Galois Theory and the Quintic Equation

By

Yunye Jiang

* * * * * * * * *

Submitted in partial fulfillment

of the requirements for

Honors in the Department of Mathematics Union College

April, 2018

Abstract

Jiang, Yunye

ADVISOR: George Todd

Most students know the quadratic formula for the solution of the general quadratic polynomial in terms of its coefficients. There are also similar formulas for solutions of the general cubic and quartic polynomials. In these three cases, the roots can be expressed in terms of the coefficients using only basic algebra and radicals. We then say that the general quadratic, cubic, and quartic polynomials are solvable by radicals. The question then becomes: Is the general quintic polynomial solvable by radicals? Abel was the first to prove that it is not. In turn, Galois provided a general method of determining when a polynomials roots can be expressed in terms of its coefficients using only basic algebra and radicals. To do so, Galois studied the permutations of the roots of a polynomial. We will use the result that the Galois group of a polynomial is solvable if the polynomial is solvable by radicals to show that the general quintic is not solvable by radicals.

Galois Theory and the Quintic Equation

Yunye Jiang

April 26, 2018

1 Introduction

Most students know the quadratic formula for the solution of general quadratic polynomial $ax^2 + bx + c = 0$ in terms of its coefficients:

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

There are also similar formulas for solutions of general cubic and quartic polynomials. General cubic polynomials in the form $x^3 + ax^2 + bx + c = 0$ can be reduced to the polynomial $y^3 + py + q = 0$. By calculation and applying the quadratic formula, we can reach the Cardano's formula for one of the solutions of a general cubic polynomial:

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \text{ ([Tig01, p.16]).}$$

These formulas are similar in the way that they are all solutions by radicals, that is the solutions for x where $f(x) = 0$ can be written by basic operations of addition, subtraction, multiplication, division and taking the n^{th} roots of the coefficients of the polynomials. Since the solution of the general quadratic, cubic, and quartic polynomials can be written in the described formula, we can say that they are solvable by radicals.

The questions then becomes: Is the general quintic polynomial solvable by radicals? In 1824, Niels-Henrik Abel$(1802-1829)$ was the first to prove that the general quintic polynomial is not solvable by radicals. Abel settled the solvability of general equations, and published his proof in 1826 in Crelle's journal. ([Tig01,

p.210]) Abel came very close to providing a necessary and sufficient condition for solving the problem, while Evariste Galois $(1811 - 1832)$ found a complete solution to this problem. Galois submitted a memoir to the Paris Academy of Sciences in which he described what is now known as the Galois group of a polynomial, and used this to determine whether the roots of a polynomial can be solvable by radicals. ([Tig01, p.232]) Galois' work was originally very hard to understand, but Joseph Liouville $(1809 - 1882)$ explained Galois's work in his own terms which helped the world to understand Galois's project. Galois associates polynomials to a group of permutation of the roots, and Galois Theory connects field theory and group theory by providing a correspondence between subfields of fields and subgroups of permutations. Thus the problem of solvability of the polynomial by radicals can now be solved in terms of the associated group.([Tig01, p.233])

The statement we will show in this thesis is that the general quintic polynomial is not solvable by radicals. We should not take this to mean that every quintic polynomial is not solvable by radicals. For some quintic polynomials, we can find a radical solution. For example, one of the solutions for the polynomial $x^5 - 5 = 0$ is $\sqrt[5]{5}$. The statement means that we cannot provide a single radical formula for every general quintic polynomial as we can for the quadratic polynomials. Therefore, to show the statement is true, it is sufficient for us to find one quintic polynomial with rational coefficients that cannot be solved by radicals, for example, $x^5 - 6x + 3 = 0$ has no radical solution. This is certainly a huge task.

In fact, this is not an amazing phenomena that the general quintics have no radical solutions. We can understand this as a limitation of the operations of addition, subtraction, multiplication, division and taking the n^{th} roots. Given the operation of addition, subtraction, multiplication, division, we can only write solutions for linear equations of one variable. In this case, we don't even have a solution for the general quadratic polynomial. This can be interpreted as a limitation of addition, subtraction, multiplication, division. By introducing the operation of taking the n^{th} root, we can finally write down quadratic formula and solve the general quadratic polynomial. Thus it shouldn't surprise us that taking the n^{th} roots are also limited just as the operations of addition, subtraction, multiplication, division.

But why is general quintic polynomials not solvable by radicals instead of general cubic, quartic or quadratic polynomials? This will be discussed in the following passage. We'll assume that the reader has had some basic abstract algebra course. After studying polynomial rings, we need to learn about field extension to find the roots of the polynomial in discussion, as in many cases the roots of the polynomials are not in the

rational field where the coefficients are in. In the exploration, we will see that what the quadratic formula does is actually extending the field $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{b^2-4ac})$. As the expression $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$ is radical and not necessary in $\mathbb{Q}$,then to find an extension field of $\mathbb{Q}$ that contains x, we can adjoin $\mathbb{Q}$ with $\sqrt{b^2-4ac}$ which is a radical expression and get $\mathbb{Q}(\sqrt{b^2-4ac})$. The radical extension field $\mathbb{Q}(\sqrt{b^2-4ac})$ has the operations of addition, subtraction, multiplication, division . The quadratic polynomial is thus solvable by radicals as there's a radical extension field where its roots are in. Though it is complicated to write out the expression for the solution to the general cubic and quartic polynomials, we know that the roots of general cubic and quartic polynomials can be found in some radical extension field of $\mathbb{Q}$, and are thus solvable by radicals. We can see from the above example that any radical expression is contained in some radical extension field. Then if we can find some radical extension field over a polynomial where all of its roots are in, we can say that the polynomial is solvable by radicals.

In the course of studying, we will show the fact that the Galois group of a polynomial is solvable if the polynomial is solvable by radicals. Generally, the Galois group of a quintic polynomial is not solvable. Using the contrapositive of this statement, we will choose a quintic polynomial and show that its Galois group is not solvable. Thus, we are able to prove that general quintic polynomials are not solvable by radicals.

2 About polynomial

In this section, we'll learn what a polynomial ring is, so that we will be able to study polynomials in the language of group theory. We will learn irreducibility of polynomials over a field, thus we will later be able to understand the constructing of an algebraic extension field, as well as the construction of a splitting field. This section will mainly follow chapter $16, 17$ from [Gal17].

We first give a definition of ring of polynomials over R. The idea is to construct a ring using the coefficient of the set of the polynomials.

Definition 2.1. Let R be a commutative ring, then

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 | a_i \in R\}$$

is called the ring of polynomials over R in the indeterminate x. We say that two elements

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

are equal if and only if $a_i = b_i$ for all $i \in \mathbb{N}$ and $a_0 = b_0$. When $i > n$, we define $a_i = 0$, when $i > m$, $b_i = 0$.

We can see that the equivalence of two elements in a polynomial ring fits our intuition of polynomials that two polynomials are equal if and only if their corresponding coefficients are equal in the commutative ring R. An obvious example of equivalence of two elements in $\mathbb{Z}[x]$ is that $f(x) = x^5 - x^3 + x$ equals to $g(x) = 0x^6 + x^5 - x^3 + x$ where $f(x), g(x) \in \mathbb{Z}[x]$. A lesser obvious example of equivalence of two elements in $\mathbb{Z}_2[x]$ is that $f(x) = g(x)$ where $f(x) = x$ and $g(x) = 3x$, the coefficients $a_1 = 1$ and $b_1 = 3$ are equal since $1 = 3 mod 2$ as $a_1, b_1 \in \mathbb{Z}_2$.

In order to define a ring, it remains for us to define the way of addition and multiplication for $R[x]$, which will be the same way as polynomials are added and multiplied.

Definition 2.2. Let R be a commutative ring, and let $f(x), g(x) \in R[x]$ be arbitrary with

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

We define addition first,

$$f(x) + g(x) = (a_l + b_l) x^l + (a_{l-1} + b_{l-1}) x^{l-1} + \ldots + (a_1 + b_1) x + (a_0 + b_0),$$

where l is the max of m and n, $a_i = 0$ when $i > n$, $b_i = 0$ when $i > m$. We now define multiplication,

$$f(x)g(x) = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \ldots + c_1 x + c_0,$$

where

$$c_i = a_i b_0 + a_{i-1} b_1 + \ldots + a_1 b_{i-1} + a_0 b_i$$

where $i = 0, \ldots, m + n$.

Complicated as these operations might seem, the addition and multiplication on elements of polynomial rings are just the way we normally add and multiply the polynomials while doing algebra.

Let's see an example of addition and multiplication. Let $f(x) = x^2 + 3, g(x) = x^5 - 5x^3 - x^2 \in \mathbb{R}[x]$. Then $f(x) + g(x) = (0+1)x^5 + 0x^4 + (0-5)x^3 + (1-1)x^2 + 3 = x^5 - 5x^3 + 3$

$$f(x)g(x) = (0{\cdot}0+0{\cdot}0+0{\cdot}(-1)+0{\cdot}(-5)+0{\cdot}0+1{\cdot}1++0{\cdot}0+3{\cdot}0)x^7+(0{\cdot}0+0{\cdot}0+0{\cdot}(-1)+0{\cdot}0+1{\cdot}0+0{\cdot}1+3{\cdot}0)x^6+$$

$$(0\cdot 0 + 0\cdot 0 + 0\cdot(-1) + 1\cdot(-5) + 0\cdot 0 + 3\cdot 1)x^5 + (0\cdot 0 + 0\cdot 0 + 1\cdot(-1) + 0\cdot(-5) + 3\cdot 0)x^4+$$

$$(0\cdot 0 + 1\cdot 0 + 0\cdot(-1) + 3\cdot(-5))x^3 + (1\cdot 0 + 0\cdot 0 + 3\cdot(-1))x^2 + (0\cdot 0 + 3\cdot 0)x + (3\cdot 0)$$

$$= x^7 - 2x^5 - x^4 - 15x^3 - 3x^2$$

Theorem 2.3. *$R[x]$ is a ring.*

Proof. We will show this by definition. Let $f(x), g(x), h(x) \in R[x]$ be arbitrary with $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, $h(x) = c_k x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_0$

1. We want to show that $f(x) + g(x) = g(x) + f(x)$. By our definition of addition, we have that $f(x) + g(x) = (a_l + b_l)x^l + (a_{l-1} + b_{l-1})x^{l-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0) = (b_l + a_l)x^l + (b_{l-1} + a_{l-1})x^{l-1} + \ldots + (b_1 + a_1)x + (b_0 + a_0) = g(x) + f(x)$ where l is the max of m and n, $a_i = 0$ when $i > n$, $b_i = 0$ when $i > m$ as R is a commutative ring.

