GALOIS THEORY: LECTURE 6

FEBRUARY 19, 2024

We start by reviewing a few concepts from last class. Given a field K, we can form $K[t]$, the set of all polynomials with coefficients in K; this set forms a ring. Some polynomials are irreducible, meaning that the only way to express them as a product of two polynomials in $K[t]$ is if one of those polynomials is a unit. And what are these units? Carlos pointed out that

$$K[t]^\times = K^\times = K \setminus \{0\}.$$

In other words, any factorization of a polynomial that's irreducible over $K[t]$ must look like a polynomial times a constant.

1. Analogies between $\mathbb{Z}$ and $K[t]$

Irreducible polynomials are highly reminiscent of prime numbers, but of course there are some differences. For example, in $\mathbb{Z}$ there are only two units (namely, ± 1), whereas in $K[t]$ there might be infinitely many! To get a better sense of how deep such analogies go, we wrote down a little table:

	$\mathbb{Z}$	$K[t]$
Units	$\mathbb{Z}^\times = \{\pm 1\}$	$K[t]^\times = K \setminus \{0\}$
Prime/Irreducible	$p \in \mathbb{Z}$ is prime iff $p = ab$ implies a or b is a unit.	$f \in K[t]$ is irreducible iff $f = gh$ implies g or h is a unit.
Factoring	Any $n \in \mathbb{Z}$ can be written as a unit times a product of primes.	Any $f \in K[t]$ can be written as a unit times a product of irreducibles.
Quotient-Remainder	For all $a, b \in \mathbb{Z}, b \neq 0$, $\exists! q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < \|b\|$	$\forall f, g \in K[t], g \neq 0$, $\exists! q, r \in K[t]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.
Structure of ideals	$\langle a, b\rangle := a\mathbb{Z} + b\mathbb{Z} = \big(\gcd(a,b)\big)$	$\langle f, g\rangle := fK[t] + gK[t] = \big(\gcd(f,g)\big)$
Prime Divisibility Property	p prime and $p \mid ab \implies p \mid a$ or $p \mid b$.	f irreducible and $f \mid gh \implies f \mid g$ or $f \mid h$.

Studying this table, we can compile a dictionary between the worlds of integers and polynomials:

$$\text{prime} \longleftrightarrow \text{irreducible}$$
$$\text{magnitude} \longleftrightarrow \text{degree}$$
$$\text{positive} \longleftrightarrow \text{monic}$$

Using this dictionary, we can make conjectures about the structure of $K[t]$ based on known results about primes, and vice-versa.

2. Introduction to Field Extensions

Motivating Question. Is $x^2 + 1$ irreducible over $\mathbb{F}_3$, the field with three elements?

If x^2+1 were reducible over $\mathbb{F}_3$, we would be able to factor it, i.e. we'd have $x^2 + 1 = (ax+b)(cx+d)$ in $\mathbb{F}_3$. But this would imply that x^2+1 has a root in $\mathbb{F}_3$, which it doesn't! Thus, x^2+1 is irreducible over $\mathbb{F}_3$.

This is reminiscent of the situation over $\mathbb{R}$: x^2+1 has no real roots and is thus irreducible over $\mathbb{R}$. On the other hand, by zooming out from $\mathbb{R}$ to $\mathbb{C}$, we *can* find roots of this polynomial. Can we do the same thing in the context of $\mathbb{F}_3$?

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

One obvious approach is to take the number i, which we know squares to -1, and simply add it to the field $\mathbb{F}_3$. What does this actually mean? More generally, how does one adjoin a number α to a field K? Tate suggested that this field—denoted $K(\alpha)$—is defined to be the smallest field containing both K and α. To make this more precise, Jonathan suggested $K(\alpha)$ should be the intersection of all fields F containing both K and α, i.e.

$$K(\alpha) := \bigcap_{\substack{F \supseteq K \\ F \ni \alpha}} F.$$

At first glance, this seems like a very reasonable definition. Closer inspection, however, reveals that this is a problematic definition. What are "all" the fields F we're looking at? It turns out that the Löwenheim-Skolem theorem implies that the collection of all fields is too big to be a set—it's what's called a *proper class*. In other words, it's not possible to intersect all sets containing K, because there are simply too many to consider.

