ANALYZING GALOIS GROUP FOR CUBIC, QUARTIC AND QUINTIC POLYNOMIAL

An M.Sc. DISSERTATION SUBMITTED BY

ARCHANA MISHRA

410MA2092

Under the supervision of

Prof. K. C. PATI

May, 2012

DEPARTMENT OF MATHEMATICS

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

ROURKELA-769 008, ODISHA, INDIA

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

DECLARATION

I hereby certify that the work which is being presented in the thesis entitled "Analyzing of Galois group for cubic, quartic and quintic polynomial**"** in partial fulfillment of the requirement for the award of the degree of Master of Science, submitted in the Department of Mathematics, National Institute of Technology, Rourkela is an authentic record of my own work carried out under the supervision of Dr. K. C. Pati.

(ARCHANA MISHRA) Date:

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Dr. K. C. PATI
Professor, Department of Mathematics
National Institute of Technology
Rourkela – 769008
Odisha,India

ACKNOWLEDGEMENTS

I wish to express my deepest sense of gratitude to my supervisor Dr. K.C.Pati, Professor, Department of Mathematics, National Institute of Technology, Rourkela for his valuable guidance, assistance and time to time inspiration throughout my project.

I am very much grateful to Prof. Sunil Kumar Sarangi, Director, National Institute of Technology, Rourkela for providing excellent facilities in the institute for carrying out research.

I would like to give a sincere thanks to Prof. G.K. Panda, Head, Department of Mathematics, National Institute of Technology, and Rourkela for providing me the various facilities during my project work.

I would like to give heartfelt thanks to Mr. Biswajit Ransingh & Ms. Saudamini Nayak for their inspirational support throughout my project work.

Finally all credit goes to my parents and my friends for their continued support and to all mighty, who made all things possible.

ARCHANA MISHRA

TABLE OF CONTENTS

	Declaration
	Acknowledgements
	Abstract
Chapter 1	Introduction
Chapter 2	Preliminary
Chapter 3	Solvability by Radicals
Chapter 4	Galois Theory
Chapter 5	Working Results
Chapter 6	Conclusions
	References

ABSTRACT

The solvability by radicals is shown through the use of Galois theory. General polynomial of degree five or more are not solvable and hence no general formulas exist. Here we study the Galois group for solvability for cubic, quartic and quintic polynomials. The Galois group has a wide physical application in the field of theoretical physics.

Introduction:- Chapter-1

Let *p(x)* be the polynomial in *F*[*x*], where *F*[*x*] be the polynomial ring in *x* over *F*, Here *p(x)* is the polynomial. We shall associate a group with *p(x)*, is called Galois group of *p(x)*. There is a very close relationship between the roots of a polynomial and its Galois group.

The Galois group will turn out to be a certain permutation group of the roots of the polynomial. We can introduce this group will be through the splitting field *p(x)* over *F*, the Galois group of *p(x)* being defined as a certain group of automorphism of this splitting field. The duality is expressed in the fundamental theorem of the Galois theory, exists between the subgroups of the Galois group and the sub field of the splitting field.

The condition is derived for the solvability by means of radicals of the roots of polynomial terms of the algebraic structure of its Galois group.

For fourth-degree polynomials, which we shall not give explicitly, by using rational operations and square roots, we can reduce the problem to that of solving a certain cubic, so here too a formula can be given expressing the roots in terms of combinations of radicals of rational functions of the coefficients.

From this will follow the classical result of Abel that the general polynomial of degree 5 is not solvable by radicals.

Let F be a field of characteristic 0 or a finite field. If E is the splitting field over F for some polynomial in F[x], then the mapping from the set of subfields of E containing F to the set of

subgroups of Gal(E/F) given by K $\rightarrow \text{Gal}(E/K)$ is a one-to-one correspondence. Furthermore, for any subfield K of E containing F,

(1) [E:K] = |Gal(E/K)| and [K:F] = |Gal(E/F)| / |Gal(E/K)|. [The index of Gal(E/K) in Gal(E/F) equals the degree of K over F.]

(2) If K is the splitting field of some polynomial in F[x], then Gal(E/K) is a normal subgroup of Gal(E/F) and Gal(K/F) is isomorphic to Gal(E/F)/Gal(E/K).

(3) K = $E_{Gal(E/K)}$ [The fixed field of Gal (E/K) is K.]

