GALOIS THEORY : LECTURE 9

LEO GOLDMAKHER

1. KRONECKER'S THEOREM, REVISITED

Recall Kronecker's Theorem:

Theorem 1 (Kronecker, 1882)**.** *Given $f \in K[t]$ a non-constant polynomial, where K is a field. Then there exists L/K in which f has a root.*

This is all well and good, but why does this theorem matter? Sure, $[t] \in L = K[t]/(f)$ is always a root of f, but this doesn't really *tell us* anything about the root of f – it's just formalism!

To explain this, we return to the familiar example of $f(x) = x^2 + 1$. When considered over $\mathbb{R}$, we're comfortable with the solution: we "zoom out" to $\mathbb{C}$, where we have the root i. But what does this symbol tell you about the solution? Absolutely nothing – we just invented a new notation. But this simple new symbol allows us to reduce many other equations to this one, and has led to numerous breakthroughs in mathematics and physics.

Similarly, Kronecker's theorem allows us to introduce and study new numbers in less familiar settings. For example, consider f as a polynomial in $\mathbb{F}_3$. It's easy to verify that we cannot find a root of f in $\mathbb{F}_3$, so we would need to zoom out to do so. The most natural guess of where to zoom out to is $\mathbb{C}$, since we know that $i \in \mathbb{C}$ is a root of f... but this doesn't work, because the characteristics of $\mathbb{F}_3$ and $\mathbb{C}$ don't match up. Kronecker's theorem tells us where to zoom out to: the field $\mathbb{F}_3[t]/(t^2+1) = \{[at+b] : a, b \in \mathbb{F}_3\}$. Note that this field has precisely nine elements. These elements look like polynomials, but I urge you to think of them as numbers – just as in $\mathbb{C}$, numbers have the form $a + bi$, which would look like linear polynomials to anyone unfamiliar with the concept of i. From Kronecker's proof we know that one of these nine numbers (the one called $[t]$) is a root of f.

The question arose of what would happen if f were reducible. We will explore this in an upcoming lecture, but the short answer is that we can write f as a product of irreducibles and then repeatedly mod out by them one at a time.

2. FLIPPING KRONECKER'S THEOREM

When working with Kronecker's theorem, we are given a field K and a polynomial $f \in K[t]$. Then, we construct an extension $K[t]/(f)$ and a number $\alpha \in K[t]/(f)$ such that $f(\alpha) = 0$. Let's flip this idea on its head: starting with a field extension L/K and some $\alpha \in L$, can we find some polynomial $f \in K[t]$ such that $K[t]/(f) \simeq K(\alpha)$? In other words, we know that α lives in *some* extension of K, and we want to find the smallest such extension; is it true that this smallest extension is of the form $K[t]/(f)$ for some $f \in K[t]$?

We first looked at an example. Consider $\mathbb{C}/\mathbb{Q}$, and $\alpha = \sqrt{2}$. Can we find some polynomial f such that $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[t]/(f)$? Sure, no problem: $f(t) = t^2 - 2$. We know by Kronecker that $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[t]/(t^2-2)$, and then we proved that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$. Note that in this case we were lucky, in that we had a major clue about how to choose the polynomial f. What about in a more general setting? How do we find an $f \in K[t]$ such that $K[t]/(f) \simeq K(\alpha)$?

In practice, we've observed that usually this breaks down into two stages: first we prove that $K[t]/(f) \simeq K[\alpha]$, and then give a separate argument showing that $K[\alpha] = K(\alpha)$. So let's focus on the less ambitious goal of finding an f such that

$$K[t]/(f) \simeq K[\alpha].$$

Date: March 1, 2018.

Based on notes by Ben Logsdon.

Right away we noticed something nice: this looks a lot like the First Isomorphism Theorem for rings! Let's recall what this says:

Theorem 2 (1st isomorphism theorem)**.** *For any ring R and any ring homomorphism $\phi : R \to S$,*

$$R/\ker \phi \simeq \text{im } \phi.$$

(As a side note, this theorem is meant to be intuitive. Modding R by $\ker \phi$ squashes everything in $\ker \phi$ into 0. Similarly, ϕ sends everything in $\ker \phi$ to 0, and sends all the elements in translations of $\ker \phi$ to translations of 0.)

Having observed the strong resemblance, we try to apply the First Isomorphism Theorem to our situation. For this to work, we need to set

$$R := K[t] \qquad \text{and} \qquad \text{im } \phi := K[\alpha].$$

Thus, we may as well choose S to be $K[\alpha]$. We are thus led to trying to construct some ring homomorphism $\phi : K[t] \to K[\alpha]$. Where do we send $f \in K[t]$? There's only one possible place: we send f to $f(\alpha)$. This is called the *evaluation map*. Formally, we've defined ϕ by

$$\phi(f) := f(\alpha).$$

Note that im $\phi = K[\alpha]$, since any polynomial in α is the image of the same polynomial with all the α's replaced by t. Thus, by the 1st isomorphism theorem, we have

$$K[t]/\ker \phi \simeq K[\alpha].$$

Note that the kernel is the set of all polynomials in $K[t]$ that have α as a root:

$$\ker \phi = \{f \in K[t] : f(\alpha) = 0\}.$$

What else can we say about the kernel?

