7. Galois Extensions

Galois Extensions

Automorphisms

Let K/F be an extension fields and let $\text{Aut}(K/F)$ be the group of field homomorphisms $\sigma : K \to K$ which are the identity when restricted to F.

Some basics:

- If $\alpha \in K$ is algebraic over F with minimal polynomial $p(x)$ over F, then $\sigma(\alpha)$ is also a root of $p(x)$.
- If $H \subset \text{Aut}(K/F)$ is a subgroup, then the set $K^H = \{x \in K : \sigma(x) = x \forall \sigma \in H\}$ is a subfield of K.
- If $H_1 \subset H_2$ are subgroups of $\text{Aut}(K/F)$, then $K^{H_2} \subset K^{H_1}$.

Galois Extensions

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

$$|\text{Aut}(E/F)| \leq [E : F].$$

If $f(x)$ is separable, then this is an equality.

Definition: E/F is called a Galois extension if $|\text{Aut}(E/F)| = [E : F]$. In this case the automorphism group is called the *Galois group* of the extension.

Proposition 5 says that separable splitting fields are Galois extensions.

The Galois correspondence

Let E/F be a Galois extension with Galois group G. Then there is a bijective (inclusion reversing) correspondence between:

- subfields L of E containing F
- subgroups of G

The correspondence is given by $H \to E^H$ for $H \subset G$ in one direction, and $L \to \text{Aut}(E/L) \subset G$ in the other direction.

Further:

- If $L = E^H$ then E/L is Galois with group H.
- If $L = E^H$ then $[E : L] = |H|$ so E is Galois over L.
- If L is a subfield of E containing F, then $|\mathrm{Aut}(E/L)| = [E : L]$ so E is Galois over L.
- The fixed field $L = E^H$ is Galois over F if and only if H is a normal subgroup of G, and in that case $\mathrm{Aut}(L/F) = G/H$.

Some examples

- Quadratic extensions
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- The splitting field of $x^3 - 2$ over $\mathbb{Q}$.
- The splitting field of $x^4 - 2$ over $\mathbb{Q}$.
- The field $\mathbb{Q}(\zeta_p)$ where ζ_p is a p^{th} root of unity.
- The fields of eigth and ninth roots of unity.
- Finite fields.

Overview of the proof

There are two "directions" we need to consider.

1. Suppose E/F is a separable splitting field extension. Then $|\mathrm{Aut}(E/F)| = [E : F]$.
2. Suppose E is a field and G is a finite group of automorphisms of E. Then the fixed field E^G satisfies $[E : E^G] = |G|$ and E/E^G is a separable splitting field.

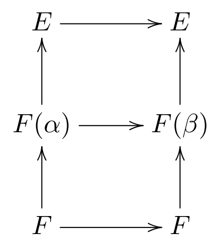
These mean together that:

- if we start with a separable extension E/F, compute its automorphism group $\mathrm{Aut}(E/F)$, and then take the fixed field in E of that group, we get a subfield of E that contains F and has $[E : E^{\mathrm{Aut}(E/F)}] = [E : F]$, so $E^{\mathrm{Aut}(E/F)} = F$.
- if we start with a field E and a group of automorphisms G, then E/E^G is a separable splitting field extension so $\mathrm{Aut}(E/E^G)$ has order $[E : E^G] = |G|$. Since G is contained in $\mathrm{Aut}(E/E^G)$, this means $\mathrm{Aut}(E/E^G) = G$.

This is the prototype of the Galois correspondence.