(4) If H is a subgroup of Gal(E/F), then H =Gal(E/ E_H). The automorphism Group of *E*, fixing E_H *is H.*

we are assuming that all our fields are of characteristic 0, By an automorphism of the field *K* we shall mean, as usual, a mapping σ *K* onto itself such that $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\ \sigma\ (b)$ all $a, b \in K$. Two automorphisms *a* and τ of *K* are said to be distinct $\sigma(a) \neq \tau(a)$ for some element *a* in K.

Preliminary

Chapter-2

2.1 Group:-

A Group is a non-empty set G together with a binary operation ●

On the elements of G such that

(1) G is closed under ●

(2) ● is associative.

(3) G contains an identity element for ●.

(4) Each element in G has an inverse in G under ●.

Example:-

Z is a group under ordinary addition.

2.2 Identity:-

A group that only contains the identity element.

2.3 Identity element:-

An element that is combined with another element with a particular binary operation that yields that element.

2.4 Subgroups:-

Let $(G, ●)$ be a group. If H is a subgroup of G, then $H \subseteq G$ and H is a group under ●.

2.5 Permutation groups:-

A permutation of a set A is a function from A to A that is both one-one and onto. A permutation group of a set A is a set of permutations of A that forms a group under function composition.

2.6 Permutation:-

A permutation is a number of arrangements of n objects. The number of permutation of n objects is n!

2.7 Symmetric group:-

If X has n elements there are n! permutations of x and the set of all these with composition of mappings as the operation forms a group called the symmetric group of degree n denoted by S_n.

2.8 Isomorphism:-

Two groups are said to be isomorphic iff there exists a one-one, onto and homomerphism.

2.9 Normal subgroup:-

A group H is normal in a group (G,*), iff

$\forall\, g \in G, g * H = H * g,$

Denoted by $H \lhd G$

Every subgroup of abelian group is normal.

2.10 Ring:-

A ring R is a set with two binary operations, i.e. addition and multiplication. $\forall\, a,b,c \in F$

(1) $a+b=b+a$

(2) $(a+b)+c=a+(b+c)$

(3) There is an element $0 \in R$, s.t $a+0=a$

(4) There is an element $(-a)$ s.t $a+(-a)=0$

(5) $a(bc)=(ab)c$

(6) $a(b+c)=ab+ac$

Example:-

$z[x]$ of all polynomials under addition and multiplication is a commutative ring with unity $f(x)=1$

If a ring has a unity it is unique and if a ring has a inverse it is unique.

2.11 Subring:-

The subset of a ring R is a subring of R, if S is itself a ring with operation R.

Example:-

For each n >0, the set $nZ=\{\pm n,\pm 2n.....,\}$ is a subring of Z.

$\{0,2,4\}$ is the subring of Z_6, the integer modulo 6.

2.12 Characteristic of a Ring:-

The characteristic of a ring *R* is the least positive integer *n* such that $nx=0$ for all *x* in *R*. If no such integer exists, we say that *R* has characteristic 0. The characteristic of *R* is denoted by char *R*.

2.13 Integral Domain:-

A commutative ring with unity is said to be integral domain if it has no zero-divisors.

2.14 Zero-Divisors:-

A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Example 1:- The ring of integers is an integral domain.

Example 2:- The ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is an integral domain.

Example 3:- The ring $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ is an integral domain.

Example 4:- The ring $Z[x]$ of polynomials with integer coefficients is an integral domain.

2.15 Field:-

A field is a commutative ring with unity in which every nonzero element is a unit.

A finite integral domain is a field.

Example:-

Q is a field

2.15.1 General polynomial equation:-

An expression of the form

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

Where $a_n, a_{n-1}...., a_1, a_0$ are rational numbers and *n* is a nonnegative integer.

2.16 Irreducible Polynomial, Reducible Polynomial:-

Let *D* be an integral domain. A polynomial *f*(*x*) from *D*[*x*] that is neither the zero polynomial nor a unit in *D*[*x*] is said to be irreducible over *D* if, whenever *f*(*x*) is expressed as a product *f(x) = g(x)h(x)* , with *g*(*x*) and *h*(*x*) from *D*[*x*], then *g*(*x*) or *h*(*x*) is a unit in *D*[*x*].

A nonzero, nonunit element of *D*[*x*] that is not irreducible over *D* is called reducible over *D.*

Example 1:- The polynomial $f(x) = 2x^2 + 4$ is irreducible over *Q* but reducible over *Z* and is irreducible over *R* but reducible over *C.*

Example 2:- The polynomial $x^2 + 1$ is irreducible over Z_3 but reducible over Z_5.

Note:- Let *F* be a field. *If* $f(x) \in F[x]$ and *deg f*(*x*) is 2 *or* 3, then *f*(*x*) is reducible over *F* if and only if *f*(*x*) has a zero in *F*.