2. We want to show that $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$. By our definition of addition, $(f(x)+g(x))+h(x) = (a_l + b_l)x^l + (a_{l-1} + b_{l-1})x^{l-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0) + c_k x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_0 = (a_p + b_p + c_p)x^l + (a_{p-1} + b_{p-1})x^{p-1} + \ldots + (a_1 + b_1 + c_1)x + (a_0 + b_0 + c_0) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 + (b_q + c_q)x^l + (b_{q-1} + c_{q-1})x^{l-1} + \ldots + (b_1 + c_1)x + (b_0 + c_0) = f(x) + (g(x) + h(x))$ where l is the max of m and n, p is the max of m, n and k,q is the ma of n, k, $a_i = 0$ when $i > n$, $b_i = 0$ when $i > m$, $c_i = 0$ when $i > k$ as R is a commutative ring.

3. Let $j(x) = 0 \in R$, we want to show that $f(x) + j(x) = f(x)$. $f(x) + 0 = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 + 0 = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = f(x)$

4. Let $d(x) = -a_n x^n - a_{n-1}x^{n-1} - \ldots - a_1 x - a_0$, it is obvious that $d(x) \in R[x]$, we want to show that $f(x) + d(x) = j(x) = 0$. $f(x) + d(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 - a_n x^n - a_{n-1}x^{n-1} - \ldots - a_1 x - a_0 = 0x^n + 0x^{n-1} + \ldots + 0x + 0 = 0 = j(x)$ by addition in the ring R.

5. We want to show that $f(x)(g(x)h(x)) = (f(x)g(x))h(x)$. We calculate $f(x)(g(x)h(x) = f(x)(c'_{m+k}x^{m+k} + \ldots + c'_1x + c'_0) = c''_{n+m+k}x^{n+m+k} + \ldots + c''_1x + c''_0$ where $c'_i = b_ic_0 + b_{i-1}c_1 + \ldots + b_0c_i$ where $i = 0, \ldots, m+k$ and $c''_o = a_ic'_0 + \ldots + a_0c'_o$ where $o = 0, \ldots, n+m+k$. Similarly for $(f(x)g(x))h(x)$, thus we have that $f(x)(g(x)h(x)) = (f(x)g(x))h(x)$.

6. We want to show that $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$ and $(g(x) + h(x))f(x) = g(x)f(x) + h(x)f(x)$. We calculate $f(x)(g(x) + h(x)) = f(x)((b_l + c_l)x^l + \ldots + (b_1 + c_1)x + (b_0 + c_0) = a'_{n+l}x^{n+l} + \ldots + a'_1x + a'_0$ where l is the max of m and k and $a' = a_i(b_0 + c_0) + \ldots + a_1(b_{i-1} + c_{i-1}) + a_0(b_0 + c_0)$ where $i = 0, \ldots, n+m+k$. Since $a' = a_i(b_0 + c_0) + \ldots + a_1(b_{i-1} + c_{i-1}) + a_0(b_0 + c_0)$, we split b_i and c_i up and get $a'_{n+l}x^{n+l} + \ldots + a'_1x + a'_0 = f(x)g(x) + f(x)h(x)$. Thus $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$. We now want to show that $(g(x) + h(x))f(x) = g(x)f(x) + h(x)f(x)$, we calculate $(g(x) + h(x))f(x) = f(x)(g(x) + h(x))$ this is shown by 5, we then have that $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x) = g(x)f(x) + h(x)f(x)$ by applying 5 again. Thus we have shown that $(g(x) + h(x))f(x) = g(x)f(x) + h(x)f(x)$, and $R[x]$ is a ring, as desired.

□

In the way we define a polynomial ring, we can see that $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{Z}[x], \mathbb{C}[x]$ are polynomials rings with coefficient of rational numbers, real numbers, integers and complex numbers respectively. In order to study more of the polynomial ring $R[x]$, such as knowing the properties of polynomial rings, our intuition is that whether the properties of the commutative ring R can be carried to the polynomial ring $R[x]$ with respect to the ring R. In fact, some of the properties do. We start with the following theorem.

Theorem 2.4. *If F is integral domain, then $F[x]$ is integral domain.*

Proof. Assume F is an integral domain, we want to show that $F[x]$ is an integral domain. Since we have that $F[x]$ is a ring, we need to show that $F[x]$ is a commutative ring with a unity and no zero-divisors. Since F is commutative, as our coefficients of our polynomials are in F, by our definition of addition and multiplication of $F[x]$, we know that $F[x]$ is commutative as well since the coefficients are also in $F[x]$.
We now show that there's a unity in $F[x]$. Since F is an integral domain, since 1 is a unity in F, we have that $f(x) = 1$ is a unity of $F[x]$.
It remains for us to show that there are no zero-divisors in $F[x]$. Assume $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ and $g(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_0$ where $a_n, b_m \neq 0$. Multiply $f(x)$ with $g(x)$, we get that a_nb_m is the leading coefficient of $f(x)g(x)$, since F is an integral domain and $a_nb_m \in F$, we have that $a_nb_m \neq 0$ since an

integral domain contains no zero-divisors. Since the leading term is not equal to 0, $f(x)g(x) \neq 0$,then there are no zero-divisors in $F[x]$. Thus $F[x]$ is an integral domain as well. □

We now introduce division algorithm on polynomials over a field. This is analogous to the division algorithm of integers that we learnt earlier.

Theorem 2.5. *Suppose F is a field and $f(x), g(x) \in F[x]$ where $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ where $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.*

Just as we normally define a root of polynomial, we say that an element a is a zero(root) of a polynomial $f(x)$ if $f(a) = 0$. Let F be a field with $a \in F$ and $f(x) \in F[x]$. We then say that a is a zero with multiplicity n where $n \geq 1$, if $(x-a)^n$ is a factor of $f(x)$ and $(x-a)^{n+1}$ is not a factor of $f(x)$.

Theorem 2.6. *A non-zero polynomial of degree n over a field has at most n zeros, counting multiplicity.*

Proof. In the case that $n = 0$, since a degree 0 non-zero polynomial has no zeros, it has at most 0 zeros. In the case that $n > 0$, assume that $f(x)$ is a degree n non-zero polynomial over a field and a is a zero of $f(x)$ of k multiplicity. Then we can write $f(x)$ as $(x-a)^k q(x)$ where $q(a) \neq 0$, since $n =$ deg $f(x) = k +$ deg $q(x)$, we have that $k \leq n$ since a degree is greater than or equal to 0. If a is the only zero, we're done. If $\exists b \neq a$ and b is a zero of $f(x)$, then we have that $f(b) = (b-a)^k q(b)$, then we have that b is a zero of $q(x)$ with the same multiplicity for $f(x)$. By induction, we have that $q(x)$ has at most deg $q(x) = n - k$ zeros, thus $f(x)$ has at most $k + n - k = n$ zeros, counting multiplicity. □

We then introduce the definition of irreducible polynomial for the future understanding of extension fields, later we'll state the method of determining whether a polynomial is reducible over the polynomial ring it's in.

Definition 2.7. If F is an integral domain, let $f(x) \in F[x]$, then if $f(x)$ is not a unit over $F[x]$ nor a zero polynomial, we say that $f(x)$ is irreducible over F if $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$, then $g(x)$ or $h(x)$ must be a unit in $F[x]$. If $f(x)$ is not irreducible over F, then it is called reducible over F.

If F is a field, then if $f(x) \in F[x]$ is irreducible over $F[x]$, then we can interpret this as $f(x)$ cannot be written in the form of a product of two other polynomials of lower degrees on variable in $F[x]$. Nevertheless, determining whether a polynomial is irreducible over an integral domain remains to be a hard task, and we want to provide some preliminaries for one to find out whether a polynomial is irreducible over $F[x]$.

Theorem 2.8. *Suppose $f(x) \in \mathbb{Z}[x]$, if $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*

Proof. Let $f(x) \in \mathbb{Z}[x]$, assume $f(x) = g(x)h(x)$ such that $g(x), h(x) \in \mathbb{Q}[x]$. We want to show that exists $m(x), n(x) \in \mathbb{Z}[x]$ such that $f(x) = m(x)n(x)$.

We want to show that exist $c \in \mathbb{Z}$ such that $cf(x) = m(x)n(x)$, and later show that $c = 1$. Let a be the least common multiple of the denominators of all coefficients for $g(x)$ and b be the least common multiple of the denominators of all coefficients for $g(x)$. (For example, if $g(x) = x^6 + \frac{1}{5}x^3 - \frac{1}{3}x^2$, then our a for $g(x)$ is 15.) We choose $m(x) = ag(x)$ and $n(x) = bh(x)$, we have that $m(x), n(x) \in \mathbb{Z}[x]$. By calculation, we know that $abf(x) = (ag(x))(bh(x)) = m(x)n(x)$, thus we have that $c = ab$.

We now show that $c = 1$. We choose c to be the smallest positive number with $c = ab$ by the minimum value theorem and proceed by contradiction, assume $c > 1$, let p be a prime divisor of c, and let $m_p(x), n_p(x) \in \mathbb{Z}_p[x]$ with modulo p operation on coefficients of $m(x), n(x)$. Since $cf(x) = m(x)n(x)$, we do mod p operation on both sides,

$$0 = (cf(x)) \bmod p = m(x)n(x) \bmod p = m_p(x)n_p(x)$$

.

