Nalanda Open University

M.Sc. Part- I

Course- Mathematics

Paper- 1 (Advanced Abstract Algebra)

Prepared by – DR. Lalit Kumar Sharan

Rtd. Professor and Head

Department of Mathematics,

V.K.S. University, Ara

Unit 5 (GALOIS GROUP):

Contents:

Section 1.

Automorphism And Group of Automorphism in previous Studies

1.1 We have already developed the concept of automorphism in previous studies.
1.2 **Definition**:

Automorphism of Field: Let F be a field then a mapping $f:F\rightarrow F$ is called an automorphism of F iff :

(i) $f(a+b) = f(a) + f(b)$
(ii) $f(ab) = f(a)*f(b)$ for every a,b □F
(iii) f is one-one, onto

Equality of two Automorphism of Fields:

Two automorphism f and g of fields are said to be equal if $f(a) = g(a)$, for every a in F. Otherwise f and g are called distinct i.e; when $f(a) \neq g(a)$ for some $a \in$ **F.**

Fixed Field: If G is the group of all automorphism of field K (of characteristic 0), then the fixed field of G is the set of all elements $a \in K$ such that $f(a) = a$ for all f in G.

Group of Automorphism of a field K: Let K be a field of characteristic **O** and let F be a subfield of K. Then the group of automorphism of K relatives to F, denotes as G (K, F) is the set of all automorphism of K leaving every element of F fixed, that is the automorphism f of K is in G (K,F) if and only if $f(\alpha) = \alpha$ for every $\alpha \in F$.

Normal Extension of A Field: A field K is normal extension of a field F if K is a finite extension of F such that F is the fixed field of G (K, F).

Theorems:

Theorem1.3 (i): The fixed of G is a subfield of K, where G is the group of all automorphism of a field K.

Proof: Let a and b be any two elements of the fixed field of G. Then for all f in G , $f(a)= a$, $f(b)=b$ implies $f(a\pm b) = f(a) \pm F(b) = a \pm b$

Also, $f(ab)= f(a)f(b)=ab$

Thus a…b, ab is again in the fixed field of G.

If $b\neq 0$ then $f(b^{-1}) = (f(b))^{-1} = b^{-1}$ is also in the fixed field of G.

Thus the fixed field of G is a subfield of G.

Theorem 1.3(ii) :

Let A(F) be the collection of all automorphism of a field F. Then A(F) is a group with respect to the composition operation of two functions.

Proof: Since A(F) =the collection of all automorphism of a field F.

Let f, g∈ A(F) implies that f, g are one-one, mapping of F onto itself Implies that gf : F on to itself .

Also, Let a, b∈ F then (gf) (ab)= g(f (ab)) =g[f(a) g(b)] g (f(a)) * g (f(b))= (gf (a)) (gf(b))

Also, (gf) (a+b) = g (f(a+b)) =g(f(a)) +f(b)) =g (f(a)) +g (f(b))= gf (a). g(f (f))

Thus gf is an automorphism implies that gf ∈ A(F) implies that A(F) is closed under the given operation.

We know that the composition of arbitrary mapping is associative. Thus the composition of Automorphism is also associative.

Further clearly the identity mapping I of F is an automorphism of M.

Also, I is one on one onto and for a_1b in F

I (ab) =ab = I (a) I(b) and I (a+b) =a+b= I(a) +I(b)

Thus I ∈A(F) and for any f ∈A(F), If=f I=f

Thus, the existence of identity element. Finally we have to show the existence of inverse:

For this, Let f ∈A(F) implies that f is one -one-onto implies f^{-1} (the inverse of f) exists.

Also, f^{-1} is one -one-onto.

Let a, b ∈F then ⍰ a', b' in F such that f^{-1} (a)= a' iff f(a') = a and f^{-1} (b)= b' iff f(b') = b

Then f^{-1} (ab) = f^{-1} [f(a') . f(b')] = f^{-1} [f(a'. b'] =a' b' = f^{-1} (a) f^{-1} (b)

And f^{-1} (a+b) = f^{-1} {f (a') + f(b')} = f^{-1} { f(a' +b') } = a' +b' = f^{-1} (a) + f^{-1} (b)

Thus f^{-1} is also an automorphism of F implies f^{-1} ∈ A (F)

But f is arbitrary.

Thus, for every f ∈A(F) implies that f^{-1} ∈A(F)

Thus A(F) satisfied all the condition to be a group.

Therefore A(F) forms a group under the given composition.

Theorem 1.3(iii)

Let K be a field. If ψ_1, ψ_2, …., ψ_n are distinct automorphism of K, then we cannot find elements a_1, a_2, ..a_n not all zero in F such that;

$a_1\psi_1$ (u)+ $a_2\psi_2$ + ….+$a_n\psi_n$ (u) =0, for all a ∈ K.

Proof: If possible, let for a moment we find elements a_1, a_2, …., a_n not all zero in F.

Such that a_1 ψ_1 (u) +a_2 ψ_2 (u)+….+ a_m ψm (u) =0 for every u in F…………………………… 1

If m=1 then (1) takes the form of a1 ψ_1(u) =0 for every u ∈ F.

