18.704: Seminar in Algebra and Number Theory
Oleg Shamovsky
05/17/05

Introduction to Galois Theory

The aim of Galois theory is to study the solutions of polynomial equations

$$f(t) = t^n + a_{n-1}t^{n-1} + \ \dots\ + a_0 = 0$$

and, in particular, to distinguish those that can be solved by a formula from those that cannot. By formula we mean a radical expression, anything that can be built up from the coefficients a_i by the operations of addition, subtraction, multiplication, and division, and also by n-th roots for $n = 2, 3, 4, \dots$.

Galois Groups

Let L be a field extension of K, denoted $L : K$, and let G be the set of automorphisms of $L : K$. In other words, G is the set of automorphisms σ of L such that $\sigma(x) = x$ for every $x \in K$, so that K is fixed. Then G is a group of transformations of L, called the Galois group of $L : K$. The Galois group of $L : K$ is denoted $Gal(L : K)$.

Let $f(x)$ be a rational polynomial of degree n and let K be the splitting field of $f(x)$ over $\mathbb{C}$. By "splitting field of $f(x)$ over $\mathbb{C}$" we mean the extension field K of a field $\mathbb{C}$ if $f(x)$ factors completely into linear factors in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing $\mathbb{C}$. In other words, K is the smallest subfield of $\mathbb{C}$ containing all the roots of f. Then, each element of the Galois group $G = Gal(K : \mathbb{C})$ uniquely permutes the roots of f. Thus, G can be identified with a subgroup of the symmetric group S_n, the group of permutations of the roots of f. If f is irreducible then G is a transitive subgroup of S_n. This means that given two roots α and β of f, there exists an element σ of G such that $\sigma(\alpha) = \beta$.

The roots of f are solvable by radicals if and only if G is a solvable group. Since all subgroups of S_n with $n \leq 4$ are solvable, the roots of all polynomials of degree up to 4 are solvable by radicals.

Galois's Theorem: An algebraic equation is algebraically solvable if and only if its group is solvable. In order that an irreducible equation of prime degree be solvable by radicals, this is necessary and sufficient that all its roots be rational functions of two roots.

The Fundamental Theorem

Let $L : K$ be a field extension in $\mathbb{C}$ with Galois group G, which consists of all K-automorphisms of L. Let $\mathcal{F}$ be the set of intermediate fields, that is, subfields M such that $K \subseteq M \subseteq L$, and let $\mathcal{L}$ be the set of all subgroups H of G. We now define two maps:

$$^* : \mathcal{F} \to \mathcal{L}$$
$$^\dagger : \mathcal{L} \to \mathcal{F}$$

as follows: if $M \in \mathcal{F}$, then M^* is the group of all M-automorphisms of L. If $H \in \mathcal{L}$, then $H^\dagger$ is the fixed field of H.

Theorem: Fundamental Theorem of Galois Theory
If $L : K$ is a finite normal filed externsion inside $\mathbb{C}$, which Galois group G, and if $\mathcal{F}$,$\mathcal{L}$,$*$,$\dagger$ are defined as above, then:
1. The Galois group G has order $[L : K]$.
2. The maps * and † are mutual inversis, and set up an order-reversing one-to-one correspondance between $\mathcal{F}$ and $\mathcal{L}$.
3. If M is an intermediate field, then

$$[L : M] = |M^*| \qquad [M : K] = |G|/|M^*|$$

4. An intermediate field M is a normal extension of K if and only if M^* is a normal subgroup.
5. If an intermediate field M is a normal extension of K, then the Galois group of $M : K$ is isomorphic to the quotient group G/M^*.

Proof. The proof of this theorem requires a few more theorems and definitions which we will not have time for in today's presentation. However, I urge the curious math enthusiasts to look up the proof in a book entitled "Galois Theory" by Ian Stewart which I have used to prepare today's presentation and notes. The first part of these notes was adapted from the "Galois Group" article on Wikipedia.com.