GALOIS THEORY: LECTURE 1

JANUARY 31, 2023

1. COURSE INTRO

Welcome to Galois Theory! This is a hard but beautiful subject. Part of what's hard about it is that it brings together a lot of different ideas, and it's easy to lose track of the big picture. Perhaps it will be helpful to have an overarching question: what limitations are there on which numbers / functions we can describe? And what does this even mean?

Example 1. Consider $x^5 - x - 1 = 0$. By the Intermediate Value Theorem, this has a real solution. Can we write it down? If we're OK with using infinitely many symbols, then sure—it's just some infinite decimal. But this is unsatisfying, since there's no obvious pattern to its digits, so the best we can really do is an arbitrarily good approximation. Here's a more structured way to write down a root:

$$\begin{aligned}
&x^5 - 1 = 0 \\
&\implies x^5 = 1 + x \\
&\implies x = \sqrt[5]{1+x} = \sqrt[5]{1+\sqrt[5]{1+x}} = \cdots = \sqrt[5]{1+\sqrt[5]{1+\sqrt[5]{1+\cdots}}}
\end{aligned}$$

This is nice, but still involved infinitely many symbols. Is there a some finite combination of symbols—say, of addition, subtraction, multiplication, division, and radicals—that expresses this? We'll prove later this semester that there is not.

Example 2. The normal distribution is fundamental throughout the sciences and social sciences. Thus, we're often led to evaluate integrals of the form $\int_a^b e^{-x^2}\,dx$. Galois theory shows that there's no way to express an antiderivative of e^{-x^2} as a finite combination of elementary functions.

In summary, Galois theory is (in part) about identifying the limitations on which numbers / functions can be described using finitely many symbols. Let's warm up with an example that will highlight some of the key ideas.

2. A MOTIVATING QUESTION: DEFINING i

Question. What is i? (Furthermore, who am i? And who are u?)

Chas suggested the very reasonable definition $i = \sqrt{-1}$, meaning i is the number you square to get -1. But Tommy pointed out that $-i$ also satisfies that definition! Alex pointed out that the issue in some sense is that this definition tells you what i *does* rather than what i *is*. We're saying i is a solution to $x^2 + 1 = 0$, but this equation has two solutions.

Can we differentiate between i and $-i$ by finding a polynomial with a root at one of them but not the other? Jonathan jokingly suggested $f(x) = x - i$, but clearly the root of that polynomial isn't a good definition for i. What about some $f \in \mathbb{R}[x]$, meaning a polynomial with real coefficients? ($\mathbb{R}[x]$ is read 'R brackets x'.) The class intuition was that there is no such polynomial, and Zoe proposed a proof:

Proposition 1. *If $f \in \mathbb{R}[x]$ and $f(i) = 0$, then $f(-i) = 0$ as well.*

Zoe's proof. Suppose $f(i) = 0$. Then $f(-i) = f(\bar{i}) = \overline{f(i)} = 0$. □

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

Remark. This proof relies on the fact that polynomials are built out of addition and multiplication, and that complex conjugation commutes with both of these, i.e.

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2 \quad \text{and} \quad \overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}.$$

This observation shows that the result should hold for any function built out of operations that commute with complex conjugation; you'll explore this on your first problem set.

Tommy asked: why doesn't the same proof go through for polynomials in $\mathbb{C}[x]$? Let's see what happens if we try to apply the same logic to $f(x) = x - i$. We have

$$f(-i) = f(\bar{i}) = \bar{i} - i = -i - i = -2i,$$

so $f(\bar{i}) \neq \overline{f(i)}$! More generally, Zoe pointed out that $f(\overline{z}) = \overline{f(z)}$ is only guaranteed to hold if $f \in \mathbb{R}[x]$.

3. Defining other numbers

As we've seen, it's difficult to define i. But what does it mean to define a number at all? Well, we typically define a new thing in terms of simpler, previously-defined things. For example, say we're comfortable with positive integers. If we start writing down equations involving just positive integers, we're quickly forced to define other numbers:

$$\begin{aligned} x + 2 = 2 \quad &\rightsquigarrow \quad \text{definition of } 0 \\ x + 2 = 0 \quad &\rightsquigarrow \quad \text{definition of } -2 \\ 17x - 3 = 0 \quad &\rightsquigarrow \quad \text{definition of } \frac{3}{17} \\ x^2 - 2 = 0 \quad &\rightsquigarrow \quad \text{definition of } \sqrt{2} \\ x^2 + 1 = 0 \quad &\rightsquigarrow \quad \text{definition of } i. \end{aligned}$$

There are a few things to notice about these definitions. First of all, each of the numbers we've defined is purely notation—sure, we can define the symbol $\frac{3}{17}$ to be the solution to $17x - 3 = 0$, but that doesn't actually help us understand anything about that number (for example, how to approximate its size). Second, as we already saw earlier, some equations have multiple solutions, so it's not obvious that each of the above definitions uniquely determines the number it's claiming to define. In fact, we saw that the definition of i doesn't quite work; similarly, the definition of $\sqrt{2}$ above doesn't work, since $-\sqrt{2}$ is also a solution.