Let $f(x) \in Z[x]$. If *f*(*x*) is reducible over *Q*, then it is reducible over *Z*.

2.17 Irreducibility Tests:-

2.17.1 Irreducible polynomial:-

The polynomial $x^2 - 5$ is irreducible over Q . The roots of the polynomial are $\sqrt{5}$ and $-\sqrt{5}$ .These values are not within the field *Q* . Therefore, the polynomial cannot be reduced to a factored form with values from the field *Q*, but can be with the field $Q(\sqrt{5})$

2.17.2 Eisenstein irreducibility criterion:-

Lets

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

where the coefficients are all integers. If there exists a prime *p* such that: (i) *p* divides each of $a_0, a_1, ..., a_{n-1}$

(ii) *p* does not divide a_n and

(iii) p^2 does not divide a_0 ; then *f* is irreducible over Q

2.17.3 Field:-

Let F be a field and let *P(x)* be irreducible over F. $\{a + < P(x) > | a \in F\}$ is a subfield of *F[x]/<P(x)>* isomorphic to F.

2.17.4 Extension Field:-

A field *E* is an extension field of a field *F* if $F \subseteq E$ and the operations of *F* are those of *E* restricted to *F*.

2.17.5 Splitting Field:-

If K is a subfield of C and f is a polynomial over *K*, then f splits over K if it can be expressed as a product of linear factors.

$$f(t) = k(x-\alpha_1)..(x-\alpha_2)$$

Example:- Consider $f(x) = x^4 - x^2 - 2 = (x^2-2)(x^2+1)$ over *Q*. Obviously, the zeros of *f* (*x*) in C are $\pm\sqrt{2}$ and $\pm i$. So a splitting field for *f* (*x*) over *Q* is

$$Q(\sqrt{2}, i) = Q(\sqrt{2})(i) = \{\alpha + \beta i \mid \alpha, \beta \in Q(\sqrt{2}\}$$
$$= \{(a + b\sqrt{2}) + (c + d\sqrt{2})i \mid a, b, c, d \in Q\}.$$

Theorem:- *F(a)* $\approx$ $F[x]/\langle p(x)\rangle$

Let F be a field and let $p(x) \in F[x]$ be irreducible over *F*. If a is a zero of *p*(*x*) in some extension *E of F*, then *F*(*a*) is isomorphic to $F[x]/\langle p(x)\rangle$. Furthermore, if $\deg p(x) = n$, then every member of *F*(*a*) can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + ... + c_1 a + c_0,$$

where $c_0, c_1, ..., c_{n-1} \in F$.

Corollary:- *F(a)* $\approx$ *F(b)*

Let *F* be a field and let $p(x) \in F[x]$ be irreducible over *F*. If a is a zero of *p*(*x*) in some extension *E* of *F* and *b* is a zero *of p*(*x*) in some extension E' of *F*, then the fields *F*(*a*) and *F*(*b*) are isomorphic.

Example:- Consider the irreducible polynomial $f(x) = x^6 - 2$ over *Q*. Since $\sqrt[6]{2}$ is a zero of *f*(*x*), so that the set $\{1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6}\}$ is a basis for $Q(\sqrt{2})$ over *Q*. Thus,

$$Q(\sqrt[6]{2}) = \{a_0 + a_1 2^{1/6} + a_2 2^{2/6} + a_3 2^{3/6} + a_4 2^{4/6} + a_5 2^{5/6} \mid a_i \in Q\}.$$

This field is isomorphic to $Q[x]/\langle x^6 - 2\rangle$.

2.18 Degree of an Extension:-

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

Solvability by Radicals

Given the specific polynomial $x^2 + 3x + 4$ over the field of rational numbers F_0, from the quadratic formula for its roots we know that its roots are $(-3 \pm \sqrt{-7})/2$; thus the field $F_0(\sqrt{-7})$ is the splitting field of $x^2 + 3x + 4$ over F_0. Consequently there is an element $y = \sqrt{-7}$ in F_0 such that the extension field $F_0(\omega)$ where $\omega^2 = y$ is such that it contains all the roots of $x^2 + 3x + 4$.

From a slightly different point of view, given the general quadratic polynomial $p(x) = x^2 - 3x + 4$ over F, we can consider it as a particular polynomial over the field $F(a_1, a_2)$ of rational functions in the two variables a_1, a_2 over F; in the extension obtained by adjoining ω to $F(a_1, a_2)$. Here $\omega^2 = a_1^2 - 4a_2 \in F(a_1, a_2)$, We find all roots of $p(x)$.

