Section 53: Galois Theory

Def: A finite extension K of F is a *finite normal extension* of F if K is a separable splitting field over F.

Thm. Let K be a finite normal extension of F, and let E be an extension of F, where $F \leq E \leq K \leq \bar{F}$. Then K is a finite normal extension of E, and $G(K/E)$ is precisely the subgroup of $G(K/F)$ consisting of all automorphisms that leave E fixed. Moreover, two automorphisms in $G(K/F)$ induce the same isomorphism of E onto a subfield of $\bar{F}$ if and only if they are in the same left coset of $G(K/E)$ in $G(K/F)$.

Def: If K is a finite normal extension of a field F, then $G(K/F)$ is the *Galois group* of K over F.

Note: Galois groups are basically groups of automorphisms on a field. They are actually very similar to permutation groups since they are groups of functions that "rearrange" a set.

Main Theorem of Galois Theory: Let K be a finite normal extension of a field E, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a 1-1 map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ:

1. $\lambda(E) = G(K/E)$
2. $E = K_{G(K/E)} = K_{\lambda(E)}$
3. For $H \leq G(K/F), \lambda(K_H) = H$
4. $[K : E] = |\lambda(E)|$ and $[E : F] = (G(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $G(K/F)$.
5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, then $G(E/F) \simeq G(K/F)/G(K/E)$.
6. The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.

Def: If $f(x) \in F[x]$ is such that every irreducible factor of $f(x)$ is separable over F, then the splitting field K of $f(x)$ over F is a normal extension of F. The Galois group $G(K/F)$ is the *group of the polynomial* $f(x)$ over F.

Thm. Let K be a finite extension of degree n of a finite field F of p^r elements. Then $G(K/F)$ is cyclic of order n, and is generated by σ_{p^r}, where for $\alpha \in K$, $\sigma_{p^r}(\alpha) = \alpha^{p^r}$.