30 Main Theorem of Galois Theory

Last class, we introduced the main theorem:

Theorem 30.1
If E/F is a Galois extension (i.e. $|\mathrm{Gal}(E/F)| = [E : F]$), then intermediate subfields $F \subset K \subset E$ are in bijection with subgroups $H \subset G$, where a subgroup H is mapped to its **fixed field** E^H, and a subfield K is mapped to the set of $g \in G$ which fix all elements of K.

Recall that E/F is Galois if and only if E is a splitting field of some polynomial (and is separable).

30.1 Examples of Galois Groups

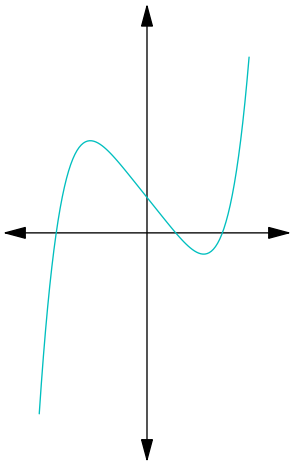
Last class, we saw the following example:

Example 30.2
If $F = \mathbb{Q}$ and $E = \mathbb{Q}(\zeta)$, where ζ is a pth root of unity for p prime, then $\mathrm{Gal}(E/F) = (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

This is an example where the Galois group is as small as possible (given the degree of the polynomial). Meanwhile, we also saw an example in the opposite direction:

Example 30.3
If $P \in \mathbb{Q}[x]$ is irreducible, has degree p (for p prime), and has exactly $p-2$ real roots, then if E is its splitting field, we have $\mathrm{Gal}(E/F) = S_p$.

It's easy to write down such a polynomial. For example, $P(x) = 2x^5 - 10x + 5$ is irreducible by Eisenstein's criterion, while by graphing (or by computing its derivative) we can see that it has three real roots.



Proof. The proof is based on a lemma about the symmetric group:

Lemma 30.4
Suppose p is prime, and $G \subset S_p$ such that G acts on $[1, \dots, p]$ transitively, and G contains a transposition (ij). Then $G = S_p$.

First we'll show how the lemma implies that $\mathrm{Gal}(E/F) = S_p$ in our example: if we let $G = \mathrm{Gal}(E/F)$, then we know G acts (by permutations) on the p roots. We know that since P is irreducible, this action is transitive (we can send any root to any other root, which we proved by comparing the abstract procedure of adjoining a root to the procedure of adjoining a specific root).

Meanwhile, complex conjugation permutes the roots of P, so $E = \mathbb{Q}(\alpha_1, \dots, \alpha_p)$ is invariant under complex conjugation — this means it's an element in the Galois group. This element clearly permutes the two non-real, and fixes the real roots; so it is a transposition.

We'll now prove the group-theoretic lemma.

Proof of Lemma 30.4. Since G acts transitively on $[1, \dots, p]$, it follows that $p \mid |G|$; so by the Sylow Theorems, G has an element of order p, which we denote by σ. Recalling the description of elements of S_p using cycle notation, we can see that the only element of order p is a long cycle (meaning a cycle of all p elements), so σ is a long cycle.

Now recall that G also contains a transposition, which we can without loss of generality assume is (12).

Now we can find some $1 \leq i < p$ such that σ^i sends $1 \mapsto 2$ (since we can follow the arrows from 1 until we reach 2). But since $i < p$, the order of $\gamma = \sigma^i$ is also p; so γ is also a long cycle.

Now G contains (12) and γ, which we can without loss of generality assume is $(123 \cdots p)$. Now recalling how conjugation in the symmetric group works (by essentially taking the same cycles, but substituting different elements into them), we have

$$\gamma(12)\gamma^{-1} = (23),\ \gamma^2(12)\gamma^{-1} = (34),\ \dots.$$

So then G contains all the standard transpositions (12), (23), (34), ... (which transpose two consecutive elements). It's a standard fact about the symmetric group that these transpositions generate S_p (given any permutation, we can swap consecutive elements to eventually sort it), so $G = S_p$. □

This shows that $\mathrm{Gal}(E/F) = S_p$, as desired. □

Student Question. *How did we show that $p \mid |G|$ in the proof of the lemma?*

Answer. *If G acts on X transitively, then we have the formula*

$$|G| = |X| \cdot |\mathrm{Stab}_G\, x|$$

for any $x \in X$. To show this, we can break the elements of G into subsets based on where they send a given point x; there will be $|X|$ groups, and each group will have $|\mathrm{Stab}_G\, x|$ elements.

Student Question. *Is the Galois group always a transitive subgroup of S_n?*

Answer. *The Galois group is always a subgroup of S_n (since it always permutes the roots of the polynomial). It's always transitive if the polynomial is irreducible, but the polynomial doesn't have to be irreducible in general (we can consider the splitting field of* any *polynomial).*

Student Question. *Does this work when there's more than two complex roots? Or does the Galois group become smaller than S_n?*

Answer. *The particular trick used in this argument doesn't work. But if you write a random polynomial, its Galois group should be S_n — for the group to be smaller, you'd need some condition on the roots.*

Note 30.5

A similar argument can be used to produce an extension of the rational function field $F = \mathbb{C}(t)$ with Galois group S_n, for n prime.