There is a formula which expresses the roots of $p(x)$ in terms of a_1, a_2 square roots of rational functions of these.

For cubic equation $p(x) = x^3 + a_1x^2 + a_2x + a_3$ an explicit formula can be given, involving combinations of square roots and cube roots of rational functions in a_1, a_2, a_3. They are explicitly given by *Cardan's formulas:* Let $p = a_2 - \left(a_1^2/3\right)$ and $q = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + a_3$.

and let

$$P = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

$$Q = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{p^3}{27}} - \frac{q^2}{4}}$$

Then the roots are

$P+Q-(a_1/3), \omega p+\omega^2 Q-a_1/3$

and $\omega^2 P+\omega Q-a_1/3$, where $\omega \neq 1$

ω is a cube root of 1.

The above formulas only serve to illustrate for us that by adjoining a certain square root and then a cube root to $F(a_1, a_2, a_3)$, we reach a field in which *p(x)* has its roots.

For fourth-degree polynomials, which we shall not give explicitly, by using rational operations and square roots, we can reduce the problem to that of solving a certain cubic, so here too a formula can be given expressing the roots in terms of combinations of radicals of rational functions of the coefficients.

For polynomials of degree five and higher, no such universal radical formula can be given, for we shall prove that it is impossible to express their roots, in general, in this way.

If F be a field and polynomial $p(x) \in F[x]$ is solvable by radical over F

If we can find a finite sentence of fields $F_1 = F(\omega_1), ...F_k = F(\omega_k)$ s.t

$\omega_1^{n_1} \in F, ...\omega_k^{n_k} \in F_{K-1}$ s.t roots of $P(x)$ lies in F_k.

If K is ,the splitting field of *p(x)* over *F*, then *p(x)* is solvable by radicals over *F* if we can find a sequence of fields as above such that $K \subset F_k$.

$$P(x) = a_0 x^n + a_1 x^{n-1} + ...a_n = 0$$

By the general polynomial of degree n over *F*,

Let $F(a_1, ..., a_n)$

be the field of rational functions in n variables over F**.**

P(x) is solvable by radicals if it is solvable by radicals over *F*. *P(x)* involves combination of nth roots. For n≥5, Abel proved that this cannot be done.

Definition:- A group *G* is said to be *solvable* if we can find a finite chain of subgroups

$G = N_0 \supset N_1 .... N_K = (e)$

where each N_i is a normal subgroup of N_{i-1} and such that every factor group N_{i-1}/N_i is abelian.

In a field of group theory a solvable group is a group that can be formed from abelian groups using extensions. The word solvable arose from Galois theory and proof of the general unsolvability of quintic equation. Specifically equation is solvable by radicals, if corresponding galois group is solvable.

Galois Theory

Chapter-4

4.1 Automorphism:-

A one-to-one correspondence mapping the elements of a set onto itself, so the domain and range of the function are the same.

For example, $f(x) = x + 2$ is an automorphism on R but $g(x) = \cos x$ is not.

Let E be an extension field of the field F. An automorphism of E is a ring isomorphism from E onto E. The Galois group of E over F, Gal(E/F) is the set of all automorphisms of E that take every element of F to itself .

If H is a subgroup of Gal (E/F) is the set

$E_H = \{x \in E / \phi(x) = x \forall \phi \in H\}$ is called the *fixed field of H.*

The set of automorphisms of E forms a group under composition. The automorphism group of E fixing F is a subgroup of the automorphism group of E and for any subgroup H of Gal(E/F),the fixed field E_H of H is a subfield of E. The group Gal(E/F) is called Galois group of E over F.

Galois group is a certain type of field extension is a specific group associated with field extension. The study of field extension via Galois group is called Galois theory.

Galois showed that an equation of degree n, where n is an integer greater than or equal to 5, can' t in general be solved by algebraic means.

Galois developed the ideas of Lagranz , Abel, and introduced the concept of a group. He discussed the functional relationship among the roots of the equation showed the relationship have symmetries associated with them under permutations of the roots.

The operators that transform one functional relationship into another are the elements of a set, that is characteristics of the equation. The set of operators is called the Galois group of the equation.

4.2 Fundamental theorem of Galois Theory:-

Let *F* be a field 0 or of characteristic a finite field. If *E* is the splitting field over *F* for some polynomial in *F[x]*, then the mapping from the set of subfields of *E* containing *F* to the set of subgroups of Gal(*E/F*) given by $K \to \mathrm{Gal}(E/K)$ is a one-to-one correspondence. Furthermore, for any subfield *K* of *E* containing *F*,

(1) *[E:K]* = |Gal*(E/K)*| and *[K:F]* = |Gal*(E/F)*| / |Gal*(E/K)*|. [The index of Gal*(E/K)* in Gal*(E/F)* equals the degree of *K* over *F*.]

