Advanced Abstract Algebra-I

DEMTH516

Edited by
Dr. Kulwinder Singh

LOVELY PROFESSIONAL UNIVERSITY

Advanced Abstract Algebra-I

Edited By:
Dr. Kulwinder Singh

CONTENT

Unit 01: Review of Groups

Contents

Expected Learning Outcomes

After studying this unit, you will be able to

- understand the binary operations on sets
- analyze different algebraic structures like groups and subgroups
- understand properties of cosets and normal subgroups
- state and prove Lagrange's theorem
- find the order of any element of a group
- define cyclic group and create quotient group/ factor group for a given group G
- define homomorphism from a group G to some group G'
- observe the isomorphisms between groups
- important results based on isomorphism

Introduction

The theory of groups is one of the oldest branches of abstract algebra. It has many applications in mathematics and other sciences. Group theory has helped in developing physics, chemistry, and computer science. Its roots go back to the work of the eighteenth-century mathematicians Lagrange, Ruffini, and Galois.

In this unit, we will study group theory in detail. We surge fine groups, subgroups and give some examples. After that, we study the properties of cosets leading to the normal subgroups, the order of an element and related properties, group homomorphisms, isomorphisms, etc. Group theory is very vast and cannot be limited to one unit. However, this unit provides us the sufficient basic knowledge about group theory, which is needed in understanding the consequent units.

1.1 Definition of Group and Subgroup

Binary operations on a set

Definition 1.1.1 Let S be a non-empty set. A function $f: S \times S \to S$ i.e., $\forall\, a, b \in S, f(a, b) \in S$ then this is called binary composition. In other words, $*$ is called a binary composition on a set S if $*(a, b) \in S \;\forall\, a, b \in S$. We will write $*(a, b)$ as $a * b$. Therefore, a binary operation associates every pair of elements of set S to a unique element in set S.

Example 1.1.2: Since addition, subtraction, and multiplication of two integers is an integer, therefore, the operations addition, subtraction, and multiplication are all binary operations on S.

Example 1.1.3: Let X be a non-empty set and F(X) be the family of all functions from X to itself, the composition of functions is a binary composition on F(X).

Now we see examples where a composition is not binary on a set S

Example 1.1.4: Subtraction is not a binary composition on set N of Natural numbers. 2 and 3 are both natural numbers but $2 - 3 = -1$ is not a natural number.

Example 1.1.5: Division is not a binary composition on set Z of Integers. 1 and 2 are both integers but $\frac{1}{2}$ is not an integer.

Next, we define some properties of Binary compositions

Let $*$ be a binary composition on a non-empty set S. Then

Closure: $*$ is closed on S, if $a * b \in S \; \forall \; a, b \in S$

All the binary compositions by definition, satisfy this property

Associative: $*$ is associative on S, if $a * (b * c) = (a * b) * c \; \forall \; a, b, c \in S$

A binary composition may or may not be associative. Here are examples to explain this

Example 1.1.6: Consider the set of integers Z, we know that addition is binary composition on Z and $(a + b) + c = a + (b + c)$ for all integers a, b, c. Addition is associative binary composition on Z.

Example 1.1.7: Consider the set of integers Z, we know that subtraction of two integers is again an integer so it is binary composition on Z. However, for $3, 4, 5 \in Z$,

$$(3 - 4) - 5 = -1 - 5 = -6$$
$$3 - (4 - 5) = 3 - (-1) = 4$$

Therefore, $(3 - 4) - 5 \neq 3 - (4 - 5)$

Hence, subtraction is not associative on Z.

Existence of Identity: Let there exists an element $e \in S$, such that $a * e = a = e * a \; \forall \; a \in S$, then S is said to have an identity element with respect to composition $*$.

Identity may or may not exist for a binary composition on a set. Following are examples

Example 1.1.8: Consider the set of integers Z, we know that addition is binary composition on Z. Note that $0 \in Z$ and $a + 0 = a = 0 + a \; \forall \; a \in Z$.

Example 1.1.9: Consider the set of integers Z, we know that subtraction of two integers is again an integer so it is binary composition on Z. However, there does not exist any $e \in Z$ such that

$$a - e = a = e - a$$

Hence, the identity element does not exist under subtraction.

Note $0 \in Z$ such that $a - 0 = a$ for all integers a but it does not satisfy the second part.

Existence of Inverse: Let $a \in S$, where S is the set with identity, if there exists an element $b \in S$ such that $a * b = e = b * a$ then we say that inverse of element a exists in S and b is said to be inverse of a. Note that $e \in S$ is its own inverse. In this case, two cases are possible

Case I: There are some elements in S that are invertible but some are not invertible.

Example 1.1.10: Consider the set of integers Z. Then multiplication is a binary operation on Z with identity element 1. Then in Z, under multiplication, only two elements 1 and -1 have inverse in Z but all other integers are not invertible in Z. For example, $2 \in Z$ but its multiplicative inverse $\frac{1}{2} \notin Z$.

Case II: All elements in the set have inverse in S

Example 1.1.11: Consider the set of integers Z. Then addition is a binary operation on Z with identity element 0 and $\forall\, a \in Z, \exists -a \in Z$ such that $a + (-a) = 0 = (-a) + a$.

Commutative: If $a * b = b * a \;\forall\, a, b \in S$ then the composition $*$ is called commutative. A set may or may not be commutative under a binary operation.

Example 1.1.12: Consider the set of integers Z, under the binary composition of addition. Then $a + b = b + a \;\forall\, a, b \in Z$ this implies that Z is commutative under addition.

Example 1.1.13: Consider the set of integers Z, under the binary composition of subtraction. Then $a - b \neq b - a$ in general. Hence it is not commutative.

Now let's see some more examples

Example 1.1.14: Let Q denotes the set of rational numbers. Define an operation $*$ on Q as $a * b = a + b - ab \;\forall\, a, b \in$ Q. Then check that the set Q satisfies which of the above-mentioned properties.

Solution: Set Q and the given composition is $a * b = a + b - ab$

Closure: Clearly, addition, multiplication, and product of two rational numbers is again a rational number so $a + b - ab \in$ Q $\forall\, a, b \in$ Q. That is, $*$ is a binary composition on Q.

Associative: Let $a, b, c \in$ Q. Then

$$\begin{aligned} a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= (a * b) * c \end{aligned}$$

Hence, Q is associative under $*$.

Existence of Identity: $0 \in$ Q and for any $a \in$ Q

$$a * 0 = a + 0 - a.0 = a + 0 - 0 = a$$

Also,

$0 * a = 0 + a - 0 \cdot a = 0 + a - 0 = a$

Therefore, 0 is the identity element of Q under the composition $*$.

Existence of Inverse: For $a \in$ Q, $a \neq 1$,

Consider $\frac{a}{a-1} \in$ Q

Then

$$a * \frac{a}{a-1} = a + \frac{a}{a-1} - a \cdot \frac{a}{a-1} = \frac{a^2 - a + a - a^2}{a-1} = 0$$

and

$$\frac{a}{a-1} * a = \frac{a}{a-1} + a - \frac{a}{a-1} \cdot a = \frac{a + a^2 - a - a^2}{a-1} = 0$$

Therefore, $\forall a \in Q, a \neq 1$, $\frac{a}{a-1} \in Q$ so, inverse exists for all $a \neq 1$.

But for $a = 1$,

$$\begin{aligned} & a * b = 0 \\ \Leftrightarrow\ & a + b - ab = 0 \\ \Leftrightarrow\ & 1 + b - b = 0 \\ \Leftrightarrow\ & 1 = 0 \end{aligned}$$

which is absurd. Therefore, inverse of 1 does not exist.

Commutative: For $a, b \in Q$

$$ab = ba$$

and

$$a + b = b + a$$

This implies

$$a + b - ab = b + a - ba$$

which gives

$$a * b = b * a$$

Therefore, it is commutative on Q.

Now, we are in a position to define some algebraic structures based on these properties of a binary operation.

We can talk about the inverse of an element in a set only if identity element exists. Otherwise, inverse is not even defined.

Group

Monoid: Monoid is any non-empty set with binary composition $*$.

Semi-group: A non-empty set S with a binary composition $*$ is called a semi-group if S is associative under the composition $*$.

Note: Every Semi-group is clearly a monoid but a monoid may not be a semi-group. For example, the set of integers Z under the binary composition of subtraction of integers is monoid but not semi-group as it is not associative.

Quasi-group: A semi-group is called Quasi group if it contains an identity element under the composition.

Note: Every Quasi-group is Semi-group but the converse is not true. For example, the set of even integers is semi-group under the composition of multiplication of integers but the identity element 1 does not belong to this set. Hence it is not a Quasi-group.

The smallest set satisfying all the above-mentioned properties under addition is {0} and under multiplication is {1}.

Definition 1.1.15 Group: A Quasi-group is called a group if all the elements of the set have inverse in the set.

In other words, a group can be defined as

A non-empty set G with a binary composition $*$ is called a group if it satisfies the following axioms

(i) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

(ii) There exists an element $e \in G$ such that $a * e = a = e * a$ for all $a \in G$.

(iii) For each $a \in G$, there exists $b \in G$ such that $a * b = e = b * a$.

Let us see some examples of Groups

Example 1.1.16: As seen earlier, the set of integers satisfies all these properties under the operation of addition, and hence (Z, +) is a group.

Example 1.1.17: The set of all non-zero rational numbers (Q^*) form a group under multiplication.

Proof:

Closure: Multiplication of two non-zero rational numbers is a rational number so it is closed.

Associative: Clearly, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in Q^*$.

Identity: $1 \in Q^*$ such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in Q^*$.

Inverse: $\forall\ a \in Q^*$, $\frac{1}{a} \in Q^*$ and $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$

Therefore, Q^* is a group.

Example 1.1.18: The set S of all square matrices of order 2 with entries from the set of real numbers is a group under the composition of the addition of matrices.

Proof:

Closure: Addition of two square matrices of order 2 with entries from the set of real numbers is again a matrix of order 2 with entries from the set of real numbers therefore, S is closed.

Associative: By definition of matrix addition and associativity in the set of real numbers under addition, we can observe that associativity holds.

Identity: Let $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Then O is a square matrix of order 2 with all the entries 0 hence $O \in S$ and $\forall A \in S, A + 0 = A = 0 + A$.

Inverse: For each $A \in S$, there exist $-A \in S$ and $A + (-A) = 0 = (-A) + A$.

Therefore, S is a group under the composition of addition of matrices.

Definition 1.1.19: A group G under the composition $*$ is called a ***commutative group or abelian group*** if $a * b = b * a\ \forall a, b \in G$. For example, set of integers under addition.

Notation: From this point onwards, group G with composition $*$ will be denoted as (G, $*$). Generally, we will assume that $*$ is multiplication and we will simply write $(G, *)$ as G. We will denote $a * b$ as ab for the sake of convenience.

Definition 1.1.20: A group G is called a ***finite group*** if it contains finite number of distinct elements, otherwise it is called an infinite group.

Definition 1.1.21: The number of distinct elements in a finite group G is called the ***order of the group.*** It is denoted as O(G). If G is infinite then we say that order G is infinite.

Example 1.1.22: The set $G = \{1, -1, i, -i\}$ is a finite group with 4 elements under the composition of multiplication of complex numbers.

Proof:

Closure: For any elements $a, b \in G, a.b \in G$.

Associative: Associativity is due to the associativity of multiplication in complex numbers.

Identity: $1 \in G$ such that $a.1 = a \; \forall \; a \in G$.

Inverse: Inverse of 1 is 1, -1 is -1, i is $-i$ and of $-i$ is i. So, the inverse of each element of G is in G.

Therefore, G is a group with 4 elements, and hence G is a finite group.

Example 1.1.23: The sets (Z, +), (Q, +), (R, +), (Q*, ·), etc. are examples of infinite groups.

Note: The fact that a group must contain an identity element and it is always a non-empty set implies that the smallest possible group is {e}. That is the minimum order of a group is 1.

Definition 1.1.24: Let S be a non-empty set. For $a, b, c \in S$, if $ab = ac$ implies $b = c$, then we say left cancellation law holds in S. Similarly, if $ba = ca$ implies $b = c$, then we say the right cancellation law holds in S.

Theorem 1.1.25: Let G be a group. Then both the cancellation laws hold in G.

Proof:

Let G be a group and $a, b, c \in G$

Let $ab = ac$ ... ... (1)

Since $a \in G$, therefore, $a^{-1} \in G$

Pre-multiplying both sides of (1) with a^{-1}

We get, $a^{-1}(ab) = a^{-1}(ac) \Rightarrow b = c$.

Similarly, we can see that the right cancellation law holds in G.

Subgroup

We have seen that set of integers Z, set of real numbers R, set of complex numbers C are all groups under addition. Also $Z \subset R \subset C$. Based on this, we define a subgroup

Definition 1.1.26: Let G be a group then a non-empty subset H of G is called a subgroup of G if it is itself a group under the same composition as G. For example, (Z, +) is a subgroup of (R, +); (R, +) is a subgroup of (C, +).

Trivial and Non-trivial Subgroups: A group G having at least two elements has at least two subgroups {e} and G. These are called ***trivial or improper*** subgroups. Any other subgroup is called ***non-trivial or proper*** subgroups.

Theorem 1.1.27: A non-empty subset H of G is a subgroup of G if and only if $ab^{-1} \in H \; \forall \; a, b \in H$.

Proof:

Let H be a subgroup of G. Then H is a group under the same composition as G. For $b \in H$, $b^{-1} \in H$ and therefore, $\forall a, b \in H, ab^{-1} \in H$.

Conversely, let $ab^{-1} \in H \; \forall \; a, b \in H$

Since H is non-empty. There exist some $a \in H$ then by given condition $aa^{-1} \in H \; \Rightarrow \boldsymbol{e \in H}$

Again, for $e, a \in H \; \Rightarrow ea^{-1} \in H \Rightarrow \boldsymbol{a^{-1} \in H}$ for all $a \in H$.

Consider $a, b \in H, b^{-1} \in H \; \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow \boldsymbol{ab \in H}$

For $a, b, c \in H$, since $H \subseteq G$ and G is a group, therefore, $a(bc) = (ab)c$

Therefore, H is a subgroup of G.

Example 1.1.28: Let G be the set of square matrices of order 2 over the field of real numbers. Then G is a group under the addition of matrices. Let H= $\left\{\begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \middle| a, b, c \in R\right\}$ then H is a subgroup of G.

Proof: Clearly, H is a non-empty subset of G.

Let $\begin{bmatrix} a_1 & b_1 \\ c_1 & 0 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & 0 \end{bmatrix} \in$ H.

Then $\begin{bmatrix} a_1 & b_1 \\ c_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ c_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ c_1 - c_2 & 0 \end{bmatrix} \in$ H

Therefore, H is a subgroup of G.

Example 1.1.29: Let G = C^* be the set of non-zero complex numbers. G is a group under the multiplication of complex numbers. Then $H = \{z \in C^* || z| = 1\}$ is a subgroup of G.

Proof: $1 \in H$ therefore, H is non-empty.

Then for $a, b \in H$

$$|ab^{-1}| = |a||b|^{-1} = 1$$

Therefore, $ab^{-1} \in H$.

Then H is a subgroup of G.

Theorem 1.1.30: Subgroup of an abelian group is abelian.

Proof:

Let G be an abelian group and H be a subgroup of G.

For $a, b \in$ H. Since H $\subseteq$ G, therefore $a, b \in$ G

G is abelian so, $ab = ba$

H is abelian.

Task: For the following binary operations defined on the set of real numbers R, determine whether they are

(1) Commutative
(2) Associative

or not.

$(i)\ x \oplus y = x + y - 5$

$(ii)\ x * y = 2(x + y)$

$(iii)\ x \Delta y = \frac{x - y}{2}$

For all $x, y \in R$

1.2 Normal Subgroups and Cosets

Coset

Definition 1.2.1: Let H be a subgroup of G. Then $\forall\ a \in G$, the set $aH = \{ah | h \in H\}$ is a subset of G. aH is called ***left coset*** of H in G. Similarly, the set $Ha = \{ha | h \in H\}$ is the right coset of H in G. Left coset and right coset may or may not be equal.

An example where a left coset is not equal to right coset

Example 1.2.2: Let G be the set of invertible matrices of order 2. Then G is a group under the composition of multiplication of matrices. Let H be the set of invertible diagonal matrices. Then for A given by

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

$$AH = \left\{ \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} B \,\middle|\, B \in H \right\} = \left\{ \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in R \right\} = \left\{ \begin{bmatrix} a & 2b \\ 3a & 4b \end{bmatrix} \middle| a, b \in R \right\}$$

$$HA = \left\{ B \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \middle| B \in H \right\} = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \middle| a, b \in R \right\} = \left\{ \begin{bmatrix} a & 2a \\ 3b & 4b \end{bmatrix} \middle| a, b \in R \right\}$$

Then $\begin{bmatrix} 1 & 4 \\ 3 & 8 \end{bmatrix} \in AH$ but $\begin{bmatrix} 1 & 4 \\ 3 & 8 \end{bmatrix} \notin AH$.

Note:
For a subgroup H of an abelian group G, right cosets are the same as left cosets.
For $e \in G$, $He = H = eH$ therefore, in any group G and its subgroup H, one left as well as right coset of H in G is H itself.

Theorem 1.2.3: Let H be a subgroup of a group G. For $a, b \in G$,

1) $a \in H \Leftrightarrow Ha = H$
2) $Ha = Hb \Leftrightarrow ab^{-1} \in H$
3) $Ha = Hb \text{ or } Ha \cap Hb = \phi$

Proof:

1) Let $a \in H$

$Ha = \{ha | h \in H\}$

Since H is a subgroup of G so it is closed. Therefore, $h \in H$ and $a \in H \Rightarrow ha \in H \Rightarrow \boldsymbol{Ha \subseteq H}$.

