University of Mary Washington
Eagle Scholar

Student Research Submissions

Spring 5-6-2020

Exploration of Solvable Quintic Polynomials

Stephen Tivenan

Follow this and additional works at: https://scholar.umw.edu/student_research

 Part of the Mathematics Commons

Recommended Citation

Tivenan, Stephen, "Exploration of Solvable Quintic Polynomials" (2020). *Student Research Submissions*. 326.
https://scholar.umw.edu/student_research/326

This Honors Project is brought to you for free and open access by Eagle Scholar. It has been accepted for inclusion in Student Research Submissions by an authorized administrator of Eagle Scholar. For more information, please contact archives@umw.edu.

Exploration of Solvable Quintic Polynomials

Stephen Tivenan

submitted in partial fulfillment of the requirements for Honors in Mathematics at the University of Mary Washington

Fredericksburg, Virginia

April 2020

This thesis by **Stephen Tivenan** is accepted in its present form as satisfying the thesis requirement for Honors in Mathematics.

Date	Approved
_____	_____
	Larry Lehman, Ph.D. thesis advisor
_____	_____
	James Collins, Ph.D. committee member
_____	_____
	Janusz Konieczny, Ph.D. committee member

Contents

Abstract

A polynomial $f(x)$ with rational coefficients is solvable by radicals if its roots (in the field of complex numbers $\mathbb{C}$) can be expressed in terms of its coefficients using the basic operations and radicals. It is known that for quintic polynomials there is no generic formula for the roots. That is, some quintic polynomials are solvable and some are not. In this paper, we address the mathematical theory that makes the formula for the roots of a polynomial. Primarily we will focus on our methodology of generating and examining quintic polynomials. In one case study, we will examine quintic polynomials that may have roots that can be expressed in a radical form. In the other case study we show the methodology of generating polynomials that do have solutions which can be expressed in a radical form from the coefficients of the polynomials.

1 Introduction

General formulas for expressing the roots of $f(x) \in \mathbb{Q}[x]$ (from the coefficients of $f(x)$ using the basic operations and radicals) exist for polynomials of degree $2, 3$, and 4. For example, the quadratic formula gives us the roots of a generic quadratic polynomial (e.g. $ax^2 + bx + c, x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$). It follows that every non-constant polynomial of degree ≤ 4 is solvable by radicals. However, no such formulas exist for the polynomials of degree 5, which was proved by Abel in the the early 19^{th} century. Thus, polynomials with degrees five are not necessarily always solvable.

Around the same time period as Abel, Evariste Galois proposed a theorem, Galois' correspondence, which connected the roots of a polynomial to the group of automorphisms of its splitting field. Interestingly enough the relationship between both the splitting field and the group of automorphisms has implications to whether a given polynomial's roots can be solved for in terms of radicals or not. In the following sections of the paper the primary focus will be showing the steps to generate a list of solvable irreducible quintic polynomials. The first part of the paper will touch upon the basic theoretic background necessary to understand Galois Theory. The following section will be about certain methodologies used to determine whether a polynomial is solvable. These same methodologies are carried over to the next section, where we discuss two pieces of python code to test if a quintic polynomial is solvable. In the last part we discuss an analysis of the polynomials and other key pieces of information that were generated from the code.

2 Background

2.1 Polynomials and Splitting Fields

For the entirety of this paper, we will restrict our attention to polynomials with integer coefficients that are irreducible in the ring $\mathbb{Q}[x]$ of polynomials with rational coefficients. Thus, we cannot factorize the polynomial into smaller degree polynomials in $\mathbb{Q}[x]$, nor will the polynomial have the same root more than once. Since the field $\mathbb{Q}$ does not contain all the roots of the polynomial (there are polynomials whose roots are real or complex numbers) we must use the splitting field of the polynomial. The splitting field of the polynomial is the smallest possible field that contains all the roots of the polynomial. In order to create the splitting field we must adjoin the roots to $\mathbb{Q}$. For example, consider the irreducible polynomial $x^2 + 1$. We know that the roots of this polynomial are $\sqrt{-1} = i$ and $-i \notin \mathbb{Q}$. By adjoining i to $\mathbb{Q}$, we have a new field $E = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ which contains all the roots of the polynomial.