(2) If *K* is the splitting field of some polynomial in *F[x]*, then Gal(*E/K*) is a normal subgroup of Gal(*E/F*) and Gal(*K/F*) is isomorphic to Gal(*E/F*)/Gal(*E/K*).

(3) $K = E_{Gal(E/K)}$ [The fixed field of Gal (*E/K*) is *K*.]

(4) If *H* is a subgroup of Gal(*E/F*), then H =Gal(E/E_H). The automorphism Group of *E*, fixing E_H *is H.*

It is much easier to determine a lattice of subgroups than a lattice of subfields. For example, it is usually quite difficult to determine, directly, how many subfields a given field has, and it is often difficult to decide whether or not two field extensions are the same. Hence, the Fundamental Theorem of Galois Theory can be a great labor-saving device. Here is an illustration. If $f(x) \in F[x]$ and the zeros of $f(x)$ in some extension of *F* are $a_1, a_2, ...a_n$ then $F(a_1, a_2, ...a_n)$ is the splitting field of $f(x)$ over *F*.

4.3 Polynomial Equation:-

If *f(x)* is a polynomial,real or complex then *f(x)*=0 is called a polynomial equation. If *f(x)* is a polynomial of second degree then it is called a quadratic equation.

4.4 Root of Equation:-

The values of the variable satisfying the given is called its roots. $x=\alpha$ is a root of the equation $f(x) = 0$, if $f(\alpha)=0$. The real roots of an equation $f(x = 0$ are the x-coordinates of the points where the curve $y=f(x)$ crosses the x-axis.

4.5 Some results of an equation:

(1) An equation of degree n has n roots, real or imaginary.

(2) If $2+\sqrt{3}i$ is a root of a equation then $2-\sqrt{3}i$ is also the root of that equation.

(3) Every equation of an even degree, whose constant term is negative and the coefficient of the highest degree term is positive, has atleast two real roots, one positive and one negative.

4.6 Relation between roots and coefficients:-

4.6.1 Quadratic Equation:-

If α, β are the roots of the quadratic equation $ax^2+bx+c=0,$ then

$$\alpha+\beta=\frac{-b}{a}, \alpha\beta=\frac{c}{a}$$

If α, β, γ are the roots of the equation $ax^3+bx^2+c+d=0,$ then

$$\alpha+\beta+\gamma=\frac{-\mathrm{b}}{\mathrm{a}}, \alpha\beta+\beta\gamma+\gamma\alpha=\frac{c}{a}$$

$$\alpha\beta\gamma=\frac{d}{a}$$

4.6.2 Algebraic fields:-

An algebraic solution of the general nth degree polynomial is

$$a_0x^n+a_1x^{n-1}+.....a_n=0$$

If an finite number of operations is allowed, solutions of the general polynomial can be obtained using transcendental function.

A transcendental function is a function that does not satisfy a polynomial equation, whose coefficients are itself polynomial in contrast to algebraic function, which satisfy the given equation.

4.6.3 Algebraic equation:-

It is a equation that satisfy a polynomial equation whose Coefficients are themselves polynomial with rational coefficients.

Example:-

An algebraic function in one variable x is a solution y for an equation $a_n(x)y^n + a_{n-1}(x)y^{n-1} + ...a_0(x) = 0$

Here $a_i(x)$ are polynomial functions of x with rational coefficients. A function that is not algebraic is called transcendental function. The coefficient a_i necessarily belong to a field which is closed under rational operations.

If the field is the set of rational numbers we need to know whether or not the solution of the given equation belong to *Q*. So we extend the field from *Q* to Q'.

In cubic equation certain functions of the roots $f(x_1, x_2, x_3)$ are symmetric under permutations of roots. The symmetry operators form the Galois group of equation. For a general polynomial

$x^n + a_1 x^{n-1} + ...a_n = 0$

Functional relations of the roots are given in terms of the coefficients in the standard way.

$$x_1 + x_2 + ... + x_n = -a_1$$
$$x_1x_2 + x_1x_3 + ... + x_{n-1}x_n = a_2$$
.
.
.
$$x_1x_2.....x_{n-1}x_n = \pm a_n$$

Other symmetric functions of roots can be written in terms of the basic symmetric polynomials, in terms of coefficients.

Rational symmetric functions also can be constructed that involve the roots and the coefficients of the equations.

