Math 210B Lecture 9 Notes

Daniel Raban

January 28, 2019

1 The Fundamental Theorem of Galois Theory

1.1 Restriction of automorphisms and the Galois group over a fixed field

Here, assume all extensions K/F will lie in $\overline{F}$.

Proposition 1.1. *If K/F is Galois and E is intermediate, then there exits a bijection of left $\operatorname{Gal}(K/F)$-sets $\operatorname{res}_F : \operatorname{Gal}(K/F)/\operatorname{Gal}(K/E) \to \operatorname{Emb}_F(E)$ sending $\sigma \operatorname{Gal}(K/E) \mapsto \sigma|_E$. Moreover, E/F is Galois if and only if $\operatorname{Gal}(K/E)$ is normal in $\operatorname{Gal}(K/F)$, in which case res_F is an isomorphism of groups.*

Proof. If $\sigma \in \operatorname{Gal}(K/F)$ and $\tau \in \operatorname{Gal}(K/F)$, then

$$\begin{aligned} \sigma\tau|_E = \sigma|_E &\iff \sigma_\tau(\alpha) = \sigma(\alpha) \; \forall \alpha \in E \\ &\iff \tau(\alpha) = \alpha \; \forall \alpha \in E \\ &\iff \tau \in \operatorname{Gal}(K/E). \end{aligned}$$

To show that this is onto, every $\varphi \in \operatorname{Emb}_F(E)$ lifts to $\sigma : K \to \overline{F}$, but this takes values in K since K/F is normal. So $\sigma \in \operatorname{Gal}(K/F)$. If $|rho \in \operatorname{Gal}(K/F)$, then

$$\operatorname{res}_F(\rho\sigma \operatorname{Gal}(K/E)) = \rho\sigma|_E = \rho \circ \sigma|_E = \rho \circ \operatorname{res}_F(\sigma \operatorname{Gal}(K/E)).$$

If E/F is Galois, then $\operatorname{Gal}(K/F) \to \operatorname{Gal}(E/F)$ sending $\sigma \mapsto \sigma|_E$ has kernel $\operatorname{Gal}(K/E)$, so it is normal.

Conversely, if $\operatorname{Gal}(K/E) \trianglelefteq \operatorname{Gal}(K/F)$, take $\varphi \in \operatorname{Emb}_F(E)$, and $\sigma \in \operatorname{Gal}(K/F)$ lifting φ. Then for all $\tau \in \operatorname{Gal}(K/E)$, $\sigma^{-1}\tau\sigma|_E = 1$. By normality, $\tau\sigma|E = \sigma|_E$. So $\sigma(E)$ is fixed by τ. So $\sigma(E) \subseteq E$, the fixed field of τ. So $\sigma(E) = E$, so E/F is Galois. □

Proposition 1.2. *Let K/F be finite and Galois, and let $H \leq \operatorname{Gal}(K/F)$. Then the Galois group $\operatorname{Gal}(K/K^H) = H$.*

Proof. H fixes K^H, so $H \leq \operatorname{Gal}(K/K^H)$. K/K^H is separable, so by the primitive element theorem, there exists $\theta \in K$ such that $K = K^H(\theta)$. Then $f = \prod_{\sigma \in H}(x - \sigma(\theta)) \in K^H[x]$. The minimal polynomial of θ over K^H divides f, so $[K : K^H] \leq \deg(f) = |H|$. This forces $H = \operatorname{Gal}(K/K^H)$. □

1.2 The Galois correspondence

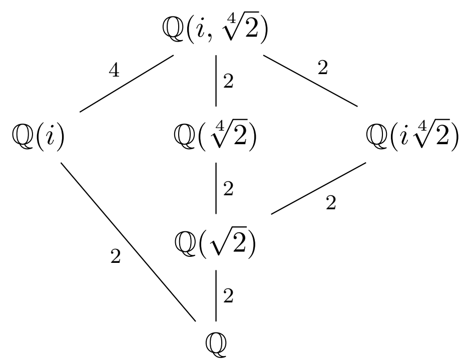
Theorem 1.1 (Fundamental theorem of Galois theory)**.** *Let K/F be finite, Galois. There are inclusion-reversing inverse bijections $\psi : \{E : K/E/F\} \to \{H : H \leq \mathrm{Gal}(K/F)\}$ and $\theta : \{H : H \leq \mathrm{Gal}(K/F)\} \to \{E : K/E/F\}$ such that $\psi(E) = \mathrm{Gal}(K/E)$, and $\theta(H) = K^H$. For such E/H, $[K : E] = |\,\mathrm{Gal}(K/E)|$, and $|H| = [K : K^H]$. These restrict to bijections between normal extensions of K and normal subgroups of $\mathrm{Gal}(K/F)$. If E/F is normal, we have the bijection $\mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E) \to \mathrm{Emb}_F(E)$, sending $\sigma\,\mathrm{Gal}(K/E) \mapsto \sigma|_E$.*

Proof. We have proved almost all the statements. We verify

$$\psi(\theta(H)) = \psi(K^H) = \mathrm{Gal}(K/K^H) = H,$$
$$\theta(\psi(E)) = \theta(\mathrm{Gal}(K/E)) = K^{\mathrm{Gal}(K/E)} = E. \qquad \square$$

Example 1.1. The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[4]{2}, i)$. The polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$. There exists $\tau \in \mathrm{Gal}(K/\mathbb{Q}(i)) \cong \mathbb{Z}/4\mathbb{Z}$ with $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$; this generates $\mathrm{Gal}(K/\mathbb{Q}(i))$. The $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[4]{2})) \ni \sigma$ such that $\sigma(i) = -i$ and $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$. We can check that $\sigma\tau\sigma^{-1}(\sqrt[4]{2}) = -i\sqrt[4]{2} = \tau^{-1}(\sqrt[4]{2})$. So $\sigma\tau\sigma^{-1} = \tau^{-1}$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_4$.

Here is a diagram of some of the intermediate fields.



Proposition 1.3. *Let K be finite and Galois over F, and let E/F be algebraic. Then the map $\mathrm{res}_K : \mathrm{Gal}(EK/E) \to \mathrm{Gal}(K/K \cap E)$ sending $\sigma \mapsto \sigma|_K$ is an isomorphism.*

Proof. Let $\sigma \in \mathrm{Gal}(EK/E)$. Then σ fixes E, so $\sigma|_K$ fixes $K \cap E$. If $\sigma|_K = 1$, then σ dixes E and K, so σ fixes EK. So $\sigma = 1$. Then res_K is injective.

Let H be the image. Then $K^H = K^{\mathrm{Gal}(EK/E)} = K \cap E$. So $H = \mathrm{Gal}(K/K^H) = \mathrm{Gal}(K/K \cap E)$. So res_K is onto. $\square$

Proposition 1.4. *Let K/F be finite, Galois of degree n. Then $\mathrm{Gal}(K/F)$ embeds into S_n.*

Proof. By the primitive element theorem, $K = G(\theta)$, so $\mathrm{Gal}(K/F)$ permutes the roots of the conjugates of θ, a set with n elements. This action is faithful and transitive. $\square$