2.2 Galois group and Automorphisms

We define the Galois group of a polynomial $f(x)$ to be the group of all automorphisms of E, the splitting field of $f(x)$. An automorphism of E, that is, an isomorphism from E to itself, must fix every rational number and permute the roots of $f(x)$ among themselves. If we index the roots as v_i for i in $\{1, 2, ..., n\}$, we can view an automorphism as a permutation of this set, that is, as an element of S_n. While we do not always obtain every element of S_n as an automorphism, as we will see in Example 2, the Galois group of $f(x)$ is always a subgroup of S_n.

2.2.1 Example 1

Consider the polynomial $x^2 - 3$, which has roots $v_1 = \sqrt{3}$ and $v_2 = -\sqrt{3}$. So we have the extension field $E = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. In this case we only have two automorphisms: one being $\theta_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and the other $\theta_2(a + b\sqrt{3}) = a - b\sqrt{3}$. The automorphism θ_1 maps $v_1 \to v_1$, while θ_2 maps $v_1 \to v_2$. Consider $\theta_2(v_2)$. Then,

$$\theta_2(v_2) = \theta_2(-\sqrt{3}) = \theta_2(-1)\theta_2(\sqrt{3}) = (-1)(-\sqrt{3}) = (\sqrt{3}) = v_1.$$

So θ_2 sends $v_2 \to v_1$. Thus we can view θ_2 as a reflection between the two roots and θ_1 as the identity element, not changing the elements of E. The Galois group for this example is the entire symmetric group S_2 where S_2 is $\{(1), (1, 2)\}$.

2.2.2 Example 2

In this case the Galois group of x^4-2 is not the entire symmetric group S_4 but rather a subgroup, isomorphic to the dihedral group D_4 the group of symmetries of the square. The polynomial $f(x) = x^4 - 2$ has the splitting field $\mathbb{Q}(\sqrt[4]{2}, i)$ and has the roots: $v_1 = \sqrt[4]{2}$, $v_2 = -\sqrt[4]{2}$, $v_3 = i\sqrt[4]{2}$, $v_4 = -i\sqrt[4]{2}$. Let α be an automorphism. There are four possibilities in which α maps $\sqrt[4]{2}$ to any roots of $f(x)$. It can be shown in each case, α maps i to i or $-i$. Hence the Galois group of $f(x)$ has 8 elements. We consider the case where $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\alpha(i) = i$. Then,

$$\begin{aligned}
\alpha(v_1) = \alpha(\sqrt[4]{2}) &= i\sqrt[4]{2} = v_3 \\
\alpha(v_3) = \alpha(i\sqrt[4]{2}) = \alpha(i)\alpha(\sqrt[4]{2}) &= i^2\sqrt[4]{2} = -\sqrt[4]{2} = v_2 \\
\alpha(v_2) = \alpha(-\sqrt[4]{2}) = \alpha(-1)\alpha(\sqrt[4]{2}) &= -i\sqrt[4]{2} = v_4 \\
\alpha(v_4) = \alpha(-1)\alpha(i)\alpha(\sqrt[4]{2}) &= -i^2\sqrt[4]{2} = \sqrt[4]{2} = v_1.
\end{aligned}$$

It is worth pointing out that by sending v_1 to v_3 led to α sending v_3 to v_2, v_2 to v_4, and v_4 to v_1. Thus, we can view the automorphism α as the permutation (1324). If we look at the compositions of the permutation (1324) with itself, we can find the rest of the permutations α has to offer; $\{(1324), (12)(34), (1423), (1)\}$. Notice that the permutation (1324) does not produce (1234) or other elements of S_4. In an attempt to produce the permutation (1234), we define the automorphism γ such that $\gamma(\sqrt[4]{2}) = -\sqrt[4]{2}$. We see that

$$\begin{aligned}
\gamma(v_1) = \gamma(\sqrt[4]{2}) &= -\sqrt[4]{2} = v_2 \\
\gamma(v_2) = \gamma(-\sqrt[4]{2}) = \gamma(-1)\gamma(\sqrt[4]{2}) &= (-1)(-\sqrt[4]{2}) = \sqrt[4]{2} = v_1.
\end{aligned}$$