Since a_1 ψ_1 (u) = 0 for u in F implies that a_1 ψ_1 (1)=0, 1 ∈ F implies that $a_1$1=0 implies that a_1=0

which goes against our assumption:

Hence, we have n> 1.

Since ψ_1 ≠ ψm implies that ∃ a. c ∈F such that ψ_1(c) ≠ ψm (c)

Also u, c ∈F implies that u.c ∈F implies that 1 holds good for uc

implies that a_1 ψ_1 (cu) + a_2 ψ_2 (cu) +…..+ a_m ψ_m (cu) = 0 for u in F

implies that a_1 ψ_1 (c) . ψ_1 (u) + a_2 ψ_2 (c) . ψ_2 (u) +…. + a_m ψ_m (c) ψ_m (u) =0 for u in F………………… 2

From 1 and 2 together we see that :

a_2 [ψ_2 (c) - ψ_1 (c)] ψ_2 (u) +…+ a_m [ψ_m (c) - ψ_1 (c)] ψ_m (u) = 0 ……………………... 3

Let v_1 = a_i { ψ_i (c) - ψ_1 (c)} for i= 1,2,…..,m.

Now since a_i , ψ_i (c), ψ_1 (c) are all in K implies that each vi is in F.

And v_m = a_m [ψ_m (c) – ψ_1 (c)] ≠ 0

Thus from (3), we get v_2 ψ_1 (u) +…..+ v_m ψ_m (u)= 0 , for every u in K ………………... 4

Since 4 contain (m-1) terms and v_m ≠0 so from 4 , we can find a relation of the type , a_1 ψ_1 (u) + a_2 ψ_2 (u) +….+ a_n ψ_n (u) = 0, for u ∈ K containing less than m non zero terms which contradicts the fact that 1 is minimal relation . Thus the theorem is observed.

Theorem 1.3 (iv)

Let K be a sub field of a field F. Let G (F, K) be the set of all those automorphism of F which leaves every element of K fixed, that is, the automorphism f of F is in G (F, K) if and only if f (α) = α, for every α in F. Then G (F,K) is a sub group of the group of all automorphism of F.

Proof: Let I be the identity automorphism of F.

Then I ∈ G (F, K) implies that G (F,K)≠ Φ

Also, I (α) = α, for every α ∈ K

Let f,g ∈ G (F, K) then for α in K , f (α) = α, g (α) = α implies that f^{-1} (α) = α , g^{-1} (α) = α

Also (g f^{-1}) (α) = g(f^{-1} (α)) = g (α) = α implies that G(F, K) is a sub group of the group of all automorphism m of F.

Theorem 1.3 (v)

Let K be normal extension of a field F of characteristic O. Then [K:F] = 0 [G(K, F)]

Proof : Let F be a field of characteristic 0

Also let K be a normal extension of F.

But then the fixed field of G (K, F) is F itself .

We also know that normal extension implies finite extension implies K is a finite extension of F.

By a theorem we know that if K be a normal extension of a field F, H be a sub group of G (K, F). KH= [a ∈ K : Ψ (a) **= a,** ∀ Ψ ∈ H] then :

(i)][K; K_H] = 0 (H) and
(ii) H= G (K, K_H)

So we take H = G [K, F] we can have K_H = the fixed field of G [K,F] = F1

Therefore 0 [G(K, F)] = [K : F]

Theorem 1.3 (vi)

Let K be the splitting field of f(x) ∈ F[x] and let p (x) be an irreducible factor of f(x) in F[x]. If the roots of p(x) are α_1, α_2,…α_i then for each I, there exists an automorphism Ψ_i in G [K,F] such that Ψ_i (α_1) = α_i

Proof: Since its given that K is the splitting field of f(x) ∈ F[x]

And p(x) is an irreducible factor of f(x) ∈ F[x]

Hence every root of p(x) is a root of p(x) implies p(x) ∈ K

Let $F_1 = F(\alpha_1)$ and $F_i = F(\alpha_i)$, α_1, α_i are roots of p(x)

Again since p(x) is irreducible in F [x], so we can get an isomorphism $\emptyset: F(\alpha_1) \to F(\alpha_i)$ such that $\emptyset(\alpha_i) = (\alpha_i)$ and $\emptyset(a) = a$, for a is in F.

Also $F \subseteq F1$ implies that if $f(x) \in F(x)$ then $f_{(x)} \in F_1 [x]$

It means K is splitting field of $f(x) \in F_1 [x]$

Similarly, K is the splitting field of $f(x) \in F_1 [x]$

Thus we shall get an isomorphism $\Psi_1 : K \to K$ such that $\Psi_1 (a) = \emptyset(a)$, $a \in F1$

But $F1 = F(\alpha_1)$, hence $\alpha_1 \in F_1$

Then we have $\Psi_i (\alpha_1) = \emptyset (\alpha_1) = \alpha_i$

Thus Ψ_i coincides with $\emptyset$ on F1 and hence on F implies $F_i (\alpha) = \alpha$, $\alpha \in F$.

Therefore $\Psi_i \in G [K, F]$.

Section- 2

<u>GALOIS GROUP, Finite Fields</u>

2.1 Introduction:

The theory of Galois gives a decent and useful interplay of group and field theory. Equivalently we can say that this theory is an excellent composite of the theory of groups with the theory

Of algebraic field extensions. It also play a vital role in the theory of equations.

