GALOIS THEORY: LECTURE 15

LEO GOLDMAKHER

1. Galois extensions and Galoisity

Recall that last class we "discovered" the following definition – which was something of a theorem. For simplicity, we write $G := \text{Aut}(L/K)$ throughout.

Definition. A finite extension L/K is *Galois* if and only if one of the following (equivalent) conditions are satisfied:

(A) $[L : K] = |G|$
(B) There exists some separable $f \in K[t]$ such that L is the splitting field of f.
(C) $\{x \in L : \sigma(x) = x \text{ for all } \sigma \in G\} = K$

Remark. The idea here is that an extension L/K is Galois if you don't lose *too* much information (or, rather, you lose precisely the right amount) going from L/K to $\text{Aut}(L/K)$. Our equivalent conditions quantify this.

Sets of the form appearing in part (C) will frequently arise, so it's worth introducing a nice notation for them.

Definition. Given $\sigma \in G$, let the *fixed field* of σ be

$$L^\sigma := \{x \in L : \sigma(x) = x\}.$$

We can extend this to collections of σ's: given $S \subseteq G$, the *fixed field of* S is

$$L^S := \{x \in L : \sigma(x) = x \,\forall \sigma \in S\}.$$

Remark. The term *fixed field* is more than just a cool-sounding name: we can verify that for any set S, L^S is an intermediate field lying between L and K.

Using this notation allows us to clean up the statement of part (C) in our definition of being Galois:
(C) $L^G = K$.
We will see that "Galois-ity" can be both quite annoying and quite nice:

Proposition 1.1. *Given $L/F/K$ a tower of finite extensions. Then*

1. *L/K is Galois $\not\Rightarrow$ F/K is Galois.*
2. *L/K is Galois $\Longrightarrow$ L/F is Galois.*
3. *L/F and F/K are both Galois $\not\Rightarrow$ L/K is Galois.*

Proof. We consider these in turn.

1. Consider $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Note that $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ is Galois, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ isn't. (It fails (A): $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, but $\mathbb{Q}(\sqrt[3]{2})$ has trivial automorphism group.)

2. Let L/K Galois. By condition (B), there exists some separable $f \in K[t]$ such that L is the splitting field of f. As f has coefficients in K, which is contained in F, so we can say that f has coefficients in F, and L remains the splitting field; by (B) L/F is Galois.

3. This appears on Problem Set 8. □

Date: April 12, 2018.
Based on notes by Beatrix Haddock.

We're now in a position to state the formal definition of the Galois group; it only took us eleven lectures since we first attempted to do so!

Definition (Galois group of an extension)**.** Given a finite Galois extension L/K, we call $\text{Aut}(L/K)$ the *Galois group* of the extension.

Definition (Galois group of a polynomial)**.** Given a polynomial $f \in K[t]$, let L/K be the splitting field of f. The *Galois group of f* is the Galois group of the extension L/K.

2. The Fundamental Theorem of Galois Theory

Recall that given a Galois extension, we noticed that the diagram of all intermediate fields is exactly the same as the diagram of all subgroups of the Galois group of the extension, just flipped upside down. This is remarkable. Most of the fields we've dealt with are infinite sets with complicated structure; for example, in Problem Set 7 you saw that even if it's straightforward to guess the intermediate fields between K and L, it can be rather difficult to prove that your list is exhaustive. By contrast, when L/K is a finite extension, then $\text{Aut}(L/K)$ is a finite group, and determining all its subgroups is therefore a finite, discrete problem which succumbs to brute force. (For example, one could write a computer program which does this.) Thus this bijective correspondence acts as a dictionary between the difficult language of fields and the much simpler language of finite groups.

We now formalize all our observations about the correspondence in the form of a single five-part theorem. Note that parts (1)–(3) can be guessed from our earlier work with the extension $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$, and that part (4) can be guessed from part (3). Thus the only aspect of this theorem which one needs to memorize is part (5); the rest are fairly intuitive.

Fundamental Theorem of Galois Theory. Given L/K a finite Galois extension, let G be its Galois group.

(1) The Galois Correspondence: There exists a one-to-one correspondence between the set of intermediate fields between L and K and the set of subgroups of G. In fact, we can explicitly describe a bijection from the set of intermediate fields to the set of subgroups:

$$F \longmapsto \text{Aut}(L/F).$$

We can also write down an explicit bijection in the reverse direction, from the set of subgroups to the set of intermediate fields:

$$H \longmapsto L^H \text{ (the fixed field of } H).$$

It turns out, remarkably, that these two bijections are inverses of one another. Thus, they both induce the same one-to-one correspondence; it is called the *Galois correspondence*.

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

(3) The degrees match up the way they should:

$$\begin{tikzcd}
L & G \\
F \arrow[u, dash, "a"] \arrow[r, leftrightarrow] & H \arrow[u, dash, "b"'] \\
K \arrow[u, dash, "b"] & \{e\} \arrow[u, dash, "a"']
\end{tikzcd}$$

Given that $F \longleftrightarrow H$ under the Galois correspondence. Then $[L : F] = |H|$ and moreover, $\text{Aut}(L/F) = H$. We also have $[F : K] = |{}^{G}/_{H}|$. Note that we *cannot* draw the conclusion the $\text{Aut}(F/K) = G/H$, for two reasons: (i) F/K might not be a Galois extension, and (ii) G/H might not be a group. It turns out these issues are secretly the same...

(4) Normal subgroups correspond to Galois extensions: F/K is Galois if and only if $H \trianglelefteq G$. Moreover, if this is the case, then $\mathrm{Aut}(F/K) \simeq G/H$.

