



In this handout all fields are of characteristic 0.

Theorem (the fundamental theorem of Galois theory in characteristic 0). Let E be a splitting field over a field F , where $\text{char } F = 0$. Then there is a bijective correspondence between the set $\{K : E/K/F\}$ of intermediate field extensions K lying between F and E and the set $\{H : H < \text{Gal}(E/F)\}$ of subgroups H of the Galois group $\text{Gal}(E/F)$ of the original extension E/F :

$$\{K : E/K/F\} \longleftrightarrow \{H : H < \text{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension K to the subgroup $\text{Gal}(E/K)$ of elements in $\text{Gal}(E/F)$ that preserve K ,

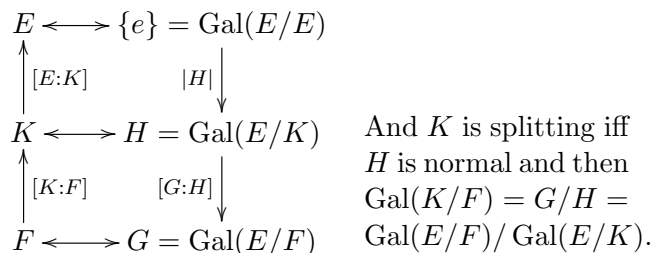
$$K \mapsto \text{Gal}(E/K) := \{\phi : E \rightarrow E : \phi|_K = I\},$$

and reversely, by mapping every subgroup H of $\text{Gal}(E/F)$ to its fixed field E_H :

$$H \mapsto E_H := \{x \in E : \forall h \in H, hx = x\}.$$

This correspondence has the following further properties:

1. It is inclusion-reversing: if $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\text{Gal}(E/K_1) \supset \text{Gal}(E/K_2)$.
2. It is degree/index respecting: $[E : K] = |\text{Gal}(E/K)|$ and $[K : F] = [\text{Gal}(E/F) : \text{Gal}(E/K)]$.
3. Splitting fields correspond to normal subgroups: K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ if and only if $\text{Gal}(E/K)$ is normal in $\text{Gal}(E/F)$ and then $\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K)$.



Proof of $E_{\text{Gal}(E/K)} = K$. Let K be an intermediate field between E and F . The inclusion $E_{\text{Gal}(E/K)} \supset K$ is easy, so we turn to prove the other inclusion. Let $v \in E \setminus K$ be an element of E which is not in K . We need to show that there is some automorphism $\phi \in \text{Gal}(E/K)$ for which $\phi(v) \neq v$; this implies that $v \notin E_{\text{Gal}(E/K)}$ and this implies the other inclusion. Let p be the minimal polynomial of v over K . It is not of degree 1 as $v \notin K$. E is a splitting extension so we know that E contains all the roots of p . Over a field of characteristic 0 irreducible polynomials cannot have multiple roots (as the gcd of an irreducible p with the lower-degree yet non-zero p' must be 1) and hence p must have at least one other root; call it w . Since v and w have the same minimal polynomial over K , we know that $K(v)$ and $K(w)$ are isomorphic via an isomorphism $\phi_0 : K(v) \rightarrow K(w)$ so that $\phi_0|_K = I$ yet $\phi_0(v) = w$. But E is a splitting field of some polynomial f over F and hence also over $K(v)$ and over $K(w)$. By the uniqueness of splitting fields, the isomorphism ϕ_0 can be extended to an isomorphism $\phi : E \rightarrow E$; i.e., to an automorphism of E with $\phi|_K = \phi_0|_K = I$ so $\phi \in \text{Gal}(E/K)$. Yet $\phi(v) = w \neq v$, as required. \square

Proof of $H = \text{Gal}(E/E_H)$. Let $H < \text{Gal}(E/F)$ be a subgroup of the Galois group of E over F . The inclusion $H < \text{Gal}(E/E_H)$ is easy, so it is enough to show that $\text{Gal}(E/E_H)$ is finite and that $|\text{Gal}(E/E_H)| \leq |H|$.