2.2 Definitions:

<u>Galois group</u> – Let K be a finite extension of a field F. The group G [F,K] of all F automorphism of K is known as Galois group of K over F. Here, K is popularly called Galois extension of F.

<u>Conjugate elements</u> - Let K be the finite extension of a field F. Then any two elements α, β in K are said to be conjugate over F, if they have the same minimal polynomial over F.

<u>Finite Field :</u> A field F having only a finite number of elements is known as finite field.

<u>Prime Field:</u> A field F is called prime if it has no proper subfield.

Normal extension: Let K be an algebraic extension of the field F. Now if the splitting field of the minimal polynomial f(x) in F [x], for each element of K is the splitting field of some polynomial over F.

Separable polynomial: Let f(x) in F [x] be an irreducible polynomial. Now if f (x) has no multiple roots in it's splitting field then f(x) is called separate over F. Clearly the roots of f(x) in it's splitting field are simple.

Separable Element: Let K be an algebraic extension of F. An element α ∈ K is called separable over F if the minimal polynomial or α over F is separable otherwise it is called inseparable element.

Separable Extension: An algebraic extension K of a field F is called separable extension of F of every element of K is separable over F.

Theorems

Theorem 2.3 (1)

An element of K which remains invariant under each member o the group G (K,F) of K over F is necessarily a member of F.

Proof: Let $\alpha \in K$ be arbitrary. Also α remains invariant under every member of $\Psi \in G(F,K)$ implies $\Psi(\alpha) = \alpha$, for each α in K , our problem is to show that α is in F and $\Psi \in G(K,F)$. For this, As G (K,F) is Galois group implies that K is finite normal extension of K itself implies that K is the splitting field of some polynomial f(x) in F[x].

Let p(x) be the minimal polynomial of α over F.

Also, since K is normal over F and one root of α over F. Also, since K is normal over F and one root of α of p(x) in K.

Thus, each root of p(x) will be in K.

Let a polynomial F(x) p (x) $\in$ F [x] implies K is splitting field of F(x) p(x).

If possible, let for a moment deg. p(x) ≥ 2

Thus, K is separable also over F and all roots of p(x) will be distinct. Hence we shall get an element $\beta \subseteq K$ where $\beta \neq \alpha$, β is a root of p(x) over F.

It means $\alpha \neq \beta$ and $\alpha 1\ \beta$ are roots of irreducible polynomial f(x) $\in$ F[x]

Hence we shall get a F- isomorphism $\Psi : F(\alpha) \rightarrow F(\beta)$ such that $\Psi(\alpha) = \beta$

Thus, Ψ can be contained to an F – automorphism of K

But then there exists Ψ in G (K, F) which maps α on β, $\beta \neq \alpha$

Thus, we arrived at a contradiction.

Thus, deg. p(x) is not greater than or equal to 2. So deg p(x) =1 so $p(x) = x- \alpha$, $\alpha \in F$ as $p(x) \in F[x]$ and $p(\alpha) = 0$

Theorem 2.3 (ii):

Let K be a finite normal extension of a field F. If α, β be any two elements of K conjugate over F, then there exists an F- automorphism Ψ of K such that $\Psi(\alpha) = \beta$

Proof: Let K be the finite normal extension of the field F.

Clearly K is the splitting field of polynomial f(x) in F [x].

Given α, β are conjugate over the field F.

Hence α, β have the same minimal polynomial over F.

Also α, β are algebraic over F. So we get an isomorphism $\theta : F(\alpha) \rightarrow F(\beta)$, given by $\theta(\alpha) = \beta$

But then K is the splitting field of f(x) over F (α), F (β) as FCF (α), FCF(β), α, β∈ K.

So we shall get an automorphism Ψ of K which is an extension of θ

Now Ψ(α) = θ (α) = β and for any element p in F, we have Ψ(ρ) = θ (ρ) = ρ

Thus Ψ is an F- automorphism of K such that Ψ(α)= β.

Theorem 2.3 (iii)

The order of the Galois group G (K, F) is equal to [K:F]

Proof: Let K be a finite separable extension of a field F. Thus K is simple extension of F. So we can get an α in K such that K= F(α)

Let p(x) be a minimal polynomial of α over F and deg.p(x) = n, Hence [K:F]= n.

As per assumption K is separable over F, hence roots of p(x)= 0 are simple.

Let these roots be $\alpha= \alpha_1, \alpha_2,\ldots,\alpha_n$

Since deg.p(x) =n implies that $\alpha_1, \alpha_2, .. ,\alpha_n$ are all distinct.

Let each F- automorphism of K maps α to another root of p(x).

Thus clearly k= F(αi) for i= 1,2,3,..,n.

We also know that F- mapping which maps α1 and αi actually determines a F- automorphism Ψi of F (α1) on F (αi) such that $\Psi(\alpha_1)$ = αi

Also, each Ψi is unique because α_i generates K over F.

Thus the Galois group G (K,F) contains Ψ1, Ψ2, …, Ψn

Hence 0 (G (K , F)) =n= [K:F]

Theorem 2.3 (iv)

Let K be a finite separable, normal extension of a field F of characteristic zero, then the fixed field of Galois group G, (K,F) is F itself.

