

California State University, San Bernardino

**CSUSB ScholarWorks**

---

Theses Digitization Project

John M. Pfau Library

---

2002

## Fundamental theorem of algebra

Paul Shibalovich

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd-project>



Part of the [Algebra Commons](#)

---

### Recommended Citation

Shibalovich, Paul, "Fundamental theorem of algebra" (2002). *Theses Digitization Project*. 2203.  
<https://scholarworks.lib.csusb.edu/etd-project/2203>

This Thesis is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact [scholarworks@csusb.edu](mailto:scholarworks@csusb.edu).

FUNDAMENTAL THEOREM OF ALGEBRA

---

A Thesis  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

In Partial Fulfillment  
of the Requirements for the Degree  
Master of Arts  
in  
Mathematics

---

by  
Paul Shibalovich

December 2002

FUNDAMENTAL THEOREM OF ALGEBRA


---

A Thesis  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---


by  
Paul Shibalovich  
December 2002


Approved by:

  
\_\_\_\_\_  
Gary R. Griffing, Committee Chair

11/21/02  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Belisario Ventura, Committee Member

  
\_\_\_\_\_  
James S. Okon, Committee Member

  
\_\_\_\_\_  
Peter Williams, Chair  
Department of Mathematics

J. T. Hallett  
\_\_\_\_\_  
Terri Hallett,  
Graduate Coordinator  
Department of  
Mathematics

## ABSTRACT

The Fundamental Theorem of Algebra (FTA) is an important theorem in Algebra. This theorem asserts that the complex field is algebraically closed. That is, if a polynomial of degree  $n$  has  $n-m$  real roots ( $0 \leq m \leq n$ ), then the Fundamental Theorem asserts that the polynomial has its remaining  $m$  roots in the complex plane.

This thesis will include historical research of proofs of the Fundamental Theorem of Algebra and provide information about the first proof given by Gauss of the Theorem and the time when it was proved. Also, it will include proofs of the Fundamental Theorem using three different approaches: algebraic approach, complex analysis approach, and Galois Theory approach.

The conclusion of the thesis will explain the similarities of the three proofs as well as their differences.

## ACKNOWLEDGMENTS

First of all, I want to thank Dr. Gary Griffing, Dr. Belisario Ventura, and Dr. Jim Okon for their willingness to assist me in working on my thesis. In addition, I would like to express a special appreciation to Dr. Gary Griffing for his help and time dedication in helping and working with me. Also, I want to thank all the professors at California State University, San Bernardino who helped me build strong mathematical foundation throughout the two years in the Master's program and prepared me to become successful in Mathematics.

DEDICATION

To

Nadya Pavlov

Timothy Shibalovich

Olga Shibalovich

Lidia Pelepchuk

Anna Pavlenko

Lubov Rudenko

## TABLE OF CONTENTS

ABSTRACT . . . . .	iii
ACKNOWLEDGMENTS . . . . .	iv
CHAPTER ONE: BACKGROUND	
1.1 Introduction . . . . .	1
1.2 Purpose of the Thesis . . . . .	1
1.3 Context of the Problem . . . . .	1
1.4 Significance of the Thesis . . . . .	1
1.5 Notations . . . . .	2
1.6 Organization of the Thesis . . . . .	2
CHAPTER TWO: HISTORY OF THE FUNDAMENTAL THEOREM OF ALGEBRA	
2.1 Introduction . . . . .	4
2.2 Development of the Fundamental Theorem of Algebra . . . . .	4
2.3 Generalization of the Fundamental Theorem of Algebra . . . . .	5
2.4 First Proof of the Fundamental Theorem of Algebra . . . . .	6
2.5 Summary . . . . .	7
CHAPTER THREE: COMPLEX ANALYSIS PROOF OF THE FUNDAMENTAL THEOREM OF ALGEBRA	
3.1 Introduction . . . . .	8
3.2 Definitions and Facts . . . . .	8
3.3 Theorems . . . . .	10
3.4 Fundamental Theorem of Algebra . . . . .	13
3.5 Summary . . . . .	15

## CHAPTER FOUR: ALGEBRAIC PROOF OF THE FUNDAMENTAL THEOREM OF ALGEBRA

4.1 Introduction . . . . .	17
4.2 Definitions . . . . .	17
4.3 Theorems . . . . .	18
4.4 Fundamental Theorem of Algebra . . . . .	30
4.5 Summary . . . . .	33

## CHAPTER FIVE: GALOIS THEORY PROOF OF THE FUNDAMENTAL THEOREM OF ALGEBRA

5.1 Introduction . . . . .	34
5.2 Definitions and Notation . . . . .	34
5.3 Theorems . . . . .	36
5.4 Lemma . . . . .	37
5.5 Fundamental Theorem of Algebra . . . . .	37
5.6 Summary . . . . .	40

## CHAPTER SIX: SIMILARITIES AND DIFFERENCES

6.1 Introduction . . . . .	41
6.2 Similarities and Differences . . . . .	41
REFERENCES . . . . .	43



## CHAPTER ONE

### BACKGROUND

#### 1.1 Introduction

The content of Chapter One presents an overview of the thesis. The contexts of the problem are discussed and are then followed by the purpose and significance of the thesis. Finally, the notation to be used is presented.

#### 1.2 Purpose of the Thesis

The purpose of this thesis is to explore development of the Fundamental Theorem of Algebra. Prior to the 17<sup>th</sup> century AD there were several attempts to prove it, but they failed. It was in 1799 that Gauss, in his dissertation, proved the Theorem for the first time.

#### 1.3 Context of the Problem

Being an instructor of Mathematics, the Fundamental Theorem of Algebra arises in College Algebra class. It is simply stated concept and the students do not have any problem understanding its importance and applicability.

#### 1.4 Significance of the Thesis

The significance of this thesis is to inform the reader about the development of the Fundamental Theorem of Algebra and its proofs. Also, the significance of this

thesis is to educate the reader about different approaches used to prove the Theorem.

## 1.5 Notations

The notational conventions used in this thesis are the following:

### 1.5.1 Definition

FTA will stand for the Fundamental Theorem of Algebra.

### 1.5.2 Definition

The set of real numbers will be denoted by  $R$ .

### 1.5.3 Definition

The set of complex numbers will be denoted by  $C$ .

### 1.5.4 Definition

A set, for example  $P$ , will be denoted by  $P$ .

## 1.6 Organization of the Thesis

This thesis is divided into six chapters. Chapter One provides an introduction to the context of the problem, purpose of the thesis, significance of the thesis, and the notation. Chapter Two consists of historical development of the FTA and its proof. Chapter Three explores the proof of the FTA using complex analysis approach. Chapter Four presents the algebraic proof of the FTA. Chapter Five gives a proof of the FTA using Galois Theory approach.

Chapter Six examines the similarities of the three proofs as well as their differences. Finally, the references include the sources used for this thesis.

