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) "$\Rightarrow$" 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 Ω is separable.
"$\Leftarrow$" 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) "$\Leftarrow$" is a special case of (a), and "$\Rightarrow$" holds by the Primitive Element Theorem (let α 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 β. □

Lemma 20.3 (Artin's Lemma)**.** *Let K be a field and G a finite subgroup of* $\mathrm{Aut}(K)$. *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* $\mathrm{Aut}(K/F) = G$.

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

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

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

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

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

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

Thus, $f_\alpha \in F[x]$ and α is a root of f_α, so $\mu_{\alpha,F}$ divides f_α. Note also that by construction f_α 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 α, by definition K/F is normal and separable, and thus Galois.

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

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 $G = \mathrm{Aut}(K/F)$. Then there is a bijective correspondence between subgroups of G and subfields of K/F given by*

$$\Phi : \textit{ subgroups of } G \to \textit{ subfields of } K/F \qquad H \mapsto K^H$$

$$\Psi : \textit{ subfields of } K/F \to \textit{ subgroups of } G \qquad L \mapsto \mathrm{Aut}(K/L)$$

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 $\mathrm{Aut}(K/L_2) \subseteq \mathrm{Aut}(K/L_1)$.

Proof. It is clear that the correspondence is inclusing reversing, so we just need to check that Φ and Ψ are mutually inverse. Both directions follow easily from Artin's Lemma.[1]

[1]Thanks to Sean for providing a simpler argument in the opposite direction

For any subgroup H of G we have $\Psi\Phi(H) = \mathrm{Aut}(K/K^H)$. By Artin's Lemma $\mathrm{Aut}(K/K^H) = H$.

Conversely, given a subfield L of K/F, let $M = \Phi\Psi(L) = K^{\mathrm{Aut}(K/L)}$. By Artin's Lemma K/M is Galois and $\mathrm{Aut}(K/M) = \mathrm{Aut}(K/L)$. 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 $M = L$. $\square$

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 $\mathrm{Aut}(K/L)$ acts transitively on the set of K-roots of $\mu_{\alpha,L}(x)$. On the other hand, by definition of M, all elements of $\mathrm{Aut}(K/L)$ fix α. Thus, $\mu_{\alpha,L}(x)$ splits completely over K and has no roots besides α. Hence $\mu_{\alpha,L}(x) = (x - \alpha)^d$. If $d > 1$, then α 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 $\alpha \in L$.