<u>Proof:</u>

We know that every finite separable extension is a simple extension. By question K is finite separable extension so as a result of which K is simple extension of F. Then k= F (α), α ∈ K.

Let p (x) is in F[x] and p(x) is a minimal polynomial of α. Also, assume E is the splitting field of p(x).

Also, splitting field of every polynomial over F is K as K is normal extension of F. Hence E ⊆ K…………………1

Also α ∈ E, as E is the splitting field of p(x) such that p(α) =0

Also α ∈ E implies F(α) ⊆ E implies K⊆E [as K=F (α)] ………………... 2

From 1 and 2 E=K implies K is the splitting field of the minimal polynomial p(x) of α.

Now if deg. p (x) =n, then [K:F] =n

Let α = α1, α2, α3,….., αn be the conjugate of α over F.

Then K= F (αi) for i=1, 2,…,n

Also, for each I we can get F- automorphism …. Of K such that Ψ (α1) is conjugate of α1

Hence Ψ1, Ψ2, ….., Ψn are contained in G (K, F)

Let T be the fixed field of G(K,F) then [K,T] = 0 (G(K,F))

Which shows the fact that F itself is the fixed field under G(K,F) = n= [K:F] implies that T = F

Which shows the fact that F itself is the fixed field under G(K, F).

Theorem 2.3 (v) :

Let F be a finite field with q elements and suppose F⊆K , where K is also a finite field , then K has elements q^n where n = [K:F]

Proof:

Since we can regard every field as a vector space over a subfield. Thus we can retard K as a vector space over the field over F.

Also the number of elements in K is finite.

Hence the vector space k (F) is finite dimensional.

Let dim. K (F) =n implies that [K:F] = n

For a moment, Let the set {b1, b2, …..,bn} be a basis of vector space k(F).

But then we can uniquely express every element of K in the form $a_1b_1 + a_2b_2 + \ldots + a_nb_n$ where each a_i is in F. Implies that the number of elements in K = the number of the terms in the linear combination $a_1b_1 + \ldots + a_nb_n$.

Because $x^q - x \in I_p(x)$ range over F.

Finally, F has q elements, so each of the n coefficients a’s can have q values.

Therefore, K have q^n elements.

Theorem 2.3 (vi): Any two finite fields having the same number of elements are isomorphic.

Proof: Let F be a finite field of characteristic P.

Also let I_p = field of integers modulo P.

We consider the polynomial $x^q - x \in I_p(x)$

We show that F can be regarded as the splitting field of the polynomial $x^q - x \in I_p(x)$.

Since F is a field of finite characteristic p so it contains a subfield Fo isomorphic to the field Ip.

So F can be regarded as an extension of the field Ip.

Now if the number of elements In F=q then we have seen in our previous study $x^q = a$,. a $\in$F implies that a in F satisfies the polynomial $x^q - x \in I_p(x)$.

Clearly $x^q - x$ can have utmost q roots in extension field Ip.

That is q elements of F are the roots of $x^q - x$.

Thus the polynomial $x^q - x \in I_p(x)$ splits in the field F.

But this polynomial can not split in any smaller field because that field must contain all the roots of this polynomial $x^q - x$. Also roots of this polynomial are distinct.

Thus F is the splitting field of $x^q - x \in I_p(x)$.

Further, Let F' be an any other finite field having q= p^n elements.

Thus continuing in the same way as we have done above , we can see that F' is also the splitting field of $x^q - x \in I_p(x)$

We also know that any two splitting fields of $x^q - x \in I_p(x)$ must be isomorphic.

Thus F' ≅ F. That is F' is equivalent to F.

Section 3

GALOIS FIELD

3.1 Introduction:

It is a field with a specific condition.

3.2 Definition:

Galois Field: Let p be any prime integer and n be an integer then a field with p^n element is known as Galois field. It is denoted by GF $(p^{n).}$

3.3 **Theorems:**

Theorem 3.3 (i): The multiplicative group of a Galois field is cyclic

Proof: Let F be a finite field with q= p^n elements and let F' denote the set of q -1 non zero elements so that F' forms a multiplicative group of finite order q -1

That is 0(F') = q -1

Also elements of F' are the roots of the polynomial $f(x) = x^{q-1}$-1

To show that F' is cyclic

Sufficient to show that ∃ an element of F' of order q -1

Let us write q -1 $= p_1^{m1}, p_2^{m2}, \dots\dots\dots p_r^{mr}$ where pi≠ p and all pi are distinct primes.

Let m= l.c.m { p_1^{m1} , p_2^{m2} , …….. p_r^{mr}}

Since F’ is finite so that the order of each element of F’ is finite.

Let α be an element of F’ with 0 (α) =m

Also, α ∈ F’ implies that α satisfies a polynomial f(x) = x^{q-1} -1

Implies that α^{q-1} -1 = 0 implies that x^{q-1} =1 implies that ∑ -1 divides m implies q-1=m (m ≤q-1)

Implies that 0 (α) = q-1= o(F’).

Thus F’ is cyclic.

Theorem 3.3 (ii):

Every finite field of characteristic p has an automorphism.