Also, for $h \in H, a \in H \Rightarrow a^{-1} \in H$.

This implies $ha^{-1} \in H \Rightarrow (ha^{-1})a \in Ha \Rightarrow h \in Ha \Rightarrow \boldsymbol{H \subseteq Ha}$

Therefore, $\boldsymbol{Ha = H}$.

Conversely, let $Ha = H$

$e \in H \Rightarrow ea \in Ha \Rightarrow a \in Ha = H$.

2) $Ha = Hb \Leftrightarrow Hab^{-1} = H$

$\Leftrightarrow ab^{-1} \in H$ (Using (1)).

3) For $a, b \in G$.

Let $Ha \cap Hb \neq \phi$.

Then there exists some element $x \in Ha \cap Hb$

$\Rightarrow x \in Ha$ and $x \in Hb$

$\Rightarrow xa^{-1} \in H$ and $xb^{-1} \in H$ (Using (2))

$\Rightarrow (xa^{-1})^{-1}(xb^{-1}) \in H$ (For $x, y \in H \Rightarrow x^{-1}y \in H$)

$\Rightarrow (ax^{-1})(xb^{-1}) \in H \Rightarrow ab^{-1} \in H$.

$\Rightarrow Ha = Hb$ (Using (2)).

That proves that either $Ha = Hb \text{ or } Ha \cap Hb = \phi$.

Note: Only one of the distinct right cosets of a subgroup H in a group G is a subgroup.

If possible, let two distinct right cosets Ha and Hb are sub-groups then

$$e \in Ha \cap Hb \Rightarrow Ha = Hb \text{ (Using (3)).}$$

So, we arrive at a contradiction. That is, there is only one right coset which is subgroup also. That right coset is H.

Let H be a subgroup of a group G. Define a relation on elements of G. For two elements $a, b \in G$, a is related to b if and only if $ab^{-1} \in H$. We denote it as $a \sim b$.

Theorem 1.2.4: The relation defined above is an equivalence relation on G.

Proof:

By definition, two elements $a, b \in G$, $a \sim b$ if and only if $ab^{-1} \in H$

Reflexive: Since H is a subgroup of G.

Therefore, $e \in H$

That is, $e = aa^{-1} \in H \; \forall \; a \in G$

$a \sim a$ for all $a \in G$.

Symmetric: For $a, b \in G$, let $a \sim b$

$\Rightarrow ab^{-1} \in H$.

Since H is a subgroup of G.

$\Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H$,

$\Rightarrow b \sim a$.

Transitive: For $a, b, c \in G$

Let $a \sim b, b \sim c$

$\Rightarrow ab^{-1} \in H, bc^{-1} \in H$.

H is a subgroup of G and hence it is closed

$\Rightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in H$.

$\Rightarrow a \sim c$.

Therefore, the relation $\sim$ is an equivalence relation on G.

Remark 1: Equivalence Class for some element $a \in G$ is Ha.

Proof: Let $C(a)$ denote the equivalence class of $a \in G$.

Then $b \in C(a) \Leftrightarrow b \sim a \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$.

This implies that $C(a) = Ha$.

With the help of this result, we can find the order of a finite group G in terms of the order of a subgroup H and the number of right (left) cosets of H in G.

Remark 2: Let $x \in G$ and $C(x)$ be the class containing x. Then for any $y \in G$, we have seen that $C(x) = C(y)$ or $C(x) \cap C(y) = \phi$, which implies that

$$G = \bigcup_{x \in G} C(x) = \bigcup_{x \in G} Hx$$

Remark 3: Let G be a finite group and H be a subgroup of G. Then the number of right (left) cosets of H in G is finite.

Proof: If possible, let the number of right cosets of H in G is infinite.

Since

$$G = \bigcup_{x \in G} Hx$$

This implies

$$O(G) = O\left(\bigcup_{x \in G} Hx\right)$$

Using the fact that for $x, y \in G$, either $Hx = Hy$ or $Hx \cap Hy = \phi$, we see that

$$O(G) = \sum_{x \in G} O(Hx)$$

Since $x \in Hx$, therefore, $O(Hx) \geq 1$ for all $x \in G$.

Also, the number of right cosets of H in G is infinite, that gives $O(G)$ is infinite.

This contradicts the fact that G is a finite group. Therefore, our assumption was wrong.

That is, the number of right cosets of H in G is finite.

Theorem 1.2.5 (Lagrange's Theorem): Let H be a subgroup of a finite group G. Then order of H divides order of group G.

Proof: Let H be a subgroup of G and $Ha_1, Ha_2, \ldots, Ha_t$ be all the right cosets of H in G.

Then

$$G = \bigcup_{i=1}^{t} Ha_i$$

$$\Rightarrow O(G) = 0\left(\bigcup_{i=1}^{t} Ha_i\right) = \sum_{i=1}^{t} O\,(Ha_i) \ldots . (1)$$

Claim: $\boldsymbol{O(Hx) = O(H)\ \forall\ x \in G}$

$$Hx = \{hx | h \in H\}$$

Let $H = \{x_1, x_2, \ldots, x_n\}$. Then

$$Hx = \{xx_1, xx_2, \ldots, xx_n\}$$

Then

$$xx_i = xx_j$$

Because cancellation laws hold in the group

$$\Leftrightarrow x_i = x_j$$

This implies $O(Hx) = O(H)$.

From (1)

$$O(G) = \sum_{i=1}^{t} 0\,(H) = tO(H)$$

Since t is the number of right cosets of H in G. That is, $t \in Z$

This implies, $O(H)$ divides $O(G)$.

Definition 1.2.6: Let G be a finite group and H be a subgroup of G. Then the number of right cosets of H in G is finite and number of right cosets of H in G is the index of H in G. It is denoted as $[G:H]$.

Example 1.2.7: Let $G = \{1, -1, i, -i\}$. Then G is a finite group under the composition of multiplication of complex numbers. Then $H = \{1, -1\}$ is a subgroup of G. Then verify Lagrange's theorem for G and subgroup H.

Solution:

Let Hx be right coset of H in G for $x \in G$.

For $x = 1, H(1) = H$

For $x = -1, H(-1) = \{1(-1), (-1)(-1)\} = \{-1, 1\} = H$

For $x = i, Hi = \{1(i), (-1)(i)\} = \{i, -i\}$

For $x = -i, H(-i) = \{1(-i), (-1)(-i)\} = \{-i, i\}$

So, there are only two distinct right cosets of H in G, H, and Hi.

$$O(G) = 4 = 2 \times 2 = [G:H]O(H).$$

Note: If G is a group under the composition of addition then for any subgroup H of G and an element $a \in G$, the right coset of H in G is defined as $H + a = \{h + a | h \in H\}$. Similarly, left coset of H in G is defined as $a + H = \{a + h | h \in H\}$.

Normal Subgroup

Definition 1.2.8: A subgroup H of a group G is such that $Ha = aH \; \forall \; a \in G$, then H is a normal subgroup of G. Clearly, every subgroup of an abelian group is a normal subgroup.

Theorem 1.2.9: H is a normal subgroup of G if and only if $g^{-1} hg \in H$ for all $g \in G, h \in H$.

Proof:

Let H is a normal subgroup of G.

For $g \in G, h \in H$

$hg \in Hg = gH$ (H is normal subgroup of G)

$\Rightarrow \; g^{-1}hg \in H$.

Conversely, Let $g^{-1}hg \in H \; \forall g \in G, h \in H$

$g^{-1}hg \in H \Rightarrow hg \in gH \; \forall \; h \in H, g \in G$

$\Rightarrow Hg \subseteq gH$.

Also, $g^{-1}hg \in H \; \Rightarrow g^{-1}hg = h_1$ for some $h_1 \in H$

$\Rightarrow gh_1 = hg$ which implies that $gH \subseteq Hg$.

Therefore, $Hg = gH$.

Definition 1.2.10: Let G be a group. Then the centre of group G is defined as the set $\{x \in G | xy = yx \; \forall \; y \in G\}$ and it is denoted as $Z(G)$. Clearly, when G is abelian then $G = Z(G)$.

Theorem 1.2.11: For any group G, the centre of group G is a normal subgroup of G.

Proof:

$$Z(G) = \{x \in G | xy = yx \; \forall \; y \in G\}$$

Let $e \in G$ be the identity element of group G.

That is $ey = y = ye \; \forall \; y \in G \; \Rightarrow e \in Z(G) \Rightarrow \boldsymbol{Z(G) \neq \phi}$

Clearly $Z(G) \subseteq G$.

Let $a, b \in Z(G) \Rightarrow ay = ya, by = yb \; \forall \; y \in G$

For $y \in G, by = \; yb \; \Rightarrow b^{-1}(by)b^{-1} = b^{-1}(yb)b^{-1} \Rightarrow yb^{-1} = b^{-1}y$

Now for any $y \in G, ab^{-1}y = ayb^{-1} = yab^{-1} \Rightarrow ab^{-1} \in Z(G)$.

Hence, $\boldsymbol{Z(G)}$ **is a subgroup of** $\boldsymbol{G}$**.**

Now, we prove that $Z(G)$ is a normal subgroup of G.

Let $g \in G, a \in Z(G)$ then $ga = ag$

Then for any $y \in G$,

$y(g^{-1}ag) = y(g^{-1}ga) = ya = ay \; (as \; a \in Z(G)) = (g^{-1}g)(ay) = (g^{-1}ag)y$

Thus, $g^{-1}ag \in Z(G)$

Hence, $Z(G)$ is a normal subgroup of G.

Theorem 1.2.12: Let G be a group and H is a subgroup of G such that $[G:H] = 2$, then H is a normal subgroup of G.

Proof:

Let H be a subgroup of G with $[G:H] = 2$.

Then the number of distinct right cosets of H in G is 2.

Let H and Ha be those two right cosets such that $H \neq Ha$.

Also, $G = H \cup Ha, H \cap Ha = \phi$

Similarly, there are only two left cosets of H in G is 2.

Let H and aH be those two left cosets of H in G

That implies, $G = H \cup aH, H \cap aH = \phi$

That is, $H \cup Ha = aH \cup H$

Let $x \in Ha \subseteq H \cup Ha = aH \cup H$

This implies $x \in aH$ or $x \in H$

But $x \notin H$

Therefore, $x \in aH$

That is, $Ha \subseteq aH$

Similarly, $aH \subseteq Ha$

That is $Ha = aH$

H is a normal subgroup of G.

Task: Write Z as union of disjoint cosets of 5Z.

For any subgroup H of a group G and any element $x \in G$, prove that $O(Hx) = O(H)$.

1.3 Order of elements and Factor Group:

Order of an element

Definition 1.3.1: Let G be a group and $a \in G$, the least positive integer n for which $a^n = e$, is called the order of a and we write $O(a) = n$. If there exists no such positive integer for which $a^n = e$ then we say that order of the element is infinite.

In case, G is a group under addition and $a \in G, O(a)$ is defined to be the least positive integer such that $na = e$.

For example, consider the group $G = \{1, -1, i, -i\}$ under the composition of multiplication of complex numbers. Then G has identity element 1.

Since $1^1 = 1$, therefore $O(1) = 1$

$(-1)^2 = 1 \Rightarrow O(-1) = 2$.

$(i)^4 = 1$ and $(i)^n \neq 1$ for any $n < 4 \Rightarrow O(i) = 4$.

$(-i)^4 = 1$ and $(-i)^n \neq 1$ for any $n < 4 \Rightarrow O(-i) = 4$.

Another example, consider (Z, +), then $2 \in Z$, and there does not exist any positive integer n such that $2n = 0$.

Theorem 1.3.2: Let G be a group and $a \in G$ be an element. Then the set $S = \{a^n | n \in Z\}$ is a subgroup of G.

Proof:

Since $a \in G$, $a = a^1 \in S \Rightarrow S \neq \phi$

Let $x, y \in S \Rightarrow \exists\ t, r \in Z$ such that $x = a^t, y = a^r \Rightarrow xy^{-1} = a^t a^{-r} = a^{t-r} \in S$.

Therefore, S is a subgroup of G.

S is called ***subgroup of G generated by a*** and we write $S = < a >$.

Definition 1.3.3: A group G is called ***cyclic group*** if there exists some element $a \in G$ such that G is generated by a. That is, $G = < a >$ and a is called generator of group G.

For example,

The group $G = \{1, -1, i, -i\}$ is a cyclic group generated by i because $G = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$.

Note: Generator of a cyclic group is not unique. For example, $G = < i > = < -i >$.

Theorem 1.3.4: Let $G = < a >$ be a cyclic group generated by a. Then $O(G) = O(a)$.

Proof: Case I: If $O(a)$ is finite.

Let $O(a) = n$,

Since $a \in G$, therefore, $a, a^2, a^3, \dots, a^{n-1}, a^n = e \in G$

Let $b \in G = < a >$

Therefore, there exist $t \in Z$, such that $b = a^t$

Divide t by n, we get unique integers q, r such that $t = nq + r; r = 0$ or $0 < r < n$

Then $a^t = a^{nq+r} = a^{nq}a^r = a^r$ (Since $O(a) = n$, therefore $a^{nq} = (a^n)^q = e$)

Thus $b \in G$ then $b = a^r$ for some $0 \leq r < n$

That is, $G = \{a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$

This implies $O(G) = n = O(a)$.

Case II: If $O(a)$ is infinite.

If possible, let $O(G)$ is finite.

Since $a, a^2, a^3, \dots \dots \in G$

$O(G)$ is finite. Therefore, there exist $s, t \in Z$ such that $a^s = a^t \Rightarrow a^{r-s} = e \Rightarrow o(a) \leq r - s \Rightarrow O(a)$ is finite. So, we arrive at a contradiction.

Hence $O(G)$ is infinite.

Therefore, in both cases, $O(G) = O(a)$.

Theorem 1.3.5: Every cyclic group is abelian.

Proof:

Let $G = < a >$ is a cyclic group.

Let $b, c \in G$, then there exist $t, r \in Z$ such that $b = a^t, c = a^r$.

Then $bc = a^t a^r = a^{t+r} = a^{r+t} = a^r a^t = cb$

This implies, G is abelian.

However, the converse is not true. That is, an abelian group may not be a cyclic group.

For example, consider Klein's 4- Group $G = \{e, a, b, ab\}$ such that $a^2 = b^2 = e, ab = ba$. Then G is an abelian group. If possible, let G be a cyclic group. Then there exists $x \in G$ such that $O(G) = O(x)$.

Consider elements in G,

$a^2 = e \Rightarrow O(a) = 2$.

$b^2 = e \Rightarrow O(b) = 2$.

$(ab)^2 = abab = aabb = a^2b^2 = e \Rightarrow O(ab) = 2$.

Therefore, there does not exist any $x \in G$ such that $O(x) = 4$. That is $O(x) \neq O(G)$ for any $x \in G$.

Hence G is not a cyclic group.

Theorem 1.3.6: Let G be a finite group then $a^{O(G)} = e \; \forall \; a \in G$.

Proof:

Let $a \in G$,

Then $H = \{a, a^2, a^3, \dots \dots\} \subseteq G$

That is, $H = < a >$ is a subgroup of G.

This implies, $O(H) = O(a)$

By Lagrange's theorem, $O(H)$ divides $O(G)$.

There exists some integer $t, O(G) = O(H)t$

Consider $a^{O(G)} = a^{O(H)t} = \left(a^{O(H)}\right)^t = \left(a^{O(a)}\right)^t = e^t = e$.

Which completes the proof.

Theorem 1.3.7: Let G be a group. Let $a \in G$, $a^k = e$ if and only if $O(a)$ divides k.

Proof:

Let $a^k = e$ and let $O(a) = n$

Divide k by n, there exists unique $q, r \in Z$ such that

$k = nq + r$; $r = 0$ or $0 < r < n$

$$a^k = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e \cdot a^r = a^r$$

If $r \neq 0$, then $a^r = a^k = e$ and $0 < r < n$ which contradicts the fact that $O(a) = n$.

Therefore, $r = 0 \Rightarrow k = nq \Rightarrow n$ divides k.

Conversely,

Let k divides n, therefore, there exists some integer q such that $k = nq$

Then $a^k = a^{nq} = (a^n)^q = e^q = e$.

Theorem 1.3.8: Let G be a group and $a \in G$ be any element. Let $O(a) = n$ and $O(a^k) = m$ then $m = \frac{n}{d}$, where $d = HCF(k, n)$.

Proof:

Given that $d = HCF(k, n)$

This implies d divides k and n both

There exist integers k_1, n_1 such that $k = dk_1, n = dn_1$; $HCF(k_1, n_1) = 1$.

Since $O(a) = n \Rightarrow a^n = e \Rightarrow a^{dn_1} = e \Rightarrow a^{dn_1 k_1} = e \Rightarrow a^{kn_1} = e \Rightarrow (a^k)^{n_1} = e \Rightarrow \boldsymbol{m}$ **divides** $\boldsymbol{n_1}$.

Again $o(a^k) = m \Rightarrow a^{km} = e \Rightarrow n$ divides $km \Rightarrow dn_1$ divides $dk_1 m \Rightarrow n_1$ divides $k_1 m$.

Since $HCF(n_1, k_1) = 1 \Rightarrow \boldsymbol{n_1}$ **divides** $\boldsymbol{m}$.

Since n_1 and m are both positive integers, therefore, $m = n_1 = \frac{n}{d}$.

