GALOIS THEORY : LECTURE 1

LEO GOLDMAKHER

At its core, Galois theory is about how to define and describe numbers. To illustrate how difficult this can be, we start with a basic example.

Question 1. *What is the definition of the imaginary number i?*

We all know the answer.

Definition. i is the square-root of -1.

This is great, but there's one problem: this doesn't uniquely define i! Indeed, as Ian pointed out, both $\pm i$ are square-roots of -1. How does one distinguish between them?[1] (Note that, by definition, a definition of i should distinguish i from all other numbers.)

Let's think a bit more carefully about this. Secretly, we're defining i to be one of the solutions of

$$x^2 + 1 = 0,$$

and this doesn't allow us to distinguish i from $-i$, the other root. But maybe there's some nice function $f(x)$ which has i as a root but not $-i$? If this were the case, we could use f to distinguish between the two numbers. One immediate choice for such a function is $f(x) := x - i$, but this is clearly a bad candidate if the goal is to define i. This prompts us to refine our question.

Question 2. *Does there exist a function $f(x)$, built out of real numbers, such that $f(i) = 0$ but $f(-i) \neq 0$?*

This is quite general, and it's not clear how to approach it. To make it more tractable, let's simplify the question.

Question 3. *Does there exist a function $f(x) \in \mathbb{R}[x]$ such that $f(i) = 0$ but $f(-i) \neq 0$?*

Here $\mathbb{R}[x]$, read '$\mathbb{R}$ brackets x', denotes the set of all polynomials with coefficients in $\mathbb{R}$.

Will conjectured a negative answer to this question, and Grace offered a nice proof:

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

Grace's proof. Write

$$f(x) = a(x^2) + x \cdot b(x^2)$$

where $a, b \in \mathbb{R}[x]$. (In other words, we're splitting the terms of f into even powers of x and odd powers of x.) Then we have

$$0 = f(i) = a(-1) + b(-1)i.$$

Since $a(-1), b(-1) \in \mathbb{R}$, this implies $a(-1) = 0 = b(-1)$. But then

$$f(-i) = a(-1) - b(-1)i = 0. \qquad \square$$

This proof is short and sweet. But it turns out there's an even shorter one:

Andrew's proof. Note that $\overline{f(x)} = f(\overline{x})$, where $\overline{z}$ (read 'z bar') denotes complex conjugation. Thus

$$f(-i) = f(\overline{i}) = \overline{f(i)} = 0. \qquad \square$$

Date: January 31, 2018.

[1] Michael suggested defining i to be the ordered pair $(0, 1)$. This is really nice idea! We'll return to this point later in the semester.

In addition to brevity, this proof has one other advantage over the first proof: nowhere did we explicitly require that f be a polynomial. The only property we need is that $\overline{f(x)} = f(\overline{x})$, which does hold for polynomials (because complex conjugation 'commutes' with addition and multiplication) but also holds for f built out of other operations and functions which commute with complex conjugation. (See Problem **1.1** on the problem set.) Thus, Andrew's proof shows that i and $-i$ are indistinguishable with respect to many types of functions, not just polynomials.

The above is an illustration of the central idea of Galois theory, that some pairs of numbers are like two faces of a single coin: they're distinct, but you can't define one without simultaneously defining the other. Such pairs (or triples or quadruples...) of numbers are yoked together. Galois' observation is that the symmetries among such conjoined numbers tells you something about the way those numbers can (or can't) be described.

To be slightly more specific about what we mean when we talk about 'describing' a number, let's return to i. This is defined (up to $\pm$) to be the solution to $x^2 + 1 = 0$, an equation written in terms of previously defined numbers. This is a general phenomenon: we recursively define new numbers in terms of equations written using simpler numbers. Let's say the positive integers are the 'simplest' type of numbers. Then

- 0 is the solution to $x + 2 = 2$
- -2 is the solution to $x + 2 = 0$
- $3/17$ is the solution to $17x - 3 = 0$
- $\sqrt{2}$ as a solution (up to $\pm$) of $x^2 - 2 = 0$.