By the Primitive Element Theorem we know that there

is some element $u \in E$ so that $E = E_H(u)$. Let p be the minimal polynomial of u over E_H . Let $n := \deg(p)$. To conclude the proof, we will show that

$$|\text{Gal}(E/E_H)| \leq n \leq |H|.$$

Distinct elements of $\text{Gal}(E/E_H)$ map u to distinct roots of p , but p splits in E and so it has exactly n roots. This proves the first inequality.

For the second inequality, let f be the polynomial

$$f = \prod_{\sigma \in H} (x - \sigma(u)).$$

Clearly, $f \in E[x]$. Furthermore, if $\tau \in H$, then the action of τ permutes the $\sigma(u)$'s, hence $\tau(f) = f$ and hence $f \in E_H[x]$. Clearly $f(u) = 0$, so $p|f$, so $n \leq |H|$.

Seeing that $E = E_H(u)$, we have also proven here that $[E : E_H] = \deg(p) = n = |H|$. \square

Proof of Property 1. Easy. \square

Proof of Property 2. If $K = E_H$, then $|\text{Gal}(E/K)| = |\text{Gal}(E/E_H)| = [E : E_H] = [E : K]$ as shown above. But every K is E_H for some H , so $|\text{Gal}(E/K)| = [E : K]$ for every K between E and F . The second equality follows from the first and from the multiplicativity of the degree/order/index in towers of extensions and in towers

of groups:

$$\begin{aligned}
 [K : F] &= \frac{[E : F]}{[E : K]} = \frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/K)|} \\
 &= [\text{Gal}(E/F) : \text{Gal}(E/K)]. \quad \square
 \end{aligned}$$

Proof of Property 3, \Rightarrow . We will define a surjective (onto) group homomorphism $\rho : \text{Gal}(E/F) \rightarrow \text{Gal}(K/F)$ whose kernel is $\text{Gal}(E/K)$. This shows that $\text{Gal}(E/K)$ is normal in $\text{Gal}(E/F)$ (kernels of homomorphisms are always normal) and then by the first isomorphism theorem for groups, we'll have that $\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K)$.

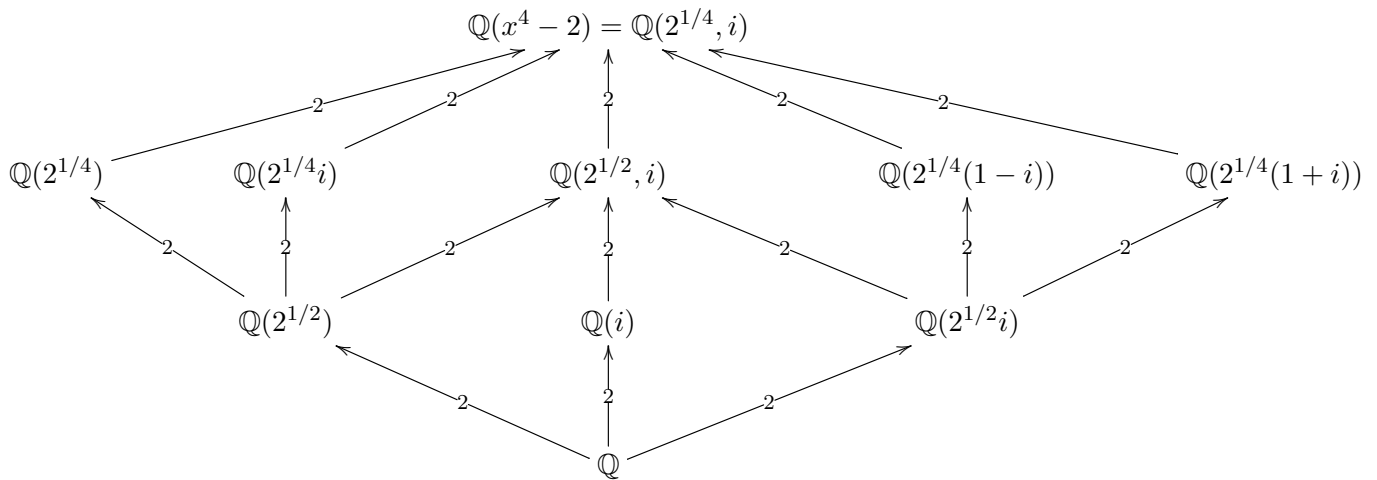
Let σ be in $\text{Gal}(E/F)$ and let u be an element of K . Let p be the minimal polynomial of u in $F[x]$. Since K is a splitting field p splits in $K[x]$ and hence all the other roots of p are also in K . As $\sigma(u)$ is a root of p , it follows that $\sigma(u) \in K$ and hence $\sigma(K) \subset K$. Similarly $\sigma^{-1}(K) \subset K$ which means $K \subset \sigma(K)$ and hence $\sigma(K) = K$. Hence the restriction $\sigma|_K$ of σ to K is an

automorphism of K and we can define $\rho(\sigma) = \sigma|_K$.

