GALOIS THEORY: LECTURE 9

FEBRUARY 29, 2024

1. FINISHING UP IRREDUCIBILITY

Last time we discussed a number of irreducibility tests. We didn't end up proving Eisenstein's criterion in class, so I wrote up the proof in the Lecture 8 summary. Also, I didn't write down Perron's test quite right in class—the corrected version is in the Lecture 8 summary.

One final irreducibility test I wanted to mention connects irreducible polynomials to prime numbers more concretely. Consider a prime number, say, 4721. There's a natural way to associate a polynomial to this number: $4x^3 + 7x^2 + 2x + 1$. It turns out that this polynomial is irreducible over $\mathbb{Q}$. Does this always happen? A result of Arthur Cohn shows that the answer is yes!

Proposition 1 (Cohn's irreducibility criterion)**.** *Suppose $f \in \mathbb{Z}[x]$ has all of its coefficients in $\{0, 1, 2, 3, \ldots, 9\}$, and that $f(10)$ is prime. Then f is irreducible over $\mathbb{Q}$.*

One can imagine many ways to generalize this, and some of these have been proved. Tommy asked about bases other than 10. Here's what's known:

Proposition 2 (Brillhart-Filaseta-Odlyzko, 1981)**.** *Fix an integer $b \geq 2$, and suppose $f \in \mathbb{Z}[x]$ has all of its coefficients in $\{0, 1, 2, \ldots, b-1\}$ and that $f(b)$ is prime. Then f is irreducible over $\mathbb{Q}$.*

Example 1. Cohn's criterion allows one to construct an irreducible polynomial out of a given prime. By contrast, Brillhart-Filaseta-Odlyzko allows one to construct *many* irreducible polynomials from a single prime. Here's an example given in their original paper. We can expand the prime number 397 base 2, 3, etc., each of which gives a different irreducible polynomial:

base	**expansion of** 397	**corresponding polynomial**
2	110001101	$x^8 + x^7 + x^3 + x^2 + 1$
3	112201	$x^5 + x^4 + 2x^3 + 2x^2 + 1$
4	12031	$x^4 + 2x^3 + 3x + 1$
5	3042	$3x^3 + 4x + 2$
6	1501	$x^3 + 5x^2 + 1$
7	1105	$x^3 + x^2 + 5$
8	615	$6x^2 + x + 5$

A different line of generalization is the following:

Proposition 3 (Filaseta-Gross, 2014)**.** *Suppose $f \in \mathbb{N}[x]$ (where $\mathbb{N}$ consists of all non-negative integers) and that $f(10)$ is prime. If $\deg f \leq 31$, then f is irreducible over $\mathbb{Q}$. Moreover, if $\deg f = 32$ and all the coefficients of f are $\leq 10^{31}$, then f is irreducible over $\mathbb{Q}$.*

2. NOTATION

We next discussed some notations.

- **Field Extensions.** There are two common notations for field extensions. The better one is $\begin{smallmatrix} L \\ | \\ K \end{smallmatrix}$. Unfortunately, this is typographically challenging, so most people end up using the simpler notation L/K. This has an obvious drawback: it looks like a quotient of L by K. In principle this is unambiguous,

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

since K is not an ideal of L (unless $L = K$); in practice, of course, this can be confusing. Just keep in mind that when you see the symbol A/B, if A and B are both fields, then this is a field extension, whereas if A is a group or a ring, then this is a quotient.

