GALOIS THEORY: LECTURE 16

LEO GOLDMAKHER

1. Galois Extensions

Last class we discussed the Fundamental Theorem of Galois Theory, which gives us a wealth of information about certain "nice" field extensions via a correspondence with the extension's automorphism group. Today, we explore the properties of these *Galois extensions* in more detail. Recall that a finite field extension L/K is Galois if and only it satisfies one of the following conditions:

(A) $|G| = [L : K]$,
(B) there exists a separable polynomial $f \in K[x]$ such that L is a splitting field of f, or
(C) $L^G = K$

where $G = \text{Aut}(L/K)$ and L^G denotes the fixed field of G in L.

Remark. In the case that L/K is Galois, we call $G = \text{Aut}(L/K)$ the *Galois group* of the extension (as opposed to the automorphism group, which is what it's usually called); we will also denote it by $\text{Gal}(L/K)$. There is literally no difference between this and the automorphism group of the extension – it's merely a convenient device to indicate that the extension is Galois.

In order to show that this definition of Galois extensions makes sense, we need to show that the conditions (A), (B), (C) are equivalent. We proved last time (A) $\implies$ (B), critically using Geck's proof of the bound $|\text{Aut}(L/K)| \leq [L : K]$ for all finite extensions L/K. We now prove (A) $\implies$ (C).

Proof that (A) $\implies$ (C). Given $|G| = [L : K]$, we want to show that $L^G = K$.

First approach.

Eli proposed the following strategy. Suppose that there exists $x \notin K$ that is also fixed by all elements of G. We proved last time that if L/K is Galois, then there exists some $\alpha \in L$ such that $L = K(\alpha)$ and so we can write x in terms of a basis consisting of powers of α:

$$x = k_0 + k_1\alpha + \cdots + k_{d-1}\alpha^{d-1}$$

for some $k_0, k_1, \ldots, k_{d-1} \in K$, where $d = \deg \alpha = [L : K]$. Then, applying any $\sigma \in G$ to α, we see that

$$k_0 + k_1\alpha + \cdots + k_{d-1}\alpha^{d-1} = x = \sigma(x) = k_0 + k_1\sigma(\alpha) + \cdots + k_{d-1}\sigma(\alpha)^{d-1}.$$

Rearranging terms, we deduce that

$$k_1\Big(\sigma(\alpha) - \alpha\Big) + k_2\Big(\sigma(\alpha)^2 - \alpha^2\Big) + \cdots + k_{d-1}\Big(\sigma(\alpha)^{d-1} - \alpha^{d-1}\Big) = 0$$

must hold for every $\sigma \in G$. Since we have d such automorphisms $\sigma \in G$, we obtain a system of equations that probably gets us to a contradiction... eventually.

This strategy will probably work, but seems messy. So we start over with a different approach.

Second approach.

Consider the tower of field extensions $L/L^G/K$. We want to look in particular at the field extension L/L^G, since if we can show that $[L : L^G] = [L : K]$, then by the Tower Law we would have that $[L^G : K] = 1$, which would imply that the fixed field of G is K, as desired. Furthermore, observe that it suffices to prove $[L : K] \leq [L : L^G]$.

Date: April 16, 2018.

Based on notes by Andrew Scharf.

Since L^G is an intermediate field, we know that Aut(L/L^G) is a subgroup of G, consisting of all the automorphisms of L that fix the field L^G. By definition of the fixed field of G, we know that all elements in G fix L^G. So, Aut$(L/L^G) = G$. Then, using our hypothesis (A) and the bound on the size of the automorphism group from last class, we deduce

$$[L : K] = |G| = |\text{Aut}(L/L^G)| \leq [L : L^G],$$

thereby completing the proof. □

Next we prove (C) $\implies$ (B).

Proof that (C) $\implies$ (B). Given $L^G = K$, we want to show that there exists a separable polynomial $f \in K[x]$ such that L is a splitting field of f. Our strategy will be to construct a finite set $A \subset L$ such that

(i) $L = K(A)$ and

(ii) the polynomial $f(x) := \prod_{\alpha \in A}(x - \alpha)$ has coefficients in K.

Note that f is automatically separable since A is a set, and hence does not contain repeated elements. Therefore, if $f \in K[x]$ and $L = K(A)$, then L is the splitting field of f and we are done.

We know L/K is finite, so by definition of a finite extension, we can write $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. We might think to make $A = \{\alpha_i\}$, but then it's not clear whether or not f has coefficients in K. Instead, let

$$A := \{\sigma(\alpha_i) : \sigma \in G, 1 \leq i \leq n\},$$

and set

$$f(x) := \prod_{\alpha \in A}(x - \alpha)$$

as above. Observe that $L = K(A)$ since $\{\alpha_i\} \subseteq A$. Furthermore, the set A is G-invariant, i.e. $\sigma(A) = A$ for every $\sigma \in G$. (This is the reason we defined A the way we did!) The G-invariance implies that for any $\sigma \in G$,

$$f(x) = \prod_{\alpha \in A}\Big(x - \sigma(\alpha)\Big).$$

What does this tell us about the coefficients of f? Since all the coefficients of f are symmetric polynomials in the roots, and since σ is a field automorphism, we deduce that every coefficient of f is fixed by every $\sigma \in G$. (See below for an example.) In other words, each coefficient lives in the fixed field of G, which by assumption is precisely K, i.e. $f \in K[x]$. □

Here's an explicit example to illustrate the concluding argument in the above proof.

