GALOIS THEORY: LECTURE 18

LEO GOLDMAKHER

1. Proof of the Fundamental Theorem of Galois Theory

Last time we demonstrated the power of the FTGT by using it to give a short proof of the Fundamental Theorem of Algebra. Today we prove (most of) the FTGT itself. The main tools we use come from Geck's proof that $|\text{Aut}(L/K)| \leq [L : K]$, with equality iff L/K is Galois. We recall a few particularly useful consequences of his proof:

Proposition 1.1. *Given a finite Galois extension L/K, there exists some $\alpha \in L$ such that*

1. *$L = K(\alpha)$,*
2. *the Galois conjugates of α are all distinct, and*
3. *the minimal polynomial of α is given by $m_\alpha(x) = \prod_{\sigma \in \text{Aut}(L/K)} \big(x - \sigma(\alpha)\big)$.*

With these results in hand, we're ready to prove the FTGT. Recall (from Lecture 15) that the statement consists of five related results; we prove them in the same order we originally listed. Throughout, we assume L/K is a given finite Galois extension, and that $G := \text{Aut}(L/K)$ is the Galois group of this extension.

(1) The Galois Correspondence. The following two maps give bijections between the set of intermediate fields F lying between K and L and the set of subgroups H of G:

$$F \longmapsto \text{Aut}(L/F) \qquad\qquad L^H \longleftarrow\!\shortmid H.$$

Moreover, these maps are inverses of one another.

Proof. The plan of the proof is to reduce the problem to a simpler one, and then to apply a familiar trick involving minimal polynomials.

STEP 1. First reduction: it suffices to prove the maps are inverses.

Recall (problem **8.3**) that G is finite; it follows that there are only finitely many subgroups. Next, it's a general fact (see problem **10.1**) that given any two functions $f : A \to B$ and $g : B \to A$ which are inverses of one, then A and B have the same cardinality and f and g must be bijections. Thus, if we prove that the two maps given in the statement of the theorem are inverses of one another, it will immediately follow that the set of intermediate fields must be finite, and that each of the maps is a bijection. We have thus reduced the claim to proving

$$L^{\text{Aut}(L/F)} = F \qquad \text{and} \qquad \text{Aut}(L/L^H) = H.$$

STEP 2. Second reduction: it suffices to prove $|\text{Aut}(L/L^H)| \leq |H|$.

Recall (from Lecture 15) that L/F must be Galois. This implies (property (C) in the definition of being Galois) that the fixed field of $\text{Aut}(L/F)$ is precisely F, i.e. $L^{\text{Aut}(L/F)} = F$. It therefore suffices to prove $\text{Aut}(L/L^H) = H$.

Observe that $H \leq \text{Aut}(L/L^H)$, since any $\sigma \in H$ fixes everything in L^H by definition. Thus, it suffices to prove $\text{Aut}(L/L^H) \leq H$. In fact, since we know H is a finite subset of the automorphism group, it's enough to prove $|\text{Aut}(L/L^H)| \leq |H|$.

Date: April 24, 2018.

Based on notes by Eleanor Lustig.

STEP 3. Compute the degree of the extension L/L^H.

As in Step 2, we know that L/L^H must be Galois, whence $\text{Aut}(L/L^H) = [L : L^H]$. Thus our goal becomes to bound the degree of the extension L/L^H by the order of H. Proposition 1.1 gives us a more concrete way to think about this extension: since it's Galois, we deduce that $L = L^H(\alpha)$ for some α, and that the minimal polynomial of α over L^H is given by

$$m_\alpha(x) = \prod_{\sigma \in \text{Aut}(L/L^H)} \big(x - \sigma(\alpha)\big) \in L^H[x].$$

Since we're trying to prove that $\text{Aut}(L/L^H) = H$, we're led to consider the polynomial

$$f_\alpha(x) := \prod_{\sigma \in H} \big(x - \sigma(\alpha)\big).$$

We claim that $f_\alpha \in L^H[x]$, i.e. that its coefficients are fixed by every automorphism in H. Indeed, applying any element $\tau \in H$ to the set of roots $\{\sigma(\alpha) : \sigma \in H\}$ simply permutes the roots of f_α, hence leaves the coefficients of f_α unaffected (since they are symmetric polynomials in the roots).[1] Since $H \leq \text{Aut}(L/L^H)$, we deduce that $f_\alpha \mid m_\alpha$. On the other hand, we know m_α divides every polynomial in $L^H[x]$ with α as a root, whence $m_\alpha \mid f_\alpha$. Since both polynomials are monic, we deduce that $f_\alpha = m_\alpha$. In particular,

$$|\text{Aut}(L/L^H)| = [L : L^H] = \deg m_\alpha = \deg f_\alpha = |H|.$$

Since we know from step 2 that $H \leq \text{Aut}(L/L^H)$, we conclude that $H = \text{Aut}(L/L^H)$. □

It turns out this is by far the hardest part of the Fundamental Theorem to prove.

(2) The Galois correspondence is inclusion-reversing. Given $F \longleftrightarrow H$ and $F' \longleftrightarrow H'$ under the Galois correspondence, $F \subseteq F'$ if and only if $H \supseteq H'$.

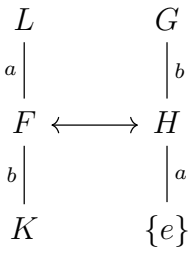
Proof. Suppose $F \subseteq F'$. Then any automorphisms that fix F' must also fix F, whence

$$H' = \text{Aut}(L/F') \subseteq \text{Aut}(L/F) = H.$$

Conversely, suppose $H' \subseteq H$. Then the elements of L that are fixed by all of H must be also be fixed by H', whence

$$F = L^H \subseteq L^{H'} = F'.$$ □

(3) Degrees are preserved under the Galois correspondence.



Given that $F \longleftrightarrow H$ under the Galois correspondence. Then

$[L : F] = |H|$ and $[F : K] = |G/H|$.

Proof. Recall that if L/K is Galois, then L/F is Galois, which implies that $[L : F] = |\text{Aut}(L/F)| = |H|$. Moreover, since L/K is Galois, we know that $[L : K] = |G|$. The Tower Law implies $[L : K] = [L : F][F : K]$ whence $|G| = |H|[F : K]$. The claim immediately follows. □

[1] This is similar in spirit to the trick we used in Lecture 16 to prove (C) $\implies$ (B).

2. Motivation for the next steps

Given L/K Galois, $G = \text{Gal}(L/K)$, and suppose $F \longleftrightarrow H$ under the Galois correspondence.

Question 1. *How can you form another intermediate field?*

(1) Alex: Adjoin an element of F to K.
(2) Eli: Adjoin an element of $L \setminus F$ to K or F.
(3) Ben: Pick any element $\sigma \in G$, and look at $\sigma(F)$.

Question 2. *How can you form another subgroup of G?*

(1) Michael: Form another field by an above method, and associate a group.
(2) Michael: Form a cyclic subgroup from an element of G.
(3) Isaac and Michael: We can form the *conjugate* of H: for any $\sigma \in G$, we have $\sigma H \sigma^{-1} \leq G$.

Next time we'll explore a connection between these: we'll show that the field and group formed in (3) of each of the above correspond under the Galois correspondence.