More on the proof - Step 1

The first assertion to consider is that, if E/F is a separable splitting field, then $|\mathrm{Aut}(E/F)| = [E : F]$. This is a consequence of the theorem on extension of automorphisms. The proof is by induction. Clearly if $E = F$ then $\mathrm{Aut}(E/F)$ is trivial and $[E : F] = 1$. Now suppose we know the result for all separable splitting fields of degree less than n and suppose E/F has degree n. Choose an element $\alpha \in E$ of degree greater than one over F and let $f(x)$ be its minimal polynomial. Let β be any other root of $f(x)$. Since E/F is a splitting field, $\beta \in E$. Consider the diagram:



Since $F(\alpha)$ is isomorphic to $F(\beta)$, the extension theorem says that there is an automorphism of E carrying α to β. Since there are $[F(\alpha) : F]$ choices of β, there are n such extensions σ_β corresponding to the n roots β of the minimal polynomial of α over F.

Now $E/F(\alpha)$ is still a separable splitting field, so our induction hypothesis says that there are $[E : F(\alpha)]$ automorphisms of E fixing $F(\alpha)$. Take any automorphism τ of E/F. It carries α to some β, so $\sigma_\beta^{-1}\tau$ fixes α and therefore $\tau = \sigma_\beta \phi$ where $\phi \in \mathrm{Aut}(E/F(\alpha))$.

It's not hard to show that this representation is unique, and so

$$|\mathrm{Aut}(E/F)| = |\mathrm{Aut}(E/F(\alpha))[F(\alpha) : F] = [E : F(\alpha)][F(\alpha) : F] = [E : F]$$

More on the proof - Step 2

Now we want to show that, if G is a group of automorphisms of a field E, then E/E^G is a separable splitting field of degree $|G|$. The key tool here is a result known as *linear independence of characters.*

Lemma: Let G be a group, let L be a field, and let $\sigma_1, \ldots, \sigma_n$ be distinct homomorphisms $G \to L^\times$. Then the σ_i are linearly independent over L, meaning that if $f = \sum_{i=1}^n a_i \sigma_i$ is the zero map for some collection of $a_i \in L$, then all a_i are zero.

Proof: Suppose that the σ_i are dependent. Choose a linear relation of minimal length where all the coefficients are nonzero:

$$f = \sum a_i \sigma_i = 0$$

Let $h \in G$ such that $\sigma_1(h)$ and $\sigma_n(h)$ are different. Now $f(g) = 0$ for all $g \in G$, and also $f(hg) = 0$ for all $g \in G$ since it's the same set of elements. Therefore

$$k = \sum a_i \sigma_i(h) \sigma_i = 0.$$

Now $k - \sigma_n(h) f$ is also identically zero. The coefficients of σ_n in k and f are both $\sigma_h(h) a_n$ so they cancel. On the other hand, the coefficients of σ_1 are $a_1 \sigma_1(h)$ and $a_1 \sigma_n(h)$ which are different; so $k - \sigma_n(h) f$ is a relation among the σ_i of shorter length. Thus the σ_i are independent.

Notice that if L is a field, $L^\times$ is a group and we can restrict an automorphism of L to $L^\times$ to obtain a character $L^\times \to L$. Therefore distinct automorphisms of L are linearly independent over L.

More on the proof - Step 3

Now we want to prove that $[E : E^G] = |G|$. Let's use $F = E^G$ to simplify the notation. Choose a basis $\alpha_1, \ldots, \alpha_n$ for E/F and let $\sigma_1, \ldots, \sigma_m$ be the elements of G. Form $m \times n$ the matrix

$$S = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_m(\alpha_1) & \sigma_m(\alpha_2) & \cdots & \sigma_m(\alpha_n) \end{pmatrix}$$

Let's first look at the row rank of this matrix. Suppose that

$$[\beta_1 \cdots \beta_m] S = 0.$$

It follows that $\sum_{i=1}^m \beta_i \sigma_i(\alpha_j) = 0$ for all α_j, and, since the α_j span E/F, we condlue $\sum_{i=1}^m \beta_i \sigma_i(x) = 0$ for all $x \in E$. By linear independence this means that all $\beta_i = 0$ and so the row rank of S is m.

