THE FUNDAMENTAL THEOREM OF GALOIS THEORY

Important Theorem. If $E/k$ is a finite extension, then the following statements are equivalent.

(i) $E$ is a splitting field of some separable polynomial $f(x) \in k[x]$.
(ii) $k = E^G$, where $G$ is the group of automorphisms of $E$ fixing $k$ (i.e. $E/k$ is Galois).
(iii) Every irreducible $p(x) \in k[x]$ having one root in $E$ is separable and splits in $E[x]$.

Fundamental Theorem of Galois theory (Rotman p. 228). Let $E/k$ be a finite Galois extension with Galois group $G = \text{Gal}(E/k)$.

(i) The function

\[ \gamma : \text{intermediate fields of } E/k \rightarrow \text{subgroups of } \text{Gal}(E/k), \]

defined by $\gamma : F \mapsto \text{Gal}(E/F)$, is an order-reversing bijection with inverse

\[ \delta : \text{subgroups of } \text{Gal}(E/k) \rightarrow \text{intermediate fields of } (E/k), \]

given by $\delta : H \mapsto E^H$.

(ii) For every intermediate field $E/B/k$, $E^{\text{Gal}(E/B)} = B$. For every subgroup $H \subset \text{Gal}(E/k)$, $\text{Gal}(E/E^H) = H$.

(iii) For any two subgroups $H, K \subset \text{Gal}(E/k)$,

\[ E^{(H,K)} = E^H \cap E^K \]

(where $\langle H, K \rangle$ means the subgroup generated by $H, K$) and

\[ E^{H \cap K} = \langle E^H, E^K \rangle \]

(where $\langle E^H, E^K \rangle$ means the subfield generated by $E^H, E^K$, called the compositum).

For any two intermediate fields $B$ and $C$ of $E/k$,

\[ \text{Gal}(E/(B,C)) = \text{Gal}(E/B) \cap \text{Gal}(E/C) \quad \text{and} \quad \text{Gal}(E/(B \cap C)) = \langle \text{Gal}(E/B), \text{Gal}(E/C) \rangle. \]

(iv) For every intermediate field $B$ between $k$ and $E$, $[B : k] = [G : \text{Gal}(E/B)]$. (The left is the degree of a field extension, and the right is an index of a subgroup!) For every subgroup $H$ of $\text{Gal}(E/k)$, $[G : H] = [E^H : k]$.

(v) If $B$ is an intermediate field, then $B/k$ is Galois iff $\text{Gal}(E/B)$ is a normal subgroup of $\text{Gal}(E/k)$. In this case, $\text{Gal}(B/k) = \text{Gal}(E/k)/\text{Gal}(E/B)$. 

Date: Thursday, December 5, 2002.