INVESTIGATION OF THE SOLUBILITY BY RADICALS OF A SELECTED TRINOMIAL OF HIGHER ORDER (DEGREE 5≤n ≤ 7) POLYNOMIALS USING

GALOIS THEORY

BY

GAMBO JEREMIAH GYAM

NSU/NAS/MSC/MAS/012/15/16

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, NASARAWA STATE UNIVERSITY KEFFI, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS DEGREE IN MATHEMATICS

DEPARTMENT OF MATHEMATICS, FACULTY OF NATURAL AND APPLIED SCIENCES, NASARAWA STATE UNIVERSITY KEFFI, NIGERIA

JUNE, 2017.

DECLARATION

I, Gambo Jeremiah Gyam, hereby declare that this dissertation titled “Generalization Through the Investigation of the Solubility by Radicals of a Special Trinomial of Higher Order (Degree n $\geq$5) Polynomials -Using Galois Theory” has been carried out by me. The topic has not been presented for the award of M. sc degree in any institution. All sources of information are acknowledged by means of reference.

Gambo Jeremiah Gyam **DATE**

NAS/NSU/M.Sc/012/15/16

CERTIFICATION

This dissertation titled "Generalization Through the Investigation of the Solubility by Radicals of a Special Trinomial of Higher Order (Degree n ≥5) Polynomials -Using Galois Theory" has been read and approved, having met the requirements governing the award of the M. sc degree of science in Mathematics department, faculty of Natural and Applied Science, Nasarawa State University Keffi. And is approved for its contribution to knowledge and literary presentation.

Dr. H.K. Oduwole **Date**
Chairman, Supervisory Committee

Dr. Abdullahi M. Ya'u **Date**
(Member, Supervisory Committee)

Prof. M.Y. Balla **Date**
Head of Department

Date
(Internal Examiner)

Prof. B.S. Jatau **Date**
Dean of Faculty

External Examiner **Date**

Prof. S.A.S. Aruwa **Date**
(Dean, of Postgraduate Studies)

ACKNOWLEDGEMENT

I remain grateful in my wildest imagination, first and foremost to the creator of heaven and earth (The Lord God Almighty) for given the insight, strength and ability to embark on this rewarding task. May His name be praised. Amen.

I remain indebted to my versatile supervisor, Dr. H. K. Oduwole who within his tight schedule gave me his all to ensure the success of this work. I have learnt so much about research work; Internet search, power point, equation editor and referencing from you Sir. It is my earnest prayer that your promotion to professorship is on the way.

To my Head of Department Professor M . Y. Balla. I am so grateful with your fatherly advise. My appreciation also goes to all the lecturers in Mathematics Department specially Dr. A.B Gimba whose resource materials were instrumental to this research, Dr. M. Ya'u may the Almighty God bless and reward all of you.

My parents Mr. and Mrs. Gambo Gyam were my back bone. My siblings; Mr. James G. Gyam, Miss Rose Gyam, Miss Esther G. Gyam , Most especially Mrs. Mary Danladi who in there helped state saw the need to offer moral, spiritual, and financial support. I do apreciate it, and I'm sure The Lord will reward your labour of love.

My wife, even in her weakest disposition of the availability of resources, deem it fit to carry the cross along. My children Praise and Prudence Jeremiah Gyam took it to heart bear with me at those trying times. I sincerely appreciated your labour of love.

This acknowledgement will not be complete without mentioning my Gallant Uncle and his wife (Mr. and Mrs. Hassan Makama). Who have immensely contributed in the rebuild of my broken walls. Uncle you made me picked up the pieces of my life and start all over again. Your timely support will never be forgotten by me and the one who gave you the strength to do that.

My Principal, Mr. D. Yamusa who understand my plight and always reasoned out with me, and the entire staff of G.S.S F/Ayu most especially Mr. Emmanuel Audu who always put smiles in my face, his words have encouraged me. Mr. Lagos (Yahaya Audu), Mr. Sesugh Iyornumbe, Mr. Joshua etc. And from F/Ayu village and environs; Mr. Akos, Oga Danmasani, David, Mr. Pele, Mr. Umar and Mr. Umar (Babban yaya). I sincerely appreciate your support in one way or the other.

My former Pastor, Pastor Bitrus Ninyo who became one of the pillars of my study, I cant forget you sir.To my friends in Kaduna, Mr. Bobby Dangana, Barriscology (Audu Ibrahim Nok),Bro Bola Amoko, Sis Jane L. and Pastor Moses Omale etc. I make bold here to say that I appreciated all your contributions to me. May the good Lord reward you abundantly. Mrs. Onyema Adiline who devoted all her time for the typing and correction of this work. The Lord will bless you richly. Amen.

DEDICATION

With all humility of heart and purpose, I dedicated this research work to God Almighty, to my parents Mr. and Mrs. Gambo Gyam, to my siblings and to my nucleated family (my wife and my two children: Praise and Prudence).

TABLE OF CONTENTS

PAGE

Title Page - - - - - - - - - i

Certification - - - - - - - - - ii

Dedication - - - - - - - - - iii

Acknowledge - - - - - - - - - iv

Table of Contents - - - - - - - - vi

Abstract - - - - - - - - - ix

CHAPTER ONE

INTRODUCTION

1.1. Background of the Study - - - - - - 1

1.2 Statement of the Problem (Motivation) - - - - 2

1.3 Aims and Objectives - - - - - - - 2

1.4 Significance of the Study - - - - - - 3

1.5 Scope and Limitations - - - - - - 3

1.6 Limitations - - - - - - - - - 4

1.7 Definition of Terms and Comment - - - - - 4

CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.1 Groups- - - - - - - - - 7

2.1.1 Symmetric Groups- -- - - - - - - 8

2.1.2 Element 9

2.1.3 Cycle 9

2.1.4 Transposition 10

2.1.5 Conjugacy Classes 11

2.2 Relationship between Roots of Polynomial and Symmetric Group 11

2.3 The Radicals 14

2.3.1 Cubic Functions 14

2.3.2 Quartic Functions 17

2.3.3 Quintic Functions 18

2.3.4 Special Solvable Cases 19

2.4 Solvable Higher Polynomial 21

2.4.1 Principal Quintic Form 23

2.4.2 Bring-Jerrard Normal Form 23

2.5 Sextic Equation 24

2.5.1 Solvable Sextic 24

2.6 Septic Equation 25

2.6.1 Solvable Septic 25

2.7 Field Extension 26

2.7.1 Definition of Field Extension 29

2.8 Splitting Field 29

2.8.1 Splitting Field and the root of polynomial 29

2.9 Fundamental Theorem of Galois Theory 30

2.10 Polynomial 31

2.10.1 Factoring Polynomial - - - - - - - - 32

CHAPTER THREE

MATERIALS AND METHODS

3.1 Galois Theory - - - - - - - - - 35

3.2 Indentifying the irreducible Polynomial - - - - 35

3.3 Galois Group - - - - - - - - - 36

3.4 Trinomial Polynomial of Solvable Quintic - - - - 37

3.5 Fixed Field of the Frobenius Subgroup - - - - 45

3.5.1 Resolvent of Equation- - - - - - - - 47

3.5.2 Resolvent Program - - - - - - 47

3.6 Trinomial Polynomial of Solvable Sextic - - -- - 48

3.7 Trinomial Polynomial of Solvable Septic - - - - 50

CHAPTER FOUR

RESULTS

4.1 Consideration of practical Problems - - - - - 51

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 Discussion - - - - - - - - - 62

5.1.1 Generalization - - - - - - - - 63

5.2 Conclusion - - - - - - - - 65

5.3 Contribution to knowledge- - - - - - - 66

5.4 Recommendations - - - - - - - 66

References - - - - - - - 67

ABSTRACT

This dissertation extends the results of the work of Galois and his contribution to the development of modern algebra. The fact is that polynomials of higher degree ($n \geq 5$) are not solvable by radicals. However, very few at that were later discovered to be solvable by radicals. In particular, we specifically identified some special polynomials which are irreducible but can be solve by radicals. These polynomials are in trinomial form ($x^5 + ax + b$).Then using the quintic, sextic, and septic polynomial as case study, we finally deduced that such type of a trinomial polynomial can be generalized and a theorem was then put forward to support our argument.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Mathematicians of the early second millennium concentrated their research explicitly on the formula for roots of polynomial that is equation having one or more unknown. Their work and solutions for linear and quadratic equation in a single unknown was well understood in antiquity for instance ax^2 + bx+ c using quadratic formula. However, it was difficult to provide solutions to real cubic and quartic equation (Postnikov, 2004).

Many results were gotten before and after the 16th century, like the construction of radicals of finding the roots of a cubic and a quartic polynomials. Until the 19th century when the French Mathematician by name EVARISTE GALOIS came. His work gave further opportunity for the analysis of higher polynomials that is a polynomial of degree ($n \geq 5$). He lived just a very short life of about 20years by dying on 21st May,1832AD.

Though at the beginning, his papers were not understood. Until his death that Joseph Liu-ville appreciated his writings. Today Abel and Galois led to a satisfactory framework for fully understanding of the problem and the realization that the general polynomial of degree at least 5 could not always be solved by radicals. He laid the foundation of Galois Theory in which he worked on finite field for the first time and expresses himself in a more spectacular way (Artin, 1998).

1.2 Statement of the Problem (Motivation)

What exactly was Galois looking for in his research and discoveries? It is the solvability of polynomials. That is when you have a polynomial P (say) of which the coefficients are in the field say F. Then the polynomial p(x)=0 is having no solution. Invariantly we can extend the field F into a field L. There by saying that if $\propto \in L$ then p($\propto$)=0.

Now this field we speak of has a great importance to not only mathematicians but to the entire science field. Felicia A.N says "Every sciences use the field of real numbers and most uses the field of complex numbers. Electrical engineers would not have a job if complex numbers did not exist."(Noelle, 2010).

For Galois to achieve the result he looked for, that is to prove that an n^th degree polynomial (for n $\geq$ 5) cannot be solved by radicals. He began to think of how the field can be extended.

However David S. Dummit and Emma Lehmer having study the work of Galois later found out that some special polynomial of degree (n $\geq$ 5) are soluble by radicals (Dummit & Foote,2014). Their result which is an off shoot of Galois Work is what we shall see, investigate and critically analyzed to see whether (i) Can some kind of generalization be done on the solubility of higher polynomial by radicals?(ii) Can a generalized theorem and proposition be constructed by such a special higher polynomial solvable by radicals ($x^n + ax + b$) where n ≥ 5 and a, b are integers.

1.3 Aim and Objectives

i. **Aim:** The aim of this study is to identify special polynomials of the form ($x^5 + ax + b$, $x^6 + ax + b$, $x^7 + ax + b$) and prove that though they are irreducible, they are solvable by radicals.

ii. **Objectives:** The objectives of this study is as follows:

a. To apply radicals in solving special trinomial polynomials of higher degree for n≥5 and observe the results to see whether such polynomials can be generalized or not, using the quintic, sextic and septic polynomial as case study.

b. To generalize the special trinomial polynomial of the form ($x^n + ax + b$) and put forward a theorem to prove such generalisation.

1.4 Significant of the Study

This study in its conciseness would help the mathematician in the field of abstract algebra to get familiarized with the modern concept of Galois Theory such as the field extension, splitting field, symmetric group of the root of the polynomials.

The harmonization and generalization both in theorem and formula for the special higher trinomial polynomial (of degree $5 \leq n \geq 7$) solvable by radicals would add value to the field of abstract algebra. Most especially for those who still believe that the radicals for solving general higher polynomial ($5 \leq n \geq 7$) can be gotten one day.

1.5 Scope and Limitations of the Study.

The scope of this study shall purely include all higher degree polynomial and we shall use the quintic, sextic, and septic polynomial as case study in order to draw our conclusion for our generalization. The quintic (polynomial of degree 5), the sextic (polynomial of degree 6), septic (polynomial of degree 7).

1.6 Limitations

Binary extension of Galois field which is used extensively in digital logic and circuiting, the operation of linear feed-back shift register (LFSR) on element are accomplished via bit vise operation such as x or and or logic, application within fields of cryptography and error correcting code. The use of Galois field to extensively in s-box implementation (bit scramblers), strong random number generators and algebraic are cumber some and may be difficult complex and beyond our consideration for analysis in this study.

1.7 Definition Terms and Comments

In our study, it is necessary we defined some terms for better understanding.

i. Modern Algebra

In algebra, which is a broad division of mathematics, abstract algebra (occasionally called the modern algebra) is the study of algebra structures. Algebraic structure includes; groups, rings, fields, modules, vector spaces, lattice and algebras.

Modern algebra is abstract algebra, which is a branch of mathematics concern with the general algebraic structures of various sets (such as real numbers, complex numbers, matrices and vector space), rather than rules and procedures for manipulating their individual element*(E-net, 2012 Wikipedia, JSTOR)*.

ii. Radicals

We defined radicals as base or roots from a word. It is a quantity forming or expressed as a root of another. A radical is any mathematical expression that has a square root, cube root and so on. They use the basic operations such as addition, subtraction, multiplication and division (Wareden, 1948).

Note that: Given $\sqrt{x}$ is a mathematical expression, then √ is called the **radicals** while the x is called the **radicands.**

iii. Monic Polynomial:

When the coefficient of the highest degree (power) of variable of a polynomial is equal to one(unity). Then such a polynomial is termed as monic polynomial. For example, the polynomial $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$. The highest degree of the variable x^5 is one. Hence the polynomial is a monic polynomial(Martin, 1999).

iv. Solubility and Solvability:

Solvable groups are groups having normal series such that each normal factor is abelian. We have special cases of solvable finite groups, which are such groups whose composition indices are all prime numbers. "*These solvable groups are sometimes called soluble groups"(E-net,2012 Wikipedia, JSTOR).*

According to Doerk and Hawkes (1992).The term solvable is derived from the type of group relationship to Galois theorem, namely that the symmetric group S_n is unsolvable for n ≥ 5 while it is solvable for n=1,2,3, and 4. Hence the result shows that the polynomial equation of degree n $\geq$5 are in general not soluble using radicals.(Doerk and Hawkes, 1992).