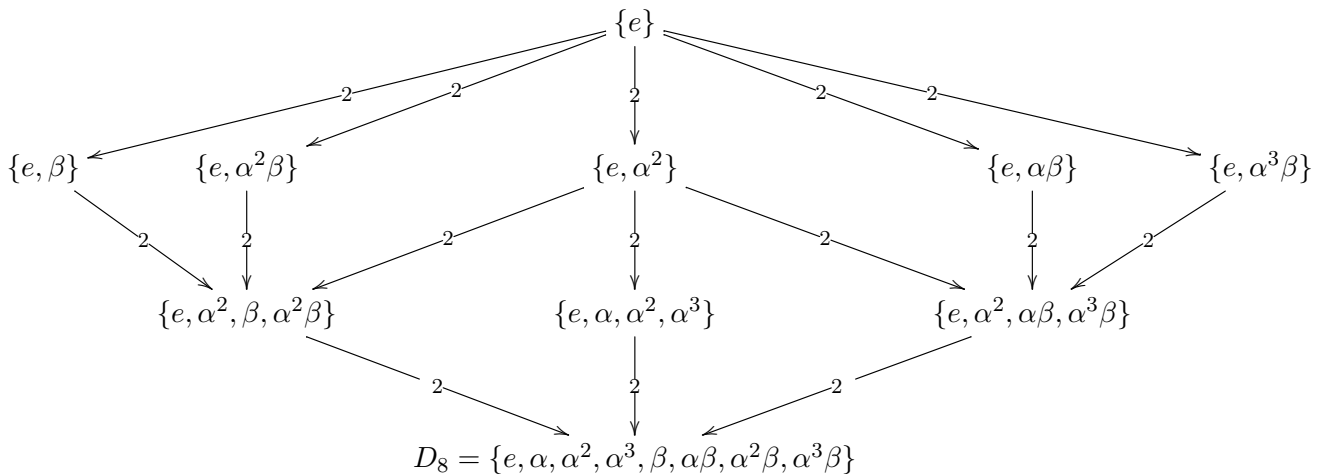
Clearly, ρ is a group homomorphism. The kernel of ρ is those automorphisms of E whose restriction to K is the identity. That is, it is $\text{Gal}(E/K)$. Finally, as E/F is a splitting extension, so is E/K . So every automorphism of K extends to an automorphism of E by the uniqueness statement for splitting extensions. But this means that ρ is onto. \square

Proof of Property 3, \Leftarrow . Suppose H is normal in G , $p \in F[x]$ is irreducible, and $u \in E_H$ is a root of p . We need to show that p splits in E_H . We know that p splits in E , so we just need to show that if $v \in E$ is a root of p , then $v \in E_H$. Let $\sigma_0 : F(u) \rightarrow F(v)$ be the isomorphism that fixes F and maps $u \rightarrow v$. By the uniqueness of splitting fields, it can be extended to an automorphism $\sigma : E \rightarrow E$. Now for any $h \in H$, $h' := \sigma^{-1}h\sigma \in H$ as H is normal, hence $h'u = u$ as $u \in E_H$, and hence $h\sigma u = h\sigma u = \sigma\sigma^{-1}h\sigma u = \sigma h'u = \sigma u = v$. So $v \in E_H$, as required. \square

The subfields of $\mathbb{Q}(x^4 - 2)$ and the subgroups of D_8 (adopted from Gallian's book, page 548).



Below $\alpha : (i, 2^{1/4}) \mapsto (i, -2^{1/4}i)$ and $\beta : (i, 2^{1/4}) \mapsto (-i, 2^{1/4})$:



Which of these subgroups are normal? Which of these extensions are splitting?