Since $\mathbb{Z}_p[x]$ is an integral domain, we know that either $m_p(x)$ or $n_p(x)$ is 0. WLOG, assume $m_p(x) = 0$. Then we know that all the coefficients of $m(x)$ are divisible by p. Then let $d = c/p$, and $m'(x) = m(x)/p \in \mathbb{Z}[x]$. Since $cf(x) = m(x)n(x)$, we divide both sides by p and get $df(x) = m'(x)n(x)$. Since $d < c$, this is a contradiction by our choice of c to be smallest one. Then we know that $c > 1$ is false. Since $c = ab \in \mathbb{Z}$ and a, b positive, we have that $c = 1$, as desired. Thus, we've shown that $f(x) = m(x)n(x)$ for some $m(x), n(x) \in \mathbb{Z}[x]$. □

With the preliminaries ready, we now introduce a straightforward method to simplify the problem of determining whether a polynomial is irreducible over $\mathbb{Q}$.

Theorem 2.9. *Eisenstein's Criterion: Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. If there's a prime p that $p \nmid a_n, p|a_{n-1}, \ldots, p|a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof. We prove by contradiction. Assume $f(x)$ is reducible over $\mathbb{Q}$, then by theorem 2.8 we have that $f(x)$ is reducible over $\mathbb{Z}$, that is, exist $g(x), h(x)$ in $\mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$ with deg $g(x) \geq 1$, and $n \geq$ deg $g(x) \geq 1$. Let $g(x) = b_r x^r + \ldots + b_0$ and $h(x) = c_s x^s + \ldots + c_0$, since by our settings, $p|a_0$, $p^2 \nmid a_0$, and $a_0 = b_0 c_0$, then we have that $p|b_0$ or $p|c_0$. If $p|b_0$, since $p \nmid a_n = b_r c_s$, we have that $p \nmid b_r$. Then we have that there exist a least integer t such that $p \nmid b_t$. Then there's $a_t = b_t c_0 + b_{t-1}c_1 + \ldots + b_0 c_t$, since $p|a_t$, by our choice of t, we have that $p|b_t c_0$. But since p is prime and $p \nmid b_t$ and $p \nmid c_0$, thus leads to a contradiction. □

3 Field extension and splitting field

In this section, we will discuss definition and properties of field extension and splitting fields. The discussion will enable us to have some necessary knowledge required to talk about Galois Theory later, which will help us with our latter goal of showing quintic polynomials are not solvable by radicals. The progression of this section follows from chapter $20, 21$ in [Gal17].

We first define what is an extension field. Let F be a field.

Definition 3.1. A field E is an extension field of field F if $F \subseteq E$ and F has the same operation as E.

Then we know that a field E is a field extension of F if F is a subfield of E. We denote that E is a extension field over F as E/F. This notation is not equivalent to the notation we used for quotient groups and rings.

Theorem 3.2. *Let F be a field and $f(x)$ be a non-constant polynomial in $F[x]$, then there's an extension field of F where $f(x)$ has a zero.*

Proof. Since $F[x]$ is a unique factorization domain, we know that $f(x)$ has an irreducible factor, $g(x)$. We want to show that there's an extension field of F where $f(x)$ has a zero, this is equivalent to showing that there's an extension field E of F where $g(x)$ has a zero. Let $E = F[x]/\langle g(x)\rangle$, since $\langle g(x)\rangle$ is prime and maximal ideal in $F[x]$, we know that E is a field, we want to show $g(x)$ has a zero in E.
Note that we still have a problem here that since F is not necessary a subset of E. But we can find a subfield of E that is isomorphic to F via composing an isomorphism. Let $\phi : F \to E$ with $\phi(a) = a + \langle g(x)\rangle$, we show that this is homomorphism and injective as we know that F exists, and we only want to find a subfield inside E that is isomorphic to F.
Let $a, b \in F$ be arbitrary, we want to show that $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.

$$\phi(a + b) = (a + b) + \langle g(x)\rangle$$

$$= a + \langle g(x)\rangle + b + \langle g(x)\rangle$$

$$= \phi(a)\phi(b)$$

We now calculate $\phi(ab) = ab + \langle g(x)\rangle$

$$= (a + \langle g(x)\rangle)(b + \langle g(x)\rangle)$$

$$= \phi(a) + \phi(b)$$

We show it is injective, assume $\phi(a) = \phi(b)$, we want to show that $a = b$. Since $a + \langle g(x)\rangle = b + \langle g(x)\rangle$ by assumption, we have that $a = b$. This shows that there's a subfield of E that is isomorphic to F. We can think of F is contained in E, that is we can just think of $a+ < g(x) >$ as same as a.
Let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$. We claim that $x + \langle g(x)\rangle$ is a zero in E, we calculate,

$$g(x + \langle g(x)\rangle) = a_n(x + \langle g(x)\rangle)^n + a_{n-1}(x + \langle g(x)\rangle)^{n-1} + \ldots + a_0$$

$$= a_n(x^n + \langle g(x)\rangle) + a_{n-1}(x^{n-1} + \langle g(x)\rangle) + \ldots + a_0$$

$$= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 + \langle g(x)\rangle$$

$$= g(x) + \langle g(x)\rangle$$

$$= 0 + \langle g(x)\rangle$$

Thus we've shown that $x + \langle g(x)\rangle$ is a zero of $g(x)$ in E, then there's an extension field of F where $f(x)$ has a zero, as desired. □

Let's see an example of the how this theorem works.

Example 3.3. Consider the polynomial $f(x) = x^3 - 2x^2 + x - 2$ over $\mathbb{Q}$.
Since $x^3 - 2x^2 + x - 2 = (x^2 + 1)(x - 2)$, we can see that the roots of the polynomial in $\mathbb{C}$ are $\pm i$ and 2. Since we know the roots, we can write down a splitting field for $f(x)$, $\mathbb{Q}(i)$ as 2 is in $\mathbb{Q}$.

We now want to turn to the algebraic structure of field extension.

Definition 3.4. Suppose E is an extension field of F and $a \in E$. Then a is algebraic over F if a is the zero of some nonzero polynomial in $F[x]$. If a is not algebraic over F, then it is transcendental over F. An extension E of F is called an algebraic extension of F if every element of E is algebraic over F, else it is a transcendental extension of F.

We continue with the following theorem to show that we make the distinction of elements that are algebraic and transcendental over a field. $F(x)$ is the field of quotients of $F[x]$, where

$$F(x) = \{f(x)/g(x) | f(x), g(x) \in F[x], g(x) \neq 0\}.$$

Theorem 3.5. *Let E be an extension field of F and $a \in E$. If a is transcendental over F, then $F(a) \approx F(x)$. If a is algebraic over F, then $F(a) \approx F[x]/\langle f(x)\rangle$ where $f(x) \in F[x]$ such that $f(a) = 0$, and $f(x)$ is irreducible over F.*

Proof. Let homomorphism $\phi : F[x] \to F[a]$ be $f(x) \to f(a)$. If a is transcendental over F, then $Ker\phi = \{0\}$, then we can write a isomorphism $\alpha : F(x) \to F(x)$ with $\alpha(f(x)/g(x) = f(a)/g(a)$.
If a is algebraic, then $Ker\phi \neq \{0\}$,then exists a polynomial $p(x)$ in $F[x]$ such that $Ker\phi = \langle p(x)\rangle$ where $p(x)$ is the minimum degree polynomial in $Ker\phi$. Then $p(a) = 0$, $p(x)$ is irreducible, as desired. □

We also know that an element a is algebraic over F if a is the zero of some polynomial $f(x) \in F[x]$.

Definition 3.6. If a is algebraic over F, then the minimal polynomial of a is the monic polynomial of minimal degree that has a as a root.

We then introduce the degree of an extension field.

Definition 3.7. Let E be an extension field of F. Then we note that E has degree n over F and write $[E : F] = n$ if E has dimension n as a vector space over F. If $[E : F]$ is finite, E is a finite extension, otherwise, E is an infinite extension.

Theorem 3.8. *If E is a finite extension of F, then E is algebraic.*

Proof. Assume that $[E : F] = n$ and $a \in E$, we have that $\{1, a, \ldots, a^n\}$ is linearly dependent over F, then we have that there are $c_0, c_1, \ldots, c_n$ in F, such that $c_n a^n + c_{n-1}a^{n-1} + \ldots + c_1 a + c_0 = 0$. Thus it is obvious to see that a is the root of the polynomial $f(x) = c_n x^2 + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$. □

The following theorem serves the function of Lagrange's Theorem for finite groups for field theory. Lagrange's Therorem states that for a group G, if H is a subgroup of G, and K is a subgroup of H, we know that $(G : K) = (G : H)(H : K)$, where $(G : K)$ is the index for the subgroup K of G (the number of the set of left cosets of K in G). We will know that the degree of the extension is able to tower up.

Theorem 3.9. *If K is a finite extension field of E and E is a finite extension of F. Then K is a finite extension field of F and $[K : F] = [K : E][E : F]$.*

Proof. Assume the settings, we want to show that the basis stacks. Assume the set $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_i\}$ form a basis for K over E and $\beta = \{\beta_1, \beta 2, \ldots, \beta_j\}$ form a basis for E over F. We want to show that the products $\alpha\beta = \{\alpha_m\beta_n | 1 \leq m \leq i, 1 \leq n \leq j\}$ form a basis for K over F. If $\gamma \in K$, then we have that γ is a linear combination of the α_is with coefficients $a_i \in E$ and the α_is are linear combinations of the β_j with

$b_{ij} \in F$. Then we know that $\alpha_i\beta_j$ span K over F. If $\sum_{i,j} \gamma_{ij}\alpha_i\beta_j = 0$, then $\sum_i \gamma_{ij}\alpha_i = 0$ for j, then we have that $\gamma_{ij} = 0$ for i, j and $\alpha_i\beta_j$ are linearly independent. Then we have that if $[E : F] = |\beta| = j$ and $[K : E] = |\alpha| = i$, then we have that $[K : F] = |\alpha||\beta| = ij$, as desired. □

We should then see some examples on degrees of field extensions.

Example 3.10. 1.

$$\begin{array}{c} F \\ \Big| 1 \\ F \end{array}$$

Given any field F, we know that F is a finite extension over itself, with degree $[F : F] = 1$.