## CHAPTER TWO

### HISTORY OF THE FUNDAMENTAL THEOREM OF ALGEBRA

#### 2.1 Introduction

The Fundamental Theorem of Algebra is one of the most important results in Algebra. In the past it provided a motivation to study the set of complex numbers and polynomials whose roots are in this set. In this paper we will research the development of the Fundamental Theorem of Algebra and prove it using different approaches. We will start with development of the FTA, and then lead the reader through to the first proof (1799) presented by Carl Friedrich Gauss (1777-1855). Then we will prove the FTA using three different approaches and explore their similarities and differences. We will prove most theorems used in this thesis. If a theorem is not proved, we will provide ample reference to the proof of the theorem.

#### 2.2 Development of the Fundamental Theorem of Algebra

Early studies of the roots of equations involved only positive real roots, so the Fundamental Theorem of Algebra was not relevant at that time. "Cardano was the first to realize that one could work with quantities more general

than the real numbers" [1]. He worked with cubic equations, in particular, the equation  $x^3 = 15x + 4$  which gave him an answer involving negative square root:  $\sqrt{-121}$ . Cardano was able to manipulate equations with 'complex numbers', but he did not understand his own mathematics. The concept of the number of roots and the degree of a polynomial was slowly developing. In 1629 Flemish mathematician Albert Girard was first to claim that for any equation of degree  $n$  there are always  $n$  roots. However, it was not considered that solutions are of the form  $a + bi$  where  $a$  and  $b$  are real numbers. Girard was the first to conjecture that "a polynomial equation of degree  $n$  must have  $n$  roots" [1]. In 1637 Descartes said that "one can 'imagine' for every equation of degree  $n$ ,  $n$  roots but these imagined roots do not correspond to any real quantity" [2]. However, his statement was merely a suggestion.

### 2.3 Generalization of the Fundamental Theorem of Algebra

The first attempt to 'prove' FTA was given by Leibniz in 1702, however, it was unsuccessful [2]. Leibniz considered the equation  $x^4 + y^4 = 0$  and claimed that this equation could never be written as a product of two real quadratic factors. Unfortunately, he was mistaken not

realizing that  $x^4 + y^4 = 0$  can be written as

$$x^4 + 2x^2y^2 + y^4 - 2x^2y^2 = 0 \text{ or } (x^2 + y^2)^2 - 2x^2y^2 = 0 \text{ or}$$

$$(x^2 + y^2 - \sqrt{2}xy)(x^2 + y^2 + \sqrt{2}xy) = 0. \text{ Leibniz' conclusion withheld}$$

him from further study of the general equation  $x^4 + y^4 = 0$ ,

and thus from finding the complex roots of the equation

$$x^4 + 1 = 0. \text{ Then in 1742 Euler showed that Leibniz'}$$

assertion was false. Later, Euler proved that every real

polynomial of degree  $n$ ,  $n \leq 6$ , has exactly  $n$  'complex

roots'. It was only in 1749 that Euler tried to prove the

FTA for the general case. At that time the FTA was

generalized and stated as follows:

*"Every polynomial of degree  $n$  with real coefficients  
has exactly  $n$  zeros in  $C$ " [1].*

Nowadays, the FTA is stated in the following way:

*"A polynomial with coefficients which are complex numbers  
has all its roots in the complex field" [3].*

## 2.4 First Proof of the Fundamental Theorem of Algebra

There were several attempts to prove the FTA for the general case, but the first legitimate proof was given by Carl Friedrich Gauss in his doctoral thesis of 1799 [1]. This proof was topological in nature. Throughout his lifetime Gauss produced several different proofs.

## 2.5 Summary

The FTA was born with an intuitive idea, which was later generalized by Girard in 1629, and finally became a fundamental result in Algebra. Since the first proof of the FTA that was done by Gauss in 1799 we have, today, at least six conceptually different proofs of this important Theorem[3]. These proofs include a complex analysis approach, and analysis approach, a purely algebraic approach without Galois Theory, and algebraic approach with some analysis, a topological approach, and Galois Theory approach. In this thesis, we will explore three proofs of the FTA using a complex analysis approach, a non-Galois Theory algebraic approach, and a Galois Theory approach.

CHAPTER THREE  
COMPLEX ANALYSIS PROOF OF THE  
FUNDAMENTAL THEOREM  
OF ALGEBRA

3.1 Introduction

The proof of the FTA using the complex analysis approach requires some complex analysis background. Section 3.2 provides definitions needed to prove the Theorem. In addition to these definitions we will use Liouville's Theorem and the Cauchy Inequality. The proofs for Liouville's Theorem and the Cauchy Inequality will be provided in sections 3.3.2 and 3.3.3 respectively. Section 3.4 will provide the complex analysis proof of the FTA.

3.2 Definitions and Facts

3.2.1 Definition

A function  $f(z)$  of the complex variable  $z$  is analytic in an open set  $G$  if it has a derivative at each point in the set  $G$ .

3.2.2 Definition

An entire function is a function that is analytic at each point in the entire complex plane.



### 3.2.3 Definition

A function  $f(z)$  of the complex variable  $z$  is said to be continuous in a region  $G$  if it is continuous at each point in  $G$ .

### 3.2.4 Definition

The function  $f(x)$  is bounded on the set  $K$  if there is a number  $M$  such that  $|f(x)| \leq M$  for all  $x \in K$ .

In the proof of Liouville's Theorem we will use Cauchy Integral Formula and Cauchy-Riemann equations stated below.

### 3.2.5 Fact (Cauchy Integral Formula)

If a function  $f(z) = u(x, y) + iv(x, y)$  is analytic at a point  $z_0 = x_0 + iy_0$  and the component functions  $u$  and  $v$  have continuous partial derivatives of all orders at that point, then

$$f^{(n)}(z_0) = \frac{n!}{2\pi i} \int_C \frac{f(z) dz}{(z - z_0)^{n+1}} \text{ for } n = 0, 1, 2, \dots$$

where  $C$  is a positively oriented simple closed contour and  $|f(x)| \leq M$  [4].

### 3.2.6 Fact (Cauchy-Riemann Equations) [4].

Let  $f(z) = u(x, y) + iv(x, y)$ . If  $f'(z)$  exists where  $z_0 = x_0 + iy_0$ , then the following are true.

$$\text{i)} \quad u_x(x_0, y_0) = v_y(x_0, y_0)$$

$$\text{ii)} \quad u_y(x_0, y_0) = -v_x(x_0, y_0)$$

### 3.3 Theorems

Theorem 3.3.1: If  $f'(z) = 0$  everywhere in a domain  $D$ , then  $f(z)$  must be constant throughout  $D$  [4].

Proof: Let  $f(z) = f(x, y) = u(x, y) + iv(x, y) \in C$  and  $z = x + iy$ . Suppose  $f'(z) = f'(x, y) = 0 \quad \forall z \in C$ . In order to show that  $f(z)$  must be constant throughout  $D$ , it suffices to show that  $f(z) = a + ib$  with  $a, b \in R$  for all  $z$ . Since  $f'(z) = 0$  and  $f'(z) = u_x + iv_x$ , we get  $u_x = 0 = v_x$ . Similarly,  $f'(z) = 0$  and  $f'(z) = u_y + iv_y$  give us  $u_y = 0 = v_y$ . So, we have equality  $u_x = u_y = v_x = v_y = 0$ . This implies that  $u = a$  and  $v = b$  with  $a, b \in R$  for all  $z$ . Thus, we conclude that  $f(z) = a + ib$  an element of  $C$  for all  $z$ . Hence,  $f(z)$  must be constant throughout  $D$ .

