ISSN: 2285-2071
Volume 10, Number 1, 2022
International Journal of Physical Science Research

ON GALOIS THEORY AND ITS APPLICATION TO SOLVABILITY OF POLYNOMIALS BY RADICALS

[1]Bukar Yusuf and [2]Ibrahim Mohammed Dibal
[1&2]Department of General Studies, The Federal Polytechnic Damaturu, Yobe State, Nigeria

ABSTRACT

It has been found that Galois Theory can be used to determine the solvability of polynomials over a field by radicals. This paper attempts to explore this theory with a view to apply it for the solvability of polynomials by radicals. Basic facts about basic algebraic structures such as normal groups quotient groups as well as solvable groups will be collected. Field extension especially normal extension and separable extension are of significant for our study. Galois group of a polynomials is defined and ways of determining it are given. Finally we shall focuses on the solvability of polynomials by radicals. Some general results in this direction are collected.

Keywords**: **Groups, Galois Theory, Solvability of Polynomials, Solvable Group, and Field Extension.

INTRODUCTION

Solution of polynomials plays fundamental role in the solution of many physical problems. Here we shall discuss some basic concepts needed for our study, especially the solvability of polynomials by radicals. However, we shall collect most of the preliminary results on the algebraic structure such as groups, rings and fields. Our main focus shall be on the groups, especially the concept of solvable groups shall be explore in more details as it plays an important role in our field of study.

1.1 Group

A group is an ordered pair $(G, *)$, where G is a non-empty set, $*$ a binary operation defined on G, satisfying the following condition:

i. Closure :$\forall\, a, b \in G,\ \ a * b \in G.$

ii. Associativity: $\forall\, a, b, c \in G,\ \ a * (b * c) = (a * b) * c.$

iii. Identity element:There exists an element $e \in G \text{ such that } for \text{ all } a \in G,$
$a * e = e * a = a.$

iv. Inverses: For every aϵ G, there exists an element $a^{-1}\epsilon$ G, called the inverse of 'a' such that
$a * a^{-1} = a^{-1} * a = e.$

Note: In addition if $\forall$ a , b $\in G\ \ a * b =$ b $*$ a, we call the group Abelian

.

SUBGROUPS

A non-empty subset H of a group G is called a subgroup of G if H is itself a group with respect to the $binary\ operation\ of\ G\ induced\ on\ H.$

Obviously, for any group G, we have two trivial subgroups that is the group G itself and the set {e}. Any other subgroup of G, if it exists is called a non-trivial subgroup of G.The following theorem is a very useful characterization of subgroups.

THEOREM: 1.1

A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup of G that is that for all a, b $\in H\ \ a^{-1} \in H.$

PROOF

Let the condition be satisfied. Then for any a $\in H, we\ have\ aa^{-1} \in$ any a, that is e $\in$ H. now for any a$\in H, e\ a \in H \Rightarrow aa^{-1} \in H. further, a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a\,(b^{-1})^{-1} = ab \in H. the\ only\ axiom\ which\ remains\ to\ be\ satisifed\ in\ order\ that\ H\ is\ a\ subgroup\ of\ G\ is\ the\ associativity.$

But the same element shows this property in G. Thus they will exhibit it in H as well.

NORMAL SUBGROUPS

A subgroup H of a group G is called a normal subgroup if for each g∈ G and h∈ H, $g^{-1}hg$ in g∈ H, or equivalently, if Hg = gH.

Let G be a group and H be a normal subgroup of G. Let us denote by $\frac{G}{H}$ the set of all the cosets of H in G. Thus $\frac{G}{H}$ = {Hg : g ∈ G}. On $\frac{G}{H}$ we define a binary operation as follows: For each Ha ∈ $\frac{G}{H}$, let Ha : Hb = Hab.

