Galois Theory, Part 1: The Fundamental Theorem of Galois Theory

Jay Havaldar

3.1 Introduction

Beginning with a polynomial $f(x)$, there exists a finite extension of F which contains the roots of $f(x)$. Galois THeory aims to relate the group of permutations fo the roots of f to the algebraic structure of its splitting field. In a similar way to representation theory, we study an object by how it acts on another.

Definition: An isomorphism σ of K with itself is called an automorphism of K. The collection of automorphism K is denoted $Aut(K)$.

Definition: If F is a subset of K (like a subfield), then an automorphism σ is said to fix F if it fixes every element of F.

Note that any field has at least one automorphism: the identity map, called the trivial automorphism.

Note that the prime subfield is generated by 1, and since any automorphism sends 1 to 1, any automorphism of a field fixes its prime subfield. For example, $\mathbb{Q}$ and $\mathbb{F}_p$ have only the trivial automorphism.

Definition: Let K/F be an extension of fields. Then, $Aut(K/F)$ is the collection of automorphisms of K which fix F.

Note that the above discussion gives us that $Aut(K) = Aut(K/F)$, if F is the prime subfield. Note that under composition, there is a group structure on automorphisms.

Proposition 1

$Aut(K)$ is a group under composition and $Aut(K/F)$ is a subgroup.

Proposition 2

Let K/F be a field extension, and $\alpha \in K$ algebraic over F. Then for any $\sigma \in Aut(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α. In other words, $Aut(K/F)$ permutes the roots of irreducible polynomials.

Suppose that α satisfies the equation:

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

Where $c_i \in F$. Then apply the automorphism σ to obtain:

$$(\sigma\alpha)^n + c_{n-1}(\sigma\alpha)^{n-1} + \cdots + c_0 = 0$$

And thus, $\sigma\alpha$ is a root of the same polynomial over F as α.

In general, if K is generated over F by some elements, then an automorphism is completely determined by its action on the generators.

In particular, if K/F is finite, then it is finitely generated over F by algebraic elements. In this case, the number of automorphisms fixing F is finite, and $Aut(K/F)$ is a finite group. In this case, the automorphisms of a finite extension are permutations of the roots of a finite number of equations (though not every permutation necessarily gives an automorphism).

We have described a field associated to each extension; we now reverse the process.

Proposition 3

> Let $H \leq Aut(K)$ be a subgroup of $Aut(K)$. The collection of all elements F of K which are fixed by H is a subfield.

This follows from readily from the definition of an field isomorphism.

Note here that we do not necessarily need a subgroup, but just a subset of K.

Proposition 4

> The above association is inclusion reversing: - If $F_1 \subseteq F_2 \subseteq K$ then $Aut(K/F_2) \leq Aut(K/F_1)$. - If $H_1 \leq H_2 \leq Aut(K)$ are two subgroups of automorphisms with fixed fields F_1 and F_2 then $F_2 \subseteq F_1$.

It maybe should be clear here that we are heading towards a bijection of some sort. We begin by investigating the size of the automorphism group of a splitting field.

Let F be a field and let E be the splitting field over F of $f(x)$. We know that we can extend an isomorphism $\varphi : F \to F'$ to an isomorphism $\sigma : E \to E'$, where E' is the splitting field over F' of $f'(x)$.

We now show that the number of such extensions is at most $[E : F]$, with equality if f is separable over F. We proceed by induction. If $[E : F] = 1$, then $E = F$ and there is only one extension (the identity).

If $[E : F] > 1$, then $f(x)$ has at least one irreducible factor $p(x)$ of degree greater than 1 which maps to $p'(x)$. Fix α, a root of $p(x)$. Then, if σ is any extension of φ to E, then σ restricted to $F(\alpha)$ is an isomorphism τ which maps $F(\alpha)$ to $F'(\beta)$, where β is a root of $p'(x)$. We have the two extensions:

$$\sigma : E \to E'$$
$$\tau : F(\alpha) \to F'(\beta)$$
$$\varphi : F \to F'$$

Now conversely, say β is a root of $p'(x)$. Then we can by the same process construct such a diagram.

Counting the number of extensions σ of φ is now counting the number of diagrams.