Theorem 3.3.2: Let  $z_0 = x_0 + iy_0$ ,  $f(z) = u(x, y) + iv(x, y)$  be an analytic function within and on a circle  $|z - z_0| = r$ , and component functions  $u$  and  $v$  have continuous partial derivatives of all orders at that point. Also, let  $C$  denote the positively oriented circle  $|z - z_0| = r$ , then

$$|f^{(n)}(z_0)| \leq \frac{n!M_r}{r^n}$$

where  $r$  is radius of the circle  $C$  and  $M_r$  is the maximum value of the function on  $C$  [4].

Proof: Assume that  $z_0 = x_0 + iy_0$  and that

$f(z) = u(x, y) + iv(x, y)$  is an analytic function within and on a circle  $|z - z_0| = r$ . Since the component functions  $u$  and  $v$  have continuous partial derivatives of all orders, and  $f$  is bounded on  $C$ , then by Cauchy Integral Formula

$$f^{(n)}(z_0) = \frac{n!}{2\pi i} \cdot \int_C \frac{f(z)dz}{(z - z_0)^{n+1}} \text{ for } n = 0, 1, 2, \dots \quad (1)$$

where  $C$  is a positively oriented circle  $|z - z_0| = r$  and

$$|f(z)| \leq M.$$

Now, the maximum value of  $|f(z)|$  on the circle  $C$

depends on the radius of  $C$ . Let  $M_r$  denote that maximum value of  $|f|$  on the circle of radius  $r$ . Using (1), we get

the Cauchy Inequality  $|f^{(n)}(z_0)| \leq \frac{n!}{2\pi} \cdot \frac{M_r}{r^{n+1}} \cdot 2\pi r$  for  $n = 1, 2, \dots$  or

$$|f^{(n)}(z_0)| \leq \frac{n!M_r}{r^n} \text{ for } n = 1, 2, \dots$$

where  $M_R$  is a bound for  $f(z)$  on  $|z - z_0| \leq r$ .

Theorem 3.3.3 (Liouville's Theorem): If  $f(z)$  is entire and bounded in the complex plane  $C$ , then  $f(z)$  is constant throughout the plane.

*Proof:* Let  $f(z)$  be an entire and bounded function in the complex plane. To prove this theorem we need to show that  $f(z)$  is a constant throughout  $C$  [4].

We are given that  $f(z)$  is entire. By definition of 3.2.2,  $f(z)$  is analytic at each point in the entire plane. Then, by definition of 3.2.1,  $f(z)$  has a derivative at each point in the set  $C$ . Now, by Theorem 3.2.2 for any circle in the plane, there exists maximum value  $M_r > 0$  that depends on the radius  $r$  of the circle  $C$  such that

$|f'(z)| \leq \frac{M_r}{r}$  for an arbitrary  $z \in C$ . In this theorem we are

also given that  $f(z)$  is bounded in the complex plane. This implies that there exists a constant  $M > 0$  such that

$|f(z)| \leq M$  for all  $z \in C$ . Since  $M_r$  is maximum value of  $f$  on  $C$  and  $M$  is maximum value in entire plane, the

inequality  $M_r \leq M$  is true independently of the radius  $r$ .

Thus,  $|f'(z)| \leq \frac{M}{r}$  where  $z$  is any fixed point and  $r$  is

arbitrary large. However, the inequality  $|f'(z)| \leq \frac{M}{r}$  with

an arbitrary large radius  $r$  can hold only if  $f'(z) = 0$ .

Since the choice of  $z$  was arbitrary, the statement

$f'(z) = 0$  must be true everywhere in the complex plane.

Hence, function  $f(z)$  is a constant.

### 3.4 Fundamental Theorem of Algebra

Theorem 3.4.1: Any polynomial

$P(z) = a_0 + a_1z + a_2z^2 + \dots + a_nz^n$  with  $a_n \neq 0$  of degree  $n \geq 1$

has at least one zero in  $C$ . That is, there exists at

least one point  $z_0$  such that  $P(z_0) = 0$  [4].

Proof: Suppose  $P(z) = a_0 + a_1z + a_2z^2 + \dots + a_nz^n$ , where

$a_n \neq 0$ . Consider  $f(z) = \frac{1}{P(z)}$ . Since  $\forall z \in C$  there exists a

derivative of  $f(z)$ , the function  $f(z)$  is analytic. By

definition 3.2.2,  $f(z)$  is an entire function. Now, we want

to show that  $f(z)$  is bounded in  $C$ . Dividing  $P(z)$  by  $z^n$ , we

get  $\frac{P(z)}{z^n} = \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \dots + \frac{a_{n-1}}{z} + a_n$  where  $a_n \neq 0$ . Now, let

$$w = \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \dots + \frac{a_{n-1}}{z} \quad (2)$$

This implies that  $P(z) = (w + a_n)z^n$ . There exists large

enough  $K \in N$  such that when  $|z| \geq K$ ,  $\frac{|a_i|}{|z^{n-i}|} < \frac{|a_n|}{2n}$

$\forall i = 1, 2, \dots, n$ , that is for each  $\frac{a_i}{z^{n-i}}$  in (2). By the

triangular inequality this implies that

$$|w| \leq \frac{|a_0|}{|z^n|} + \frac{|a_1|}{|z^{n-1}|} + \dots + \frac{|a_{n-1}|}{|z|} < \frac{|a_n|}{2} \text{ for all values of } z. \text{ So}$$

when  $|z| \geq K$ ,  $|w| < \frac{|a_n|}{2}$ . Thus,  $|w| - |a_n| < \frac{|a_n|}{2} - |a_n|$  or

$$|w| - |a_n| < -\frac{|a_n|}{2}, \text{ and hence } |a_n| - |w| > \frac{|a_n|}{2}. \text{ Consequently,}$$

we get that

$$||a_n| - |w|| > \frac{|a_n|}{2} \quad (3)$$

However,  $|a_n + w| \geq ||a_n| - |w||$  is always true. This and

inequality (3) then gives us  $|a_n + w| \geq ||a_n| - |w|| > \frac{|a_n|}{2}$  or

$$|a_n + w| > \frac{|a_n|}{2} \quad (4)$$

Since  $P(z) = (w + a_n)z^n$  and because of inequality (4), we

can say that  $|P(z)| = |a_n + w| \cdot |z^n| > \frac{|a_n|}{2} \cdot |z|^n \geq \frac{|a_n|}{2} \cdot K^n$  whenever

$|z| \geq K$  for arbitrary positive real number. This then

implies that  $|P(z)| > \frac{|a_n|}{2} \cdot K^n$  or  $|f(z)| = \frac{1}{|P(z)|} < \frac{2}{|a_n| \cdot K^n}$

whenever  $|z| \geq K$ . This shows that  $f$  is bounded in the

region exterior to the disk  $|z| \geq K$ . The function  $f(z)$  is continuous in the closed disk  $|z| \leq K$  because  $f(z) = \frac{1}{P(z)}$  is differentiable at each  $z \in C$ . Therefore  $f(z)$  is bounded in the closed disk  $|z| \leq K$ . This implies that  $f(z)$  is bounded in the entire plane.