It can be easily seen that under this operation, $\frac{G}{H}$ forms a group. The closure axiom is obvious; the associativity is thrown back to the associativity in G. The identity element is He or simply H, and the inverse of Ha for instance is Ha^{-1}, where a^{-1} is the inverse of a in G. We call this group the factor or quotient group of the group G determined by H. of order 6

As an example , consider a cyclic group G of order 6, namely

$G = \{ e, a, a^2 a^3 a^4 a^5 \}$.

The two normal sub groups of G are

$H = \{ e, a^2, a^4 \}$ and $K = \{ e, a^3 \}$

Now the elements in the factor groups $\frac{G}{H}$ are the cosets of H, namely

$\frac{G}{H} = \{ \{ e, a^2, a^4 \}, e, \{ a, a^3, a^5 \} a \}$

$= \{ \{ e, a^2, a^4 \} , \{a, a^3, a^5 \} \}$

It is obvious that the above set of cosets forms a group with respect to the multiplication of cosets as defined earlier. It then also be seen that $\frac{G}{H}$ is also cyclic with $\{a, a^3, a^5 \}$ as the generator. Similarly, we can find the elements of $\frac{G}{K}$.

It can be seen immediately that if the order of G is n and the order of h is m, then the order of $\frac{G}{H}$ is $\frac{n}{m}$, which is the index of H in G, denoted by [G : H].

SOLVABLE GROUPS

We first give the following definitions.

SUBNORMAL SERIES

A sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq - - - G_\lambda = e \quad \_\_\_\_\_ \quad (1)$$

of a group G is called a subnormal series og G, if G_{i+1} is a normal subgroup of G_i ∀ I = 0, 1, 2, …, λ – 1. The factor group $\frac{G_i}{G_{i+1}}$ are called the factor groups of the subnormal series. Further if each G_i is a normal subgroup of G itself, then the series is said to be a normal series of G.

SOLVABLE GROUPS

A group G is said to be solvable if it has a subnormal series.

$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq - - - \supseteq G_s = (e)$

Such that each of its factor groups G_i/G_{i-1} is an Abelian group. The above series then is referred to as a solvable series of G.

EXAMPLE 1

Any Abelian group G is solvable. Now G ⊇ (e) is a normal series of G and its only factor group is G/{e}, which being isomorphic to G, is commutative.

EXAMPLE 2
Consider the series $S_3 \supseteq A_3 \supseteq \{I\}$, its factor groups are S_3/A_3 and $A_3/\{I\}$ which are of is normal in order 2 and 3, respectively. Since any group of prime order is commutative, it follws that both the factor groups are commutative. Hence S_3 is solvable.

EXAMPLE 3
Consider $S_4 \supseteq A_4 \supseteq V_4 \supseteq \{I\}$ is a subnormal series of S_4, where $V_4 = \{I, (12)(34), (13)(24), (14)(23)\}$. Its factor groups are S_4/A_4, A_4/V_4 and $V_4/\{I\}$, which are of orders 2 , 3 and 4, respectively. Since every group of order 4 is Abelian, it follows that all the factor groups are Abelian, hence S_4 is solvable.

THEOREM 2.1
Any Subgroup H of a solvable group G is solvable.

PROOF
Let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 \supseteq \text{- - -} \supseteq G_n = (e)$$

be a solvable series for G. We claim that

$$H = H_0 \supseteq (H \cap G_1) \supseteq (H \cap G_2) \supseteq \text{- - -} \supseteq H \cap G_n = (e) \quad \text{(2)}$$

Is a solvable series for H. Since for I = 0, 1, 2, . . ., n, G_{i+1} is normal in G_i, we get $H_{i+1} \cap G_{i+1}$ is normal in $H_i = H \cap G_i$. Define a mapping $f : H_i \to \frac{G_i}{G_{i+1}}$ such that $f(x) = xG_{i+1}$ $\forall$ x $\in H_i$, f is a homomorphism. Further x ε Kerf $\Leftrightarrow xG_{i+1} = G_{i+1}$

$$\Leftrightarrow x \in G_{i+1}$$
$$\Leftrightarrow x \in H \cap G_{i+1}, \text{ since } x \in H_i \subseteq H.$$

This yields that Kerf $= H \cap G_{i+1} = H_{i+1}$, hence by the Fundamental Theorem of homomorphism $\frac{H_i}{H_{i+1}} \cong f(H_i)$ as (H_i) is a subgroup of $\frac{G_i}{G_{i+1}}$ and $\frac{G_i}{G_{i+1}}$ is Abelian. $f(H_i)$ is also Abelian. Consequently $\frac{H_i}{H_{i+1}}$ is Abelian, this proves that (1) is a solvable series for H, hence H is a solvable group.

