8. Galois Theory Examples and Applications

Examples and Applications

The "general polynomial"

The polynomial $F_n(T) = (T - x_1) \cdots (T - x_n)$, where the x_i are indeterminants, is called the general polynomial of degree n. The group S_n permutes the x_i and acts as automorphisms of the field $E(x_1, \ldots, x_n)$ where E is any field.

The coefficients of $F_n(T)$ are, up to sign, the elementary symmetric functions s_i of the roots x_i. Therefore the field $E(s_1, \ldots, s_n)$ is contained in the fixed field of S_n on $E(x_1, \ldots, x_n)$. Therefore $[E(x_1, \ldots, x_n) : E(s_1, \ldots, s_n)] \geq n!$.

On the other hand, $E(x_1, \ldots, x_n)$ is the splitting field of $F_n(T)$ over $E(s_1, \ldots, s_n)$. Therefore $[E(x_1, \ldots, x_n) : E(s_1, \ldots, s_n)] \leq n!$.

Thus the galois group of this extension is S_n.

In particular any symmetric function in the roots of a polynomial can be written in terms of the coefficients of the polynomial.

The discriminant

The discriminant of a polynomial is the product of the differences of its distinct roots squared:

$$\Delta = \prod_{i<j} (x_i - x_j)^2$$

It is a symmetric function of the roots.

If Δ is a square, then the galois group of the polynomial is contained in the alternating group.

Solvability by radicals

A radical extension K/F is a field extension that can be constructed by a succession of simple radical extensions where $K_{i+1} = K_i(\alpha_{i+1})$ where $\alpha_{i+1}^{n_{i+1}} \in K_i$.

Notice that any field extension generated by roots of unity is a radical extension.

Theorem (Kummer): Suppose that F is a field containing the n^{th} roots of unity where the characteristic of F does not divide n. Then K/F is a cylic galois extension (i.e. has cyclic galois group) of degree n if and only if $K = F(\alpha)$ where $\alpha^n \in F$.

Solvability by radicals

A polynomial is "solvable by radicals" (meaning its roots like in a radical extension) if and only if the Galois group is solvable.

The polynomial $x^5 - 6x + 3$ has Galois group S_5.