Since  $f(z)$  is entire and bounded in  $C$  by the Liouville's Theorem,  $f(z)$  is a constant. Since  $f(z)$  is a constant,  $f(z) = \frac{1}{P(z)}$  and  $\deg P(z) \geq 1$ ,  $P(z)$  is also a constant. But this is a contradiction. Thus, the assumption  $P(z) \neq 0$  for every value of  $z$  is not true. Hence, there exists at least one point  $z_0 \in C$  such that  $P(z_0) = 0$ .

### 3.5 Summary

The complex analysis proof of the FTA is concise, and is proved by contradiction. The argument in this proof goes as follows: if a non-constant polynomial has no zeros, the multiplicative inverse of this polynomial is a bounded analytic function. However, Liouville's Theorem shows that such a function is constant. Thus, the polynomial itself has to be a constant, which is a

contradiction to the assumption. Although the complex analysis proof does require additional knowledge from Complex Analysis, it is not hard to understand it.



CHAPTER FOUR  
ALGEBRAIC PROOF OF THE  
FUNDAMENTAL THEOREM  
OF ALGEBRA

4.1 Introduction

The algebraic proof of the FTA requires some background from Abstract Algebra. Section 4.2 presents definitions used for theorems in this chapter. Theorems needed to prove the FTA using an algebraic approach without the use of Galois Theory are reviewed in section 4.3. The proof of the FTA is presented in section 4.4.

4.2 Definitions

4.2.1 Definition

A field  $F$  is called formally real if  $-1$  is not expressible in it as a sum of squares.

4.2.2 Definition

A field  $P$  is called a real closed field if  $P$  is formally real, but no proper algebraic extension of  $P$  is formally real.

4.2.3 Definition

A field  $F$  is algebraically closed if every polynomial equation with coefficients in  $F$  has a solution

in  $F$ . That is,  $F$  is algebraically closed if any  $P(x) \in Q[x]$  has its roots in  $Q[x]$ .

#### 4.2.4 Definition

Commutative ring  $F$  in which the set of nonzero elements forms a group with respect to multiplication is called a field. Field  $E$  is said to be an extension of  $F$ , if  $E$  contains a subfield isomorphic to  $F$ .

#### 4.2.5 Definition

Assume that  $E$  is an extension of  $F$ . An element  $a \in E$  is said to be algebraic over  $F$  if  $a$  is a solution of some polynomial equation with coefficients in  $F$ .

#### 4.2.6 Definition

A field  $K$  is called an ordered field if the property of positiveness ( $> 0$ ) is defined for its elements and if it satisfies the following postulates.

- i)  $\forall a \in K, a = 0, a > 0, -a > 0$
- ii) If  $a > 0$  and  $b > 0$ , then  $a + b > 0$  and  $ab > 0$

### 4.3 Theorems

Theorem 4.3.1: In the field of complex numbers the equation  $x^2 = a + bi$  with  $a$  and  $b$  being real numbers is always solvable. That is, every number of the field has a square root in the field[5].

Proof: Let  $x = c + di$  where  $c$  and  $d$  are real numbers.

This implies that  $x^2 = (c + di)^2 = c^2 + 2cdi - d^2 =$   
 $= (c^2 - d^2) + (2cd)i$ .

Now, let's define  $a$  and  $b$  as

$$a = c^2 - d^2 \quad (1)$$

$$b = 2cd \quad (2)$$

So that  $a + bi = (c^2 - d^2) + (2cd)i$ . Then  $a^2 + b^2$  gives us  
 $a^2 + b^2 = (c^2 - d^2)^2 + (2cd)^2 = c^4 - 2c^2d^2 + d^4 + 4c^2d^2 =$   
 $= c^4 + 2c^2d^2 + d^4$  or  $a^2 + b^2 = c^4 + 2c^2d^2 + d^4 = (c^2 + d^2)^2$ . From  
the last statement we get  $c^2 + d^2 = \sqrt{a^2 + b^2}$ , since  
 $c^2 + d^2 \geq 0$ . Now, from (1) we have  $a = c^2 - d^2$  or  $d^2 = c^2 - a$ .  
This implies that  $c^2 + d^2 = c^2 + c^2 - a$  or  $2c^2 = a + c^2 + d^2$   
or

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \quad (3)$$

Similarly, from (1) we have  $a = c^2 - d^2$  or  $c^2 = d^2 + a$ . This  
implies that  $c^2 + d^2 = d^2 + a + d^2 = \sqrt{a^2 + b^2}$  or

$$d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2} \quad (4)$$

From (3) we get  $c = \pm \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$ , and from (4) we get

$$d = \pm \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}. \text{ This shows that for every choice of}$$

$c$  and  $d$  a square root of  $a + bi$  is in the field of complex numbers.

Now, we will extend previous theorem in the following way.

Theorem 4.3.2: Let  $K$  be any arbitrary ordered field with the property that if  $a \in K$ ,  $a > 0$ , then  $\sqrt{a} \in K$ . If

$a + bi \in K(i)$ , where  $i^2 = -1$ , then there exists  $c + di \in K(i)$  such that  $(c + di)^2 = a + bi$  [5].

Proof: Assume that if  $a \in K$  and  $a > 0$ , then  $\sqrt{a} \in K$ .

Let  $a + bi \in K(i)$ . Need to show that there exists

$c + di \in K(i)$  such that  $(c + di)^2 = a + bi$ . From Theorem 4.3.1

we found that  $c = \pm \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$ ,  $d = \pm \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}$ .

Choose  $c = \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$  and  $d = \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}$ , then

$$(c + di)^2 = \left( \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \right)^2 =$$

that for every  $M > 0$  there exists  $0 < x_0$  such that for all

$x_0 < x_1$ ,  $0 < M < \frac{P(x_1)}{x_1^{n-1}}$  and therefore  $P(x_1) > 0$ .

Similarly,  $\lim_{x \rightarrow -\infty} \frac{P(x)}{x^{n-1}} = \lim_{x \rightarrow -\infty} \frac{a_n x^n + \dots + a_1 x + a_0}{x^{n-1}} =$   
 $= \lim_{x \rightarrow -\infty} (a_n x + a_{n-1} + \frac{1}{x}(a_{n-2} + \frac{a_{n-3}}{x^2} + \dots + \frac{a_0}{x^{n-1}})) = -\infty$ . This implies

that for every  $M < 0$  there exists  $x_0 < 0$  such that for

all  $x_1 < x_0$ ,  $\frac{P(x_1)}{x_1^{n-1}} < M < 0$  and therefore  $P(x_1) < 0$ . Since

$P(x_1) > 0$  and  $P(x_2) < 0$ , from the Intermediate Value Theorem it follows that there exists an  $x_3$  between  $x_1$  and  $x_2$  such that  $P(x_3) = 0$ . Hence, if  $P(x)$  is of odd degree, then it must have a real root. Similarly, when leading coefficient  $a_n < 0$ ,  $P(x)$  also has a real root. Thus, if  $P(x)$  is of odd degree, then it must have a real root.