2.

$$\begin{array}{c} \mathbb{Q}(\sqrt{5}) \\ \Big| 2 \\ \mathbb{Q} \end{array}$$

Since $\{1, \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$, we know that the degree of the extension is 2.

3.

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{5}) \\ \Big| 4 \\ \mathbb{Q} \end{array}$$

We know that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\sqrt{5}$, and $\{1, \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$. Thus $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$.

4.

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}) \\ \Big| 3 \\ \mathbb{Q} \end{array}$$

As shown by the previous examples, $\sqrt[3]{2}$ is a root for $f(x) = x^3 - 2$, and is irreducible over $\mathbb{Q}$, we know that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Theorem 3.2 and the above example show us that one can adjoin any root of a polynomial of $f(x)$ to the extension field. In fact, if $a_1, a_2, \ldots, a_n$ are algebraic over F, we can adjoin a_i to obtain the field in the following way and get the finite extension $E = F(a_1, \ldots, a_n)$. We first adjoin a_1 to F, we will get $F(a_1)$ and then adjoin a_2 to $F(a_1)$ and get $F(a_1)(a_2) = F(a_1, a_2)$, repeating the same process, we can get

$F(a_1, a_2, \ldots, a_n)$ in the end. This is an extension field consisting of all polynomials over F with the a_is as the root.

We now can see that the quadratic formula for the general quadratic polynomial $f(x) = ax^2 + bx + c$ where $f(x) \in \mathbb{Q}[x]$ is essentially showing that in which extension field are the roots of the quadratic polynomial $f(x)$ contain. Recall the quadratic formula:

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

since $\sqrt{b^2 - 4ac}$ is not necessary contained in $\mathbb{Q}$, we now know that we can adjoin $\sqrt{b^2 - 4ac}$ to $\mathbb{Q}$ and find the root there, that is, we have the extension field $\mathbb{Q}(\sqrt{b^2 - 4ac})$ over $\mathbb{Q}$ where the roots of $f(x)$ is in. This example can also be considered in the later context of solvable by radicals. We will know by then that the quadratic formula for general quadratic formula is in fact an example of solvable by radicals, that is, there is an expression of the root of the polynomial in terms of the coefficients with basic algebraic operations and taking nth roots. In other words, we can find an extension field in which contains the roots of the polynomial over the base field in which contains the coefficients of the polynomial.

As the degree of the extension is able to tower up, we consider that whether the algebraic properties can tower up.

Theorem 3.11. *If K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.*

Proof. Let $a \in K$, we need to show that a is in some finite extension of F. Since a is algebraic over E, we have that a is the root of some irreducible polynomial $p(x)$ in $E[x]$, let a_i be coefficients of f. Since $a_i \in E$, so a_is are algebraic over F, then we can write a finite extension field of F that $L = F(a_0, a_1, \ldots, a_i)$, and (x) is also a polynomial in $L[x]$ and $p(a) = 0$ so a is algebraic over L. We have that $L(a)$ is a finite extension of L. Then we have that $[L(a) : F] = [L(a) : L][L : F]$, then $L(a)$ is a finite extension of F. thus we have that$a$ is algebraic over F as L, since a is arbitrary in K, we have that K is an algebraic extension of F, as desired. □

Corollary 3.12. *Let E be an extension field of field F. The set of all elements of E that are algebraic over E is a subfield of E.*

Proof. Suppose that $a, b \in E$ are algebraic over F and $b \neq 0$,we want to show that $a+b$,$a-b$,ab, and a/b are algebraic over F, it is sufficient to show that $[F(a,b) : F]$ is finite. Since $[F(a,b) : F] = [F(a,b) : F(b)][F(b) : F]$, and a is algebraic over F, then a is algebraic over $F(b)$. Thus, $[F(a,b) : F(b)]$ and $[F(b) : F]$ are finite, then $[F(a,b) : F]$ is finite, as desired. □

By theorem 3.11, we're able to see the following example,

Example 3.13. Let f be an irreducible polynomial over $\mathbb{Q}$, we have that $\mathbb{C}$ contains the splitting field of f.

We are interested in the field extensions that are created by adjoining algebraic elements to a base field. Let F be a field and a be algebraic over F, then we know that $F(a)$ is an algebraic over F. Moreover, $F(a)$ is the smallest field containing F and a. We can adjoin any finite number of algebraic elements over F to F to get an algebraic extension.

We should see an example of polynomial ring that will motive us to provide the definition of splitting field.

Example 3.14. Let $R = \mathbb{R}[x]$ be the set of all polynomials with real coefficients, e.g. $x+1$, $x^5+x^4-2x^2-8$. Let $A = \langle x^2+1\rangle$ where the elements look like $\langle x^2+1\rangle = \{f(x)(x^2+1) | f(x) \in \mathbb{R}[x]\}$. Since A is a maximal ideal, we have that $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field. Since $f(x)+\langle x^2+1\rangle = g(x)+\langle x^2+1\rangle$ iff $f(x)-g(x) \in \langle x^2+1\rangle$, particularly, if $f(x) = x^2$ and $g(x) = -1$, then we know that $x^2 + \langle x^2+1\rangle = (-1) + \langle x^2+1\rangle$, since $x^2-(-1) = x^2+1 \in \langle x^2+1\rangle$.
The idea here for us is that one can think of x^2 as -1 in $\mathbb{R}[x]/\langle x^2+1\rangle$. Also, considering the zero for $f(x) = x^2+1$, we can see there is no zero for $f(x)$ in $\mathbb{R}$, but as we have that the zero can be found in $\mathbb{R}[x]/\langle x^2+1\rangle$, thus $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$.

By example 3.14, we know that $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field that has a zero of x^2+1, this will motivate us to have the intuition of the following fact.

Definition 3.15. If E is an extension field of F and $f(x) \in F[x]$ which degree is at least 1. Then $f(x)$ splits in E if there exists $a \in F$ and $a_1, a_2, \ldots, a_n \in E$ such that $f(x) = a(x-a_1)(x-a_2)\ldots(x-a_n)$. E is a splitting field for $f(x)$ over F is $E = F(a_1, a_2, \ldots, a_n)$.

A splitting field depends on both polynomial and the field that the polynomial is over. If we have that $f(x) \in F[x]$ and $f(x)$ splits over E, then we can pick any root a of $f(x)$ and adjoin it to F and get the extension $F(a)$. Thus we can see that a splitting field E of $f(x)$ over F is a smallest extension field

of F where $f(x)$ splits, in the sense that E is a subfield of every field containing F and all the roots of $f(x)$. We then show there the existence of a splitting field for a non-constant polynomial. With the previous knowledge, we know that $F(a_1, a_2, \ldots, a_n)$ is actually an algebraic extension over F if the a_is are algebraic over F.

We want to then show the existence of a splitting field for every $f(x) \in F[x]$.

Theorem 3.16. *Suppose F is a field and $f(x)$ is a non-constant polynomial in $F[x]$, then exists a splitting field for $f(x)$ over F.*

Proof. We prove by induction on degree of $f(x)$. We first show the base step, if deg $f(x) = 1$, then $f(x)$ obviously splits as $f(x)$ is linear. We then show the inductive step, we first assume that there exists a splitting field for all polynomials of degree less than $f(x)$'s over F, then by theorem 3.2, we know that there's an extension E of F where $f(x)$ has a zero, we name such zero a_1, then we can write $f(x)$ as $(x - a_1)g(x)$, where $g(x) \in E[x]$. Since deg $g(x)$ <deg $f(x)$, by our assumption in induction step, we have that there's a field contains E and all the zeros of $g(x)$, $a_2, \ldots, a_n$. Thus a splitting field for $f(x)$ over F can be $F(a_1, a_2, \ldots, a_n)$. □

We will use the next theorem to show that $F(a) \cong F[x]/\langle p(x)\rangle$ if $p(x)$ is irreducible over F and a is a zero of $p(x)$ in some extension of F.

Theorem 3.17. *Suppose F is a field and $p(x) \in F[x]$ is irreducible over F, if a is a zero of $p(x)$ in some extension E of F, then $F(a) \cong F[x]/\langle f(x)\rangle$. If deg $p(x) = n$ (a is algebraic over F),then element of $F(a)$ is uniquely in the form $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \ldots + c_1a + c_0$, where $c_i \in F$.*

Proof. We show that $\phi : F[x]/\langle f(x)\rangle \to F(a)$where $\phi(f(x)) = f(a)$ is an isomorphism. We first show ϕ is a homomorphism.
We want to show that $\phi(f(x)) + \phi(g(x)) = \phi(f(x) + g(x))$ and $\phi(f(x)) \cdot \phi(g(x)) = \phi(f(x) \cdot g(x))$ for $f(x), g(x) \in F[x]$. Let $h(x) = f(x) + g(x)$, $k(x) = f(x) \cdot g(x)$. We calculate,

$$\phi(f(x)) + \phi(g(x)) = f(a) + g(a) = h(a) = \phi(h(x)) = \phi(f(x) + g(x))$$

We then show,

$$\phi(f(x)) \cdot \phi(g(x)) = f(a) \cdot g(a) = k(a) = \phi(k(x)) = \phi(f(x) \cdot g(x)).$$

We first show that $ker(\phi) = \langle p(x)\rangle$. Since we know that $p(a) = 0$ and $p(x) \in F[x]$, thus $\langle p(x)\rangle \subseteq ker(\phi)$,

we have that $ker(\phi) \neq 0$. As $ker(\phi) \neq F[x]$ since it does not contain constant polynomials, we have that $ker(\phi) = \langle p(x) \rangle$. As we know this fact, then we have that $F[x]/\langle p(x) \rangle \cong F[a]$ by first isomorphism theorem. Since $F[x]$ is a principle domain, we have that $F[a]$ is a domain. Then $ker(\phi)$ is a prime ideal, thus a maximal ideal, and that $F[a]$ is a field.Since $F(a)$ is the smallest field containing $F[a]$, then $F(a) = F[a] \cong F[x]/\langle p(x) \rangle$, we rewrite that,$F(a) \cong F[x]/\langle f(x) \rangle$, as desired.

