GALOIS THEORY : LECTURE 7

LEO GOLDMAKHER

1. KRONECKER'S THEOREM

Recall that last lecture, we introduced the following theorem.

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

Before proving the theorem in general, we work through the special case $f(t) = t^2+1$. Consider $L := \mathbb{Q}[t]/(f)$, which consists of the equivalence classes with respect to the ideal generated by f. In other words,

$$L = \{[g] : g \in \mathbb{Q}[t]\}$$

where $[g_1] = [g_2]$ if and only if $g_1 \equiv g_2 \pmod{t^2+1}$. We claimed that a more explicit way to describe the elements of L is

$$L = \{[at+b] : a, b \in \mathbb{Q}\}.$$

Remark. We claim that all equivalence classes $[at + b]$ are distinct. For, suppose not. Then we have some $[at + b] = [ct + d]$, say. But this implies $[(a - c)t + (b - d)] = [0]$, or in other words,

$$(t^2 + 1) \mid (a - c)t + (b - d).$$

Since the degree of the left side is larger than the degree of the right, this can only happen if the right side is 0, i.e. if $a = c$ and $b = d$ as claimed.[1]

We also note that L is an extension of $\mathbb{Q}$. We show this by finding an injective homomorphism from $\mathbb{Q}$ into L. It turns out that the most natural mapping $\alpha \mapsto [\alpha]$ fits the bill. Indeed, it is injective by the above remark regarding distinctness, and is clearly a homomorphism.

Finally, we observe that there is a root of $f(t) := t^2 + 1$ in L, namely $[t]$. Indeed, given our embedding of $\mathbb{Q}$ in L, we see that in the language of K the polynomial f is written $f(t) = [t]^2 + [1]$. Thus

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

Having considered a special case, we're now ready to attack the general case of Kronecker's Theorem. We do this in three steps:

(1) Show L is a field.
(2) Show L/K.
(3) Show f has a root in L.

Proof. First note that we may assume that f is irreducible over $K[t]$. Indeed, if f were not irreducible, we can take an irreducible factor and proceed with the same proof.

Why is L a field? Well, (f) is a maximal ideal of $K[t]$, whence $K[t]/(f)$ must be a field. See the supplementary notes on Ring Theory for more on these assertions.

Next, we wish to show that L is a field extension of K. In other words, we wish to show that there exists an injective homomorphism $\phi : K \hookrightarrow L$. Once again we consider the most natural map: $\alpha \longmapsto [\alpha]$. This is easily checked to be an injective homomorphism.

Date: February 22, 2018.

Based on notes by Grace Mabie.

[1]More generally, if $f \mid g$ then $\deg f \le |\deg g|$.

All that remains is to show that f has a root in L. We claim that $[t]$ is a root:

$$f([t]) = [f(t)] = [0].$$

The theorem is proved! $\square$

Let's briefly return to our example,

$$L = \mathbb{Q}[t]/(t^2+1) = \{[at+b] : a, b \in \mathbb{Q}[t]\}.$$

Does L look familiar? Indeed it does: it's isomorphic to $\mathbb{Q}(i)$. We can even construct an explicit isomorphism $L \to \mathbb{Q}(i)$: the one which maps $[at+b] \mapsto ai+b$. It's straightforward to verify that this it's a bijective homomorphism.

Above we applied the proof of Kronecker's theorem to construct $\mathbb{Q}(i)$. What if instead we wanted to construct $\mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/3}$? Andrew observed that ω is a root of t^3-1, and thus suggested

$$\mathbb{Q}(\omega) \simeq \mathbb{Q}[t]/(t^3-1) = \{[at^2+bt+c] : a, b, c \in \mathbb{Q}\}$$

However, there was a problem with this: by playing around we found that $[3t^2-3t]+[t-1]^3 = [0]$, which simplifies to

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

However, there are no zero-divisors in a field! The other Andrew identified the problem: t^3-1 isn't irreducible, which means that the ideal generated by it isn't maximal, which means that when we mod out by this ideal we don't get a field!

Thus, it's important for us to be able to identify whether or not a given polynomial is irreducible. And so, without further ado...

2. Tests for Irreducibility

Test 1 (Rational Root Test)**.** Suppose $f(t) = a_nt^n + ... + a_1t + a_0 \in \mathbb{Z}[t]$. If $\frac{r}{s}$ is a reduced fraction such that $f(\frac{r}{s}) = 0$, then $r \mid a_0$ and $s \mid a_n$.

Example. Let $f(x) = x^3+x+1$. The rational root test states that for any root $\frac{r}{s}$, it must be the case that $r \mid 1$ and $s \mid 1$, which is only true for $\frac{r}{s} = \pm 1$. However, $f(\pm 1) \neq 0$, so f has no roots over $\mathbb{Q}$. We can then conclude that f is irreducible, since f has degree 3 and has no linear factors.

CAUTION! Just because $f \in \mathbb{Q}[t]$ doesn't have a root in $\mathbb{Q}$ doesn't mean f is irreducible over $\mathbb{Q}$. Indeed, the polynomial $x^4+3x^2+2 = (x^2+1)(x^2+2)$ is reducible but does not have a root in $\mathbb{Q}$.

Test 2 (Reduction to $\mathbb{Z}$)**.** It's easy to see that if f is irreducible over $\mathbb{Q}$, then it must also be irreducible over $\mathbb{Z}$. Perhaps surprisingly, the converse also holds:

Proposition 2. *Given $f \in \mathbb{Z}[t]$. Then f is irreducible over $\mathbb{Q}$ if and only if f is irreducible over $\mathbb{Z}$*

Before proving this, we describe our primary tool:

Lemma 3 (Gauss)**.** *The product of two primitive polynomials is a primitive polynomial.*

Of course to make sense of this we need to define the term *primitive*...

Definition. A polynomial $f \in \mathbb{Z}[t]$ is primitive if and only if all of its coefficients are relatively prime.

Proof of Proposition 2. We show that if f is reducible over $\mathbb{Q}$, then it is also reducible over $\mathbb{Z}$. First off, we may as well assume f is primitive, because if not we can divide through by the gcd of the coefficients of f, creating a primitive polynomial which is reducible iff the original was.

Now suppose $f = gh$ for some $g, h \in \mathbb{Q}[t]$. There exists some $\alpha, \beta \in \mathbb{Z}$ such that $\alpha g, \beta h \in \mathbb{Z}[t]$, and $\alpha g, \beta h$ are both primitive. Now observe that

$$\alpha\beta f = (\alpha g)(\beta h).$$

This implies that $\alpha\beta f$ is the product of two primitive polynomials, hence must itself be primitive. But, since we also assumed f to be primitive, we deduce that $\alpha, \beta = \pm 1$. Therefore, it must have been the case that $g, h \in \mathbb{Z}[t]$, and the theorem is proved. $\square$

Test 3 (Eisenstein Criterion)**.** Suppose $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that p does not divide the leading coefficient, p divides all other coefficients, and p^2 does not divide the constant term, then f is irreducible over $\mathbb{Q}$.

For example, $x^3 - 3x + 3$ must be irreducible over $\mathbb{Q}$. We will prove Eisenstein's criterion (and see other examples of how useful it can be!) next time.