Theorem 4.3.4: Let  $P$  be a real closed field, then  $P$  can be ordered in one and only one way[3].

Proof: In order to prove this Theorem we need to show two things. First, if  $a \neq 0 \in P$ , then either  $a$  or  $-a$  is a square. Moreover, these cases are mutually exclusive. So we need to show that either  $a$  is a square or  $-a$  is a

square. Second, we need to show that the ordering of real closed field  $P$  is unique.

Suppose  $\gamma \in P$  is not the square of an element in  $P$ , then  $\sqrt{\gamma}$  is a root of  $x^2 - \gamma$  and it follows that  $P \subset P(\sqrt{\gamma})$ . This implies that  $P(\sqrt{\gamma})$  is not formally real. Since  $P(\sqrt{\gamma})$  is not formally real,

$$-1 = \sum_{i=1}^n (\alpha_i \sqrt{\gamma} + \beta_i)^2$$

This implies that  $-1 = \sum_{i=1}^n (\gamma \alpha_i^2 + 2\alpha_i \beta_i \sqrt{\gamma} + \beta_i^2)$  with  $\alpha_i, \beta_i \in P$

or  $-1 = \gamma \sum_{i=1}^n \alpha_i^2 + \sum_{i=1}^n 2\alpha_i \beta_i \sqrt{\gamma} + \sum_{i=1}^n \beta_i^2$ . Since by hypothesis

$\sqrt{\gamma} \notin P$ , we get  $2 \sum_{i=1}^n \alpha_i \beta_i = 0$  and therefore

$$-1 = \gamma \sum_{i=1}^n \alpha_i^2 + \sum_{i=1}^n \beta_i^2.$$

However, we know that  $P$  is formally real. This implies that  $\gamma \sum_{i=1}^n \alpha_i^2 \neq 0$ . Consequently,  $\gamma \sum_{i=1}^n \alpha_i^2 = -1 - \sum_{i=1}^n \beta_i^2$

$$\text{and} \quad \gamma = \frac{-1 - \sum_{i=1}^n \beta_i^2}{\sum_{i=1}^n \alpha_i^2} \quad (5)$$

Thus,  $\gamma \in P$  is not the square of an element in  $P$ , because

$\gamma$  cannot be expressed as a sum of squares in  $P$ ; for otherwise  $-1$  is a sum of two squares in  $P$ . Equivalently, by contrapositive, if  $-\gamma$  is a sum of two squares then  $-\gamma \in P$  is the square of an element in  $P$ . So, we need to show that  $-\gamma$  is a sum of two squares. Now, from (5) we obtain

$$-\gamma = \frac{1 + \sum_{i=1}^n \beta_i^2}{\sum_{i=1}^n \alpha_i^2}$$

But since  $1^2 + \sum_{i=1}^n \beta_i^2$  is a sum of squares, both the numerator and denominator are sums of squares. Hence, both numerator and denominator are squares. This implies that  $-\gamma = c^2$  for some  $c \in P$ .

Now, we need to prove the uniqueness of ordering on  $P$ . Let ' $<$ ' be an ordering on  $P$  defined by  $0 < a$  if and only if  $a = b^2$  ( $b \neq 0$ ). Suppose there exists any other ordering ' $<<$ ' on  $P$ . In order to show uniqueness of the ordering on  $P$ , we need to show two things.

- i) Assume  $0 << a$ . By proof either  $a$  or  $-a$  is a square. But squares are positive. This implies that we cannot have  $-a$  as a square. Therefore, we

must have  $a = b^2$  ( $b \neq 0$ ). Hence, by the definition of the ordering of ' $<$ ', we get  $0 < a$ .

ii) Now suppose that  $0 < a$ . By definition of ' $<$ ' this implies that  $a = b^2$  ( $b \neq 0$ ).

a) If  $b >> 0$ , then by definition 4.2.6  $b^2 >> 0$ .

Therefore, we get  $a = b^2 >> 0$ . Hence, we conclude that  $a >> 0$ .

b) If  $-b >> 0$ , then by definition 4.2.6  $(-b)^2 >> 0$ .

Therefore, we get  $a = (-b)^2 >> 0$ . Hence, we conclude that  $a >> 0$ .

Therefore, if  $P$  is a real closed field, then it can be ordered in one and only one way.

Theorem 4.3.5: In a real closed field (*r.c.f.*)  $P$  every polynomial of odd degree has at least one root in  $P$ . Let  $P$  be a *r.c.f.*, then every  $f(x) \in P[x]$  of odd degree has at least one root [5].

Proof: Let  $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in P[x]$ ,  $n$  is odd,  $a_n \neq 0$ , and  $P$  be a *r.c.f.*

Assume that all odd polynomials of odd degree less than  $n$  have at least one root.

Either  $f(x)$  is reducible or irreducible in  $P[x]$ .



Case 1) Suppose  $f(x)$  is reducible in  $P[x]$ , then this implies that  $f(x) = f_1(x) \cdot q(x)$  where  $f_1(x)$  is irreducible and  $q(x)$  may or may not be reducible in  $P[x]$ . If  $q(x)$  is reducible we can apply induction on  $q(x)$  and reduce  $f(x)$  to  $f(x) = f_1(x) \cdots f_m(x)$  where each  $f_i(x)$  is irreducible in  $P[x]$ . Since  $f(x)$  is of odd degree, one of  $f_i(x) \in P[x]$  is of odd degree and, by induction on degree of  $f$ ,  $f(x)$  has a root in  $P$ . Hence,  $f(x)$  has a root in  $P$ .

Case 2) Suppose  $f(x)$  is irreducible in  $P[x]$ . Then  $f(x)$  has a root in an extension field  $P(\alpha)$ . This then implies that  $f(x) = c \cdot (x - \alpha) \cdot f_1(x) \cdots f_k(x)$  with  $f_i(x)$  irreducible for  $1 \leq i \leq k \leq n$  in  $P(\alpha)[x]$ . Since  $P$  is a r.c.f., by definition 4.2.2  $P(\alpha)$ , a proper extension of  $P$ , is not formally real. So, then we can express  $-1$  as

$$-1 = \sum_{i=1}^r (h_i(\alpha))^2 \text{ for some } r \in \mathbb{N} \quad (6)$$

where  $h_i(\alpha) = c_{0,i} + c_{1,i}\alpha + c_{2,i}\alpha^2 + \cdots + c_{m,i}\alpha^m, c_i \in P$  with  $m < n$ . The degree of  $h_i(x)$  is at most  $n-1$  since  $\deg f(x) = n$ , and  $\alpha$  is a symbolically adjoined root of  $f(x)$ . Now, applying the division algorithm we get

$$\sum_{i=1}^r (h_i(x))^2 = f(x) \cdot g(x) + r(x) \quad (7)$$

where  $\deg r(x) < \deg f(x)$  and  $\deg f(x) = n$ .