In technical language of Mathematics, "soluble" is interchangeable with "solvable" the former is British usage while the later is American *(E-net,2012 Wikipedia, JSTOR).*

v. Symmetric Groups (S_n)

S_n in abstract algebra and on a finite set with symbol n, which is the group whose permutations operation of its element can be performed on n distinct symbols. The order (number of elements) of the symmetric group S_n is n!.

Symmetric group is important to diverse of mathematics such as Galois Theory, Invariant theory, the representation of Lie Group and combinatories. Cayley's theorem states that every group G is isomorphic to a subgroup of the symmetric group on G. It is the group on a finite set whose elements are all bijective functions from X to X and whose group operation is that of functional composition. For finite sets, "permutations" and "bijective functions" refer to the same operations, namely arrangements. The symmetric group of degree n is the symmetric group on the set X={1,2,…,n} (Cameroon,1999).

vi. Trinomial Polynomial:

These are polynomial in three forms irrespective of the degree of the polynomial. Such as ($x^n + ax + b$) especially within the cycle of our discussion (Mohammed & Daniel,2014).

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction: The Concept of Groups and Rings.

Concept of Groups.

In Mathematics, a group is an algebraic structure consisting of elements equipped with operation combining any two elements to form the third element. The operation satisfied four (4) conditions which are called the group axioms, namely

(i) Closure. That is ∀ a, b, then a + b exist

(ii) Associativity, that is ∀ a, b and c $\in G$; (a + b) + c= a+(b + c)

(iii) Identity. By identity we mean a*e =e*a = a, where e is the identity, and a∈ G

(iv) Existence of Inverse. If a^{-1} is the inverse of a, then a* a^{-1} =e. * is the additional operation.

Subgroups: Suppose G is a group and H is a subgroup of G, then if the elements of H are in G and they satisfy the axioms of a group, then H is said to be a group.

Lie Groups: These are symmetric groups used in the standard mode of particles in Physics and molecular chemistry.

Cyclic Groups: Is a group whose elements are powers of a particular element a.

Finite Groups: They are groups that have the finite number of element.

Galois group were developed to help solve polynomial equation by capturing their symmetric features, for examples $ax^2 + bx + c = 0$.

A **Field** is an integral domain in which every non zero element has an inverse. With this we can say that an integral domain is a commutative ring, with identity with non zero divisor. For example, the integers.

Note that: A skew field is a non commutative field.

Another definition of a field would be necessary at this point that a field is a set of two or more element with two binary operation; addition and multiplication, satisfying the following axioms.

i) Association of both addition and subtraction.

ii) Existence of identities for both addition and subtraction. (0,1)

iii) Existence of inverses

iv) Commutative of both addition and subtraction.

v) Distributives of both addition and subtraction.

Clearly, we can see that the set of integers is not a field, this is because the element 2 has no multiplicative inverse in Z. but Q, R and C are fields.(Fraleigh, 2006)

2.1.1 Symmetric Groups (S_n):

In our discussion in chapter one, we gave some definition of what a symmetric group is. Hence we shall discuss finite sets and their applications, elements, subgroup, conjugacy classes and their subgroups.

The symmetric groups denoted by Sym(x) or S_n , n is the order of the group.

Symmetric group of order n is abelian if and only if $n \leq 2$. When n=0 and n=1, they are both empty sets and singleton respectively. A symmetric group is trivial which is in agreement to 0! = 1! = 1. And for Alternating group, it equals the symmetric group instead of being the index two subgroups. Hence the group S_n is solvable if and only if n ≤ 4. This is the essential part of Abel-Ruffini theorem that shows that for every n > 4 there are polynomial of degree n which are not solvable by radicals, that is the solution cannot be express by performing a finite number of operations of addition, subtraction, multiplication, division and root extraction on the polynomials coefficients(Baker,2013).

Subgroups of symmetric groups are called permutation groups and are widely studied because their importance in understanding group action, homogenous spaces and automorphism group.

2.1.2 Elements:

Elements of the symmetric group on a set x are the permutations of x. Operations on symmetric group is of composite function, for example, suppose f= (13)(45) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$, g=(125)(34)= $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$. Applying f after g maps 1 first to 2 and then 2 to itself, 2 to 5 and then 4 ; 3 to 4 and then to 5 and so on. Composing f and g gives fg= f o g= (124)(35) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$.

2.1.3 Cycles:

This is length of the symmetric group say L=k.m **.** taken to the K-th power will decompose into K=Cycle of length m. For example (k=2, m=3)

$(12345)^2$= (135)(246). Is symmetric group a group? We can show this, if the elements from S_n

Obeys the axiom of a group. That is:

(1) The operators of function composition is closed in the set of permutation of a given set x.

(2) The function composition is always associative.

(3) The trivial bijection that assigns each element of x to itself serves as an identity for the group.

(4) Every bijection has an inverse function that undoes its action, and thus each element of asymmetric group does have an inverse which is a permutation too.

Thus the sign of permutation goes thus :

$$\text{Sign f}= \begin{Bmatrix} +1, if\ f\ is\ even \\ -1, if\ f\ is\ odd \end{Bmatrix}$$

2.1.4 Transpositions

A transposition is a permutation which exchanges two elements and keeps all others fixed; for example (1 3) is a transposition. Every permutation can be written as a product of transpositions; for instance, the permutation *g* from above can be written as *g* = (1 2)(2 5)(3 4). Since *g* can be written as a product of an odd number of transpositions, it is then called an odd permutation, whereas *f* is an even permutation.

The product of two even permutations is even, the product of two odd permutations is even, and all other products are odd.

The kernel of this homomorphism, i.e. the set of all even permutations, is called the **alternating group** A_n. It is a normal subgroup of S_n, and for $n \geq 2$ it has $n!/2$ elements.

The group S_n is the semidirect product of A_n and any subgroup generated by a single transposition.

2.1.5 Conjugacy Classes

The conjugacy classes of S_n correspond to the cycle structures of permutations; that is, two elements of S_n are conjugate in S_n if and only if they consist of the same number of disjoint cycles of the same lengths. For instance, in S_5, (1 2 3)(4 5) and (1 4 3)(2 5) are conjugate; (1 2 3)(4 5) and (1 2)(4 5) are not. A conjugating element of S_n can be constructed in "two line notation" by placing the "cycle notations" of the two conjugate permutations on top of one another. Continuing the previous example:

Which can be written as the product of cycles, namely: (2 4).

This permutation then relates (1 2 3)(4 5) and (1 4 3)(2 5) via conjugation, i.e.

$$(2\ \ 4)\circ(1\ \ 2\ \ 3)(4\ \ 5)\circ(2\ \ 4)=(1\ \ 4\ \ 3)(2\ \ 5).$$

It is clear that such a permutation is not unique (Cameron, 1999).

2.2 Relationship Between Roots of Polynomial and Symmetric Group

The n roots determine the polynomial, and when they are considered as independent variables, the coefficients of the polynomial are symmetric polynomial functions of the roots. The fundamental theorem of symmetric polynomials implies that a polynomial function f of the n roots can be expressed as (another) polynomial function of the coefficients of the polynomial determined by the roots if and only if f is given by a symmetric polynomial.

This yields the approach to solving polynomial equations by inverting this map, "breaking" the symmetry – given the coefficients of the polynomial (the elementary symmetric polynomials in the roots), how can one recover the roots? This leads to studying solutions of polynomials using the permutation group of the roots, originally in the form of Lagrange resolvents, later developed in Galois theory.

The symmetric groups on the empty set (S_0) and the singleton set (S_1) are trivial, which corresponds to 0! = 1! = 1. In this case the alternating group agrees with the symmetric group, rather than being an index 2 subgroup, and the sign map is trivial. In the case of S_0, its only member is the empty function.

The S_2 group consists of exactly two elements: the identity and the permutation swapping the two points. It is a cyclic group and is thus abelian. In Galois theory, this corresponds to the fact that the quadratic formula gives a direct solution to the general quadratic polynomial after extracting only a single root. In invariant theory, the representation theory of the symmetric group on two points is quite simple and is seen as writing a (y) function of two variables as a sum of its symmetric and anti-symmetric parts: Setting $f_s(x, y) = f(x, y) + f(y, x)$, and $f_a(x, y) = f(x, y) - f(y, x)$, one gets that $2\cdot f = f_s + f_a$. This process is known as symmetrization.

The symmetric group $\mathbf{S_3}$ can be defined as the first nonabelian symmetric group. This group is isomorphic to the dihedral group of order 6, the group of reflection and rotation symmetries of an equilateral triangle, since these symmetries permute the three vertices of the triangle. Cycles of length two correspond to reflections, and cycles of length three are rotations. In Galois theory, the sign map from S_3 to S_2 corresponds to the resolving quadratic for a cubic polynomial, as discovered by Gerolamo Cardano, while the A_3 kernel corresponds to the use of the discrete Fourier transform of order 3 in the solution, in the form of Lagrange resolvents.

The group S_4 is isomorphic to the group of proper rotations about opposite faces, opposite diagonals and opposite edges, 9, 8 and 6 permutations, of the cube. Beyond the group A_4, S_4 has a Klein four-group V as a proper normal subgroup, namely the even transpositions {(1), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}, with quotient S_3. In Galois theory, this map corresponds to the resolving cubic to a quartic polynomial, which allows the quartic to be solved by radicals, as established by Lodovico Ferrari. The Klein group can be understood in terms of the Lagrange resolvents of the quartic. The map from S_4 to S_3 also yields a 2-dimensional irreducible representation, which is an irreducible representation of a symmetric group of degree n of dimension below $n - 1$, which only occurs for $n = 4$.

S_5 is the first non-solvable symmetric group. Along with the special linear group SL(2, 5) and the icosahedra group $A_5 \times S_2$, S_5 is one of the three non-solvable groups of order 120, up to isomorphism. S_5 is the Galois group of the general quintic equation, and the fact that S_5 is not a solvable group translates into the non-existence of a general formula to solve quintic polynomials by radicals. There is an exotic inclusion map $S_5 \to S_6$ as a transitive subgroup; the obvious inclusion map $S_n \to S_{n+1}$ fixes a point and thus is not transitive. This yields the outer automorphism of S_6, discussed below, and corresponds to the resolvent sextic of a quintic.

Unlike all other symmetric groups, S_6 has an outer automorphism. Using the language of Galois theory, this can also be understood in terms of Lagrange resolvents. The resolvent of a quintic is of degree 6—this corresponds to an exotic inclusion map $S_5 \to S_6$ as a transitive subgroup (the obvious inclusion map $S_n \to S_{n+1}$ fixes a point and thus is not transitive) and, while this map does not make the general quintic solvable, it yields the exotic outer automorphism of S_6—see automorphisms of the symmetric and alternating groups for details.

Note that while A_6 and A_7 have an exceptional Schur multiplier (a triple cover) and that these extend to triple covers of S_6 and S_7, these do not correspond to exceptional Schur multipliers of the symmetric group.

A subgroup of a symmetric group is called a permutation group. (Cameron, 1999)

2.3 The Radicals

We are much familiar with the concept of linear and quadratic radicals or formulas (which is called The Quadratic Formula) used in solving problems relating to both linear and quadratic equations.

2.3.1 Cubic Functions

Solving Cubic functions can be done using Cardano's method, which transforms the general cubic equation into a depressed cubic without the x^2 term.

This method is believed to have originated from Scipione del Ferro, and was later adapted by Niccolò Tartaglia, and published in Cardano's 1545 paper.

The method is as follows.

We begin with the general form of a polynomial of degree three.

$$ax^3 + bx^2 + cx + d = 0$$

Since it is easier to work with a polynomial of leading coefficient one, we can divide a out of the entire equation.

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0$$

Substitute the following equation into (4)

$$x = y - \frac{b}{3a}$$

The polynomial becomes

$$\left(y - \frac{b}{3a}\right)^3 + \frac{b}{a}\left(y - \frac{b}{3a}\right)^2 + \frac{c}{a}\left(y - \frac{b}{3a}\right) + \frac{d}{a}$$

$$= y^3 + y\left(\frac{b^2}{3a^2} - \frac{b^2}{3a^2} + \frac{c}{a}\right) + \left(-\frac{b^3}{27a^3} + \frac{b^3}{27a^3} + \frac{cb}{3a^2} + \frac{d}{a}\right)$$

Thus we are reduced to the cubic polynomial of the form $y^3 + py + q = 0$

Where $p = \frac{b^2}{3a^2} - \frac{2b^2}{3a^2} + \frac{c}{a}, q = \frac{b^3}{27a^3} + \frac{b^3}{9a^3} - \frac{cb}{3a^2} + \frac{d}{9}$

Thus the general solution for the equation (4) are

$$x = -\frac{b}{3a} + \frac{wi}{3a}\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt{-\frac{q}{2} = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\right)$$

$let\ f(n) = x^3 + px + q$

We have the relations $y_1 + y_2 + y_3 = 0$

$y_1\, y_2 + y_2\, y_3 + y_3\, y_1 = p$

$y_1\, y_2\, y_3 = -q$

Observe that

$$(U + V)^3 - 3UV(U + V) - (U^3 + V^3) = 0$$

Equation (6) corresponds to equation (5) since we can let

$$(U + V) = y, 3UV = -P, U^3 + V^3 = -q$$

Thus we can solve for y

$$y = Wa\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt{-\frac{q}{2} = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\right)$$

Where $i \in \{1, 2, 3\}$ and wi is one of the 3rd roots of unity

Thus the general solutions for the equation (4) are

$$x = -\frac{b}{3a} + \frac{wi}{3a}\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt{-\frac{q}{2} = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\right)$$

$let\, f(n) = x^3 + px + q$

We have the relations $y_1 + y_2 + y_3 = 0$

$y_1\, y_2 + y_2\, y_3 + y_3\, y_1 = p$

$y_1\, y_2\, y_3 = -q$

2.3.2 Quartic Functions

Solving Quartic polynomials can be done using Ferrari's method, which transforms a quartic polynomial into a depressed quartic which has no x^3 term.

We begin with the general form of a quartic equation.