Proof: Let F be a finite field of characteristic p.

We consider a mapping Ψ : F→ F such that Ψ (0) a^p ∀ a in F

Then we see that:

For a b ∈ F then Ψ(a) = Ψ(b) implies that $a^{p =} b^p$ implies that $a^{p-} b^p$ = 0 implies that (a-b) ;.^{p} = 0

(Since in a field of characteristic p, we have $(a-b)^p$ = $a^{p\,-} b^p$)

Implies a-b= 0

implies a=b

That is Ψ(a) = Ψ(b) implies a=b implies Ψ is one on one.

Also, since the set F is finite and we have already proved that Ψ is one- one so Ψ is onto.

Finally, let a, b ∈ F, then we find that,

Ψ(a+b) = $(a+b)^p$ = $a^{p\,+} b^p$ (Since in a field of characteristic p, we have $(a+b)^p$ = $a^{p\,+} b^p$)

= Ψ(a) + Ψ(b)

Similarly Ψ(ab) = $(ab)^p$ = $a^p b^p$ = Ψ(a) Ψ(b)

Thus Ψ is an automorphism of the field F.

Section 4

Cyclotomic Field and solvability by Radicals.

4.1 **Introduction:** The study of the above is in fact an advanced study of Galois group and its applications.

4.2 **Definitions:**

Cyclotomic Field: The splitting field x^{n-1} ∈ Q [x] which is contained in the field of complex numbers is known as nth cyclotomic field.

Primitive nth roots of unity: Let F be a field. The roots of_x^{n-1} = 0 over F are known as the primitive nth roots of unity in its splitting field if $W^n = 1$, but $W^n \neq 1$ for any positive integer

Solvable by Radicals: Any field extension which can be reached through a finite series of successive pure extensions is known as solvable by radicals or radical tower.

Pure Equation and pure Extension: The equation of the form x^{n-1}-a =0 is called pure equation whereas an extension field F [$(a)^{1/n}$] is called pure extension of F.

Solvable by Radicals over a field F: Let F be a field and f(x) =0 is said to be solvable by radicals over F, if the splitting field K of f(x) is a tower of F.

Normal Radical Tower: However, K is a normal extension of F, then the tower is called normal radical tower over F.

Solvability by Radicals of Cyclotomic Fields: A group G of finite order is said to be solvable if their composition factors are prime.

4.3 Theorems

Theorem 4.3(i)

(Fundamental theorem):

Let F be a field of characteristic 0. Then, a polynomial f(x) in F[x] is solvable by radicals over F if and only if its splitting filed K over F has solvable Galois group G [K, F]

Proof:

Let G [K, F] be solvable. To prove f(x)= 0 is solvable by radicals. Let [K:F] = 0 [G(K,F)] =n

And F contains a primitive nth root of unity. Then clearly F contains primitive m th root of unity such that m/n.

Let G= G(K, F) and G is solvable and finite.

So G= $G_0 \supset G_1 \supset \dots$ ⊃Gs =1 is a chain of sub groups of G such that i= I,2,…, s and Gi is a normal subgroup of G_{i-1} and Gi_{-1}/ G is cyclic.

Let Fi is the fixed of Gi, then F=F0 ⊃ F1 ⊃F2 ⊃Fs = K ------------ 1

If ni= [Fi/ Fi-1] , then ni/n , hence Fi-1 contains a primitive $n_{i\,th}$ root of unity.

Also, Fi/ F_{i-1} is cyclic because G(Fi, Fi-1) is isomorphic to G i-1/ Gi.

Implies Fi is Cyclic extension of Fi-1.

Implies Fi is the slitting field of an irreducible polynomial x^{n-I} - ai ∈ F i-1 (x)

Also, Fi= Fi-1(αi), where αi is a root of x^{ni} - ai = 0

Implies that I is solvable by radicals over F and Fs is the splitting field of f(x) over F.

Implies f(x)= 0 is solvable by radicals.

Again let C be an algebraic closure o F such that K ⊆C.

Let t be a primitive nth root of unity in C then C(t) is the splitting field of f(x) over F(t).

Also, G [C(t), K] is isomorphic to a subgroup of G.

Also, G is solvable implies G[Ct), K] is solvable implies c(t) is radical extension of F(t).

Implies C(t) is radical extension of F and hence f(x) is solvable by radicals.

Conversely, Let f(x) = 0 is solvable by radicals.

To prove G [K, F] is solvable.

For this, As f(x) = o is solvable by radicals so we have a normal radicals tower of F such that

F= Ko ⊆ K1 ⊆ K2 ⊆Kr over F, Kr contains a splitting field K of f(x) over F.

Also Ki-1 (ai) = Ki and a_i^{ni} = bi ∈ Ki-1 for i= 1,2,…,r

Let n=n1, n2….nr, t be primitive nth root of unity in some algebraic closure of F which contains Kr.

Let Ei = Ki (t) for I =1, 2, …, r then F(t) = E0 ⊆E1 ⊆E2 ⊆Er is a normal radical tower over F(t).

Again, We have Ei= Ei-1 (ai) and E i-1 contains nith root of unity.

Thus Ei / E i-1 is cyclic.