Evaluating (7) at  $\alpha$ , we get

$-1 = \sum (h_i(\alpha))^2 = 0 \cdot g(\alpha) + r(\alpha) \in P(\alpha)$ , because  $f(\alpha) = 0$ . This implies that  $r(\alpha) = -1$ . Now,  $\forall h_i(x) \in P(\alpha)[x]$  where  $\alpha$  is symbolically adjoined root of  $f(x)$ , we have  $r(x) = -1$ . From equality (2) we get  $\sum (h_i(x))^2 = f(x) \cdot g(x) + (-1)$ . This gives us an identity

$$-1 = \sum (h_i(x))^2 + (-1)f(x) \cdot g(x) \quad (8)$$

We know that  $\sum (h_i(x))^2$  is of even degree greater than one. This means that the leading coefficients of  $(h_i(x))^2$  are squares which implies that leading coefficients of  $(h_i(x))^2$  can not cancel out in addition. Moreover,  $\deg h_i(x)$  is less than or equal to  $n-1$ . This implies that  $\deg \sum (h_i(x))^2 \leq 2n-2$ , since the leading coefficient  $(x^{n-1})$  raised to the second power gives us  $(x^{n-1})^2 = x^{2n-2}$ . Since  $\deg \sum (h_i(x))^2 \leq 2n-2$  is even, from equality (7) we get that  $\deg f(x) \cdot g(x) \leq 2n-2$  also must be even. Moreover,  $\deg f(x) = n$  is odd. This implies that  $\deg g(x) \leq n-2$  also

is odd. By induction on  $n$  there exists  $a \in P$  such that  $g(a) = 0$ . Using identity (8) we get  $-1 = \sum (h_i(a))^2$  since  $a$  is a root of  $g(x)$ . So this means that  $P$  is not formally real, but by assumption  $P$  is formally real. This gives us a contradiction. So then  $f(x)$  is reducible in  $P[x]$ , and it has a root in  $P$ . Thus, every  $f(x) \in P[x]$  of odd degree has at least one root in  $P$ .

Theorem 4.3.6: If  $F$  is of characteristic zero and if  $a, b$  are algebraic over  $F$ , then there exists  $c \in F(a, b)$  such that  $F(a, b) = F(c)$  [3].

Proof: Let  $f(x), g(x) \in F[x]$  both be irreducible and let  $f(a) = 0, g(b) = 0$  where  $a, b \notin F$ . This implies that there exists an extension field of  $F$  in which  $f(x)$  and  $g(x)$  can be factored completely. Let  $a = a_1, a_2, \dots, a_n$  be roots of  $f(x)$  and  $b = b_1, b_2, \dots, b_n$  be roots of  $g(x)$ . Since characteristic of  $F$  is zero, the roots of  $f(x)$  and  $g(x)$  are all distinct. Since, we have finitely many distinct roots for  $f(x)$  and  $g(x)$ , so for  $k \neq 1$  we must have  $b_k \neq b_1$ .

This implies that the equation  $a_i + xb_k = a_1 + xb_1$  has at most one root  $x$  in  $F(a,b)$  for every  $i$  and every  $k \neq 1$ . Let  $\gamma \in F$  be different from the roots of each equation

$a_i + xb_k = a_1 + xb_1$ . This gives us an equation  $a_i + \gamma b_k \neq a_1 + \gamma b_1$

for every  $i$  and every  $k \neq 1$ . Let  $c = a_1 + \gamma b_1 = a + \gamma b$ , then we have  $c \in F(a,b)$ . To prove  $F(a,b) = F(c)$ , we still need to show that  $F(a,b) \subseteq F(c)$ .

Let's take  $c = a + \gamma b$  and solve it for  $a$ . This gives us  $a = c - \gamma b$ . We have  $g(b) = 0$  and  $f(a) = f(c - \gamma b) = 0$  with coefficients of  $f(x)$  in  $F(c)$ . Since  $c - \gamma b_k \neq a_i$  for  $k \neq 1$  and  $i = 1, \dots, n$ , the polynomials  $g(x)$  and  $f(c - \gamma x)$  have only the root  $b$  in common. This implies that  $f(c - \gamma b_k) \neq 0$  for  $k \neq 1$ . Moreover, polynomials  $g(x)$  and  $f(c - \gamma x)$  have only one linear factor  $x - b$  in common, because  $b$  is a simple root of  $g(x)$ . So we need to show that  $\gcd(f(c - \gamma x), g(x)) = x - b$ .

Suppose that  $\gcd(f(c - \gamma), g(x))$  has a factor other than  $x - b$ . Recall that  $g(b_j) = 0$  for  $b_j \neq b$ . This implies that  $f(c - \gamma b_j) \neq 0$  since  $c - \gamma b_j$  for  $j \neq 1$  avoids all roots  $a_i$  of  $f(x)$ . Thus,  $x - b_j$  with  $j \neq 1$  does not divide the gcd. Also  $(x - b)^2$  does not divide  $g(x)$  since  $b = b_1, b_2, \dots, b_n$  are all distinct roots. This implies that  $(x - b)^2$  does not divide the gcd. Thus,  $\gcd(f(c - \gamma), g(x)) = x - b$  over some extension of  $F$ . Since  $\deg(x - b) = 1$  and  $\gcd(f(c - \gamma), g(x)) \in F(c)[x]$ , we have  $(x - b) \in F(c)[x]$ . This implies that  $b \in F(c)$ . So we have  $\gamma \in F$ ,  $c \in F(c)$ , and  $b \in F(c)$ . Since  $a = c - \gamma b$ , we conclude that  $a \in F(c)$ . Thus,  $a, b \in F(c)$  implies that  $F(a, b) \subseteq F(c)$ . Finally,  $F(c) \subseteq F(a, b)$  and  $F(a, b) \subseteq F(c)$  implies that  $F(a, b) = F(c)$ .

#### 4.4 Fundamental Theorem of Algebra

Theorem 4.4.1: If, in an ordered field  $K$ , every positive element possesses a square root and every polynomial of odd degree has at least one root, then the field obtained by adjoining  $i$ ,  $K(i)$ , is algebraically closed[5].

Proof: Let  $K$  be an ordered field and every  $a > 0 \in K$  possess a square root. Assume that every  $f_i(x) \in K[x]$  of odd degree has at least one root in  $K$ .

We need to show that  $K(i)$  is algebraically closed.

Let  $a \in K$ , then  $\sqrt{a} \in K(i) \forall a \in K$ . By Theorem 4.3.1 any  $f(x) \in K[x]$  with  $\deg f(x) = 2$  is solvable in  $K(i)$ . In order to show algebraic closure of  $K(i)$ , it suffices to show that every  $f(x) \in K[x]$ ,  $f(x)$  irreducible, has a root in  $K(i)$ .

Let  $f(x) \in K[x]$  be a polynomial with no double roots and  $\deg f(x) = n$  such that  $n = 2^m \cdot q$  where  $q$  is odd. This implies that  $f(x) = a_n x^n + \dots + a_1 x + a_0, a_i \in K[x]$ .

