GALOIS THEORY: LECTURE 10

MARCH 4, 2024

1. A THRILLING THEOREM

Recall that last class we took up a kind of reverse Kronecker: given $\alpha \in L/K$, can we find $f \in K[t]$ such that $K[t]/\langle f \rangle \simeq K(\alpha)$? Our main idea was to use the first isomorphism theorem for rings (given ϕ a ring homomorphism out of R, we have $R/\ker \phi \simeq \text{im } \phi$). Following Tate's suggestion, we take $\phi : K[t] \to K(\alpha)$ defined by $f \mapsto f(\alpha)$; 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:

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

Since every ideal in $K[t]$ is principal, we know ker $(\phi) = \langle m_\alpha \rangle$ for some polynomial $m_\alpha \in K[t]$. Thus,

$$K[t]/\langle m_a \rangle \simeq K[\alpha].$$

Recall that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}(i) = \mathbb{Q}[i]$; these examples suggest that $K[\alpha] = K(\alpha)$ more generally. This all makes plausible the following:

Thrilling Theorem 1. *Given $\alpha \in L/K$, there exists $m_\alpha \in K[t]$ such that $K[t]/\langle m_a \rangle \simeq K(\alpha)$. Moreover,*

(i) *m_α is irreducible and*
(ii) *m_α has α as a root.*

Proof. There are three claims being made; our discussion led us to prove them in reverse order. First, Noah pointed out that since m_α generates ker ϕ, and the latter consists of all polynomials in $K[t]$ that vanish at α, we must have $m_\alpha(\alpha) = 0$. This proves claim (ii).

Next, Jake and Felix proposed the following argument to prove that m_α is irreducible. Suppose that $m_\alpha = gh$ for some polynomials $g, h \in K[t]$. Thus $0 = m_\alpha(\alpha) = g(\alpha)h(\alpha)$, so either $g(\alpha) = 0$ or $h(\alpha) = 0$. Without loss of generality say $g(\alpha) = 0$, whence $g \in \ker(\phi) = \langle m_\alpha \rangle$; it follows that $m_\alpha \mid g$, which implies $\deg m_\alpha \leq \deg g$. On the other hand, by definition of g, we have $\deg g \leq \deg m_\alpha$. Thus $\deg g = \deg m_\alpha$, whence h is a unit. We deduce that m_α must be irreducible over K.

Finally, recall that we know $K[t]/\langle m_\alpha \rangle \simeq K[\alpha]$, so it suffices to prove $K[\alpha] = K(\alpha)$. Jenna noted that since m_α is irreducible over K, the ideal $\langle m_\alpha \rangle$ is maximal, whence $K[t]/\langle m_\alpha \rangle$ is a field. Thus $K[\alpha]$ is a field, which implies that $K[\alpha] = K(\alpha)$. □

We quickly realized that something is amiss: Tate observed that π isn't the root of any polynomial in $\mathbb{Q}[t]$. (This is not at all obvious, and we'll discuss it below.) Something in our proof must be wrong! But what?

After some discussion, Zoe figured out the issue. Recall that we asserted that ker ϕ must be principal, and therefore can be written in the form $\langle m_\alpha \rangle$. The rest of the proof is fine if m_α is nonzero, but, as Zoe pointed out, 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 nontrivial polynomial exists. To make this easier to discuss, we label these scenarios:

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

Definition. Given $\alpha \in L/K$ we say α is **algebraic** over K iff there exists a non-constant $f \in K[t]$ such that $f(\alpha) = 0$. Otherwise we say α is **transcendental** 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 $\alpha \in L/K$.*

- *If α is algebraic over K, then there exists some $m_\alpha \in K[t]$, irreducible over K, such that $m_\alpha(\alpha) = 0$, $K[t]/\langle m_\alpha \rangle \simeq K(\alpha)$, and $K[\alpha] = K(\alpha)$.*
- *If α is transcendental over K, then $K[t] \simeq K[\alpha]$; in particular, $K(\alpha) \simeq K(t)$.*

Colloquially, the second part of the theorem asserts that from the point of view of K, α is indistinguishable from an indeterminate.

1.1. **Transcendence of π and e.** It's known that e and π are both irrational; moreover, both e and π are transcendental. At the heart of both proofs is the following result:

Theorem 1 (Hermite-Lindemann-Weierstrass)**.** *If $\alpha_1, \ldots, \alpha_n$ are algebraic over $\mathbb{Q}$ and linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$, meaning there are no nontrivial polynomial relations among them.*

Corollary 2. *e is transcendental over $\mathbb{Q}$.*

Proof. Take $n = 1$ and $\alpha_1 = 1$. □

Corollary 3. *π is transcendental over $\mathbb{Q}$.*

Proof. If π were algebraic over $\mathbb{Q}$ then $i\pi$ would also be algebraic over $\mathbb{Q}$ (see your problem set). But then Hermite-Lindemann-Weierstrass would imply that $e^{i\pi}$ is algebraically independent over $\mathbb{Q}$, a clear contradiction. □

Remarkably, it remains unknown whether $e + \pi$ or $e\pi$ are irrational, much less transcendental! However:

Corollary 4. *At least one of $e + \pi$ or $e\pi$ is irrational.*

Proof. If both were rational, then $x^2 - (e + \pi)x + e\pi = (x - e)(x - \pi)$ would have rational coefficients, contradicting that e is transcendental. □

2. The degree of an extension

We finished the lecture by considering two familiar field extensions: $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$. Which is bigger? Needless to say, this is a silly question: from the point of view of cardinality, they have the same size (they're both countable). But observe that

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \qquad \text{and} \qquad \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c, \in \mathbb{Q}\}.$$

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 $\{1, \sqrt{2}\}$ and $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$, 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 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Noah clarified our definition by pointing out that vectors are elements of L, while scalars are elements of K. How do we multiply a scalar (an element $k \in K$) by a vector (an element $x \in L$)? We can't multiply them directly, since k might not live inside of L. However, by definition of field extension, there's an embedding $\varphi : K \hookrightarrow L$, so that we have an isomorphic copy of K sitting inside L. This provides a natural way to define how to multiply $x \in L$ by the scalar $k \in K$:

$$kx := \varphi(k)x.$$

To solidify our intuition for the degree of a field extension, we considered a couple examples.

Example 1. $[\mathbb{C} : \mathbb{R}] = 2$

To determine the degree of this extension, we notice that $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. This suggests that the set $\{1, i\}$ forms a basis for $\mathbb{C}$. It is clear from how we described $\mathbb{C}$ that $\{1, i\}$ spans $\mathbb{C}$. Furthermore, 1 and i are linearly independent over $\mathbb{R}$. Thus $\{1, i\}$ forms a basis for the space, so the dimension of $\mathbb{C}$ as a vector space over $\mathbb{R}$ is 2.

Example 2. $[\mathbb{R} : \mathbb{Q}] = \infty$

This extension presents a greater challenge than the previous one. Carlos, Zoe, and Jamie all proposed ideas for how to prove this. Perhaps the simplest was that $\mathbb{Q}$ is countable, so the $\mathbb{Q}$-linear combinations of any finite set can only span countably many elements of $\mathbb{R}$.