GALOIS THEORY: LECTURE 17

LEO GOLDMAKHER

1. Separability of Polynomials

Last time, we discovered that to determine the separability of a polynomial $f \in \mathbb{R}[x]$ one doesn't need to find its roots – studying the behavior of its derivative f' tells you all you need to know. The following result generalizes this to polynomials over arbitrary fields:

Proposition 1.1. *A polynomial $f \in K[x]$ is separable if and only if f and f' are coprime.*

Remark. We say two polynomials $f, g \in K[x]$ are *coprime* if and only if their only common factors in $K[x]$ are units.

Note that the proposition doesn't require us to find the roots of f; in fact, we never have to leave the world of $K[x]$! On the other hand, for the result to be useful we need to be able to figure out whether or not f and f' are coprime. Fortunately, this turns out to be easy to determine, as the following example illustrates.

Example 1. Let $f(x) = x^7 + 9x + 6 \in \mathbb{Q}[x]$. Is this polynomial separable?

The derivation of f is $f'(x) = 7x^6 + 9$. Let $\pi \in \mathbb{Q}[x]$ be a common factor of f and f', i.e. $\pi \mid f$ and $\pi \mid f'$. Then π must also divide any multiple of f and f', and more generally, any linear combination of f and f'. We construct such a polynomial so that the leading terms of f and f' cancel:

$$\pi \mid 7f - xf' = 54x + 42 = 6(9x + 7).$$

Therefore $\pi(x)$ must be either a constant multiple of $9x + 7$, or simply a constant. The former cannot hold, since $\frac{-7}{9}$ is not a root of f. (There are several ways to verify this; perhaps the simplest is to observe that f is Eisenstein at 3, hence irreducible. This suggests a result that we will come back to later.) Thus π must be constant, which shows that f and f' are coprime. By Proposition 1.1, f must be separable.

Note that we were quite lucky with this example, because we were able to get a linear polynomial using f and f'. What if canceling the leading terms leaves some higher order polynomial g with $\pi \mid g$? Then we can iterate the process, using g and f' to produce another polynomial of smaller degree that is divisible by π, etc. Note the similarity of this process with Euclid's algorithm for the integers.

Now we will actually prove Proposition 1.1.

Proof of Prop. 1.1. As usual, we prove the two directions individually.
($\Rightarrow$) Suppose f is separable. Let L be a splitting field of f, and pick any root $\alpha \in L/K$ of f. Then we can write $f(x) = (x - \alpha)g(x)$; note that $x - \alpha \nmid g$ (since f is separable). Product rule implies

$$f'(x) = g(x) + (x - \alpha)g'(x),$$

whence $x - \alpha \nmid f'$. Since α was an arbitrary root of f, we've shown that any linear factor of f cannot be a factor of f'. Thus, f and f' share no nontrivial factors, hence must be coprime.
($\Leftarrow$) Suppose f is inseparable. Then it has some root α such that $f(x) = (x - \alpha)^2 g(x)$. Product rule yields

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x),$$

whence $x - \alpha \mid f'(x)$. In other words, f and f' share the common factor $x - \alpha$, so f and f' are not coprime. $\square$

Date: April 19, 2018.
Based on notes by Daishiro Nishida.

Note that for both directions of the above proof, the key was identifying linear factors $x - \alpha$. But there's something fishy going on here: $x - \alpha$ lives in a splitting field of f, but might not live in $K[x]$. Thus, what we actually proved was that f is separable iff f and f' share no roots in a splitting field of f. It turns out, however, that this condition is equivalent to the polynomials being coprime (see problem **9.5**):

Lemma 1.2. *Polynomials $f, g \in K[x]$ are coprime if and only if they do not share roots in any splitting field.*

Combining this with our work above completes the proof of Proposition 1.1. Now we derive some awesome consequences.