Earlier, we saw a ramified covering $X \to Y = \mathbb{C}$, where X is the zero set of a polynomial $P(t, x) \in F[x]$. The analog of our conditions here becomes that there should be one *simple* ramification point (meaning that at this ramification point y_0, there are $n-1$ pre-images $x_1, \dots, x_{n-1}$; f is an isomorphism at $x_2, \dots, x_{n-1}$, while at x_1, f looks (locally) like the map $z \mapsto z^2$.

Then if E is the splitting field of P, we can show $\mathrm{Gal}(E/F) = S_n$ in a similar way — P is assumed to be irreducible, and the condition on ramification ensures that the Galois group contains a transposition.

30.2 Proof of Main Theorem

We'll now prove the theorem.

Lemma 30.6

Both maps in the correspondence send $[E : K]$ to $|H|$.

Note that in the tower of extensions $E/K/F$, we're looking at the degree of the *top* extension E/K, rather than the bottom one K/F.

Proof. One direction is clear — if we start with a subfield K, the corresponding subgroup is $\mathrm{Gal}(E/K)$ (we can forget that F exists, and just look at the extension E/K — then we've defined the corresponding subgroup as the automorphisms of E which fix K, which is just this Galois group). But we know E is a splitting field over K (if E is the splitting field of a polynomial over F, then it's also the splitting field of the same polynomial over K). So then $|\mathrm{Gal}(E/K)| = [E : K]$. To prove the other direction, fix a subgroup $H \subset G$, and consider its fixed field $K = E^H$; we want to show that $[E : E^H] = |H|$.

First, by definition H is a subgroup of $\mathrm{Gal}(E/E^H)$, which means

$$|H| \leq |\mathrm{Gal}(E/E^H)| = [E : E^H].$$

So it suffices to show the other direction of this inequality, meaning that $[E : E^H] \leq |H|$.

Let $|H| = n$. By the Primitive Element, we know $E = E^H(\alpha)$ for some α. So it's enough to check that α is a root of some polynomial in $E^H[x]$ of degree n.

We now apply a version of the averaging trick we saw earlier. Set

$$P(x) = \prod_{g \in H} (x - g(\alpha)).$$

(For example, if $E = \mathbb{C}$ and H consisted of the identity and complex conjugation, this would give $(x-z)(x-\overline{z})$.)

This polynomial starts its life as a polynomial in $E[x]$, but it actually has coefficients in E^H — to see this, observe that the action of any $h \in H$ just permutes the factors g from P (since $hH = H$ for any $h \in H$). So P is a degree n polynomial in $E^H[x]$ with α as a root, which shows that $[E : E^H] \leq n$, as desired. □

Proof of Main Theorem. Once we have the equality of degrees, the remaining part is essentially just formal — suppose $H \to E^H \to H'$. By definition we know $H \subset H'$; but the lemma implies $|H| = |H'|$, so $H = H'$. Similarly, if $K \to H \to K'$, then $K' \supset K$ (since K' consists of all elements fixed by H, but H is defined as the set of elements which fix K). But $[E : K] = [E : K']$, so then $K = K'$. □

30.3 Properties of the Correspondence

Note that the correspondence *reverses* inclusion — the larger the group, the smaller its fixed field (each element of the group gives a condition on the elements of the field; if there are more conditions, fewer elements will satisfy them).

Consider the tower of extensions $E/K/F$. By definition, the extension E/K is always Galois (we have $[E : K] = |H| = |\mathrm{Gal}(E/K)|$). On the other hand, K/F may or may not be a Galois extension.

Proposition 30.7
The extension K/F is Galois if and only if K is invariant under all $g \in \mathrm{Gal}(E/F)$, which happens if and only if the corresponding $H \subset G$ is normal. In that case, $\mathrm{Gal}(K/F) = G/H$.

Proof. First we'll prove K/F is Galois if and only if K is invariant under all $g \in G = \mathrm{Gal}(E/F)$.

If K/F is Galois, then it's a splitting field. Every $g \in \mathrm{Gal}(E/F)$ has to permute the roots of any polynomial in $F[x]$; this means $G : K \to K$ (since K is generated by the roots of some such polynomial).

Meanwhile, if K is invariant under all $g \in G$, then we have a homomorphism $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ by restricting the automorphisms to K (since they are automorphisms of K as well). The kernel of this homomorphism is $\mathrm{Gal}(E/K)$. So by the homomorphism theorem, the image of this homomorphism has cardinality

$$\frac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/K)|} = \frac{[E : F]}{[E : K]} = [K : F].$$

We saw that we must have $|\mathrm{Gal}(K/F)| \leq [K : F]$, so then equality must hold, and K/F is Galois.

We've now shown that K/F is Galois if and only if K is invariant under G; so now it suffices to show that K is invariant if and only if H is normal. But it's clear that if H corresponds to $K = E^H$, then gHg^{-1} corresponds to $g(K)$. So K is invariant under all $g \in G$ if and only if $gHg^{-1} = H$ for all $g \in G$, meaning H is normal. $\square$

Student Question. *Why does gHg^{-1} correspond to $g(K)$?*

Answer. *This is because an element γ fixes x if and only if $g\gamma g^{-1}$ fixes $g(x)$.*

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng