Math 332

A Brief Introduction to Galois Theory

David Perkinson

Reed College
Portland, OR

Spring 2009

An algebraic extension $E \supset F$ is a Galois extension if it is normal and separable.

normal: Every irreducible $p \in F[x]$ having a root in E splits into linear factors over E.

separable: No irreducible $p \in F[x]$ has repeated roots in an algebraic closure of F. (Separability is automatic if $\mathrm{char}(F) = 0$, e.g. $F = \mathbb{Q}$.)

Suppose $E \supset F$ is a Galois extension. Then the Galois Group for E/F is

$$\begin{aligned} \mathrm{Gal}(E/F) &= \mathrm{Aut}_F E \\ &= \{\text{invertible } \sigma\colon E \to E \mid \sigma(x) = x \text{ for all } x \in F\} \end{aligned}$$

The Galois group is the group of field automorphisms of E fixing the base field, F.

Galois Correspondence

Let $E \supset F$ be a Galois extension.

Fields		Groups
$E \supseteq K \supseteq F$	$\longrightarrow$	$\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$
$\mathrm{Fix}(H)$	$\longleftarrow$	$H \leq \mathrm{Gal}(E/F)$

where $\mathrm{Fix}(H) = \{x \in E : \sigma(x) = x \text{ for all } \sigma \in H\}$.

Fundamental Theorem of Galois Theory

Theorem. The Galois correspondence is an inclusion reversing 1-1 correspondence.

Facts:

- $[E : K] = |\mathrm{Gal}(E/K)|$.
- $E \supseteq K$ is a normal extension iff $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$.
- If $H \leq \mathrm{Gal}(E/F)$ and $\sigma \in \mathrm{Gal}(E/F)$, then $\mathrm{Fix}(\sigma H \sigma^{-1}) = \sigma(\mathrm{Fix}(H))$.
- There are finitely many intermediate fields $E \supseteq K \supseteq F$.

Radical Extensions

$E \supseteq F$ is a simple radical extension if $E = F(\alpha)$ where $\alpha^n \in F$ for some $n > 0$. Thus, α satisfies on equation of the form $x^n - \beta$ for some $\beta \in F$.

$E \supseteq F$ is a radical extension if there exist intermediate fields

$$E = F_n \supset F_{n-1} \supset \cdots \supset F_0 = F$$

where $F_i \supset F_{i-1}$ is a simple radical extension for all i.

Solvablility

$f \in F[x]$ is solvable by radicals if the field generated by its roots in an algebraic closure of F is contained in a radical extension of F.

A finite group G is solvable if its composition series

$$G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

has cyclic factors, G_i/G_{i-1}.

Galois' Theorem

Theorem. Suppose $\mathrm{char}(F) = 0$. Let $f \in F[x]$, and let E be the field generated by the roots of f in some algebraic closure of F. Then f is solvable by radicals iff $\mathrm{Gal}(E/F)$ is a solvable group.