29 Galois Theory

29.1 Review: Primitive Element Theorem

Last class, we proved the Primitive Element Theorem:

Theorem 29.1
If E/F is a finite separable extension, then $E = F(\alpha)$ for some α.

Example 29.2
Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$. Then all but finitely many linear combinations $\alpha = r\sqrt{3} + \sqrt[3]{7}$ (with $r \neq 0$) generate E. The exceptions correspond to ratios $r = (\beta_i - \beta_j)/(\alpha_k - \alpha_\ell)$, where we take a different square root of 3 or cube root of 7. In this case, such r are not even real, so they are certainly not rational; and there are no exceptions.

Recall that an extension is separable if the minimal polynomial of any $\alpha \in E$ has nonzero derivative, or equivalently, has no multiple roots. All extensions are separable when working in characteristic 0 or with finite fields; more generally, separability is sometimes true and sometimes not. But we will only work with characteristic 0 and finite fields in this class, so we will assume all extensions are separable.

29.2 The Galois Group

Our main object of study is the Galois group:

Definition 29.3
The **Galois group** of an extension E/F, denoted $\mathrm{Gal}(E/F)$, is the group of automorphisms of E which are the identity on F.

Example 29.4
The Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ consists of two elements — the identity and complex conjugation.

The Galois group can store a lot of information about the structure of the field extension. But it only works well for *some* classes of extensions — we'll see that the extensions for which it works well are exactly the splitting fields. For this reason, we'll look at one more preliminary result, which is somewhat surprising:

Theorem 29.5
Suppose that E/F is a splitting field of some polynomial. Then for *any* $\alpha \in E$, the minimal polynomial of α must split completely (into linear factors) in E.

Example 29.6
Take $F = \mathbb{Q}$, and E to be the splitting field of $x^5 - 2$; then $E = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. By the Primitive Element Theorem, it's generated by one element $\alpha = \sqrt[5]{2} + \zeta_5$. We know ζ_5 has degree 4 over $\mathbb{Q}$ and $\sqrt[5]{2}$ has degree 5, and $x^5 - 2$ remains irreducible even after adjoining a fifth root of unity; so $[E : \mathbb{Q}] = 20$. Then the minimal polynomial of α over $\mathbb{Q}$ has degree 20.

The theorem then states that all 20 complex roots of this minimal polynomial are inside E. We can actually explicitly describe these roots — they're of the form $\sqrt[5]{2}\zeta_5^i + \zeta_5^j$ for some integers $0 \leq i \leq 4$ and $1 \leq j \leq 4$ (by varying our choice of fifth root of 2 and primitive 5th root of unity), which are indeed in E.

Proof of Theorem 29.5. The proof is somewhat abstract; we'll deduce this theorem from the uniqueness of the splitting field.

Suppose E is the splitting field of some polynomial Q, and fix $\alpha \in E$ with minimal polynomial P; then we want to show that P splits completely in E.

Let $K \supset E$ be a field where P splits completely (for example, the splitting field for P over E). Then in K, we have

$$P(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $\alpha_i \in K$ for all i and $\alpha_1 = \alpha$. We need to check that $\alpha_i \in E$ for all i (and we already know $\alpha \in E$).

But we have that $F(\alpha_i) \cong F(\alpha)$, since α_i and α have the same minimal polynomial. Now consider E from the perspective of these two intermediate fields. We know that E is the splitting field for Q over $F(\alpha)$. We don't yet know whether α_i is in E or not, but we know that if we adjoin it, then $E(\alpha_i)$ is the splitting field for Q over $F(\alpha_i)$ — this is clear from the definition of the splitting field (the polynomial clearly splits in $E(\alpha_i)$, but E is generated over F by the roots of P; so $E(\alpha_i)$ is generated over $F(\alpha_i)$ by the roots of P as well).

