GALOIS THEORY: LECTURE 7

FEBRUARY 22, 2024

1. FINISHING UP THE EXAMPLE FROM LAST CLASS

Recall from last time that we tried to solve $x^2 + 1 = 0$ over $\mathbb{F}_3$, which led to the following theorem.

Theorem 1 (Kronecker, 1882)**.** *Given a polynomial $f \in K[t]$, there exists a field extension L of K such that f has a root in L.*

The term *field extension*, which we defined last time, is fundamental to this course but also slightly subtle, so we recall it:

Definition. We say L is a *field extension* of K iff L is a field and there exists an injective homomorphism from K into L, which we write $K \hookrightarrow L$.

The big idea of the proof is to let $L := \frac{K[t]}{\langle f \rangle} = \{[g] : g \in K[t]\}$, where $[g] := g + fK[t]$. Before writing down a proof of the general case, let's work out an example.

Example 1. (*Solving $x^2 + 1 = 0$ over $\mathbb{F}_3$*) Consider $L := \frac{\mathbb{F}_3[t]}{\langle t^2+1 \rangle}$. For any $g \in \mathbb{F}_3[t]$, the set $[g]$ is an element of L. Note, however, that there's often a way to simplify a given element. For example,

$$[t^4 + 2] = [t^4 + 2] - [0] = [t^4 + 2] - [(t^2 + 1)t^2] = [t^4 + 2 - t^4 - t^2] = [2t^2 + 2] = [0].$$

More generally, your intuition (or, more formally, the quotient-remainder theorem!) should tell you that $[g]$ can always be simplified to the form $[at+b]$ for some $a, b \in \mathbb{F}_3$. Moreover, it's not hard to see that $[at+b] \neq [a't+b']$ unless $a = a'$ and $b = b'$. It's therefore reasonable to guess that $L = \{[at + b] : a, b \in \mathbb{F}_3\}$, and this is indeed the case. Note that $|L| = 9$. Addition is unsurprising, but multiplication looks a bit weirder; for example,

$$[t + 1][t] = [t + 2].$$

After some playing around, Jonathan pointed out a nice trick for simplifying an element $[g] \in L$: replace every instance of t^2 by -1.

Because L is finite (and relatively small), we can write down a complete multiplication table for L:

$\times$	1	2	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$
1	1	2	t	$t+1$	$t+2$	$2t$	$2t+1$	$2t+2$
2	2	1	$2t$	$2t+2$	$2t+1$	t	$t+2$	$t+1$
t	t	$2t$	2	$t+2$	$2t+2$	1	$t+1$	$2t+1$
$t+1$	$t+1$	$2t+2$	$t+2$	$2t$	1	$2t+1$	2	t
$t+2$	$t+2$	$2t+1$	$2t+2$	1	t	$t+1$	$2t$	2
$2t$	$2t$	t	1	$2t+1$	$t+1$	2	$2t+2$	$t+2$
$2t+1$	$2t+1$	$t+2$	$t+1$	2	$2t$	$2t+2$	t	1
$2t+2$	$2t+2$	$t+1$	$2t+1$	t	2	$t+2$	1	$2t$

Multiplication table for $\mathbb{F}_3[t]/\langle t^2 + 1 \rangle$

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

Note that, formally speaking, there should be brackets around all the entries. Molly, in particular, was keen to know whether the brackets were really necessary. After all, when writing complex numbers we don't use brackets! This is exactly the same situation as when we describe $\mathbb{F}_3$ itself: most commonly people think of $\mathbb{F}_3$ as the set $\{0, 1, 2\}$ under the operations $+$ (mod 3) and $\times$ (mod 3), but formally $\mathbb{F}_3$ is the set $\{[0], [1], [2]\}$ under ordinary $+$ and $\times$. The difference between these is aesthetic: the former consists of ordinary numbers but with weird operations, while the latter consists of weird elements but with familiar binary operations.

One instant deduction from the multiplication is that every nonzero element of L is invertible, since there's a 1 in every row. Since L is also clearly a ring, we deduce that L must be a field. Is L a field extension of $\mathbb{F}_3$? Yes: Noah proposed the map $\mathbb{F}_3 \hookrightarrow L$ with $\alpha \mapsto [\alpha]$. Finally, observe that $f(x) = x^2 + 1$ has a root in L. Indeed,

$$\begin{aligned} f([t]) &= [t]^2 + [1] \\ &= [t^2 + 1] \\ &= [0]. \end{aligned}$$

2. Proof of Kronecker's Theorem

Given a nonconstant polynomial $f \in K[t]$, without loss of generality we may assume f is irreducible (if not, replace f by one of its irreducible factors). Let $L := \frac{K[t]}{\langle f \rangle}$.

- Claim 1: L is a field.
- Claim 2: L is a field extension of K.
- Claim 3: f has a root in L.

We will prove each of these claims. The latter two proofs are straightforward generalizations of how we handled our example from above, but the proof of the first claim requires some new ideas. This isn't a surprise: in our example, we proved that L was a field by writing down the multiplication table and observing that each row has $[1]$ in it, but clearly that approach won't work in the general case.

Proof of Claim 1. We can see that L is a ring by the way it's defined, so it's enough to show that every nonzero element has a multiplicative inverse. Pick $[g] \in L$ such that $[g] \neq 0$, which means g is not a multiple of f. It immediately follows that

$$\langle f \rangle \subsetneq \langle f, g \rangle \subseteq K[t].$$

As discussed last class, $K[t]$ has the nice property that any ideal is principal, i.e. is generated by a single polynomial. Thus there exists some $h \in K[t]$ such that

$$\langle f, g \rangle = \langle h \rangle .$$

Since $f \in \langle h \rangle$, we deduce $f = hr$ for some $r \in K[t]$. But f is irreducible, so either h or r must be a unit... and r can't be a unit, since in that case we'd have $\langle f \rangle = \langle h \rangle = \langle f, g \rangle$. Thus we conclude that h must be a unit, whence

$$\langle f, g \rangle = \langle h \rangle = K[t].$$

In particular, we deduce that $1 \in \langle f, g \rangle$, or in other words, $\exists h_1, h_2 \in K[t]$ such that $gh_1 + fh_2 = 1$. Taking brackets of both sides, we deduce

$$[1] = [gh_1 + fh_2] = [gh_1] = [g][h_1].$$

We conclude that $[g]$ has an inverse (namely, $[h_1]$). □

Remark. Our proof technique implies something much more general: if M is a maximal ideal of a ring R (i.e. there's no ideal strictly between M and R), then R/M is a field. Given this, the main thrust of our proof was to show that $\langle f \rangle$ is a maximal ideal of $K[t]$ whenever f is irreducible.

The other two claims are easy to prove, because they're the same as in our example. For Claim 2, it's not hard to verify that the map $\alpha \mapsto [\alpha]$ is an injective homomorphism from K to L, so L is a field extension of K. As for Claim 3, write $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n$. Then

$$\begin{aligned} f([t]) &= a_0 + a_1[t] + a_2[t^2] + \ldots a_n[t^n] \\ &= [a_0 + a_1 t + a_2 t^2 + \ldots a_n t^n] \\ &= [f(t)] \\ &= [0]. \end{aligned}$$

This completes the proof of Kronecker's Theorem.