THEOREM 1.2
If H is a normal subgroup of a solvable group G, then $\frac{G}{H}$ is also solvable.

PROOF
Let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 \supseteq \text{- - -} \supseteq G_n = (e)$$

be a solvable series for G. Consider the series

$$\frac{G}{H} = \frac{G_0}{H} \supseteq \frac{G_1 H}{H} \supseteq \frac{G_2 H}{H} \supseteq \text{- - -} \supseteq \frac{G_n H}{H} = (e)$$

For each I = 0, 1,2, …,n, n -1, G_{i+1} is normal in G_i. Consider any $x \in G_i H$ then $x = gh$ for some $g \in G_i$, $h \in H$.

Thus
$\times G_{i+1} H = gh\, G_{i+1} H$
$= ghH\, G_{i+1}$ (since for any subgroup k of Gi HK = KH)
$= g\, G_{i+1} H$ (since hH = H)
$= G_{i+1} gH = G_{i+1} ghH$ (since $G_{i+1} \Delta$ Gi, and $g \in G$)
$= G_{i+1} Hgh = G_{i+1} H\times$.

This proves that $G_{i+1} H$ is a normal subgroup of $G_i H$.

Hence $\frac{Gi\, H}{Gi+1} \cong \frac{\frac{Gi\, H}{H}}{\frac{Gi\, H}{H}}$ (3)

Now define f: $G_i \rightarrow \frac{Gi\ H}{Gi+1\ H}$ such that

$F(\times) = G_{i+1} H\times \forall \times \in Gi.$
Then f is homomorphism as $G_iH = H\ G_i$ given $y \in GiH$, we can write $y = hg$ for some $h \in H, g \in G$, then
$G_{i+1} Hy = G_{i+1} Hgh = G_{i+1} Hg = f(g).$
This shows that f is also onto clearly $G_{i+1} \subseteq ker$ f, and hence induces a homorphism.

$\overline{f}: \frac{Gi}{Gi+1} \rightarrow \frac{Gi\ H}{Gi+1\ H}$

Such that
$\overline{f}: (G_{i+1} x) = G_{i+1} Hx \forall x \in G_i.$

This $\overline{f}: is\ also\ onto. thus\ \frac{Gi\ H}{Gi+1\ H}$ is a homorphic image of the Abelion group $\frac{Gi}{Gi+1}$,
So that it must be itself Abelian. Consequently each factor group of the subnormal series (I) is Abelian. This proves that G/H is solvable.

RINGS

A ring consists of a set R on which are defined binary operations of addition and multiplication satisfying the following axioms.

(i) X + y = y + x for all elements x and y of R
(ii) (x + y) + Z = x + (Y + Z) for all elements x,y, and z of R (i.e. addition is associative).
(iii) There exists an element 0 of R (known as the zero element) with the property x + (-x) = 0
(iv) X(y z) = (x y) for all elements x, y, and z of R (i.e. multiplication is associative).
(v) X(y + z) = xy + xz and (x + y)z = xz + yz for all elements x, y and z of R (the distributive law)

Field

A field consists of a non-empty set K on which are defined binary operations of addition and multiplication satisfying the following axioms.