Factor Groups

Theorem 1.3.9: Let G be a group and H be a normal subgroup of G. Let S be the collection of all the right cosets of H in G. Then S is a group of G under the composition $HaHb = Hab \; \forall \; a, b \in G$.
Proof:

Closure: For $a, b \in G \Rightarrow ab \in G \Rightarrow Hab$ is a right coset of H in G. Therefore, $Hab \in S$.
Associative: For $a, b, c \in G, Ha(HbHc) = Ha(Hbc) = Ha(bc) = H(ab)c = (HaHb)Hc$.
Identity: For $a \in G, HaHe = Hae = Ha = Hea = HeHa$
Therefore, $He = H$ is the identity element of S.
Inverse: For $a \in G, a^{-1} \in G$ that is for each $Ha \in S, Ha^{-1} \in S$ such that

$$HaHa^{-1} = Haa^{-1} = He = H$$

Similarly,

$$Ha^{-1}Ha = Ha^{-1}a = He = H$$

That is inverse of Ha is Ha^{-1}.
Definition 1.3.10: Let G be a group and H be a normal subgroup of G. The set $S = \{Ha | a \in G\}$ consisting of all right cosets of H in G is a group under the composition $HaHb = Hab \; \forall \; a, b \in G$. It is called ***quotient group*** and is denoted as G/H. Order of quotient group G/H is number of elements in G/H that is number of right cosets of H in $G = [G:H] = \frac{O(G)}{O(H)}$.
Remark 4: G/H is a quotient group then H is a normal subgroup.
Proof:

G/H is a group then for $a, a^{-1} \in G$,

$$eaHa^{-1} \subseteq HaHa^{-1} = Haa^{-1} = H$$

$$aHa^{-1} = H \Rightarrow aH = Ha$$

H is a normal subgroup of G.

Task: Consider the group G of all diagonal matrices of order 2 under the composition of addition of matrices. Then prove that every subgroup of H is normal subgroup of G.

1.4 Group Homomorphisms

Definition 1.4.1: Let $(G,*)$ and (G',o) be two groups. Then a function $f:(G,*) \to (G',o)$ is called a homomorphism if $\forall\ a,b \in G, f(a*b) = f(a)of(b)$. For convenience, we write f is a homomorphism from G to G'.

Example 1.4.2: Let G be the group of integers under addition and $G' = \{2^n | n \in Z\}$, the group under multiplication. Define $f: G \to G'$ as $f(n) = 2^n$. Then f is a group homomorphism.

Proof:
For $n, m \in Z$

$$f(n+m) = 2^{n+m} = 2^n 2^m = f(n)f(m)$$

This proves that f is a group homomorphism.

Properties of Homomorphism

Let f is a homomorphism from G to G' .

1) **Let e and e' be the identity elements of G and G' respectively. Then $f(e) = e'$.**
Proof:
For $a \in G$,

$$f(ae) = f(a)f(e)$$
$$\Rightarrow f(a) = f(a)f(e)$$
$$\Rightarrow f(a)e' = f(a)f(e)$$
$$\Rightarrow e' = f(e) \text{ (By cancellation law in group } G')$$

2) **For $x \in G, f(x^{-1}) = (f(x))^{-1}$**
Proof:
For $x \in G$,

$$f(xx^{-1}) = f(e) = e'$$

Also,

$$f(x^{-1}x) = f(e) = e'$$

That is,

$$f(xx^{-1}) = e' = f(x^{-1}x)$$
$$\Rightarrow f(x)f(x^{-1}) = e' = f(x^{-1})f(x)$$
$$\Rightarrow f(x^{-1}) = (f(x))^{-1}$$

Definition 1.4.3: A homomorphism f from a group G to a group G' is called a monomorphism if f is a one-one function.

Example 1.4.4: Let $G = G' = Z$ be the group of integers under addition. Define $f: G \to G'$ be defined as $f(x) = 2x$. Then f is a monomorphism.

Proof:
For $x, y \in G, f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$
This proves that f is a homomorphism.
Again, for $x, y \in G$

$$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$$

This proves that f is one-one and hence it is a monomorphism.

Definition 1.4.5: A homomorphism f from a group G to a group G' is called an epimorphism if f is onto function.

Example 1.4.6: Let G be a group of invertible matrices of order 2 over the field of real numbers and G' be the set of non-zero real numbers. Then G is a group under multiplication of matrices and G' be the group under the multiplication of real numbers. Define $f: G \to G'$ as $f(A) = \det A$.

Proof:
For $A, B \in G, f(AB) = \det AB = \det A \det B = f(A)f(B)$
This proves that f is a homomorphism.
Again, for any non-zero real number n, there exists matrix $A = \begin{bmatrix} n & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that $f(A) = n$.
This implies that f is an epimorphism.

Definition 1.4.7: A homomorphism f from a group G to a group G' is called an endomorphism if $G = G'$. The function defined in example 10 is an endomorphism.

Definition 1.4.8: Let G and G' be two groups. Let $f: G \to G'$ be a homomorphism. Then Kernel of homomorphism f is defined as the set $Ker\ f = \{x \in G | f(x) = e'\}$.

Example 1.4.9: Let $G = G' = Z$ be the group of integers under addition. Define $f: G \to G'$ be defined as $f(x) = 2x$. Find Kernel f.

Solution: $Ker\ f = \{x \in G | f(x) = 0\} = \{x \in G | 2x = 0\} = \{0\}$.

Theorem 1.4.10: Let $f: G \to G'$ be a homomorphism. Then Kernel f is a normal subgroup of G.

Proof:
Since $f(e) = e'$. That is, $e \in Ker\ f \Rightarrow \boldsymbol{Ker\ f \neq \phi}$.
Let $a, b \in Ker\ f \Rightarrow f(a) = e'$ and $f(b) = e'$.
Consider $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)\left(f(b)\right)^{-1} = e'e'^{-1} = e'$
This implies $ab^{-1} \in Ker\ f$
Hence $\boldsymbol{Ker\ f}$ **is a subgroup of** $\boldsymbol{G}$.
Let $g \in G, a \in Ker\ f$ so that $f(a) = e'$.
Consider $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)\ e'\left(f(g)\right)^{-1} = e'$
Therefore, $gag^{-1} \in Ker\ f$
This implies, $\boldsymbol{Ker\ f}$ **is a normal subgroup of** $\boldsymbol{G}$.

Theorem 1.4.11: Let $f: G \to G'$ be a homomorphism. Then Kernel $f = \{e\}$ if and only if f is one-one.

Proof:
Let $f: G \to G'$ be a homomorphism.
Let $Ker\ f = \{e\}$
For $x, y \in G,$ such that
$f(x) = f(y)$
$\Rightarrow f(x)\left(f(y)\right)^{-1} = e'$
$\Rightarrow f(xy^{-1}) = e'$
$\Rightarrow xy^{-1} \in Ker\ f = \{e\}$
$\Rightarrow xy^{-1} = e$
$\Rightarrow x = y$
$\Rightarrow f$ is a one-one function.
Conversely, let f is a one-one function.
Let $x \in Ker\ f$
This implies $f(x) = e'$
But $f(e) = e'$
Given that f is one-one.
$\Rightarrow x = e \Rightarrow Ker\ f = \{e\}$.

Definition 1.4.12: Let $f: G \to G'$ be a homomorphism. Then the set $R = \{f(x) | x \in G\}$ is called ***range set*** of homomorphism f.

Theorem 1.4.13: Range set R of homomorphism $f: G \to G'$ is a subgroup of G'.

Proof:
Since $f(e) = e'$
Therefore, $e \in R \Rightarrow \boldsymbol{R \neq \phi}$
Let $x, y \in R$ therefore, there exists, $x_1, y_1 \in G$ such that
$f(x_1) = x$ and $f(y_1) = y$

$$f(x_1 y_1^{-1}) = f(x_1)f(y_1)^{-1} = xy^{-1}$$

This implies that $xy^{-1} \in R$

Hence, R is a subgroup of G'.

Definition 1.4.14: A homomorphism f from a group G to a group G' is called an ***isomorphism*** if f is one-one and onto function.

Example 1.4.15: Let $G = Z$ and $G' = 2Z$, the function $f: G \to G'$ defined as $f(x) = 2x$ is one-one, onto, and homomorphism. Then f is an isomorphism.

Solution:

For $x, y \in G, f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$

This proves that f is a homomorphism.

Again, for $x, y \in G$

$$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$$

This implies f is one-one.

Also $\forall\, x \in 2Z, x = 2y$ for some $y \in Z$

$$f(y) = 2y = x$$

This implies f is onto.

Hence $f: G \to G'$ is an isomorphism.

Definition 1.4.16: An isomorphism f from a group G to a group G' is called an ***automorphism*** if $G = G'$. For example, $f: Z \to Z$ defined as $f(x) = x$ is a trivial automorphism.

Example 1.4.17: Let G be a group. For $g \in G$, define $f_g: G \to G$ as $f_g(a) = g^{-1}ag$. Then f_g is an automorphism.

Solution:

The function $f_g: G \to G$ is defined as $f_g(a) = g^{-1}ag$.

For $a, b \in G, f_g(ab) = g^{-1}(ab)g = (g^{-1}ag)(g^{-1}bg) = f_g(a)\, f_g(b)$

This implies, $\boldsymbol{f_g}$ **is a homomorphism.**

For $a, b \in G, f_g(a) = f_g(b)$

$\Rightarrow g^{-1}ag = g^{-1}bg$

$\Rightarrow a = b$ (Using cancellation laws)

Therefore, $\boldsymbol{f_g}$ **is one-one.**

For $a \in G$, since $g \in G$

Since G is closed, therefore, $gag^{-1} \in G$ and G

$f_g(gag^{-1}) = g^{-1}(gag^{-1})g = a$

This implies, $\boldsymbol{f_g}$ **is onto.**

Hence $\boldsymbol{f_g}$ is an automorphism.

Definition 1.4.18: Let G be a group. For $g \in G$, define $f_g: G \to G$ as $f_g(a) = g^{-1}ag$. Then f_g is an automorphism and it is called an inner automorphism.

Theorem 1.4.19 (Fundamental Theorem of Homomorphism): Let G and G' be two groups and $f: G \to G'$ be an onto homomorphism. Then G' is isomorphic to a quotient group of G.

Proof:

The function $f: G \to G'$ is an onto homomorphism. Let $Ker\ f = H$.

Define a map $g: G/H \to G'$ as $g(Ha) = f(a)$.

Then $Ha = Hb$

$\Leftrightarrow ab^{-1} \in H = Ker\ f$

$\Leftrightarrow f(ab^{-1}) = e'$

$\Leftrightarrow f(a)\big(f(b)\big)^{-1} = e'$

$\Leftrightarrow f(a) = f(b)$

$\Leftrightarrow g(Ha) = g(Hb)$

Therefore, $\boldsymbol{g}$ **is well defined and one-one**.

Let $b \in G'$

Since $f: G \to G'$ is onto

There exists some $a \in G$ such that $f(a) = b$

This implies $g(Ha) = f(a) = b$

Hence $\boldsymbol{g}$ **is onto.**

Let $Ha, Hb \in G/H$

Then $g(HaHb) = g(Hab) = f(ab) = f(a)f(b) = g(Ha)g(Hb)$

Thus, $\boldsymbol{g}$ **is homomorphism.**

This implies $\boldsymbol{G/Ker\ f \cong G'}$.

As applications to this theorem, we have the following results.

Theorem 1.4.20 (First theorem of Isomorphism): Let f be a homomorphism of a group G onto a group G' and $H = Ker\ f$, K' is a normal subgroup of G' and $K = \{x \in G | f(x) \in K'\}$. Then K is a normal subgroup of G containing H and $G/K \cong G'/K'$.

Proof:

Define function $g: G \to G'/K'$ as $g(x) = K'f(x)\ \forall\ x \in G$.

For $x, y \in G, g(xy) = K'f(xy) = K'f(x)f(y) = (K'f(x))(K'f(y)) = g(x)\ g(y)$.

This implies, $\boldsymbol{g}$ **is homomorphism.**

For $K'y \in G'/K'\ ;\ y \in G'$

The function $f: G \to G'$ is onto

Therefore, there exist $x \in G$ such that $f(x) = y$

Consider $g(x) = K'f(x) = K'y$

Thus $\boldsymbol{g}$ **is onto.**

By Fundamental theorem of Homomorphism, $\boldsymbol{G/Ker\ g \cong G'/K'}$

$$\begin{aligned} \boldsymbol{Ker\ g} &= \{\boldsymbol{x \in G | g(x) = K'}\} \\ &= \{x \in G | K'f(x) = K'\} \\ &= \{x \in G | f(x) \in K'\} \\ &= K \end{aligned}$$

Hence $G/K \cong G'/K'$

Theorem 1.4.21 (Second theorem of Isomorphism): Let H be a normal subgroup of a group G and K is any subgroup of G. Then $K/(H \cap K) \cong HK/H$.

Proof:

Since H is a normal subgroup of G, $HK = KH$. Consequently, HK is a subgroup of G and thus H is a normal subgroup of HK. Therefore, HK/H is defined.

Define $f: K \to HK/H$ by $f(k) = Hk$

For $k_1, k_2 \in K$

$$f(k_1k_2) = Hk_1k_2 = (Hk_1)(Hk_2) = f(k_1)f(k_2)$$

This implies f is homomorphism.

Let $Ha \in HK/H$

$\Rightarrow a \in HK\ \Rightarrow a = hk$ for $h \in H, k \in K$

Consider $f(k) = Hk = Hhk = Ha$

Hence f is onto.

By Fundamental theorem of homomorphism $\boldsymbol{K/Ker\ f \cong HK/H}$

$\boldsymbol{Ker\ f} = \{\boldsymbol{x \in K | f(x) = H}\}$

$= \{x \in K | Hx = H\}$

$= \{x \in K | x \in H\} = H \cap K$

This implies, $K/H \cap K \cong HK/H$.

Theorem 1.4.22 (Freshmen's theorem): Let H and K be two normal subgroups of a group G such that $H \subset K$. Then K/H is a normal subgroup of G/H and

$$G/K \cong \frac{\frac{G}{H}}{\frac{K}{H}}$$

Proof:

Let $Hk \in K/H$ and $Hg \in G/H$

Consider $(Hg)^{-1}(Hk)(Hg) = Hg^{-1}kg$

Since K is a normal subgroup of G therefore, $g^{-1}kg \in K\ \forall\ g \in G, k \in K$

Therefore $Hg^{-1}kg \in K/H$

That proves that $\boldsymbol{K/H}$ **is a normal subgroup of** $\boldsymbol{G/H}$.

Define $f: G \to G/H$ defined by $f(x) = Hx$ then f is onto homomorphism.

Consider $f^{-1}(K/H) = \{x \in G | Hx \in K/H\} = K$.

By the first theorem of isomorphism, we get the desired result.

Task: Show that identity map defined on any group G is automorphism on G

Show that zero map defined on a group G is always a homomorphism but not isomorphism.

1.5 Permutation Groups and groups of integers modulo n

The Permutation / Symmetric Group

Theorem 1.5.1: Let S be a non-empty set. Then the collection G of all invertible functions from S to itself is a group under the composition of composite maps.

Proof:

Closure: For $f, g \in G$

f and g are invertible functions from set S to itself.

Then by definition of the composite map, $\boldsymbol{f \circ g}$ **is a function from** $\boldsymbol{S}$ **to itself**.

Consider $f \circ g(x) = f \circ g(y)$ for some $x, y \in S$

This implies $f\big(g(x)\big) = f\big(g(y)\big)$

Since f is one-one $g(x) = g(y)$

Also, g is one-one $x = y$

This implies, $\boldsymbol{f \circ g}$ **is one-one**

Let $x \in S$, since $f: S \to S$ is onto

Therefore, there exists $y \in S$ such that $f(y) = x$

Also, $g: S \to S$ is onto

Therefore, there exists $z \in S$ such that $g(z) = y$

That is $f\big(g(z)\big) = f(y) = x$

Hence, $\boldsymbol{f \circ g}$ **is onto.**

This implies $\boldsymbol{f \circ g \in G}$.

Associativity holds trivially as the composite map composition is associative.

Identity of the set G is given by the identity map on set S.

Inverse For each function f on S, since f is invertible. Therefore, for every $x \in S$, there exists an element $y \in S$ such that $f(y) = x$. Define a map $g: S \to S$ as $g(x) = y$ if and only if $f(y) = x$.

Then $g = f^{-1}$ is one-one and onto function from S to itself.

That proves that G is a group.

Now, we proceed to the concept of symmetric groups as under.

Let S be a finite set having n elements. Then the corresponding group G as defined above is called the symmetric group on n symbols and it is denoted as S_n. Any function in S_n is called a permutation.

Number of Permutations on $\boldsymbol{n}$ **symbols**

Let $S = \{1, 2, \ldots, n\}$ and f be any permutation on S. Then $f(1)$ has n choices. Once $f(1)$ is fixed $f(2)$ now has $n - 1$ choices and so on we get that total choices of function f are $n(n-1)(n-2) \ldots 1 = n!$

Therefore, the number of permutations on a set of n symbols is $n!$. So, $O(S_n) = n!$.

Representation of a permutation

Let $f \in S_n$. f can be represented in two different ways.

Method I: Two-row representation

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

Advanced Abstract Algebra - I

For example, Let $n = 4$

Let f be a permutation on S_4, given by $f(1) = 3, f(2) = 1, f(3) = 4, f(4) = 2$

Then f is represented as a two-row form

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

Method II: One-row representation

In one row representation, a permutation is written as $(1 \quad f(1) \dots \dots)$

For example, let f be a permutation on S_4, given by $f(1) = 3, f(2) = 1, f(3) = 4, f(4) = 2$

Then f is represented as a one-row form $(1 \quad 3 \quad 4 \quad 2)$

In one row representation, fixed elements are not explicitly included

For example, let f be a permutation on S_4, given by $f(1) = 3, f(2) = 2, f(3) = 4, f(4) = 1$

Then f is represented as a one-row form $(1 \quad 3 \quad 4)$.

Definition 1.5.2: In one-row representation, $f = (i_1 \quad i_2 \quad i_3 \dots \dots \quad i_k)$ where $f(i_1) = i_2, f(i_2) = i_3, \dots, f(i_{k-1}) = i_k, f(i_k) = i_1$ is called a cycle and the number of distinct terms in a cycle is called the length of the cycle.

