GALOIS THEORY: LECTURE 19

LEO GOLDMAKHER

1. Creating New Subfields and Subgroups

Given a finite Galois extension L/K, set $G := \text{Gal}(L/K)$, and pick $\sigma \in G$. At the end of last class we noticed that for any intermediate field F and any subgroup $H \leq G$ we have

- $\sigma(F)$ is also an intermediate field, and
- $\sigma H \sigma^{-1}$ (the *conjugate* of H by σ) is also a subgroup of G.

This inspires the following:

Lemma 1.1. *Given L/K a finite Galois extension, an intermediate field F, and a subgroup H such that $F \longleftrightarrow H$ under the Galois Correspondence, then for any $\sigma \in G$ we have $\sigma(F) \longleftrightarrow \sigma H \sigma^{-1}$ under the Galois correspondence.*

Remark. In words, the lemma sets up a correspondence between applying an automorphism on the field side with conjugating on the group side.

Proof. By the Galois Correspondence, $F = L^H$. We'd like to show $\sigma(F) = L^{\sigma H \sigma^{-1}}$. Let's follow our nose and push some symbols around:

$$\begin{aligned}
\sigma(F) = \sigma(L^H) &= \{\sigma(x) : x \in L^H\} \\
&= \{\sigma(x) : \tau(x) = x \text{ for each } \tau \in H\} \\
&= \{y : \tau\big(\sigma^{-1}(y)\big) = \sigma^{-1}(y) \text{ for each } \tau \in H\} \\
&= \{y : \sigma\tau\sigma^{-1}(y) = y \text{ for each } \tau \in H\} \\
&= L^{\sigma H \sigma^{-1}}.
\end{aligned}$$

Success! □

Remark. The lemma implies its own converse: if $\sigma(F) \longleftrightarrow \sigma H \sigma^{-1}$ then $F \longleftrightarrow H$.

2. Finishing Up the Fundamental Theorem of Galois Theory

Before we pick up the proof of the Fundamental Theorem of Galois Theory where we left it, recall that for any finite Galois extension L/K, Geck's proof implies the existence of $\alpha \in L$ such that:

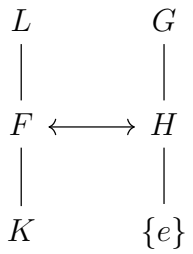
(A) $L = K(\alpha)$,
(B) all the Galois conjugates of α are distinct, and
(C) the minimal polynomial of α over K is

$$m_\alpha(x) = \prod_{\sigma \in \text{Gal}(L/K)} \big(x - \sigma(\alpha)\big).$$

With this and Lemma 1.1 at our disposal, we resume our proof of the FTGT. Throughout, assume L/K is finite and Galois, and set $G := \text{Gal}(L/K)$.

(4) Normal subgroups correspond to Galois extensions. Suppose F is an intermediate field of L/K with $F \longleftrightarrow H$ under the Galois Correspondence. Then F/K is Galois if and only if $H \trianglelefteq G$.

Date: April 26, 2018.
Based on notes by Michael Curran.



Proof. Recall from group theory that $H \trianglelefteq G$ if and only if $H = \sigma H \sigma^{-1}$ for all $\sigma \in G$. Thus Lemma 1.1 implies $H \trianglelefteq G$ if and only if $\sigma(F) = F$ for all $\sigma \in G$. Furthermore, Daishiro observed that $\sigma(F) = F$ for all $\sigma \in G$ if and only if $\sigma(F) \subseteq F$ for all $\sigma \in G$. Our claim is therefore equivalent to proving

$$F/K \text{ is Galois} \qquad \iff \qquad \sigma(F) \subseteq F \text{ for all } \sigma \in G.$$

($\Rightarrow$) Suppose F/K is Galois. Then $F = K(\alpha)$ for some $\alpha \in F$, so it suffices to prove that $\sigma(\alpha) \in F$ for all $\sigma \in G$. Jonah pointed out that

$$m_\alpha(x) = \prod_{\sigma \in \mathrm{Gal}(F/K)} \big(x - \sigma(\alpha)\big) \in K[x],$$

so certainly $\sigma(\alpha) \in F$ for all $\sigma \in \mathrm{Gal}(F/K)$. But what about all $\sigma \in G$? Andrew pointed out that since $m_\alpha \in K[x]$ we know that $\sigma(\alpha)$ must be a root of m_α for all $\sigma \in G$. But we already know all of the roots of m_α! In particular, we know they all live in F. Therefore $\sigma(\alpha) \in F$ for all $\sigma \in G$. ♣

($\Leftarrow$) Given that $\sigma(F) \subseteq F$ for all $\sigma \in G$, we want to show that F/K is Galois. Our strategy for the proof is to construct a separable polynomial in $K[x]$ with splitting field F. To do this, we employ a trick we used when proving the three definitions of a Galois extension to be equivalent. Since we know F/K is finite, we can write $F = K(\alpha_1, \ldots, \alpha_n)$. Beatrix pointed out that $\{\alpha_i\}$ should be a minimal set, in that none of the α_i can be removed without changing the field formed by adjoining the α_i. Now we form the polynomial