□

Corollary 3.18. *If a is a zero of $p(x)$ in some extension E of F and b a zero of $p(x)$ in some extension G of F, then $F(a) \cong F(b)$.*

Proof. Since $p(x) \in F[x]$ be irreducible, and a is a zero of $p(x)$ in some extension E of F, we know by theorem 3.17, $F(a) \cong F[x]/\langle p(x) \rangle$. Similarly, we know that $F(b) \cong F[x]/\langle p(x) \rangle$. Thus, we have that $F(a) \cong F[x]/\langle p(x) \rangle \cong F(b)$, as desired. □

Now that we have shown the existence of splitting fields for every $f(x) \in F[x]$, we now want to know if there's more than one non-isomorphic splitting field, that is the uniqueness of splitting fields. We will utilize the following theorem to show that the splitting fields of a polynomial are in fact unique with respect to isomorphism.

Lemma 3.19. *Let F, G be field, and $g(x) \in F[x]$ be irreducible over F, and let a be a zero of $g(x)$ in some extension of F. Then if ϕ is a field isomorphism from F to G and b is a zero of $\phi(g(x))$ in some extension of G, then there is an isomorphism from $F(a)$ to $G(b)$ that takes a to b.*

Proof. Since $g(x)$ irreducible over F, we have that $\phi(g(x))$ is irreducible over G.Then the mapping from $F[x]/\langle g(x) \rangle$ to $G[x]/\langle \phi(g(x)) \rangle$ is $f(x) + \langle g(x) \rangle \to \phi(f(x)) + \langle \phi(g(x)) \rangle$ is field isomorphism.By theorem 3.17, we have that there exist an isomorphism α from $F(a)$ to $F[x]/\langle g(x) \rangle$, this carries a to $x + \langle g(x) \rangle$. Similarly, exists an isomorphism ω from $G[x]/\langle \phi(g(x)) \rangle$ to $G(b)$ carries $x + \langle \phi(g(x)) \rangle$ to b, thus $\omega\phi\alpha$ is the desired mapping. □

Theorem 3.20. *Let F, F' be field and $f(X) \in F[x]$ and ϕ be an isomorphism from F to F'. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F', then there's an isomorphism from E to E' that agrees with ϕ on F.*

Proof. We prove by induction on the degree of $f(x)$.
Base case: deg $f(x) = 1$, we have that $E = F$, $E' = F'$, then we have that ϕ is the isomorphism we want.
Induction case: deg $f(x) > 1$, let $g(x)$ be an irreducible factor of $f(x)$, let a be a zero of $g(x)$ in E, b be a

zero of $\phi(g(x))$ in E'. We know that there exists isomorphism $\tau : F(a) \to F'(b)$ that agrees with ϕ on F and carries a to b by lemma 3.19. Let $f(x) = (x-a)g(x)$. Then we know that E is a splitting field for $g(x)$ over $F(a)$ and E' splits for $\tau(g(x))$ over $F'(b)$. As deg $g(x) <$ deg $f(x)$, we have that there exists an isomorphism from E to E' that agrees with τ on $F(a)$, thus agrees with ϕ on F, as desired. □

Corollary 3.21. *If F is a field and $f(x) \in F[x]$, then splitting fields of $f(x)$ over F are isomorphic.*

Proof. Let E and E' be two arbitrary splitting fields of $f(x)$ over F. We choose ϕ be the identity isomorphism from F to F, then by theorem 3.20, we have that there's an isomorphism from E to E',thus that $E \cong E'$. □

Knowing the fact that the splitting fields of $f(x)$ over F are isomorphic enables us to say that roots of the irreducible $f(x)$ gives us the same extension of F. We now construct some splitting fields.

Example 3.22. We can adjoin the positive cube roots of 3 to $\mathbb{Q}$ and get $E = \mathbb{Q}(\sqrt[3]{3})$. We know that the roots of the irreducible polynomial $f(x) = x^3 - 3$ are $\sqrt[3]{3}$, $\omega\sqrt[3]{3}$ and $\omega^2\sqrt[3]{3}$, where omega is the primitive roots of unity. We can see that though $f(x)$ has a root in E, but $f(x)$ doesn't splits in E. Since there are two complex roots while $\mathbb{Q}(\sqrt[3]{3})$ are entirely made up of real numbers.

More generally,

Example 3.23. The splitting field of $x^n - a$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[n]{a}, \omega)$. Let a be positive real number and ω be nth root of unity, then $a^{\frac{1}{n}}, \omega a^{\frac{1}{n}}, \omega^2 a^{\frac{1}{n}}, \ldots, \omega^{n-1} a^{\frac{1}{n}}$ are zeros of $x^n - a$ in $\mathbb{Q}(\sqrt[n]{a}, \omega)$.

We then show that if an irreducible polynomial has multiple zeros, the zeros will have the same multiplicities.

Theorem 3.24. *Let $f(x)$ be irreducible over a field F, and E is a splitting field of $f(x)$ over F. Then all the zeros of $f(x)$ in E have the same multiplicity.*

Proof. Let a,b be different roots of $f(x)$ in E. Let a have multiplicity m, then $f(x) = (x-a)^m g(x)$ in $E[x]$. We also have that there exist an isomorphism ϕ from E to E that carries a to b, then we have that $f(x) = \phi(f(x)) = (x-b)^m \phi(g(x))$, thus the multiplicity of b is greater than or equal to m. Similarly, repeat the process by switching a and b, we have that the multiplicity of a is greater than or equal to that of b. Thus a,b have the same multiplicity. □

Thus we can write the following corollary.

Corollary 3.25. *Let $f(x)$ be an irreducible polynomial over field F and E a splitting field of $f(x)$ over E. Then $f(x)$ can be written as $a(x-a_1)^m(x-a_2)^m\dots(x-a_n)^m$, where $a_1, a_2, \dots a_n$ are distinct in E and $a \in F$.*

4 Galois Theory

Now we move on to the Galois theory to solve the question if a polynomial can be solved by radicals . Galois linked any polynomial $p \in \mathbb{C}[x]$ with a group of permutation, these groups are also known as Galois groups. We wish to use Galois theory to study the solutions of polynomial equations, whether they can be expressed by a radical formula. A radical expression consists of the coefficients of the polynomial with operations of addition, multiplication, subtraction, division, as well as taking n^{th} root. This section mainly builds on chapter 32 of [Gal17, p. 535], and the proof of the Fundamental Theorem of Galois theory partially follows chapter 8 and 12 from [Ste04]. The aim of learning this is to study the solutions of polynomial equations, and to know whether a polynomial can be solved by a formula with radicals or not. We will begin with the definition of the Galois Group of E over F.

Definition 4.1. Let E be an extension field of F. The automorphism of E is a ring isomorphism from E to itself. The Galois group of E over F, denoted: $Gal(E/F)$, is the set of all automorphisms of E taking every element of F to itself, that is the set $\{\phi \in Aut(E)\}$. If H is a subgroup of $Gal(E/F)$, the set $E_H = \{x \in E | \phi(x) = x \forall \phi \in H\}$ is the fixed field of H.

Before moving on, let's see an example of how the definition works.

Example 4.2. Let $E = \mathbb{Q}(\sqrt[n]{a})$ where $a \in \mathbb{Z}$. Since a ring isomorphism must map the unity to unity, and we know that field automorphisms are ring isomorphisms, then we have that $\mathbb{Q}$ will be fixed by all $\phi \in Aut(E)$. Thus we know that $Aut(E) = Gal(E/\mathbb{Q})$, and $\mathbb{Q} \subseteq E_H$. Since E is generated as a ring by 1, $\sqrt[n]{a}$, we know that $\phi \in Aut(E)$ is completely determined by $\phi(\sqrt[n]{a})$. We know that what this automorphism is going to do to 1, what we care about is what this automorphism does to $\sqrt[n]{a}$, i.e. where does the automorphism send $\sqrt[n]{a}$ to.

To show the Fundamental Theorem of Galois Theory, we need some preliminaries...

Lemma 4.3. *Let E be an extension field of F, and K be the fixed field of $Gal(E/F)$, then $Gal(E/F) = Gal(E/K)$.*

Proof. We show mutual containment. Let $p \in F$, then for all $\phi \in Gal(E/F)$, $\phi(p) = p$. Since K is the fixed field of $Gal(E/F)$ and $p \in K$, we have that $F \subseteq K$. Then $Gal(E/K) \leq Gal(E/F)$.
Let ϕ in $Gal(E/F)$. Then we have that $\phi(p) = p$ for all $p \in K$. Then $\phi \in Gal(E/K)$, and $Gal(E/F) \leq Gal(E/K)$, as desired. □

Lemma 4.4. *Let E be a normal extension of field F, and K be an intermediate extension of E/F. For $\phi \in Gal(E/F)$, $Gal(E/\phi(K)) = \phi Gal(E/K)\phi^{-1}$.*

Proof. Let $\phi(K) = G$, and $\tau \in Gal(E/K)$ be arbitrary, and $g \in G$. We have that $g = \phi(k)$ for some $k \in K$. Then we have that

$$\phi\tau\phi^{-1}(g) = \phi\tau(k) = \phi(k) = g.$$

Then we have that $\phi Gal(E/K)\phi^{-1} \subseteq Gal(E/G)$. Let $\omega \in Gal(E/G)$ be arbitrary, similarly, $\omega \in \phi Gal(E/K)\phi^{-1}$, thus

$$Gal(E/\phi(K)) = \phi Gal(E/K)\phi^{-1},$$

as desired. □

Theorem 4.5. *[Gal17, p. 535] Fundamental Theorem of Galois Theory(The theorem is the version of : Let F be a field with characteristic 0, if E splits over F for some polynomial in $F[x]$, then the mapping from the set of subfields of E containing F to the set of subgroups of $Gal(E/F)$ from $K \to Gal(E/K)$ is one to one. For subfield K of E containing F,*

1. *$[E : K] = |Gal(E/K)|$ and $[K : F] = |Gal(E/F)|/|Gal(E/K)|$.*
2. *If K splits in $F[x]$, we have that $Gal(E/K)$ is a normal subgroup of $Gal(E/F)$ and $Gal(K/F)$ is isomorphic to $Gal(E/F)/Gal(E/K)$*
3. *The fixed field of $Gal(E/K)$ is K.*
4. *Let H be a subgroup of $Gal(E/F)$, we have that $H = Gal(E/E_H)$*

Proof. 1. Assume E splits over F for some polynomial in $F[x]$, and let $K \subseteq E$ be arbitrary with containing F, $H \leq Gal(E/F)$, we want to show that there is a bijection under the operation $K \to Gal(E/K)$.
We first show $K \to Gal(E/K)$ is injective. Let $K_1, K_2 \subseteq E$ be arbitrary with containing F, and assume $Gal(E/K_1) = Gal(E/K_2)$, we want to show that $K_1 = K_2$. Since K_1, K_2 contains F, we can write that $K_1 = E_{H_1}, K_2 = E_{H_2}$ where $H_1, H_2 \leq Gal(E/F)$. Since $H_1 = Gal(E/E_{H_1})$ and

$H_2 = Gal(E/E_{H_2})$, and $Gal(E/K_1) = Gal(E/K_2)$ by assumption, we have that $H_1 = H_2$, then we have that $K_1 = E_{H_1} = E_{H_2} = K_2$, as desired.