Thus, because of the roots and how γ defined we cannot create an automorphism that sends:

$$\sqrt[4]{2} \to -\sqrt[4]{2}$$
$$-\sqrt[4]{2} \to i\sqrt[4]{2}$$
$$i\sqrt[4]{2} \to -i\sqrt[4]{2}$$
$$-i\sqrt[4]{2} \to \sqrt[4]{2}.$$

Our first automorphism α generates only four of the eight possible permutations. In order to construct the rest of the permutations we define the automorphism β, where $\beta(i) = -i$ and $\beta(\sqrt[4]{2}) = \sqrt[4]{2}$. Applying β to each of the roots we find,

$$\beta(v_1) = \beta(\sqrt[4]{2}) = v_1$$
$$\beta(v_2) = \beta(-1)\beta(\sqrt[4]{2}) = -\sqrt[4]{2} = v_2$$
$$\beta(v_3) = \beta(i)\beta(\sqrt[4]{2}) = -i\sqrt[4]{2} = v_4$$
$$\beta(v_4) = \beta(-1)\beta(i)\beta(\sqrt[4]{2}) = (-1)(-i)\sqrt[4]{2} = i\sqrt[4]{2} = v_3.$$

Hence, we can regard β as the permutation (34). From the multiple compositions of just these two elements ($\alpha = (1324)$ and $\beta = (34)$), we can form a Galois group $D_4 = \{1, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$. From these examples we see that Galois group is dictated by how the automophisms map each of the roots; which is ultimately determined by the roots themselves. The Galois group, as we will see, will play a critical role in determining whether a polynomial is solvable by radicals or not.

2.3 Galois Correspondence

If σ is an automorphism of E, the splitting field of a polynomial $f(x)$, we say that σ fixes an element z in E if $\sigma(z) = z$. When H is a subgroup of the Galois group G, the set of all elements of E that are fixed by every automorphism in H forms a subfield F_H of E, which we call the fixed field of H. The mapping that sends H to F_H is a one-to-one correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and E, called the Galois correspondence.[1] Consider the example of $f(x) = x^4 - 2$ with the previously defined automorphisms of $f(x)$. Let G be the Galois group of $f(x)$ and E the splitting field of $f(x)$. All of the subgroups and corresponding subfields are show below in a subgroup lattice and a field lattice.

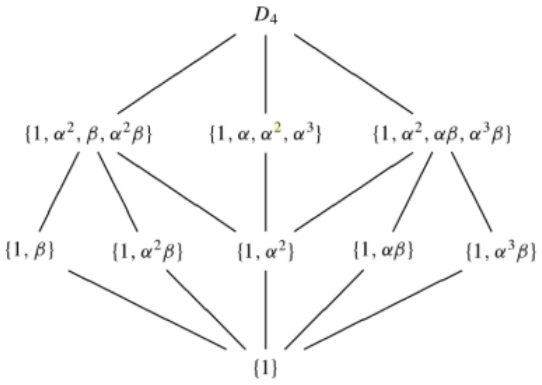


Figure 1: Subgroup Lattice [3]

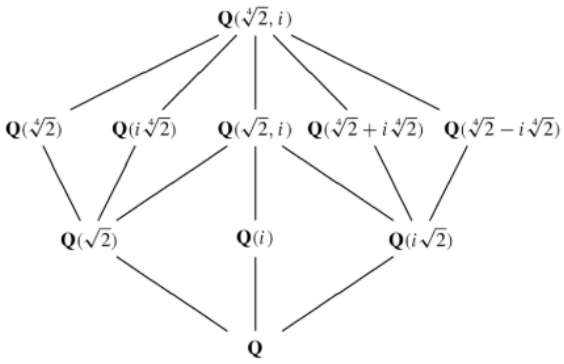


Figure 2: Field Lattice [3]