(i) X + y = y + x for all elements x and y of K (i.e. addition is commutative)
(ii) (x + y) + z = x (y + z) for all elements x, y and z (i.e. addition is associative)
(iii) There exist an element O of K known as the zero element with the property that x + 0 = x for all element –x of K.
(iv) Given any element x of k, there exists an element –x of k with the property that x + (-x) = 0;
(v) Xy = yx for all element x and y of k (i.e. multiplication is commutative)
(vi) X(yz) = (xy) for all element x, y and z of k (i.e. multiplication is associative)
(vii) There exist a non-zero element 1 of K with the property that 1x = x for all element x of K.
(viii) Given any non-zero elelemnt x of k, there exist an element x^{-1} of k with the property that $xx^{-1} = 1$;
(ix) X(y+z) = xy +xyz and (x+y)z = xz + yz for all elelement x, y and z of k (the distrib utive law).

An examination of the relevant definitions shoiws that a genital commutative ring R is a field if and only if, given any non-zero element x of R, there exists an element x^{-1} of R such that $xx^{-1} = 1$.
Moreover, a ring R is a field if and only if the set of non-zero elements of R is an Abelian group with respect to the operation of multiplication.

POLYNOMIAL RINGS

In this section we shall discuss the polynomial rings. The polynomials that we studied at O'level were special polynomials, which were usually taken over the ring of integers. But here we shall discuss the polynomials which may be taken over an arbitrary ring. Since our intention is to find the solution of polynomials by radicals, we shall deliberate only on the related topics in polynomials.

POLYNOMIALS OVER A RING

Let R be a ring. Polynomials in an indeterminate x with coefficients in the ring R is an expression f(x) of the form.

$F(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots\ldots\ldots,$

where the coefficients $a_0, a_1, a_2, \ldots\ldots\ldots$ of the polynomials are element of the ring R and only finitely many of these coefficients are non-zero. If $a_k = 0$ then the term $a_k x^k$ may be omitted when writing down the expression defining the polynomials. therefore every polynomials can be represented by an expression of the form.

$F(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots + a_m x^m$

And we call it a polynomial of degree m if $a_m \neq 0$, and a_m is referred to as the leading coefficient of the polynomials.

We see from the definition of a polynomials that a polynomials with coefficient in a ring R determines and is determined by an infinite sequence $a_0, a_1, a_2, \ldots\ldots\ldots$ of elements of the ring R, where a_k is the coefficient of x^k in the polynomials. An infinite sequence $a_0, a_1, a_2 \ldots\ldots\ldots$ of elements of R determines a polynomials $a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots$.., if and only if the number of values of k for which $a_k \neq 0$ if the polynomials in the usual fashion. Thus if

$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots,$

And

$g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \ldots,$

then

$f(x) - g(x) = (a_0 + b_0) + (a_1 + b_1) + (a_2 + b_2) x^2 + (a_3 + b_3) x^2 \ldots$

and

$f(x)\, g(x) = V_0 + V_1 x + V_2 x^2 + V_3 x^3 + \ldots$

where , for each integer I, the coefficient V_i of x^i in f(x) g(x) is then sum of the products $a_j b_k$ for all pairs (j, k) of non – negative integers satisfying $j + k = i$. (thus $V_0 = a_0 b_0, V_1 = a_0 b_1 + a_1 b_0, V_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$ e.t.c). straight forward calculations shows that set R(x) of all polynomials over a ring R forms a ring with respect to the addition and multiplication of polynomials. The zero element this ring is the polynomials whose coefficient are all equal to zero.

Field extension

A field E containing a field F is called an extension field of F (or simply an extension of F). such an E can be regarded in an obvious fashion as an F-vector space. We write (E:F) for the dimension, possibly infinite, of E as an F-vector space, and call (E:F) the degree of E over F. we often say that E is finite over F when it has finite degree over F.

Example 1.

(a) The field of complex number C has degree 2 over R (basis (I,i))
(b) The field of real numbers IR has infinite degree over Q – because Q is countable, verey finite dimensional Q-vector space is also countable, but famous argument of cantor shows that R is not countable, more explicitly, there are specific real numbers x, for example π where powers 1, x, x^2, … are linearly independent over Q.

FUNDAMENTAL THEOREM OF GALOIS THEORY

Let us first take some definitions.