Corollary 1.3. *Suppose $f \in K[x]$ is irreducible. Then f is separable if and only if $f' \neq 0$.*

Proof. ($\Rightarrow$) Suppose $f' = 0$. Then f and f' are not coprime, so by Proposition 1.1, f is inseparable.
($\Leftarrow$) Suppose f is not separable. Then by Proposition 1.1, there exists some $\pi \in K[x]$ with $\deg \pi \geq 1$ such that $\pi \big| f$ and $\pi \big| f'$. But f is irreducible, so π must be a unit multiple of f. It follows that $f \big| f'$. Since the degree of f' is strictly smaller than the degree of f, this means that we must have $f' = 0$. □

Over $\mathbb{Q}$, the derivation is 0 iff the polynomial is constant. In a general field, however, the condition $f' = 0$ is *not* equivalent to f being constant; for example, the derivation of $x^p - 2 \in \mathbb{F}_p$ has derivation zero.

Example 2. Consider the polynomial $f(x) = x^3 + 2x + 2 \in \mathbb{F}_3[x]$. In order to apply Corollary 1.3, we must show that f is irreducible over $\mathbb{F}_3$. Since $\deg f = 3$, it suffices to check that it has no roots in the field, a straightforward verification. Thus, we can apply Corollary 1.3 to dedce that f must be separable since $f'(x) = 2$.

Example 3. As a non-example, consider the polynomial $f(x) = (x-1)^2(x-2) \in \mathbb{F}_3[x]$. By construction, f is reducible. To see that Corollary 1.3 fails as a result, we notice that f is not separable ($x = 1$ is a root of multiplicity 2) and yet $f' \neq 0$:

$$f(x) = (x-1)^2(x-2) = x^3 - x^2 + 2x - 2 \implies f'(x) = -2x + 2.$$

When char $K = 0$, it turns out that the situation is quite clean:

Corollary 1.4. *Suppose* char $K = 0$. *Then every nonconstant irreducible $f \in K[x]$ is separable.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If f is inseparable, then by Corollary 1.3, we must have $f'(x) = 0$. Thus,

$$0 = f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

This implies

$$k a_k = 0 \quad \text{whenever } 1 \leq k \leq n.$$

In this range of k we have $k \neq 0$, since char $K = 0$. Therefore,

$$a_k = 0 \quad \text{whenever } 1 \leq k \leq n.$$

It follows that $f(x) = a_0$, a constant. □

As an immediate consequence, we see that the polynomial in Example 1 is separable.

2. Fundamental Theorem of Algebra

We will now switch gears and use the Fundamental Theorem of Galois Theory to prove the Fundamental Theorem of Algebra. The statement of the theorem is probably familiar:

Fundamental Theorem of Algebra. Any $f \in \mathbb{C}[x]$ has all of its roots in $\mathbb{C}$.

However, we will prove an equivalent statement that is formulated in terms of field extensions:

Fundamental Theorem of Algebra (Second version)**.** There does not exist any finite extension of $\mathbb{C}$.

Note that if a polynomial has a root outside of $\mathbb{C}$, then this element gives us a finite extension of $\mathbb{C}$. Conversely, if there exists a finite extension of $\mathbb{C}$, then it must be an algebraic extension, so there is some polynomial with a root lying outside of $\mathbb{C}$. Thus, we see that these two formulations of the Fundamental Theorem of Algebra are indeed equivalent.

Before diving into the proof of the theorem, we warm up by proving a simple case of the result. A field extension of degree 2 is called a *quadratic* extension.

Proposition 2.1. *There do not exist any quadratic extensions of* $\mathbb{C}$.

Proof. Suppose $K/\mathbb{C}$ has degree 2. Then, by Problem **5.2(c)**, there exists some $\alpha \in K \setminus \mathbb{C}$ such that $K = \mathbb{C}(\alpha)$ and $\alpha^2 \in \mathbb{C}$. But then we can write $\alpha^2 = re^{i\theta}$ for some real $r \geq 0$ and $\theta \in \mathbb{R}$, which implies $\alpha = \pm\sqrt{r}e^{i\theta/2} \in \mathbb{C}$, a contradiction. Therefore there do not exist any quadratic extensions of $\mathbb{C}$. □

Remark. At the heart of the above proof is that the roots of any quadratic polynomial in $\mathbb{C}[x]$ can be expressed in terms of arithmetic operations and a square root – and that none of these operations force us to leave $\mathbb{C}$. For higher degree polynomials, expressing the roots in terms of operations were familiar with (and which don't exit the world of $\mathbb{C}$) becomes more challenging. Fortunately, the Fundamental Theorem of Galois Theory allows us to bypass this difficulty.

