Isomorphisms, automorphisms, and embeddings of fields.

Suppose that F and K are subfields of $\mathbf{C}$ and that K is a finite extension of F. As defined in class, a map $\sigma : K \to \mathbf{C}$ is called an *"embedding of K into $\mathbf{C}$ over F"* if σ is an injective ring homomorphism and $\sigma(a) = a$ for all $a \in F$. If $Im(\sigma) = K$, then we can regard σ as an isomorphism of K to itself. Still assuming that $\sigma(a) = a$ for all $a \in F$, we will then say that σ is an *"automorphism of K over F"*.

The set of embeddings of K into $\mathbf{C}$ over F will be denoted by $Emb_F(K, \mathbf{C})$. The set of automorphisms of K over F will be denoted by $Aut(K/F)$.

Propositions. We will make the assumptions that K/F is a finite extension and that the fields F and K are subfields of $\mathbf{C}$.

1. If $\sigma \in Emb_F(K, \mathbf{C})$, then $Im(\sigma)$ is a subfield of $\mathbf{C}$ containing F and is isomorphic to K. Furthermore, if $\alpha \in K$, $f(x) \in F[x]$, and α is a root of $f(x)$, then $\sigma(\alpha)$ is also a root of $f(x)$.

2. Suppose that $K = F(\alpha_1, \ldots, \alpha_t)$. Let $A = \{\alpha_1, \ldots, \alpha_t\}$. Suppose that $\sigma \in Emb_F(K, \mathbf{C})$. Then σ is completely determined by the restriction $\sigma|_A$.

3. The cardinality of $Emb_F(K, \mathbf{C})$ is equal to $[K : F]$.

4. Suppose that $K = F(\theta)$. Let $m(x)$ denote the minimal polynomial for θ over F. The cardinality of $Aut(K/F)$ is equal to the number of complex roots of $m(x)$ which are in K.

5. Suppose that $f(x) \in F[x]$ and that K is the splitting field for $f(x)$ over F. Suppose that $\sigma \in Emb_F(K, \mathbf{C})$. Then $Im(\sigma) = K$. Furthermore, we have $|Aut(K/F)| = [K : F]$.

6. Suppose that $f(x) \in F[x]$ and that K is the splitting field for $f(x)$ over F. Let $\theta_1, \ldots, \theta_n$ denote the distinct complex roots of $f(x)$. Let $B = \{\theta_1, \ldots, \theta_n\}$. Then the restriction $\sigma|_B$ is a bijection of the set B to itself.

7. Suppose that $f(x) \in F[x]$ and that K is the splitting field for $f(x)$ over F. Assume that $f(x)$ has n distinct roots in $\mathbf{C}$. Let $\theta_1, \ldots, \theta_n$ denote these roots. Let $B = \{\theta_1, \ldots, \theta_n\}$. Define a map

$$\rho : Aut(K/F) \longrightarrow S_B$$

by $\rho(\sigma) = \sigma|_B$ for all $\sigma \in Aut(K/F)$. Then ρ is an injective group homomorphism from $Aut(K/F)$ to S_B. The image of ρ is a subgroup of S_B whose order is equal to $[K : F]$.

8. We have $|Aut(K/F)| = [K : F]$ if and only if K is the splitting field over F for some polynomial $f(x) \in F[x]$.