Splitting field of a polynomials let f(x) be a polynomial over a field F. we say that an extension K:F is the splitting field of F(x) over F if F(x) splits over K, but not over any proper subfield of k, into linear factors. In other words, the splitting field of F(x) is the smallest extension of F containing all roots of f(x).

FIXED FIELD

Let G be a subgroup of the group A (K) of all automorphisms of field k. then the fixed field of G, written k_G , is the set of all elements a$\in k$ such that $\delta\,(a) = a\ for\ all\ \delta \in G$.

GROUP OF F-AUTOMORPHISMS

The subset of the set of all automorphisms A(K) of a field K containing all those automorphisms of K which keep the element of F fixed is denoted that it is a subgroup of A(K). We call it the group of F-automorphisms of K.

NORMAL EXTENSIONS

An extensions k of a field F is called a normal extension if the fixed field of G(K,F) is F.

Theorem
Let k be a finite normal extension of a field, F. if E is any subfield of K containing F then k is also a normal extension of E.
PROOF.
Since k is a finite normal extension of f, there exist a polynomials f (x) over f such that k is also a splitting field of F(x) over E. hence k is a normal extension of E.
SEPARABLE EXTENSION
an element a is an extension k of F is called separable over f if it satisfies a polynomial over F having no multiples roots.
An extension k of a field f is therefore a separable extension if each element of k separable over f.
GALOIS EXTENSION
A field extension is said to be Galois extension if it is finite, normal and separable.

FUNDAMENTAL THEOREM F GALOIS THEORY
Let k be a finite normal extension of a field f of characteristic zero an let G(K,F) be the Galois group of k over f. then the correspondence E ↔ G (K,F) where E is a subfield of k containing F is 1-1 between the family of the subfield of k containing f and the family of sub-group of G (k,f) satisfying the following conditions.
Given any subfield E of K containing f and subgroup H (k,F).

i. $E = K_{G(k1\ E)}$
ii. $H = G\ (K_1\ K_H)$
iii. (K:E) =0 (G (k,E)) and (E:F) = index of G (k,E) in G (k,F).
iv. E is a normal extension of f if and only if and only if G (K,E) is normal subgroup of G (K,F).
v. When E is a normal extension of F, then G (E,F) is Isomorphic to $\frac{G\ (k,F)}{G\ (k:F}$

Proof
Since k is a finite normal extension of F and F $F \subseteq E \subseteq$K, we get that K is a finite normal extension of E, so E is same as the fixed $K_{G(K,\ E).}$ thus (i) follows
By definition, k_H = (x E K / $\delta\ (x) = \forall\ \delta\ \in H$) each $\delta \in H$ is a K_H automorphisms of k, so that H $\subseteq G\ K_1$ K_H). However, $\delta\ (H)$ = (K: K_H). At the same time as k is a normal extension of K_H given that K_H is the fixed field under G (K_1 K_H) so (K : K_H) = 0 (G (K_1 K_H)). Thus
0H = 0 (G (K_1 K_H) and consequently H= G (K_1 K_H), this proves (ii)
Now as K is a normal extension of E, then (K:F) = 0 (G (K, E) thus
0 (G (K,F)) = (K:F) = (k:E) (E:F)n = 0 (G (k, E)) (E:F) gives
(E : F) = $\frac{0(G\ (\ K,F)\ )}{0\ (\ G\ (K,E\ ))}$
This proves (iii)
Let E be a normal extension of F. consider any a$\in E$, then the splitting field of the minimal polynomial of a over F is contained in E. that gives every conjugate of a over F in K again in E. since for any $\delta\ \in$ $G\ (\ K,F), \delta\ (a)$ is a conjugate of a, we have $\delta\ (a)\ \in E$ thus for any y$\in G\ (K,E), y\ (\delta\ (a) = \delta\ (a)\ )$ and hence $(\delta - y\ \delta\ )\ (a) = a$, this proves $\delta^1\ \delta\ \in G\ (k,E)$. consequently, G (K,E) is a normal subgroup of G (K,F).
Conversely let G (k, E) be normal subgroup of G (K,F). Consider a $\in E\ as\ K\ is\ a$ normal extension of F, K contains a splitting field say L of the minimal polynomial P(x) of a over F. consider any. Root of P(x) in L. then b is a conjugate of a over F, so there exist an F-automorphisms δ of k such $\delta\ (K,E)$. however, E is the fixed field under G (K,E). this gives that b = δ^1 (a) E K hence L $\subseteq E$. this proves that E is a normal extension of F. Hence (iv) is proved.
Let E be a normal extension of F, now E = F (a) for some a $\in E$ for any $\delta \in G\ (K,F) let\ \delta_E$ denotes the restriction of $\delta\ to\ E\ since\ \delta(a)\ \in E, we\ get\ \ \delta\ (E)\ \subseteq E\ as\ (\ \delta\ (E):F\ ) = (E:F), we\ get\ \ \delta\ (E) = E, hence\ \delta_E$ is an F-automorphisms of E and so $\delta_E\ \in G\ (E:F)$. define a mapping λ : G (k,f) → G by (E,F) by $\lambda = (\delta)\ \delta_E\ \in \forall\ \delta\ \in (G\ K,F)$ clearly for any δ, n $\in G\ (K,F)$, $(\delta_n)_E = \delta_E\ n_{E.}$ However