$x^4 + ax^3 + bx^2 + cx + d = 0$........ (2.7)

We can reduce all quartic polynomials to monic polynomials by dividing throughout by the leading coefficient, and replacing the coefficients of the other terms with a,b,c,d.

Substitute the following equation into (2.7)

$$x = y - \frac{a}{4}$$

to get a equation of the form

$$y^4 + py^2 + qy + r = o$$

We can add $2zy^2 + z^2$ to the above equation, to obtain

$y^4 + 2zy^2 + 2^2 = (2z - p)y^2 - qy + (z^2 - r)$

Since we want the left side to be a square as well, we can let the discriminant of the quadratic on the RHS be 0. Therefore,

$q^2 - 4(z^2 - r)(2z - p) = 0$

Rearranging the terms we get a cubic in z,

$8z^3 - 4(pz)^2 - 8rz + 4rp - q^2 = 0$

We can thus find the root of this equation, and solve for y by substituting that value into (1) to get a quadratic in y^2.

Solving the resultant quadratic in y^2 gives the roots of the depressed quartic, from which we can derive x.

2.3.3 Quintic Functions

We defined a quintic function as a polynomial for degree five (5). It is a function of the form $g(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$, where a, b, c, d, e and f are members of a field. A general quintic polynomials are insolvable by radicals. This proof makes use of group theory and Galois Theory, and is unlike Abel's 1819 paper. We will use the result below:

Theorem 2.1 A polynomial is solvable by radicals if and only if the Galois group of the splitting field of the polynomial f(x)∈F[x] is solvable.[1]

Let $y_1, y_2, \dots, y_5$ be independent transcendental elements over Q. Consider

$$\mathrm{F}(x) = (x - y_1) \dots (x - y_5) = x^5 - S_1x^4 + S_2x^2 + S_3x^2 + S_4x - S_5$$

By Vieta's formulas, we know that

$S_1 = y_1 + \cdots + y_{5,}$

$S_2 = y_1\, y_2 + \cdots + y_4\, y_5,$

$S_5 = y_1\, y_2 y_3 y_4 y_5$

are elementary symmetrical functions in yi .

Set $E = Q(\, y_1, y_2, \dots, y_5)$ and $F = Q(\, S_1, S_2, \dots, S_5)$. Then the polynomial f(x) in F[x] has the E as its splitting field. The proof of the insolvability of f(x) by radicals is as follows.

Suppose on the contrary that $G = G(K/F) = G_0$ is solvable for some polynomial of degree five p(x)∈F[x]

Consider the composition series of subgroups from $G = G(K/F) = G_0$ to G_r = (1):

$G = G_0 \Delta\, G_1 \Delta \dots . \Delta G_{r-1} \Delta G_r$

This corresponds to the extension fields of
$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r$

Each extension is cyclic and Galois.

We know that S_5 = Gal(E/F), the commutator group [S_5, S_5] = A_5 and that A_5 has no nontrivial normal subgroup. Indeed, the composition series of S_5 is as follows:

$S_5 \rhd A_5$

Thus Gal(E/F) is not solvable. Hence f(x) is not solvable by radicals by Theorem 1.1.

2.3.4 Special Solvable Cases

By the proof above, we know that it is impossible to solve all quintics by radicals, and thus no general solution can be found. However, there are few cases of quintics which are solvable by radicals.

Consider the general quintic polynomial

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

If a=0, then the quintic becomes a quartic polynomial, and is thus solvable by radicals using the aforementioned Ferrari's method.

By some Theorems and results we know that a polynomial is solvable if and only if its Galois group is solvable.

Consider the cyclotomic polynomial x^5-1=0.

This equation is solvable in radicals as its splitting field is generated by the 5th roots of unity, so the resultant Galois group is solvable.

The roots of this equation are simply the 5th roots of unity,

where k∈{0,1,-1,-2,2} .

These roots of unity can be expressed by radicals.

Similarly, all equations of the form $x^5 - m = 0$, where m is a constant, are solvable by radicals, since the roots are simply

$w_k = e^{2\pi ik/5}\sqrt[5]{m}$

Eisenstein's Irreducibility Criterion

For any polynomial of the form

$x^n + a_n - a_{n-1}x^{n-1} + \cdots + a_1x + 0_0, a_1$∈Z

If for some prime number p,

$a_{n-1}, \ldots, a_1 a_0$ are divisible by p,

a_0 is not divisible by p^2,(Lee & Zang, 2008)

2.4 Solvable Higher Polynomial

Solving higher degree polynomials have been mind tasking, challenging and fascinating. David Dummit in solving solvable quintic gives a powerful method that permits one to determine when is a quintic is solvable and to solve its roots(Dummits , 2006)

Emma Lehmer's quintics are quintics that are known to have Z_5 as their galois group and one might hope that expressing the roots in terms of radicals would give simple expression from which Emma Lehmer's polynomial could be recovered. But we shall see the expression of the roots in terms of radicals is much more complicated than expectd.

Now, suppose we consider the simple equation $f(x) = x^5 + ax + p$ and show that for a fixed non zero integer p, the polynomial is solvable by radicals for only infinite many $a \epsilon$ Z .

David Dummit in summarizing his work (method) enumerated some steps to be followed, such as (a) The sextic resolvent is constructed which has a rational roots if and only if the general reduces quintics $f(x)= x^5 + px^3 + qx^2 + rx + s \epsilon Q[x]$ is solvable. (b) The Langranges resolvent r_1 of the roots of f are defined; (c) The fifth – power of the resolvent are expressed as linear combinations of roots of unity. Let x_1, x_2, x_3, x_4, and x_5 be the roots of the general quintic polynomial $x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5$ where s_i are the elementary symmetric functions in the roots.

We assume that $s_1, s_2, s_3, s_4, s_5 \epsilon Q$. Let $\theta = x_1^2x_2x^5 + x_1^2x_3x_4 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_5 + x_3^2x_2x_4 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_4 + x_5^2x_2x_3$.

The stabilizer of θin s_5 is precisely F_{20} , the Frobenius group of order 20, with generators (12345) and (2354), since S_3 , generated by (12) and (123), is a complement of F_{20} in S_5 (that is every element of S_5 can be writing uniquely as an element of S_3 times an element of F_{20}).It follows that θ and its conjugates satisfy a polynomial g(x) of degree six over Q.

By making a translation, we may assume our quintic is f(x) = $x^5 + px^3 + qx^2 + rx + s$. Hence Dammit put forward a theorem. The theorem saying that the irreducible quintic f(x) = $x^5 + px^3 + qx^2 + rx + s \in$ Q[x] is solvable by radicals, if and only if the polynomial g(x) has a rational roots. If this is the case the sextics g(x) factors into product of a linear polynomial and an irreducible quintic (proof may not be given)(Checa, 2004)

You may solve the sextic equation using the supplementary equation C_0=0 and prove that the roots are related.

Now consider the numerical Examples of the following sextic equation using proposed method.

$$x^6 - 8x^3 + 32x^4 - 78x^3 + 121x^2 - 110x + 50 = 0 \ldots \qquad (1)$$

The first step is to check whether the coefficient in the above sextic equation satisfy the condition stipulated by the expression or not. Evaluating a_0 from the expression $a_{0\,=}$ 50 and thus we note that this condition is met. Having evaluated we have b_2= -4,b_1=8, b_0= -7, c_1= i, and c_0 = I respectively, where i = $\sqrt{-1}$ using these values above in equation (1) (King, 1996).

George Jerrard also put up a unique real roots of the polynomial $x^5 + x + a$ which is called Bring Radicals or an ultra radicals of a real number a is the unique real root of the polynomial. Bring radicals of a complex number is a polynomial (it is thus partially undefined) or a specific roots , which is usually chosen in order that Bring radicals is a function of a, which is real – valued when a is real and is analytic function in a neighbourhood of the real line.

George Jerrard showed that some quintic equation can be solved in closed form using radicals and bring radicals which had been introduced by Erlang Bring. The general form is;

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

Attempt to simplify the quintic using Tschirnhaus transformation to reduce the number of independent coefficient.

2.4.1 Principal Quintic Form

The reduced general qunitic may be deduced into what is known as the principal quintic form with the quartic and cubic terms removed.

$$x^5 + C_2x^2 + C_1x^2 + C_0 = 0$$

If the roots of a general quintic and that of principal quintic are related by the quadratic Tschirnhaus transformation. $Y_k = x_k^2 + \alpha x_k + \beta$, α and β may be determined by using the resultant.

2.4.2 Bring-Jerrard Normal Form

It is possible to simplify the quintic still further and eliminate the quadratic term. Producing the Bring-Jerrard norm form $x^5 + d_1 + d_0 = 0$

Using the power – sum formulae again with a cubic transformation as Tschirnhaus trend does not work since the resulting system of equation results in a sixth – degree equation.

He found a way around this by using a quartic Tschinhaus transformation to relate the roots of a principal quintic to those of Bring –Jerrard quintic .

$Z_k = x_k^4 + \alpha x_k^3 + \beta x_k^2 + \gamma x_k + 8$. The method discovered by Jerrard in 1852. He employs a computer packages (Maple) to help him as he might expect some complexity. To regard it as an algebraic function the solution to $x^5 + d_1 x + d_0 = 0$, the two variables d_1 and d_0 are showing that the reduction is actually to an algebraic function of one variable. Because further reduction of Bring –Jerrard set $Z = \frac{x}{\sqrt{-d_{1/5}}}$ to be reduced to the for $Z^5 - 5Z - 4t = 0$. The single variable $t = -(d_0/4)\ (-d1/5)^{-5/4}$

2.5 Sextic Equation (Kulkarni,2008)

The sextic polynomial is a polynomial of degree six. A sextic equation or hexic equation is an equation whose left hand side is a sextic polynomial and whose left hand side is a sextic polynomial and whose right hand side is zero. That is;

$ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + fx + g = 0$, $a \neq 0$ as the coefficients a, b, c, d, e, f, g may be integers, rational numbers, real numbers, complex numbers or members of any field.

2.5.1 Solvable Sextic (Kulkarni,2008)

Some sixth degree equation, such as $ax^6 + dx^3 + g = 0$, can be solved by factorizing in to radicals, but other sextics cannot. Evariste Galois developed a techniques for determining whether a given equation could be solved by radicals which gave rise to the field of Galois theory.

The sextic equation is solvable in terms of radicals if and only if its Galois group is contained either the group of order 48 which stabilises a partition of a set of the order 72 which stabilises a portion of the set of the roots into two subsets of three roots.

There are formulas to test either case, and if the equation is solvable, compute the roots in terms of radicals (Hagedorn, 2000).

2.6 Septic Equation

Septic polynomial is a polynomial of degree 7, f(x) = ax^7 bx^6 + cx^5 + dx^4 +ex^3 + fx^2 + gx + h and for the sextic equation is ax^7 + bx^6 + $^{C}x^{5}$ + dx^4 +ex^3 + fx^2 + gx + h = 0 where a≠0, as a, b, c, d, e, f, g, h may be integers, rational numbers, real numbers, complex numbers or a member of any field.

2.6.1 Solvable Septic

Some seventh degree polynomial can be solved by factorising into radicals, but other septics cannot. The technique developed by Evasriste Galois can determine whether a given equation of Galois theory. To give an example of an irreducible by solvable septic, one can generalise the solvable de moivre quintic to get;

$x^7 + 7\alpha x^5 + 14\alpha^2 x^3 + 7\alpha^3 x + \beta = 0$ where the auxiliary equation is $y_2 + \beta_y - \alpha^7 = 0$

This means that the septic is obtained by eliminating u and v between x = u + v, uv + α = 0 and $u^7 + v^7 + \beta = 0$

It follows that the septics seven roots are given by x_k = w_k $\sqrt[7]{y_1}$ + w_k^6 $\sqrt[7]{y_2}$, where w_k is any of the 7th roots of unity. The Galois group of this septic is the maximal solvable group of order 42. This is easily generalised to any other degree K not necessarily prime.

Another solvable family is x^7 - $2x^6$ + (α+1) x^5 + (α - 1) x^4 - αx^3 – (α + 5) x^2 – $6x$ – 4 = 0 whose members appears in Kluner's database of number fields it descriminant is

$\Delta = 4^4 (4\alpha^3 + 9a\alpha^2 - 34\alpha + 467)^3$

The Galois group of the septic is the dihedral group of order 14(Mohammed & Daniel, 2014).

2.7 Field Extension

Galois from the origin of his work wrote the theory of solving polynomials in the complex field. Though many mathematicians today use arbitrary fields.

We want to begin by defining a field extension. A field L is an extension of a field F if F≤L. that is if any field F is an extension of Q, if F is of characteristics 0, otherwise F is an extension of Zp if F is of characteristics P. Also, for example when you take a field of real numbers R and the field of complex numbers C. We denote the extension of R by C as R≤ Ȼ. Note that there are two minimal fields, Q and Zp. While the extension of Q is relatively easy to construct, the construction of a field extension of Zp, requires a review of polynomials.

In another look at the field extension we say; Suppose a field L is an extension of a field F if F≤L. Any field F is an extension of Q, if is of characteristics O; otherwise F is an extension of Z_p if F is of characteristics P. also, take for example, the field of IR and ⊄, we denote the extension of IR by Ȼ as IR ≤ Ȼ. We have 2 natural fields, Q and Z_p, Q is easy while Z_p requires review of polynomials.

An example of field extension of can be gotten from the use of Z_p. Let p(x) be an irreducible polynomial in f[x]. This means that ∄ element α in f[x] + p(α) = 0.now ⟨p(x)⟩ are all polynomial that have p (x) as a factor; this is called an “ideal” past as we can find ideal by taking a quotient field and an ideal –(gZ_5 = 2/52 = 2/⟨5⟩ so is the field extension.

E = f(x)/⟨p(x)⟩. In other word if an ideal polynomial p(x) ∈f[x], then there is a field extension E of F, such that ∝ ∈ f and so p(∝) = 0

For example let f be a field, then F=Z_2, and let $P_{(n)} = x^2 + x + 1$ which is an element of $Z_2[x]$ then we must extend Z_2. The extension E of Z_2 $[x]/\langle x^2 + x + 1\rangle$. The class of x mod (p(x)) = ∝ ⇒ the reminders are 0, 1, ∝, 1 +∝, these reminders create Galois fields GF (4) ={0. 1. ∝, 1+∝}, since we know that $\propto^2$+∝+1= 0, we can form a table for this field.