To extend φ to τ is to count the number of distinct roots β of $p'(x)$. Since $p(x)$ and $p'(x)$ both have degree $[F(\alpha) : F]$, the number of extensions of φ to τ is at most $[F(\alpha) : F]$, with equality if the roots are distinct.

Now, since E is the splitting field of f over $F(\alpha)$ and E' is the splitting field of f' over $F'(\beta)$, and by hypothesis $[E : F(\alpha)] < [E : F]$, we apply the induction hypothesis to say that the number of extensions of τ to σ is at most $[E : F(\alpha)]$, with equality if f has distinct roots.

Finally, since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that the number of extensions of φ to σ is at most $[E : F]$, with equality if $f(x)$ has distinct roots.

In particular, when $F = F'$ and φ is the identity map, the isomorphisms σ are exactly the automorphisms of E fixing F.

Corollary 1

Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then:

$$|Aut(E/F)| \leq [E : F]$$

With equality if $f(x)$ is separable over F.

Therefore, the splitting field of a separable polynomial is exactly the ``bijective'' correspondence we are looking for, in which $[E : F] = |Aut(E/F)|$.

Definition: Let K/F be a finite extension. Then K is said to be **Galois** over F and K/F is a Galois extension if $|Aut(E/F)| = [K : F]$. The group of automorphisms is called the Galois group of K/F, denoted $Gal(K/F)$.

Corollary 2

If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

We will see that the converse is also true.

Note also that this tells us that the splitting field of any polynomial over $\mathbb{Q}$ is Galois, since the splitting field of a polynomial is the same as the one obtained by removing multiple factors, which is separable.

Definition: If $f(x)$ is a separable polynomial over F, then the Galois group of f over F is the Galois group of the spliting field of $f(x)$ over F.

3.2 The Fundamental Theorem of Galois Theory

Definition: A character of a group G with values in a field L is a homomorphism from G to the multiplicative group $L^{\times}$.

Definition: The characters $\chi_1, \chi_2, \ldots, \chi_n$ are linearly independent if they are linearly independent functions on G.

Theorem 1

If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G, then they are linearly independent.

Now, consider an injective homomorphism σ of a field K into a field L, which is called an embedding of K into L. In particular, σ can be viewed as a character of $K^{\times}$ with values in L.

Corollary 3

If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings of K into L, then they are linearly independent as functions on K. In particular, the distinct automorphisms of a field K are linearly independent as functions on K.

Theorem 2

Let $G = \sigma_1, \ldots \sigma_n$ be a subgroup of automorphisms of a field K and let F be its fixed field. Then:

$$[K : F] = n = |G|$$

This proof will be omitted; it follows from analyzing systems of equations.

Corollary 4

Let K/F be any finite extension. Then:

$$|Aut(K/F)| \leq [K : F]$$

With equality iff F is the fixed field of $Aut(K/F)$. This tells us that K/F is Galois iff F is the fixed field of $Aut(K/F)$.

To prove this, let F_1 be the fixed field of $Aut(K/F)$. In other words:

$$F \subseteq F_1 \subseteq K$$

By Theorem 2, we have:

$$[K : F_1] = |Aut(K/F)|$$

Hence, we have:

$$[K : F] = |Aut(K/F)|[F_1 : F]$$

And this proves the corollary.

Corollary 5

Let G be a finite subgroup of automorphisms of a field K and let F be its fixed field. Then every automorphism of K fixing F is contained in G, i.e.:

$$Aut(K/F) = G$$

Therefore, K/F is Galois, with Galois group G.

Note that by definition $G \leq Aut(K/F)$. But by the theorem we have $|G| = [K : F]$. By the previous corollary we have $|Aut(K/F)| \leq [K : F] = |G|$. This gives:

$$[K : F] \leq |Aut(K/F)| \leq [K : F]$$

And therefore, if we have a subgroup of automorphisms, then K is a Galois extension over its fixed field.

Corollary 6

> If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K, then their fixed fields are also distinct.

If the fixed fields $F_1 = F_2$, then by definition F_1 is fixed by G_2. But then $G_2 \neq G_1$, and similarly $G_1 \leq G_2$ adn thus the two groups are equal.