λ *is a group hormophisms*. consider any Y (E, F). now , $\delta(a)$*is a conjugat* of a over F. thus there exist an F – automorphisms δ *of k such that* $\delta(a) = Y(a)$. *further* as δ and Y are both identical on F and E is generated by a over F. we get $\delta(x) = Y(x) \forall x \in F(a) = E$ *i.e.* $Y = \delta_E = \lambda(a)$. This proves λ *is* onto mapping . hence G (E,F) $\cong G(K, F$. now δ_E ker λ *if and only if* δ_E ker λ is e and only if only on E i.e. if $\delta(x) = x \forall x \in E$ i.e. if and only if δ_E G (K,E) hence Ker λ = G (K,E) and we obtain

$$G(E,F) \cong \frac{G(G,F)}{G(K,E)}.$$

This proves (V), hence the theorem is proved.

SOLVABILITY OF POLYNOMIALS BY RADICALS

In much of what we have done so far in previous discussions the solution and application of Galois theory to the solvability of polynomials by radicals has been at the back of our minds.

Here we shall discuss an application of Galois Theory to the solvability of polynomials by radicals. But first we give an example to illustrate the use of fundamental theorem of Galois theory.

Example 1.

Consider f (x) = $x^4 - 5x^3 + 6$

Since f (x) = $(x^2 - 3)(x^2 - 2)$, $\pm\sqrt{3}$ *and* $\pm\sqrt{2}$ are roots of (x) . the splitting field k of f(x) over Q is K = Q ($\pm\sqrt{2}$, $\pm\sqrt{3}$) = $Q(\sqrt{2}, \sqrt{3})$. now Q $\subset$ Q $\sqrt{2}$ $\subset Q(\sqrt{2}, \sqrt{3})$. to prove last containment it is sufficient to show that $\sqrt{3} \notin Q(\sqrt{2})$. *suppose this* were not true, then $\sqrt{3} = a + b\sqrt{2}$ *for some* $a, b \in Q$. *this would* in turn imply $3 = (a^2 + 2b^2) + 2\sqrt{ab} \Rightarrow 2\sqrt{ab} = 3 - a^2 - 2b^2$. Now a = 0 $\Rightarrow \sqrt{3} = b\sqrt{2} \Rightarrow \sqrt{6} = 2b \Rightarrow \sqrt{6}$*is rational, which is a* absurd. If b = 0 then$\sqrt{3}$ would be rational which is again absurd. Thius the only choice left is $\sqrt{2} = \frac{3 - a2 - 2b2}{2a}$, a rational number. Hence our 2ab supposition in wrong and as a consequence Q ($\sqrt{2}$, $\sqrt{3}$) $\neq Q(\sqrt{2})$. similarly it can be shown that Q $\subset Q(\sqrt{3}) \subset Q(\sqrt{2}, \sqrt{3})$. thus we see that (K:Q) = 4. Then the Galois group G (K,Q) being of order 4 is either cyclic or klein's 4 – group . now k has at least two subfields.