At the top of each lattice is the entire subgroup or the entire splitting field. Continuing down the lattice we see subgroups and subfields that are found within the entire subgroup or splitting field. Notice that the number of fields in the second and third row of the field lattice flips with the number of subgroups with the second and third row of the subgroup lattice. This is due to the reverse order of inclusion; that is for all subgroups H_1 and $H_2 \in G$ where $H_1 \subseteq H_2$ then $F_{H_2} \subseteq F_{H_1}$. Thus, both lattices leave us with a counter intuitive subgroup and field correspondence. For example, $\{1, \alpha^2, \beta, \alpha^2\beta\}$ corresponds to $\mathbb{Q}(i\sqrt{2})$ and $\{1, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ corresponds to $\mathbb{Q}(\sqrt{2})$. As we will see in the next section, each subgroup of G (which corresponds to an intermediate field) will determine whether a polynomial is solvable by radicals.

2.4 Solvable Groups

A polynomial is solvable by radicals when its Galois group is solvable. A group G said to be solvable if it has a finite series of subgroups

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_{n-1} \subseteq G_n = G$$

such that for every i with $1 \leq i \leq n$, G_{i-1} is normal as a subgroup of G_i with the factor group G_i/G_{i-1} as an abelian group.[1] For example, take the Galois group D_4 from the polynomial $x^4 - 2$. We have,

$$\{1\} \subseteq \{\alpha^2, 1\} \subseteq \{\alpha, \alpha^2, \alpha^3, 1\} \subseteq D_4.$$

Since each subgroup G_{i-1} has exactly half the elements of the larger group G_i, then each subgroup G_{i-1} is normal in G_i. As an example let G_1 be $\{\alpha^2, 1\}$ and let G_2 be $\{\alpha, \alpha^2, \alpha^3, 1\}$. We want to show that $g^{-1}ng \in G_1$ such that $g \in G_2$ and $n \in G_1$. Because α^2 and 1 are their own inverses; we just have to consider α^3 and α in G_2. Then,

$$\alpha^3\alpha^2 * \alpha = \alpha^2$$
$$\alpha^3 * 1 * \alpha = 1.$$

Since 1 and $\alpha^2 \in G_1$, the subgroup $\{1, \alpha^2\}$ is normal in $\{\alpha, \alpha^2, \alpha^3, 1\}$.

Now we want to show that quotient groups: $\{\alpha^2, 1\}/\{1\}$, $\{\alpha, \alpha^2, \alpha^3, 1\}/\{\alpha^2, 1\}$, and $D_4/\{\alpha, \alpha^2, \alpha^3, 1\}$ are abelian. It turns out that the each of the quotient groups has two elements because each quotient subgroup has half the number of elements in the larger group. Thus each quotient group is abelian, since groups of prime order are cyclic. Therefore all the quotient subgroups G_i/G_{i-1} are abelian, every G_{i-1} is normal in G_i, and $\{1\} \subseteq \{\alpha^2, 1\} \subseteq \{\alpha, \alpha^2, \alpha^3, 1\} \subseteq D_4$, then D_4 is solvable.

2.5 Solvable Quintic Polynomials

One of the consequences of a solvable Galois group is that we can solve for the roots of polynomial numerically by radicals. However not every polynomial has a solvable Galois group. In the case of an irreducible degree five polynomial there only three possible solvable Galois groups $\mathbb{Z}_5$, D_5, and F_{20}.[2] Below is a chart that displays all of the possible Galois groups for an irreducible quintic polynomial.

cycle type:	1	2	(2,2)	3	(2,3)	4	5
$\mathbb{Z}_5$	1						4
D_5	1		5				4
F_{20}	1		5			10	4
A_5	1		15	20			24
S_5	1	10	15	20	20	30	24

[2, pg. 557]

The numbers in the chart represent the numbers of elements with that given cyclic type. In S_n all of the permutations can be separated into seven different cyclic types. The identity element (1) has length 1 and is the only element with cyclic type 1. The permutations which reflect between two roots can written permutations as cyclic type 2; e.g.(13). The cyclic types $(2,3)$ and $(2,2)$ are permutations that are separated by two cycles which correspond to the length of the cycle type (e.g. (12)(345), (12)(35)) . Permutations with the cyclic type 3, 4, and 5 (e.g. $(123), (1234), (12345)$) have permutations lengths equivalent to their cyclic type. The Galois group A_5 is the subgroup group of all the even[1] permutations in S_5. As we see the cyclic types of A_5 include $1, (2,2), 3$ and 5. Both S_5 and A_5 are not solvable Galois groups.