Definition 1.5.3: A cycle of length 2 is called a transposition.

Every permutation can be expressed as a product of either even or odd number of transpositions. The permutation which can be expressed as even (odd) number of transpositions is called even (odd) permutation.

Example 1.5.4: The permutation I is an even permutation.

Proof:

For $I \in S_n$,

For any two symbols n, m such that $n \neq m$

Let f be any permutation $f = (n \quad m), f(p) = p$ for every $p \neq n, m$

Then $fof(n) = f\big(f(n)\big) = f(m) = n$

$fof(m) = f\big(f(m)\big) = f(n) = m.$

For $p \neq n, m$; $fof(p) = f\big(f(p)\big) = f(p) = p.$

That is, $fof = I$.

$I = fof = (n \quad m)(n \quad m)$ i.e., the product of an even number of transpositions.

Therefore, I is an even permutation.

Definition 1.5.5: Half of the permutations in S_n are even and the other half are odd permutations. If we collect all the odd permutations then since I is an even permutation, therefore, I does not belong to the set of odd permutations therefore, it is not a group.

Definition 1.5.6: Set of all even permutations forms a group under the composition of composite maps. This group is called the Alternating group. We denote this group on n symbol by A_n and $O(A_n) = \frac{n!}{2}$.

Group of integers under addition modulo n

Consider the set of integers Z and $n \in N$. Let us define the relation of congruence on Z by a is congruent to b modulo n if and only if n divides $a - b$ and we denote it as $a \equiv b$. For example, 4 □ 1 (mod 3), since 3 divides $4 - 1$. It can be seen easily that

$\equiv$ is an equivalence relation, and hence partitions Z into disjoint equivalence classes called congruence classes modulo n. We denote the class containing r by $\bar{r}$.

Thus $\bar{r} = \{m \in Z | \, m \equiv r(mod\ n)\}$

So, an integer m belongs to $\bar{r}$ for some r, $0 \leq r < n$, iff n divides $r - m$, i.e., if and only if $r - m = nk$ for some $k \in Z$.

$$\bar{r} = \{r + kn | k \in Z\}$$

Now, if $m \geq n$, then the division algorithm says that $m = nq + r$ for some $q, r \in Z, 0 \leq r < n$. That is, $m \equiv r\ (mod\ n)$, for some $r = 0, 1, \ldots, n-1$. Therefore, all the congruence classes modulo n are $\bar{0}, \bar{1}, \ldots \ldots \overline{n-1}$. Let $Z_n = \{\bar{0}, \bar{1}, \ldots \ldots \overline{n-1}\}$. We define the composition on Z_n as $\bar{a} + \bar{b} = \overline{a+b}\ \forall\ \bar{a}, \bar{b} \in Z_n$.

Theorem 1.5.7: Z_n is a group under the composition defined as $\bar{a} + \bar{b} = \overline{a+b}\ \forall\ \bar{a}, \bar{b} \in Z_n$.

Proof:

Closure: For $\bar{a}, \bar{b} \in Z_n$

Then $\bar{a} + \bar{b} = \overline{a+b}$

Case I: If $a + b < n$

Then clearly $\overline{a+b} \in Z_n$

Case II: If $a + b \geq n$

Divide $a + b$ by n, there exist unique integers q, r such that

$a + b = nq + r$ where $0 \leq r \leq n$

This implies

$$a + b - r = nq$$

That is n divides $a + b - r$

$$a + b \equiv r(mod\ n)$$

$$\overline{a+b} = \bar{r} \in Z_n$$

Therefore, Z_n **is closed** under this composition.

Associative:

For $\bar{a}, \bar{b}, \bar{c} \in Z_n$

$$\bar{a} + \left(\bar{b} + \bar{c}\right) = \bar{a} + \overline{b+c} = \overline{a + (b+c)} = \overline{(a+b)+c}\ \ (Integers\ are\ associative\ under\ addition)$$

$$= \overline{a+b} + \bar{c} = \left(\bar{a} + \bar{b}\right) + \bar{c}$$

Therefore, Z_n **is associative**.

Existence of Identity: For $\bar{a} \in Z_n$, $\bar{O} \in Z_n$ such that

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \overline{0+a} = \bar{0} + \bar{a}$$

That is, Z_n has an identity element.

Existence of Inverse: For $\bar{a} \in Z_n$,

We know that $0 \leq a < n$ so that $0 \leq n - a < n$; $\overline{n-a} \in Z_n$

Also, $\bar{a} + \overline{n-a} = \overline{a+n-a} = \bar{n} = \bar{0}$ and $\overline{n-a} + \bar{a} = \overline{n-a+a} = \bar{n} = \bar{0}$.

Inverse exists for each element of Z_n.

Therefore, Z_n is a group under the composition addition modulo n.

Remark 5: Z_n is not a group under multiplication modulo n.

Consider, $n = 6$; $\bar{2}$, $\bar{3} \in S_6$ both are non-zero but $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ so S_6 is not a group under multiplication modulo n.

Task: Prove that $Z_5 - \{0\}$ is a group under multiplication modulo 5.

Summary

- A binary operation is defined and its types are explained
- Groups and subgroups are defined and elaborated with the help of examples
- Coset and its properties are discussed
- Lagrange's Theorem is stated and proved
- The order of an element is defined and related theorems are proved
- Cyclic groups are defined and for a given group G, construction of a quotient group is done
- A homomorphism from a group G to some group G′ is explained
- Isomorphic groups and their properties are discussed

Keywords

- Binary operations on a set
- Semi-group
- Group
- Cyclic group
- Homomorphisms
- Order of element of a group

Self-assessment

Choose the most suitable answer from the options given with each question.

Question 1: Which of the following algebraic structures is NOT a semi-group?

A: (Q, +)

B: (Q, ·)

C: (Z, +)

D: (Z, −)

Question 2: Which of the following is not a binary operation on Z?

A: Addition

B: Multiplication

C: Division

D: Subtraction

Question 3: A monoid is called a group if

A: it satisfies the associative property

B: it has an identity element

C: inverse of each element exists

D: all above should exist

Question 4: Let G be a group of order n and $a \in G$. Then

A: $O(a) = n$

B: $O(a) < n$

C: $O(a)$ is a multiple of n

D: $O(a)$ is a divisor of n

Question 5: Let G be a cyclic group of order n and $G = < a >$. Then

A: $O(a) = n$

B: $O(a) < n$

C: $O(a) > n$

D: $O(a)$ is a proper divisor of n

Question 6: True/False Number of generators of a cyclic group is unique

A: True

B: False

Question 7: Let G be a group. Let $a \in G$ such that $O(a) = 5$. Then $O(a^3)$ is …….

A: 2

B: 3

C: 4

D: 5

Question 8: Let G be a group and $a \in G$ such that $O(a) = 32$. Then a^{100} is …….

A: a^4

B: a^3

C: a^2

D: a

Question 9: Let G be a group of order 30. Then G can not have an element of order

A: 2

B: 3

C: 7

D: 6

Question 10: Let $Z(G)$ denote the center of group G. Then $Z(G)$ is

A: a subgroup of G but not a normal subgroup of G.

B: a normal subgroup of G.

C: a cyclic subgroup of G.

D: is non-abelian.

Question 11: Consider the group G of all integers then which of the following is an automorphism on G.

A: $f(x) = x + 1$

B: $f(x) = x^2$

C: $f(x) = 3$

D: $f(x) = 2x$

Answers:

1	D	2	C	3	D
4	D	5	A	6	B
7	D	8	A	9	C
10	B	11	D		

Review Questions

1) Consider the set S = $\{1, \omega, \omega^2\}$ consisting of cube roots of unity. Prove that it is a finite group under the composition of multiplication of complex numbers.
2) Let Q^+ denotes the set of positive rational numbers. Define $*$ on Q^+ as $a * b = \frac{ab}{3}$ for all $a, b \in Q^+$. Verify that $(Q^+, *)$ is an abelian group.
3) Give an example of a non-abelian group.
4) Determine which of the following systems are groups. Give reasons why the remaining are not groups

(i) The set G of all non-singular matrices of order n over complex numbers under matrix multiplication
(ii) Set of Natural numbers under addition
(iii) Set of real numbers under multiplication
(iv) S= $\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} | a \in R\}$ under the multiplication of matrices

Also, check which of the above are abelian groups?

5) Prove that the identity element of a group is always unique.
6) Calculate (1 3)(1 2) in S_3.
7) Obtain the left and right cosets of $H = <(1\ 2)>$ in S_3. Show that $Hx \neq xH$ for some $x \in S_3$.
8) Find the order of the following elements
   a) $(1\ 2) \in S_3$
   b) $I \in S_4$
   c) $\overline{3} \in Z_4$
   d) $1 \in R, R$ denotes the set of real numbers
9) Prove that if H and K are normal subgroups of G, then prove that HK is a normal subgroup of G.
10) Let $f: Z \to Z$ be defined as $f(x) = 2x$. Then check whether f is homomorphism or not. If yes, find Ker f and Im f.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal, Cambridge university press

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 02: Solvable Groups

CONTENTS

Expected Learning Outcomes

After studying this unit, you will be able to

- define and form a subnormal series and check if a subnormal series is solvable or not
- check whether a group is solvable or not
- define proper normal subgroups and understand composition series
- understand isomorphic composition series
- state and prove Jordan Holder Theorem
- define nilpotent group and normal series for a group
- understand nilpotent groups through examples
- relate nilpotent groups with solvable groups

Introduction

The word solvable comes from the solvability of polynomials. In terms of solvable groups, more specifically in the field of group theory, a solvable group or soluble group is a group that can be constructed from abelian groups using extensions. Equivalently, a solvable group is a group whose derived series terminates in the trivial subgroup.

2.1 Subnormal Series and Factor Groups

Definition 2.1.1: (Subnormal Series) Let G be a group. Then a decreasing series $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ is called a subnormal series if G_{i+1} is a normal subgroup of G_i for every i. Since, G_{i+1} is a normal subgroup of G_i for every i therefore, G_i/G_{i+1} is a group and it is called a factor group. We write the subnormal series as $\{G = G_0, G_1, G_2, \ldots, G_n\}$ in set form.

Example 2.1.2: Let $G = \{1, -1, i, -i, j, -j, k, -k\}$ then G is a group under the composition of the cross product of vectors. Then G has a subnormal series.

Solution:
Consider $G = \{1, -1, i, -i, j, -j, k, -k\}, G_1 = \{1, -1, i, -i\}, G_2 = \{1, -1\}, G_3 = \{1\}$
Then $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 = \{1\}$ is a decreasing series of subgroups of G. Also,

$$[G: G_1] = \frac{O(G)}{O(G_1)} = \frac{8}{4} = 2$$
$$[G_1: G_2] = \frac{O(G_1)}{O(G_2)} = \frac{4}{2} = 2$$
$$[G_2: G_3] = \frac{O(G_2)}{O(G_3)} = \frac{2}{1} = 2$$

This implies, G_1 is a normal subgroup of G, G_2 is a normal subgroup of G_1, G_3 is a normal subgroup of G_2 (Refer to Theorem 1.5.5 for explanation) Therefore, the series is subnormal.

The next example shows that the subnormal series is not unique.

Example 2.1.3: Let $G = \{1, -1, i, -i, j, -j, k, -k\}$ then G is a group under the composition of the cross product of vectors. Then G has two distinct subnormal series.

Solution:
One subnormal series of group G is given in Example 2.1.2.
Let us consider the series

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq H_3 = \{1\}$$

where $H_1 = \{1, -1, j, -j\}$ and $H_2 = \{1, -1\}$
Then with the same reasoning as given in Example 2.1.2, this is a subnormal series.
Therefore, subnormal series may not be unique.

Definition 2.1.4: Let G be a group and $M = \{G = G_0, G_1, G_2, \dots, G_n\}$ and $N = \{G = H_0, H_1, H_2, \dots, H_m\}$ be two subnormal series of G. Then N is called ***refinement*** of M if $M \subseteq N$. For example, in Example 2.1.2, we can consider, $M = \{G_0, G_2, G_3\}$ and $N = \{G_0, G_1, G_2, G_3\}$ then clearly, N is a refinement of M.

Length of Subnormal Series: If in a subnormal series, $G_i = G_{i+1}$ for some i then the subnormal series is called redundant otherwise it is called irredundant. Removing all the G_{i+1}, for which $G_i = G_{i+1}$, the number of subgroups left in the series is called the length of subnormal series. For example, the subnormal series given in Example 2.1.2 is 4.

Task:
Let a group G has a subnormal series. Then observe that every subgroup of G has at least one subnormal series.

2.2 Solvable Groups

Definition 2.2.1: Let G be a group and $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$ be a subnormal series of G such that G_i/G_{i+1} is abelian for all i, then this series is called solvable series and G is called solvable group.

Example 2.2.2: Any abelian group is solvable.

Solution:
Let G be an abelian group. Then the series $G \supseteq \{e\}$ is the series and $G/\{e\} \cong G$, as G is abelian therefore, $G/\{e\}$ is abelian. Hence G is solvable.

Example 2.2.3: The permutation group on 3 symbols S_3 is solvable.

Solution:
The group $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
Consider $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$
$H = \{I\}$.
Clearly, $S_3 \supseteq A_3 \supseteq H = \{I\}$
Also, $[S_3: A_3] = O(S_3)/O(A_3) = 6/3 = 2$.
Therefore, S_3/A_3 is abelian
Similarly, A_3/H is abelian

Therefore, S_3 is solvable.

Theorem 2.2.4: Subgroup of a solvable group is solvable.
Proof:
Let G be a solvable group and

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\} \ldots\ldots\ldots\ldots (1)$$

be a solvable series for G.

Consider any subgroup H of G and

$$H = G \cap H = G_0 \cap H \supseteq G_1 \cap H \supseteq G_2 \cap H \supseteq \cdots \supseteq G_n \cap H = \{e\} \ldots\ldots\ldots\ldots (2)$$

We claim that (2) is solvable series for H.

Series (1) represents solvable series for G. G_{i+1} is a normal subgroup of G_i for all i. This implies $G_{i+1} \cap H$ is a normal subgroup of $G_i \cap H$.

Let $G_i \cap H = H_i$

Again, G_i/G_{i+1} is abelian for all i.

Define $f: H_i \to G_i/G_{i+1}$ as

$f(x) = G_{i+1}x$ for all $x \in H_i$

***f* is homomorphism:**

For $x, y \in H_i$

$$f(xy) = G_{i+1}xy = G_{i+1}x\, G_{i+1}y = f(x)f(y)$$

Therefore, f is a homomorphism.

Kernel *f*

Let $x \in Ker\ f \subset H_i$
$x \in H_i$ and $f(x) = G_{i+1}$
$G_{i+1}x = G_{i+1} \Rightarrow x \in G_{i+1} \Rightarrow x \in G_{i+1} \cap H = H_{i+1}$.
$Ker\ f \subseteq H_{i+1}$.

Let $x \in H_{i+1} = G_{i+1} \cap H$
$x \in G_{i+1} \Rightarrow G_{i+1}x = G_{i+1} \Rightarrow f(x) = G_{i+1} \Rightarrow x \in Ker\ f$.
Therefore, $H_{i+1} \subseteq Ker\ f$
Hence $Ker\ f = H_{i+1}$

By the fundamental theorem of homomorphism

$$\frac{H_i}{H_{i+1}} \cong f(H_i)$$

and $f(H_i)$ is a subgroup of G_i/G_{i+1}.
Since $\frac{G_i}{G_{i+1}}$ is abelian for all i and subgroup of an abelian group is abelian. That is, $f(H_i)$ is abelian and being isomorphic to $f(H_i)$, the factor group H_i/H_{i+1} is abelian for all i.
Hence every factor group in series (2) is abelian and series (2) is solvable series for H.
Therefore, every subgroup of a solvable group is solvable.

Theorem 2.2.5: Let H be a normal subgroup of G. If G is solvable then G/H is solvable.
Proof:
Let G be a solvable group and

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\} \ldots\ldots\ldots\ldots (1)$$

be a solvable series for G.
Consider the series

$$\frac{G}{H} = \frac{G_0}{H} \supseteq \frac{G_1H}{H} \supseteq \frac{G_2H}{H} \supseteq \cdots \supseteq \frac{G_nH}{H} = H \ldots\ldots\ldots\ldots (2)$$

We claim that the series (2) is solvable series for G/H.
Since G_{i+1} is a normal subgroup of G_i for all i.
Let $x \in G_iH \Rightarrow x = gh; g \in G_i, h \in H$
Then $xG_{i+1}H = ghG_{i+1}H = ghHG_{i+1} = gHG_{i+1} = gG_{i+1}H = G_{i+1}gH = G_{i+1}ghH = G_{i+1}Hgh = G_{i+1}Hx$.

$xG_{i+1}H = G_{i+1}Hx$ for all $x \in G_iH$.
This implies that $G_{i+1}H$ is a normal subgroup of G_iH.
Using Theorem 1.8.22, we get that

$$\frac{G_iH}{G_{i+1}H} \cong \frac{\frac{G_iH}{H}}{\frac{G_{i+1}H}{H}}$$

Now define a function $f: G_i \to \frac{G_iH}{G_{i+1}H}$ as $f(x) = G_{i+1}Hx$ for all $x \in G_i$.

Then f is a homomorphism.
For all $y \in G_iH, y = gh; g \in G_i, h \in H$

$$G_{i+1}Hy = G_{i+1}Hhg = G_{i+1}Hg = f(g)$$

Therefore, f is onto.
Let $x \in G_{i+1} \Rightarrow f(x) = G_{i+1}Hx = G_{i+1}xH = G_{i+1}H$ (Since H is a normal subgroup of G, $Hx = xH \; \forall \; x \in G$
So, $f(x)$ is the identity element of the codomain set.
This proves that $G_{i+1} \subseteq Ker\, f$
Define a function

$$\bar{f}: \frac{G_i}{G_{i+1}} \to \frac{G_iH}{G_{i+1}H}$$

as

$$\bar{f}(G_{i+1}x) = G_{i+1}Hx$$

$\bar{f}$ is homomorphism and onto. Thus $\frac{G_iH}{G_{i+1}H}$ is a homomorphic image of abelian group $\frac{G_i}{G_{i+1}}$. This proves that G/H is solvable. Hence quotient group of a solvable group is solvable.