Note that $\propto^2 = \propto + 1$

Table 2.1 Group of GF(4) under addition

+	0	1	∝	1+∝
0	0	1	∝	1+∝
1	1	0	1+∝	∝
∝	∝	1+∝	0	1
1+∝	1+∝	A	1	0

Table 2.2 Group of GF(4) under multiplication

X	0	1	∝	1+∝
0	0	0	0	0
1	0	1	∝	∝ +2
∝	0	A	1+∝	1
1+∝	0	1+2	1	20 ∝

In a different look at the definition of field extension we assume that F≤E is a simple extension and α∈E. we say that α is algebra over F if some non-zero polynomial f(x) ∈F[x] factors in F[x], so that f(x) = g(x)h(x) for g(x) = f(α) =φ_a(g$_{(n)}$ $\varphi_a(x)$) = f(α)h(α) thus if α∈E, then f(α) = 0 iff either g(α) = 0 or h(α) = 0 otherwise, when f(x)≠0, α is transcendental over F.

LH K be s field, by field extension of K as a subfield let a field L/K [read: L over K] as an extension. The L can be x considered as a vector space over K. The degree of L over K, denoted by [L:K] is defined as [L:K] = dm$_k$ L = the v.s dimension of L over K.

If [L:K] < ∝, we say that L is a finite extension of K or that L is finite over K. a subfield K of Ȼ ∋ [K:Q) < ∝ is called algebraic number field or simply a number filed, L is finite (Noelle, 2010).

2.7.1 Field Extension in Factoring polynomial.

Suppose F is a field and F$[x]$ is the set of all polynomials over F, that is, polynomial, with coefficient in F. We know that F$[x]$ is a Euclidean domain, and therefore a principal ideal domain and a unique factorization domain. Thus, any non-zero polynomial F in F$[x]$ can be factored uniquely as a product of irreducible polynomials. Any root of F must be a root of one of the irreducible factors, though we have no concrete information about the existence of roots and how to look for them. That is if $X^2 + 1$ has no real roots, though going through the larger concept of complex number we have two roots such i and $-i$ (Jacobson, 1964).

2.8 Splitting Field

Definition 3.24: let f$[x]$ be a non constant polynomial. By a splitting field of f(x) over K we mean an extension L of K + f(x) splits into their factors in h and L is generated over K by the roots f(x) in L

i. f(x) = c $(x\text{-}\alpha)\ldots(x\text{-}\alpha_n)$ for some C $\in$K and α, ..$\alpha_n \in$L

ii. L= K$(\alpha\ldots\alpha_n)$

2.8.1 Splitting Field and the root of polynomial

Suppose E is an extension of F and $f \in F[x]$, then we can say that $fsplit$ over E if f can be written as $\lambda(x - \boxed{?} \propto_1) \ldots (x - \propto_k)$ for some $\propto_1, \ldots, \propto_k \in E \; and \; \lambda \in F$

Note that; suppose we refer to $\propto_i$ as the root of f. That is implicitly we assume that if β is an element of some extension E$'$ of E and F(β) = 0, then β must be one of $\propto_i$, that is through the substitution of β into the equation F(x) = $\lambda\ _{\boxed{?}}(x-\propto_1),\ldots.(x-\propto_k)=0$

Now suppose K is an extension of F and $f\in F[x]$, we say that K is a splitting field for f over F. If f splits – over K but not cover any proper subfield of K containing F.

Equivalently, K is a splitting field for f over F if f splits over k and K is generated over F by the roots $\propto_1,\ldots,\propto_k$ of f, in other words, F$(\propto_1,\ldots,\propto_k)$ = K. For if K is a splitting field for f, then since f split over K we have all $\propto_j\in K,$ so F$(\propto_1,\ldots,\propto_k)$⊆k.

But f splits over F$(\propto_1,\ldots,\propto_k)$, and it follows that F$(\propto_1,\ldots,\propto_k)$ cannot be a proper subfield; it must coincide with K. Conversely, if f split over K and F$(\propto_1,\ldots,\propto_k)=K$. Let L be a subfield of K containing F. If f splits over L then all $\propto_i$ belong to L so K= F$(\propto_1,\ldots,\propto_k)$⊆L⊆K, so L= K

If f$\in F[x]$ and f splits over the extension E of F, then E contains a unique splitting field for f, namely F$(\propto_1,\ldots,\propto_k)$(Stillwell, 2010)

2.9 Fundamental Theorem of Galois Theory (Andrew, 2013)

The intrinsic property of the polynomials f(x) or the extension L/K are merely captured in this group. A main result of Galois theory established a 1-1 correspondence between the subgroup G and the sub fields of L containing K. this Galois celebrated his results in theory of equations.

Definition 3.20: let L/K denoted by Galois (L/K) is defined by Galois (L/K) = the group of all K-automorphism

2. L/K is said to be Galois extension of it is finite, normal and separable. It it is not solvable for n≥ 5, of poly degree 5 cannot be solved by radicals.
3. For a subgroup H of Galois (L/K), the field of H, denoted by L^H, is defined L^H = $\{\alpha \in L\ \alpha\ (\alpha)=\alpha\forall\alpha E^1 H\}$

Note that Galois (L/K) is induced a group (with composition map as the gap operation and that L^H is a sub field E of L containing K, L/E is also Galois extension and Gal (L/E) is a subgroup of Gal (L/K).

Also, let L/K be a Galois extension. Then Galois (L/K) is a finite group of order [L:k] and this is a bijection between the subfield E of L and the subgroups H of Galois (L/K), given by E → Gal (L/E) with the inverse given by H → L^H in particular, K is the fixed field of Gal (L/K).

2.10 Polynomials

Suppose a_o + a_1 x + …. + a_n x^n where a_o, …., a_n ∈R, 0≤ $n \in z$, and x is undefined. The element a_o, …., a_n are called the coefficients of the polynomial. Sum and product of this polynomial can be easily expressed as: suppose f(x)= a_o+ $a_1\, x +$…+$a_n x^n$ and g(x) = $b_0 +\ b_1 x + \cdots + b_n x^n$. So by adding them we have, f(x) + g(x) = (a_o+ b_0) + (a_o+ b_1)x + …. + (a_n+ b_n) x^n. The coefficient are simply added, though for the multiplication K(x) = f(x) g(x) = d_o+ $d_1 x +$………+$d_n x$, where $d_o = \overset{n}{\underset{1=0}{\Sigma}} a_i\ b_{n-1}$. When the coefficients of two different polynomial of the same degree are equal, we defined the polynomial as equal.

Now, we need to defined (x) as the set of all the polynomial with coefficient in the field. Thus $\langle [f], +, * \rangle$ satisfies all the axiouns of a filed, except that not all of the elements have multiplicative inverses. From the definition of Rings we can say that $\langle Z, +, * \rangle$, $(Q, +, * \rangle$ and $\langle C, +, * \rangle$ are lall set of rings but Z does not have multiplicative inverse under multiplication. Hence Z is not a field but a ring.

F $[x]$ is a ring for any field F, e.g Q $[x]$ is a ring, Z_5 is a ring and also a field which means there are possible reminders when Z is divided by Z_5. That is Z_5 is the field equal to the quotient field $Z/5Z$. Just as the integers have remainders. This division is commonly referred to as ***factoring***, in other word F $[x]$ = q $[x]$ h $[x]$ +r$[x]$, where the degree of the remainder r(x) is less than the degree of q$[x]$(Pan & garret, 2012)

2.10.1 Factoring Polynomials

By factoring we mean the Zeros of a polynomial which is very important in this our study. In fact, the purpose for the scientific pursuit of Galois. The theorem shown.

Theorem 2.33 (Neolle, 2010)

Any element $\propto \in$F(a field) is a zero of f $(x) \in$ F $[x]$ if and only if $x - \propto$ is a factor of f(x) in F $[x]$. E.g the polynomial f (x) = x^4+ 4, can be factored into linear factor in $Z_5[x]$.

Let $\propto$ = 1. Using division, we see that $x - 1$ = $x + 4$ is a factor of f(x). We continue with $\propto$ = 2, $\propto = 3$ and $\propto = 4$. Finally, f$(x) = (x + 1)(x + 2)(x + 3)(x + 3)$

Thus we can say that $\propto = 1, 4, 2, 3$ *are* the zero of f(x) in Z_5. Factor theorem is important in solving polynomials.

Now a polynomial f(x) is irreducible over F if f(x) cannot be expressed as product g(x) h(x) of two polynomials g(x) and h(x) in F$[x]$ where both g(x) and h(x) are of lower degree than the degree of f(x). In other words, an irreducible polynomial is a polynomial over a filed F that is unable to be factored in F into a product of polynomials of lower degree. We must note that irreducible polynomial is analogous to prime numbers. However, just because of polynomial is irreducible over F does not mean that it is not reducible over a large field E containing F, e.g. f(x) = x^2 + 1 is irreducible over the real number, yet it is reducible over complex number system.

f(x) = x^2 + 1 factors into $(x - i)$ $(x + i)$, where i is imaginary number such that $i = \sqrt{-1}$

Theorem 2.24 (Vander, 1991)

Let f(x) ∈F$[x]$, and f(x) be of degree 2 or 3. Then f(x) is reducible over F if and only if f(x) has a zero in F . In other words, if a polynomial of degree 2 or 3 is factorable, then it has zeros or conversely, if a polynomial of degree 2 or 3 has zeros in F, then it is reducible.

Polynomial in f(x) can be factored into a product of irreducible polynomial in F(x) in a unique way.

Theorem 2.25 (Neolle, 2010)

Let P(x) be an irreducible polynomial in F(x). If P(x) divides r(x)S(x) in F$[x]$, for r(x), S(x)in F$[x]$, then either p(x) divides $r(x)$ or P(x) divides S(x).

From above we let $\mathrm{P}(x) = x - i$. Thus $\mathrm{P}(x)$ is irreducible and also divided $(x^2 + 1)\ (x + 1)$. In generalization.

Theorem 2.26 (Neolle, 2010)

If F is a field, then every no constant polynomial $\mathrm{f}(x) \in \mathrm{F}[x]$ can be factored in $\mathrm{F}[x]$ into a product of irreducible polynomials that are unique except for order and for unit (that is, non zero constant).

Necessary, understanding how to factor polynomial is imperative to comprehending field extensions. After all, this was the problem that Galois faced and ultimately solved.

Now as we have said. Let $\mathrm{P}(x)$ be an irreducible polynomial in $\mathrm{F}[x]$. this means that there is no element $\propto in\ \mathrm{F}[x]$ such that $\mathrm{P}(\propto) = 0$. Now $\langle \mathrm{P}(x) \rangle$ are all polynomials that have $\mathrm{P}(x)$ as a factor; this is called an "ideal". Just as we can find a field by taking quotient of a field and an ideal, we can use the same idea with polynomials. Just as above Z_5 = $\mathrm{Z}/5\langle \mathrm{Z} \rangle$, so is the field extension. E = $\mathrm{F}[x]/\langle \mathrm{p}(x)\mathrm{Z} \rangle$. In other words, if there is an irreducible polynomial $\mathrm{p}(x) \in \mathrm{F}[x]$, then there is a field extension E or F, such that there exist and $\propto \in E$, such that $\mathrm{P}(\propto) = 0$. (Neolle, 2010)

CHAPTER THREE

MATERIALS AND METHODS

3.1 Galois Theory

In this chapter we shall discuss the apparatus and instrument that a polynomial need to be soluble by radicals. We begin with what a Galois theory is? In which we say that it is the principles put in place (theories) put in place to solve polynomial equation of degree n. Further more we can assert that solving general polynomial by radicals mean the repeatedly taking n-th root for various n.

3.2 Identifying the irreducible polynomial.

From Gauss's Lemma, suppose $f(x) \in \mathbb{Z}[x]$ having a proper factorisation over $\mathbb{Z}$ if and only if it has a proper factorisation over Q. Hence using Esienstein test to identify irreducible polynomial. Given s = 0,and s$\in$ $\mathbb{Z}$ and choosing $a_i \in \mathbb{Z}$. Then $f(x) = a_0 + a_1(x-s) + \cdots + a_{d-1}(x-s)^{d-1} + a_d(x-s)^d$ where d=deg$f(x)$ and suppose p> 0 is a prime for which the following holds:

-$a_k \equiv 0(mod\, p)$ for k=0,...,d-1

-$a_0 \not\equiv 0(mod\, p^2)$;

-$a_d \not\equiv 0(mod\, p)$

Then $f(x)$ is irreducible in $Q[x]$ and so is in $\mathbb{Z}[x]$. For example, let p≥ 2 be prime. Then the polynomial ϕ_p (x)=$1 + x + \cdots + x^{p-1} \in \mathbb{Z}$ is irreducible in $Q[x]$ and also in $\in \mathbb{Z}$. This is also in relation to cyclotomic polynomial ϕ_p $(x) \in \mathbb{Z}$. Defined for all values of n≥ 1, with the formular $x^n - 1 = \prod_{\boldsymbol{d/n}} \phi\mathrm{d}\ (x)$

3.3 Galois Group

Let L be an extension on field of K, denoted by L/K and G be the set of automophism of L/K, that is the set of automophism σ of L such that σ(x)=x for every $x\epsilon$ K, so that K is a field. Then G is a group of transformation of L, called the Galois group of L/K and is denoted by Gal(L/K) or Aut(L/K).

Let f(x) be a rational polynomial of degree n and let K be the splitting field of f(x) over Q, that is the smallest subfield of C containing all the roots of f. Then each element of the Galois group G(K/L) permutes the roots of f in unique way. Thus G can be identified with a subgroup of the symmetric group S_n, the group of permutation of the roots f. If f is irreducible, then G is transitive subgroup of S_n that is given two roots $\alpha\ and\ \beta$ of f, there exist an element $\sigma(\ \alpha)= \beta$.

The root of f is solvable by radical if and only if G is a solvable group. Since all the subgroup of S_n with $n\leq 4$ are solvable, the roots of all polynomial of degree 5 or greater are generally not solvable by radicals since S_n (and the alternating group A_n) are not solvable for $n\geq 5$.