In contrast, the Galois group $\mathbb{Z}_5$, D_5 and F_{20} are solvable groups. In $\mathbb{Z}_5$ there is the identity element and four elements with cyclic degree 5. The dihedral group D_5, the symmetries of a pentagon, has five elements which elements have cycle type $(2,2)$, four with cyclic type 5 and the identity element. The Frobenius group F_{20} is a group that has 20 elements which has four elements with cyclic type 5, ten elements with cyclic type 4, five elements with cyclic type 2 and the identity element.[2, pg. 633]

In the following sections we will categorize each of the solvable and possibly solvable polynomials into their potential Galois groups. Thus, we will have an idea of how many solvable polynomials will correspond their potential Galois group.

3 Solvable Python Code

In this section we will discuss two methods, one being the factorization of a polynomial modulo primes to predict its Galois group, and the other to test if the same polynomial is solvable. Then, we will go into detail about our conducted research and our findings.

3.1 Factorization Method

We must start by defining the discriminant in order to apply a theorem to describe the factorization method. Let's reiterate that our polynomial $f(x)$ is separable and has integer coefficients

[1]The parity of a permutation is determined by whether the number of transpositions is even or odd. All elements can be broken down into cycles of length two, also known as transpositions. Take (145), we can rewrite (145) = (14)(45), thus (145) has an even permutation because it can be broken into two transpositions. No permutation can rewritten with a different parity; that is no even permutation can be rewritten as odd permutation or vice a versa.

and let $\alpha_1, \alpha_2, ...\alpha_n$ be generic roots of the polynomial $f(x)$. As a result, the discriminant D defined by

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

[2, pg. 525]

is not zero. In our study, we are unaware of the roots of the polynomials. Therefore in order to determine the discriminant of the polynomial, we used a more complicated formula for the discriminant in terms of the coefficients of the polynomial, which is derived from this definition. Once we find the discriminant of the polynomial, we can apply the following theorem to our polynomial.

Theorem: For any prime p not dividing the discriminant D of $f(x) \in \mathbb{Z}[x]$, the Galois group over $\mathbb{F}_p$ of the reduction $f_p(x) = f(x) (\text{mod } p)$ is a permutation group isomorphic to a subgroup of the Galois group over $\mathbb{Q}$ of $f(x)$.[2, pg. 553]

Since we can reduce our polynomial $f(x)$ into a new form $f_p(x) = f(x) (\text{mod } p)$, we can determine a subgroup of the Galois group of the polynomial for the given prime. For example consider the polynomial, $f(x) = x^5 - 1x^4 - 3x^3 - 3x^2 - 2x - 1$ with discriminant equal to 103^2. Then,

$$x^5 - 1x^4 - 3x^3 - 3x^2 - 2x - 1 \equiv (x^5 + 2x^4 + 0x^3 + 0x^2 + x + 2) \text{ mod}(3)$$
$$x^5 + 2x^4 + x + 2 \equiv (x^2 + x + 2)(x^2 + 2x + 2)(x + 2) \text{ mod}(3)$$

Thus, we have $x^5 - 1x^4 - 3x^3 - 3x^2 - 2x - 1 \equiv (x^2 + x + 2)(x^2 + 2x + 2)(x + 2) \text{ mod}(3)$. Since we have the factorization of $f(x)$ into two quadratic polynomials and one linear polynomial, the subgroup of the Galois group of the modular polynomial over $\mathbb{F}_p$ can be represented as a permutation that has the cycle type $(2, 2)$ (e.g. $(12)(35)$), where a linear factor is implicit. It is important to note that the factorization of the polynomial is only for modulo 3 and the factorization can change depending on the prime p. Consider $f(x)$ modulo 7, in this case $f(x)$ factorizes into the subgroup of the Galois group with cyclic type 5 and $f(x)$ modulo 107 factorizes into all linear factors (1,1,1,1,1) denoted by 1 on the chart. If we continue this pattern for a large number of primes that don't divide the discriminant, 103^2, the only cyclic types we find are $\{5, 1, (2, 2)\}$. Our finding would indicate that the Galois group of $f(x)$ is most likely D_5. However, by just looking at only a couple of examples there is no way in which we can identify the Galois group for $f(x)$ to be D_5. In order to determine a good estimate for the Galois group, many modular prime factorization are applied to a given polynomial to give us an idea of all the possible factorization.