Theorem 2.2.6: Let H be a normal subgroup of G. If both H and G/H are solvable then G is solvable.
Proof:
Given that G/H is a solvable group.
Let $\frac{G}{H} = \frac{G_0}{H} \supseteq \frac{G_1}{H} \supseteq \frac{G_2}{H} \supseteq \cdots \supseteq \frac{G_t}{H} = \{H\}$ is the solvable series for $\frac{G}{H}$.
This implies that $\frac{G_{i+1}}{H}$ is a normal subgroup of $\frac{G_i}{H}$ and $\frac{G_i/H}{G_{i+1}/H}$ is abelian for all i.
Again, $\frac{G_{i+1}}{H}$ is a normal subgroup of $\frac{G_i}{H}$ implies G_{i+1} is a normal subgroup of G_i containing H.
Also,

$$\frac{G_i}{G_{i+1}} \cong \frac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}}$$

Therefore, $\frac{G_i}{G_{i+1}}$ is abelian for every i.
That is $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = H$ is such that $\frac{G_i}{G_{i+1}}$ is abelian for all i.
Given that H is solvable.
Let $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{e\}$ is a solvable series for H.
Consider

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{e\}$$

Then it is clearly a solvable series for G. Therefore, G is solvable.

Definition 2.2.7: Let $G_1, G_2, \ldots, G_n$ be n groups with their respective compositions $*_1, *_2, \ldots, *_n$. Then $G = G_1 \times G_2 \times \ldots \times G_n$ is called the direct product of $G_1, G_2, \ldots, G_n$. Any $x \in G; x = (x_1, x_2, \ldots x_n); x_i \in G_i$.
Then G is a group under the composition

$$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (x_1 *_1 y_1, x_2 *_2 y_2, \ldots, x_n *_n y_n)$$

For example, let $G_1 = (Z, +), G_2 = (G, \times)$ where $G = \{2^n | n \in Z\}$
Then $G = G_1 \times G_2 = \{(x, y) | x \in Z, y \in G\}$

$$(x_1, x_2) * (y_1, y_2) = (x_1 + y_1, x_2 y_2)$$

Identity of G is $(0, 1)$.

Theorem 2.2.8: Let H and K be two subgroups of a group G and $G = H \times K$. Then G is solvable if and only if H and K are solvable.
Proof:
Let G is solvable group. $H \times \{e\}$ is a subgroup of G.

$$H \times \{e\} = \{(h, e) | h \in H\}$$

Since G is solvable and a subgroup of a solvable group is solvable. Therefore, $H \times \{e\}$ is solvable.

Define a function $f: H \to H \times \{e\}$ as

$$f(h) = (h, e)$$

Then for $h_1, h_2 \in H$,

$$f(h_1 h_2) = (h_1 h_2, e) = (h_1, e)(h_2, e) = f(h_1) f(h_2)$$

So, ***f* is a homomorphism.**

For $h_1, h_2 \in H$,

$$f(h_1) = f(h_2)$$
$$\Rightarrow (h_1, e) = (h_2, e)$$
$$\Rightarrow h_1 = h_2$$

Hence ***f* is one-one.**
For all $(h, e) \in H \times \{e\}, h \in H$ such that $f(h) = (h, e)$
Thus, ***f* is onto.**
Therefore, $H \cong H \times \{e\}$.
So, being isomorphic to solvable group $H \times \{e\}$, H is solvable.
Similarly, K is solvable.
Conversely,
Let H and K are solvable groups.
Then as proved $H \times \{e\} \cong H$ so. $H \times \{e\}$ is solvable.
$H \times \{e\}$ is a normal subgroup of G.
Also, $G/H \times \{e\} \cong K$, which is solvable
Using Theorem 2.2.6, G is solvable.

Definition 2.2.9: Let p be a prime number. Then a group G is called p-group if and only if $O(a) = p^k; k \in Z \; \forall \; a \in G$. In this case, $O(G) = p^n$ for some integer n. For example, $G = \{1, -1, i, -i\}$ is a group under the multiplication of complex numbers. Order of 1 is 1 that is $2^0, the$ order of -1 is 2 that is $2^1, the$ order of i and $-i$ is 4 that is 2^2. The order of group G is 4 that is 2^2. Hence G is a 2-group.

Theorem 2.2.10: Every p-group is solvable.
Proof:
Let G be a p −group of order p^n for some integer n.
For $n = 1, G$ is a group of prime order p.
Since every group of prime order is cyclic and hence abelian.
By Theorem 2.2.2, G is solvable.
Let the result is true for all groups G' such that $O(G') = p^m < O(G); O(G) = p^n$
Consider $Z(G)$, the center of group G
Since $O(G) = p^n$, therefore, $Z(G) \neq \{e\}$
So, $Z(G)$ is a subgroup of G, $O\big(Z(G)\big) < O(G)$
By Lagrange's theorem, $O\big(Z(G)\big)$ divides $O(G)$.
So, $O\big(Z(G)\big) = p^m, 1 < m \leq n$

$$O\left(\frac{G}{Z(G)}\right) = \frac{p^n}{p^m} = p^{n-m}; n - m < n$$

By the induction hypothesis, $\frac{G}{Z(G)}$ is solvable. Also, $Z(G)$ is solvable.
Using Theorem 2.2.6, G is a solvable group. Hence every p −group is solvable.

Definition 2.2.11: For elements a, b in a group G. The element $a^{-1}b^{-1}ab \in G$ is called ***commutator of* a, b**. We denote it as $[a, b]$. The subgroup of G generated by all commutator elements is called ***commutator/derived subgroup*** of G and it is denoted as G'. It can be easily seen that G' is a normal subgroup of G.

Note: If G is abelian then $ab = ba$ for all $a, b \in G$
Hence $a^{-1}b^{-1}ab = e \; \forall \; a, b \in G$
That is $G' = \{e\}$

Definition 2.2.12: Denote G as $G^{(0)}$, G' as $G^{(1)}$, $(G')'$as $G^{(2)}$ so on then $G^{(n)}$ is called nth commutator subgroup of G.

Theorem 2.2.13: For any normal subgroup H of G, G/H is an abelian group if and only if $G' \subseteq H$.
Proof:

Let G/H is abelian group.
This implies $HaHb = HbHa \; \forall \; a, b \in G$
$\Rightarrow Hab = Hba \; \Rightarrow a^{-1}b^{-1}ab \in H$ (Using Theorem 1.4.3)
Hence $G' \subseteq H$.
Conversely, Let $G' \subseteq H$
$\Rightarrow a^{-1}b^{-1}ab \in H \; \forall \; a, b \in G,$
$\Rightarrow Hab = Hba \; \forall \; a, b \in G,$
$\Rightarrow G/H$ is abelian.

Note: In particular, since $G' \subseteq G'$ and hence G/G' is always abelian.

Theorem 2.2.14: A group G is solvable if and only if $G^{(n)} = \{e\}$ for some non-negative integer n.
Proof:
Let G be a solvable group.
Let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ be solvable series for G.
Claim: $G^{(k)} \subseteq G_k$ for all $k \in N$
We will prove this result by using the principle of mathematical induction
For $k = 0, G^{(k)} = G^{(0)} = G = G_0 = G_k$
So, the result is true for $k = 0$.
Let the result is true for k i.e., $G^{(k)} \subseteq \; G_k$
Now, $G_k/G_{(k+1)}$ is abelian this implies, $G_k' \subseteq G_{k+1}$
Also, $G^{(k+1)} = (G^{(k)})' \subseteq G_k{}' \subseteq G_{k+1}$
Thus, $G^{(k+1)} \subseteq G_{k+1}$
Therefore, by the induction hypothesis, $G^{(k)} \subseteq G_k$ for all $k = 0, 1, 2, \ldots$
$G^{(n)} \subseteq G_n = \{e\}$
Thus $G^{(n)} = \{e\}$.
Conversely,
let $G^{(n)} = \{e\}$
then $G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$ is subnormal series for G such that $G^{(i)}/G^{(i+1)}$ is abelian.
Therefore, G is a solvable group.

Theorem 2.2.15: S_n is solvable for $n \leq 4$ and S_n is not solvable for $n > 4$.
Proof:
$S_2 = \{I, (1\ 2)\}$ being abelian is a solvable group.
Form Theorem 2.2.3, S_3 is a solvable group.
Consider the series $S_4 \supseteq A_4 \supseteq V_4 \supseteq A \supseteq \{I\}$,
where $V_4 = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, A = \{I, (\ 1\ 2)(3\ 4)\}$
$[S_4 : A_4] = 2, [A_4 : V_4] = 3, [V_4 : A] = 2, [A : \{I\}] = 2.$
This implies that all the factor groups are abelian.
Hence S_4 is a solvable group.
For $n > 4$,
A_n is a simple non-commutative group, so $A_n' \neq \{I\}$.
However, A_n is simple, so its only normal subgroups are A_n and $\{I\}$.
Consequently, $A_n' = A_n \Rightarrow A_n^{(2)} = (A_n')' = A_n$.
In general, $A_n^{(k)} = A_n$ for all positive integers k, thus $A_n^{(k)} \neq \{e\}$ for all k.
Hence, A_n is not solvable.
Since subgroup of a solvable group is solvable and a subgroup A_n is not solvable, therefore, S_n is not solvable.

Task:
1) Prove that every group G of order pqr, p, q, r are distinct primes is always solvable. Discuss the case if p, q, r are not distinct.
2) Let G be a group with $O(G) = p^2q; p, q$ are distinct primes. Then prove that G has at least one solvable series.

2.3 Composition Series

In a group G, the relation of normal subgroups that is, two subgroups H and K are related if and only if H is a normal subgroup of K, is not a transitive relation.

Definition 2.3.1: Let G be a group. Then a normal subgroup H of G is called ***maximal normal subgroup*** if there does not exist any K of G such that $H \subset K \subset G; H \neq K, K \neq G$.
For example, let $G = \{1, -1, i, -i\}, H = \{1, -1\}$

$$O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)} = 2$$

Let K be a normal subgroup of G such that $H \subset K \subset G; H \neq K, K \neq G$

$$\Rightarrow \frac{O(G)}{O(H)} > \frac{O(G)}{O(K)}$$

That is, $\frac{O(G)}{O(K)} = 1$, which is possible only if $G = K$ but $G \neq K$.
So, our supposition was wrong.
That is such a normal subgroup K does not exist.
Hence, H is the maximal normal subgroup of G.

Theorem 2.3.2: H is a maximal normal subgroup of G if and only if G/H is simple.
Proof:
Any subgroup K/H of G/H is such that K is a subgroup of G containing H. Similarly, any normal subgroup K/H of G/H is such that K is a normal subgroup of G containing H. H is a maximal normal subgroup of G implies there does not exist any normal subgroup K other than H such that $H \subset K$.
There does not exist any proper normal subgroup of G/H this implies G/H is simple.
Conversely, let G/H is simple.
Let there exists some normal subgroup K of G such that $H \subset K \subset G; K \neq H, K \neq G$.
This implies that K/H is a proper normal subgroup of G/H which is a contradiction to the fact that G/H is simple.
Therefore, H is the maximal normal subgroup of G.

Definition 2.3.3: A group is called a simple group if it has no proper normal subgroup or in other words, a simple group has only trivial normal subgroups that are {e} and itself.

Theorem 2.3.4: Every group of prime order is simple.
Proof:
Let G be a group of order p; where p is a prime number.
Let H be a normal subgroup of G. Then by Lagrange's theorem
Order of H divides the order of G.
That is $O(G) = tO(H)$ for some integer t.
Since $O(G)$ is a prime number, therefore, $t = 1$ or $t = p$
If $t = 1, O(G) = O(H), H = G$,
If $t = p, O(H) = 1, H = \{e\}$.
So, there are only two normal subgroups of G, $\{e\}$ and G.
Hence, G is simple.

Definition 2.3.5: Let G be a group and $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$ be a subnormal series of G such that G_i/G_{i+1} is simple for all i, then this series is called composition series. This implies G_{i+1} is a maximal normal subgroup of G_i.

Example 2.3.6: Let $G = < a >$ is a cyclic group of order 24.

Consider $G = < a > \supseteq < a^2 > \supseteq < a^6 > \supseteq < a^{12} > = \{e\}$

$[< a >: < a^2 >] = 2, [< a^2 >: < a^6 >] = 3, [< a^6 >: < a^{12} >] = 2, [< a^{12} >: \{e\}] = 2.$

All the indices are prime numbers hence all the factor groups are simple.

Therefore, the series is composition series.

Definition 2.3.7: Let G be a group then two composition series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$$

and

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{e\}$$

are called equivalent series if $n = m$ and

$$\frac{G_i}{G_{i+1}} \cong \frac{H_{\pi(i)}}{H_{\pi(i)+1}}$$

where π is a permutation on $\{1, 2, 3, \ldots, n\}$.

For example,

$$G = < a > \supseteq < a^2 > \supseteq < a^6 > \supseteq < a^{12} > = \{e\} \ldots (1)$$

and

$$G = < a > \supseteq < a^2 > \supseteq < a^6 > \supseteq < a^{12} > = \{e\} \ldots (2)$$

Factor groups of (1) are $< a > / < a^2 >, < a^2 > / < a^6 >, < a^6 > / < a^{12} >, < a^{12} > / \{e\}$.
Factor groups of (2) are $< a > / < a^3 >, < a^3 > / < a^6 >, < a^6 > / < a^{12} >, < a^{12} > / \{e\}$.
$< a > / < a^2 > \cong < a^3 > / < a^6 >$, $< a^2 > / < a^6 > \cong < a > / < a^3 >$, the rest two factor groups are the same.
Hence (1) and (2) are isomorphic subnormal series.

Theorem 2.3.8: Every finite group with at least two elements has at least one composition series.

Proof:

Let $O(G) = n$

Let $n = 2, G = \{e, a\}, a \neq e$

Then $G \supseteq \{e\}$ is the only possible composition series and hence the result is true for $n = 2$.

Let $n > 2$,

If G is simple then G has only one normal subgroup $\{e\}$ other than G. Then $G \supseteq \{e\}$ is the composition series and hence the result is true in this case.

If G is not simple then G will have at least one proper normal subgroup. Let M be the proper normal subgroup with maximum elements. M is maximal normal subgroup this implies G/M is simple; $M \subset G$. Now if M is simple then $G \supset M \supset \{e\}$ is the required series.

If not, then there exists some M_1 such that $M \supset M_1 \supset \{e\}$

Continuing so on, if M_1 is simple then $G \supset M \supset M_1 \supset \{e\}$ is the composition series.

If not, we get some M_2 and so on

We get $G \supset M \supset M_1 \supset M_2 \supset \cdots \supset \{e\}$ a composition series for G.

Hence G has a composition series.

Task:

1) Prove that a field has only one composition series.

2) Prove that a division ring has a unique composition series.

2.4 Jordan Holder Theorem

Theorem 2.4.1: Let H and K be two subgroups of a group G such that $kH = Hk$ for all $k \in K$. Then HK is a subgroup of G, H is a normal subgroup of $HK, H \cap K$ is a normal subgroup of K and

$$HK/H \cong K/H \cap K$$

Proof:

Define a function $f: K \to HK / H$ as $f(k) = Hk \; \forall \; k \in K$.

For $k_1, k_2 \in K, f(k_1k_2) = Hk_1k_2 = (Hk_1)(Hk_2) = f(k_1)f(k_2)$.

That is, ***f* is a homomorphism.**

$\forall\, Hx \in HK/H\,, x \in\ HK; x = hk$ for some $h \in H, k \in K$

Then $Hx = Hhk = Hk = f(k)$ which proves that ***f* is onto.**

$$Ker\ f = \{k \in K | f(k) = H\}$$
$$= \{k \in K | Hk = H\}$$
$$= \{k \in K | k \in H\}$$
$$= H \cap K$$

By Fundamental Theorem of Homomorphism,

$$K/H \cap K \cong HK/H$$

Equivalently,

$$HK/H \cong K/H \cap K$$

and $H \cap K$ being Kernel of a homomorphism is a normal subgroup of K.

Theorem 2.4.2: (Zassenhaus) Let B and C be two subgroups of a group G. B_0 and C_0 be normal subgroups of B and C respectively, then

$$\frac{B_0(B \cap C)}{B_0(B \cap C_0)} \cong \frac{C_0(C \cap B)}{C_0(C \cap B_0)}$$

Proof:

Let $K = B \cap C$, $H = B_0(B \cap C_0)$

Since B_0 is a normal subgroup of B.

$$bB_0 = B_0b\ \forall\ b \in B$$

In particular since $K \subseteq B$

$$kB_0 = B_0k\ \forall\ k \in K$$

Also, C_0 is a normal subgroup of C.

