

Frank Moore
 Algebra 901 Notes
 Professor: Tom Marley

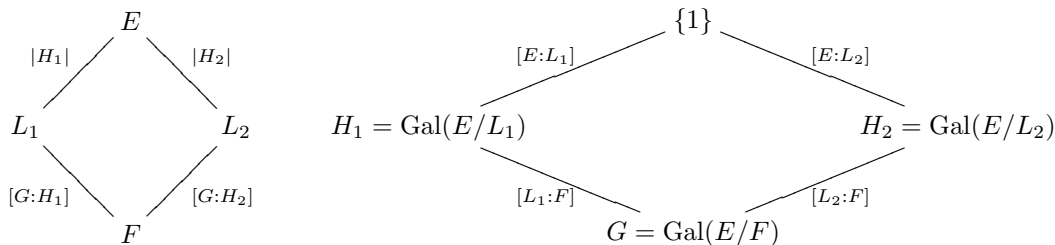
Fundamental Theorem of Galois Theory: Let E/F be a finite Galois extension. Then there exists a 1-1 inclusion reversing correspondence between

$$\left\{ \text{Intermediate fields of } E/F \right\} \longleftrightarrow \left\{ \text{Subgroups of } \text{Gal}(E/F) \right\}$$

$$L \longmapsto \text{Gal}(E/L)$$

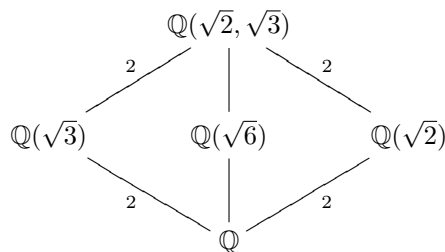
$$E_H \longleftarrow H$$

such that if $L_1 \subseteq L_2$ then $\text{Gal}(E/L_1) \supseteq \text{Gal}(E/L_2)$. Similarly, if we have $H_1 \subseteq H_2$ then $E_{H_1} \supseteq E_{H_2}$. Also, note that $[E : E_H] = |\text{Gal}(E/E_H)| = |H|$ and thus $[E_H : F] = \frac{[E:F]}{[E:E_H]} = \frac{|G|}{|H|} = [G : H]$. In other words, we have the following picture below as an illustrative example.



Examples:

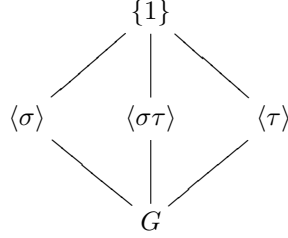
1. Find all intermediate fields of E/\mathbb{Q} where $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have calculated above what the field diagram looks like:



We also know that $G = \text{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ where σ and τ are given by:

$$\begin{array}{l} \tau : E \longrightarrow E \quad \sigma : E \longrightarrow E \\ \sqrt{2} \mapsto -\sqrt{2} \quad \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \quad \sqrt{3} \mapsto -\sqrt{3} \end{array}$$

The (upside down) subgroup lattice of G is



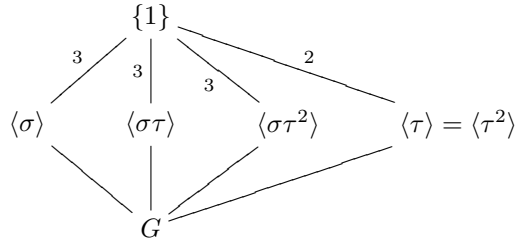
Where the subgroups of G correspond to the intermediate subfields of E/F that are in the same place. To justify this, note that σ clearly fixes $\sqrt{2}$ and τ clearly fixes $\sqrt{3}$. Also, note that $\sigma\tau(\sqrt{6}) = \sqrt{6}$ and therefore $\mathbb{Q}(\sqrt{6}) \subseteq E_{\langle\sigma\tau\rangle}$. Since $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2 = [G : \langle\sigma\tau\rangle] = [E_{\langle\sigma\tau\rangle} : \mathbb{Q}]$, we have that $\mathbb{Q}(\sqrt{6}) = E_{\langle\sigma\tau\rangle}$.

Let $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Check that $\sqrt{2} + \sqrt{3}$ is not fixed by any $\sigma \in G \setminus \{1\}$. Therefore, $\text{Gal}(\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}) = \{1\}$ and hence $K = E$. This is another way to come up with a primitive element for an extension.