3.1.1 Factorization Code

To find potentially solvable quintic polynomials, we need to find the factorization type of a given polynomial modulo a large number of primes. Fortunately, we were able to apply a theorem from a previous undergraduate research project by Christopher Triola, under the direction of Dr. Lehman.[5, Cor.14] This theorem determines the factorization type of a degree five polynomial $f(x)$ modulo a prime p (that is, the degrees of its irreducible factors in $Z_p[x]$) in terms of powers of a particular element in the quotient ring $\mathbb{Z}_p[x]/ < f(x) >$. We adapted this result into an efficient algorithm to predict the Galois group of the polynomial. If the polynomial produces a factorization type of $3, (2, 3)$ or 2, as noted by the factorization table of degree five polynomial, the Galois group in these cases is either S_5 or A_5 and the polynomial's root cannot be expressed by radicals. In this case the polynomials are disregarded. If the factorization output consists only of a cyclic type are $1, (2, 2), 4$, or 5 the program would deem it to be potentially solvable and store it in a Dataframe

and print it in a text file. For all the polynomials that were potentially solvable the program would print the possible Galois group and print the discriminant of the polynomial. It is worth pointing out, it is possible that at higher primes that the polynomial may have a factor type of 4, $(2,2)$, or even $(3,2)$ so by using this method we do not know what the exact Galois group is. To give an example the polynomial $x^5 + 10x^4 + 8x^3 + 3x^2 + 8x + 1$ takes until the prime p=107 to find a factorization type that shows it is unsolvable.

This code was extremely efficient in determining the factorization types of the polynomials which in turn allowed us to generate a long list of potentially solvable quintic polynomials with its predicted Galois group, and its discriminant.

3.2 Resolvent Method

In the previous section, we noted that the factorization method suggests what the polynomial's Galois groups might be. In [4] Dummit describes a theorem in which it is possible to determine the Galois group of a given quintic polynomial, thus in many cases verifying that the polynomial is solvable. The process of determining if a polynomial is solvable or not is based off creating an associated degree six resolvent polynomial. The resolvent polynomial is tested to determined whether it has a rational root. If the resolvent polynomial has a rational root, then the original polynomial is solvable and it is possible to determine the roots of the original quintic polynomial. Dr. Lehman created python code which generated the resolvent polynomial for each of the quintic polynomial candidates and tested whether each of the polynomials had a rational root. If the resolvent polynomial has a rational root, the quintic polynomial, the rational root, and the resolvent polynomial are printed to a text file along with all the information from the factorization method.

3.3 Quintic Polynomial Case Study 1

In our first case study we tested all of the polynomials that had the form:

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e : a, b, c, d, e \in \{-10, -9, ...9, 10\}$$

where the coefficients of the polynomial were between -10 and 10. In this study we did not prove that these polynomials were in fact solvable. We just applied the factorization python code to generate possible solvable polynomials with their possible Galois groups and their discriminant. In this study there was in total 1358 unique possible solvable polynomials. Of the 1358 polynomials there were 10 of them had the possible Galois group of $\mathbb{Z}_5$, 898 of them had the possible Galois group of D_5, and 476 of them had the possible Galois group of F_{20}.

3.4 Quintic Polynomial Case Study 2

In the next case study we used both the resolvent polynomial method and the factorization method to generate multiple polynomials that are solvable. The first part of the test we used the factorization code to generate potentially solvable polynomials. In our test we decided that the factorization for each polynomial would be for all primes p that did not divide the discriminant and between the interval $2 < p < 500$. All the polynomials that were collected were then passed into the resolvent polynomial code where a text file was created which contained all the polynomials with their discriminant, possible Galois group, resolvent polynomial, and the resolvent root. In our second study we looked at polynomials with the form:

$$f(x) = x^5 + ax^3 + bx^2 + cx + d \text{ where } a, b, c, d \in \{-20, -19...19, 20\} \ .$$