$B \cap C_0$ is a normal subgroup of $B \cap C = K$.

$$k(B \cap C_0) = (B \cap C_0)k\ \forall\ k \in K$$

Hence $Hk = \ B_0(B \cap C_0)k = B_0k(B \cap C_0) = \ kB_0(B \cap C_0) = kH\ \forall\ k \in K$

Therefore, using Theorem 2.4.1,

$$\frac{HK}{H} \cong \frac{K}{H \cap K} \ldots (1)$$

Now $HK = \ B_0(B \cap C_0)(B \cap C) = B_0(B \cap C)$ ($B \cap C_0$ is a normal subgroup of $B \cap C$)

Further $y \in H \cap K\ \Rightarrow y \in H\,, y \in K$

$\Rightarrow y = b_0b; b_0 \in B_0, b \in B \cap C_0$ and $y = d; d \in B \cap C$

$\Rightarrow\ b_0b = d\ \Rightarrow b_0 = db^{-1} \in B_0 \cap C = \ C \cap B_0$

Therefore, $y = b_0b \in (C \cap B_0)(B \cap C_0)$

This implies $H \cap K \subseteq (C \cap B_0)(B \cap C_0)\ \subseteq B \cap C = K$

Also, $C \cap B_0 \subseteq B_0$

$\Rightarrow\ (C \cap B_0)(B \cap C_0) \subseteq B_0(B \cap C_0) = H$

Therefore, $(C \cap B_0)(B \cap C_0) \subseteq H \cap K$

$H \cap K = (B \cap C_0)(C \cap B_0)$ and $HK = B_0(B \cap C)$

From (1),

$$\frac{B_0(B \cap C)}{B_0(B \cap C_0)} \cong \frac{B \cap C}{(C \cap B_0)(B \cap C_0)} \dots (2)$$

Interchanging the roles of B and C, we get

$$\frac{C_0(C \cap B)}{C_0(C \cap B_0)} \cong \frac{C \cap B}{(B \cap C_0)(C \cap B_0)} \dots (3)$$

Since $B \cap C_0$ is a normal subgroup of $B \cap C$ and $C \cap B_0 \subseteq B \cap C$

Therefore, $(B \cap C_0)(C \cap B_0) = (C \cap B_0)(B \cap C_0)$

Also, $B \cap C = C \cap B$

From (2) and (3), we get that

$$\frac{B_0(B \cap C)}{B_0(B \cap C_0)} \cong \frac{C_0(C \cap B)}{C_0(C \cap B_0)}$$

Theorem 2.4.3: (Schreier's Refinement theorem) Any two subnormal series of a group G have equivalent refinements.

Proof:

Let G be a group and two subnormal series are given by

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_s = \{e\} \dots (1)$$

and

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_t = \{e\} \dots (2)$$

That is G_{i+1} is a normal subgroup of G_i for all i. Similarly, H_{i+1} is a normal subgroup of H_i for all i.

we get,

$$G_{i,j} = G_{i+1}(G_i \cap H_j), i = 0,1,2, \dots, s-1; j = 0,1,2, \dots, t \dots (3)$$

$$H_{k,l} = H_{k+1}(H_k \cap G_l), k = 0,1, \dots, t-1; l = 0,1,2, \dots, s \dots (4)$$

are subgroups of G.

Now H_{j+1} is a normal subgroup of H_j implies that $G_{i,j+1}$ is a normal subgroup of $G_{i,j}$. Similarly, $H_{k,l+1}$ is a normal subgroup of $H_{k,l}$.

Since $H_t = \{e\}$ and $H_0 = G$, we have

$$G_{i,t} = G_{i+1}(G_i \cap H_t) = G_{i+1}\{e\} = G_{i+1} \dots (5)$$

Also,

$$G_{i,0} = G_{i+1}(G_i \cap H_0) = G_{i+1}(G_i \cap G) = G_{i+1}G_i = G_i \dots (6)$$

Thus, $G_{i,t} = G_{i+1} = G_{i+1,0} \; \forall \; i = 0,1,2, \dots, s-1$

Similarly, $H_{k,s} = H_{k+1} = H_{k+1,0} \; \forall \; k = 0,1,2, \dots, t-1$

Consider two series

$$G = G_0 = G_{0,0} \supseteq G_{0,1} \supseteq G_{0,2} \supseteq \cdots \supseteq G_{0,t}(= G_1 = G_{1,0}) \supseteq G_{1,1} \supseteq G_{1,2} \supseteq \cdots \supseteq G_{1,t}\,(= G_2 = G_{2,0})$$
$$\supseteq \cdots \supseteq G_{s-1,0} \supseteq G_{s-1,1} \supseteq \cdots \supseteq G_{s-1,t} = G_s = \{e\} \dots (7)$$

and

$$G = H_0 = H_{0,0} \supseteq H_{0,1} \supseteq H_{0,2} \supseteq \cdots \supseteq H_{0,s}(= H_1 = H_{1,0}) \supseteq H_{1,1} \supseteq H_{1,2} \supseteq \cdots \supseteq H_{1,t}\,(= H_2 = H_{2,0})$$
$$\supseteq \cdots \supseteq H_{t-1,0} \supseteq H_{t-1,1} \supseteq \cdots \supseteq H_{t-1,s} = H_t = \{e\} \dots (8)$$

Both (7) and (8) have the same number of terms i.e.; $ts + 1$.

Clearly, G_0 occurs in (7) and for each $m = 1, 2, \dots, s$, as $G_m = G_{m-1,t}$ by (5), we see that each G_m occurs in (7). Thus (7) is a refinement of (1). Similarly, (8) is a refinement of (2).

By Zassenhaus theorem,

$$\frac{G_{r,s}}{G_{r,s+1}} = \frac{G_{r+1}(G_r \cap H_s)}{G_{r+1}(G_r \cap H_{s+1})} \cong \frac{H_{s+1}(H_s \cap G_r)}{H_{s+1}(H_s \cap G_{r+1})} = \frac{H_{s,r}}{H_{s,r+1}}$$

for all $r = 0, 1, 2, \ldots, s-1$ and $s = 0, 1, 2, \ldots, t-1$.

Thus (7) and (8) are equivalent.

Theorem 2.4.4: Every simple abelian group is of prime order.

Proof:

Let G is simple abelian group. This implies that G has only two normal subgroups G and $\{e\}$.

Since G is abelian so every subgroup of G is a normal subgroup of G.

That is, G has only two subgroups G and $\{e\}$.

Let $a \in G, a \neq e$

Then $H = < a >$ is a subgroup of G.

This implies, $H = \{e\}$ *or* G

Since $a \neq e, H \neq \{e\}$

Thus $H = G$

That is, $G = H = < a >$

The group $G = < a >$ is cyclic.

Consider $K = < a^2 >$

Again $K = \{e\}$ *or* $K = G$

If $K = \{e\} \Rightarrow a^2 = e \Rightarrow O(a) = 2$ and $O(G) = 2$ that is, a prime number.

If $K = G \Rightarrow < a^2 > = < a > \Rightarrow a \in < a^2 > \Rightarrow a = a^{2i}$ for some $i \in Z$

$\Rightarrow a^{2i-1} = e \Rightarrow O(a) \leq 2i - 1$ that is $O(a)$ and hence $O(G)$ is finite.

If $O(G) = rs; r, s \in Z, r, s > 0$

then, G has at least one subgroup of order r.

Since G is simple, $r = 1$ or $r = O(G)$

That is, any divisor of $O(G)$ is either 1 or $O(G)$.

Hence $O(G)$ is a prime number.

Theorem 2.4.5: A commutative group with a composition series cannot be infinite.

Proof:

Let G be a commutative group.

Let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ be a composition series of G.

Then $G_{n-1} \,/\, G_n$ is simple.

Also, $G_{n-1}/G_n = G_{n-1} \,/\, \{e\} \cong G_{n-1}$ is simple.

Also, being a subgroup of commutative group G_{n-1} is abelian

Thus, G_{n-1} is a simple abelian group.

By Theorem 2.4.4, $O(G_{n-1})$ is a prime number.

Let $O(G_{n-1}) = p_{n-1}$

Further G_{n-2}/G_{n-1} is simple and abelian.

So, $O\left(\frac{G_{n-2}}{G_{n-1}}\right) = p_{n-2}$; a prime

so that

$$O(G_{n-2}) = \frac{0(G_{n-2})}{0(G_{n-1})} O(G_{n-1}) = O\left(\frac{G_{n-2}}{G_{n-1}}\right) O(G_{n-1}) = p_{n-2} p_{n-1}$$

Continuing so on,

We see that $O(G) = p_0p_1p_2 \dots p_{n-1}$ that is, a product of finite number of prime numbers hence G is a finite group.

A field with characteristic 0 is always infinite and commutative. Hence it does not have a composition series.

Theorem 2.4.6: A composition series of a group G cannot have a proper refinement.

Proof:

Let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\} \dots (1)$ is a composition series for G. Suppose $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{e\}$ be a refinement of (1).

If it is proper refinement then for some $1 \leq j \leq m, H_j \neq G_i$ for any i.

$\Rightarrow G_i \supset H_j \supset G_{i+1}$ for some i.

Choose j such that $H_{j-1} \not\subset G_i \Rightarrow G_{i+1} \subset H_j \subset G_i \subset H_{j-1}$

As H_j is a normal subgroup of H_{j-1}, this implies that H_j is a normal subgroup of G_i.

Therefore, $\frac{H_j}{G_{i+1}}$ is a proper normal subgroup of $\frac{G_i}{G_{i+1}}$ but $\frac{G_i}{G_{i+1}}$ is simple.

So, we arrive at a contradiction. This proves that a composition series has no proper refinement.

Theorem 2.4.7: (Jordan Holder Theorem): If a group G has a composition series, then all its composition series are equivalent.

Proof:

Let G has two composition series (A) and (B).

By Schreier's Refinement theorem, (A) and (B) have some proper refinements (C) and (D) such that (C) is isomorphic to (D).

Since a composition series has no proper refinement, therefore, (C)= (A) and (D)= (B), this proves that (A) and (B) are isomorphic series.

From Jordan Holder Theorem, it is clear that an infinite group having a composition series cannot be commutative.

Task:

1) Show that if N is a normal subgroup of G and G has a composition series then N has a composition series.

2) Show that a field with characteristic 0 has no composition series.

2.5 Nilpotent Groups

Example 2.5.1: Let G be a group and H and K be two subgroups of G such that H is a normal subgroup of G and K is a normal subgroup of H then K need not be a normal subgroup of G.

Let $G = A_4$ that is an alternating group on 4 symbols

$V_4 = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $H = \{I, (1\ 2)(3\ 4)\}$

$$[G: V_4] = \frac{O(G)}{O(V_4)} = \frac{4!}{2 \times 4} = 3$$

$$[V_4: H] = \frac{O(V_4)}{O(H)} = \frac{4}{2} = 2$$

This implies that V_4 is a normal subgroup of A_4 and H is a normal subgroup of V_4.

Consider $(1\ 2\ 3) \in A_4, (1\ 2)(3\ 4) \in H$

$$(1\ 2\ 3)(1\ 2)(3\ 4) = (1\ 3\ 4)$$

but

$$(1\ 2)(3\ 4)(1\ 2\ 3) = (2\ 4\ 3)$$

Thus

$$(1\ 2\ 3)(1\ 2)(3\ 4) \neq (1\ 2)(3\ 4)(1\ 2\ 3)$$

This implies that H is not a normal subgroup of V_4.

Definition 2.5.2: Let G be a group and $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ be a series such that each G_i is a normal subgroup of G for all i.

It is subnormal series for which G_i is not only a normal subgroup of G_{i-1} but also of G.

Definition 2.5.3: Let G be a group. Define

$$Z_0(G) = \{e\}$$

$$Z_1(G) = \{x \in G | x^{-1}\, y^{-1}xy \in Z_0(G)\ \forall\ y \in G\}$$

$$= \{x \in G | x^{-1}y^{-1}xy = e\ \forall\ y \in G\}$$

$$= \{x \in G | xy = yx\ \forall\ y \in G\}$$

Therefore, $Z_1(G) = Z(G)$

Similarly, $Z_{m+1}(G) = \{x \in G | x^{-1}y^{-1}xy \in Z_m(G)\ \forall\ y \in G\}$

This series is known as the upper central series.

Remark 1: Sequence $\{Z_n(G)\}$ is increasing.

Proof:

We use the principle of mathematical induction to prove this

For $n = 0, Z_0(G) = \{e\},\ Z_1(G) = Z(G)$

Clearly, $Z_0(G) \subset Z_1(G)$

Let the result is true for some $m, Z_m(G) \subset Z_{m+1}(G)$

If possible, let $Z_{m+1}(G) \not\subset Z_{m+2}(G)$

$\Rightarrow\ \exists\ x \in Z_{m+1}(G)$ such that $x \notin Z_{m+2}(G)$

Since $x \in Z_{m+1}(G) \Rightarrow x^{-1}y^{-1}xy \in Z_m(G)\ \forall\ y \in G$

and $x \notin Z_{m+2}(G) \Rightarrow x^{-1}y^{-1}xy \notin Z_{m+1}(G)$ for at least one $y \in G$

but by the induction hypothesis,

$$Z_m(G) \subset Z_{m+1}(G)$$

$$\Rightarrow x^{-1}y^{-1}xy \in Z_{m+1}(G)$$

So, we arrive at a contradiction

Hence $Z_{m+1}(G) \subset Z_{m+2}(G)$

Remark 2: $\left(Z_{m+1}(G)\right)' \subset Z_m(G)\ \forall\ m$

Proof:

$$Z_{m+1}(G) = \{x \in G | x^{-1}y^{-1}xy \in Z_m(G)\ \forall\ y \in G\}$$

For all $x \in Z_{m+1}(G)$

$$x^{-1}y^{-1}xy \in Z_m(G)\ \forall\ y \in G$$

So, every commutator is in $Z_m(G)$.

$$\Rightarrow \left(Z_{m+1}(G)\right)' \subset Z_m(G)$$

Definition 2.5.4: A group G is said to be nilpotent if there exists a normal series $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ such that $\frac{G_i}{G_{i+1}} \subseteq Z\left(\frac{G_i}{G_{i+1}}\right)$

Or, in the increasing series

$$Z_0(G) \subseteq Z_1(G) \subseteq \cdots$$

there exists $m \in N$ such that $Z_m(G) = G$.

Example 2.5.5: Every abelian group is nilpotent.

Proof:

For abelian group G, $G = Z(G) = Z_1(G)$

So, the upper central series is terminating at $m = 1$.

Hence G is nilpotent.

Example 2.5.6: Every cyclic group is nilpotent.

Proof:

Every cyclic group is abelian and from example 2.5.5, every abelian group is nilpotent. Hence every cyclic group is nilpotent.

Example 2.5.7: Every p-group is nilpotent.

Proof:

Let G be a p-group. This implies $O(G) = p^n; n \in N$

For $n = 1$,

$O(G) = p$; a prime number

Therefore, G is a group of prime order hence G is cyclic.

By Example 2.5.6, G is nilpotent.

Thus, the result is true for $n = 1$.

For $n > 1, Z(G) \neq \{e\}$

$\Rightarrow Z(G)$ is a proper subgroup of G.

By Lagrange's theorem, $O\big(Z(G)\big)$ divides $O(G) = p^n$

$$\Rightarrow O\big(Z(G)\big) = p^k; 1 \leq k \leq m$$

$$\Rightarrow O\left(\frac{G}{Z(G)}\right) = p^{n-k} = p^r; r < n$$

$\Rightarrow G/Z(G)$ has a non-trivial centre.

$$\Rightarrow Z\left(\frac{G}{Z(G)}\right) \neq \{Z(G)\}$$

$$\Rightarrow O\big(Z(G)\big) = O\big(Z_1(G)\big) < O\big(Z_2(G)\big)$$

$$Z_1(G) \subset Z_2(G) \subset \cdots \subset G$$

Continuing so on, we get some $k \in Z$

$$O\big(Z_k(G)\big) = p^n;\ k \leq n$$

$$O\big(Z_k(G)\big) = O(G)$$

This implies, G is nilpotent.

Theorem 2.5.7: Subgroup and homomorphic image of a group is nilpotent

Proof:

Let G is a nilpotent group. Therefore, there exists series

$$Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_m(G) = G$$

Let H be a subgroup of G.

Then since $H \cap Z(G) \subset Z(H)$.

For all $x \in Z_2(G), y \in G, xyx^{-1}y^{-1} \in Z_1(G)$

Hence, for all $x \in H \cap Z_2(G), y \in H, xyx^{-1}y^{-1} \in H \cap Z_1(G)$.

Therefore, $H \cap Z_2(G) \subset Z_2(H)$.

By repeating the argument, we see that $H \cap Z_i(G) \subset Z_i(H), 1 \leq i \leq m$

Hence $H = H \cap G = H \cap Z_m(G) \subset Z_m(H)$.

Hence H is nilpotent.

Let $\phi: G \to H$ be an onto homomorphism. Then

$\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)(\phi(x))^{-1}(\phi(y))^{-1}$ for all $x, y \in G$

Hence

$$\phi(x)\phi(y)(\phi(x))^{-1}(\phi(y))^{-1} \in \phi(Z(G)) \subset Z(H)$$

Because ϕ is onto, therefore, $\phi(x) \in Z_2(H)$. Therefore, $\phi\big(Z_2(G)\big) \subset Z_2(H)$.

Continuing the process, we get

$$\phi\big(Z_i(G)\big) \subset Z_i(H); i = 1, 2, 3, \ldots, m$$

Hence, $H = \phi(G) = \phi\big(Z_m(G)\big) \subset Z_m(H)$

Therefore, H is nilpotent.

Theorem 2.5.8: Every nilpotent group is solvable. The converse is not true.

Proof:

Let G be a nilpotent group. Then there exists a normal series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$$

such that

$$\frac{G_i}{G_{i+1}} \subset Z\left(\frac{G}{G_{i+1}}\right)$$

That is, G_i/G_{i+1} is a subgroup of $Z\left(\frac{G}{G_{i+1}}\right)$ i.e., an abelian group

Therefore, G_i/G_{i+1} is abelian and every normal series is a subnormal series.

This implies that G is solvable.

The converse part is not true

Consider symmetric group S_3 and alternating group A_3

Since A_3 is a normal subgroup of S_3 of index 2 and $\{I\}$ is a normal subgroup of A_3 with index 3

So, we have a solvable series

$$S_3 \supseteq A_3 \supseteq \{I\}$$

Then the series is having abelian factor groups. Hence S_3 is a solvable group.