If Hi = G (Er, Ei), then G (Er, F(t)) = Ho⊃Hi⊃…. ⊃ Hr = 1 and H1/ Hi ≜ G (Ei, Ei-1) is cyclic then G (Er, F(t)) is solvable .

Again, we have G (Er, F(t)) ≜ G (Kr, Kr ∩ F(t)) and F(t) is an abelian extension of F. Implies Kr ∩ F(t) is an abelian extension of F.

Thus G (Kr ∩ F(t), F) is solvable

Hence G (Kr, F) has a solvable normal subgroup G (Kr, Kr ∩ F(t)) ≜ G(Kr ∩ F(t), F)

Such that the factor group G (Kr, F) / G (Kr, Kr ∩F(t)) ≜ G (Kr ∩ F(t), F) is solvable.

Therefore, G (K, F) is solvable.

Hence the if and only if conditions are well established.

Theorem 4.3 (ii)

The Galois group x^n - 1 over any field of characteristic zero is abelian.

Proof:

Let F be a field of characteristic 0.

Again, let K be the splitting field of x^n - 1 over the field F.

Now if t is supposed to be a primitive nth root of unity then K = F(t).

We also know that in every F- automorphism of K, t is mapped on t^a and we determine such automorphism by its effect on t.

Thus G (K, F) = [Ψa- Ψa (t)= t^a]

Ψa, Ψb, ∈ G (K, F) then (Ψa Ψb) (t) = Ψa (Ψb (t))= Ψa (t^b) = $[\Psi a(t)]^b = [t^a]^b = t^{ab} = t^{ba} = (t^b)^a$

$= [\Psi b(t)]^a = \Psi b(t)^a$ = (Ψa Ψb)t implies that Ψa Ψb commute implies G(K,F) is abelian.

Theorem 4.3 (iii)

For a prime integer p, the Galois group of x^p -1 over the prime field of characteristic zero is the cyclic group of order p-1.

Proof: Let F be a prime field. Let also that the characteristic of F is 0.

Since $x^p -1 = (x+1)\, \Phi_p (x)$.

Obviously, the splitting field K of x^p -1∈ F[x] is the same as that of

$\Phi_p(x) = x^p -1 + x^p -2 + ... + x + 1$

Also, $\Phi_p(x)$ is irreducible over F.

Now if t be a root of $\Phi_p(x)$ then t, t^2,…, t^{p-1} are (p-1) roots of $\Phi_p(x)$.

Clearly all roots are distinct

Thus if we define an automorphism given by Ψa(t) = t^a then we can verify it easily that Ψa→ a is an isomorphism of the Galois group of automorphism of order p-1 with the group of p-1 integers

1,2,3,…., p-1 for multiplication modulo p.

Also, (Ψa Ψb) (t) = Ψa (Ψb (t))= Ψa (t^b) = $[t^b]^a = t^{ba} = \Psi a\, \Psi b \rightarrow ab$

Hence the set {1,2,..,p-1} forms a multiplicative group of prime field I_p of characteristic p, which is cyclic of order p-1.

Section 5

Solved Examples:

Example 1. (2016, 2017, 2019) Find the Galois group of the x^3 -2 ∈ Q[x] over Q, the field of rational number.

Solution: Let K be the splitting field of f(x) = x^3 -2 over the field Q of rational numbers. The roots of f(x) are not all reals.

Hence K may be considered as subfield of the field of complex number.

Let α = $2^{1/3}$ We must obtain K we first adjoin α to Φ

In Q (α) [x], we have f(x) = (x- α) (x^2 + αx + α^2) = (x- α) g(x)

The field Q (α) is a real field and g(x) has no real root, so that g(x) is irreducible Q (α) [x].

The roots of g(x) are α $\boldsymbol{\omega}$ and α $\boldsymbol{\omega}^2$…, where $\boldsymbol{\omega}$ = $\frac{-1+\sqrt{3i}}{2}$ and $\boldsymbol{\omega}^2$ = $\frac{-1-\sqrt{3\,i}}{2}$

Hence, K = Q (α, $\sqrt{3i}$)

We have [K : Q] = 6 and hence O (G (K, Q)) = 6

Thus, if we can find a distinct Q- automorphism of K, they will constitute all of G (K, Q) , one element of this group is its identity I.

Again let, Ψ be the Q-automorphism of K which leaves a fixed and maps $\sqrt{3i}$ and - $\sqrt{3i}$

Let T be the Q – automorphism of K such that –

T (α) = a.. , T($\sqrt{3i}$) = - $\sqrt{3i}$

Thus we have the following table which gives the image of α and $\sqrt{3i}$ under indicative Q- automorphism of K.

	1	**Ψ**	**T**	**ΨT**	**TΨ**	**ΨTΨ**
A	**A**	**α**	**Aω**	**αω2**	**αω**	**αω2**
$\sqrt{3i}$	$\sqrt{3i}$	- $\sqrt{3i}$	- $\sqrt{3i}$	$\sqrt{3i}$	$\sqrt{3i}$	- $\sqrt{3i}$

Thus, the Galois group of x^3 -2 ∈ Q [x] is { I, Ψ, T,TΨ, ΨT, ΨTΨ}

Example 2. (2018)

The group G [Q (α), Q], where $\alpha^5 = 1$ and $\alpha \neq 1$, is isomorphic to cyclic group of order 4.