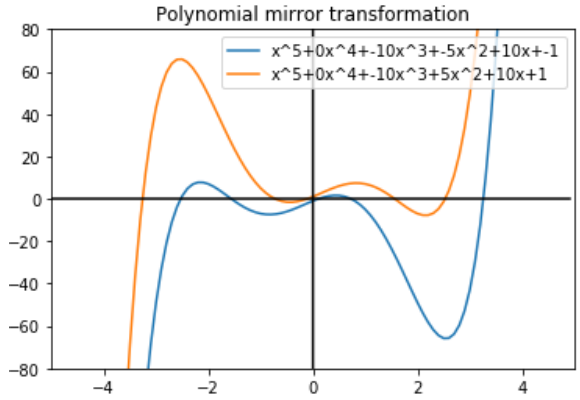
The main reason why we looked at possible solvable quintic polynomials with the form: $f(x) = x^5 + ax^3 + bx^2 + cx + d$ is because when creating the resolvent polynomial, all the polynomials must be transformed into this form. The transformation is possible for every single quintic polynomial. However, we restricted attention to these cases because there were plenty of examples that did not require the transformation necessary to apply Dummit's method.

After running both the factorization python code and the resolvent polynomial code we were able to generate 618 polynomials with the form $f(x) = x^5+ax^3+bx^2+cx+d$ where all the coefficients are integer coefficients between -20 and 20. Categorizing all the polynomials by their Galois group we found that there were 6 polynomials with the Galois group being $\mathbb{Z}_5$, 280 polynomials for F_{20}, and 332 polynomials for D_5.

3.5 Notable Findings from both Studies

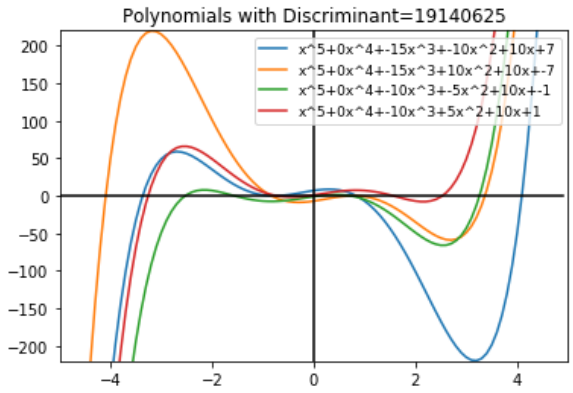
In both case studies, we computed the prime factorization of the discriminant of each (potentially) solvable polynomial. As an example, take the polynomial $f(x) = x^5+10x^4-2x^3+8x^2-x+2$ with the discriminant $13436928 = 2^{11} * 3^8$. One of the things that we verified was that all of the polynomials with the possible Galois group $\mathbb{Z}_5$ or D_5 had square discriminants.[2] Take $f(x) = x^5 + 10x^4 + 10x^3 + 5x^2 + 4x + 4$ with the possible Galois group D_5. The discriminant of the polynomial is equal to $396487744 = 2^6 * 19^2 * 131^2$. Notice that all of the prime powers are squared numbers, $2^3 * 2^3 = 2^6$, $19 * 19 = 19^2$, and $131 * 131 = 131^2$. In the case where the possible Galois group was F_{20} we found that the prime factorization of the discriminant contained at least one prime with an odd exponent, but no prime whose exponent was 1. To demonstrate this point, take the polynomial $f(x) = x^5 + 10x^4 + 0x^3 + -10x^2 + 0x + 2$ with the possible Galois group being F_{20} and the discriminant is $11250000 = 2^4 * 3^2 * 5^7$. We see that $2^2 * 2^2 = 2^4$, $3 * 3 = 17^2$, but 5^7 is not a square and 7 is greater than 1. This is not a property that we were previously aware of, and it could be a matter of further research to determine if it is always true.

Another pattern that was shown in our research was that every single irreducible solvable polynomial had a matching polynomial that had the same discriminant which flips the roots about the y-axis. The difference between the polynomials was a transformation that made the coefficient in front of x^2 term and the constant term negative. One of the many examples of pairs that we found is, $x^5 - 10x^3 + 5x^2 + 10x + 1$ and $x^5 - 10x^3 - 5x^2 + 10x - 1$ which both had the discriminant 19140625. We can see how the mirror each other, once plotted.