Now we show that $K \to Gal(E/K)$ is surjective. Assume $H \leq Gal(E/F)$ be arbitrary, we want to show that there exists $K \subset E$ containing F such that $Gal(E/K) = H$. We choose $K = E_H$, then we have that $H = Aut(E/K)$. Since E/F is Galois, and K is an intermediate field where $F \subset K \subset E$, we have that E/K is Galois as well, thus $Gal(E/K) = H$, as desired.

2. Since $K = E_{Gal(E/K)}$ is a fixed field of $Gal(E/K)$ and $|Gal(E/F)| = [E : F]$, we have that $[E : K] = |Gal(E/K)|$ and $[E : F] = |Gal(F/E)|$, with theorem 3.9 we know that $|Gal(E/F)|/|Gal(E/K)| = [E : F]/[E : K] = [K : F]$,as desired.

3. Assume K is a splitting field of some $f(x) \in F[x]$ over F, then we know that the zeros of $f(x)$ in K are also the zeros of $f(x)$ in E. We know that $Gal(E/K)$ generates the zeros of $f(x)$ in E, thus the zeros of $f(x)$ in K is also generated by $Gal(E/K)$. Let $\phi \in Gal(E/F)$ be arbitrary, by the previous discussion, we know that $\phi(K) = K$. Then by lemma 4.4, we have that

$$Gal(E/K) = Gal(E/\phi(K)) = \phi Gal(E/K)\phi^{-1},$$

thus $Gal(E/K)$ is normal in $Gal(E/F)$. It now remains to show that $Gal(K/F) \cong Gal(E/F)/Gal(E/K)$. Since $Gal(E/K)$ is normal in $Gal(E/F)$, we have that for all $\phi \in Gal(E/F)$, $Gal(E/K) = \phi Gal(E/K)\phi^{-1}$. Then by lemma 4.4, we know that $Gal(E/K) = Gal(E/\phi(K)$, thus ϕ is an automorphism of K. By the first isomorphism theorem, we have that $Gal(E/F)/Gal(E/K)$ is isomorphic to a subgroup of $Gal(K/F)$. By part 1 we proved, we have that $[K : F] = |Gal(E/F)|/|Gal(E/K)| \leq |Gal(K/F)|$. Since $|Gal(K/F) \leq [K : F] = |Gal(E/F)/Gal(E/K)|$. Then by simple algebraic calculation of the degrees, we know that this subgroup is $Gal(K/F)$ itself, thus $Gal(K/F) \cong Gal(E/F)/Gal(E/K)$, as desired.

4. Suppose $f(x)$ is monic irreducible polynomial over K. Since E splits on $f(x)$ over K, let K' be the fixed field of $Gal(E/K)$. We have that E is also the splitting field of $f(x) \in K'[x]$. By previous proof 1, we have that $[E : K] = |Gal(E/K)|$ and $[E : K'] = |Gal(E/K')|$. By lemma 4.3, we have that $Gal(E/K) = Gal(E/K')$. Then $[E : K] = [E : K']$. By theorem 3.9, we have that $[E : K] = [E : K'][K' : K]$. Thus $[K' : K] = 1$, by our choice of K', we know that $K = K'$, that is ,K is the fixed field of $Gal(E/K)$, as desired.

□

The following example help us to understand field extensions and Galois correspondence.

Example 4.6. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$. We want to show that E is Galois over $\mathbb{Q}$ and identify $Gal(E/\mathbb{Q})$.

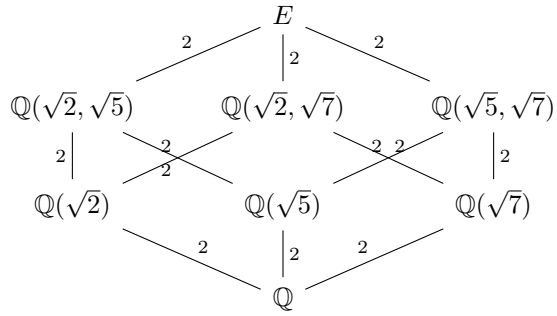
We know that E is Galois over $\mathbb{Q}$ as it is the splitting field for $f(x) = (x^2 - 2)(x^2 - 5)(x^2 - 7)$. We can see that $f(x)$ splits in E with the way it is constructed.

We can also understand the degree of E over $\mathbb{Q}$ by adjoining the roots of the polynomial to the base field. Let $F = \mathbb{Q}(\sqrt{2})$, we know that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$, and we have that the minimal polynomial of F over $\sqrt{5}$ is $x^2 - 5$. Then we adjoin $\sqrt{5}$ to F and get $K = F(\sqrt{5})$. Similarly, $\sqrt{7} \notin K$, then the minimal polynomial of K over $\sqrt{7}$ is $x^2 - 7$, then we can adjoin $\sqrt{7}$ to G and result us E. This shows that $E = K(\sqrt{7}) = F(\sqrt{5}, \sqrt{7})$ has degree 8 over $\mathbb{Q}$.

Now that we have the size of $Gal(E/\mathbb{Q})$, we want to see what it does. Since we defined $G = F(\sqrt{5})$, we can now extend the identity map on the intermediate field G to an element α of $Gal(E/\mathbb{Q})$ that sends $\sqrt{7}$ to $-\sqrt{7}$, but fixes $\sqrt{2}$ and $\sqrt{5}$. Similarly, we can get a member β of $Gal(E/\mathbb{Q})$ that sends $\sqrt{5}$ to $-\sqrt{5}$ from the extension of identity map on $\mathbb{Q}(\sqrt{2}, \sqrt{7})$ and a member ϕ of $Gal(E/\mathbb{Q})$ sending $\sqrt{2}$ to $-\sqrt{2}$ from the extension of identity map on $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.

We can see that all the 3 mappings have order 2. Since these mappings are elements of $Gal(E/\mathbb{Q})$ which is a group, we can compose them together in the following way, $\alpha\beta$ sending $\sqrt{7}$ to $-\sqrt{7}$ and $\sqrt{5}$ to $-\sqrt{5}$ but fixing $\sqrt{2}$, $\alpha\phi$ that sends $\sqrt{7}$ to $-\sqrt{7}$ and $\sqrt{2}$ to $-\sqrt{2}$ but fixing $\sqrt{5}$, $\beta\phi$ sending $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{5}$ to $-\sqrt{5}$ but fixing $\sqrt{7}$, $\alpha\beta\phi$ send each square roots to their negatives. Note that all the above maps have order 2. We now have 7 members of $Gal(E/\mathbb{Q})$ and the identity map. Thus by theorem 4.5, since $|Gal(E/\mathbb{Q})| = 8$, we have that the collection of the maps is $Gal(E/\mathbb{Q})$. Since there's 7 elements of order 2, by previous study of group theory, we have that $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

We also know that there are 3 degree 2 field extensions $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{7})$ and 3 degree 4 extensions $\mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{7}), \mathbb{Q}(\sqrt{5}, \sqrt{7})$, and E itself is a degree 8 extension.



Knowing the fundamental theorem of Galois Theory let us apply group theory to polynomials. Later, we will study solvable groups to see how a group can be solvable and then we will show that if a polynomial is solvable by radicals, its corresponding Galois group is a solvable group. After that, we will apply this fact to show that our choice of quintic polynomial is not solvable by radicals since its Galois group is not solvable.

5 Solvable groups

Let's start with defining what it means to be solvable for a group, and learn some properties of solvable group. We will link solvable groups with solvable by radicals in the latter chapter. We'll also introduce the definition of simple groups, these will help to prove the simplicity of the alternating group of degree 5. Then tinkering with the definition of simple groups and the definition of solvable groups will yield us the fact that S_5 is not solvable. This fact will be extremely helpful to our final proof, as we will later show that the Galois group of the quintic polynomial selected in the final proof is isomorphic to S_5. The progression of definition and theorems is based on chapter 14 "Solubility and Simplicity" from [Ste04, p. 143].

Below is the definition for a solvable group.

Definition 5.1. A group G is solvable if it has a finite series of subgroups

$$1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$$

such that

1. $G_i \triangleleft G_{i+1}$ for $i = 0, \ldots, n-1$.
2. G_{i+1}/G_i is abelian for $i = 0, \ldots, n-1$.

The following lemma is indeed the first and the second isomorphism theorem.

Lemma 5.2. *Suppose G, H, A are groups, then*

1. *If $H \triangleleft G$ and $A \subseteq G$, then $H \cap A \triangleleft A$ and*

$$\frac{A}{H \cap A} \cong \frac{HA}{A}$$

2. *If $H \triangleleft G$ and $H \subseteq A \triangleleft G$ then $H \triangleleft A$, $A/H \triangleleft G/H$ and*

$$\frac{G/H}{A/H} \cong \frac{G}{A}$$

We now proceed to show some properties of solvable groups with the previous lemma, that is solvable groups remain solvable with certain operations.