We saw above that $\pm i$ are algebraically indistinguishable over $\mathbb{R}$, i.e. there's no algebraic (polynomial) relation satisfied by one that's not also satisfied by the other. What about $\pm\sqrt{2}$? Can we find a function $f \in \mathbb{Q}[x]$ such that $f(\sqrt{2}) = 0$ but $f(-\sqrt{2}) \neq 0$? (By the way, why did we switch to $\mathbb{Q}[x]$ here?)

Proposition 2. *There does not exist such a function $f \in \mathbb{Q}[x]$ such that $f(\sqrt{2}) = 0$ but $f(-\sqrt{2}) \neq 0$.*

Zoe's proof from earlier clearly doesn't work, since there are no longer any complex numbers involved so complex conjugation doesn't tell us anything. Friedrich suggested that we could modify Zoe's proof by developing a new type of conjugation that maps $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. This is a good idea that we'll explore in the future, but in the meantime, Jonathan and Carlos suggested a simpler proof: divide any f into even and odd powers, and derive a contradiction that way. More precisely:

Proof. Given $f \in \mathbb{Q}[x]$, we can write

$$f(x) = a(x^2) + xb(x^2)$$

with $a, b \in \mathbb{Q}[x]$. Suppose $f(\sqrt{2}) = 0$. Then $a(2) + b(2)\sqrt{2} = 0$. Jake pointed out this instantly implies $a(2) = 0 = b(2)$, since otherwise we'd have $\sqrt{2} = -\frac{a(2)}{b(2)} \in \mathbb{Q}$. But then

$$f(-\sqrt{2}) = a(2) - b(2)\sqrt{2} = 0,$$

as claimed. □

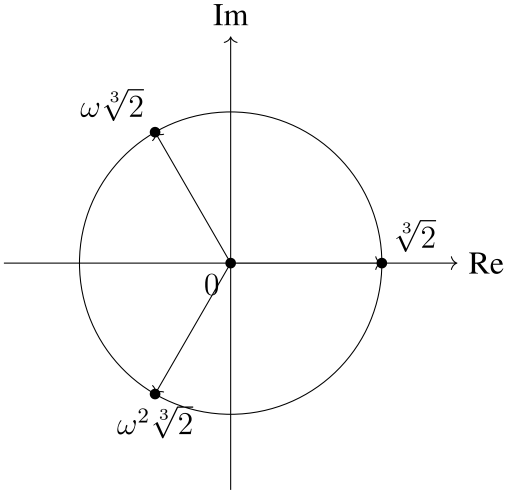
Thus, we see that $\sqrt{2}$ and $-\sqrt{2}$ are algebraically indistinguishable over $\mathbb{Q}$.

4. Other algebraically indistinguishable numbers

We've proved thus far that $\pm i$ are algebraically indistinguishable over $\mathbb{R}$, and that $\pm\sqrt{2}$ are algebraically indistinguishable over $\mathbb{Q}$. Put differently, algebraic relations are insufficient to distinguish between the two numbers. Are all numbers yoked together in algebraically indistinguishable pairs like this?

Question. What is $\sqrt[3]{2}$ algebraically indistinguishable from?

Tommy suggests the other cube roots of 2, which we can visualize as lying equally spaced around a circle in the complex plane:



Here $\omega = e^{\frac{2\pi i}{3}}$ is a cube root of unity. (Recall here that $e^{i\theta} := \cos\theta + i\sin\theta$. Thus $e^{\frac{i\pi}{2}} = i$ and $\omega^3 = (e^{\frac{2\pi i}{3}})^3 = 1$. Similarly, $\omega^2 = e^{\frac{4\pi i}{3}}$.)

Everyone seemed to agree that Tommy's conjecture was plausible, so we left it as a challenge problem to think about over the weekend:

Challenge Problem 1. Prove that $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ are algebraically indistinguishable.