

Frank Moore
 Algebra 901 Notes
 Professor: Tom Marley

Definition: Let E/F be a field extension. Then denote the set of automorphisms of E that fix F by

$$\text{Aut}(E/F) := \{\phi : E \rightarrow E \mid \phi_F = \text{Id}_F\}$$

Clearly the above is a group.

Examples:

1. $E = \mathbb{Q}(\sqrt[3]{2})$. What is $\text{Aut}(E/\mathbb{Q})$? We know that $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, and the roots of this polynomial are $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. If $\phi : E \rightarrow E$ fixes \mathbb{Q} then $\phi(\sqrt[3]{2}) = \omega^i\sqrt[3]{2}$ for some i . But the only root in E is $\sqrt[3]{2}$. Hence $\text{Aut}(E/\mathbb{Q}) = \{\text{Id}\}$.
2. Let $E = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/n}$. To compute $\text{Aut}(E/\mathbb{Q})$, first recall that $\text{Irr}(\omega, \mathbb{Q}) = \Phi_n(x) = \prod_{(i,n)=1}^n (x - \omega^i)$. For each ω^i with $(i, n) = 1$, there exists a $\phi : E \rightarrow E$ sending ω to ω^i . Therefore, we have that $\text{Aut}(E/\mathbb{Q}) = \{\phi_i : E \rightarrow E \mid \phi(\omega) = \omega^i\}$. Hence $|\text{Aut}(E/\mathbb{Q})| = \phi(n)$.

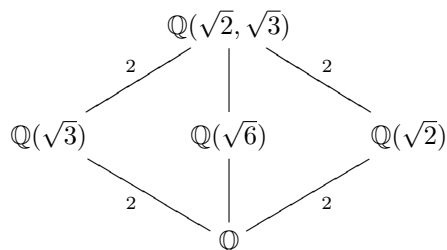
Proposition: Let E/F be finite. Then $|\text{Aut}(E/F)| \leq [E : F]_s$ with equality $\Leftrightarrow E/F$ is normal. Also, we have $|\text{Aut}(E/F)| = [E : F] \Leftrightarrow E/F$ is normal and separable.

Proof: Recall that $[E : F]_s = |S|$ where $S = \{\phi : E \rightarrow \bar{F} \mid \phi|_F = \text{Id}_F\}$. But $\text{Aut}(E/F) \subseteq S$ and is the whole set if and only if E/F is normal. For the second assertion, certainly we have that $|\text{Aut}(E/F)| = [E : F]_s$ as E/F is normal. But since E/F is separable, we also have that $|\text{Aut}(E/F)| = [E : F]$. Note that all of the above implications reverse.

Definition: An algebraic extension E/F is **Galois** if E/F is normal and separable. In this case, the group $\text{Aut}(E/F)$ is called the **Galois group** of E/F and is denoted $\text{Gal}(E/F)$.

Examples:

1. Let $E = \mathbb{Q}(\omega)$ where ω was a primitive n th root of unity, we have that $\text{Gal}(E/\mathbb{Q}) = \mathbb{Z}_n^\times$.
2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. It is clear that E/\mathbb{Q} is Galois and that $|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 4$. We have the following field diagram:



Where we have the above degrees of extensions since $x^2 - 2$ is irreducible over both \mathbb{Q} and $\mathbb{Q}(\sqrt{3})$ and $x^2 - 3$ is irreducible over both \mathbb{Q} and $\mathbb{Q}(\sqrt{2})$. So, there are automorphisms (since we may

only permute roots of the same polynomial)

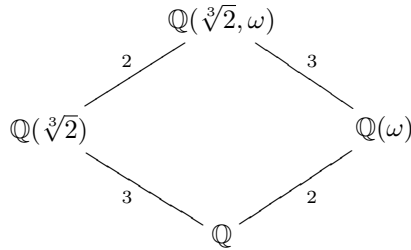
$$\begin{array}{l} \tau : E \longrightarrow E \quad \sigma : E \longrightarrow E \\ \sqrt{2} \mapsto -\sqrt{2} \quad \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \quad \sqrt{3} \mapsto -\sqrt{3} \end{array}$$

Note that the identity map works too, and composing the above maps gives us the map:

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

Therefore, we have that $\text{Aut}(E/\mathbb{Q}) \cong C_2 \times C_2$, the Klein 4-group.