There's a funny pattern here. In each of the above, we introduce a notation which *defines* a solution in terms of the equation it solves. *This is very different from telling us what the solution actually is*! For example, all the notation $\sqrt{2}$ tells you is that when you square it, you get 2; it's telling you what the number *does*, as opposed to what it *is*. (For example, it doesn't tell you anything about how to approximate the number.) This is sort of like defining a car by saying 'it takes you from one place to another'. Great, but what *is* a car?

Let's consider $\sqrt{2}$ more carefully. It's defined to be the positive solution to $x^2 - 2 = 0$. But suppose we forget about the notion of ordering the reals. Can we *algebraically* distinguish between $\sqrt{2}$ and $-\sqrt{2}$? In other words, can we find some polynomial (expressed in terms of simpler numbers) which distinguishes between the two? Of course, this is highly reminiscent of our discussion of i above. But this time, it turns out that Grace's proof (which didn't generalize nicely to non-polynomial functions f) is the proof which works best:

Proposition 2. *If $f \in \mathbb{Q}[x]$ and $f(\sqrt{2}) = 0$, then $f(-\sqrt{2}) = 0$.*

Proof. Write

$$f(x) = a(x^2) + x \cdot b(x^2)$$

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

$$0 = f(\sqrt{2}) = a(2) + b(2)\sqrt{2}.$$

Ben and Grace observed that this implies $a(2) = 0 = b(2)$, since $a(2), b(2) \in \mathbb{Q}$, while $\sqrt{2} \notin \mathbb{Q}$. But then

$$f(-\sqrt{2}) = a(2) - b(2)\sqrt{2} = 0. \qquad \square$$

This shows that $\pm\sqrt{2}$ are algebraically indistinguishable; one needs some additional information about the structure of $\mathbb{R}$ (e.g. a notion of order) to separate them.

More generally, it turns out that if $a, b \in \mathbb{Q}$ and $\sqrt{b} \notin \mathbb{Q}$, then the two numbers $a \pm \sqrt{b}$ are algebraically indistinguishable (see problem **1.2**). Recall (from high school?) that these two numbers are called *conjugates*, so the quick way to say this is 'conjugates are algebraically indistinguishable'. Complex conjugates are also algebraically indistinguishable (see problem **1.3**). Is the appearance of the word 'conjugate' in both contexts a coincidence? Only time will tell.

Let's see whether we can generalize this to other numbers. How about $\sqrt[3]{2}$? What numbers are algebraically indistinguishable from it? Beatrix and Wyatt made the following guess:

Proposition 3. *Let $\omega := e^{2\pi i/3}$ be a third root of unity. The three numbers $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ are algebraically indistinguishable.*

Proof. Suppose $f \in \mathbb{Q}[x]$ has $\sqrt[3]{2}$ as a root; our goal is to prove that the other two numbers in the statement are also roots of f. In view of the clear similarity to Proposition 2, we proceed by modifying its proof.

Write

$$f(x) = a(x^3) + x \cdot b(x^3) + x^2 \cdot c(x^3),$$

where $a, b, c \in \mathbb{Q}[x]$. If $f(\sqrt[3]{2}) = 0$ then

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

whence $a(2) = b(2) = c(2) = 0$. But then

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

and similarly $f(\omega^2\sqrt[3]{2}) = 0$. □

There's one major subtlety in this proof: how did we deduce that $a(2) = b(2) = c(2) = 0$? This step is significantly harder than the corresponding step in the proof of Proposition 2, which was an immediate consequence of knowing that $\sqrt{2} \notin \mathbb{Q}$. Let's highlight what this step is really saying:

Claim. *If $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 = 0$ for some $a, b, c \in \mathbb{Q}$, then $a = b = c = 0$.*

Will noticed that this bears more than a passing resemblance to the notion of linear independence – we can rephrase the claim as saying that the three numbers $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ are linearly independent over $\mathbb{Q}$. This point of view will play an important role later in the course, allowing us to bring all the tools from linear algebra to bear on this and similar problems. In the meantime, we can make do with pure thought; see problem **1.4**.

Thus we see that the proof technique introduced by Grace to prove the $\pm i$ are indistinguishable works beautifully to prove the analogous statement for $\sqrt{2}$, but is more complicated when used to prove the analogous statement for $\sqrt[3]{2}$. The method really breaks down when you apply it to $\sqrt[4]{2}$. (Try it!) Is there a different proof which generalizes more easily? We'll return to this question a few lectures from now.