20. GALOIS CORRESPONDENCE

20.1. Further characterization of Galois extensions.

**Proposition 20.1.** Let $K/F$ be a field extension.

(a) $K/F$ is Galois if and only if $K$ is a splitting field (over $F$) for some family of separable polynomials $\Omega \subseteq F[x]$.

(b) Assume that $K/F$ is finite. Then $K/F$ is Galois if and only if $K$ is a splitting field (over $F$) for some irreducible polynomial $p(x) \in F[x]$.

*Proof.* (a) “⇒” Since $K/F$ is normal, we know that $K$ is a splitting field for the set $\Omega = \{\mu_{\alpha,F}(x) : \alpha \in K\}$, and since $K/F$ is separable, each polynomial in $\Omega$ is separable.

“⇐” We only need to show that $K/F$ is separable. We are given that $K = F(A)$ where $A$ is the set of $K$-roots for some family of separable polynomials in $F[x]$. Then each $\alpha \in A$ is separable over $F$, whence by Corollary 18.6 $K/F$ is separable.

(b) “⇐” is a special case of (a), and “⇒” holds by the Primitive Element Theorem (let $\alpha$ be such that $K = F(\alpha)$, and set $p(x) = \mu_{\alpha,F}(x)$). □

Proposition 20.1(b) can be interpreted as a characterization of finite Galois extensions “from the bottom” – for a fixed field $F$, Proposition 20.1 tells us how to “produce” all finite Galois extensions of the form $K/F$. Below we will obtain a simple characterization of finite Galois extensions “from the top”, called Artin’s lemma.

**Lemma 20.2.** Let $K/F$ be a separable extension, ans suppose that there exists $n \in \mathbb{N}$ s.t. $[F(\alpha) : F] \leq n$ for all $\alpha \in K$. Then $K = F(\beta)$ for some $\beta \in K$ and thus $[K : F] \leq n$.

*Proof.* Let $\beta \in K$ be such that $m = [F(\beta) : F]$ is largest possible. If $K = F(\beta)$, we are done.

Suppose not, so there exists $\gamma \in K \setminus F(\beta)$. The extension $F(\beta, \gamma)/F$ is finite and separable, so by Primitive Element Theorem there exists $\delta \in K$ s.t. $F(\beta, \gamma) = F(\delta)$. Then $[F(\delta) : F] > [F(\beta) : F]$, contrary to the choice of $\beta$. □

**Lemma 20.3** (Artin’s Lemma). Let $K$ be a field and $G$ a finite subgroup of $\text{Aut}(K)$. Let $F = K^G = \{k \in K : gk = k \text{ for all } g \in G\}$ be the fixed field of $G$. Then $K/F$ is a finite Galois extension and $\text{Aut}(K/F) = G$. 

Proof. Take any $\alpha \in K$, and let $m = |Ga|$ be the size of the $G$-orbit of $\alpha$. Choose $\sigma_1, \ldots, \sigma_m \in G$ s.t. the elements $\sigma_1 \alpha, \ldots, \sigma_m \alpha$ are all distinct (note that one of these elements is equal to $\alpha$).

Take any $\tau \in G$. Then $\tau \sigma_1 \alpha, \ldots, \tau \sigma_m \alpha$ are also $m$ distinct elements of the $G$-orbit of $\alpha$, so

$$(\tau \sigma_1 \alpha, \ldots, \tau \sigma_m \alpha) \text{ is a permutation of } (\sigma_1 \alpha, \ldots, \sigma_m \alpha). \quad (*)$$

Consider the polynomial $f_\alpha = (x - \sigma_1 \alpha) \ldots (x - \sigma_m \alpha) \in K[x]$. As before, for any $\tau \in G$ let $\tau^*$ be the automorphism of $K[x]$ which applies $\tau$ to each coefficient. Then

$$\tau^* f_\alpha = (x - \tau \sigma_1 \alpha) \ldots (x - \tau \sigma_m \alpha) = (x - \sigma_1 \alpha) \ldots (x - \sigma_m \alpha) = f_\alpha,$$

where the middle equality holds by $(*)$. Hence $f_\alpha$ is $\tau^*$-invariant, which means that all its coefficients are $\tau$-invariant. Since this is true for any $\tau \in G$, the coefficients of $f_\alpha$ lie in $K^G = F$.