3. Let E be the splitting field of $x^3 - 2$ over \mathbb{Q} . Then E/\mathbb{Q} is Galois and $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a cube root of unity. Then as we have calculated before, we have that $[E : \mathbb{Q}] = |\text{Gal}(E/\mathbb{Q})| = 6$. We have the following diagram:



So we have two mappings right away

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

Which are indeed field maps that fix \mathbb{Q} since $x^3 - 2$ is irreducible over $\mathbb{Q}(\omega)$ and $x^2 + x + 1$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$. Note also that $|\sigma| = 3$ and $|\tau| = 2$. Therefore, we get that $\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$. This is S_3 , as note that $\sigma\tau : E \rightarrow E$ sends $\sqrt[3]{2}$ to $\omega \sqrt[3]{2}$ and $\tau\sigma$ sends $\sqrt[3]{2}$ to $\omega^2 \sqrt[3]{2}$, hence $\text{Gal}(E/\mathbb{Q})$ is nonabelian (and so S_3). Note also that $E = \mathbb{Q}(\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2})$. Any $\pi : E \rightarrow E$ permutes the set $\{\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}\}$. This gives a natural isomorphism from $\text{Gal}(E/\mathbb{Q}) \rightarrow S_3$ where σ corresponds to (123) and τ corresponds to (12).

Remark:

1. Let E/F be a Galois extension and L an intermediate field. Then E/L is Galois and $\text{Gal}(E/L) < \text{Gal}(E/F)$.

2. Also, let E/F be Galois and H a subgroup of $\text{Gal}(E/F)$. Then let $E_H := \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$. Then E_H is an intermediate field of E/F , and is often called the **Fixed Field of H** . In fact we have the **Galois Correspondence**.

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

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

$$E_H \longleftarrow H$$

We will show that $L = E_{\text{Gal}(E/L)}$ and $\text{Gal}(E/E_H) = H$, i.e. that the above functions are mutually inverses.

Theorem: Suppose that E/F is Galois and let $G = \text{Gal}(E/F)$. Then $F = E_G$.

Proof: Certainly we have that $F \subseteq E_G$. Let $\alpha \in E_G$. Let $\sigma : F(\alpha) \rightarrow \bar{F}$ be an embedding which fixes F . Extend σ to $\tau : E \rightarrow E$ as E is normal. Hence $\tau \in G$. Since $\alpha \in E_G$, $\tau(\alpha) = \alpha$. Hence $\sigma(\alpha) = \alpha$. Therefore σ is the identity map. Hence $[F(\alpha) : F]_s = 1$ and since $F(\alpha)/F$ is separable, $[F(\alpha) : F] = 1$. Therefore $\alpha \in F$.

Corollary: Let E/F be Galois and L an intermediate field of E/F and $H = \text{Gal}(E/L) < \text{Gal}(E/F)$. Then $E_H = L$. Then the map:

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

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

is injective.

Proof: Suppose that $\text{Gal}(E/L_1) = \text{Gal}(E/L_2) = H$. Then by the above theorem, $L_1 = E_H = L_2$. This proves half of the Galois correspondence.

Lemma: Let E/F be a separable extension. Suppose that there exists $n \in \mathbb{Z}$ such that $[F(\alpha) : F] \leq n$ for all $\alpha \in E$. Then E/F is finite and of degree n .

Proof: Choose $\alpha \in E$ such that $[F(\alpha) : F] = m$ is maximal. We claim that $E = F(\alpha)$. If not, then $\exists \beta \in E \setminus F(\alpha)$. Then $F(\alpha, \beta) \supsetneq F(\alpha)$ and by the primitive element theorem, there exists a primitive element for $F(\alpha, \beta)$ whose degree would violate maximality of m . Therefore $E = F(\alpha)$, for some $\alpha \in E$ and $[F(\alpha) : F] = m \leq n$.

Artin's Theorem: Let E be an arbitrary field and G a finite group of automorphisms of E . Let $F = E_G$, the fixed field of G in E . Then we have that E/F is Galois and finite and $G = \text{Gal}(E/F)$.

Proof: Let $\alpha \in E$. Let $\{\sigma_1, \dots, \sigma_r\}$ be a maximal subset of G such that $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ are distinct. If $\tau \in G$, then $\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)$ are also distinct since τ is injective. Let $f_\alpha(x) = \prod_{i=1}^r (x - \sigma_i(\alpha))$. Note that $f_\alpha^\tau = \prod_{i=1}^r (x - \tau\sigma_i(\alpha)) = f_\alpha$. Hence $f_\alpha \in F[x]$. Since $\alpha = \sigma_i(\alpha)$ for some i , α is a root

of f_α . Hence we have that $\text{Irr}(\alpha, F) \mid f_\alpha(x)$. Therefore $[F(\alpha) : F] \leq r \leq |G|$. Also, f_α has distinct roots, hence $\text{Irr}(\alpha, F)$ does, and hence α is separable over F . Therefore E/F is separable. By the lemma, $[E : F] \leq |G|$. As f_α splits over E , so does $\text{Irr}(\alpha, F)$ for all $\alpha \in E$. Therefore, E/F is normal and so it is Galois. Note that $G \subseteq \text{Gal}(E/F)$. Then $|G| \leq |\text{Gal}(E/F)| = [E : F] \leq |G|$. Hence $G = \text{Gal}(E/F)$ (and so $|G| = [E : F]$).