Although every single polynomial had a mirror reflection between the x and y axis, there were

other polynomials which had the same discriminant. But in these cases it is not necessarily obvious exactly what the transformations are between each of the polynomials. This is easy to see with all the polynomials with the discriminant being 19140625.



One semi-pattern that I was able make out was that polynomials with the same discriminant seem to have maximas and minimias around the same places along x axis. The graph of the polynomials with the discriminants equaling 19140625 depicts the layering of maximas and minimas between the polynomials fairly well, as seen between the intervals of $-4 < x < -2$ and $2 < x < 4$. In case study one, the most amount of polynomials with the same discriminant (the discriminant being 2209) was 36. In case study two, the most amount of solvable polynomials with the same discriminant (the discriminant being 102515625) was 6 polynomials. The difference in the number of polynomials that have the same discriminant is most likely do to the increase of possible solvable polynomials by including the term x^4 in case study one.

The last finding worth mentioning is that the number of real roots for all the polynomials in both of the case studies is either 5 or 1. Categorizing our findings to the polynomials with a particular Galois group we found that polynomials with the possible Galois group of $\mathbb{Z}_5$ had only polynomials with 5 real roots while polynomials with possible Galois groups either being F_{20} or D_5 had either one real root or five real roots. The majority of the polynomials in both F_{20} and D_5 had one real root. However, there were some cases in which there were five real roots of the polynomials.

I was able to find the number of real roots from all of the polynomials by writing a program to keep track of how many times the sign changes between the output values of the polynomials. The input values of the polynomials for the code was between -25 to 25 in increments of .1. The reason why I choice the interval $-25 \leq x \leq 25$ was to identify all of the roots of the polynomial. I notice that when $x = 25$ and $x = -25$ the x^5 term seem to dominate the function for each of the polynomials. Thus, suggesting that polynomial would be decreasing as x becomes more negative and increasing as x increases. Consequently, there would be no more roots of the polynomial. Consider the example $f(x) = x^5 + 20x^3 + 20x^2 + 20x + 20$. Then $f(-25) = -10066105$ and $(-25)^5 = -9765625$. As we see at -25 (the same case for $x = 25$) the polynomial's value is largely based off of x^5 which would imply that the polynomial does not return the x axis and there is no additional root. Our finding in both case studies would seem to suggest that there would be an underlying reason for why we only found polynomials with the number of real roots being 5 or 1, however it was not common knowledge amongst us before we began the research.

4 Conclusion and Future Work

In this paper we covered the basics of Galois Theory and how it can be applied to finding a quintic solvable polynomial. By simply using a a factorization method and resolvent polynomial method we were able to determine possible candidates for a solvable polynomial and actually construct solvable polynomials. From there, we looked at the pattern amongst the discriminant and the Galois group. Further exploration needs to be done in order to explain two findings. One being that of the polynomials that were generated we only found polynomials which had 1 or 5 real roots. The other finding involves polynomials with the potential Galois group of F_{20}. These polynomials have the pattern of a prime factorization of the discriminant which contained at least one prime with an odd exponent, but no prime whose exponent was 1. It may be that these findings have been established by someone, but it had not been known by us. Therefore further exploration can be done to validate these findings. It is also worth noting that a possible interesting path of research could be exploring the transformations between the polynomials with the same discriminant. However, from what I have seen there does not seem to be an obvious connection between the transformations of polynomials with the same discriminant.

References

[1] Stewart, Ian Nicolas. Galois Theory, Fourth Edition. CRC Press, 2017.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra.* Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[3] Beachy, John A., and William D. Blair. Abstract Algebra. pg. 385 Waveland Press, 2006.

[4] D. S. Dummit, Solving solvable quintics, Mathematics of Computation, Volume 57, Number 195, July 1991, pages 387-401

[5] J. L. Lehman and C. Triola, Recursive sequences and polynomial congruences, Involve, Volume 3, Number 2, 2010, pages 129-148