Day 2: Galois Theory

Tom Gannon

August 15, 2017

1 Introduction

We'll review the basics of Galois Theory and prove a theorem which determines the structure of a composite of two fields when the Galois group of the two subfields are known.

1.1 Primer on Galois Theory

As always, let F be a field, and any field extension mentioned will take place a fixed algebraic closure of F.

Recall that the term "**Galois group**" is just the group of automorphisms of K fixing F pointwise for certain, specific field extensions K/F called *Galois Extensions*. Roughly, a "Galois Extension" means that there are as many automorphisms as there can be.

Definition 1.1. *A field extension K/F is **algebraic** if for all $\alpha \in K$, there exists an $f(x) \in F[x]$ such that $f(\alpha) = 0$. An extension K/F is **normal** if it the splitting field of some collection of polynomials (i.e. the smallest[1] field containing all the roots of those polynomials), and K/F is **Galois** if it is a normal, separable, algebraic extension.*

This doesn't always happen:

Exercise 1.2. *(Finite, Separable Extension That Isn't a Galois Extension): Show that the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has trivial automorphism group, meaning there is exactly one embedding $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{Q}(\sqrt[3]{2})$. Find a field K where there are 3 distinct embeddings $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow K$. If you looked at the "separability" sheet, you can prove this is the maximal number of extensions.*

Exercise 1.3. *(Finite, Normal Extension That Isn't Galois) Show that if $F := \mathbb{F}_2(x)$ and $K := F[t]/(t^2 - x)$ (i.e. adjoining a square root of x), then $Aut(K/F)$ is trivial.*

Exercise 1.4. *(Finite Extension Implies Algebraic Extension) Show that if K/F is a finite extension (that is K is a finite dimensional vector space over $F \subset K$) then K/F is an algebraic extension. (Hint: If $\alpha \in K$, consider the set $\{1, \alpha, \alpha^2, ...\}$). Conclude that any finite, normal, separable extension is a Galois extension.*

This is good for us in particular because for finite, normal, separable extensions we have an easy to remember relation between the dimension of the field and the order of the Galois group.

Theorem 1.5. *If K/F is a finite Galois extension with $G := Gal(K/F)$, then $|G| = [K : F]$.*

Exercise 1.6. *Prove the above theorem! You will probably want all of the results covered on "separability" day, and also to prove that if K/F is a Galois extension, then any field embedding $i : K \to \overline{F}$ actually sends $K \to K$.*

Exercise 1.7. *(Galois Groups aren't necessarily finite) Construct a Galois extension with infinite Galois group. Note that $\mathbb{C}/\mathbb{Q}$ doesn't satisfy this criterion–$\mathbb{C}$ has some elements that are not algebraic, i.e. **transcendental** over $\mathbb{Q}$. (Hint: It's "close" to being Galois, though. You'll have to use ideas from the last day to solve this, depending on the route you take. This is definitely the hardest exercise of the day, and least important for the course.)*

[1] We'll be working in a fixed algebraic closure of any field we talk about, which always exists. So if you had some technical worry, don't.

2 Primer on Using Galois Theory in Non Galois Extensions

Recall that the **Fundamental Theorem of Galois Theory** says that given any finite Galois extension K/F (one for which $[K : F]$ finite, or equivalently $|G|$ finite) with Galois group G, there is a bijective correspondence $\{\text{subgroups of } G\} \leftrightarrow \{ \text{ intermediate subfields } F \subseteq L \subseteq K\}$ given by taking a subgroup and mapping to the set of elements fixed pointwise by every element of that subgroup and taking an intermediate field to the group of elements fixing that field pointwise. But we can get even more out of this theorem:

Exercise 2.1. *(Distinct Field Embeddings) Let L/F be a finite separable field extension, not necessarily Galois. Show that there is a finite Galois extension K/F containing L. Let $G := Gal(K/F)$ and let H denote the set of elements fixing L pointwise. Show that any field embedding of L fixing F must map into K. Show that the **distinct** embeddings are given by picking a representative of each coset in G/H. Can two distinct embeddings map into the same field? Determine a condition on H and G which determines when L/F is Galois, and prove it.*

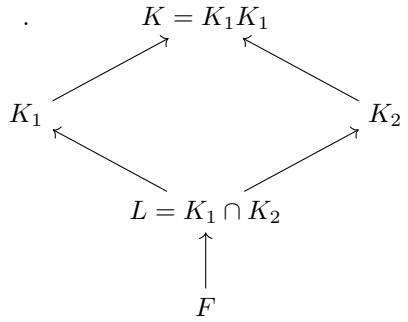
3 Primer on The "Sliding Lemma"

The "Sliding Lemma" is a term I made up to describe a lemma which describes the Galois group of the composite of two fields when the automorphism groups of the two fields are known. Maybe once these Primer Exercises achieve world class fame, everyone will call it the sliding lemma one day! But until then, here's the lemma:

Exercise 3.1. *Define the "composite" of two fields $K_1, K_2 \subset \overline{F}$ if you haven't heard the term yet. Informally, it is the union of the two fields, but closed under all of the field operations.*

Lemma 3.2. *Assume that K_1, K_2 are finite extensions of F and K_1/F is Galois. Then if $K := K_1K_2$ denotes the composite field, then K/K_2 (for emphasis, over K_2–not over F) is Galois, and if $L := K_1 \cap K_2$, then $Gal(K/K_2) \cong Gal(K_1/L)$.*

A good reference for this is section 14.4 of Dummit and Foote. Here's a picture taken from that section that I use a lot, where the arrows denote "inclusion" and also denote "I couldn't figure out how to get rid of them."



Exercise 3.3. *Show that, with the above setup, that K/K_2 is Galois.*

Exercise 3.4. *Let $G := Gal(K/K_2)$ and $H := Gal(K_1/L)$. Define a map $\psi : G \to H$ that seems like a good candidate for an isomorphism. Show it is an injective group homomorphism.*

Exercise 3.5. *Show that ψ above is surjective by arguing that if $K_1^{\psi(G)}$ denotes the elements in K_1 fixed by $\psi(G)$, then $K_1^{\psi(G)} = L$. (Hint: $K_2 \subset K_1^{\psi(G)}K_1 \subset K$. Use the fundamental theorem of Galois Theory.)*

Exercise 3.6. *Show that given two extensions K_1, K_2 over a field F such that at least one is Galois, then $[K_1K_2 : K_1 \cap K_2] = [K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2]$. Show that this conclusion need not hold if neither extension is Galois. (Hint: I like to use $\mathbb{Q}[\sqrt[3]{2}]$ for all of my "Galois hypothesis is necessary" needs.) Conclude that if two extensions $K_1/F, K_2/F$ are **linearly disjoint**–i.e. $K_1 \cap K_2 = F$, then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.*

This idea comes up because one basic question you can ask in number theory is "given the integral closure of a 'Dedikind'[2] ring in two fields, what does the integral closure in the composite field look like?"

[2]Dedikind rings are rings in which every ideal factors into a product of prime ideals, a generalization of UFDs. They're one of the first things in Algebraic Number Theory that make you think, "Woah! This is cool."