Solution:

Since we have $\alpha^5 - 1 = 0$ implies that $(\alpha - 1)(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4) = 0$

Implies that $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1$ implies that α is a root of polynomial.

$f(x) = 1 + x + x^2 + x^3 + x^4 \in Q[x]$.

Since f(x) is irreducible over Q, then $[Q(\alpha) : Q] = 4$

Also, all the roots of the polynomial $g(x) = x^5 - 1 \in Q[x]$ are $1, \alpha, \alpha^2, \alpha^3, \alpha^4$

Thus Q (α) is normal extension of Q

Hence $O[G\, Q(\alpha), Q] = [Q(\alpha) : Q] = 4$

This shows that, there are four Q- automorphism of Q (α). Since $[1 + \alpha + \alpha^2 + \alpha^3]$ is the basis of Q (α) over Q, then $Q(\alpha) = [a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c, d \in Q]$

Let $G(Q(\alpha), Q) = [\Psi 1, \Psi 2, \Psi 3, \Psi 4]$ with Ψ1 an identity automorphism.

The four Q automorphism of Q (α) are as follows:

$\Psi 1 (a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\alpha + c\alpha^2 + d\alpha^3$

$\Psi 2 (a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\alpha^2\, c\alpha^4 + d\alpha$

$\Psi 4 (a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\alpha^4\, c\alpha^3 + d\alpha^2$

Clearly, $[\Psi 1, \Psi 2, \Psi 3, \Psi 4]$ forms a cyclic group of order 4 generated by Ψ2 and Ψ3.

Example 3.(2018)

Show that every element in a finite field can be written as the sum of two squares.

Solution:

Let F be a finite field of order $p^{n.}$

If p=2. Define Ψ:2 → F given by $\Psi(b) = b^2$ implies that clearly Ψ is one-one.

Also since Ψ:F → F is one-one and F is finite implies Ψ is onto.

Also, $\Psi(b_1+b_2) = (b1+b2)^{2 =} b_1^{2 +} b_2^{2 =} \Psi(b_1)_{+} {}^{=} \Psi(b_2)$ and $\Psi(b_1 b_2) = (b_1 b_2)^{2 =} b_1^2 b_2^{2 =} \Psi(b_1)\Psi(b_2)$

Thus Ψ:F → F is homomorphism

Since for a in F we get b in F such that $\Psi b = a$ implies $a = b^2 = b^{2 +} o^2$ = sum of two squares.

Again, if p≠2 then Let $a \in F$, $x = [a - x^2 : x \in F]$

Then $a - x_1^2 = a - x_2^2$, $xix_2 \in F$ implies that $x_1^2 = x_2^2$ implies $x1 = -x2$ if $x_1 \neq x_2$

Implies $O(x) = p^n - 1/2 + 1 = p^n + 1/2$

Let Y = [y^2 : y∈ F] then proceeding in the same way as we have done above , we get O (Y) = $p^n + 1/2$

Therefore X, Y … F and O(F) = p^n, X∩Y≠Φ

Thus a- $x^2 = y^2$, for some x,y∈ F implies a = $x^2 + y^2$= sum of two squares in F.

Example 4. (2018)

Show that the Galois group of $x^4 + x^2 + 1$ is the same as that of $x^6 - 1$ and is of order 2.

Solution: We know that the primitive nth root of unity is given by

e2π i/n = cos 2π/n + I Sin 2π/n

Also the primitive 3rd root of unity is given by e2π i/3 = cos 2π /3 + i sin 2π /3 = - ½ + i$\sqrt{3}$/ 2

Let $x^2 = y$ then $x^4 + x^2 + 1 = y^2 + y + 1$

But - ½ + i$\sqrt{3}$/ 2is a root of $y^2 + y + 1 = 0$

Hence $y^2 + y + 1$ is the minimal polynomial for a primitive 3rd root of unity.

Thus the splitting field of $x^4 + x^2 + 1$ will contain the square root of e2π i/3 and e4π i/3. Thus we need to adjoint.

eπ i/3 = (e2π i/3)^{½}, e4π i/3 = - e π i/3 = - (e2πi /3)^{½}, e2πi /3 = (e4π i/3) and e5π i/3 = - e2π i/3= - (e4π i/3)^{½}

From which K= Q (α), where α = $x^4 + x^2 + 1$ over Q.

Now α is a primitive sixth root of unity.

Implies K is also a splitting field of x^6-1 over Q

But then G(K, Q) = (Z/ (6))* = { T, F} is a group of order 2.

Example 5: (2018)

Let K be the splitting field of $x^n - a \in F[x]$. Then show that G(K, F) is a solvable group.

Solution: Let a field F contains a primitive nth root of unity. Then as we already know that G(K,F) is abelian so it is solvable. We assume the case that F contains no primitive nth root of unity .

Let t ∈ F^- and t is generator of the cyclic group of the nth root of unity.

If α be a root of x^n-a =0 then αt is also a root of it.

It means t = α^{-1} (αt) in K and K is a splitting field of $x^n - a$ in F[x].

Let F⊆F (t) ∈ K implies F(t) is the splitting field of $x^n - 1$.