However, S_3 is not nilpotent as $Z_m(S_3) = \{I\}$ for all m.

That is in the upper central series, there does not exist any $Z_m(S_3)$ such that $Z_m(S_3) \neq S_3$.

This is S_3 is not nilpotent group.

Task:

Prove that a subgroup and homomorphic image of a nilpotent group are nilpotent.

Determine a composition series of $A_n; n \neq 4$.

Summary

- Subnormal series is defined and condition for a subnormal series to be solvable or not is discussed
- Method to check whether a group is solvable or not is elaborated with the help of examples
- Results about the cartesian product of solvable groups and p-groups are proved
- Proper normal subgroups and composition series are defined and elaborated with the help of examples.
- The concept of isomorphic series is studied
- Jordan Holder Theorem is proved.
- Nilpotent group and normal series are defined
- The relation of nilpotent groups with solvable groups is explained.

Keywords

- Subnormal Series
- Composition Series
- Jordan Holder Theorem
- Nilpotent Groups
- Isomorphic composition series

Self-assessment

Choose the most suitable answer from the options given with each question.

Question 1: Which of the following statements is NOT true?

A: Every p −group is solvable

B**:** Every abelian group is solvable

C: Every solvable group is abelian

D: Every cyclic group is solvable

Question 2: Necessary and sufficient condition for a subnormal series to be a composition series is

A: Each of the subgroups in this series is simple

B**:** Each of its factor group is abelian

C: The number of factor groups in the series is a prime number

D: Each of its factor group is simple

Question 3: The number of composition series for the group of rational numbers is

A: 0

B**:** 1

C: Infinite

D: 2

Question 4: A subgroup of a solvable group is

A: always a normal subgroup

B: never a normal subgroup

C: always a solvable group

D: never a solvable group

Question 5: An abelian group is

A: Always solvable and has a composition series

B: Always solvable but never has a composition series

C: Never solvable

D: May or may not be solvable

Question 6: S_n is not solvable then n is

A: 2

B: 3

C: 4

D: 5

Question 7: A finite group has 2 composition series then both are

A: Same

B: Isomorphic

C: Redundant

D: Non-isomorphic

Question 8: Let G be a group. Then for two subgroup H and K of G

A: H is a normal subgroup of G and K is any subgroup of H then K is a normal subgroup of G

B: H is a normal subgroup of G and K is a normal subgroup of H then K is a normal subgroup of G

C: H and K are any subgroups of G then HK is a subgroup of G

D: H and K are normal subgroups of G then HK is a subgroup of G

Question 9: Let G be a commutative group with a composition series then

A: G is always infinite

B: G is always finite

C: G may or may not be finite

D: G is always a group with 2 elements

Question 10: Let $G^{(n)}$ denote the nth commutator of a group G. Then G is solvable if and only if

A: $G^{(n)} = G$ for some n

B: $G^{(n)} = \phi$ for some n

C: $G^{(n)} = \{e\}$ for some n

D: $G^{(n)} = G'$ for some n

Question 11: Let G be a group of order pq where p and q are distinct prime numbers. Then

A: G has a normal series of its subgroups but it is not a solvable group

B: G is a solvable group.

C: G is always a non-abelian group.

D: G has a composition series of its subgroups but it is not a solvable group.

Question 12: Let S_3 be the symmetric group of degree 3. Then the series $I \subseteq A_3 \subseteq S_3$ is

A: It is a subnormal but not a normal series

B: It is a normal series.

C: It is a composition series but not a normal series

D: It is a normal series but not a composition series

Question 13: Statement I: Every composition series has a proper refinement.

Statement II: Homomorphic image of a solvable group is solvable.

A: Statement I is true but II is false.

B: Statement I and II both are false.

C: Statement II is true but I is false.

D: Statement I and II both are true.

Question 14: True/False Let $O(G) = 35$. Then G is a solvable group.

A: True

B: False

Question 15: A group of order 30 is solvable group.

A: True

B: False

Answers:

1)	C	2)	D	3)	B	4)	C	5)	A
6)	D	7)	B	8)	D	9)	B	10)	A
11)	B	12)	B	13)	C	14)	A	15)	A

Review Questions

1) Determine the composition series for A_n $(n \neq 4)$.
2) Prove that a finite p −group (p is a prime number) is cyclic if and only if it has only one composition series.
3) Let G and H are solvable groups. Show that $G \times H$ is solvable.
4) Prove that the cartesian product of two nilpotent groups is nilpotent.
5) Prove that S_n is not solvable for $n \geq 3$.
6) Prove that every group of order pqr; p, q, r are prime numbers, is solvable.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal, Cambridge university press

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 3: Basic Theory of Field Extension

CONTENTS

Expected Learning Outcomes

After studying this unit, you will be able to

- define rings, fields, and related algebraic structures
- understand field as a vector space
- define field extension, its degree, and basis
- define monic and minimal polynomial
- understand the concept of algebraic extension
- find algebraic closure of a field
- find the multiplicity of a root of a polynomial
- understand factor theorem
- analyze that the maximum number of roots of a polynomial over any field cannot exceed its degree
- state and prove Kronecker's result

Introduction

In this unit, we will introduce you to the field extensions and subfields. We will use irreducible polynomials for obtaining field extensions of a field F from $F[x]$. We will also show you that every field is a field extension of Q or Z, for some prime p. Because of this, we call Q and the Z_p as prime fields. We will discuss these fields briefly. Finally, we will look at finite fields. These fields were introduced by the young French mathematician Evariste Galois while he was exploring number theory. We will discuss some properties of finite fields which will show us how to classify them. Before reading this unit, we suggest that you go through the definitions of irreducibility.

3.1 Fields and Subfields

Throughout this chapter R denotes the set of real numbers, C denotes the set of complex numbers and Q denotes the set of rational numbers.

We start this section by defining rings.

Definition 3.1.1: A non-empty set R, with two binary compositions, called addition $(+)$ and multiplication $(.)$ is called a ring if

(i) R is an abelian group under addition

(ii) R is a semi-group under multiplication

(iii) For $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Clearly, $(R, +, \cdot)$ is an **abelian group under addition** implies that under addition R is closed, associative, has an identity element called zero, each element of R has an additive inverse in R and it is abelian.

$(R, \cdot)$ is closed and associative. Further multiplication is distributive over addition.

Example 3.1.2: The set of integers Z under the compositions of usual addition and multiplication is a ring.

Example 3.1.3: The set of square matrices of order 2 with all entries from real numbers is a ring under the matrix addition and matrix multiplication.

Note that a ring is closed and associative under the multiplication but it may or may not have a multiplicative identity. For example, ring if integers Z has multiplicative identity 1 but the ring of even integers does not contain identity element under multiplication.

Definition 3.1.4: A ring containing its multiplicative identity is called a ring with unity and the multiplicative identity of the ring is called unity of ring. Unity of a ring is generally denoted as 1.

Theorem 3.1.5: Let R be a ring with unity such that $1 = 0$. Then $R = \{0\}$.

Proof: Let $r \in R$ and $1 = 0$

Then $r = r \cdot 1 = r \cdot 0 = 0$

Therefore, $R = \{0\}$.

Let R be a ring with unity. Then $a \in R$ is called a unit if there exists an element $b \in R$ such that $ab = 1 = ba$.

A ring with unity has at least one unit that is its unity as it is its own inverse.

0 is an element in every ring with unity which is never a unit.

There are rings in which every non-zero element is a unit, for example, the ring of rational numbers under usual addition and multiplication of rational numbers.

Some rings are such that a few elements are units but not all are units for example, in the ring of integers Z, only 1 and -1 are units. No other integer is a unit.

Definition 3.1.6: A ring is called a division ring if it is with unity and all of its non-zero elements are units. For example, the ring of rational numbers, the ring of real numbers, etc. Z is not a division ring because elements other than 1 and -1 are not units.

Definition 3.1.7: A commutative division ring is called a field.

Clearly, F is a field then F is an additive abelian group. $F - \{0\}$ is a commutative group under multiplication. Multiplication is distributive over addition.

Definition 3.1.8: Let R be a ring. An element $a \in R$ is said to be zero divisor if there exists $b \in R$ such that $a \cdot b = 0$. If a and b are both non-zero but $a \cdot b = 0$ then a and b are called proper zero divisors. A ring that has proper zero divisors is called a ring with zero divisors.

For example, consider the ring M of square matrices of order 2 then M is a ring under the usual matrix addition and multiplication.
Consider, the matrices $[1\ 0\ 0\ 0\ ], [0\ 0\ 0\ 1\ ] \in M$
Then both the matrices are non-zero. However, $[1\ 0\ 0\ 0\ ][0\ 0\ 0\ 1\ ] = [0\ 0\ 0\ 0\ ]$
Therefore, both the matrices are proper zero-divisors of M and hence M is called a ring with proper zero divisors.

Definition 3.1.9: A commutative ring R with unity and without zero divisors is called an Integral domain. Clearly, the set of integers Z is an integral domain.

1) Every field is an Integral domain.

Let F be a field. Then by definition F is commutative and a ring with unity.

Let $a, b \in F$ such that $a \cdot b = 0$

If $a \neq 0$, then $a^{-1} \in F$

$$a \cdot b = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow b = 0$$

which implies that a or b is equal to 0. Hence F is without zero divisors.

Hence F is an Integral domain.

2) Not every Integral domain is a field

For example, the ring of integers is an Integral domain but not a field.

Definition 3.1.10: Let V be a non-empty set defined over a field F. Then V together with two compositions called addition (+ defined on V) and a scalar multiplication $V \times F \to V$ such that to each pair $(x, \alpha) \in V \times F$ it assigns a unique element $\alpha x \in V$, is called a vector space if it satisfies the following axioms

(i) $(V, +)$ is an abelian group

$$(ii)\ (\alpha + \beta)x = \alpha x + \beta x \ \forall\ \alpha, \beta \in F, x \in V$$

$$(iii)\ (x + y)\alpha = x\alpha + y\alpha \ \forall\ \alpha \in F, x, y \in V$$

$$(iv)(\alpha\beta)x = \alpha(\beta x) = (\alpha x)\beta \ \forall\ \alpha, \beta \in F, x \in V$$

$$(v)\ 1x = x \ \forall\ x \in V$$

For example, set of square matrices of order 2 with entries from the field of real numbers is a vector space under the usual matrix addition and scalar multiplication.

1) Every field is a vector space over itself
2) Since every vector space has a basis, therefore, every field also has a basis.

Definition 3.1.11: A non-empty subset S of a field F is called a subfield if it is a field under the induced compositions.

Theorem 3.1.12: A non-empty subset S containing at least two elements of a field F is a subfield of F if and only if $a - b \in S \ \forall\ a, b \in S$ and $ab^{-1} \in S \ \forall\ a \in S, b \in S - \{0\}$.

Proof: Let S be a subfield of F.

Then S is a field under the induced compositions.

This implies

$a - b \in S \ \forall\ a, b \in S$, and $ab^{-1} \in S \ \forall\ a \in S, b \in S - \{0\}$

Conversely, given that $a - b \in S \ \forall\ a, b \in S$

which implies that $(S, +)$ **is a group.**

Also, $ab^{-1} \in S \ \forall\ a \in S, b \in S - \{0\}$ implies that $S - \{0\}$ is a group under multiplication.

Distributive properties hold since $S \subseteq F$ and F is a field.

Hence S is a subfield of F.

Theorem 3.1.13: Intersection of two subfields of a field F is again a subfield.

Proof: Let S_1 and S_2 are two subfields of a field F.

Let $S = S_1 \cap S_2$

Since S_1 and S_2 are subfields of field F. Therefore $0, 1 \in S_1, S_2$

That is, $0, 1 \in S_1 \cap S_2 = S$

For $a, b \in S$

That is, $a, b \in S_1 \cap S_2$

$\Rightarrow a, b \in S_1$and $a, b \in S_2$

Since S_1 and S_2 are subfields of F.

$\Rightarrow a - b \in S_1$ and $a - b \in S_2$

$$\Rightarrow a - b \in S_1 \cap S_2 = S$$

Again, for $a \in S, b \in S - \{0\}$

$\Rightarrow a \in S_1, b \in S_1 - \{0\}$ since S_1 is a subfield therefore, $ab^{-1} \in S_1$

and $a \in S_2, b \in S_2 - \{0\}$ since S_2 is a subfield therefore, $ab^{-1} \in S_2$

$$\Rightarrow ab^{-1} \in S_1 \cap S_2 = S$$

Hence S is a subfield of F.

Corollary 3.1.14: Intersection of any non-empty family of subfields of a field F is a subfield of F.

Definition 3.1.15: Let S be the family of all the subfields of field F. Then $\bigcap S_\alpha$; $S_\alpha \in S$ is again a subfield of S and this is the smallest subfield contained in field F. The smallest subfield is called the prime subfield for example the field of rational numbers is a prime subfield of the field of real numbers.

Definition 3.1.16: A field that does not contain any other field, is called a prime field for example field of rational numbers is a prime field. The field of real numbers contains the field of rational numbers hence; field of real numbers is not a prime field.

Definition 3.1.17: Let R be an integral domain with unity element e. If there exists some $n \in N$ for which $ne = 0$, then the smallest such number is called characteristic of R. If such a natural number does not exist, that is, $ne \neq 0$ for every natural number n, then we say characteristic R is zero. The characteristic of ring R is denoted as Ch. R.

Theorem 3.1.18: The characteristic of an integral domain is either 0 or a prime number.

Proof: Let R be an integral domain with unity e.

Let Ch. $R = n \neq 0$

If possible, let n is a composite number.

Then $n = rs; 1 < r, s < n$

Since Ch.$R = n$

$$\Rightarrow ne = 0$$

$$\Rightarrow (rs)e = 0$$

$$\Rightarrow (re)(se) = 0$$

$\Rightarrow re = 0$ or $se = 0$ (R *is* integral domain and hence without zero divisors)

But $r, s < n$

and n, by the definition of the characteristic of a field, is the smallest positive integer for which $ne = 0$

Therefore, re, ne are both non-zero.

So, we arrive at a contradiction.

Hence our supposition was wrong.

That is, n is a prime number.

Therefore, Ch. R is either 0 or a prime number.

Note: Since every field is an integral domain, therefore, characteristic of a field is also either 0 or a prime number.

Task: Prove that the following are the subfields of the field of real numbers?

(a) $\{a + b\sqrt{2} | a, b \in Q\}$

(b) $\left\{a + \sqrt[3]{5}b + \left(\sqrt[3]{5}\right)^2 c | a, b, c \in Q\right\}$

3.2 Basic Theory of Field Extension

A field extension of a field F is a pair (K, σ), where K is a field containing F and σ is a monomorphism of F into K. For example, let F be a subfield of K then σ given be i that is $i(x) = x \; \forall \; x \in F$ is a monomorphism of F into K. Thus, for every subfield F of a field K, K is a field extension of F.

Symbolically, if K is a field extension of field F. then symbolically we write it as

Note:

1. Let K is a field extension of a field F. Then $(K, +)$ is an abelian group. Define $\sigma: K \times F \to K$ as $(x, \alpha) \mapsto \alpha x$. Then K can be treated as a vector space over the field F. For example, the field of complex numbers is a field extension of the field of real numbers and hence the field of complex numbers can be treated as a vector space over the field of real numbers.
2. Since every finitely generated vector space has a basis and from 1) we can conclude that every field extension K over F has a basis over F.

Definition 3.2.1: Let K is a field extension of field F, that is, K is vector space over F then basis of K over F is called the basis of field extension and number of elements in the basis is called the dimension of K over F or degree of extension of K over F, and it is denoted as $[K: F]$. For example, the set $\{1, i\}$ is a basis of field extension C over R and dimension of C over R is 2 that is $[C: R] = 2$.

Definition 3.2.2: Let K is a field extension of field F then $[K: F]$ is defined. K is called a finite extension of field F if $[K: F]$ is finite. We call it infinite if $[K: F]$ is infinite.

Now we give examples of finite and infinite field extensions

Example 3.2.3: Let $F = Q$ be the field of rational numbers and $K = Q(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in Q\}$

Consider $S = \{1, \sqrt{2}\}$

Every element of K can be written as $a + b\sqrt{2}; a, b \in Q$.

That means S spans K over F.

Also, S is linearly independent. Therefore, S is the basis of K over F. Hence $[K: F] = 2$ i.e., degree of K over F is 2 that is finite. K is a finite extension of F.

Example 3.2.4: Consider an indeterminate x over a field F. Let K be the field of quotients of $F[x]$. Then for $\alpha_0, \alpha_1, \alpha_{2'} \ldots, \alpha_n \in F$

$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n = 0$ implies that $\alpha_i = 0 \; \forall \; i$

$\Rightarrow \{1, x, x^2, \ldots \ldots\}$ is a linearly independent subset of K, which is an infinite set.

Hence, $[K: F]$ is infinite.

Theorem 3.2.5: Let K is a finite extension of F and L is a finite extension of K then L is a finite extension of F and $[L: F] = [L: K][K: F]$.

Proof: Let $[K: F] = n$ and $[L: K] = m$

Then there exist bases $\{x_1, x_2, \ldots, x_n\}$ of K over F and $\{y_1, y_2, \ldots, y_n\}$ of L over K.

Consider $s = \{x_i y_j | 1 \leq i \leq n, 1 \leq j \leq m\}$

Claim: S is the basis of L over F.

To prove that S is linearly independent

Let $\alpha_{ij} \in F$ such that

$$\sum_{i,j} \alpha_{ij} x_i y_j = 0$$

$$\Rightarrow \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} x_i \right) y_j = 0$$

Since $y_1, y_2, \ldots, y_n$ are linearly independent.

$$\Rightarrow \sum_{i=1}^{n} \alpha_{ij} x_i = 0 \; \forall \; 1 \leq j \leq m$$

Also, $x_1, x_{2,\ldots}, x_n$ are linearly independent

$$\Rightarrow \alpha_{ij} = 0 \forall 1 \leq i \leq n, 1 \leq j \leq m$$

This implies S is a linearly independent set.

