GALOIS THEORY: LECTURE 13

LEO GOLDMAKHER

1. Exploring Field Extensions

Recall one of our motivating questions for the course: given a function $f \in \mathbb{Q}[t]$, what do its roots look like? How can we describe them? One of the big tools we introduced in the first half of the course was Kronecker's Theorem, which produces a field extension $K/\mathbb{Q}$ and a root of f in K.

Question 1. *Does the field extension $K = \mathbb{Q}[t]/(f)$ from Kronecker's Theorem contain <u>all</u> roots of f?*

Eli noted that we should assume that f is irreducible as we did in Kronecker's Theorem, since we can only mod out by an irreducible and therefore in the best case scenario could only find the roots of a single irreducible component by applying Kronecker.

Michael suggested the counterexample $f(t) = t^3 - 2$. It is irreducible by Eisenstein's criterion, and we know that its roots are the cube roots of 2: $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where $\omega = e^{2\pi i/3}$. Kronecker's Theorem produces the field $\mathbb{Q}[t]/(t^3-2) \simeq \mathbb{Q}(\sqrt[3]{2})$. But note that $\mathbb{Q}(\sqrt[3]{2})$ doesn't contain $\omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$, since these are complex numbers and $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of $\mathbb{R}$. Thus, Kronecker's Theorem is not enough to generate all of the roots of our polynomial.

One curious point is that we have alternative (equally good) interpretations of the field $\mathbb{Q}[t]/(t^3-2)$ given by Kronecker's theorem: rather than $\mathbb{Q}[t]/(t^3-2) \simeq \mathbb{Q}(\sqrt[3]{2})$, we could have said $\mathbb{Q}[t]/(t^3-2) \simeq \mathbb{Q}(\omega\sqrt[3]{2})$ or $\mathbb{Q}[t]/(t^3-2) \simeq \mathbb{Q}(\omega^2\sqrt[3]{2})$. In each of these cases, however, the field produced contains precisely one of the cube roots of 2. This motivates:

Question 2. *What is the smallest field containing all the cube roots of 2?*

Ian observed that, by definition, $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is the smallest field containing all three roots. However, this field can be rewritten in a more informative way. Will conjectured the following:

Proposition 1.1. *$\mathbb{Q}(\omega, \sqrt[3]{2})$ is the smallest field containing all cube roots of 2.*

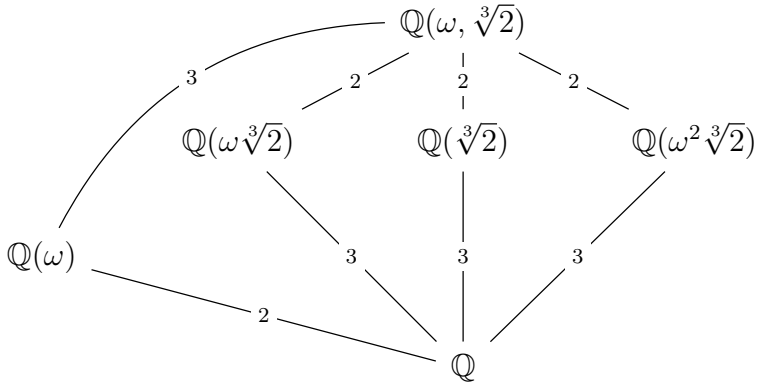
Proof. Implicit in this proposition are two claims: first, that this field contains all the roots, and second, that it is the smallest such field. The proof of the first claim is clear: since it is a field, we can multiply the generators ω and $\sqrt[3]{2}$ as needed to produce the roots $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$.

To prove the second claim, suppose that some field K contains all three cube roots. Then, since K is a field, we have $K \ni \frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} = \omega$. Also, by hypothesis $K \ni \sqrt[3]{2}$. Thus, any field containing all three cube roots of 2 also contains $\mathbb{Q}(\omega, \sqrt[3]{2})$, implying that $\mathbb{Q}(\omega, \sqrt[3]{2})$ is the smallest such field. □

Date: April 5, 2018.

Based on notes by Andrew Aramini.

The field $\mathbb{Q}(\sqrt[3]{2})$ we constructed using Kronecker's theorem lies strictly in between $\mathbb{Q}$ and $\mathbb{Q}(\omega, \sqrt[3]{2})$. We also came up with some other intermediate fields:



We know immediately there are three intermediate fields obtained by adjoining each of the three cube roots of 2 to the rationals. For each of these, the minimal polynomial over $\mathbb{Q}$ is $t^3 - 2$, so the degree of each of these extensions over $\mathbb{Q}$ is 3, as indicated in the diagram above.