Hence G(K, F(t)) is a normal subgroup of G (K, F)

Again since K is the splitting field of $x^n - a \in F[x]$ so that G(K, F(t)) is abelian.

Then (e) $\subseteq$ G (K, F (t)) $\subseteq$ G(K,F) serves as a normal series. Thus by the fundamental theorem of Galois theory , we have G(K, F) / G(K, F(t)) $\equiv$ G (F (t), F)

Now since G (F(t), F) is abelian , so that G(K, F) has a normal series with abelian factors.

Hence G (K,F) is solvable.

Example 6: (2016)

Find the splitting field K of polynomial $x^4 - x^2 + 1$ over the field of rational numbers. Also determine the Galois group of K over Q. Show that it is not a cyclic group.

Solution:

$x^4 - x^2 + 1 = (x^2 + 1)^2 - 3x^2 = \{x + \sqrt{3}/2\}^2 + (1/2)^2\} \{(x - \sqrt{3}/2)^2\} + (1/2)^2\}$

Thus, splitting field of $x^4 - x^2 + 1$ over Q is given by Q ($x\sqrt{3} \pm i/2$) = Q ($\sqrt{3}$, i) = K

Clearly, [K:Q] = 4.

Also, the given polynomial is irreducible over Q.

Thus we can get $p_1, p_2, p_3, p_4 \in$ G (K, Q) such that ,

$p_1 (\sqrt{3} + i/2) = (\sqrt{3} + i/2)$; $p_2 (\sqrt{3} + i/2) = (\sqrt{3} - i/2)$, $p_3 (\sqrt{3} + i/2) = -\sqrt{3} + i/2$, $p_4 (\sqrt{3} + i/2) = -\sqrt{3} - i/2$

Also for any p in G (K, Q), p ($\sqrt{3} + i/2$) is a root of given polynomial.

Thus G (K, Q) = { p_1, p_2, p_3, p_4 }

Clearly $p_1 (\sqrt{3} - i/2) = \sqrt{3} - i/2$

$p_1 (-\sqrt{3} - i/2) = (-3 - i/2)$

$p_1 (-\sqrt{3} + i/2) = (-\sqrt{3} + i/2) = p_1 (-\sqrt{3} + i/2) + (\sqrt{3} - i/2) = \sqrt{3}$

Also, $p_1 (i) = i$ and $p_1 (i\sqrt{3}) = i\sqrt{3}$

Since {1, $\sqrt{3}$, i, $i\sqrt{3}$) is a basis of K and Q. So $p_1 = 1$, the identity is morphism of K.

Similarly, we can see that.

$p_2 (\sqrt{3}) = -i\sqrt{3}$

$p_3 (\sqrt{3}) = i\sqrt{3}$

$p4(\sqrt{3}) = i\sqrt{3}$

Also, $p_2^2 (\sqrt{3}) = \sqrt{3}$

$p_2^2 (i) = p_2 (-i) = i$

$p_2^2 (\sqrt{3}i) = p_2 (-i\sqrt{3}) = i\sqrt{3}$

Thus $p_2^2 = 1$

Similarly, we can also see that each of p1, p2, p3, p4 is of order 2 while G(K,Q) = { p1, p2, p3, p4} of order 4. Hence it is not a cyclic group.

Example 7: (217, 2019)

If $K = \Phi(\sqrt{2})$, Φ is the field of Q then Φ is the field of the group of automorphism of K.

Solution: Let Automorphism (K) = set of all automorphism of K such that $K = \Phi(\sqrt{2})$

Now the minimal polynomial of $\sqrt{2}$ over Q is $x^2 - 2$ and $\{1, \sqrt{2}\}$ forms a basis of K over Q implies that any n in K is of the form of $a + b\sqrt{2}$, where $a_1 b \in Q$.

Let g be any automorphism of K such that $g(a) = a$, for every $a \in Q$.

Now $g(\sqrt{2})$ is conjugate of $(\sqrt{2})$ over Q. But $\sqrt{2}$ and $-\sqrt{2}$ are the only roots of $x^2 - 2$.

Thus, we have $g(\sqrt{2}) = (\sqrt{2})$ or $g(\sqrt{2}) = -\sqrt{2}$

Thus we consider two following cases:

Case1. Let$\sqrt{2}$ now $p(x) = p(a+b\sqrt{2}) = p(a)\, p(b)\, p(\sqrt{2}) = a + b\sqrt{2} = x$, $x \in K$

Thus p= 1, the identity map on K

Case 2. Let $p\sqrt{2} = -\sqrt{2}$. Thus $p(x) = p(a+b\sqrt{2}) + p(a) = p(b)(p\sqrt{2}) = a - b\sqrt{2}$, each $x \in K$

Let this automorphism be donated by g. Thus (K) contains only two elements 1 and g

Let F_0 be fixed field under Aut (K) and let $x \in F_0$

Hence $p(x) = x$ that is $a - b\sqrt{2} = a + b\sqrt{2}$ implies $b=0$

Thus $x = a \in \Phi$

Thus, F_0 C Q. But Q is a prime field so $Q \subseteq F_0$

Hence $F_0 = Q$

Therefore, Q is the fixed field under automorphism (K).