Math 368

Field Extensions and Galois Theory

Ömer Küçüksakallı - Spring 2011, METU

Many mathematicians describe a mathematical theory to be elegant if it connects two different mathematical concepts in a surprising way. In this sense Galois theory provides a beautiful connection between field theory and group theory. Certain problems in field theory can be reduced to the problems in group theory which are better understood.

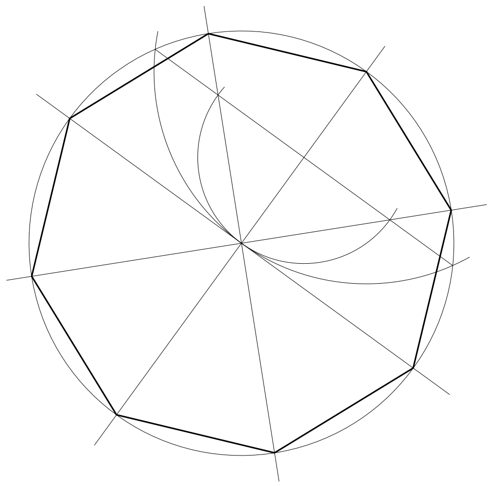
$$\text{An interesting problem in field theory} \xrightarrow{\text{Galois theory}} \text{A well-understood problem in group theory}$$

One of the most important application of Galois theory is the criteria for solvability by radicals. We say that a polynomial equation can be solved by radicals if its roots can be written using n-th roots. For example, the equation $x^6 - 2x^3 - 1 = 0$ can be solved by radicals since $\sqrt[3]{1+\sqrt{2}}$ is a root (the other roots can be found similarly). The roots of the quadratic equation $ax^2 + bx + c = 0$ can be obtained by

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

One can find general formulas for cubic and quartic equations with increasing complexity. However there are quintic equations which cannot be solved by radicals, such as $x^5 - x - 1 = 0$. There is a natural group which permutes the roots of any polynomial equation. This group is called the Galois group and enables us to give a criteria for solvability by radicals.

Compass-and-straightedge construction is one of the most well-known problems in field theory. A basic question is whether or not we can create a regular polygon with n edges by using a ruler and a compass. For example, starting with two distinct points, we can create two circles. From these circles, two new points are created at their intersections. Drawing lines between the two original points and one of these new points completes the construction of a regular polygon with 3 edges, namely the equilateral triangle. We can also construct a regular polygon with 8 edges as shown in the figure. There is a surprising connection between this geometric problem and field theory. Using this connection we can determine those values of n, for which we can construct a regular n-gon with a ruler and a compass.



Field extensions and Galois theory are fundamental tools in modern number theory. For example, consider the Fermat's equation $x^p + y^p = z^p$ which has only trivial solutions for odd primes p. Once we factorize this equation

$$\prod_{j=0}^{p-1} (x + \zeta_p^j y) = z^p,$$

we start to feel the close relationship between the integer solutions of Fermat's equation and the cyclotomic field extension $\mathbb{Q}(\zeta_p)$.