Theorem 5.3. *Suppose G is a group, $H \leqslant G$, and $N \triangleleft G$.*

1. *If G is solvable, then H is solvable.*

2. *If G is solvable, then G/N is solvable.*

3. *If N and G/N are solvable, then G is solvable.*

Proof. 1. Assume G is solvable, we want to show that H is solvable. Since G is solvable by assumption. let $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$ be a series for G where G_{i+1}/G_i is abelian. Let $H_i = G_i \cap H$. Then H has a series $1 = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = H$, it remains to be show that H_{i+1}/H_i is abelian. We calculate

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

by lemma 5.2(1), and since $\frac{G_i(G_{i+1} \cap H)}{G_i} \leqslant \frac{G_{i+1}}{G_i}$ where G_{i+1}/G_i is abelian, hence H_{i+1}/H_i is abelian, thus we have that H is solvable.

2. Assume G is solvable, we want to show that G/N is solvable. Let $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$ be a series for G where G_{i+1}/G_i is abelian. Then G/N has a series

$$1 = N/N = G_0N/N \triangleleft G_1N/N \triangleleft \ldots G_nN/N = G/N,$$

it remains to show that $\frac{G_{i+1}N/N}{G_iN/N}$ is abelian,

$$\frac{G_{i+1}N/N}{G_iN/N} \cong \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}$$

by lemma 5.2, and is a quotient of G_{i+1}/G_i which is abelian, hence $\frac{G_{i+1}N/N}{G_iN/N}$ is abelian, thus G/N is solvable.

3. Assume N and G/N are solvable, we want to show that G is solvable. Let $1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_m = N$, and $1 = G_0/N \triangleleft G_1/N \triangleleft \ldots \triangleleft G_n/N = G/N$ be series for N and G/N. Then we can combine the two series together and get $1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_m = N = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$, then we have that the quotients of the series are either in the form of N_{i+1}/N_i or G_{i+1}/G_i, which are both abelian by our assumption that N and G/N are solvable and $G_{i+1}/G_i \cong \frac{G_{i+1}/N}{G_i/N}$. Thus, we have that G is solvable.

□

We now wish to introduce the definition of simple group, then we will move on to show that $\mathbb{A}_5$ is indeed a simple group. The main idea is to use this fact, and correlate it with the fact that $\mathbb{A}_5$ is simple to show that S_5 is not solvable.

Definition 5.4. Let G be a group, then G is simple if its only normal subgroups are 1 and G.

We will proceed to show that $\mathbb{A}_5$ is simple using the definition of a simple group.

Theorem 5.5. *The alternating group $\mathbb{A}_5$ is simple.*

Proof. If $\mathbb{A}_5$ had a nontrivial proper normal subgroup H, then the order of H must be equal to $2, 3, 4, 5, 6, 10, 12, 15, 20$ or 30. Since $\mathbb{A}_5$ contains 24 elements of order 5, 20 elements of order 3, and no element of order 15. Then if $|H| = 3, 6, 12$ or 15, we have that $|\mathbb{A}_5/H|$ is prime to 3, and H need to contain all 20 elements of order 3, a contradiction. If $|H| = 5, 10$ or 20, then $|\mathbb{A}_5/H|$ is prime to 5, and H needs to contain all 24 elements of order 5, a contradiction. If $|H| = 30$, $|\mathbb{A}_5/H|$ is prime to 5 and 3,thus H needs to contain all 44 elements of 3 and 5, a contradiction. If $|H| = 2$ or $|H| = 4$, then $|\mathbb{A}_5/H| = 30 or 15$, but groups of order 30 or 15 contains an element of order 15 which $\mathbb{A}_5$ doesn't have, then we reach another contradiction. Thus we have that $\mathbb{A}_5$ is simple, as desired. □

We now use the definition of solvable group and simple group to show that the condition of a solvable group being simple. Later we will use this theorem to show that S_5 is not solvable by contradiction.

Theorem 5.6. *A solvable group G is simple if and only if G is cyclic and has prime order.*

Proof. $\longleftarrow$: Assume G is simple, we want to show it is cyclic and has prime order. Since G is solvable, then we know that it has series $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$, with $G_i \neq G_{i+1}$. Then G_{n-1} is a normal subgroup of G. Since G is simple by assumption, we have that $G = G_n/G_{n-1}$, and G is abelian. Since subgroups of an abelian group is normal, and elements of G generates a cyclic subgroup, G is cyclic without non-trivial proper subgroups. Thus we have that G has prime order.
$\longrightarrow$: Assume G is cyclic, then we have that it s only normal subgroups are 1 and itself, thus G is simple. □

We now show that S_5 is not solvable as a corollary to the since in the final proof we will be showing that the Galois group of the choosing quintic is not solvable, where we will show that the Galois group for the choosing quintic is isomorphic to S_5. Thus we can show that Galois group in question is not solvable.

Corollary 5.7. *The symmetric group S_5 is not solvable.*

Proof. We prove by contradiction. Assume S_5 are solvable, then by theorem 5.3, $\mathbb{A}_5$ is solvable since $\mathbb{A}_5 \leqslant S_5$, also $\mathbb{A}_5$ is simple by theorem 5.5, then by theorem 5.6, $\mathbb{A}_5$ has prime order. Since $|\mathbb{A}_5| = \frac{1}{2}(5!) = 60$ which is not a prime order, thus we have a contradiction, then S_n of degree n is not solvable for $n = 5$, as desired. □

We now show the fact that a 2-cycle and a 5-cycle generate S_5, thus we will later be able to show that Galois group of the quintic polynomial selected is isomorphic to S_5, as it will permute all five zeros of the polynomial, where the polynomial has exactly three real zeros and two complex zeros.

Theorem 5.8. *A 2-cycle and a 5-cycle generate S_5.*

Proof. Let $\alpha = (12)$ be the 2-cycle, and $\beta = (12345)$ be the 5-cycle. We want to show that α and β can generate S_5. We calculate that $\beta\alpha\beta^{-1} = (23)$. Similarly, $\beta(23)\beta^{-1} = (34)$, and $\beta(34)\beta^{-1} = (45)$. Similarly, we can get (51) from operations by α and β. Now we let $a, b \in \{1, 2, 3, 4, 5\}$ be arbitrary with $a < b$. Then for any 2-cycles (ab), we can write (ab) as composition of 2-cycles that can be generated from α and β, that is $(ab) = ((a+1)a)((a+2)(a+1)) \ldots ((b-1)(b-2))((b-1)b)((b-2)(b-1)) \ldots ((a+1)(a+2))(a(a+1))$. Since every permutation in S_5 is a product of 2-cycles, and these 2-cycles can be generated by α and β, we have that a 2-cycle and a 5-cycle can generate S_5. □

6 Final Proof

A radical expression is written by the coefficients of the formula by operation of addition, multiplication, subtraction, division, as well as taking the nth root. We now want to understand such an expression in

the sense of extension field. In this section, we will show that any polynomial equations that are solvable by radicals satisfy the condition that the associated Galois group is a solvable group. We will, in the end, construct a quintic function, $x^5 - 4x + 2 = 0$, and show that this quintic equation cannot be solved by radicals. Some of the techniques of the proof in this section are partially based on chapter 32 of [Gal17].

Definition 6.1. Let E be an extension field of F in $\mathbb{C}$, then E is radical if $E = F(a_1, a_2, \ldots, a_n)$ and for each $i = 1, \ldots, n$, exist integer k_i such that $a_i^{k_i} \in F(a_1, a_2, \ldots, a_{i-1})$. The elements a_i form a radical sequence for E/F, and the degree of a_i is k_i.

Then we say that a polynomial is solvable by radicals if all of its roots can be written in radical expressions over the rational field. We first see a radical expression.

Example 6.2. The following expression is radical:

$$\sqrt[3]{11}\sqrt[5]{\frac{3+\sqrt{2}}{6}},$$

as this involves only basic operations and taking n^{th} root.
To see it is contained in a radical extension, let $a = \sqrt[3]{11}$, $b = \sqrt{2}$, $c = \sqrt[5]{\frac{3+b}{6}}$. We can then find a radical extension E over $\mathbb{Q}$ where $E = \mathbb{Q}(a, b, c)$. To see why this is radical, we calculate that $a^3 = 11$, $b^2 = 2$, $c^5 = \frac{3+b}{6}$.
We can understand that any radical expressions are contained in radical extensions.

By the following example, we will able to understand why the quadratic formula is in fact a radical expression, and general quadratic polynomials can be solved by radicals.

Example 6.3. All the roots of general quadratic polynomial of rational coefficients in the form $ax^2 + bx + c$ can be written in quadratic formula,

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

It is obvious that this is an radical expression. A radical extension field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{b^2 - 4ac})$ as $(\sqrt{b^2 - 4ac})^2 = b^2 - 4ac$. Thus we can say that the general quadratic polynomials are solvable by radicals.

Our target is to show that general quintic polynomials are not solvable by radicals. That is, not all of the roots can be written in radical expressions. To show this straight forwardly is overwhelming, but thanks

to the previous study of Galois Theory, we can transform the problem to solvability of the Galois group corresponding to the polynomial in discussion.

The theorem we want to show next is that the Galois group of a polynomial is solvable implies the polynomial is solvable by radicals. However, we need one more trick to help us with the proof. We want to show the following theorem.

Theorem 6.4. *Let F be a field with $char(F) = 0$ and $a \in F$. Suppose E is the splitting field of $x^n - a$ over F, then $Gal(E/F)$ is solvable.*

Proof. There are two cases, either F contains the primitive nth root of unity ω, or F doesn't.
In the case that F contains the primitive nth root of unity, let b be a zero of $f(x) = x^n - a$ in E, then we know that the roots of $f(x)$ are $b, \omega b, \omega^2 b, \ldots, \omega^{n-1} b$, then we know that $E = F(b)$. Since E splits over F, we know that $\omega \in F$. We want to show that $Gal(E/F)$ is abelien. Since b is a zero of $f(x)$, we have that elements in $Gal(E/F)$ take b to another zero of $f(x)$. Let $\phi, \tau \in Gal(E/F)$ be arbitrary. Since $\omega \in F$ is constant, we know that ϕ, τ fix ω, and $\phi(b) = \omega^i b$ and $\tau(b) = \omega^j b$, we want to show that $\phi\tau = \tau\phi$. We calculate that $\phi(\tau(b)) = \phi(\omega^j b) = \phi(\omega^j)\phi(b) = \omega^j \omega^i b = \omega^{i+j} b$, and $\tau(\phi(b)) = \tau(\omega^i b) = \tau(\omega^i)\tau(b) = \omega^i \omega^j b = \omega^{i+j} b = \phi(\tau(b))$, thus we have that $Gal(E/F)$ is abelian, since all subgroups of an abelian group is normal, we have that $Gal(E/F)$ is solvable by definition of solvable group.
In the case that F doesn't contain the nth root of unity, ω, let b be a zero of $f(x) = x^n - a$ in E. In the case $a = 0$, we have that $b = 0$, then we know that the automorphisms fix b, then $Gal(E/F)$ is abelian,and thus solvable. In the case that $a \neq 0$, assume $b \neq 0$. Since we know that b and $\omega b \in E$, then we have that $\omega b/b = \omega \in E$, thus $F(\omega) \subset E$, and $F(\omega)$ is the splitting field of $x^n - 1$ over F. Let $\phi, \tau \in Gal(F(\omega)/F)$, where $\phi(\omega) = \omega^i$ and $\tau(\omega) = \omega^j$, then we wish to show that $\phi\tau = \tau\phi$, we calculate $\phi(\tau(\omega)) = \phi(\omega^j) = (\phi(\omega))^j = (\omega^i)^j$, and $\tau(\phi(\omega)) = \tau(\omega^i) = tau(\omega))^i = (\omega^j)^i = (\omega^i)^j = \phi(\tau(\omega))$, thus we have that $Gal(F(\omega)/F)$ is abelian. Since E is also the splitting field of $f(x)$ over $F(\omega)$ where $F(\omega)$ contains ω the primitive nth root of unity, by the previous proof in the above case we have that $Gal(E/F(\omega))$ is abelian. By theorem 4.5, we have that the series $1 \subseteq Gal(E/F(\omega)) \subseteq Gal(E/F)$ is a normal series. Since we have that $Gal(E/F(\omega)), Gal(F(\omega)/F)$ are abelian, where $Gal(F(\omega)/F) \cong Gal(E/F)/Gal(E/F(\omega))$, they are solvable by previous argument, thus by theorem 5.3, we have that $Gal(E/F)$ is solvable, as desired. □

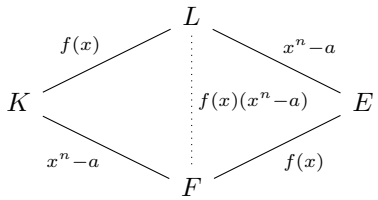
We now show that a function is solvable implies its Galois group is solvable by radicals. But what we will actually be using for the final proof is its contrapositive statement, if Galois group of the polynomial is not solvable, then the polynomial is not solvable by radicals, that is we won't be able to produce a radical

expression for the solutions of the polynomial in discussion.

Theorem 6.5. *Let $f(x) \in F[x]$ and $char(F) = 0$, then suppose that $f(x)$ is solvable by radicals , then the Galois group of f over F is solvable.(contrapositive: If the Galois group of f over F is not solvable, f is not solvable by radicals.)*

Proof. Assume that $f(x)$ is solvable by radicals, that is, $f(x)$ splits in $F(a_1, a_2, \ldots, a_t)$, where ${a_i}^{n_1} \in F$ and ${a_i}^{n_i} \in F(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, t$. Let E be the splitting field for $f(x)$ over F in $F(a_1, a_2, \ldots, a_t)$, we want to show that $Gal(E/F)$ is solvable. We proceed by induction on t.
Base step: $t = 1$. We have that $F \subseteq E \subseteq F(a_1)$ since E is the splitting field for $f(x)$ over F in $F(a_1)$. Let $a = {a_1}^{n_1}$ and L be a splitting field of $x^{n_1} - a$ over F, then we know that $E \subseteq L$ since $a \in F$. Since E and L are splitting fields of polynomial over F, by theorem 4.5, we know that $Gal(E/F) \cong Gal(L/F)/Gal(L/E)$. We have that $Gal(L/F)$ is solvable by theorem 6.4, then by theorem 5.3, we know that $Gal(L/F)/Gal(L/E)$ is solvable. Thus we have that $Gal(E/F)$ is solvable as $Gal(E/F) \cong Gal(L/F)/Gal(L/E)$.

Induction step: Let $t > 1$, let $a = {a_1}^{n_1} \in F$, and L be a splitting field of $x^{n_1} - a$ over E, and $K \subseteq L$ be the splitting field of $x^{n_1} - a$ over F. Since E is a splitting field for $f(x)$ over F, we have that L is a splitting field for $f(x)(x^{n_1} - a)$ over F. Since $K \subseteq L$ and K is a splitting field of $x^{n_1} - a$ over F by our definition, we have that L is a splitting field of $f(x)$ over K. Since $F(a_1) \subseteq K$, we have that $f(x)$ splits in $K(a_2, \ldots, a_t)$, by induction, we have that $Gal(L/K)$ is solvable, and since K is a splitting field of $x^{n_1} - a$ over F, then by theorem 6.4, we have that $Gal(K/F)$ is solvable. As $Gal(L/K)$ and $Gal(K/F)$ solvable, then by theorem 4.5, we have that $Gal(L/F)/Gal(L/K)$ is solvable as $Gal(K/F) \cong Gal(L/F)/Gal(L/K)$. By theorem 5.3, we then know that $Gal(L/F)$ is solvable, by theorem 4.5 and theorem 5.3, we have that $Gal(E/F) \cong Gal(L/F)/Gal(L/E)$ is solvable.



□

Now with all the prerequisites we needed, we are now able to prove a general quintic is not solvable by radicals. We start with choosing a specific quintic polynomial, by showing it is not solvable by radicals, we will be able to show that quintic polynomials don't have a general radical expression. To prove this, it is sufficient for us to find out that its Galois group is not solvable. We will first show that this Galois group is isomorphic to S_5, we will then capitalize the fact that we proved in the previous chapter that S_5 is not solvable.

We choose the polynomial $x^5 - 4x + 2$.

Theorem 6.6. *The Galois group of the polynomial $x^5 - 4x + 2$ over $\mathbb{Q}$ is S_5*

Proof. Let $f(x) = x^5 - 4x + 2$, we have that f is irreducible over $\mathbb{Q}$ by theorem 2.9. Since there are two sign changes in the polynomial, then by Descartes' rule of signs, we have that $f(x)$ has 2 or 0 positive real roots. Since $f(0) = 2$ and $f(1) = -1$, then by intermediate value theorem, we have that $\exists x \in (0, 1)$ such that $f(x) = 0$, thus we have that $f(x)$ has at least one positive real zero, then by previous proof, we have that $f(x)$ has 2 positive real roots. By calculation, we have that $f(-x) = -x^5 + 4x + 2$, and there's one change of signs, then by corollary to Descartes' rule of signs, we have that $f(x)$ has 1 real negative zero. By combination, we have that $f(x)$ has 3 real zeros, each has multiplicity 1. Then we know that there are 2 complex conjugating zeros, namely $a + bi$ and $a - bi$ by theorem 2.6.
It remains for us to show that the Galois group of f over $\mathbb{Q}$ is S_5. Let the five roots of $f(x)$ be a_1, a_2, a_3, a_4, a_5, let $K = \mathbb{Q}(a_1, a_2, a_3, a_4, a_5)$, a K-automorphism that permutes a_i, thus we know that $Gal(K/\mathbb{Q})$ is isomorphic to a subgroup of S_5. Since we know that a_1 is a zero of an irreducible polynomial of degree 5, we have that $[\mathbb{Q}(a_1) : \mathbb{Q}] = 5$, and $5|[K : \mathbb{Q}]$. By theorem 4.5, we know that $5||Gal(K/\mathbb{Q})|$, then we have that $Gal(K/\mathbb{Q})$ contains an element of order 5. Since $Gal(K/\mathbb{Q})$ is isomorphic to a subgroup of S_5, and $Gal(K/\mathbb{Q})$ has an element of order 5, we know that $Gal(K/\mathbb{Q})$ contains a 5-cycle. We also have that $Gal(K/\mathbb{Q})$ contains a mapping α sending $a + bi$ to $a - bi$, which fixes the three real roots and permutes the two complex roots, then we have that α is a 2-cycle since it has 2 distinct elements. By theorem 5.8, we know that a 2-cycle and a 5-cycle generates S_5, thus we have that $Gal(K/\mathbb{Q}) \cong S_5$, as desired. □

Corollary 6.7. *The polynomial $x^5 - 4x + 2$ over $\mathbb{Q}$ is not solvable by radicals.*

Proof. Since the Galois group of $x^5 - 4x + 2$ over $\mathbb{Q}$ is S_5 b y theorem 6.6, and by theorem 5.7 that S_5 is not solvable, then it follows that the Galois group of $x^5 - 4x + 2$ over $\mathbb{Q}$ is not solvable. Thus by theorem 6.5, we have that $f(x)$ is not solvable by radicals, as desired. □

We now come to the final conclusion...

Theorem 6.8. *General quintic polynomials are not solvable by radicals.*

Proof. As we have shown in corollary 6.7 that the polynomial $x^5 - 4x + 2$ over $\mathbb{Q}$ is not solvable by radicals, we know that there is at least one quintic polynomial not solvable by radicals. Thus we can conclude that general quintic polynomials of rational coefficients are not solvable by radicals, as desired. □

References

[Gal17] Joseph Gallian. *Contemporary Abstract Algebra*. Cengage Learning, 2017.

[Ste04] Ian Stewart. *Galois Theory*. Chapman & Hall/CRC Mathematics. Chapman & Hall/CRC, Boca Raton, FL, third edition, 2004.

[Tig01] Jean-Pierre Tignol. *Galois' theory of algebraic equations*. World Scientific Publishing Co., Inc., River Edge, NJ, 2001.