- **Polynomial rings.** We've discussed this: given a field K, we denote the collection of all polynomials with coefficients in K by $K[x]$ or $K[t]$ (depending on which variable we use).
- **Adjoining an element.** We've seen this as well: given two fields $K \subseteq L$ and $\alpha \in L$, we can construct an intermediate field "K adjoin α", denoted $K(\alpha)$, by setting it to be the smallest subfield of L containing both K and α. More formally,

$$K(\alpha) := \bigcap_{\substack{K \subseteq F \subseteq L \\ \text{s.t. } \alpha \in F}} F.$$

- **Rational functions.** Given the above notations, what might $K(x)$ mean? Tommy proposed that it should be the smallest field containing K and the formal variable x; in plainer terms,

$$K(x) := \left\{ \frac{f}{g} : f, g \in K[x], g \neq 0 \right\}.$$

  This is called the field of rational functions.
- **Polynomials in α.** The remaining recombination of our previous notations is $K[\alpha]$, where $K \subseteq L$ are fields and $\alpha \in L$. What might this mean? Carlos proposed that it should be all the polynomials in α, i.e.

$$K[\alpha] := \{f(\alpha) : f \in K[x]\}.$$

We now have four different types of sets we can build out of a field K: $K[x]$ and $K(x)$ consist of functions, while $K[\alpha]$ and $K(\alpha)$ consist of numbers (where by 'numbers' we actually mean elements of L). Occasionally, though, these different notations refer to the same set. For example, we verified in class that

$$\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\} = \mathbb{Q}(i).$$

Similarly,

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}).$$

3. Kronecker's Theorem, Revisited

Recall Kronecker's Theorem:

Theorem 4 (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, $[t] \in L = K[t]/\langle f \rangle$ is always a root of f, but this doesn't really *tell us* anything about the root of f—it's just a formalism!

To explain why we care about this result, we return to the familiar example $f(x) = x^2 + 1$. 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. The same idea holds true for Kronecker's theorem in general.

3.1. **Reverse Kronecker.** When working with Kronecker's theorem, we are given a field K and a polynomial $f \in K[t]$. Then, we construct an extension $K[t]/\langle f \rangle$ and a number $\alpha \in K[t]/\langle f \rangle$ 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 $K[t]/\langle f \rangle \simeq K(\alpha)$? 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 $K[t]/\langle f \rangle$ for some $f \in K[t]$?

Let's look at an example. Can we find some $f \in \mathbb{Q}[x]$ such that $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[t]/\langle f \rangle$? Sure, no problem: $f(t) = t^2 - 2$. We know by Kronecker that $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[t]/\langle t^2 - 2 \rangle$, and then we saw above that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$. Similarly, we see that $\mathbb{Q}(i) \simeq \mathbb{Q}[t]/\langle t^2 + 1 \rangle$. Note that in both these cases 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 $K[t]/\langle f \rangle \simeq K(\alpha)$?

In the above examples with $\alpha = \sqrt{2}$ and $\alpha = i$ we first proved that $K[t]/\langle f \rangle \simeq K[\alpha]$, and then gave a separate argument showing that $K[\alpha] = K(\alpha)$. So let's focus on the less ambitious goal of finding an f such that

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

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

Theorem 5 (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, given ϕ, there are two natural maps out of R: we can apply ϕ, or we can project from R onto $R/\ker \phi$. The first isomorphism 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 $h \in K[t]$? Tate proposed that we send $h \mapsto h(\alpha)$. (This is called the *evaluation map*.) Formally, we've defined ϕ by

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

Note that $\text{im } \phi = K[\alpha]$, since any polynomial in α is the image of the same polynomial with each α replaced by t. Thus, by the 1st isomorphism theorem, we have

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

What's $\ker \phi$? It's the set of all polynomials in $K[t]$ that have α as a root:

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

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, $\ker \phi = \langle m_\alpha \rangle$ and $K[t]/\langle m_\alpha \rangle \simeq K[\alpha]$. 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 $\langle m_\alpha \rangle$ is a maximal ideal—in other words, if m_α is irreducible over K—then $K[t]/\langle m_\alpha \rangle$ 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 $\langle m_\alpha \rangle = \ker \phi$, which is the set of polynomials in $K[t]$ that have α as a root. In particular, we must have $g \in \langle m_\alpha \rangle$, 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 $K[t]/\langle m_\alpha \rangle \simeq K(\alpha)$.*

Proof. From above we have $K[t]/\langle m_\alpha \rangle \simeq K[\alpha]$. 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, $K[\alpha] = K(\alpha)$. □