Consider the equation $x^5 - x^4 - x + 1 = (x^2 + 1)\ (x + 1)\ (x - 1)^2$ (3.1)

and the equation $y^5 + py^3 + qy^2 + ry + s = 0$ (3.2)

3.1 and 3.2 does not follow the same pattern. But consider $x^5 + ax + b$ which we can later relate it to that of a sextic and septic.

Also lets consider $x^7 + 7\alpha\ x^5 + 14\alpha^2\ x^3 + 7\alpha^3\ x + B$ (3.3) and $x^7 - 2x^6 + (\alpha + 1)\, x^5 + (\alpha -1)\, x^4 - \alpha x^3 - (\alpha + 5)\, x^2 - 6x - 4 = 0$ (3.4).

No proper pattern is followed other than $x^6 + \mathrm{a}x + \mathrm{b} = 0$ and for the septic polynomial

$$x^7 + 7\alpha\, x^5 + 14\alpha^2 x^3 + 7\alpha^3 x + \mathrm{B} = 0 \qquad (3.5)$$

as $x^7 + 2x^6 + (\alpha + 1)\, x^5 + (\alpha - 1)\, x^4 - \alpha\, x^3 + (\alpha + 1)\, x^2 - 6x - 4 = 0$ (3.6)

It also does not follow the same pattern as $x^7 + \alpha x + \mathrm{b} = 0$ did.

From the discussion, we can lay a foundation for our analysis in order to say that trinomial equations of higher degree polynomial in $x^5 + \mathrm{a}x + \mathrm{b} = 0$, $x^6 + \mathrm{a}x + \mathrm{b} = 0$, and $x^7 + \mathrm{a}x + \mathrm{b} = 0$. Hence we can generalised by saying $x^{\mathrm{n}} + \mathrm{a}x + \mathrm{b} = 0$ can be used in place of these case study. Subsequently we can now prove it. The three sampled polynomials are irreducible over $\mathrm{Q}(x)$ for $|\mathrm{a}, \mathrm{b}| < 1000$. For example the polynomial $x^6 + 3x + 3 = 0$, $x^8 - 5x - 5 = 0$, $x^7 - 14x - 13 = 0$ and $x^6 + 133x + 209$ are all irreducible but solvable by radicals.

We want to begin with the trinomial of solvable quintic.

3.4 Trinomial Polynomial of Solvable Quintics Functions.

Let $x^5 + \mathrm{a}x + \mathrm{b} = 0$ be the general form of a trinomial solvable quintic with a, b non zeros. The roots of (3.9) cannot be expressed as algebraic functions of the coefficients a and b. We want to characterize (3.9) completely, in its irreducible state but solvable by radicals. Our main aim is to extend the cardono's method for solving the cubic equation $x^5 + \alpha x + \mathrm{b} = 0$. Recall the cardono's method in such a way that we can apply it to quintics (3.9).

Suppose u, u_2 are complex numbers and w is a complex cube root of unity, expanding the product.

$$(x - (u_1 + u_2))\ (x - (wu_1 + w^2u_2))\ (x - (w^2u_1 + wu_2)) \qquad (3.10)$$

We obtain the polynomial

$$x^3 - 3u_1\ u_2\ x - (u_1^3 + u_2^3) \qquad (3.11)$$

As $x_j = w^ju_1 + w^{2j}u_2$ (j = 0, 1, 2) is a root of the cubic polynomial (3.10)

substituting it into (3), we obtain the identity valid for j = 0, 1, 2

$w^ju_1 + w^{2j}u_2 - 3u_1u_2\ (w^ju_1 + w^{2j}u_2) - (u_1^3 + u_2^3) = 0$

Thus the cube $x^3 + \alpha x + b = 0$ has three solution $x_j = w^ju_1 + w^{2j}u_2$ (j = 0, 1, 2) where u_1^3 and u_2^3 are determined from $u_1^3 + u_2^3 = -b1\ u_1^3\ u_2^3 = -\ (a/3)^3$.

An obvious generalisation of this is to consider the quintic polynomial.

$$\prod_{j=0}^{4}(x - (w^ju_1 + w^{4j}u_2\ )) \qquad (3.12)$$

Where w is now a complex fifth root of unity. Expanding the product (3.12)

and proceeding as above, we find that the quintic $x^5 + \alpha x^3 + (a^2/5)x + b$ (sometimes called de moivres quintic) has the solution $x_j = w^ju_1 + w^{4j}u_2$, j = 0,1, 2, 3, 4 where u_1^5 and u_2^5 are determined from $u_1^5 + u_2^5 = -b1\ u_1^5u_2^n = -\ (a/5)^5$

We refine this method by considering instead of (3.12) the quintic polynomial.

$$\prod_{j=0}^{4}(x-(u^{j}u_1+u^{3j}u_2+w^{3j}u_3+w^{4j}u_4)) \qquad (3.13)$$

Where u_1, u_2, u_3, u_4 are nonzero real numbers and w is a complex fifth root of unity. Multiplying out (3.13) is somewhat more challenging than (3.12), so MAPLE was employ to do the work. Replacing x by $w^{j}u_1 + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4$ in the expanded product, we obtain the identity valid for j = 0, 1, 2, 3, 4

$(w^{j}u_1, + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4)^5 - 5u(w^{j}u_1, + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4)^3 - 5v\ (w^{j}u_1, + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4)^2 + 5w\ (w^{j}u_1, + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4) + 5\ (X - Y) - Z = 0$ (3.14)

Where;

$U = u_1u_4 + u_2u_3$

$V = u_1u_2^2 + u_2u_4^2 + u_3\,u_1^2 + u_4u_3^2$

$W = u_1u_4^2 + u_2^2u_3^2 - u_1^3u_2 - u_2^3u_4 - u_3^3u_1 - u_4^3u_3 - u_1u_2u_3u_4$

$X = u_1u_3^3u_4 + u_2^3\mathrm{u1}u_3 + u_3^3u_2u_4 + u_4^3u_1u_2$

$Y = u_1u_3^2u_4^2 + u_2u_1^2u_3^2 + u_3u_2^2u_4^2 + u_4u_1^2u_2^2$

$Z = u_1^5 + u_2^5 + u_3^3 + u_4^5$

The essential ingredient of the proof of our characterization of solvable quintic trinomial is the determination of real algebraic number u_1, u_2, u_3,u_4 satisfying.

$$u_1u_4 + u_2u_3 = 0 \qquad (3.15)$$

$u_1 u_2^2 + u2u_4^2 + u3u_1^2 + u4u_3^2 = 0$ (3.16)

$5(u_1^2u_4^2 + u_2^2u_3^2 - u_1^3u_2 - u_2^3u_4 - u_4^3u_3 – u_1u_2u_3u_4) = a$ (3.17) and

$5\ (u_1^3u_3u_4 + u_2^3u_1u_3 + u_3^3u_2u_4 + u_4^3u_1u_2) – (u_1u_3^2u_4^2 + u_2u_1^2u_3^2 + u_3u_2^3u_4^3 + u_4u_1^2u_2^2) – (u_1^5 + u_2^5 + u_3^5 + u_4^5) = b$ (3.18)

So that the quintic polynomial (3.13) becomes $x5 + ax + b$ and has the roots $x_j = (w^ju_1, + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4)$ (j = 0, 1, 2, 3, 4) (3.19)

Theorem 3.1: let a and b be rational numbers such that the quintic trinomial $x^5 + ax + b$ is irreducible. Then the equation $x^5 + ax + b = 0$ is solvable by radical if and only if there exist rational numbers $\epsilon\ (= \pm 1)$, $C\ (\geq 0)$ and $e\ (\neq 0)$ such that

$a = \frac{5e^4\ (3-4\epsilon c)}{c^2+1},\ b = \frac{4e^4\ (11\epsilon-2c)}{c^2+1}$ (3.20)

In which case the roots $x^5 + ax + b = 0$

$x_j = (w^ju_1, + w^{2j}u_2 + w^{3j}u_3 + w^{4j}u_4)$ (j = 0, 1, 2, 3, 4) (3.21)

Where $w = \exp\ (\frac{2^{\pi i}}{5})$ and

$u_1 = (\frac{v_1^2v_3}{D^2})^{1/5},\ u_2 = (\frac{v_3^2v_4}{D^2})^{1/5,}\ u_3 = (\frac{v_2^2v_1}{D^2})^{1/5},\ u_4 = (\frac{v_4^2v_2}{D^2})^{1/5}$ (3.22)

$$\begin{cases} v_1\sqrt{D} + \sqrt{D - \epsilon\sqrt{D},\ v_2} = -\sqrt{D} - \sqrt{D + \epsilon\sqrt{D}} \\ v_3\sqrt{D} + \sqrt{D - \epsilon}\sqrt{D},\ v_4 = \sqrt{D} - \sqrt{D} - \epsilon\sqrt{D} \end{cases} \qquad (3.23)$$

$D = c^2 + 1$

Proof: suppose that the irreducible quintic polynomial $x^5 + ax + b$ is solvable by radical. Thus the resolvent sextic of $x^5 + ax + b$, namely

$$x^6 + 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^3 + (512a^5 - 3125b^4)\, x + (256a^6 - 9375ab^4)$$

Has a rational root r. Therefore r satisfies

$$(r + 2a)^4 (r^2 + 16a^2) - 5^5b^4 (r + 3a) = 0 \qquad (3.24)$$

Which shows that $r \neq 2a, -3a$ as $a \neq 0$. We defined the non-negative rational number c and the nonzero rational number e by

$$\epsilon C = \frac{3r-16a}{4(r+3a)},\ e = \frac{-5b\epsilon}{2(r+2a)},\ \text{where } \epsilon = \pm 1 \qquad (3.25)$$

Then $C^2 + 1 = \frac{25(r^2 + 16a^2)}{16(r+3a)^2}$

$$3 - 4\epsilon C = \frac{25a}{r+3a}$$

$$11\epsilon + 2C = \frac{25(r+2a)\epsilon}{2(r+3a)},\ \text{so that}$$

$$\frac{5e4\,(3-4\epsilon C)}{C^2+1} = \frac{5^5ab^5\,(r+3a)}{(r+2a)(r^2+16a^2)} = a \text{ and}$$

$$\frac{-4e^5(11\epsilon+2C)}{C^2+1} = \frac{5^5ab^5\,(r+3a)}{(r+2a)^4(r^2+16a^2)} = b$$

Given the required parameterization. We now shows that the irreducible quintic trinomial

$$x^5 + \frac{5e4\,(3-4\epsilon C)}{C^2+1}\ x - \frac{-4e^5(11\epsilon+2C)}{C^2+1} \qquad (3.26)$$

Where e = 1 is solvable by radical with roots given (3.19). in fact it is not necessary to assume that the quintic is irreducible. For general e the transformation $x \rightarrow \mathrm{e}x$ gives the required result (3.21). from (3.23) we see that

$$\begin{cases} v_1 + v_4 = 2\sqrt{D}, \ \ v_2 + v_3 = 2\sqrt{D} \\ v_1 v_4 = \epsilon\sqrt{D}, \ \ v_2 v_3 = \epsilon\sqrt{D} \end{cases} \tag{3.27}$$

And so $\begin{cases} v_1 + v_2 + v_3 + v_4 = 0 \\ v_1 v_4 + v_2 v_3 = 0 \end{cases}$ (3.28)

Further from (3.22) we obtain

$$u_1^5 = \frac{v_1^2 v_3}{D^2}, u_2^5 = \frac{v_3^2 v_4}{D^2}, u_3^5 = \frac{v_2^2 v_1}{D^2}, u_4^5 = \frac{v_4^2 v_2}{D^2} \tag{3.29}$$

Easy calculations making use of (3.27) as (3.29) and (3.29) yield

$$u_1 u_4 = -\frac{\epsilon}{\sqrt{D}}, u2u3 = \frac{\epsilon}{\sqrt{D}} \tag{3.30}$$

$$u_1 u_2^2 = \frac{v_3}{D}, u_3^2 v_4 = \frac{v_2}{D}, \ u_1^2 v_3 = \frac{v_1}{D}, u_4^2 v_2 = \frac{v_4}{D} \tag{3.31}$$

and $u_1^3 v_2 = \frac{\epsilon v_1 v_2}{D\sqrt{D}}, \ u_2^3 v_4 = \frac{-\epsilon v_3 v_4}{D\sqrt{D}}, u_3^3 v_1 = \frac{-\epsilon v_1 v_2}{D\sqrt{D}}, u_4^3 v_3 = \frac{\epsilon v_2 v_4}{D\sqrt{D}}$ (3.32)

Which give the required equations (3.15) and (3.16) in view (3.28). from (3.23), (3.29), (3.30), (3.31) and (3.32). We deduced that

$$5(u_1^2 u_4^2 + u_2^2 u_3^2 - u_1^3 u_2 - u_2^3 u_4 - u_3^3 u_1 - u_4^3 u_3 - u_1 u_2 u_3 u_4)$$

$= \frac{5(3-4\epsilon\sqrt{D-1})}{D} = \frac{5(3-4\epsilon C)}{C^2+1}$ and

$5((u_1^3 v_3 v_4 + u_2^3 v_1 v_3 + u_3^3 v_2 v_4 + u_4^3 v_1 v_2) - (u_1 u_3^2 u_4^2 + u_2 u_1^2 u_3^2 + u_3 u_2^2 u_4^2 + u_4 u_1^2 u_2^2)) - (u_1^5 + u_2^5 u_3^5 u_4^5) = - \frac{(44\epsilon + 8\sqrt{D-1}}{D} = \frac{-4(11\epsilon+2C}{C^2+1}$

Which are the required equations (9) and (10). This proves that

$x^5 + \frac{5\,(3-4\epsilon C)}{C^2+1}\, x - \frac{-4e^5(11\epsilon+2C)}{C^2+1}$ is solvable by radical and has the root given in (3.18).