Thus, $f_\alpha \in F[x]$ and $\alpha$ is a root of $f_\alpha$, so $\mu_{\alpha,F}$ divides $f_\alpha$. Note also that by construction $f_\alpha$ is separable and splits completely over $K$, so $\mu_{\alpha,F}$ is also separable and splits completely over $K$. Since this is true for any $\alpha$, by definition $K/F$ is normal and separable, and thus Galois.

For any $\alpha \in K$ we have $[F(\alpha) : F] = \deg \mu_{\alpha,F} \leq \deg f_\alpha \leq |G|$. So, by Lemma 20.2 $[K : F] \leq |G|$, whence $|\text{Aut}(K/F)| \leq [K : F] \leq |G|$ by Theorem 19.1. On the other hand, it is clear that $G \subseteq \text{Aut}(K/F)$. Thus, we must have $G = \text{Aut}(K/F)$. \qed

20.2. Fundamental theorem of Galois theory.

Terminology: If $K/F$ is a field extension, by a subfield of $K/F$ we shall mean a field $L$ with $F \subseteq L \subseteq K$.

**Theorem 20.4** (Fundamental Theorem of Galois Theory). Let $K/F$ be a finite Galois extension and $G = \text{Aut}(K/F)$. Then there is a bijective correspondence between subgroups of $G$ and subfields of $K/F$ given by

$$\Phi: \text{subgroups of } G \rightarrow \text{subfields of } K/F, \quad H \mapsto K^H \quad \Psi: \text{subfields of } K/F \rightarrow \text{subgroups of } G, \quad L \mapsto \text{Aut}(K/L)$$

This correspondence is inclusion reversing, that is, if $H_1 \subseteq H_2$ are subgroups of $G$, then $K^{H_2} \subseteq K^{H_1}$, and if $L_1 \subseteq L_2$ are subfields of $L$, then $\text{Aut}(K/L_2) \subseteq \text{Aut}(K/L_1)$.

**Proof.** It is clear that the correspondence is inclusion reversing, so we just need to check that $\Phi$ and $\Psi$ are mutually inverse. Both directions follow easily from Artin’s Lemma. \footnote{Thanks to Sean for providing a simpler argument in the opposite direction}
For any subgroup $H$ of $G$ we have $\Psi \Phi(H) = \text{Aut}(K/K^H)$. By Artin’s Lemma $\text{Aut}(K/K^H) = H$.

Conversely, given a subfield $L$ of $K/F$, let $M = \Phi \Psi(L) = K^{\text{Aut}(K/L)}$. By Artin’s Lemma $K/M$ is Galois and $\text{Aut}(K/M) = \text{Aut}(K/L)$. Since $K/M$ and $K/L$ are both Galois, Theorem 19.1 implies that $[K : M] = [K : L]$. On the other hand, it is clear that $L \subseteq M$, and thus we must have $M = L$. □

Note: Here is a different (longer) proof of the inclusion $M \subseteq L$ which was given in class. Take any $\alpha \in M$. Since $K/F$ is normal, $K/L$ is also normal. Thus, by Lemma 19.3 $\text{Aut}(K/L)$ acts transitively on the set of $K$-roots of $\mu_{\alpha,L}(x)$. On the other hand, by definition of $M$, all elements of $\text{Aut}(K/L)$ fix $\alpha$. Thus, $\mu_{\alpha,L}(x)$ splits completely over $K$ and has no roots besides $\alpha$. Hence $\mu_{\alpha,L}(x) = (x - \alpha)^d$. If $d > 1$, then $\alpha$ is not separable over $L$, hence not separable over $F$, which is impossible as $K/F$ is separable. Therefore, $d = 1$, whence $\mu_{\alpha,L}(x) = x - \alpha$. This implies that $\alpha \in L$. 