GALOIS THEORY

We will assume on this handout that Ω is an algebraically closed field. This means that every irreducible polynomial in $\Omega[x]$ is of degree 1. Suppose that F is a subfield of Ω and that K is a finite extension of F contained in Ω. For example, we can take $\Omega = \mathbb{C}$, the field of complex numbers.

Definition: We will say that *"K is a normal extension of F"* if the following statement is true:

(1) If σ is any embedding of K into Ω over F, then $\sigma(K) = K$.

Equivalent statements. The following statements are equivalent to **(1)**.

(2) There exists a polynomial $f(x) \in F[x]$ such that K is the splitting field for $f(x)$ in Ω over F.

(3) If $\beta \in K$, then the minimal polynomial $p(x)$ for β over F factors as a product of linear polynomials in $K[x]$.

The basic propositions of Galois Theory

We will make the following assumptions in all of the propositions on this handout without further mention.

Assumption A: *The field F is either a field of characteristic zero or a finite field.*

Assumption B: *The field K is a finite, normal extension of F.*

Remark about terminology. If assumption **A** is satisfied, then *"normal extensions"* of F are also called *"Galois extensions"* of F. For such extensions, $Aut(K/F)$ is usually denoted by $Gal(K/F)$.

Proposition 1: $|Gal(K/F)| = [K : F]$.

Proposition 2: Suppose that L is a normal extension of F contained in K. Consider the map

$$\lambda : \; Gal(K/F) \longrightarrow Gal(L/F)$$

defined by $\lambda(\sigma) = \sigma|_L$ for all $\sigma \in Gal(K/F)$. Then λ is a surjective group homomorphism and $Ker(\lambda) = Gal(K/L)$. Consequently, $Gal(K/L)$ is a normal subgroup of $Gal(K/F)$ and we have a group isomorphism

$$Gal(K/F)\big/Gal(K/L) \;\cong\; Gal(L/F) \quad .$$

Proposition 3: Suppose that L is a subfield of K containing F. Let $G = Gal(K/F)$ and let $H = Gal(K/L)$. Then H is a subgroup of G and

$$L = K^H ,$$

where we define K^H by $K^H = \{a \in K \mid \sigma(a) = a \ \ for\ all\ \sigma \in H \}$.

Proposition 4: Suppose that $G = Gal(K/F)$. Suppose that H is a subgroup of G. Let $L = K^H$. Then we have

$$H = Gal(K/L) .$$

Notation. We will let $Int_{K/F}$ denote the set of fields L satisfying $F \subseteq L \subseteq K$. This is the set of *intermediate fields* for the extension K/F. We will let $Sub_{K/F}$ denote the set of subgroups H of the group $G = Gal(K/F)$.

Proposition 5: (The Fundamental Theorem of Galois Theory.) There is a one-to-one correspondence between the sets $Int_{K/F}$ and $Sub_{K/F}$ defined by the following maps Γ and Φ:

If $L \in Int_{K/F}$, define $\Gamma(L) \ = \ Gal(K/L)$.

If $H \in Sub_{K/F}$, define $\Phi(H) \ = \ K^H$.

The maps Γ and Φ are inverses of each other.

Proposition 6: Suppose that $L \in Int_{K/F}$ and $H \in Sub_{K/F}$ correspond to each other under the maps defined in proposition 5. Then $[K : L] = |H|$ and $[L : F] = [G : H]$.

Proposition 7: Suppose that L_1 and L_2 in $Int_{K/F}$ correspond to H_1 and H_2 in $Sub_{K/F}$, respectively, under the maps defined in proposition 5. Then $L_1 \subseteq L_2$ if and only if $H_2 \subseteq H_1$.

Proposition 8: Suppose that L_1 and L_2 in $Int_{K/F}$ correspond to H_1 and H_2 in $Sub_{K/F}$, respectively, under the maps defined in proposition 5. Then L_1 is isomorphic to L_2 over F if and only if H_1 and H_2 are conjugate in G.

Proposition 9: Suppose that $L \in Int_{K/F}$ and $H \in Sub_{K/F}$ correspond to each other under the maps defined in proposition 5. Then L is a normal extension of F if and only if H is a normal subgroup of G.