For the proof of the full version, we require the following two tools. The first tool appears in the same 1872 paper as its more famous cousins, the 1st, 2nd, and 3rd Sylow theorems.

Theorem 2.2 (Sylow, 1872)**.** *If G is a finite group and $p^n \big| |G|$, then there exists a subgroup $H \leq G$ of order p^n. (As usual, p denotes a prime.)*

The second tool allows us to enlarge a field extension to a Galois extension.

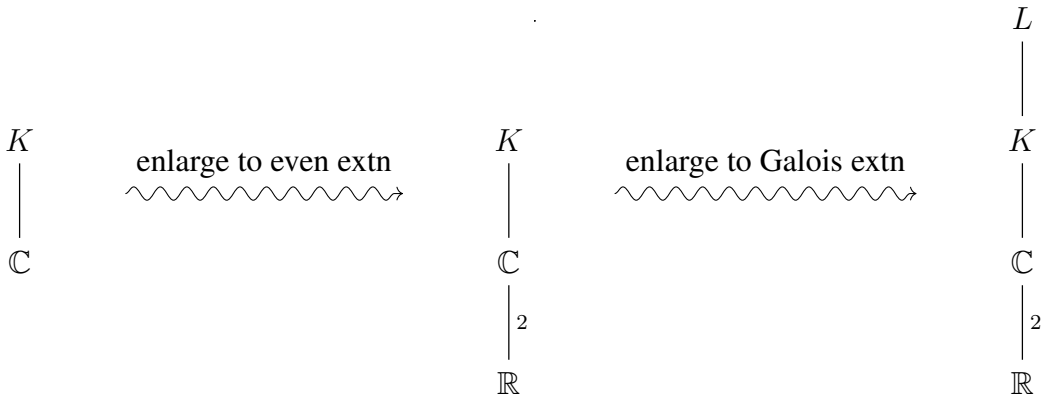
Proposition 2.3. *Let K be a field with* char $K = 0$. *Given any finite F/K, there exists a finite extension L/F such that L/K is Galois.*

Remark. See Problem **9.4** for a proof of this result. It turns out that this proposition is also true when K is a finite field, but we don't need this for the proof of the FTA.

And with that, we're ready to prove the Fundamental Theorem of Algebra!

Proof of FTA. Suppose K is a finite extension of $\mathbb{C}$; our goal is to show that $K = \mathbb{C}$. We will accomplish this by using the Fundamental Theorem of Galois Theory as a dictionary between field theory and group theory, applying tools on each side (the tower law, Sylow's theorem) and translating back and forth to obtain more and more information about each. In other words, it's a proof by pong!

Step 1. *Enlarge our extension to a Galois extension $L/\mathbb{R}$ of even degree.*



First, observe that $K/\mathbb{R}$ is a field extension of even degree, by the tower law. Next, enlarge $K/\mathbb{R}$ to a Galois extension $L/\mathbb{R}$; it still has even degree.

Step 2. *Use the FTGT dictionary and group theory to prove* $[L : \mathbb{R}] = 2^m$.