The galois group of an equation associated with a field F that has a property that if a rational functions of the roots of the equation is invariant under all permutations of Galois group then it is equal to a quantity in F.

Example:-

$$x^6 = \text{y}$$
$$\Rightarrow \text{y}^2 = 3$$
$$\Rightarrow y = \sqrt{3}$$
$$\Rightarrow x = \left(\sqrt{3}\right)^{\frac{1}{3}}$$

To solve the square and cube roots not sixth roots are necessary.

4.7 Invariant theory:-

It dealt with the description of polynomial function that do not change or are invariant under a trasformation from a given linear group.

4.8 Quintic function:-

It is a function of the form $g(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$.

Working Results

Chapter-5

5.1 Cubic Functions:-

Solving Cubic Equation:

Consider solutions of general cubic equation $Ax^3+3Bx^2+3cx+D=0,$ where $A-D$ are rational constants. If the substitution $Y=Ax+B$ is made, then the equation becomes $Y^3+3Hy+G=0,$ where $H=$ $AC\text{-}B^2, G=A^2D-3ABC+2B^3$.

The cubic has three real roots if $G^2+4H^3<0$ and two imaginary roots if $G^2+4H^3>0.$

The fourier series of $\cos^3 u$ is $\cos^3 u=(3/4)\cos u+(1/4)\cos 3u$.

Putting $Y=S\cos u$ in the equation $Y^3+3HY+G=0,$ gives

$$\cos^3 u+(3H/S^2)\cos u+G/S^3=0.$$

Comparing the Fourier series with this equation leads to

$$S=2\sqrt{(-H)} \text{ and } \cos 3u=-4G/S^3$$

If v is any value of u satisfying $\cos 3u=-4G/S^3$ the general solution is $3u=2n\pi\pm 3v,$ where n is the integer. Three different values of cos$u$ are given by

$$u=v \text{ and } (2\pi/3)\pm v.$$

The three solution of the cubic equation are then

$$S\cos v, \text{ and } S\cos(2\pi/3)\pm v$$

Consider solutions of the equation $x^3-3x+1=0,$

In this case $H=-1, G^2+4H^3=-3$

All the roots are real and they are given by solving

$$\cos 3u=-4G/S^3=-1/2$$

$$3u = \cos^{-1}\left(-1/2\right).$$

The values of u are therefore $2\pi/9, 4\pi/9, 8\pi/9$ and the roots are

$$x_1 = 2\cos\left(2\pi/9\right), x_2 = 2\cos\left(4\pi/9\right) \text{and } x_3 = 2\cos\left(8\pi/9\right).$$

5.1.1 Symmetries of the roots:-

The x_1, x_2, x_3 exhibit a simple pattern. Relationship among them can be found by writing in a complex form,

$2\cos\theta = e^{i\theta} + e^{-i\theta}$, where $\theta = 2\pi/9$,so that

$$x_1 = e^{i\theta} + e^{-i\theta}, x_2 = e^{2i\theta} + e^{-2i\theta}, x_3 = e^{4i\theta} + e^{-4i\theta}$$

Squaring this values gives

$$x_1^{\,2} = x_2 + 2, x_2^{\,2} = x_3 + 2, x_3^{\,2} = x_1 + 2$$

The relationships among the roots have the functional form $f\left(x_1, x_2, x_3\right) = 0.$

Other relationship exists.

Example: - sum of roots, i.e.

$$x_1 + x_2^2 + x_2 - 2 = 0$$
$$x_2 + x_3^2 + x_3 - 2 = 0$$
$$x_3 + x_1^2 + x_1 - 2 = 0$$

Transformations from one root to another can be made by doubling the angle θ.

The functional relationships among the roots have an algebraic symmetry associated with them under interchanges of roots.

If Ω is the operator that changes $f\left(x_1, x_2, x_3\right)$ into $f\left(x_2, x_3, x_1\right)$.

Then

$$\Omega f\left(x_1, x_2, x_3\right) \rightarrow f\left(x_2, x_3, x_1\right)$$
$$\Omega^2 f\left(x_1, x_2, x_3\right) \rightarrow f\left(x_3, x_1, x_2\right)$$
$$\Omega^3 f\left(x_1, x_2, x_3\right) \rightarrow f\left(x_1, x_2, x_3\right)$$

The operator $\Omega^3 = I,$ is the identity.

$$\Omega\left(x_1^{\,2} - x_2 - 2\right) = \left(x_2^2 - x_3 - 2\right) = 0$$
$$\Omega^2\left(x_1^2 - x_2 - 2\right) = \left(x_3^2 - x_1 - 2\right) = 0$$

5.1.2 The Galois group of an equation:-

The set of operators $\{I, \Omega, \Omega^2\}$ introduced above, is called the Galois group of equation $x_1 + x_3^2 + 1 = 0.$

The element of a Galois group are operators that interchange the roots of an equation in such a way that the transformed functional relationship are true relationship.