Recall that $\ker \phi$ is an ideal of $K[t]$. Moreover, $K[t]$ is a principal ideal domain, so $\ker \phi$ is generated by a single polynomial; let's call this polynomial m_α. In other words, $\ker \phi = (m_\alpha)$ and $K[t]/(m_\alpha) \simeq K[\alpha]$. We're now very close to what we want – what we'd really like is for $K[\alpha]$ to be a field. How can we prove this? Well, we know that if (m_α) is a maximal ideal – in other words, if m_α is irreducible over K – then $K[t]/(m_\alpha)$ is a field. It therefore suffices to show that m_α is irreducible, and we'll be done!

Suppose that $m_\alpha = gh$ for some $g, h \in K[t]$. Since $m_\alpha(\alpha) = 0$, either $g(\alpha) = 0$ or $h(\alpha) = 0$. Without loss of generality, assume that $g(\alpha) = 0$. Recall that $(m_\alpha) = \ker \phi$, which is the set of polynomials in $K[t]$ which have α as a root. In particular, we must have $g \in (m_\alpha)$, or in other words, $m_\alpha \mid g$. But we also have $g \mid m_\alpha$! This gives $\deg m_\alpha \leq \deg g \leq \deg m_\alpha$, whence $\deg m_\alpha = \deg g$. This proves that h is a unit, so we conclude that m_α is indeed irreducible. We summarize our results:

Thrilling Theorem 1. *Given $\alpha \in L/K$, there exists an $m_\alpha \in K[t]$ such that m_α is irreducible over K, $m_\alpha(\alpha) = 0$, and $K[t]/(m_\alpha) \simeq K(\alpha)$.*

Proof. From above we have $K[t]/(m_\alpha) \simeq K[\alpha]$. Thus, it suffices to show that $K[\alpha] = K(\alpha)$. To this end, note that $K[\alpha] \subseteq K(\alpha)$. Furthermore, by definition, $K(\alpha)$ is the smallest field containing K and α. But from Kronecker's theorem, we know that $K[\alpha]$ is a field containing K and the element α, so it must also contain $K(\alpha)$! Thus, $K[\alpha] = K(\alpha)$. □

We quickly realized, however, that something is amiss: Ian noted that π isn't the root of any polynomial in $\mathbb{Q}[t]$. (This is not at all obvious – there's a proof in the textbook.) Something in our proof must be wrong! But what?

Recall that we asserted that $\ker \phi$ must be principal, and therefore can be written in the form (m_α). The rest of the proof is fine if m_α is nonzero, but we neglected the possibility that $m_\alpha = 0$. Note that this really is a polynomial with α as a root.

So, our Thrilling Theorem above isn't quite right; it handles the case when α is the root of some polynomial in $K[t]$, but ignores the possibility that no such polynomial exists. To make this easier to discuss, we label these scenarios:

Definition. If $\alpha \in L/K$ doesn't satisfy any equation of the form $f(\alpha) = 0$ with $f \in K[t]$, we say α is *transcendental* over K. Otherwise, we say that α is *algebraic* over K.

For example, $\sqrt{2}$ is algebraic over $\mathbb{Q}$, as it is the root if $t^2 - 2$. It is also algebraic over $\mathbb{R}$, as it is the root of $t - \sqrt{2}$. By contrast, π is transcendental over $\mathbb{Q}$ (a fact that is difficult to prove!) but algebraic over $\mathbb{R}$ (it is the root of $t - \pi$). Note that numbers are transcendental or algebraic *over particular fields*, and the same number can be transcendental over one field and algebraic over another.

Now that we have distinguished between algebraic and transcendental numbers, we can state the reverse of Kronecker's theorem correctly.

Thrilling Theorem 2 (Legit version)**.** *Given $\alpha \in L/K$.*

(1) If α is algebraic over K, then there exists some $m_\alpha \in K[t]$ irreducible such that $m_\alpha(\alpha) = 0$, $K[t]/(m_\alpha) \simeq K(\alpha)$, and $K[\alpha] = K(\alpha)$.

(2) If α is transcendental over K, then $K[t] \simeq K[\alpha]$.

Note that there are multiple choices of m_α, since we can multiply by a unit to get a different choice. We call the choice of m_α which is monic the *minimal polynomial of α over K*.

We observed that this theorem proves some known results quickly, e.g. $\mathbb{Q}(i) = \mathbb{Q}[i]$ and $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$.

3. The Degree of a Field Extension

We finished the lecture by considering two familiar field extensions: $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt[3]{2})$. Which is bigger?

This is a silly question, of course: from the point of view of cardinality, they have the same size (they're both countable). But observe that $\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ and $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c, \in \mathbb{Q}\}$. The latter feels like a larger extension of $\mathbb{Q}$, since we're taking linear combinations of more things. This reminds us of an approach to measuring size from linear algebra: dimension. In fact, these two field extensions are vector spaces over $\mathbb{Q}$, with bases $\{1, i\}$ and $\{a, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$, respectively. This leads to another definition:

Definition. The *degree* of a field extension L/K, denoted $[L : K]$, is the dimension of L when viewed as a vector space over K.

So, for the two previous examples, we have $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. We will discuss the notion of degree more next lecture.