# Expository Paper: Galois Theory and Polynomials

Chris Hayduk

December 15, 2020

### Abstract

Galois theory has been a fundamental topic in the overarching field of algebra. Its development spurred the creation of many concepts which are today central to the field, such a groups [1, 5]. Most notably though, Galois theory furnished us with the ability to describe the solutions to polynomials of arbitrary degree, an achievement that eluded mathematicians for thousands of years [1]. In this expository paper, we will build up the necessary background knowledge in polynomials and abstract algebra in order to understand Galois' elegant theorems. We will then demonstrate the power of these theorems in finding solutions to polynomial equations.

# 1 Polynomials

## 1.1 Introduction

A *polynomial* is defined by Wikipedia as "an expression consisting of variables and coefficients, that involves only the addition, subtraction, multiplication, and non-negative integer exponentiation of variables" [7]. To be more precise, we can define a *polynomial* over the rational numbers, $QQ$, in the variable $x$ to be the expression,

$$p(x) = r_0 + r_1 x + \cdots + r_n x^n$$

where $r_0, \ldots, r_n \in \mathbb{Q}$, $0 \leqslant n \in \mathbb{Z}$, and $x$ is undefined [4, §2.1, p. 36]. We can denote the set of all polynomials over $\mathbb{Q}$ in $x$ by $\mathbb{Q}[x]$.

Polynomials of this form have been a central theme of mathematics for thousands of years, dating back to at least the Babylonians of 1600 BC [4, p. 2]. During this early period of research into polynomials, mathematicians were primarily concerned with polynomials in one variable. That is, the polynomial was represented by an equation with a single variable that could potentially have separate different exponential terms. For example, the equation $x^2 + 2x + 1$ is a common polynomial in one variable. The variable $x$ is an element of a field. For earlier mathematicians, this usually meant rational numbers, until eventually real numbers were introduced. The term with the highest *degree* (that is, the largest value of an exponent of $x$) gives us the degree of the polynomial. In our previous example, we have a polynomial in one variable with degree 2. Formally, we can define this as follows,

**Definition** ([4, Definition 2.1]). If $f$ is a polynomial and $f \neq 0$, then the *degree* of $f$ is the highest power of $t$ occurring in $f$ with non-zero coefficient. We write $\partial f$ for the degree of $f$.

Finding the zeros of polynomials was a very active field of research for many centuries, with the goal of finding a general, closed form solution for the polynomials of each degree [4, p. 3-5]. If we take a degree 1 polynomial, such as $x + 1$, finding the zeros amounts to solving the equation $x + 1 = 0$, which is $x = -1$ by our basic rules of algebra and arithmetic. However, the situation rapidly becomes significantly more complicated as the degree of the polynomial increases.

In the situation of *quadratic polynomials* (that is, polynomials of degree 2), we need to solve them using radicals. For example, the equation $x^2 - 2 = 0$ is solved by $x = \pm\sqrt{2}$. However, note here that, although our coefficients are in $\mathbb{Q}$, our answer does not exist in $\mathbb{Q}$. Thus, for quadratic equations, we must extend from $\mathbb{Q}[x]$ to $\mathbb{R}[x]$ in order to find a solution. Similarly, the equation $x^2 + 2 = 0$ is solved by $x = \pm\sqrt{-2}$. Hence, once we get to the case of degree 2 polynomials, we need to go beyond real numbers and use the complex numbers ($\mathbb{C}$) in order to furnish a general theory for their solution. We denote the set of such polynomials by $\mathbb{C}[x]$. We can now give the general quadratic formula to solve equations of the form $ax^2 + bx + c = 0$, given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Closed form equations of this kind were eventually found for cubic (degree 3) and quartic (degree 4) polynomials [4, §1.4, p. 25-29]. However, a closed form for solutions to quintic (degree 5) polynomials continued to elude mathematics researchers for centuries [4, §1.4, p. 31]. Many mathematicians began to ask if the number system they were working in needed to be expanded yet again, just as the extensions to the real numbers and eventually the complex numbers allowed them to solve polynomials of greater complexity [4, §2.2, p. 39]. However, equipped with the following theorem, we can show that this is not the case [4, §2.2, p. 41]:

**Theorem** ([4, Thm. 2.4], **The Fundamental Theorem of Algebra**). *If $p(z)$ is a non-constant polynomial over $\mathbb{C}$, then there exists $z_0 \in \mathbb{C}$ such that $p(z_0) = 0$.*

Hence, we can see that every polynomial over $\mathbb{C}$ also has a root in $\mathbb{C}$, avoiding the pitfall we ran into when considering $x^2 + 1 = 0$ over $\mathbb{R}$. Thus, it is not necessary to expand to a more "general" number system in order to solve higher degree polynomials.

## 1.2 Factorization

We can now begin to discuss the factorization of polynomials. Factoring a polynomial into several polynomials of smaller degree allows us to simply the root-finding problem, as we can then search for the roots of the new polynomials, rather than the original equation. A familiar example would be $x^2 - 1$. This polynomial can be factored into $(x+1)(x-1)$, and so finding the roots of $x^2 - 1 = 0$ simplifies to finding the roots of $x + 1 = 0$ and $x - 1 = 0$. The two degree 1 equations yield $x = -1$ and $x = 1$ quite quickly.