(5) Conjugation yields field isomorphisms: Given intermediate fields F, $\widehat{F}$, and subgroups H, $\widehat{H}$ such that $F \longleftrightarrow H$ and $\widehat{F} \longleftrightarrow \widehat{H}$ under the Galois correspondence. Then $F \simeq_K \widehat{F}$ if and only if H and $\widehat{H}$ are conjugate (i.e. there exists $\sigma \in G$ such that $\sigma H \sigma^{-1} = \widehat{H}$). [Here the notation $F \simeq_K F'$ indicates that F and F' are *K-isomorphic*: there exists an isomorphism from F to F' which fixes every element of K.]

Remark. A crucial assumption in the Fundamental Theorem of Galois theory is that L/K is finite. However, a version of the theory can be developed in the case of infinite extensions. We leave this for another course.

3. Bounding the size of $\mathrm{Aut}(L/K)$: Geck's proof

Recall the first of the three equivalent criteria for being Galois: that $|\mathrm{Aut}(L/K)| = [L : K]$. What if L/K isn't Galois? Is there any relationship between these two quantities? It turns out that there is:

Proposition 3.1. *We have* $|\mathrm{Aut}(L/K)| \leq [L : K]$ *for any finite extension* L/K.

Our proof of this follows an elegant innovation by Meinolf Geck from 2014, which allows us to bypass the heavy machinery usually deployed in the proof of the Fundamental Theorem of Galois theory.

Proof. For brevity, set $G := \mathrm{Aut}(L/K)$. (Note, however, that G is not called the Galois group unless L/K is Galois.) We break the proof into three steps.

I. $L^\sigma = L$ if and only if $\sigma = e$.

If $\sigma = e$, then everything is fixed by σ, so $L^\sigma = L$. Conversely, if $L^\sigma = L$ then everything in L is fixed by σ, so σ must by definition be the identity map, e.

II. There exists $\alpha \in L$ such that $\sigma(\alpha) \neq \alpha$ for all $\sigma \in G \setminus \{e\}$.

From step **I**, we see that it suffices to prove

$$L \neq \bigcup_{\sigma \neq e} L^\sigma. \tag{1}$$

Since $|G| < \infty$ (see Problem Set 8), this is a finite union of proper subfields of L. Viewing L and all the L^σ as vector spaces over K, we see that (1) is a consequence of the following lemma from linear algebra:

Lemma 3.2. *A finite dimensional vector space over K can not be written as a union of finitely many proper subspaces.*

See problem set 8 for a proof of this result.

III. The degree of α lies between the degree of the extension and the order of $|G|$.

Note $[L : K] \geq [K(\alpha) : K] = \deg m_\alpha$. We know α is a root of m_α, which implies that all Galois conjugates of α, i.e. $\{\sigma(\alpha) : \sigma \in G\}$, are also roots of m_α. Since α is not fixed by any nontrivial automorphism (by step **II**), all of these roots are distinct. It follows that m_α has at least $|G|$ roots in L, so $\deg m_\alpha \geq |G|$. Combining this with our earlier bound, we deduce

$$|G| \leq \deg m_\alpha = [K(\alpha) : K] \leq [L : K]. \tag{2}$$

This concludes the proof. □

The above proof technique is very robust, in that it can be tweaked to give strong consequences. For example, with minimal effort it yields a very short proof that (A) $\Longrightarrow$ (B) in our list of equivalent conditions for being Galois:

Proposition 3.3. *If L/K is finite and $[L:K] = |\mathrm{Aut}(L/K)|$ then there exists some separable polynomial $f \in K[t]$ such that L is the splitting field of f.*

Proof. Set $G := \mathrm{Aut}(L/K)$, and pick $\alpha \in L/K$ as in the proof of Proposition 3.1 (so that α is moved by every nontrivial automorphism in G). If $[L:K] = |G|$ then (2) must be a chain of equalities, i.e.

$$|G| = \deg m_\alpha = [K(\alpha):K] = [L:K].$$

It follows that m_α has at most $|G|$ distinct roots. On the other hand, we know that the Galois conjugates $\{\sigma(\alpha) : \sigma \in G\}$ are a set of $|G|$ distinct roots of m_α, whence these must form a complete set of roots of m_α. We deduce that m_α splits in L (since the Galois conjugates all belong to L) and that m_α is separable (since the Galois conjugates are all distinct). Finally, Ian observed that $[K(\alpha):K] = [L:K]$ implies $L = K(\alpha)$, whence L is a splitting field of m_α. This concludes the proof. □

From the above proof we derive the following consequence for free:

Corollary 3.4. *Let L/K be a finite Galois extension. There exists $\alpha \in L$ such that $L = K(\alpha)$.*

Example 1. We saw before that $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ is a finite Galois extension. It follows that there is some number $\alpha \in \mathbb{Q}(\omega, \sqrt[3]{2})$ such that $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\alpha)$.

It turns out that the above is a special case of a much more general result:

Primitive Element Theorem (due to Emil Artin)**.** L/K has finitely many intermediate fields if and only if there exists $\alpha \in L$ such that $L = K(\alpha)$. In this case, L/K is called a *simple extension* and α is called a *primitive element* of the extension.

Remark. A finite extension of $\mathbb{Q}$ is called a *number field*; these play a fundamental role in algebraic number theory. It can be shown that a number field only has finitely many subfields, whence the Primitive Element Theorem implies that any number field K can be written in the form $K = \mathbb{Q}(\alpha)$ for some complex number α.