The discrimination of the trinomial quintic x^5+ ax + b is $4^4a^5 + 5^5b^4$ the equation x^5 + ax + b = 0 has exactly one real root if $4^4a^5 + 4^4b^4 > 0$ the discriminant of the quintic (3.20) is

$\frac{4^4\, 5^5 e^{20}}{D^5} (4\epsilon C^3 - 84C^2 - 37\epsilon C - 122)^2 > 0$

So the quintic (3.20) has exactly one real root. Suppose now that (3.20) is irreducible over Q. By some of our results, it is solvable by radical, and so its Galois group is solvable. Hence its Galois group is isomorphic to the Frobenius group F_{20} of order 20, the dihedral group D_5 of order 10, or to the cyclic group of order 5. However (3.20) has complex roots, so its Galois group cannot be cyclic of order 5. By the Galois group of (3.20) is the dihedral group D_5 of order 10 if and only if 5D is a perfect square in Q. Otherwise the Galois group is the forbenius group F_{20} of order 20.

Now suppose $f(x) = x^5 + ax + b$ is an irreducible polynomial of degree 5 with rational coefficients. The construction of an explicit resolvent which has rational root became paramount and expedient for our solution of f(x) if and only if f(x) is solvable by radicals. Which is to say that the Galois group is contained in the Frobenius group F_{20} of order 20 in the symmetric group S_5 . The Galois group is said to be isomorphic to F_{20}, to the dihedral group D_{10}, of order 10 Or to the cyclic group $\mathbb{Z}/5\,\mathbb{Z}$. Generally, for any prime p, we can easily see that a solvable subgroup of the symmetric group S_p whose order is divisible by p contained in the normalizer of the sylow p- subgroup of S_p. (Sticklan, 2009).

The main purpose here is to give a criterion for the solvability of such a general quintic in terms of the existence of a rational root of an explicit associated resolvent sextic polynomial, and when this is the case, to give formula for the roots analogous to Cadarno's formula for the general cubic and quartic polynomials. Precisely to determine the Galois group in particular, the roots are produced in an order which is a cyclic permutations of the roots, this is very useful in other computations.

3.5 Fixed Field Of The Frobenius Subgroups.

Let x_1 , x_2, x_3, x_4, x_5 be the roots of the general quintic polynomial

$$x^5 - S_1x^4 + S_2x^3 - S_3x^2 + S_4x - S_5$$

Where the S_i , are the elimentary symmetric functions in the roots. Let $F_{20} < S_5$ be the Frobenius group of order 20 with generators (12345) and (2354). Then the stabilizer in S_5 of the element.

$$\theta = \theta_1 = x_1^2x_2x_5 + x_1^2x_3x_4 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_5 + x_3^2x_2x_4 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_4 + x_5^2x_2x_3$$

Is precisely F_{20} . It follows that θ_1 satisfies a polynomial equation of degree b over Q(S_1 , S_2, S_3, S_4, S_5) with conjugates.

$\theta_2 = (123)\theta_1$

$$= x_1^2x_2x_5 + x_1^2x_3x_4 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_5 + x_3^2x_2x_4 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_4 + x_5^2x_2x_3$$

$\theta_3 = (132)\theta_1$

$$= x_1^2x_2x_3 + x_1^2x_4x_5 + x_2^2x_1x_4 + x_2^2x_3x_5 + x_3^2x_1x_5 + x_3^2x_2x_4 + x_4^2x_1x_3 + x_4^2x_2x_5 + x_5^2x_1x_2 + x_5^2x_3x_4$$

$\theta_4 = (12)\theta_1$

$$= x_1^2x_2x_3 + x_1^2x_4x_4 + x_2^2x_1x_5 + x_2^2x_3x_4 + x_3^2x_1x_4 + x_3^2x_2x_5 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_3 + x_5^2x_2x_4$$

$\theta_5 = (23)\theta_1$

$$= x_1^2x_2x_4 + x_1^2x_3x_5 + x_2^2x_1x_5 + x_2^2x_3x_4 + x_3^2x_1x_2 + x_3^2x_4x_5 + x_4^2x_1x_3 + x_4^2x_2x_5 + x_5^2x_1x_4 + x_5^2x_2x_3$$

$\theta_6 = (13)\theta_1$

$$= x_1^2x_2x_4 + x_1^2x_3x_5 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_4 + x_3^2x_2x_5 + x_4^2x_1x_5 + x_4^2x_2x_3 + x_5^2x_1x_2 + x_5^2x_3x_4$$

By computing the elementary symmetric functions of the θ_i which are symmetric polynomials in

x_1, x_2, x_3, x_4, x_5. It is relatively a straight forward straight forward matter to express these elements in terms of S_1, S_2, S_3, S_4, S_5 to determine the resolvent sextic F_{20} with θ as a root. By making a translation we may assume $S_1=0$

A particular case is when $f(x) = x^5 + ax + b$. Then the values for T are as follows

$T_1 = (512a^5 - 15625b^4 + 416a^3\theta^2 + 112a\theta^3 + 24a\theta^4 + 4\theta^5)/150b^3)$

$T_2 = (3840a^5 - 78125b^4 + 4480a^4\theta + 2480a^3\theta^2 + 760a^2\theta^3 + 140a\theta^4 +$
$30\theta^5)/512a^2b + 6250b^5)$

$T_2 = (1880a^5 + 71825b^4 - 3424a^4\theta - 21260a^2\theta^2$- $5980a^2\theta^2 - 122a\theta^4 -$
$240\theta^5)/(2b^2)$

$T_2 = (68800a^5 + 2500a^4\theta + 11500a^4\theta^2 + 3250a^2\theta^3 + 375a\theta^4 + 100\theta^5)/$
$(512a^5 + 6250b^4)$

Computing these expression in terms of our given rational θ, and chose a specific Δ as our square root of D_1 then the root of the quadratics in (7)……….

Will give us { l_1, l_4} and { l_2, l_3} up to permutation of the two pairs. This is not sufficient to solve for the resolvent R_1, R_2, R_3, R_4, however, since for example if our choice of the roots in fact corresponds to { l_1, l_3, l_2, l_3} then we do not simply obtain a permutation of the R_1 (this permutation is not obtained by the element of F_{20}). This difficulty is overcome by introducing an ordering condition. For this, observe that { l_1, l_4} { l_2, l_3}= $\theta\Delta$ for some element $\theta \in$K. Computing this e it as before, we write.

$\theta = (r_0 + r_1\theta + r_2\theta^2 + r_3\theta^3 + r_4\theta^4 + r_5\theta^5)(DF)$

where again the value of r_1, ……r_5 for general f(x) are given in Appendix for such a case as f(x) =$x^5 + ax + b$ then we have $\theta = (-1036800a^5 + 48828125b^4 - 228000a^4\theta - 1290500a^3\theta^2 - 399500a^2\theta^3 - 76625a\theta^4 - 16100\theta^5)/256a^5 + 3125b^4)$

3.5.1 Resolvent of Equation

Simple derivations of the classic resolvent which have been obtained hence fore by elaborate computations. Jacob established the form of remarkable resolvent, but neither found the values of the coefficient nor gave the simple details which lead directly to that form.

Cayley not aware of Jacob's work when he fully computed the same resolvent. The coefficient of the equations are semi invariants. Which is the simple method to be employed, which can be gotten through inspection.

3.5.2 Resolvent program

We want to find formular for roots of f(z) = (2$-x_1$)…, (Z-x_n)

(R_1) find a poly $\emptyset \in F$ [x_1, …., x_n] a resolvent

(R_2) find a poly in F[x_1, …., x_n][z] having symmetric functions as coefficient and which has $\emptyset$ as a root, the resolvent equation.

(R_3) use into about $\emptyset$ to determine whether the original equation can be solved and, if so, solve.

(R_2) given $\emptyset \in F$ [x_1, …., x_n] find a poly in F [x_1, …., x_n][Z] having symmetric equation as coefficients and which has $\emptyset$ as root.

The construction principle Let $\emptyset$= $\emptyset_1$……,$\emptyset_m$ be all the images of $\emptyset$ under then symmetric group Sn put R(z) = (z-$\emptyset_1$) …., (z-$\emptyset_m$).

3.6 Trinomial Polynomial of Solvable Sextic

Suppose f (x) = x^6 + ax + b an irreducible polynomial (hence b≠0) with coefficients in the rational numbers. Q if C is a nonzero rational number such that g(x) = C^6F(x/c) = x^6 + a $C^5 x$ + bC^6, then f(x) and g(x) are equivalent under scaling and have the same Galois group.

Now if a≠ 0, then f(x) is indeed a trinomial. We will show there is a unique such trinomial up to equivalent under scaling.

We must note that the radicals of the trinomial sextic polynomial goes hand in hand with that of the quintic with reference that it was fully discussed and that the value 6 instead of 5 should be taken into cognisance. We want to consider the following theorems for clarity of our discussion.

Theorem 3.2: let f (x) = x^6 + ax + b be irreducible over the rational numbers, with a nonzero. If the Galois group of f(x) is isomorphic to the cyclic group of order 6 then f(x) is equivalent under scaling to f(x) = x^6 + 133x + 209.

We want to drive the correspondence between trinomial of a given type and the set of rational points on a gems two curve, determining this (finite) set of points. This is accomplished showing that a rational point on the gems 2 curve induces a point on one of a finite set of elliptic curves defined over a number field, with X-coordinate satisfying a simple “q-rationality” condition. The mathematical ideas behind this approach can be found in a paper of Bruin and the latest version of Magma which is containing Bruins routine for implementing these ideas. We make use of these routine.

Lemma 3.4: If the Galois group of the irreducible polynomial f(x) = x^6 + ax + b is isomorphic to the cyclic group of order b then discriminant of f (x) is negative.

Proof: By Galois theory L is either totally real or totally imaginary. However any trinomial x^6 + ax + b cannot have six real roots (by Rolle’s theorem), therefore none of the six roots of f(x) is real. A simple calculation shows that the disciminant of f(x) equals the product of the three disciminant of the quadratics times a squares so is clearly negative.

In the sextic we may sometimes introduces the resolvent polynomial and how to use the resolvent; namely the disciminant. We would show that there is no way to use only the degrees of irreducible factors of a single resolvent to compute the Galois group of an irreducible degree six polynomial. For example, the stem field of

$$g(x) = x^6 + 2x + 2 \tag{3.35}$$

Contains only one root of g, which can be verified by factoring g(x) over its stem field and searching for linear factors. Though the Galois group of g(x) is S_6 mean the splitting field taken above would be significantly more computationally expensive. The use of absolute resolvent is one way to improve this.

Now the degree six resolvent R_6 (x) for f(x) = g(x) is R_6 (x) = $x^6 - 36x^5 - 540x^4\ 25920x^3 - 3185984x – 674336$.

Which remains irreducible over Q. Thus the Galois group of f is either T_{10}, T_{13}, T_{15} or T_{16}. The discriminant of f is disc (f) = $-2^6.289.227$

37 Trinomial Polynomial of Solvable Septic

Given that f(x) = $x^7 + ax + b$ an irreducible polynomial (hence b ≠ 0, a, b are integers). Now since the septic polynomial and that of quintic polynomial are both prime and odd at the same time. Pattern for their radical will be the same, only for the split and the extension of fields that will come into play.

As few as the trinomial septic polynomial are, there are many equivalent classes of irreducible of degree. The trinomial in Q(x) whose Galois group is not A_7 or S_7.

Christian U. Jensen put up an inverse Galois problem of a trinomial septic polynomial ($x^7 + ax + b$) that is p(15,20) which is irreducible but solvable thus;

P35 (a, b, x) = $x^{35} + 40ax^{29} + 302bx^{28} – 1614a^2x^{21} – 5072a^3x^{17} + 2778a^2bx^{16} – 18084ab^2x^{15} + 36250b^3x^{14} – 5147a^4x^{11} – 1354a^3bx^{10} – 21192a^2b^2x^9 – 26326ab^3x^8 – 7309b^4x^7 – 1728a^5x^5 – 1728a^4bx^4 + 720a^3b^2x^3 + 928a^2b^3x^2 – 54ab^4x – 128b^5$.

Has factorization pattern (degree of irreducible factors) one of (14,21), (7, 7, 7, 21), (7, 7, 7, 7, 7).

However, Kulkarni in 2008 Described a method to solve septic equation in radicals. The salient features of such a solvable septic is that the sum of its four roots is equal to the sum of its remaining roots. The conditions to be satisfied by the coefficients of the septics are given.

Suppose you have a septic equation $x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$,which is solvable by radicals. Here $a_1 , a_2, a_3 , a_4, a_5, and\ a_6$ are rational coefficient. What Kulkarni did was to was to multiply the equation by x, in order to convert it to octic equation. This shows that the roots have increase from seven to eight. He then decomposes the equation for easier means of solution by quartic and cubic or double quartic. The resulting quartic equations are solved to obtain the roots of the given septic. The condition for the coefficients to satisfy in order that the given septic is solvable in such a fashion derived. Then discussed the behavior of the roots. (Ruchavendra, 2008)

CHAPTER FOUR

RESULTS

4.1 Consideration of Practical Problems

In this chapter, we shall concentrate on the use and application of those radicals of the trinomial qųntic, sextic and the septic polynomials. Practical examples would be solved, to aid the generalization of the whole concept of the trinomial polynomial and the proof of the theorem, proposition and corollary to support our argument.