By induction on  $m$  we can assume that every  $f$  in  $K[x]$  whose degree is divisible by  $2^{m-1}$  but not by  $2^m$  has a root in  $K(i)$ . So if  $m=1$ , then  $\deg f(x) = q$ . Now,  $q$  is odd and, by hypothesis, there exists a root of  $f(x) \in K$ , which implies that there exists root of  $f(x) \in K(i)$ .

Now, suppose every polynomial  $f(x)$  of degree  $2^{m-1} \cdot q^1$  where  $q^1$  is odd has a root in  $K(i)$ . Let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be the roots of  $f(x)$  in an extension of  $K$ . Choose  $c \in K$  such that  $\alpha_j \alpha_k + c(\alpha_j + \alpha_k) = d_{jk}$  are all different expressions for  $1 \leq j < k \leq n$  by reasoning similar to that given in

Theorem 4.3.6. Choosing two  $\alpha$ 's out of  $n$   $\alpha$ 's gives us  $\binom{n}{2}$

different expressions for  $d_{jk}$ . But when  $n = 2^m \cdot q$ ,  $\frac{n(n-1)}{2} =$

$$= \frac{2^m q (2^m q - 1)}{2} = 2^{m-1} q (2^m q - 1). \text{ This implies that } 2^{m-1} \text{ divides}$$

$$\frac{n(n-1)}{2} \text{ but } 2^m \nmid \frac{n(n-1)}{2}. \text{ Consider the polynomial}$$

$$p(x) = \prod_{jk} (x - d_{jk}) \text{ of degree } \frac{n(n-1)}{2}. \text{ As shown above } 2^{m-1}$$

divides  $p(x)$ , but  $2^m \nmid p(x)$ . Therefore, by induction

hypothesis there exists at least one root  $d_{jk} \in K(i)$ .

For ease in notation suppose  $d_{12} = \alpha_1 \alpha_2 + c(\alpha_1 + \alpha_2) \in K(i)$

be one of the expressions with  $\alpha_1, \alpha_2$  roots of  $f(x)$ . By

Theorem 4.3.6  $K(\alpha_1 \alpha_2, \alpha_1 + \alpha_2) = K(\alpha_1 \alpha_2 + c(\alpha_1 + \alpha_2)) \subseteq K(i)$ .

Thus,  $\alpha_1 + \alpha_2 \in K(i)$  implies that  $(\alpha_1 + \alpha_2)^2 \in K(i)$ . But since

$$\alpha_1 \alpha_2 \in K(i) \text{ and } (\alpha_1 + \alpha_2)^2 = \alpha_1^2 + 2\alpha_1 \alpha_2 + \alpha_2^2, \quad \alpha_1^2 + \alpha_2^2 \in K(i).$$

Now, consider  $(\alpha_1 - \alpha_2)^2$ ,  $(\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1 \alpha_2 + \alpha_2^2 =$

$$= \alpha_1^2 + \alpha_2^2 - 2\alpha_1 \alpha_2. \text{ But } \alpha_1^2 + \alpha_2^2 \in K(i) \text{ and } \alpha_1 \alpha_2 \in K(i) \text{ implies}$$

that  $(\alpha_1 - \alpha_2)^2 \in K(i)$  and consequently by Theorem 4.3.2

$\alpha_1 - \alpha_2 \in K(i)$ . So we have  $\alpha_1 + \alpha_2 \in K(i)$  and  $\alpha_1 - \alpha_2 \in K(i)$  which

implies that  $\alpha_1 + \alpha_2 + \alpha_1 - \alpha_2 = 2\alpha_1 \in K(i)$  and  $\alpha_1 \in K(i)$ . Since

$\alpha_1 \in K(i)$ ;  $-\alpha_1$  is also in  $K(i)$ . Thus,  $(\alpha_1 + \alpha_2) + (-\alpha_1) = \alpha_2$ , which implies that  $\alpha_2 \in K(i)$  and consequently all roots of  $f(x)$  are in  $K(i)$ . Hence,  $K(i)$  is algebraically closed.

#### 4.5 Summary

The proof of the FTA without the use of Galois Theory requires a solid background in Abstract Algebra. The argument in the proof in this chapter goes as follows: pick an arbitrary function  $f(x) \in K[x]$  where  $f(x)$  is irreducible, and show that all the roots of  $f(x)$  are in  $K(i)$ .



CHAPTER FIVE  
GALOIS THEORY PROOF OF THE  
FUNDAMENTAL THEOREM  
OF ALGEBRA

5.1 Introduction

The Galois Theory proof of the FTA requires a strong background in Group Theory and Galois Theory. Section 5.2 provides the reader with definitions needed to prove the Theorem in this chapter. Then we provide statements of theorems and a lemma used to prove the FTA using Galois Theory approach. Finally, section 5.4 presents the proof of the Theorem.

5.2 Definitions and Notation

5.2.1 Definition

If  $\alpha$  is a root of  $f(x)$ , then  $\alpha$  has multiplicity  $m \geq 1$  if  $f(x) = (x - \alpha)^m g(x)$  where  $g(\alpha) \neq 0$ . If  $m = 1$ , then  $\alpha$  is a simple root otherwise it is a multiple root.

5.2.2 Definition

A Galois extension of  $F$  is a finite separable splitting field over  $F$ .

### 5.2.3 Definition

Let  $G$  be a finite group with  $|G| = p^m \alpha$ , with  $p$  being a prime and with  $(p, \alpha) = 1$ . Then a  $p$ -Sylow subgroup is a subgroup of order  $p^m$ .

### 5.2.4 Definition

Let  $K$  be a finite extension of  $F$  and  $\alpha \in K$ . Then  $\alpha$  is separable over  $F$  if  $\alpha$  is a simple root of  $\text{irr}(\alpha, F)$ .  $K$  is a separable extension if every  $\alpha \in K$  is separable over  $F$ .

### 5.2.5 Definition

$F'$  is a splitting field for  $f(x)$  over  $F$  if  $F'$  is the smallest extension field of  $F$  in which  $f(x)$  splits completely.

### 5.2.6 Definition

If  $p$  is a prime, then a  $p$ -group is a group  $G$  where every element has order a power of  $p$ . If  $G$  is finite, this implies that  $|G| = p^n$  for some  $n$ .

### 5.2.7 Definition

Let  $K$  be a Galois extension of  $F$ . Then the group of automorphisms of  $K$  that fix  $F$  is called the Galois group of  $K$  over  $F$ , denoted by  $\text{Gal}(K/F)$ . If  $H$  is a subgroup of

$Gal(K/F)$ , we let  $K^H$  denote the elements of  $K$  fixed by  $H$ .

#### 5.2.8 Notation

$irr(\alpha, F)$  will denote an irreducible polynomial with coefficients in  $F$  and root  $\alpha$ .

### 5.3 Theorems

Theorem 5.3.1 (Fundamental Theorem of Galois Theory):

Let  $K$  be Galois extension of  $F$  with Galois group  $G = Gal(K/F)$ . For each intermediate field  $E$  let  $\tau(E)$  be the subgroup of  $G$  fixing  $E$ . Then:

- i)  $\tau$  is a bijection between intermediate fields containing  $F$  and subgroups of  $G$ .
- ii)  $E$  is Galois over  $F$  if and only if  $\tau(E) \triangleleft G$  where  $\tau(E)$  is normal in  $G$ .
- iii)  $|G| = |K:F|$ .
- iv)  $|E:F| = |G:\tau(E)|$ . That is, the degree of an intermediate field over the ground field is the index of the corresponding subgroup in the Galois group[6].

