

From Groups to Fields, an introduction to Galois Theory and its applications.

Bianca B. Dornelas*, Francesco Matucci

Abstract

In this project we studied all the fundamental tools in Galois Theory. We moved from groups and their properties to rings and fields, concluding with the analysis of when polynomials in one variable of any degree have a solution expressible by radicals. The main results we studied are Galois Theorem for Polynomials and the Fundamental Theorem of Galois Theory.

Key words:

Groups, Galois correspondence, solvability by radicals

Introduction

Galois Theory proposes to verify whether or not a polynomial in one variable of any degree has a solution **expressible by radicals**, i.e., if its roots have a formula that depends only on the coefficients of the polynomial. This is carried out through the analysis of the corresponding Galois Group and its properties.

In this project we learned methods related to finite groups, rings, fields, rings and fields extensions and polynomials rings, connecting groups properties with the solvability by radicals of polynomials.

Results and Discussion

Given a set G with operation $*$, the pair $(G, *)$ is said to be a **group** if, for any $a, b \in G$, we have that $a*b \in G$ and the operation $*$ is associative, has an identity e and admits inverses. A **subgroup** G is a subset H of G that is also a group under $*$.¹

A **field** is a triple $(F, *, +)$ where F is a set that is an abelian group under the operation $+$ and where all of its non-zero elements form an abelian group under $*$.²

An **isomorphism** is a bijective function $f: G \rightarrow H$ that preserves the operation of two groups G and H , i.e., it is a bijection $f: (G, *) \rightarrow (H, +)$ groups such that $f(a*b) = f(a)*f(b)$ for all $a, b \in G$ and $.$ If G and H are fields (rather than groups), the same must hold for the second operation too in order to have a **field isomorphism**.²

These basic concepts and some of their properties allow us to define different types of groups and fields that will be useful in the study of the main theorems of the research:

If E and F are fields such that $F \subseteq E$ (they form a **field extension**) and G is the set of all isomorphisms from E to E that fix pointwise all elements of F , then G is a group under composition and we call it the **Galois Group** of the extension.³

One can see E as the splitting field of a polynomial with coefficients in F , i.e., the smallest field that contains all the zeros of the polynomial. It is possible to prove that the Galois group of the polynomial is unique up to isomorphism.

A field extension $F \subseteq E$ is said to be a **Galois extension** (also known as a **normal extension**), if every

irreducible polynomial with coefficients in F that has a zero in E is separable and has all its zeros in E .

Now we are able to state the main results that we learned through this research, Theorems 1 and 2 below.

Theorem 1 (Fundamental Theorem of Galois Theory)

– If $F \subseteq E$ is a Galois extension, then there is an isomorphism between the set of {subgroups of the Galois group} and the set of {subfields of E which contain F }. Moreover, if H is a normal subgroup of the Galois group, then $F \subseteq E^H$ is a normal extension, where E^H is the **fixed field** of H in E ; in addition, if H is subgroup of K subgroup of G , then $E^H \supseteq E^K$.

Theorem 2 (Galois Theorem) –

Given a field F with **characteristic 0** (it is never possible to get the additive identity by adding an element $a \in F$ finitely many times) and $f(x)$ a polynomial with coefficients in F , then $f(x)$ is solvable by radicals if, and only if, the Galois group of the extension $F \subseteq E$ with E the splitting field of $f(x)$ is a **solvable group**.

It was verified, through a lot of examples, that Theorem 1 is very helpful in the process to find out whether or not a Galois group is solvable. This allows us to use Theorem 2 and determine if a polynomial is solvable by radicals, independently of the degree of the polynomial.

Conclusions

The student has learned all the basics about groups, rings, fields, their properties and main examples. Moreover, the mathematical language was practiced through written reports.

With this new language available, it was then possible to study the solvability of polynomials and verify the proof of Galois Theorem.

¹ L. Gilbert, Elements of Modern Algebra, Cengage Learning, 2008

² A. Papantonopolous, Algebra - Pure and Applied, Pearson Education, 2001

³ I. N. Herstein, Topics in Algebra, John Wiley & Sons, 1975