EX : - If the equation $x_1 + x_2^2 + x_2 - 2 = 0$ is valid, then so is

$$\Omega(x_1 + x_2^2 + x_2 - 2) = x_1 + x_2^2 + x_2 - 2 = 0$$

5.2 Quartic Functions:-

Lets consider group structure of quartic equation

$$Ax^4 + Bx^3 + Cx^2 + Dx + E = 0$$

Its solution can be found by means of following calculations.

$$\alpha = -3B^2/8A^2 + \frac{C}{A}$$

$$\beta = \frac{B}{8A^3} - \frac{BC}{2A^2} + \frac{D}{A}$$

$$\gamma = \frac{-3B}{256A^4} + \frac{CB^2}{16A^3} - \frac{BD}{4A^2} + \frac{E}{A}$$

If $\beta = 0,$ then

$$x = \frac{-B}{4A} \pm \sqrt{\frac{-\alpha \pm \sqrt{-\alpha^2 - 4\gamma}}{2}}$$

Otherwise

$$P = -\frac{\alpha^2}{12} - \gamma$$

$$Q = -\frac{\alpha^3}{108} + \frac{\alpha\gamma}{3} - \frac{\beta^2}{8}$$

$$R = -\frac{Q}{2} \pm \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}},$$

$$U = \sqrt[3]{R}\ ,$$

$$\mathrm{y} = \begin{cases} -\frac{5}{6}\alpha + U - \frac{P}{3U}, \text{if } U \neq 0 \\ -\frac{5}{6}\alpha + U - \sqrt[3]{Q}, \text{if } U = 0 \end{cases}, \quad w = \sqrt{\alpha + 2y}$$

$$x = -\frac{B}{4A} + \frac{w \pm \sqrt{-\left(3\alpha + 2y \pm {}^{2\beta}\!/_{w}\right)}}{2}$$

$$x_1 = \left(-a_2 + \mu/2\right)^{1/2}, x_2 = -x_1$$

$$x_3 = \left(-a_2 - \mu/2\right)^{1/2}, x_4 = -x_3$$

where $\mu = \left(a_2{}^2 - 4a_4\right)^{1/2}$

The field F of the quartic equation contains the rational Q and the rational expressions formed from the coefficients a_1 and a_2. The relations $x_1 + x_2 = x_3 + x_4 = 0$ are in the field.

Only of the 4! Possible permutations of the roots leave these relations invariant in F. they are $\mathrm{P}_1, ..., \mathrm{P}_8$. This is of the form

$$\mathrm{P}_1 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_1x_2x_3x_4 \end{Bmatrix}, \mathrm{P}_2 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_1x_2x_4x_3 \end{Bmatrix}, \mathrm{P}_3 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_2x_1x_3x_4 \end{Bmatrix}$$

$$\mathrm{P}_4 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_2x_1x_4x_3 \end{Bmatrix}, \mathrm{P}_5 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_3x_4x_1x_2 \end{Bmatrix}, \mathrm{P}_6 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_3x_4x_2x_1 \end{Bmatrix}$$

$$\mathrm{P}_7 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_4x_3x_1x_2 \end{Bmatrix}, \mathrm{P}_8 = \begin{Bmatrix} x_1x_2x_3x_4 \\ x_4x_3x_2x_1 \end{Bmatrix}$$

The set $\{\mathrm{P}_1 ..... \mathrm{P}_8\}$ is the Galois group of the quartic in F. It is a subgroup of set of 24 permutations. We can form an infinite number of true relations among the roots in F.

If we extend the field F by adjoining irrational expressions of the coefficients, other true relations among the roots can be formed in the extended field F'.

Ex : - The extended field formed by adjoining μ to F ,so that the relation $x_1{}^2 - x_3^2 = \mu$ are in F'.

$x_1^2 = x_2^2$ and $x_3^2 = x_4^2$, so $x_2^2 - x_4^2 = \mu$.

The permutations that leave these relations true in F', are $\{P_1....P_4\}$.

It is a sub group of the set $\{P_1....P_8\}$.