Since $[L : \mathbb{R}]$ is even, we can write

$$[L : \mathbb{R}] = 2^m \ell$$

where $m \geq 1$ and ℓ is odd. Let $G := \text{Gal}(L/\mathbb{R})$. The Fundamental Theorem of Galois Theory gives us the following picture:

$$\begin{array}{c} L \\ \Big| {\scriptstyle 2^m\ell} \\ \mathbb{R} \end{array} \qquad\qquad \begin{array}{c} G \\ \Big| {\scriptstyle 2^m\ell} \\ \{e\} \end{array}$$

By Sylow's theorem, there must exist a subgroup $H \leq G$ of order 2^m. The Galois correspondence yields a mirror image on the field side:

$$\begin{array}{c} L \\ \Big| {\scriptstyle 2^m} \\ L^H \\ \Big| {\scriptstyle \ell} \\ \mathbb{R} \end{array} \qquad\qquad \begin{array}{c} G \\ \Big| {\scriptstyle \ell} \\ H \\ \Big| {\scriptstyle 2^m} \\ \{e\} \end{array}$$

In particular, we have $[L^H : \mathbb{R}] = \ell$, an odd integer. I claim this implies that $L^H = \mathbb{R}$. Why? Pick $\alpha \in L^H$, and let $m_\alpha \in \mathbb{R}[x]$ denote its minimal polynomial over $\mathbb{R}$. By Tower Law, $\deg m_\alpha = [\mathbb{R}(\alpha) : \mathbb{R}]$ must be odd, whence the Intermediate Value Theorem implies that m_α has a root in $\mathbb{R}$. Since m_α is irreducible over $\mathbb{R}$, it must have degree 1, so

$$[\mathbb{R}(\alpha) : \mathbb{R}] = \deg m_\alpha = 1.$$

It follows that $\alpha \in \mathbb{R}$. Since $\alpha \in L^H$ was arbitrary, we have shown that $L^H = \mathbb{R}$. In particular, $\ell = 1$, and our picture becomes

$$\begin{array}{c} L \\ \Big| {\scriptstyle 2^m} \\ \mathbb{R} \end{array} \qquad\qquad \begin{array}{c} G \\ \Big| {\scriptstyle 2^m} \\ \{e\} \end{array}$$

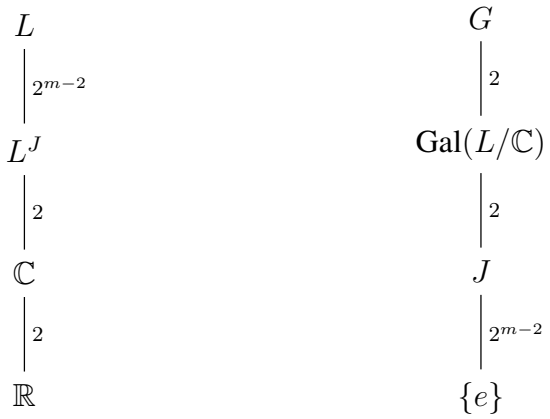
Step 3. *Produce a forbidden quadratic extension of* $\mathbb{C}$.

Since $\mathbb{C}$ is an intermediate field of the Galois extension $L/\mathbb{R}$, the Galois correspondence and the Tower Law give

$$\begin{array}{c} L \\ \Big| {\scriptstyle 2^{m-1}} \\ \mathbb{C} \\ \Big| {\scriptstyle 2} \\ \mathbb{R} \end{array} \qquad\qquad \begin{array}{c} G \\ \Big| {\scriptstyle 2} \\ \text{Gal}(L/\mathbb{C}) \\ \Big| {\scriptstyle 2^{m-1}} \\ \{e\} \end{array}$$

We wish to show that $m = 1$. Suppose otherwise, i.e., $m \geq 2$. Then, again by Sylow's theorem, there would exist a subgroup $J \leq \text{Gal}(L/\mathbb{C})$ of order 2^{m-2}. The Galois correspondence would

then yield the hypothetical picture



But this would necessitate the existence of a quadratic extension $L^J/\mathbb{C}$, contradicting Proposition 2.1! Thus, no such J can exist, whence $m = 1$. We deduce that $[L : \mathbb{C}] = 1$; since $\mathbb{C} \subseteq K \subseteq L$, we conclude that $K = \mathbb{C}$. The Fundamental Theorem of Algebra is proved. $\square$