Example 4.1(Blair and Kenneth,1996)

Let $f(x) = x^5 + 15x + 12,$ where determinant D = $2^{10}3^4 5^5$. Then corresponding resolvent sextic $f_{20}(x)$ is the polynomial $x^6 + 120x^5 + 9000x^4 + 54000x^3 + 2025000x^2 + 324000000x$ which clearly has θ = 0 as a root. It follows that the Galois group of f(x) is the frobenius group F_{20} and that f(x) is solvable by radicals with Δ= $7299\sqrt{5}$, where $\zeta + \zeta_{=}^{-1}$(-1 + $\sqrt{5}$)/2, the roots l_1, $l_{2,}$ l_3, l_4 of the quadratics in (7) subject to the ordering condition in (9) are

L_1 = -375=750$\sqrt{5} + 75i\sqrt{625 + 29\sqrt{5}}$

L_4 = -375-750$\sqrt{5} - 75i\sqrt{625 + 29\sqrt{5}}$

L_2 = -375+750$\sqrt{5} - 75i\sqrt{625 - 29\sqrt{5}}$

L_3 = -375+750$\sqrt{5} + 75i\sqrt{625 - 29\sqrt{5}}$

Then

R_1 = $-1875-75\sqrt{1635+385\sqrt{5}}+75\sqrt{1635-385\sqrt{5}}$

R_4 = $-1875+75\sqrt{1635+385\sqrt{5}}-75\sqrt{1635-385\sqrt{5}}$

R_2 = $-5625+75\sqrt{1490+240\sqrt{5}}-75\sqrt{1490-240\sqrt{5}}$

R_3 = $-5625+75\sqrt{1490+240\sqrt{5}}+75\sqrt{1490-240\sqrt{5}}$

Viewing these as real numbers, and letting r_1 be the fifth root of R_1, we concluded that the correspondence r_2, r_3, and r_4 are the real fifth roots of $R_{2,}$ R_3 and R_4 respectively and then (3) gives the roots of $f(x)$. For example, the sum of the real fifth roots of $R_{1,}$ $R_{2,}$ R_3 R_4 above gives five times the (unique) real roots of $x^2+15x+12$

Example 4.2(Blair and Kenneth,1996)

Consider the trinomial quintic polynomial f(x) = $x^5 - 5x + 12$ which is irreducible as $f_1(x\text{-}2)$ is 5-Eisen stein. The resolvent sextic of f_1 is

$X^6 - 40x^5 + 1000x^4 + 2000x^3 + 250000x_2 - 6640000x + 97600000$ which has the rational root r =40, from f(x) we see that E=1, C=2, e=-1, so that by (16) D=5. Since 5D = 5^2 the Galois group of f_1 is D5. The unique real root of f_1 is

$$x = -\left(\frac{\left(\sqrt{5}+\sqrt{5-\sqrt{5}}\right)^2\left(-\sqrt{5}+\sqrt{5+\sqrt{5}}\right)}{25}\right)^{1/5} - \left(\frac{\left(-\sqrt{5}+\sqrt{5+\sqrt{5}}\right)^2\left(-\sqrt{5}-\sqrt{5-\sqrt{5}}\right)}{25}\right)^{1/5} -$$

$$-\left(\frac{\left(-\sqrt{5}+\sqrt{5+\sqrt{5}}\right)^2\left(\sqrt{5}+\sqrt{5-\sqrt{5}}\right)}{25}\right)^{1/5} - \left(\frac{\left(\sqrt{5}-\sqrt{5-\sqrt{5}}\right)^2\left(-\sqrt{5}-\sqrt{5+\sqrt{5}}\right)}{25}\right)^{1/5}$$

A little manipulation shows that this root can be written as x=$^1/_5$ ($R_1^{1/5} + R_2^{1/5} + R_3^{1/5}$ $+ R_4^{1/5}$). The values for R_1, R_2, R_3, R_4 are obvious.

Example 4.3: (Blair and Kenneth,1996)

We now take t=1, e= $^5/_2$, c=$^7/_{24}$, so D= 1+ $(^7/_{24})^2$ =$(^{25}/_{24})^2$, and the quntic (19) is f(x) = x^5 +330x – 4170, which is irreducible as f (x) is 5-Eisenstein. Since 5D =$5^5/(2^6.3^2)$ the Galois group of f is F_{20}. Hence by the theorem of the unique rial root f becomes

X=$54^{1/5}$ + $12^{1/5}$ + $648^{1/5}$-$144^{1/5}$

Example 4.4(Dummit, 1999)

Consider the polynomial f(x) =x^5 – 5x +12 which is equivalent to x^5-tx + t, where t= -3125/20736. The Galois group of x^5-5x +12 is D10 and so L, the smallest field over which f(x) factors as the product of a quadratic and a enbric is K=Q(x), where x^5-5x + 12 =0. The elliptic curve E is isomorphic to 72 = x^3 – 675x – 79650 over K($\sqrt{-10}$), the splitting field of the quntic (i) It follows that E is the -10 quadratic twist of Eo, and our mode for E can be given by E: y^2=x^3 – x^2 – 833x + 109537.

Note that from Galois who says that there is no general formula to solve aquintic equation in terms of radicals. F or example, x^5-4x+2 it is known that it has a root that is not expressible in the above mention operations (as its Galois group is S_5). It is Bring-Jerrard form of the quntic equation.

Example 4.5:

Consider the sextic equation x^6+x^2 +1x +c = 0 is solvable and its Galois group is a subgroup of J if and only if the resolvent equation.

X^{15} -6$e^2 x^{13}$-(42e+3)$e^3 x^{12}$+7$e^4 x^{11}$ + (222e-21d^2)e^5 x^{10} +(453e^2 +57e+8)$e^9 x^6$ –(340e – 109d^2)$e^7 x^8$ – (1716e^2 – 288d^2e +17) x^7 – (1232e^2 – 300e + 144d^2) $e^9 x^6$ + (1534e^2 + 538d^2e -358e^2e -353d^4 +2)$e^{10} x^5$ + (2592e^3 – 96$d^2 e^2$ – 258e +48d^2)$e^{11} x^4$-(1728e^4 + 1012e^2 284d^2e +94d^4-9)$e^{12} x^3$ +(432e^3 – 2160$d^2 e^2$ +792d^4e +118e +5d^2) $e^{13} x^2$ + (1296$d^2 e^3$ – 27e^2 +13d^2e-60d^4 – 4)$e^{14} x$ + (144d^4e-32d^6-3d^2) e^{15}=0 which is the simplest example that can require the constant term on the left hand side (6) to vanish which gives

$c = \frac{32d^4\ +3}{144d^2}$ ---(7)

Thus if d = ½ we find that Galois group of the irreducible polynomial 36 x^6+36 x^2 +18x +5 is a group of J and is solvable.

Example 4.6:

Let x^5 + ax +b E Q(x) (a≠0, b≠0) be an irreducible quntic trinomial with Galois group D5. "Then by separation and Williams, pg 987, 990)". There exist a rational number c($\geq$ 0), e(≠0) ($\pm$1), t(>0) such that

a= 5e^4 (3 – 4EC)/(c^2+1)

b= -4e^5 (11E + 2c)/(c^2 +1)

5(c^2 +1) =t^2

Moreover, any choice of C, e, E, t satisfying (3.1) gives an irreducible quntic trinomial with Galois group D_5 except C=11/2, e≠0, E= -1, t= 5/2

We now present a theorem together with it proof for the generalization of the solubility of selected polynomial in trinomial form of higher degree. $5 \leq n \geq 7$

Theorem 4.1

Suppose a and b are rational number such that the general form of a trinomial poly

$x^n + ax + b$ which is irreducible. Then the equation $x^n + ax + b = 0$ is solvable by radicals. If and only if there exist a rational number E(=$\underline{+}$1), c($\underline{>}$0) and e (≠0) such that a= $\frac{ne^{n-1}\,(n-2)-(n-1)Ec)}{c^{n-3}+1}$, b= $\frac{-(n-1)e^{n}\,(\,(2n+1)E+(n-3)c)}{c^{n-3}+1}$

In which case the root of $x^n + ax + b = 0$ are

$X_i = e\,(w^j u, + w^{2j} u_2 + \ldots + w^{nj} u_n)$ (j=0, 1,2,3,...,n)

where $w = \exp\,(\frac{2\pi i}{5})$ and

$u_1 = (\frac{v_1^2 v_n}{D^2})^{\frac{1}{n}}$, $u_2 = (\frac{v_3^2 v_4}{D^2})^{\frac{1}{n}}$, $u_3 = (\frac{v_2^2 v_1}{D^2})^{\frac{1}{n}}$, $u_4 = (\frac{v_4^2 v_2}{D^2})^{\frac{1}{n}}$,...., $u_n = (\frac{v_n^2 v_{n-2}}{D^2})^{\frac{1}{n}}$,

$$\begin{cases} v_1 = \sqrt{D} + \sqrt{D - \epsilon\sqrt{D},} & v_2 = -\sqrt{D + \epsilon\sqrt{D}} \\ v_3 = -\sqrt{D} + \sqrt{D + \epsilon\sqrt{D},} & v_4 = \sqrt{D} - \sqrt{D - \epsilon\sqrt{D}} \end{cases} ,...., u_n = \sqrt{D} - \sqrt{D - \epsilon\sqrt{D}}$$

where n is basically depending on the Galois group of the polynomial and it is good to note that an equation $x^5 + 2px + 2p^2 = 0$ is not solvable by radicals

Expressing the rational numbers c and e in the form, c =m/n and e= r/s where m, n, r, s are integers with gcd (m,n) = gcd(r,s)=1 and appealing to and (2a)

$$2p(m^2 + n^2)\, s^{n-1} = 5r^{n-1}\,(3n-4Em)n$$

$$2p^2\,(m^2 + n^2)s^n = -4r^n(11nE + 2m)n$$

If p is a prime = 3(mod4) and gcd(m,n)=1, p does not divide $m^2 + n^2$, and gcd(r,s) =1, p does not divide r.

The general quintic equation may, by elimentary operations [solutions of equations of a lower degree than the fifth] be transformed into $x^5 = gx$ +b, Where m is one of the numbers 5,6,7,… all these are included under the form $x^n = gx^m + \beta$ where n and m are positive whole numbers, prime to each other, and where n $>$ m.

Proof

Suppose $f_n(x)$ is a polynomial of the form $f_n(x) = x^n + ax + b$, we can extend Dummits formula by substituting the coefficients of the equation $f_n(x)$ to obtain a formula for $f_{n+1}(x) = x^{n+1} + ax + b$, or we call the equation $g_n(x) = x^{n+1} + ax + b$. If b is a fixed integer a$\neq$ 0, then the polynomial f is solvable by radicals for only finitely many integers a. When b is odd we can show that if the polynomial is irreducible and the same time then there is a need to construct a Galois group for it which is also solvable. This Galois group would be a subgroup of the group for all n, by symmetrization to help in forming the composition series putting into cognizance the complex roots.

Now let L denote the splitting field of f . Let r denote the unique rational root of the resolvent sextic of $x^5 + ax + b$ and we set

$c = \left[\frac{3r-16a}{4r+12a}\right]$, ϵ =sgn$\left(\frac{3r-16a}{4r+12}\right)$, e=$\frac{-5b\epsilon}{2r+4a}$

So that c is non negative rational number $\epsilon = \pm 1$, and c is non zero rational number, it is shown in (3) such that

$a = \frac{5e(3-4\epsilon c)}{c^2+1}$, $b = \frac{-4e^5(11\epsilon+2c)}{c^2+1}$

The Galois group G_r of f is the dihedral group D_5 of order 10 if $5(c^2+1)\epsilon$ Q^2 and is the Frobenius group F_{20} of order 20 if $5(c^2+1)\not\epsilon$ Q^2 If G_t= D_5 then has five subgroups of order 2, and one of order 5. The five quintic subfield of L are Q(θ_1), i=1,2,3,4,5

We can show that if the roots of equations are considered as function of the variable.

$\zeta = (-1)^{n-m} \frac{n^n}{m^m(n-m)^{n-m}} . \frac{\beta^{n-m}}{g^n}$, they are particular intergrals of higher hypergeometric differential equation of order n-1

$$\zeta^{n-2}(\zeta-1)\frac{d^{n-1}}{d\zeta^{n-1}} + \zeta^{n-3}(A_1\,\zeta - \beta_1)\frac{d^{n-2}}{d\zeta^{n-2}} + \cdots + (A_{n-2}\,\zeta - \beta_{n-1})\frac{dA}{d\zeta}$$

Where the Quantities A,B,C are constant. We can the group of this differential equation and consequently find how the roots vary and interchange around the critical point just as completely as in the case of the binomial equation. So far as it is known that they are the first group found where n-1> 3.

Using the Viera's Principles we can consider the indeterminate $y_1 y_2 \ldots y_n$ and let E = Q($y_1 y_2 \ldots y_n$) also let $P(x) = (x-y_1)(x-y_2)\ldots(x-y_n) \in E[x]$. Expanding P(x) out yields the symmetric function of y_i

$S_1 = y_1 + y_2 + \cdots + y_n$

$S_2 = y_1y_2 + y_1y_3 + \cdots + y_1y_n + y_2y_3 + \cdots + y_2y_n + \cdots + y_{n-1}y_n$

$\vdots$

$S_n = y_1y_2 \dots y_n$

So let F = Q($S_1\,, S_2, S_3, S_4, \dots S_n$) be field obtained by adjoining the symmetric functions to the rationals. Then the P(x) ∈ F[x] because $y_i{}'s$ are indeterminate. Every permutation σ in the symmetric on n letters S_n induces a distinct automorphism σ on E that leaves Q fixed and permutes the elements y_i. So the elements of the Galois group Gal(E/F) which means that $S_5 \subseteq$ Gal(E/F), but there may be an automorphism that may not be in S_5 . However the Galois group of the splitting field of a quintic polynomial has at most 5! Elements of P(x) showing that Gal(E/F) is isomorphic to S_5 . By generalization we show that the Galois group of every polynomial of degree n is isomorphic to S_n. The composition S_5 now becomes $S_5 \geq A_5 \geq \{e\}$, A_5 is the alternating group.

Proposition: For each non zero fixed integer b. There are only finitely many integer values of a for which polynomial is irreducible.

Proof: For each, the rational roots test allows only finitely many roots each of these is a factor of b. Each such roots allows only one value of a.

Now, assume f factors as $(x^n + ux^{n-1} + vx^{n-2} + s)(x^{n-1} + wx + t) = x^n + ax + b.$ By Gauss's Lemma, if it factors the factors have integer coefficients. Then we can deduced the following sets of equations:

(i) u + w =0

(ii) t + uv + v=0

(iii) $ut + vw + s=0$
(iv) $sw + tv=a$
(v) $st=a$

From (i) we have u = -w which we substituted into (ii) to get (ii) $v = w^2 - t$ substituting v and u in (iii) we get $-wt + (w^2 - t)w + s = 0$ from which we deduce the equation of the form

$$g(w) = w^3 - 2tw + s = 0$$

At most this has rational roots w, there is only one u, 1 and then by 2, there is only one v. By 4, we get a. Therefore, (s, t) yields at most 3 values of a. There are only finitely many (s, t) so this proves the result. In the particular case where b is 1 or an odd prime.