To extend from $\mathbb{Q}(\sqrt[3]{2})$ all the way up to $\mathbb{Q}(\omega, \sqrt[3]{2})$, we need to adjoin ω, which is an extension of degree at least 2 since ω is complex and hence doesn't live in $\mathbb{Q}(\sqrt[3]{2})$. On the other hand, ω has degree at most 2 over $\mathbb{Q}(\sqrt[3]{2})$, since we know it has degree 2 over $\mathbb{Q}$. Thus, we conclude that $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, as indicated in the diagram. The Tower Law implies

$$[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6.$$

From this, we can use the Tower Law again to deduce that

$$[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\omega\sqrt[3]{2})] = 2 = [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\omega^2\sqrt[3]{2})] \qquad \text{and} \qquad [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\omega)] = 3$$

as indicated in the diagram. Note that $\mathbb{Q}(\omega)$ is positioned below the other three intermediate fields, because it's only a quadratic extension from $\mathbb{Q}$, whereas the others are cubic extensions.

At first glance, one might wonder whether there are any redundancies in this diagram. You will prove on your problem set that all the fields appearing in the diagram are distinct. Another natural question is: are there any intermediate fields missing from the diagram? For example, $\mathbb{Q}(\omega^2)$ doesn't appear. A bit of thought shows that $\mathbb{Q}(\omega^2) = \mathbb{Q}(\omega)$, so in fact this field is already listed in the diagram. However, it's surprisingly challenging to prove that there are no intermediate fields apart from those listed; you will tackle this on your problem set.

2. Galois' Idea

We now describe Galois' key idea (albeit in modern language). Given a polynomial $f \in \mathbb{Q}[t]$, we start by zooming out to the smallest field containing all the roots of f, or equivalently, the smallest field over which f splits into linear factors. We formalize this notion:

Definition. Given a polynomial $f \in K[t]$, the *splitting field* L/K is the smallest field containing all the roots of f.

Remark. Despite our use of the definite article, it's not obvious that the splitting field is unique. It turns out that it is, up to isomorphism.

Example 1. Our work above shows that $\mathbb{Q}(\omega, \sqrt[3]{2})$ is the splitting field of $t^3 - 2$.

The next step in Galois' program is to associate to this splitting field a nice group which captures properties of the field (and hence, of the polynomial we started with). This leads us to a general question:

Question 3. *How can we associate a group to a given field K?*

Idea 1 (Jonah) K itself under $+$ forms a group.

Idea 2 (Anya) $\mathrm{Aut}(K)$, the set of all automorphisms of K (i.e. all isomorphisms $K \xrightarrow{\sim} K$), forms a group under composition.

Idea 3 (Chetan): Given $[K : \mathbb{Q}] = n$, we can associate the group S_n to the field K.

Of these, the second idea is the most promising. Here's why. The first idea leaves too much information – pretending that you don't know how to multiply doesn't really give you a new perspective on the structure of K. The third idea, by contrast, strips away too much information – it's a way of associating a meaningful number to K, but the structure of S_n doesn't take K into account beyond the information already given by the number n. The second idea, by contrast, creates a group which measures something nontrivial about K (the different ways it can be rewritten), but is far simpler than K itself. Among other things, while K is usually an infinite set in practice, $\mathrm{Aut}(K)$ is a usually a finite set (we'll see an example shortly). Thus, the automorphism group strips away a lot of the complications of the given field, but still preserves some interesting information.

To build up our intuition, we consider a few examples.

Example 2. $\mathrm{Aut}(\mathbb{Q})$ is the trivial group.

This was conjectured by Beatrix. Indeed, suppose $\sigma : \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}$; we wish to show that it must be the identity map. Note that

$$\sigma(0) = \sigma(0 + 0) = \sigma(0) + \sigma(0),$$

whence $\sigma(0) = 0$. Next, $\sigma(1)^2 = \sigma(1)$ implies that $\sigma(1) = 0$ or 1; since σ is a bijection and $\sigma(0) = 0$, we deduce that $\sigma(1) = 1$. Inspired by a nice observation by Emily, Michael noted that $\sigma(-1) = -1$, since

$$0 = \sigma(0) = \sigma(1 - 1) = \sigma(1) + \sigma(-1) = 1 + \sigma(-1).$$

Grace gave an alternative argument:

$$\sigma(-1)^2 = \sigma(1) = 1$$

implies that $\sigma(-1) = \pm 1$, but σ is a bijection and we've already assigned the value 1 to $\sigma(1)$.

Putting this all together shows that $\sigma(n) = n$ for $n = 0, \pm 1$. Since σ preserves addition, we immediately deduce that $\sigma(n) = n$ for all integers n. Finally, since σ preserves multiplication, we find that for any nonzero n,

$$\sigma(1/n)\sigma(n) = \sigma(1),$$

whence $\sigma(1/n) = 1/n$. We conclude that $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbb{Q}$. In other words, σ is the identity map. Since it was an arbitrary element of $\mathrm{Aut}(\mathbb{Q})$, we deduce that this group must be trivial.

