Abstract Algebra

Introduction to Galois Theory

ThinkBS: Basic Sciences in Engineering Education

Kadir Has University, Turkey

In this part we will try to answer the question that "Are there general solutions by radicals for polynomials of degree 5 and higher?"

The answer as you may probably know is No.

Here we translate this question into question about fields and use Galois theory to translate into question about groups and answer it.

When we talk about solving an equation by radicals, we mean if that given a polynomial $p(x)$ with coefficients in K and of degree 5 or higher, is there a sequence of radical extensions

$$K_0 = K \subseteq K_1 = K(\sqrt[r_1]{a_1}) \subseteq \cdots \subseteq K_n = K_{n-1}(\sqrt[r_{n-1}]{a_{n-1}})$$

with $r_i \in \mathbb{N}$ and $a_{i+1} \in K_i$, such that all of the roots of $p(x)$ are in $K_n = K(\sqrt[r_1]{a_1}, \sqrt[r_2]{a_2}, \ldots, \sqrt[r_{n-1}]{a_{n-1}})$?

Here we should note that all radical extensions are algebraic extensions.

Separable Extensions

We have talked about simple, Algebraic and normal field extensions. Here we also need to define separable and Galois extensions as following:

A **separable extension** L of K is a field extension such that for all $a \in L$, there exists an irreducible polynomial $m(x)$ with coefficients in K with distinct roots.

Example: Any algebraic extension of $\mathbb{Q}$, such as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a separable extension.

A **Galois extension** of K is a field extension that is algebraic, normal, and separable over K.

Galois Group

Let σ be an automorphism of the field E. Then the set E_σ of all the elements $a \in E$ that remain fixed by σ forms a subfield of E. Also if $\{\sigma_i \mid i \in I\}$ is a collection of automorphisms of a field E, then the set $E_{\{\sigma_i\}}$, of all $a \in E$ that remain fixed by every σ_i for $i \in I$, is a subfield of E.

Let $K \leq L$ be a field extension. We define the set $Gal(L/K)$ as the set of all automorphisms of the field L that fix every element of the field K. This is a group and it is called the Galois group.

Fundamental Theorem of Galois Theory

If L is a finite Galois extension of K, then there is a one-to-one correspondence between the field extensions of K that are contained in L and the subgroups of $Gal(L/K)$.