To formalize factorization of polynomials, we first need to introduce a few theorems:

**Theorem** ([4, Thm. 2.5], **Remainder Theorem**). *Let $p(x) \in \mathbb{C}[x]$ with $\partial p \geqslant 1$, and let $\alpha \in \mathbb{C}$.*

1. *There exist $q(t) \in \mathbb{C}[x]$ and $r \in \mathbb{C}$ such that $p(x) = (x - \alpha)q(x) + r$*
2. *The constant $r$ satisfies $r = p(\alpha)$*

**Proposition** ([4, Prop. 3.1], **Division Algorithm**). *Let $f$ and $g$ be polynomials over $K$ and suppose that $f$ is non-zero. Then there exist unique polynomials $q$ and $r$ over $K$, such that $g = fq+r$ and has strictly smaller degree than $f$.*

The above theorem and proposition allow us to divide polynomials by other polynomials, paving the way for us to discuss the polynomial equivalent of prime numbers: *irreducible polynomials.* A non-constant polynomial over a subring $R$ of $\mathbb{C}$ is *reducible* if it is a product of two polynomials over $R$ of smaller degree. Otherwise it is *irreducible* [4, §3.2, p. 51].

**Examples.**

1. All degree 1 polynomials are irreducible
2. As above, $x^2 - 1 = (x+1)(x-1)$ and is hence a reducible polynomial

Now we can assert an analogue of prime factorization for polynomials in $\mathbb{C}$:

**Theorem** ([4, Thm. 3.12])**.** *Any non-zero polynomial over a subring $R$ of $\mathbb{C}$ is a product of irreducible polynomials over $R$.*

*Proof.* Let $g$ be a polynomial over $R$ such that $g \neq 0$. We will proceed with this proof through induction. Let us start with cases $\partial g = 0$ and $\partial g = 1$. A fact about polynomials is, for two polynomial $f, h$ over $R$, we have $\partial fh = \partial f + \partial h$. So in both cases for $g$, it is not possible to find two polynomials $f, h$ with degree smaller than $g$ such that $g = fh$. Now fix $n \in \mathbb{N}$ with $n > 1$, let $\partial g = n$, and suppose for all $k < n$, we have that polynomials of $\partial k$ are reducible. We have two possible cases: either $g$ is irreducible (in which case we are done) or $g = fh$ for two polynomial $f, h$ with $\partial f, \partial h < \partial g$. But by our induction hypothesis, $f$ and $g$ are products of irreducible polynomials, and so $g$ is the product of irreducible polynomials. □

The framework for the above poor is taken from: [4, §3.2, p. 52].

### 1.3 Zeros of Polynomials

We can now discuss some useful properties of the zeros of polynomials. If $R$ is a subring of $\mathbb{C}$ and $f$ is a polynomial over $R$, then an element $\alpha \in R$ such that $f(\alpha) = 0$ is a *zero of $f$ in $R$.*

**Definition** ([4, Definition 3.26]). Let $f$ be a polynomial over the subfield $K$ of $\mathbb{C}$. An element $\alpha \in K$ is a *simple zero* of $f$ if $(x-\alpha)|f(x)$ but $(x-\alpha)^2$ does not divide $f(x)$. The element $\alpha$ is a zero of $f$ of *multiplicity* $m$ if $(x-\alpha)^m|f(x)$ but $(x-\alpha)^{m+1}$ does not divide $f(x)$. Zeros of multiplicity greater than 1 are *repeated* or *multiple zeros.*

**Lemma** ([4, Lemma 3.27])**.** *Let $f$ be a non-zero polynomial over the subfield $K$ of $\mathbb{C}$, and lets its distinct zeros be $\alpha_1, \ldots, \alpha_r$ with multiplicities $m_1, \ldots, m_r$ respectively. Then,*

$$f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r} g(x)$$

*where $g$ gas no zeros in $K$. Conversely, if the above equation holds and $g$ has no zeros in $K$, then the zeros of $f$ in $K$ are $\alpha_1, \ldots, \alpha_r$ with multiplicities $m_1, \ldots, m_r$ respectively.*

Lastly, from this lemma we get an important theorem:

**Theorem** ([4, Thm. 3.28])**.** *The number of zeros of a nonzero polynomial over a subfield of $\mathbb{C}$, counted according to multiplicity, is less than or equal to its degree.*

# 2 Field Theory

## 2.1 Introduction

While Galois Theory initially was treated by examining polynomials directly, algebraists eventually switched to examining the more general field extensions related to a polynomial [4, §4, p. 63]. We'll start by providing some definitions regarding fields in order to have the necessary background to discuss field extensions.