If we extend the field F' by adjoining the irrational expression $(-a_2 - \mu/2)^{1/2}$ to form the field F'', then the relation $x_3 - x_4 = 2(-a_2 - \mu/2)^{1/2}$ is in F''. This relation is invariant under the two permutations $\{P_1, P_3\}$.

If we extend the field F'' by adjoining the irrationals $(-a_2 + \mu/2)^{1/2}$ to form the field F''', then the relation $x_1 - x_2$ is in F'''.

This relation is invariant under the identity transformation P_1, alone. The full group and the sub group associated with the quartic equation are of the order 24, 8,4,2,1. The order of full group divided by order of sub group is called index of the sub group.

Galois introduced the idea of normal or invariant sub group.

For a general polynomial:

$$x^n + a_1 x^{n-1} + ...a_n = 0$$

Functional relations of the roots are given in terms of the coefficients in the standard way

$$x_1 + x_2 + ... + x_n = -a_1$$
$$x_1x_2 + x_1x_3 + ... + x_2x_3 + ..x_{n-1}x_n = a_2$$
$$x_1x_2x_3 + ... + x_{n-2}x_{n-1}x_n = -a_3$$
.....
.....
$$x_1x_2x_3.....x_{n-1}x_n = \pm a_n$$

Other symmetric functions of the roots can be written in terms of these basic symmetric polynomials and so in terms of coefficients. Rational symmetric functions also can be constructed that involve the roots and the coefficient of given equation.

Application :-

Events of finite extension and duration are the part of physical world. It will be convenient to introduce the notion of ideal events that have neither extension nor duration. Ideal events may be represented as mathematical points in a space time geometry.

5.3 Quintic Functions:-

Generally, 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 1:- An irreducible polynomial $f(x)$ defined over a field *F* of characteristic zero (e.g. $F = Q, R$) is solvable by radicals if and only if the *Galois group* $Gal(E/F)$ of the *splitting field* E of the polynomial z is a solvable group [1], [2].

Let $y_1,...y_5$ be independent transcendental elements over the field Q of rational numbers. Consider

$f(x) = (x - y_1)..(x - y_5) = x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5$.

By Vieta's formula, we know that

$s_1 = y_1 + \cdots + y_5, s_2 = y_1y_2 + \cdots + y_4y_5, ..., s_5 = y_1y_2y_3y_4y_5,$

are elementary symmetrical functions in y_i . Thus $f(x)$ is a polynomial defined over the field $F = Q(s_1,...,s_5)$ .We now show that this $f(x)$ is not solvable by taking radicals.

Set $E = Q(y_1,...,y_5)$. Then the polynomial $f(x)$ in $F[x]$ has E as its splitting field.

Suppose on the contrary that $G = Gal(E/F)$ is solvable for the above polynomial $f(x)$ of degree five.

Consider the composition series of subgroups from $G = G_0$ to $G_r = 1$:

$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r-1} \triangleright G_r$.

This corresponds to the following extension of fields:

$F = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r$.

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:

$S_5 \triangleright A_5 \triangleright 1$.

Thus $Gal(E/F)$ is not solvable. Hence $f(x)$ is not solvable by radicals by Theorem 1.

5.3.1 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 many cases of quintics which are solvable by radicals. A case will be discussed below.

5.3.2 Cyclotomic Polynomials

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

By Theorem 1, we know that a polynomial is solvable if and only if its Galois group is solvable. This equation is solvable in radicals as its splitting field is generated by the 5th roots of unity, so the resultant Galois group is also solvable.

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

$w_k = e^{\frac{2\pi ik}{5}}$,

where $k \in \{0,1,2,3,4\}$.

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

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

Conclusions

Chapter-6

Polynomials and the solving of its roots have practical and widespread use in computer applications, the foremost of which is cryptography, or the encryption of sensitive data for sending over the internet. This is especially useful in banking transactions where secrecy and privacy of the individual customer is paramount. Polynomials can be used in public key encryption, as a means to encrypt information. The decryption of a polynomial is hence directly linked to the solvability of this polynomial. Only those with the required decryption key will get to know the real message behind the encrypted message. Being able to solve for a polynomials roots will enable one to create a decryption key, and hence solvability or the lack thereof of such a polynomial, is important in choosing a polynomial as a possible encryption key so that it cannot be hacked.

References:-

1. Gallian Joseph A., Contemporary Abstract Algebra, Seventh edition, Richard Stratton (2008)
2. Herstein I. N., Topics in Algebra, Second edition, John wiley & sons(1975)
3. Artin, M.,Algebra, Prentice-Hall Inc.(1991).
4. Fraleigh, J.B., A First Course in Abstract Algebra, Addison- Wesley(1997)