But by the uniqueness of the splitting field, there exists an isomorphism $E \cong E(\alpha_i)$ extending the isomorphism $F(\alpha) \cong F(\alpha_i)$ (we've identified $F(\alpha)$ and $F(\alpha_i)$, and since Q has coefficients in F (which is preserved by the isomorphism), it's the same polynomial in both fields — the isomorphism takes one copy of Q to the other). Since our isomorphism is the identity on F, this means

$$[E : F] = [E(\alpha_i) : F],$$

and since $E(\alpha_i) \supset E$, this means we must have $E(\alpha_i) = E$, and therefore $\alpha_i \in E$. □

Student Question. *How did we show $E(\alpha_i)$ is the splitting field of Q over $F(\alpha_i)$?*

Answer. *More explicitly, we can suppose $E = F(\beta_1, \ldots, \beta_n)$, where the β_j are the roots of Q. Then $E(\alpha_i)$ is obtained by adjoining $\beta_1, \ldots, \beta_n$ as well as α_i. But we can also adjoin these in a different order, as $E(\alpha_i) = F(\alpha_i)(\beta_1, \ldots, \beta_n)$. So as an extension of $F(\alpha_i)$, it's generated by the roots of Q.*

Now we can get to some interesting results.

Proposition 29.7
For any finite (separable) extension E/F, we have

$$|\mathrm{Gal}(E/F)| \leq [E : F],$$

with equality if and only if E is the splitting field of some polynomial.

Example 29.8
We saw earlier that $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$. Meanwhile, it's a degree 2 extension, and it's the splitting field of $x^2 + 1$.

Proof of Proposition 29.7. Using the Primitive Element Theorem, we can let $E = F(\alpha)$ for some α. Then

$$[E : F] = \deg(\alpha) = \deg P,$$

where P is the minimal polynomial of α.

Meanwhile, an automorphism $\sigma : E \to E$ which fixes F is clearly uniquely determined by $\sigma(\alpha)$ (since α generates the extension), so it suffices to find the number of possible choices for $\sigma(\alpha)$. But $\sigma(\alpha)$ can be any root of the minimal polynomial of α; so $|\mathrm{Gal}(E/F)|$ is equal to the number of roots of P in E.

The number of roots of P in E is at most $\deg P$, which immediately proves

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

If equality holds, then P must split completely in E; this immediately implies that E is the splitting field of P (since E is also generated by a root α of P).

On the other hand, if E is a splitting field, then by Theorem 29.5, P must split completely in E. Since P cannot have multiple roots (by separability), this means it has exactly $\deg P$ roots in E, and therefore there are exactly $\deg P$ automorphisms. □

Student Question. *Was the condition that E/F is separable only used to show that P does not have multiple roots?*

Answer. *We also used it when using the Primitive Element Theorem; but in fact, it's not necessary to rely on the Primitive Element Theorem for that step, and* $|\mathrm{Gal}(E/F)| \leq [E:F]$ *is always true (it's possible to induct on the number of generators instead). So it's possible to avoid assuming separability there, but it* is *necessary for the last step.*

Definition 29.9
A finite extension E/F is **Galois** if $[E:F] = |\mathrm{Gal}(E/F)|$.

29.3 Main Theorem

The main theorem we will discuss is the following:

Theorem 29.10
If E/F is a Galois extension with Galois group $\mathrm{Gal}(E/F)$, then there is a bijection between subgroups of G, and intermediate subfields $F \subseteq K \subseteq E$ — where a subgroup $H \subset G$ is mapped to its **fixed field**

$$K = E^H = \{x \in E \mid \sigma(x) = x \text{ for all } \sigma \in H\},$$

and a subfield K is mapped to the set of $\sigma \in G$ which fix all elements of K (which by definition is $\mathrm{Gal}(E/K)$).

This bijection has many properties. For now, note that E/K is still a Galois extension, so if $H \mapsto K_H$, then $|H| = [E : K_H]$.

Student Question. *Can any finite group be a Galois group?*

Answer. *Yes, although whether any finite group can be a Galois group over* $\mathbb{Q}$ *is still open. We'll later discuss how to construct an extension with* S_n *as its Galois group, and any finite group is a subgroup of some* S_n*.*

We will discuss the proof and some applications later; first, we will discuss how to compute the Galois group in a few examples (there is no *general* easy answer).

