we guessed above), and then solve for s and t using an auxiliary quadratic. One curiosity is that there are instances in which a cubic has three real roots, but the cubic formula will only produce these if one is willing to use complex numbers (the imaginary parts ultimately cancel out). Thus, the cubic formula *necessitated* the discovery of complex numbers! You will explore this further on your next problem set.