Modern Algebra 2 (MATH 6140)
HANDOUT 7 (April 16, 2008)

THE FUNDAMENTAL THEOREM OF GALOIS THEORY

Definition 1. The *Galois group* of an algebraic extension $\mathbb{E}/\mathbb{F}$ is $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) := \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$. If $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then the relation $\{(g,k) \in G \times \mathbb{E} \mid g(k) = k\}$ determines a Galois connection from G to $\mathbb{E}$, called *the GC of Galois theory*. An extension $\mathbb{E}/\mathbb{F}$ is *Galois* if $\mathbb{F}$ is closed in the GC of Galois theory.

$\mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$ is equal to the group of automorphisms of $\mathbb{E}$ that fix the elements of $\mathbb{F}$.

Example 2. Let G be a group of automorphisms of a field $\mathbb{K}$, and let $\mathbb{F}$ be the fixed field of G. If G is finite, it can be shown that $\mathbb{K}/\mathbb{F}$ is finite, hence algebraic. It is immediate from the definitions that $\mathbb{K}/\mathbb{F}$ is Galois. (In fact, every finite Galois extension arises this way.)

Lemma 3. *The following conditions are equivalent for finite extensions.*

(1) $\mathbb{E}/\mathbb{F}$ *is Galois.*
(2) $\mathbb{E}/\mathbb{F}$ *is separable and normal.*
(3) $\mathbb{E}$ *is the splitting field for a separable polynomial* $p(x) \in \mathbb{F}[x]$.

Theorem 4. *(Fundamental Theorem) Let* $\mathbb{E}/\mathbb{F}$ *be Galois with Galois group* G.

(1) *Every subgroup of* G *is closed in the GC of Galois theory.*
(2) *Every* $\mathbb{F}$*-subalgebra of* $\mathbb{E}$ *closed in the GC of Galois theory.*
(3) *If* $M < N < G$, *then* $[N : M] = r$ *iff* $[M^{\perp} : N^{\perp}] = r$.
(4) *If* $M < N < G$, *then* $M \lhd N$ *iff* $M^{\perp}$ *is a normal extension of* $N^{\perp}$. *When these hold,* $\mathrm{Gal}(M^{\perp}/N^{\perp}) = N/M$.
(5) *If* $M, N < G$, *then* M *is conjugate to* N *iff* $M^{\perp}$ *is conjugate to* $N^{\perp}$ *(which means some* $\sigma \in G$ *maps* $M^{\perp}$ *to* $N^{\perp}$*).*