29.4 Examples of Galois Groups

For a polynomial P with splitting field E (over F), we use $\mathrm{Gal}(P)$ to refer to $\mathrm{Gal}(E/F)$.

It's not easy to compute the Galois group — it's not even easy to compute the *degree* of the extension. One observation we can make is that G acts faithfully on the roots of P (meaning it permutes these roots). There is a bit more we can say:

Proposition 29.11
If P is irreducible, this action is transitive — any root can be sent to any other root.

Proof. Write $P(x) = (x - \alpha_1) \cdots (x - \alpha_n)$; then we want to show that for any i and j, there exists $\sigma \in \mathrm{Gal}(P)$ such that σ sends $\alpha_i \mapsto \alpha_j$.

But we know $F(\alpha_i) \cong F(\alpha_j)$ (since α_i and α_j have the same minimal polynomial). Further (similarly to the argument we used in the proof of Theorem 29.5), E is the splitting field of P over both $F(\alpha_i)$ and $F(\alpha_j)$. So by the uniqueness of the splitting field, the isomorphism between $F(\alpha_i)$ and $F(\alpha_j)$ extends to an isomorphism $\sigma : E \to E$ which sends $\alpha_i \mapsto \alpha_j$. □

However, this is pretty much everything we can say in general — even knowing that $\mathrm{Gal}(P)$ acts transitively on a set of n elements, its size can range from n to $n!$.

Example 29.12
Let $F = \mathbb{Q}$, and $E = \mathbb{Q}(\zeta_n)$ where $\zeta_n = \exp(2\pi i/n)$. For simplicity, assume $n = p$ is prime.

Solution. Let $\zeta = \zeta_p$. We proved earlier that $[E:F] = p - 1$, and E is the splitting field of $x^{p-1} + x^{p-2} + \cdots + 1$.

Any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ must send $\zeta \mapsto \zeta^i$ for some $1 \leq i \leq p-1$ (since every root of unity is some power of ζ). Denote this automorphism by σ_i.

In order to compute the group, it suffices to understand how these automorphisms compose — we have

$$\sigma_i \sigma_j(\zeta) = \sigma_i(\zeta^j) = \zeta^{ij},$$

which means $\sigma_i \sigma_j = \sigma_{ij}$. So in this case, we have

$$\mathrm{Gal}(E/F) = (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}. \qquad \square$$

In this case, we were lucky because all roots of the polynomial were powers of one root ζ. In general, after fixing one root and sending it to another root, we still need to figure out what we can do with the remaining roots (which is forced by the algebraic relations between the roots).

Student Question. *The main theorem relates the subgroups of G to fixed fields; are there any interesting properties of the relations here?*

Answer. *We'll discuss that more next class — but using this result, you can actually solve the compass and ruler problem, which we'll discuss next time.*

This is an example of a case where the Galois group is as small as possible. There are also examples where the Galois group is as *big* as possible:

Example 29.13
Let P be an irreducible polynomial over $\mathbb{Q}$ of degree n, and suppose that P has exactly $n-2$ real roots, and 2 roots which are complex conjugates. Also suppose that $n = p$ is prime. Then if E is the splitting field of P, we have

$$\mathrm{Gal}(E/\mathbb{Q}) = S_n.$$

Proof Sketch. We'll just discuss the outline today, and prove this in more detail next time. The proof relies on an algebraic lemma — if $G \subset S_n$ where n is prime, and G contains a transposition (i, j) and a long cycle, then $G = S_n$. Here the transposition is given by complex conjugation, and the long cycle comes from the fact that the Galois group permutes the roots transitively, so its order divides $\deg P = p$; by Sylow's Theorems it must then contain an element of order p, and the only such element is a long cycle. $\square$

MIT OpenCourseWare
https://ocw.mit.edu

Resource: Algebra II Student Notes

Spring 2022

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

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.