GALOIS THEORY : LECTURE 3

LEO GOLDMAKHER

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).

Remark. It is in fact possible to express a root of $x^5 - x - 1$ using infinitely many radicals: if $x^5 - x - 1 = 0$ then $x^5 = 1 + x$, whence

$$x = \sqrt[5]{1+x} = \sqrt[5]{1+\sqrt[5]{1+x}} = \sqrt[5]{1+\sqrt[5]{1+\sqrt[5]{1+\cdots}}}$$

By truncating the right hand side after a finite number of radicals, one can obtain arbitrarily good approximations to a root.

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

First, let's try solving the quadratic to gain some intuition:

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

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.

Date: February 8, 2018.
Based on notes by Eli Cytrynbaum.

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 $x^2 + 2$.

Let's return to the cubic. How do we find the roots of

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

After trying out a few interesting proposals (which, unfortunately, didn't seem to lead anywhere), we decided to try completing the cube, i.e., finding the cube which looks most like f. Playing around a bit, we figured out that

$$f(x) = (x-1)^3 - 6(x-1) + 2.$$

This reduces our problem to finding the roots of the simpler-looking cubic

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

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

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

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 unexpected: that any cubic formula *must involve square-roots.* To see this, suppose we magically knew one of the roots, say 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 shows that any cubic formula *must* involve square-roots. (Of course, it must also involve cube-roots!)

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.*

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

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

In view of the table, we were led to guess that the roots of the cubic take the form

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

This would imply

$$\begin{aligned} g(x) &= (x - (r + \sqrt[3]{s}))(x - (r + \omega\sqrt[3]{s}))(x - (r + \omega^2\sqrt[3]{s})) \\ &= x^3 - (3r + \sqrt[3]{s} + \omega\sqrt[3]{s} + \omega^2\sqrt[3]{s})x^2 + \cdots \end{aligned}$$

Observing that

$$1 + \omega + \omega^2 = 0, \tag{1}$$

our expansion above becomes

$$g(x) = x^3 - 3rx^2 + \cdots$$

which immediately implies $r = 0$ and greatly simplifies our computations:

$$g(x) = (x - \sqrt[3]{s})(x - \omega\sqrt[3]{s})(x - \omega^2\sqrt[3]{s}) = x^3 - s.$$

Unfortunately, this is clearly false, since no matter how we pick s the linear coefficient won't match up with the linear coefficient of $g(x)$. 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. Ian suggested that the three roots should look like

$$r + s + t, \qquad r + \omega s + \omega^2 t, \qquad r + \omega^2 s + \omega t.$$

Repeating our previous computations under this hypothesis, we find

$$\begin{aligned} g(x) &= (x - (r + s + t))(x - (r + \omega s + \omega^2 t))(x - (r + \omega^2 s + \omega t)) \\ &= x^3 - 3rx^2 + \cdots \end{aligned}$$

so once again $r = 0$, which greatly simplifies our computations. (This, incidentally, is the purpose of completing the cube.) Thus,

$$\begin{aligned} g(x) &= \big(x - (s + t)\big)\big(x - (\omega s + \omega^2 t)\big)\big(x - (\omega^2 s + \omega t)\big) \\ &= x^3 + a_1 x + a_0 \end{aligned}$$

where

$$a_1 = (s + t)(\omega s + \omega^2 t) + (s + t)(\omega^2 s + \omega t) + (\omega s + \omega^2 t)(\omega^2 s + \omega t)$$

and

$$a_0 = -(s + t)(\omega s + \omega^2 t)(\omega^2 s + \omega t)$$

We simplify these one at a time. a_0 is the easier of the two: pulling ω's out of the factors we find

$$a_0 = -(s + t)(s + \omega t)(s + \omega^2 t) = -(s^3 + t^3).$$

The coefficient a_1 looks more complicated, but really only has three types of terms which arise when we expand it: s^2, t^2, and st. Applying the useful identity (1) shows that both of the s^2 and t^2 vanish, while the st term has coefficient -3. Putting all this together, we find

$$g(x) = x^3 - 3st - (s^3 + t^3)$$

Thus, $st = 2$ and $s^3 + t^3 = -2$, so we can define the auxiliary quadratic

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

The quadratic formula implies $s^3, t^3 = \frac{-2 \pm \sqrt{-28}}{2}$, whence $s, t = \sqrt[3]{-1 \pm \sqrt{-7}}$. We can now write down a root of $g(x)$: it's $r + s + t = \sqrt[3]{-1 + \sqrt{-7}} + \sqrt[3]{-1 - \sqrt{-7}}$. Now that we have one root, it's straightforward to determine the other two (as discussed above).

Remark. It turns out that the cubic formula one gets from this forces the invention of imaginary numbers, since it occasionally fails to produce solutions to cubics with three real roots – unless one admits the possibility of taking the square-root of a negative number. See problem **2.4** for an example of this.