Now let's look at the column rank. For this, notice that if $\sigma : E \to E$ is an automorphism, then $\sigma(S)$ (obtained by applying σ to each entry of S) is obtained from S by rearranging the rows. In other words

$$\sigma(S) = \Pi(\sigma) S$$

where $\Pi(\sigma)$ is an $m \times m$ permutation matrix. Now suppose $\boldsymbol{\beta} = [\beta_1, \ldots, \beta_n]$ satisfies

$$S\boldsymbol{\beta} = S \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = 0.$$

Then, for any $\sigma \in G$, we have

$$\sigma(S\boldsymbol{\beta}) = \sigma(S)\sigma(\boldsymbol{\beta}) = \Pi(\sigma) S \boldsymbol{\beta} = 0$$

In other words, if $\boldsymbol{\beta}$ is in the (left) kernel of S, so is $\sigma(\boldsymbol{\beta})$.

Now suppose $\boldsymbol{\beta}$ is nonzero and satisfies $S\boldsymbol{\beta} = 0$ and let $y = \sum_{i=1}^{m} \sigma_i(\boldsymbol{\beta})$. This is a column vector whose entries are $\sum_{i=1}^{m} \sigma_i(\beta_j)$. These sums are all fixed by G, since $\sigma(\sum_{i=1}^{m} \sigma_i(\beta_j))$ is just a permutation of the terms in the sum. We can introduce a function $Y : E \to E$ by setting

$$Y_j(x) = \sum_{i=1}^{m} \sigma_i(x\beta_j) = \sum_{i=1}^{m} \sigma_i(\beta_j)\sigma_i(x).$$

Since $\boldsymbol{\beta}$ is nonzero, by linear independence at least one of Y_j is nonzero so there is an $x \in E$ such that

$$\boldsymbol{Y} = \sum_{i=1}^{m} \sigma_i(x\boldsymbol{\beta}) \neq 0$$

But $\boldsymbol{Y}$ is in F^n and $S\boldsymbol{Y} = 0$. This means

$$\sigma_i(\sum_{j=1}^{n} Y_j(x)\alpha_j) = 0$$

for all i; and since the $Y_j(x) \in F$ and the α_j are independent we must have $Y_j(x) = 0$. This contradiction means that there cannot be a nonzero $\boldsymbol{\beta}$ with $S\boldsymbol{\beta} = 0$. We conclude that the column rank of S is n.

Since the row and column ranks of a matrix are the same, we have $n = m$.

More on the proof - Step 4

We finally need to verify that E/E^G is a separable splitting field. First, let $\alpha \in E$ be any element of E with minimal polynomial $q(x)$. Consider the orbit $\{\alpha_1, \ldots, \alpha_k\}$ of α under the action of G. The polynomial

$$p(x) = \prod_{i=1}^{k} (x - \alpha_i)$$

is fixed by G so has coefficients in E^G; it also has α as a root so $q(x)$ divides $p(x)$. Therefore all roots of $q(x)$ belong to E. Since every polynomial with coefficients in E^G that has a root in E splits in E, E is a splitting field over E^G.

To show separability, let $\beta_1, \ldots, \beta_n$ be a basis for E/E^G. Let $p_i(x)$ be the minimal polynomial of β_i over E^G. We've shown already that each $p_i(x)$ splits completely in E. Consider the product $f(x)$ of all the p_i and let $f_1(x)$ be its square free part (that is, the product of its irreducible factors, all to the first power). Then $f_1(x)$ is separable and has the β_i as roots, and therefore E is the splitting field of the separable polynomial $f_1(x)$.

Definition: If $\alpha \in E$, the elements $\sigma(\alpha)$, with $\sigma \in G$, are called the conjugates of α (or the Galois conjugates).

The full proof of the correspondence

See the proof in Dummit and Foote, which basically applies our numerical result that $[E : E^G] = |G|$, the fact that E/E^G is a separable splitting field, and our existence theorem that, if E/F is a separable splitting field, then $|\mathrm{Aut}(E/F)| = [E : F]$j to obtain the correspondence.

View as slides