Though for the quintic equation $f(x) = x^5 + ax + b \in Q[x]$. Runge proves the following result. That if f(x) is irreducible and a≠0, then f is solvable by radicals if and only if there are s, t ∈ Q such that

$$a = \frac{312\,st^4}{(s-1)(s^2-6s+25)}, b = \frac{3125\,st^5}{(s-1)^4(s^2-6s+25)}$$

This result now produce the characterization proved by Spearman & Williams.

Let $f(x) = x^5 + ax + b \in Q[x]$ (a≠0,b≠0) be an irreducible quintic trinomial with Galois group D_5 there exist a rational number c(≥ 0), e(≠0),$\varepsilon(= \pm 1)$ t(> 0) such that

$$\left\{ \begin{array}{c} a = 5e^4(3-4\varepsilon c)/(c^2+1) \\ b = -4e^5(11\varepsilon + 2c)/(c^2+1) \\ 5(c^2+1) = r^2 \end{array} \right. \tag*{4.1}$$

Moreover any choice of c, e, ε, t, satisfying 4.1 gives an irreducicble quintic trinomial with Galois group D_5, except c=11/2, e$\neq$ 0,ε=-1, t=5/2, using Mapple we found that $g_1(x)$ and $h_1(x)$ are solvable by radicals.

Let Q denote the field of rational number and set Q^*=Q\{0}. Let a ϵ Q^* and b ϵQ^* be such that the quintic trinomial $f(x) = x^5 + ax + b$ is both irreducible and solvable. Polynomial of this type are characterized in (3).

But F = Q (x_1,.., x_5), with r= (123456)

l =K(l_1) = k (l_1, l_2, l_3, l_4) to say that k= K(θ)

That k= Q($S_1 \dots S_5$)

Galois group of L/K is cyclic of 4, it follows that l_1, $l_{2,}$ l_3, l_4 are the roots of a quartic over K which factor over K(Δ) into the product of two conjugae quadractics.

$$[x^2 + (T_1 + T_2\Delta)x + \left((T_3 + T_4\Delta)\right][x^2 + (T_1 + T_2\Delta)x + (T_3 - T_4\Delta)$$

Where $T_1, T_2, T_3, T_4 \in K$

The roots of one of these two quadratic factors are $\{l_1 e_4 (= e^2 l_1)\}$ and the roots of the other are conjugates $\{l_2 (= e l_1), e_3 (= e^3 l_1)\}$ for the specific l_i defined in equation

CHAPTER FIVE

DISCUSSION, CONCLUSION & RECOMMENDATIONS

5.1 Discussion

In example 4.1, consideration of the R_n as real numbers, and letting r_1 be the fifth root of R_1, we concluded that the correspondence r_2, r_3, and r_4 are the real fifth roots of $R_{2,}$ R_3 and R_4 respectively and then (3) gives the roots of $f(x)$. For example, the sum of the real fifth roots of $R_{1,}$ $R_{2,}$ R_3 R_4 above gives five times the (unique) real roots of $x^2 + 15x + 12$

In Example 4.2, this follows the Eisenstein. It has to use the resolvent sextic of f which aimed at simplifying the work for us. Having the rational root, the value for R are gotten in example 4.6.

In example 4.3 this does not give much stress, our rational values are clearly defined. The use of the Frobenins group F_{20} of order 20 was applied and the roots then becomes unique. Though the discriminant of the question was not clearly stated. Showing that its Galois group is solvable and so the equation is also solvable by radicals.

In example 4.4 a change in the sign of the constant term of the equation makes the whole work more complex. The basic concept of the Bring-Jerrard form was also applied to arrive at the expression of the roots.

In example 4.5 though this question speaks about cyclic native of the sextic but it goes with the fact that $x^n + ax + b$ = 0 can be solved by radicals: the resolvent equation was also used to ascertain the Galois group and the subgroup is to show its ability to be solve by radicals.

In example 4.6 concentrated on the choice of c,ϵ, E, of which it has great effect on the equation. The numbers are rational numbers having the Galois group to be D_5 of order 10. Some numerical values promoted the use of maple to in the end show that if r_1 and r_2 are any two roots of $x^2 - 5x + 12$, the other three roots is also given.

In example 4.7 the concept is basically the application of the rational numbers u and v. in such a way that the value for a and b are satisfied. This will lead us to the discriminant and subsequent parameterization representation of the formula.

5.1.1 Generalization:

Our analysis on the three sets of trinomial polynomial (Quntic, sextic and septic) show that we can generalize the formula and such generalisation can speak volumes of the solution to every polynomial of higher degree ($5\leq n \underline{>} 7$) that though they are irreducible, can be solvable by radicals. Hence we have $x^n + ax + b$ ($a\neq0$, $b \neq 0$) for ($5\leq n \underline{>} 7$). The following theorem would concretize our positions.

Suppose $g_1(x) = a_0 + a_1x + a_2 x^2 + a_3x^3 + a_4 x^4$ and $h_1(x) = b_0 + b_1 x + b_2x^2 + b_3 x^3 + b_4 x^4$

(4.3)

Where $a_0 = 20eE(4Ec-3)t/E$

$a_1 = 1/2+(2Ec+1)(Ec-7)t/E$

$a_2 = -E(2c^2 + 2Ec + 13)t/E$

$a_3 = (3Ec+4)(2Ec+1)t/2e^2E$

$a_4 = -Et^3/e^3E1$

b_0= -5e^2(2(4Ec-3)^2+(2Ec+1)(3Ec+4)/t)E

b_1=-eE((265+85Ec+110C^2)+55+10Ec)t)12E

b_2 = ((4Ec-3)(2c^2+2Ec+13)+(20Ec-15)t)12E

b_3 = -E(5(2Ec+11)(c^2+1)+(2Ec+1)(Ec-7)t)12E

b_4= (5(4Ec-3)(c^2+1)+(2c^2+2Ec+13)t)12c^{2}E

E= 4Ec^2-84c^2-37Ec-122

The polynomials g_2(x) and h_2(x) are formed from $g_1(x)$ and $h_1(x)$ by changing t to –t. taking c=2, e=-1, E=1, t=5, we obtain f(x) =x^5-5x +12. The above formula gives

g_1(x) = ¼ ($-x^4$- x^3- x^2+3 x +4)

h_1(x) = ¼ (x^4 – x^3+ x^3-5 x +8)

g_2(x)= ¼ (x^4+ x^3+ x^2+ x -4) (4.4)

h_2(x) = ¼ (-2 x^3-2 x -4)

thus if r_1, and r_2 are any two roots of x^5-5x +12 the other three roots are given by (4.3) with g, h, g_2, h_2 as in (4.4) the root of x^5-5x +12 in radical form are obvious.

In example 4.7, suppose x^6 +a x +b is irreducible over the rational numbers and suppose that a is non-zero. The Galois group of f(x) is isomorphic to the cyclic group of order 6. Let Ø be a root of f(x). Then L = Q (Ø) is a cyclic sextic field. By Galois theory L contains a cyclic cubic subfield. Therefore we can use of the following results.

Now suppose a and b are non zero rational numbers such that f(x) = x^{6} + ax +b is irreducible then f(x) defines a sextic field containing a cyclic cubic subfield if and if there exist rational number u and v such that

a = $4u(u^2 + 3)(3u^2+1)3u^2+25)^2u^5$

b = $(u^2-5)(3u^2+1)(u^4+10u^2+5)(3u^2 +25)^2u^6$

The polynomial discriminant of f(x) is equal to $-64(3u^2+1)5\ (3u^2+25)10\ (u^6-15u^4-225u^2-225)f(u)2v^3$,

$f(u) = 27u^{12} + 540u^{10} +6075u^8 +29600u^6 +20625u^4 +22500u^2 +5625 -3$ a and b can have the parametric representation given.

5.2 Conclusion

Having gone through the rigor, we have clearly seen, that testing the trinomial, quintic polynomials, the trinomial of the sextic polynomial, and the trinomial of the septic polynomial. All have proven that the equation $x^5 + ax + b = 0,\ x^6 + ax + b = 0$, $x^7 + ax + b = 0$ are irreducible polynomial but are all solvable by radicals, despite the facts of Abel- Ruffini’s theorem and the Galois Theory which says that any higher degree ($5\leq$n ≤ 7) polynomial can be solvable by radicals if and if only if its Galois group is solvable. The formulas have the same form and can share in approach to get its roots.

Therefore we conclude that the equation of the form $x^n + ax + b = 0$ can be used to generalized the trinomial of higher degree (5≤n≤ 7) polynomial equation. And so we prove it using a generalized theorem to cover for all values of n, 5≤n ≤7**.**

5.2.1 Contribution to Knowledge

Though Abel and Galois have proven and asserted that any polynomial of higher degree (5≤n ≤7) is not solvable by radicals. However, this research work identified the very few higher polynomials of degree (5≤n ≤7) in a special form, generalising such a form of the trinomial polynomial $x^n + ax + b = 0$, a≠0,b≠0 and finally proved a theorem following the argument. This has immensely contributed in the extension of the work of Galois and others and the entire modern algebra with the believe that other mathematicians can build on this research work.

5.3 Recommendations

I recommend that the equation of the form $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ (for the quintic) can also be tried for higher polynomials, 5≤n ≤7 to see it irreducible nature, and to show whether it can also be solvable by radicals or is there any means for generalization. Secondly, to show that the trisection of a generic angle is impossible can be investigated and be drawn conclusion accordingly as an extension of the work of Galois.

REFERENCES

Andrew Baker (2013). “*An Introduction to Galois Theory”* School of Mathematics and Statistics, University Of Gaslow (1997).

Artin, Emil (1998), *Galois Theory*. Dower Publication. ISBN 0-486-62342-4 (Reprinting of second review edition of 1944, the University of Notre.

Blair K. Spearman & Kenneth S. Williams (1996), Characterization of Solvable Quintics (PDF).

Broswell, C. And Glasser, M.L. (2005) Journal “*Solvable Sextic Equation*” Department of Mathematics and Computer Science, Clarkson University Potsdam NY13699-5820.

Cameron, Peter J. (1999) *Permutation Group* London Mathematical Society Student Texts, 45, Cambridge. University Press, ISBN 978-0-521-65378-7.

Vella, D. And Vella, A. ((2002). *Cyclic in Generalize Fibonacci Module A Prime*, Math, Mag. 75

Dummit, D.S. And Foote, R.M. (2014) *Abstract Algebra, 3rd Edition*. John Wiley and Sons Inc..

Dummit, D.S. (1999) *Solving Solvable Qunitic*, Mathematics of Competition Vol. 57, No. 195, July 1991 page 387-401.

E-Net, (2012) Google Search; Wikipedia. JSTOR. Question & Answer in Mathematics; Definition Subset Over (Non Standard) Finite Fields.

Euler, Leonhard (1984) [1765], “*Of A New Method of Resolving Equations of the Fourth Degree”*, Element of Algebra, Springer – Verlag, ISBN 978-1-4613-851)-0261 0557. 01014.

Fraliegh, J.B (1999); *A First Course In Abstract Algebra*, Addison Wesley ISBN 0201 335964

Gimba A.B.(2015), MTH 801: *Abstract Algebra* Lecture Note 2015/2016 Academic Session NSUK.

Jacobson, N. (1964) *Lectures In Abstract Algebra*, Vo. III, Van Nostrand, Princeton (1948)

Stillwell John (2010), “*Galois Theory For Beginners”*. The American Mathematical Monthly Vol. 101. No.1 (Jan 1994) Pp22-27.

King, B.R. (1996), *Beyond the Quartic Equation,* Birkhouser, Boston

Lazard, D. (1988). "Quantifier Elimination: Optional Solution For Two Classical Examples". *Journal Of Symbolic Computation* 5:261-266. Doi:101016 50747-7171(88) 80015-4.

Lee Si Ying and Zhaug De-Qi (2008) Solving Polynomial Equation By Radicals. Department Of Mathematics, National University Singapore, 2 Science Drive. 117543.

Martin, L. (1999). *The First Lecture In Italy On Galois Theory*; Bologna, 1886 1887, Historian Mathematics, 26, 201-223.

Mohammed A. Faggai And Daniel Lizard (2014) Solving Quintics And Septic By Radicals. National Grid, Dammam, Saudi Arabia. Upmc University Paris 06, Lip6, F-75005, Paris, France.

Morand, P. (1996) *"Field And Galois Theory"* Springer-Verlag, New York.

Neolle Felicia Adams (2010), *Galois and field extension*, Liberty University Spring

Pan Garrett and Robert B. Ash (2012). *"Introduction To Abstract Algebra".* Edited By National Mathematical Centre, Abuja – Lokoja Highway, Kwali, Abuja.

Postnikov, M. M. (2004) *Foundation* of *Galois Theory.* Dover Publication ISBN 0-486-4318-0.

Rees, E.L. (1922). "*Graphical Discussion of The Roots Of A Quadratic Equation".* The American Mathematical Monthly. 29(2) 31-55 Doi:102307/2972804. JSTOR 2972804.

Rotman J. (1998), *Galois Theory,* Springer – Verlag ISBN03879854

Ruchavendra G. Kulkarni (2008), Extracting The Root Of Septic By Polynomial Decomposition:, HMC Division, Bharat Electronic Ltd, Bangalore, India.

Stewart, I. (1980), Galois Theory: Chapman and Hall ISHN 041234550-1 *International Journal Of Pure And Applied Mathematics.* 71, 251 – 259.

Stricklan, N.P. (2009), Fields And Galois Theory, Cambridge University, University Press.

Sudhir R. Ghorpade (1994). *"Notes On Galois Theory".* Department Of Mathematics, Indian Statutete Of Technology, Bombay 40076 (Pdf).

Vander Wareden, Bartel Leendert (1991). *"The Galois Theory"* Equations Of The Second, Third, And Fourth Degrees", Algebra 1 (7th Ed). Springer – Verlag, ISBN 0-387-97 424-5, 26100048827.