The corollaries above tell us that taking fixed field for distinct finite subgroups of $Aut(K)$ gives distinct subfields of K over which K is Galois. The degrees of the extensions are given by the orders of the subgroups.

The next result completely characterizes Galois extensions.

Theorem 3

> The extension K/F is Galois iff K is the splitting field of some separable polynomial over F. If this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K (K/F is in particular separable).

We showed earlier that the splitting field of a separable polynomial is Galois. We now show, essentially, the converse.

Let $G = Gal(K/F)$ and let $\alpha \in K$ be a root of $p(x)$, an irreducible polynomial in $F[x]$ which has a root in K. Consider the elements:

$$\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha) \in K$$

Where σ_i represent the elements of the Galois group. Of this list, denote the distinct elements by:

$$\alpha, \alpha_2, \ldots, \alpha_r$$

If $\tau \in G$ then since G is a group applying τ to the first list just permutes it. In particular, teh following polynomial has coefficients which are fixed by all the elements of G:

$$f(x) = (x - \alpha)(x - \alpha_2) \ldots (x - \alpha_r)$$

The coefficients thus lie in the fixed field of G. However, note that K/F is Galois iff F is the fixed field of $Aut(K/F)$, so the fixed field of G is exactly F. Thus, $f(x) \in F[x]$.

Since $p(x)$ is irreducible and has α as a root, $p(x)$ is the minimal polynomial for α over F, and it follows that $p(x)$ divides $f(x)$ in $F[x]$. So we have:

$$p(x) = f(x)$$

This shows that $p(x)$ is separable and all its roots lie in K.

To complete the proof, suppose K/F is Galois and let $\omega_1, \ldots, \omega_n$ be a basis for K/F. let $p_i(x)$ be the minimal polynomial for ω_i. Then $p_i(x)$ is separable and has all its roots in K. Let $g(x)$ be the polynomial obtained by removing multiple factors in this product. Then the splitting field of the two polynomials is the same and this field is K. Hence, K is the splitting field of the separable polynomial $g(x)$.

Definition: Let K/F be a Galois extension. If $\alpha \in K$ then the elements $\sigma\alpha$ for $\sigma \in Gal(K/F)$ are called the Galois conjugates of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the conjugate field of E over F.

The proof of Theorem 3 shows that in a Galois extension K/F, if we have $\alpha \in K$ which is a root of a minimal polynomial over F, then the other roots are precisely the distinct conjugates of α under the Galois group of K/F.

The theorem also says that K is not Galois over F if we can find an irreducible polynomial over F which has a root in K but not all its roots in K. Now we have four characterizations of Galois extensions K/F:

- Splitting fields of separable polynomials over F.
- Fields where F is precisely the fixed field of $Aut(K/F)$ (in general, the fixed field may be larger than F).
- Fields with $[K : F] = |Aut(K/F)|$.
- Finite, normal, and separable extensions.

Theorem (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and let $G = Gal(K/F)$. Then there is a bijection between subfields:

$$F \subseteq E \subseteq K$$

And subgroups of the Galois group:

$$1 \subseteq H \subseteq G$$

In particular, the correspondence identifies E to the elements of G which fix E. Conversely, it identifies H with the fixed field of H. - The correspondence is inclusion reversing. - $[K : E] = |H|$, and $[E : F] = [G : H]$. - K/E is always Galois, with Galois group $Gal(K/E) = H$. - E is Galois over F iff H is a normal subgroup in G. If this is the case then $Gal(E/F) \cong G/H$. More generally, the isomorphisms of E which fix F correspond with cosets of H in G. - If E_1, E_2 correspond to H_1, H_2, then the intersection $E_1 \cap E_2$ corresponds to the group generated by H_1, H_2. The composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$.

We will number these points 1 through 5 and prove each separately.

Part 1

Given any subgroup H of G, we saw that there is a unique fixed field $E = K_H$. The correspondence is thus injective from subgroups to subfields. We now need to see that it is surjective, i.e. we can find a subgroup of the Galois group which fixes any subfield.

