GALOIS THEORY: LECTURE 2

FEBRUARY 5, 2023

1. Algebraic Indistinguishability

Recall: Last time we showed that i and $-i$ are algebraically indistinguishable over $\mathbb{R}$, and that $\sqrt{2}$ and $-\sqrt{2}$ are algebraically indistinguishable over $\mathbb{Q}$. More generally, as you'll prove on your problem set, $a + bi$ and $a - bi$ are algebraically indistinguishable over $\mathbb{R}$ for any $a, b \in \mathbb{R}$, and $a + \sqrt{b}$ and $a - \sqrt{b}$ are algebraically indistinguishable over $\mathbb{Q}$ for all $a, b \in \mathbb{Q}$ such that $\sqrt{b} \notin \mathbb{Q}$. The former type of pair are called *complex conjugates*; the latter, *conjugates*. Is this a coincidence? Only time will tell.

Thus far we've seen pairs of algebraically indistinguishable numbers, but last time we conjectured the existence of a triple:

Proposition 1. *$\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ are algebraically indistinguishable over $\mathbb{Q}$, where $\omega = e^{2\pi i/3}$.*

Proof. Eli started us off by suggesting we begin with $f \in \mathbb{Q}[x]$ such that $f(\sqrt[3]{2}) = 0$. Jenna took the next step, suggesting we write

$$f(x) = a(x^3) + xb(x^3) + x^2c(x^3),$$

where $a, b, c \in \mathbb{Q}[x]$. We have

$$0 = f(\sqrt[3]{2}) = a(2) + b(2)\sqrt[3]{2} + c(2)\sqrt[3]{2}^2.$$

Since $a(2)$, $b(2)$, and $c(2)$ must all be rational, this equations forces

$$a(2) = b(2) = c(2) = 0.$$

Thus

$$f(\omega\sqrt[3]{2}) = a(2) + \omega\sqrt[3]{2}b(2) + \omega^2\sqrt[3]{2}^2c(2) = 0,$$

and similarly,

$$f(\omega\sqrt[3]{2}^2) = a(2) + \omega\sqrt[3]{2}^2b(2) + \omega^2\sqrt[3]{2}c(2) = 0.$$

We conclude that any such $f(x)$ that has $\sqrt[3]{2}$ as a root must also have $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, so these three complex numbers are all algebraically indistinguishable over $\mathbb{Q}$. □

Jenna pointed out that this doesn't exactly prove the proposition: we've only shown that if f has $\sqrt[3]{2}$ as a root, then the other cube roots of 2 must also be roots. To complete the proof, we'd have to further prove that if f has any one cube root of 2 as a root, then it must also have the other two. Fortunately, the proof is exactly the same!

Molly asked a good clarifying question: How do we know we can write $f(x)$ in the form $f(x) = a(x^3) + xb(x^3) + x^2c(x^3)$? Well, write $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \ldots$. We can group terms into three columns:

$$\begin{aligned} f(x) = a_0 &+ a_1x + a_2x^2 \\ +a_3x^3 &+ a_4x^4 + a_5x^5 \\ +a_6x^6 &+ a_7x^7 + a_8x^8 \\ &+ \cdots \end{aligned}$$

The terms in the first column all have x^n with $n \equiv 0 \pmod{3}$; since it's a polynomial in x^3, we can call this they form $a(x^3)$. Similarly, the second column is $xb(x^3)$, and the third column is $x^2c(x^3)$.

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

Tommy asked a fundamental question: how on earth did we deduce that $a(2) = b(2) = c(2) = 0$? Molly pointed out that this feels like linear algebra; Jamie built on that by saying it felt like linear independence. It's not quite linear algebra, though–rather than a linear combination of vectors, we have a linear combination of numbers. Here's the formal claim

Claim. If $\alpha + \beta\sqrt[3]{2} + \gamma(\sqrt[3]{2})^2 = 0$ with $\alpha, \beta, \gamma \in \mathbb{Q}$, then $\alpha = \beta = \gamma = 0$. $(1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ are "linearly independent" over $\mathbb{Q}$.)

You will prove this in Problem Set 1.

As we'll see, thinking about the behavior of numbers through the lens of linear algebra will be terrifically useful for us throughout the semester.

2. There is no quintic formula

We sketched—with lots of colors and hand-waving—Arnold's remarkable proof that there doesn't exist a quintic formula (aka the Abel-Ruffini theorem). See the course website for detailed notes on this proof.