Q $\sqrt{2}$ and Q $\sqrt{3}$ *lying properly between Q* and k, by Fundamental theorem of Galois theory G (K,Q) has at least two proper subgroup lying between (1) itself.

Since (K: Q $\sqrt{2}$) = 2 and (K:Q $(\sqrt{3})$) = 2

G (K, $\mathbb{Q}$) has at least two subgroups of order 2.

SOLVABILITY OF POLYONOMIALS BY RADICALS

Now we shall discuss how to apply the result obtained in the last section to determine the solvability of polynomials by radicals.

Example 1

Let f (x) = x^2 + ax + b be a monic quadratic polynomials over $\mathbb{Q}$. its two roots are $\alpha_1 = \frac{-a + \sqrt{a^2 - 4b}}{2}$, and $\alpha_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}$. If we take L = $\mathbb{Q}(\mu)$, where $\mu = \sqrt{a^2 - 4b}$, then we see that $\mu^2 \in \mathbb{Q}$. So that L is a radical extension of $\mathbb{Q}$. Further L itself is the splitting field of f (x) over $\mathbb{Q}$. Hence f (x) is solvable by radicals.

Example 2

Consider the cubic f (x) = x^3 + 3a x^2 + 3bx + c over $\mathbb{Q}$. if we put z = x + a, then the above equation becomes the equation of the form g (z) = z^3 + 3b_1 z + c_1 , $c_1 \in \mathbb{Q}$. If we know the roots of g (z) then the roots of f (x) are obtained from them by subtracting a from each roots of g (z). since a $\in \mathbb{Q}$, we see that the splitting fields of f (x) and g (z) are the same. Cardan's famula gives that the roots of g (z) are p + q, ωp + ω^2q, ω^2p + ωq, where ω is imaginary cube root of unity,

P = $\sqrt[3]{\frac{-c}{2} + b_1^3 + \frac{c_1^2}{4}}$

and

q = $\sqrt[3]{\frac{-c}{2} - b_1^3 + \frac{c_1^2}{4}}$

Take $\propto_1 = \sqrt{b_1^3 + \frac{c_1^2}{4}}$ $\propto_2 = \sqrt{\frac{-c}{2} + \propto_1}$, $\propto_3 = \sqrt{-3}$.

Now take F_0 = $\mathbb{Q}$ $F_1 = F_0(\propto_1)$, $F_2 = F_1(\propto_2)$, F_3 $F_2(\propto_3)$. We find that $F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3$;

$\propto_1^2 \in f_0$, $\propto_2^2 \in f_1$, $\propto_3^2 \in f_2$. Further F_3 contains all the roots of g(z). Hence g(z) and consequently f(x) is solvable by radicals.

REFERENCES

Ash, R.B (2000), Abstract Algebra, The basic graduate year, AMS Online, Illinois, U.S.A .

Bhattacharya, P.B, S.K. Jain and S.R. Nagpaul (1995), Basic Abstract Algebra, Second Edition, Foundation Books, New Delhi, India.

Cohn, P. M. ((1977), Algebra, Vols. ! and 2, John Wiley, New York, U.S.A.

Dummit, D. S. and Richard M. F (1977), Abstract Algebra, 2nd Edition, Wiley Eastern Limited, New Age International Limited, New Delhi India.

Jacobson, N. (1974, 1980), Basic Algebra I, II, W.H. Freeman, San Francisco, U.S.A.

Singh, S. and Qazi, Z. (1999), Modern Algebra, Revised Edition, Vikas Publishing House Pvt Ltd, New Delhi, India.