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

where

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

This definition of A forces f to be separable. We claim that $f \in K[x]$. Indeed, we know that all the coefficients of f are fixed by all $\sigma \in G$ since the set A is G-invariant. Thus $f \in L^G[x]$, and since L/K is Galois, we know that $L^G = K$. Since $A \subseteq F$ by hypothesis, f splits over F; moreover, F is a splitting field of f over K, since all the α_i are roots of f. Thus we conclude that F is the splitting field of a separable polynomial over K, whence F/K is Galois. □

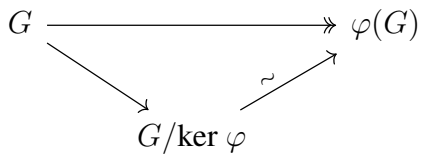
Our original statement of part 4 of the Fundamental Theorem of Galois Theory (in lecture 15) contained an additional assertion about the extension F/K. We prove this now:

Corollary 2.1. *If F/K is Galois, then* $\mathrm{Gal}(F/K) \simeq G/H$.

Remark. Note that in all the other parts of the Fundamental Theorem of Galois Theory, we assert that subgroups of G are *equal* to the corresponding automorphism groups of L/F for intermediate fields F, not just isomorphic. So in a sense this is slightly weaker than the other parts of the FTGT. This is because we lose some information when taking quotients in a group: G/H does not contain K-automorphisms, but equivalence classes of K-automorphisms.

We're trying to prove that a given group is isomorphic to a quotient. This smacks of our old friend, the first isomorphism theorem:

Theorem 2.2 (First Isomorphism Theorem)**.** *If $\varphi : G \to G'$ is a group homomorphism, then* $\ker \varphi \trianglelefteq G$ *and* $G/\ker \varphi \simeq \mathrm{im}\, \varphi$. *(See picture below.)*



We now have everything we need to prove Corollary 2.1.

Proof. We want to construct a homomorphism $\varphi : G \to \text{Aut}(F/K)$ with $\ker \varphi = H = \text{Aut}(L/F)$. So given a K-automorphism of L, we need to construct a K-automorphism of F. Emily suggested the map

$$\sigma \longmapsto \sigma|_F,$$

where the output is the restriction of σ to F. Note this restriction is well-defined, since $\sigma(F) = F$ by the proof of part 4 of the FTGT. Additionally, we know that multiplication and addition are preserved since σ is an automorphism, so φ is a homomorphism. Finally we see that

$$\begin{aligned}\ker \varphi &= \{\sigma \in G : \varphi(\sigma) = \text{id}_F\} \\ &= \{\sigma \in G : \sigma(x) = x \text{ for all } x \in F\} \\ &= \text{Aut}(L/F).\end{aligned}$$

The result follows by the First Isomorphism Theorem. □

Remark. Daishiro pointed out that to use the First Isomorphism Theorem, we need to show that φ is surjective. This is problem **10.4** on the problem set.

We only have one more part of the Fundamental Theorem of Galois Theory remaining:

(5) Conjugation yields field isomorphisms. Given intermediate fields F, F' and subgroups H, H' such that $F \longleftrightarrow H$ and $F' \longleftrightarrow H'$ under the Galois Correspondence, then $F \simeq_K F'$ iff H and H' are conjugate subgroups.

Proof sketch. Subgroups H and H' are conjugate if and only if there exists some $\sigma \in G$ such that $H = \sigma H' \sigma^{-1}$. Therefore, by Lemma 1.1 it suffices to show that $F \simeq_K F'$ if and only if $\sigma(F) = F'$. The ($\Leftarrow$) direction is straightforward, since σ is a K-isomorphism. To prove the ($\Rightarrow$) direction, given $\varphi : F \xrightarrow{\sim} F'$, it suffices to prove that φ can be lifted to an automorphism $\sigma \in G$. This is a bit tedious to carry out and is quite similar to problem **9.6**, so we omit the details here. □

3. Minimal Polynomials

Let L/K be a finite Galois extension. From Geck's proof we know that this is a simple extension, and that there exists some primitive element for this extension whose minimal polynomial we can describe explicitly in terms of $\text{Gal}(L/K)$.

What about for some random $\alpha \in L$? What can we say about its Galois conjugates, or its minimal polynomial over K? Note that the Galois conjugates of a generic α might not all be distinct. After some discussion, Ben conjectured the following:

The Fundamental Lemma. Given any $\alpha \in L$, its minimal polynomial m_α over K is separable. Moreover, we can describe it explicitly:

$$m_\alpha(x) = \prod_{\beta \in A} (x - \beta)$$

where $A := \{\sigma(\alpha) : \sigma \in G\}$.

Proof. Problem **10.3**. □