Theorem 5.3.2 (Sylow Theorem): Let  $G$  be a finite group of order  $p^m \alpha$  with  $p$  a prime and with  $(p, \alpha) = 1$ , then  $G$  has a  $p$ -Sylow subgroup [6].

#### 5.4 Lemma

Lemma 5.4.1: If  $G$  is a finite  $p$ -group of order  $p^n$ , then  $G$  has a subgroup of order  $p^{n-1}$  and hence of index  $p$  [6].

#### 5.5 Fundamental Theorem of Algebra

Theorem 5.5.1: The complex number field  $C$  is algebraically closed; i.e., any non-constant complex polynomial has a root in  $C$  [6].

Proof: Let  $f(x) \in C[x]$  and  $f(x)$  be non-constant complex polynomial. There exists splitting field  $K$  for  $f(x)$  over  $C$ . Since  $K$  is a finite extension of  $C$  and  $C$  is a finite extension of  $R$ ,  $K$  must be a finite extension of  $R$ . So,  $K$  is a finite, separable (characteristic zero) splitting field over  $C$  and, by the Definition 5.2.2, it is a Galois extension of  $R$ . In order to prove the FTA, we will show that any nontrivial Galois extension of  $C$  must be  $C$  itself.

For the  $K$  above, any finite extension of  $R$  with  $|K:R| = 2^m q$  where  $(2, q) = 1$  and  $K \neq R$ . Suppose  $m = 0$ , then  $|K:R| = q$ . This implies that  $K$  is an odd-degree extension of  $R$ . By Theorem 4.3.6  $K$  is a simple extension and therefore  $K = R(\alpha)$  where  $\text{irr}(\alpha, R)$  is of odd degree. However, by Theorem 4.3.3 odd-degree real polynomials always have a real root. Thus,  $\text{irr}(\alpha, R)$  is of degree one, since  $\text{irr}(\alpha, R)$  is irreducible having a real root. But this implies that  $\alpha \in R$  and  $K = R$ , which is a contradiction. Therefore, if  $K$  is a nontrivial extension of  $R$  with  $|K:R| = 2^m q$  where  $(2, q) = 1$ , then  $m > 0$ .

Now suppose that  $K$  is a  $2^{\text{nd}}$  degree extension of  $C$ , which means that  $m = 1$  and  $q = 1$ . By Theorem 4.3.6 this implies that  $K = C(\alpha)$  where  $\deg \text{irr}(\alpha, C) = 2$ . However, by Theorem 4.3.1 complex quadratic polynomials always have roots in  $C$ , which implies that we have  $\deg \text{irr}(\alpha, C) = 1$ . But this is a contradiction. Therefore,  $C$  has no two degree extensions.

Now let  $K$  be a Galois extension of  $C$ . Since  $C$  is finite extension over  $R$ ,  $K$  is also Galois extension over  $R$ . Suppose  $|K:R| = 2^m q$  with  $(2, q) = 1$  and  $m > 1$ . Let

$G = \text{Gal}(K/R)$  be the Galois group. This implies that  $|G| = |K:R| = 2^m q$  with  $(2, q) = 1$  and  $m > 1$ . Since 2 is a prime number and  $(2, q) = 1$ , by Lemma 5.4.1  $G$  has a 2-Sylow subgroup of order  $2^m$  and index  $q$ . By Theorem 5.3.1(iv) there exists an intermediate field  $E$  with  $|K:E| = 2^m$  and  $|E:R| = q$ , but then  $E$  is an odd-degree finite extension of  $R$ . From the argument above this means that  $q = 1$  and hence  $E = R$ . Therefore,  $|K:R| = 2^m$  and  $|G| = 2^m$ . Since  $|K:R| = 2^m$ , we must have  $|K:C| = 2^{m-1}$ .

Now suppose  $G_1 = \text{Gal}(K/C)$ , then  $|G_1| = 2^{m-1}$ . By the definition 5.2.6  $G_1$  is a 2-group. Moreover,  $G_1$  is either trivial or a nontrivial 2-group. Suppose that  $G_1$  is nontrivial 2-group, then by the Lemma 5.4.1 there exists a subgroup of order  $2^{m-2}$  and index 2. Then by the Theorem 5.3.1 this implies that there exists an intermediate field  $E$  of degree two over  $C$ . However, we showed that  $C$  has no degree two extensions. So then  $G_1$  must be a trivial 2-group and  $|G_1| = 1$ . Hence,  $|K:C| = 1$  and  $K = C$ .

## 5.6 Summary

The Galois Theory proof of the FTA uses many facts stated in this chapter as well as in Chapter Four. The argument of this proof goes as follows. First, pick an arbitrary non-constant function  $f(x) \in C[x]$ . Then consider an algebraic extension of  $C$  and show that any such nontrivial extension of  $C$  must be  $C$  itself.

## CHAPTER SIX

### SIMILARITIES AND DIFFERENCES

#### 6.1 Introduction

Among the three proofs of the FTA, we find some similarities and differences. It is interesting that using different mathematical tools—Complex Analysis, non-Galois Theory Algebra, and Galois Theory—we can prove the same concept. Section 6.2 will present will present similarities and differences of those proofs.

#### 6.2 Similarities and Differences

Comparing the three proofs, we find that the Galois Theory proof and the algebraic proof have some similarities. In both of these proofs we picked a polynomial  $f(x)$  in a field, and then studied the proper extension of the field associated with the roots of  $f(x)$ . Even though Theorems 4.4.1 and 5.4.1 have similar approaches to prove the Fundamental Theorem of Algebra, they utilize different tools to prove it.

The three proofs also have some differences. The Complex analysis proof of the Fundamental Theorem of Algebra is different from the other two. The complex



analysis proof is done by contradiction. In this proof, we picked a non-constant analytic function in the complex plane, and showed that the assumption was false.

## REFERENCES

- [1] [http://www-groups.dcs.stand.ac.uk/~history/  
HistTopics/Fund\\_theorem\\_of\\_algebra.html](http://www-groups.dcs.stand.ac.uk/~history/HistTopics/Fund_theorem_of_algebra.html)
- [2] [http://physics.rug.ac.be/fysica/Geschiedenis/  
HistTopics/Fund\\_theorem\\_of\\_algebra.html](http://physics.rug.ac.be/fysica/Geschiedenis/HistTopics/Fund_theorem_of_algebra.html)
- [3] Herstein, I. N. Topics in Algebra, 2<sup>nd</sup> edition, John Wiley & Sons, New York, 1974.
- [4] Brown, James W. & Churchill Ruel V., Complex Variables and Applications, 6<sup>th</sup> edition, McGraw-Hill, Inc., New York, 1996.
- [5] Waerden, Van Der, Algebra, vol. 1, New York, 1970.
- [6] Fine, Benjamin & Rosenberger, Gerhard The Fundamental Theorem of Algebra, Springer, New York, 1997.