Jonathan responded by pointing out that α has to live somewhere to start with. Let's say $\alpha \in L$, a field. Then we can adjust the above definition to fix our earlier problem: given a field K, a field L, and $\alpha \in L$, we define K adjoin α to be

$$K(\alpha) := \bigcap_{\substack{F \ni \alpha \\ K \subseteq F \subseteq L}} F.$$

Now that we have a proper definition, we can return to our initial idea: adjoining i to $\mathbb{F}_3$. But there's a problem: by definition, $i \in \mathbb{C}$, so $\mathbb{F}_3(i)$ is a field living between $\mathbb{F}_3$ and $\mathbb{C}$. But Felix pointed out $\mathbb{F}_3$ isn't a subfield of $\mathbb{C}$, since $2 + 2 = 1$ in $\mathbb{F}_3$ but $2 + 2 \neq 1$ in $\mathbb{C}$! Thus it doesn't make sense to adjoin i to $\mathbb{F}_3$.

But maybe this is a linguistic issue? In other words, sure, we can't literally adjoin i to $\mathbb{F}_3$ the way they're written, but perhaps there's a subfield of $\mathbb{C}$ that's isomorphic to $\mathbb{F}_3$ so that we can adjoin i to this subfield? No:

Proposition 1. $\mathbb{F}_3$ *does not embed into* $\mathbb{C}$.

Proof. Suppose $\phi : \mathbb{F}_3 \to \mathbb{C}$ is a homomorphism; we claim ϕ cannot be injective. To see this, first observe that

$$\phi([0]) = \phi([0] + [0]) = \phi([0]) + \phi([0]),$$

whence $\phi([0]) = 0$. Thus, we have

$$0 = \phi([0]) = \phi([1] + [1] + [1]) = \phi([1]) + \phi([1]) + \phi([1]) = 3\phi([1]).$$

It follows that $\phi([1]) = 0 = \phi(1)$, so ϕ is not injective. □

We conclude that there's no way to adjoin the number $i \in \mathbb{C}$ to the field $\mathbb{F}_3$, since the proposition above shows that we can't describe $\mathbb{F}_3$ using the language of complex numbers (and in particular, there's no good way to describe the interaction between i and $\mathbb{F}_3$). Notice that the heart of the proof above is the idea that $[1] + [1] + [1] = [0]$ in $\mathbb{F}_3$ but $1 + 1 + 1 \neq 0$ in $\mathbb{C}$. This idea motivates a useful definition:

Definition. The *characteristic* of a field K (denoted by char K) is the least positive $n \in \mathbb{N}$ such that

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If no such n exists, then we say that char $K = 0$.

Proposition 2. *If* char $K \neq$ char K'*, then* K *does not embed into* K'.

Proof. On the problem set. □

Remark. Note that Proposition 2 immediately implies that if $K \simeq K'$, then char $K =$ char K'. The converse of this statement does not hold, however.

It turns out that the characteristic of a field is always either 0 or a prime (see this week's problem set). In practice, proofs of theorems about field theory often split into two cases: characteristic 0 and positive characteristic, employing two different approaches. This led us to a story about Hironaka and his resolution of singularities theorem.

When we discussed generating a field from a given set of elements, we required two additional pieces of information: a small field and a large ambient field. But as we've seen, we don't need to require that the small field literally live inside the large one; an isomorphic copy will do. We formalize this in the following definition:

Definition. Given two fields K and L we say that L is a *field extension* of K if and only if K embeds into L, i.e. that there exists an injective homomorphism $K \hookrightarrow L$.

This is all great, but doesn't resolve our initial motivating question about solving $x^2 + 1 = 0$ over $\mathbb{F}_3$. It turns out this is possible, as was first discovered by Kronecker in the 1880s:

Theorem 1. *Given $f \in K[t]$, there exists a field extension L of K such that f has a root in L.*

We'll prove this theorem, and apply it to resolve our motivating question, next class.