**Definition** ([3, §7.1]). A ring $R$ with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field.*

**Definition** ([3, §7.1]). A *subring* of the ring $R$ is a subgroup of $R$ that is closed under multiplication.

**Definition** [4, §1.2]] A *monomorphism* is a homomorphism which is injective but not necessarily surjective.

Now, with these three definitions in mind, we can introduce field extensions.

## 2.2 Field Extensions

We define a field extensions as follows:

**Definition** ([4, Definition 4.1]). A *field extension* is a monomorphism $\tau : K \to L$ where $K$ and $L$ are subfields of $\mathbb{C}$. We say that $K$ is the *small* field and $L$ is the *large* field.

We make this distinction between $K$ and $L$ as the small and large fields due to the properties of $\tau$ as a monomorphism. Since $\tau$ is injective but not necessarily surjective, we know that $L$ is at least as large as $K$ but could potentially be larger. Hence, we call it the *large* field. We can also use the notation $L : K$ to denote a field extension, and we say that $L$ is an *extension* of $K$. We now need to introduce two more definitions before moving on to simple extensions:

**Definition** ([4, Definition 4.3]). Let $X$ be a subset of $\mathbb{C}$. Then the subfield of $\mathbb{C}$ *generated* by $X$ is the intersection of all subfields of $\mathbb{C}$ that contain $X$

**Definition** ([4, Definition 4.7]). If $L : K$ is a field extension and $Y$ is a subset of $L$, then the subfield of $\mathbb{C}$ generated by $K \cup Y$ is written $K(Y)$ and is said to be obtained from $K$ by *adjoining* $Y$.

### 2.3 Simple Extensions

Simple extensions are field extensions obtained by adjoining one element:

**Definition** ([4, Definition 4.10]). A *simple extension* is a field extension $L : K$ such that $L = K(\alpha)$ for some $\alpha \in L$.

**Example.** We have that $\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$ is a simple extension of the field $\mathbb{Q}$.

## 3 Galois Theory

### 3.1 Overview

We can now return to the main objective of our work: finding a general solution for polynomials of degree 5 (or higher). The general idea Galois used to approach this idea was associating to each polynomial $p \in \mathbb{C}[x]$ a group of permutations which we now call the *Galois group* of $p$ [4, §8, p. 107]. In this way, we are able to reduce very difficult questions about a polynomial to simpler questions about its Galois group. Galois specifically introduced this concept in order to study solutions to quintic polynomials and, as we will soon demonstrate, he showed that there is no quintic formula [5]. Moreover, he was able to describe *which* degree 5 polynomials are solvable by radicals [5].

We will start by illustrating an example from [4, §8.2] in order to give some intuition behind Galois theory. Consider the polynomial $f(x) = x^4 - 4x^2 - 5 = 0$. As discussed before, we can factor this polynomial into the product of irreducible polynomials, yielding $f(x) = (x^2 + 1)(x^2 - 5) = 0$. As a result, we find the following roots: $x = i, -i, \sqrt{5}, -\sqrt{5}$. There is a natural sort of relation between $i, -i$ and $\sqrt{5}, -\sqrt{5}$, and we actually see that the elements in each of these pairs are indistinguishable from the other element in the pair algebraically. That is, if we construct a polynomial equation with rational coefficients that is satisfied by a subset of our four roots, we can interchange $i$ and $-i$ or $\sqrt{5}$ and $-\sqrt{5}$ without altering the equation. If we label the roots in the following manner,

$$\alpha = i, \ \beta = -i, \ \gamma = \sqrt{5}, \ \delta = -\sqrt{5}$$

then we can label the "allowable" symmetries using the notation from Dummit and Foote:

$$(\alpha\beta), \ (\alpha\beta)(\gamma\delta), \ (\gamma\delta), \ I$$

where $I$ is the identity. These four symmetries make up the symmetry group of the roots of our polynomial $f(x)$. We can use these polynomial equations of our roots to solve any polynomial that shares this same root structure. That is, the solutions of a polynomial are tied directly to the structure of the symmetric group of its roots.

## 4 Conclusion

Galois' main point of relating the symmetric group of polynomials' roots to its solutions provided an elegant and powerful new paradigm for addressing the solutions of polynomials.

## References

[1] Bewersdorff, Jorg. *Galois Theory for Beginners.* American Mathematical Society, 2006.

[2] Brzeziński, Juliusz. *Galois Theory Through Exercises.* Springer, 2018.

[3] Dummit, David Steven., and Richard M. Foote. *Abstract Algebra.* 3rd ed., John Wiley & Sons, 2004.

[4] Stewart, Ian. *Galois Theory.* Chapman & Hall/CRC, 2015.

[5] "Wikipedia – Galois Theory." *Wikipedia*, Wikimedia Foundation, `https://en.wikipedia.org/wiki/Galois_theory`.

[6] "Wikipedia – Fundamental Theorem of Galois Theory." *Wikipedia*, Wikimedia Foundation, `https://en.wikipedia.org/wiki/Fundamental_theorem_of_Galois_theory`.

[7] "Wikipedia – Polynomial." *Wikipedia*, Wikimedia Foundation, `https://en.wikipedia.org/wiki/Polynomial`.