Now, if K is the splitting field of a separable polynomial $f(x) \in F[x]$ then it is an element of $E[x]$ for any subfield $F \subseteq E \subseteq K$. Thus, K is also the splitting field of f over E, and therefore K/E is Galois. Thus, E is the fixed field of $Aut(K/E) \leq G$. This shows that indeed our correspondence is bijective. Concretely, the automorphisms fixing E are precisely $Aut(K/E)$ since K/E is Galois.

The Galois correspondence is evidently inclusion reversing.

Part 2 If $E = K_H$ is the fixed field of H (which is Galois), then by Theorem 2 $[K : E] = |H|$, and similarly $[K : F] = |G|$. Taking the quotient gives $[E : F] = [G : H]$.

Part 3 Since E is the fixed field of a subgroup $H \leq G$, by Corollary 5, K/E is Galois with Galois group $Gal(K/E) = H$.

Part 4

Lemma

> Let E be the fixed field of a subgroup H. Then σ is an embedding of E iff it is the restriction of some automorphism $\sigma \in G$ to E.

Let $E = K_H$ be the fixed field of the subgroup H. Then every $\sigma \in G$, when restricted to E, gives an embedding of E with a subfield $\sigma(E)$ of K. We shall show that these are indeed the only embeddings of E.

Conversely, let $\tau : E \to \tau(E) \subseteq \overline{F}$ be any embedding of E (into a fixed algebraic closure $\overline{F}$ containing K) which fixes F. Then, if $\alpha \in E$ has minimal polynomial m_α over F then $\tau(\alpha)$ is another root of $m_\alpha(x)$ and so K contains $\tau(\alpha)$ as well. Thus, $\tau(E) \subseteq K$.

As above, K is the splitting field of $f(x)$ over E and so it is also the splitting field of $\tau f(x) = f(x)$ (since τ fixes F) over $\tau(E)$.

So, we can extend τ to an isomorphism σ from K to K. Since σ fixes F, what we have just shown is that every embedding τ of E fixing F can be extended to an automorphism σ of K fixing F. In other words, every embedding of E is the action of some $\sigma \in G$.

Proof

Now, two automorphisms $\sigma, \sigma' \in G$ restrict to the same embedding of E iff $\sigma^{-1}\sigma'$ is the identity on E. But then $\sigma^{-1}\sigma' \in H$ since the automorphisms of K which fix E are exactly H. Another way of saying this is that $\sigma' \in \sigma H$.

What we have just shown is that distinct embeddings of E are in bijection with cosets σH of H in G. In particular, this gives us that:

$$|\text{Emb}(E/F)| = [G : H] = [E : F]$$

Where Emb denotes the set of embeddings of E into a fixed algebraic closure of F. Note that Emb(E/F) contains the automorphisms $Aut(E/F)$, since any automorphism admits to an embedding by our lemma.

The extension E/F is Galois iff $|Aut(E/F)| = [E : F]$. By the equality above, this is the case iff each embedding of E is an automorphism of E, i.e. $\sigma(E) = E$.

Now note that if $\sigma\alpha \in \sigma(E)$, then:

$$(\sigma h \sigma^{-1})(\sigma\alpha) = \sigma(h\alpha) = \sigma\alpha$$

For any $\alpha \in E$, since H fixes E. Thus $\sigma H \sigma^{-1}$ fixes $\sigma(E)$. The group fixing $\sigma(E)$ has order equal to $[K : \sigma(E)] = [K : E] = |H|H$, so indeed $\sigma H \sigma^{-1}$ is precisely the group fixing $\sigma(E) = E$.

Because the Galois correspondence is a bijection, $\sigma H \sigma^{-1} = H$ and hence H is normal. Thus, E is Galois over F iff H is normal in G.

Furthermore, this proof shows that the group of cosets G/H is identified with the group of automorphisms of the Galois extension E/F. Thus, $G/H \cong Gal(E/F)$.

Part 5

Suppose H_1 is the subgroup of elements fixing E_1 and H_2 the subgroup of elements fixing E_2. Then any element in $H_1 \cap H_2$ fixes both E_1 and E_2 and hence fixes the composite. Conversely, if an automorphism σ fixes the composite E_1E_2, then in particular $\sigma \in H_1 \cap H_2$. Similarly, the intersection $E_1 \cap E_2$ corresponds to the subgroup generated by H_1, H_2, and this proves the final part.