Example 3. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$ is also trivial.

This was conjectured and proved by Anya. Indeed, pick any $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$. The same argument presented in the last example shows that $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbb{Q}$. Where does σ send $\sqrt[3]{2}$? Anya noted that

$$\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2$$

Thus, $\sigma(\sqrt[3]{2})$ must be a cube root of 2. However, the two complex cube roots of 2 are not elements of $\mathbb{Q}(\sqrt[3]{2})$, so we deduce that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Since σ is determined by where it sends rationals and $\sqrt[3]{2}$, we conclude that σ is the identity map, and hence, that $\mathrm{Aut}(\sqrt[3]{2})$ is the trivial group.

However, not all automorphism groups are trivial.

Example 4. $\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})) \simeq S_3$.

For brevity, set $K := \mathbb{Q}(\omega, \sqrt[3]{2})$. Pick any $\sigma \in \mathrm{Aut}(K)$. Once again, $\sigma(\alpha) = \alpha$ for every $\alpha \in \mathbb{Q}$, so it remains to determine where σ sends ω and $\sqrt[3]{2}$. By the same argument as in the previous example, we know that $\sigma(\sqrt[3]{2})$ must a cube root of 2, but now all three cube roots live in K. Similarly, ω must be sent to a third root of unity. Thus, our options are

$$\sqrt[3]{2} \longmapsto \sqrt[3]{2},\ \omega\sqrt[3]{2},\ \text{or}\ \omega^2\sqrt[3]{2}$$

$$\omega \longmapsto \omega,\ \omega^2,\ \text{or}\ 1.$$

But σ is a bijection, and we already have $\sigma(1) = 1$, so really we can only have $\sigma(\omega) = \omega$ or ω^2. Thus, there are six possible choices we can make for σ.

We can describe all these choices in terms of two particularly nice automorphisms: one which leaves $\sqrt[3]{2}$ fixed, and the other which leave ω fixed. More precisely, we define $r, f \in \mathrm{Aut}(K)$ by

$$r(\sqrt[3]{2}) = \sqrt[3]{2} \qquad f(\sqrt[3]{2}) = \omega\sqrt[3]{2}$$
$$r(\omega) = \omega^2 \qquad f(\omega) = \omega$$

We observed that r has order 2, f has order 3, and $fr = rf^2$. This implies

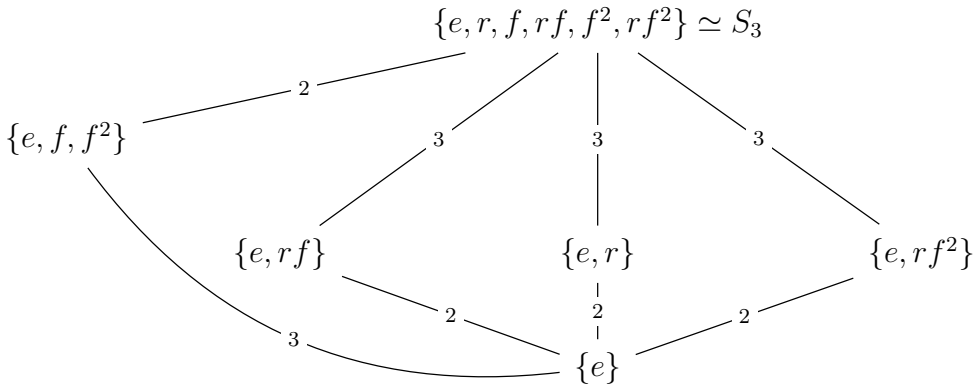
$$\mathrm{Aut}(K) = \{e, r, f, rf, f^2, rf^2\},$$

which is the dihedral group of order 6. This in turn is isomorphic to the symmetric group S_3.

Remark. We've secretly proved that the Galois group of $t^3 - 2$ is S_3. But we postpone giving a formal definition of the Galois group to next lecture, and instead explore a remarkable discovery.

3. The Galois correspondence

We've just associated the group S_3 to the field $\mathbb{Q}(\omega, \sqrt[3]{2})$. Recall that earlier in the class we drew a diagram of all the subfields of $\mathbb{Q}(\omega, \sqrt[3]{2})$. Now we draw a diagram of all subgroups of S_3:



Amazingly, this has the *exact* same structure as our earlier field diagram – just upside down! Note that here we mark each edge with the index of one group inside the one it's connected to.

To recap: we began with a polynomial, found its splitting field K, determined the automorphism group $\mathrm{Aut}(K)$, and discovered a remarkable correspondence between the diagram of all subfields of K and all subgroups of $\mathrm{Aut}(K)$. In fact, there are even more parallels hidden in these diagrams than meets the eye. This is the subject of the Fundamental Theorem of Galois Theory, which we take up next lecture.