Example 1. Let $f(x) := (x-1)(x-2)$, and consider the polynomial $f_\sigma(x) := \big(x - \sigma(1)\big)\big(x - \sigma(2)\big)$ where σ is an arbitrary automorphism of $\mathbb{C}$. Then

$$f_\sigma(x) = x^2 - \big(\sigma(1) + \sigma(2)\big)x + \sigma(1)\sigma(2) = x^2 + \sigma(-3)x + \sigma(2).$$

Thus if we happen to know that $f_\sigma = f$, the coefficients of f (in this case -3 and 2) are fixed by σ. In general, given a field extension L/K and a polynomial $f \in L[x]$, if $f_\sigma = f$ for all $\sigma \in G$ then the coefficients of f must be elements of L^G.

Remark. Note that the above proof doesn't work when L/K is an infinite extension! This is one reason why we restrict our attention to finite extensions (in this course – there is a Galois theory for infinite extensions).

So far we have shown that (A) $\implies$ (B), (A) $\implies$ (C), and (C) $\implies$ (B). All we need to complete the proof that the three conditions are equivalent is to show that (B) $\implies$ (A). This is left as a homework exercise; see problem **9.6**. Thus, from now on we will assume that any Galois extension satisfies all three of the above properties.

2. SEPARABILITY

Condition (B) in the characterization of Galois extensions uses separable polynomials, and so in general we would like to be able to determine efficiently whether or not a given polynomial f is separable.

Question 1. *Is the polynomial* $x^7 + 15x^6 - 2x^4 + x^3 - 102x^2 + 17$ *separable?*

Typically, to see whether or not a polynomial is separable we would find all the roots in $\mathbb{C}$, but this seems very difficult for this polynomial. Is there any other way to determine separability without going through this process? We start this investigation with an easier question.

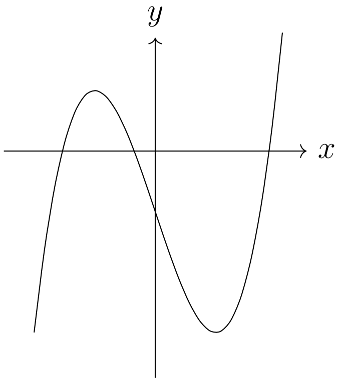
Question 2. *Is the polynomial* $f(x) = x^3 - 3x - 1$ *separable?*

We could use the cubic formula to find all the roots, but (as we've seen earlier) this process is both annoying and often unhelpful. Moreover, it's answering a more precise question than the one we're interested in: we don't care about what the roots *are*, only whether or not they're distinct!

Emily proposed the idea of using the derivative to test for repeated roots: a double real root touches the x-axis at a local minimum or maximum and so the value of f' would vanish at that point. This motivates us to determine the maxima and minima of f (by using its derivative); this will allow us to draw the graph of f, which will tell us whether or not any roots are repeated. First note that since f is cubic, it satisfies the disco property:

$$\lim_{x\to-\infty} f(x) = -\infty \qquad \text{and} \qquad \lim_{x\to\infty} f(x) = \infty.$$

What about the behavior in between? Since $f'(x) = 3x^2 - 3 = 3(x+1)(x-1)$, the "bumps" of the graph are at $x = \pm 1$, corresponding to the values $f(-1) = 1$ and $f(1) = -3$. This implies that f must cross the x-axis in three distinct places, and so must have three distinct roots.



Thus, we were able to determine that f is separable not by studying f, but by studying its derivative f'. It turns out that this is a general phenomenon:

Proposition 2.1. *A given* $f \in K[x]$ *is separable if and only if* f *and* f' *are coprime in* $K[x]$.

There's one fishy part in this statement: taking the derivative in our example above made sense because $f \in \mathbb{R}[x]$, but in a general field K limits might not be well-defined! We circumvent this issue by capturing the purely algebraic properties of polynomial derivatives over $\mathbb{R}$.

Definition. Let $f \in K[x]$, say

$$f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then the *derivation* of f is

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

Remark. Note that the derivation satisfies all the algebraic properties we care about with derivatives (e.g. $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$, etc.), but applies only to polynomial functions. However, as a word of caution, note that derivations can behave unintuitively. For example, the derivation of $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ vanishes, even though the polynomial is non-constant.

Derivations give us a beautiful way to check whether or not a polynomial is separable without having to calculate the roots or graphing. Next time we'll prove the proposition and deduce from it some unexpected (and very useful!) consequences.