- Let E be the splitting field of $x^3 - 2$ over \mathbb{Q} . We know that $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is a primitive 3rd root of unity. Also, we know that $\text{Gal}(E/\mathbb{Q}) \cong S_3 = \{1, \sigma, \tau, \tau^2, \sigma\tau, \sigma\tau^2\}$, where

$$\begin{array}{l} \tau : E \longrightarrow E \quad \sigma : E \longrightarrow E \\ \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} \quad \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega \quad \omega \mapsto \omega^2 \end{array}$$

The subgroup lattice of $\text{Gal}(E/\mathbb{Q})$ is below:



Note that $E_{\langle\sigma\rangle} = \mathbb{Q}(\sqrt[3]{2})$. Indeed, we know that $\mathbb{Q}(\sqrt[3]{2}) \subseteq E_{\langle\sigma\rangle}$ and also $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 = [G : \langle\sigma\rangle] = [E_{\langle\sigma\rangle} : \mathbb{Q}]$. Hence $E_{\langle\sigma\tau\rangle} = \mathbb{Q}(\omega \sqrt[3]{2})$. Similar arguments may be given for why $E_{\langle\sigma\tau\rangle} = \mathbb{Q}(\omega \sqrt[3]{2})$, $E_{\langle\sigma\tau^2\rangle} = \mathbb{Q}(\omega^2 \sqrt[3]{2})$, and $E_{\langle\tau\rangle} = \mathbb{Q}(\omega)$. Note also that here $\omega + \sqrt[3]{2}$ is not fixed by any non-identity element in G . Therefore $E = \mathbb{Q}(\omega + \sqrt[3]{2})$.

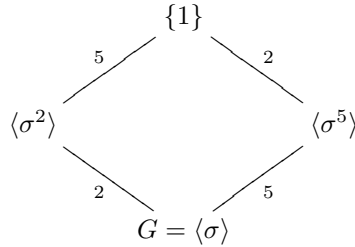
Proposition: Let E/F be a finite Galois extension and H a subgroup of $\text{Gal}(E/F)$. Let $\alpha \in E$ and $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$ be a maximal set of distinct conjugates of α where $\sigma_i \in H$. Then $\sigma_1(\alpha) + \dots + \sigma_r(\alpha) \in E_H$ and so is $\sigma_1(\alpha) \cdots \sigma_r(\alpha)$.

Proof: Let $\tau \in H$. Then $\tau(\sigma_1(\alpha) + \dots + \sigma_r(\alpha)) = \tau\sigma_1(\alpha) + \dots + \tau\sigma_r(\alpha)$. Also, since τ is injective, we have that $\tau\sigma_i(\alpha) \neq \tau\sigma_j(\alpha)$ for all $i \neq j$. As $\tau \in H$, and $\sigma_i \in H$, we have that $\tau\sigma \in H$. Then the above list $\{\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)\}$ is a permutation of $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$. Therefore, the sum and the product are fixed by τ and hence in E_H .

Theorem: Let ω be a primitive n th root of unity over \mathbb{Q} . Then $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.

Proof: If $[i]_n \in \mathbb{Z}_n^\times$, define $\psi([i]_n) = \sigma_i$ where $\sigma_i : \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ sends ω to ω^i . This is clearly an isomorphism.

Example: Let ω be a primitive n th root of unity. Thus by the above theorem, $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_{11}^\times$, where $E = \mathbb{Q}(\omega)$. Now $\mathbb{Z}_{11}^\times = \langle \bar{2} \rangle$. Therefore $G = \langle \sigma \rangle$ where $\sigma : \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ sends ω to ω^2 . The subgroup lattice for G is below:



Note that in the above correspondence $\sigma^j \in G \longleftrightarrow \bar{2}^j \in \mathbb{Z}_{11}^\times$. By the proposition applied to $\langle \sigma^5 \rangle = \{1, \sigma^5\}$, we have that $\omega + \omega^{10} \in E_{\langle \sigma^5 \rangle}$. So, we know that $\mathbb{Q}(\omega + \omega^{10}) \subseteq E_{\langle \sigma^5 \rangle}$. Since 5 is prime, we only need to check if $\omega + \omega^{10} \in \mathbb{Q}$. Suppose that $\omega + \omega^{10} = q \in \mathbb{Q}$. Then ω is a root of $x^{10} + x - q \in \mathbb{Q}[x]$. But we know that $\text{Irr}(\omega, \mathbb{Q}) = x^{10} + x^9 + \dots + x + 1$ which does not divide $x^{10} + x - q$. So $\omega + \omega^{10} \notin \mathbb{Q}$, and hence $\mathbb{Q}(\omega + \omega^{10}) = E_{\langle \sigma^5 \rangle}$. Now consider $\langle \sigma^2 \rangle = \{1, \sigma^2, \sigma^4, \sigma^6, \sigma^8\}$. Note that the complete set of conjugates of ω in this group are $\omega, \omega^4, \omega^5, \omega^9$, and ω^3 (listed in the same order as the σ s above). Therefore, $\beta = \omega + \omega^3 + \omega^4 + \omega^5 + \omega^9 \in E_{\langle \sigma^2 \rangle}$. By a similar argument as above $\beta \notin \mathbb{Q}$ and hence $\mathbb{Q}(\beta) = E_{\langle \sigma^2 \rangle}$.

Definition: An algebraic extension E/F is called abelian (resp. cyclic) if E/F is Galois and $\text{Gal}(E/F)$ is abelian (resp. cyclic).

Theorem: Let E/F be a finite Galois extension and L an intermediate field. Let $G = \text{Gal}(E/F)$ and $H = \text{Gal}(E/L)$. Then

1. L/F is normal $\Leftrightarrow H \triangleleft G$.
2. If L/F is normal then $\text{Gal}(L/F) \cong G/H$ (note that we always have that $[L : F] = [G : H]$).

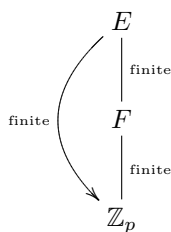
Proof: Suppose that L/F is normal. Define a map

$$\begin{aligned} \phi : G &\rightarrow \text{Gal}(L/F) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

Then ϕ is a group homomorphism. Furthermore, any $\tau \in \text{Gal}(L/F)$ can be extended to a $\sigma \in G$ and $\sigma|_L = \tau$. Therefore ϕ is surjective. Furthermore, we have that $\sigma \in \ker \phi \Leftrightarrow \sigma|_L = \text{Id}_L \Leftrightarrow \sigma \in H$. Hence H is the kernel, hence normal in G , and so $\text{Gal}(L/F) \cong G/H$. Now, for the reverse direction, suppose that $H \triangleleft G$. Let $\psi : L \rightarrow \bar{F}$ be a map which fixes F . Let $\alpha \in L$. It is enough to show that $\psi(\alpha) \in L$. Extend ψ to $\sigma \in G$. Now it is enough to show that $\sigma(\alpha) \in L$. Now $L = E_H$, so it is enough to show that $h(\sigma(\alpha)) = \sigma(\alpha)$ for all $h \in H$. So, let $h \in H$. Then $\sigma^{-1}h\sigma \in H$ as $H \triangleleft G$. Thus, if $\alpha \in L$, we have that $\sigma^{-1}h\sigma(\alpha) = \alpha$. Therefore, $h(\sigma(\alpha)) = \sigma(\alpha)$. Hence $\sigma(\alpha) \in E_H = L$, as desired.

Theorem: Let E/F be a finite extension where F is a finite field. Then $\text{Gal}(E/F)$ is cyclic.

Proof: Let $p = \text{Char } F$. Then we have the tower of fields



Note that $\text{Gal}(E/F)$ is a subgroup of $\text{Gal}(E/\mathbb{Z}_p)$. Therefore, it is enough to show that $\text{Gal}(E/\mathbb{Z}_p)$ is cyclic. Let $n = [E : \mathbb{Z}_p]$. Then E is the splitting field of $x^{p^n} - x$ over \mathbb{Z}_p . Let $\sigma : E \rightarrow E$ be the automorphism of E that sends $a \in E$ to a^p . Note that this automorphism fixes \mathbb{Z}_p . Therefore, we have that $\sigma \in \text{Gal}(E/\mathbb{Z}_p)$ so it is enough to show that it has order n . Suppose that $\sigma^k = 1$ for some $k < n$. Then $a^{p^k} = a$ for all $a \in E$. Hence $x^{p^k} - x$ has p^n roots, a contradiction as $p^n > p^k$. Thus, $k = n$ and $\text{Gal}(E/\mathbb{Z}_p) = \langle \sigma \rangle$.