Next, we prove that S spans L over F

Let $x \in L$

$\{y_1, y_2, \ldots, y_m\}$ is a basis of L over K.

This implies there exist $a_1, a_{2,\ldots}, a_m \in K$ such that $x = \sum_{j=J} \quad a_j y_j \ldots\ldots (1)$

Now $a_j \in K \; \forall \; j$ and $\{x_1, x_2, \ldots, x_n\}$ is a basis of K over F, there exist $\alpha_{ij} \in F$ such that

$$a_j = \sum_{i=1}^{n} \alpha_{ij} x_i$$

Put in (1)

$$x = \sum_{j=j}^{m} \sum_{i=1}^{n} \alpha_{ij} x_i y_j$$

Therefore, S **spans** L **over** F.

S is the basis of L over F. $[L:F]$ = number of elements in $S = nm = [L:K][K:F]$

Definition 3.2.6: Let S be a non-empty subset of a field F then K is called a subfield generated by S if

(i) K is a field containing S.

(ii) If there exists a field K' containing S then $K \subset K'$

In other words, K is the smallest subfield of F containing S.

If S is finite. Let $S = \{a_1, a_2, \ldots, a_n\}$. Then we write $K = F(a_1, a_{2,\ldots}, a_n)$. If S is infinite then we denote $K = F(S)$. If $S = \{a\}$ is a singleton set then $K = F(a)$.

Definition 3.2.7: Let $K = F(a)$ be an extension of F generated by elements of F and singleton set $\{a\}$. Then K is called a simple extension of F. For example, the extension $Q(\sqrt{2})$ is a simple extension of Q.

Note that $F(a)$ is the subfield of K generated by $\{a\}$ over F where $a \in K$. Then for $\alpha_0, \alpha_1, \cdots, \alpha_n \in F$

$$\alpha_0 + \alpha, a + \alpha_2 a^2 + \cdots + \alpha_n a^n \in F(a)$$

This implies

$$F[a] \subseteq F(a) \cdots (1)$$

Let T be the field of quotients of $F[a]$

From (1)

$$T \subseteq F(a)$$

Also $F \subset T$and $a \in T \Rightarrow F(a) \subset \top$

This implies $T = F(a)$

Similarly, if we take S containing more than one element then $F(S)$ is the field of quotients of subring of K generated by $F \cup S$.

Task: 1) Find the degree of extension and basis of $Q(\sqrt{3}+i)$ over Q.

2) Give an example of a field that has no proper field extension.

3.3 Algebraic Extension and Minimal Polynomial

Definition 3.3.1: (Roots of a polynomial) Let F is a field and K is a field extension of F. Then for $f(x) \in F[x], a \in K$ is called a root or zero of $f(x)$ if $f(a) = 0$. For example, C is a field extension of R. Then $i = \sqrt{-1} \in C$ is a root of the polynomial $x^2 + 1$ over R.

Definition 3.3.2: (Algebraic element over a field) Let F is a field and K is a field extension of F. Then $a \in K$ is called an algebraic element over the field F if there exists some non-zero polynomial $f(x) \in F[x]$ such that a is the root of $f(x)$. For example, C is a field extension of R. Consider $i = \sqrt{-1} \in C$, then i being the root of the polynomial $x^2 + 1$ over R is an algebraic element over R.

Note 1) $F \subseteq K$, any $a \in K$, if $a \in F$ then the polynomial $x - a \in F[x]$ such that a is a root of this polynomial. Hence every element of F is algebraic over F.

2) Let $a \in K$ such that $a \notin F$ then a may or may not be algebraic over F. for example, let $F = Q$ and $K = R$ then $\sqrt{2} \notin Q$ but it is a root of the polynomial $x^2 - 2 \in Q[x]$ and hence $\sqrt{2}$ is algebraic over Q.

Consider $\pi \in R, \pi$ is not algebraic over R.

Definition 3.3.3 (Algebraic extension of a field): A filed extension K of a field F is called an algebraic extension if every element of K is algebraic over F. For example, C is an algebraic extension of R.

Theorem 3.3.4: Let F be a field and K be a field extension of F. Let $a \in K$ is a root of polynomial $f(x)$ over F such that $f(0) \neq 0$. Then f is non-constant polynomial.

Proof: Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$.

Given that $f(0) \neq 0 \Rightarrow \alpha_0 \neq 0$

If possible let f is a constant polynomial. That is, $deg\ deg\ (f) = 0$.

Then $f(x) = \alpha_0\ \forall\ x$

In particular, $f(a) = \alpha_0 \neq 0$

which is in contradiction to the fact that a is the root of $f(x)$.

Therefore, our assumption was wrong. That is f is not a constant polynomial.

Definition 3.3.5: (Monic Polynomial) Let F be a field. A polynomial $f(x) \in F[x]$ is called a monic polynomial if the coefficient of the highest power of x is the unity of field F. For example, Let $F = R$ then polynomial $x^2 + 1$ is monic polynomial. Another example, consider the field Z_7 then $8x^5 + 2x^3 + 3$ is a monic polynomial as $8 \equiv 1$ in Z_7.

Theorem 3.3.6: Let K is a field extension of F. If an element $a \in K$ is algebraic over F, then there exists a unique monic polynomial $p(x)$ of a positive degree over F, such that

$$(i)\ p(a) = 0$$

(ii) If any $f(x) \in F(x)$ such that $f(a) = 0$ then $p(x)$ divides $f(x)$.

Proof: Since $a \in K$ is algebraic over F, therefore there exists some non-zero polynomial $f(x) \in F[x]$ such that $f(a) = 0$.

Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$ is a polynomial of least degree n such that $f(a) = 0$.

Degree $f(x) = n, \Rightarrow \alpha_n \neq 0$

That is, α_n is a non-zero element of field F and hence $\alpha_n^{-1} \in F$.

Let

$$\begin{aligned} p(x) &= \alpha_n^{-1} f(x) \\ &= \alpha_n^{-1}(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n) \\ &= \alpha_n^{-1}\alpha_0 + \alpha_n^{-1}\alpha_1 x + \alpha_n^{-1}\alpha_2 x^2 + \cdots + x^n \end{aligned}$$

Thus $p(x)$ is a monic polynomial with degree n that is the same as degree $f(x)$.

Also, $p(a) = \alpha_n^{-1} f(a) = \alpha_n^{-1} \cdot 0 = 0$

That is, a is a root of $p(x)$.

From Theorem 3.3.4, we get that $p(x)$ is non-constant polynomial.

Therefore, $deg\ deg\ p(x) > 0$

Let $f(x)$ be any other polynomial such that $f(a) = 0, f(x) \in F[x]$

Divide $f(x)$ by $p(x)$, by division algorithm of polynomials, there exists $q(x), r(x) \in F[x]$ such that

$f(x) = q(x)p(x) + r(x);\ r(x) = 0$ or $deg\ deg\ r(x) < deg\ deg\ p(x)$

Put $x = a, f(a) = q(a)p(a) + r(a)$

Since $f(a) = p(a) = 0$, therefore, we get $r(a) = 0$.

If $r(x) \neq 0$ then $deg\ deg\ r(x) < deg\ deg\ p(x)$ and $r(a) = 0$ is a contradiction to the choice of $p(x)$ as a polynomial of least degree with a as a root. Therefore, $r(x) = 0$.

That is, $f(x) = q(x)p(x)$

$p(x)$ divides $f(x)$ which proves part (ii).

For the uniqueness of part (i) let $f(x)$ is another monic polynomial such that $f(a) = 0$ and with least degree so that $deg\ deg\ p(x) = deg\ deg\ f(x) = n$.

Then by part (ii) $f(x)\ and\ p(x)$ divide each other that is, $f(x) = cp(x), c \in F$

Using this and the fact that $f(x)$ and $p(x)$ are both monic, comparing the leading coefficients on both sides we get that $c = 1$

That is $f(x) = p(x)$

which completes the proof of part (i).

Definition 3.3.7: (Minimal Polynomial) Let K be a field extension of a field F. Let $a \in K$ be an algebraic element over F. Then a non-zero polynomial $p(x) \in F[x]$ is called minimal polynomial of a over F if

$(i)\ p(x)$ is monic

$$(ii)\ p(a) = 0$$

$(iii)\ p(x)$ is the polynomial with the least degree such that it is monic and a is a root of $p(x)$

For example, let $F = R, K = C$

Then minimal polynomial of $i \in K$ is $x^2 + 1$

Note:

1) Theorem 3.3.6 ensures that minimal polynomial exists for every algebraic element of K over F and it is unique.

2) Let $p(x)$ be a minimal polynomial of some $a \in K$ over the field F. Then a is a root of any polynomial which is multiple of $p(x)$. In other words, if $f(x)$ is a polynomial over F such that $f(a) = 0$ then either $f(x)$ is itself a minimal polynomial of a over F or a multiple of a minimal polynomial of a over F.

3) A polynomial $f(x) \in F[x]$ is called reducible polynomial if $f(x) = g(x)h(x); g(x), h(x) \in F[x]$ and both $g(x)$ and $h(x)$ are of a positive degree. If $f(x)$ is a monic polynomial over F such that $f(a) = 0$ and it is not a minimal polynomial of $a \in K$. Let $p(x) \in F[x]$ is minimal polynomial of a, then $p(x)$ divides $f(x)$. That means, $f(x) = p(x)q(x)$ for some $q(x) \in F[x]$. $p(x)$ being minimal polynomial is of positive degree. If possible, let $deg\ deg\ q(x) = 0$, then $q(x) = c \in F$ this implies, $deg\ deg\ p(x) = deg\ deg\ f(x)$ and since $f(x)$ is monic therefore by the uniqueness of minimal polynomial $f(x) = p(x)$ which is a contradiction to the fact that $f(x)$ is not a minimal polynomial over F. So, our supposition was wrong. That is, $deg\ deg\ q(x) > 0$ and hence $f(x)$ is reducible polynomial. That is, a non-zero monic polynomial $f(x) \in F[x]$ for which $f(a) = 0$ for some $a \in K$, is either minimal polynomial for a or it is reducible.

4) We can observe that irreducible polynomial over the field F having a root $a \in K$ is always a minimal polynomial of a over F.

Example 3.3.8: Consider the polynomial $f(x) = x^2 + x + 1 \in Q[x]$ then $\omega = \frac{-1 \pm \sqrt{3}i}{2} \in C$ is a root of $f(x)$. Now $\omega \notin Q$ hence the degree of its minimal polynomial is at least 2 and $f(x)$ is a polynomial of degree 2 with ω as a root this implies that $f(x)$ is minimal polynomial of ω over Q.

Task: 1) Find the minimal polynomial of $\sqrt{5}$ over Q.

2) If an element $a \in K$ has minimal polynomial $f(x)$ over some field F then $deg\ deg\ f(x) = 1$ if and only if $a \in F$.

3.4 Algebraic and Finite Extensions

Theorem 3.4.1: An element a of K is algebraic over F if and only if $[F(a): F]$ is finite.

Proof: Suppose $[F(a): F]$ is finite.

Number of elements in the basis of $F(a)$ over the field F is finite. Let $[F(a): F] = n$.

Let $T = \{1, a, a^2, \dots, a^n\}$. Then S contains $n + 1$ elements which are more than n. Hence, S is linearly dependent. There exists $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n \in F$ (not all zero) such that

$$\alpha_0 \cdot 1 + \alpha_1 \cdot a + \alpha_2 \cdot a^2 + \cdots + \alpha_n a^n = 0$$

Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$. Then $f(x) \in F[x]$ such that $f(a) = 0$

This implies that a is an algebraic element over the field F.

Conversely, let a is the algebraic element over the field F and $p(x)$ is minimal polynomial of a over F of degree n.

Claim: $F[a]$ **is a field.**

We know that $F[a]$ is a ring with unity. To prove that it is a field it is sufficient to prove that every non-zero element of $F[x]$ is a unit.

Let $0 \neq f(a) \in F[a]$

This implies that $p(x)$ does not divide $f(x)$.

So, we can choose $A(x), B(x) \in F[x]$ such that $p(x)A(x) + f(x)B(x) = 1$

In particular, for $x = a$,

$$p(a)A(a) + f(a)B(a) = 1 \dots (1)$$

Using the fact that $p(x)$ is minimal polynomial for a, we get that $p(a) = 0$

Hence, (1) becomes $f(a)B(a) = 1 = B(a)f(a)$

$$\Rightarrow B(a) = \big(f(a)\big)^{-1} \in F[a]$$

That is, $f(a)$ is a unit in $F[a]$.

Hence, $F[a]$ is a field.

However, $F(a)$ is the field of quotients of $F[a]$

We get, $F(a) = F[a]$

Consider $S = \{1, a, a^2, \dots, a^{n-1}\}$. Now we prove that S is a basis of $[F(a): F]$.

If possible, let $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in F$ such that $\alpha_0 \cdot 1 + \alpha_1 \cdot a + \cdots + \alpha_{n-1} a^{n-1} = 0$.

Consider, $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \in F[x]; f(a) = 0$

$$deg\ deg\ f(x) = n - 1 < deg\ deg\ p(x)$$

So, we arrive at a contradiction unless $\alpha_i = 0\ \forall\ i$

which proves that S **is linearly independent.**

Let $f(a) = \beta_0 + \beta_1 a + \cdots + \beta_m a^m \in F[a] = F(a)$

Then $f(x) = \beta_0 + \beta_1 x + \cdots + \beta_m x^m$

Divide $f(x)$ by $p(x)$, by division algorithm of polynomials, there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = q(x)p(x) + r(x)$; $r(x) = 0$ or $deg\ deg\ r(x) < deg\ deg\ p(x)$.

At $x = a, f(a) = q(a)p(a) + r(a) \Rightarrow f(a) = r(a)$

Either $r(x) = 0$ or $deg\ deg\ r(x) < deg\ deg\ p(x)$

$$\Rightarrow r(x) = \delta_0 + \delta_1 x + \cdots \vdash \delta_{n-1} x^{n-1}; \delta_i \in F$$

$$f(a) = r(a) = \delta_0 + \delta_1 a + \cdots + \delta_{n-1} a^{n-1} \in L(S)$$

That is, S **spans** $F(a)$

Hence, S is the basis of $F(a)$ over F. $[F(a): F]$ = number of elements in set $S = n$ i.e.; finite.

Theorem 3.4.2: Every finite extension of a field is an algebraic extension.

Proof:

Let K be a finite extension of a field F; $[K: F] = n$

Let $a \in K$ be an arbitrary element of K.

Then $F(a)$ is a subfield of K.

That is, $[F(a): F]$ divides $[K: F] = n$

This implies, $[F(a): F] \leq n$

So, $[F(a): F]$ is finite. By Theorem 3.4.1, we get that a is an algebraic element over F. This proves that every element of K is algebraic over F. Hence, K is an algebraic extension of F.

Remark: Let F, F_1 and K be fields such that $F \subseteq F_1 \subseteq K$. Let $a \in K$ be algebraic element over F then $[F_1(a): F_1] \leq [F(a): F]$.

Proof:

Let $[F_1(a): F_1] = m$

That is, the degree of the minimal polynomial $p_1(x)$ of a over F_1 is m.

Similarly, let $[F(a): F] = n$

That is, degree of minimal polynomial $p(x)$ of a over F is n.

Since $p(x)$ is minimal polynomial of a over F, therefore, $p(a) = 0$

Also, $F \subseteq F_1; p(a) = 0$ where $p(x)$ can be considered as a polynomial over F_1.

Therefore, $p_1(x)$ divides $p(x)$

$$\Rightarrow deg\ deg\ p_1(x) \leq deg\ deg\ p(x)$$

$\Rightarrow m \leq n$ that is, $[F_1(a): F_1] \leq [F(a): F]$

Theorem 3.4.3: Let L is an algebraic extension of K and K is an algebraic extension of F then L is an algebraic extension of F.

Proof: Since L is an algebraic extension of K, for $a \in L, a$ is an algebraic element over K.

Let $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} + x^n$ is minimal polynomial of a over K of degree n; $\alpha_i \in k\ \forall\ 0 \leq i \leq n-1$ that is, $p(a) = 0$.

K is also an algebraic extension of F.

Define a chain

$$F_0 = F$$

$$F_1 = F_0(\alpha_0)$$

$$F_2 = F_1(\alpha_1) = F_0(\alpha_0, \alpha_1)$$

$$\vdots$$

$$\vdots$$

$$F_n = F_{n-1}(\alpha_{n-1}) = F_0(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$$

Clearly, $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$

Since each α_i is algebraic over F and over F_{i-1}, so by the remark,

$$[F_i: F_{i-1}] = [F_{i-1}(\alpha_{i-1}): F_{i-1}] \leq [F(\alpha_{i-1}): F]$$

That is, $[F_i: F_{i-1}]$ is finite for every i.

Also,

$$[F_n: F] = [F_n: F_{n-1}][F_{n-1}: F_{n-2}] \cdots [F_1: F]$$

That is a finite product of finite positive integers. Hence, $[F_n: F]$ is finite.

Also, $\alpha_i \in F_n \; \forall \; i$

$\Rightarrow a$ is algebraic over F_n

Therefore, $[F_n(a): F_n]$ is finite.

Also, $[F_n(a): F] = [F_n(a): F_n][F_n: F]$

This implies, $[F_n(a): F]$ is finite.

That means, $F_n(a)$ is algebraic extension of F.

$\Rightarrow a$ is algebraic over F as $a \in F_n(a)$

$\Rightarrow L$ is algebraic extension of F.

Theorem 3.4.4: The set S of all those elements of K, which are algebraic over F, is a subfield of K containing F such that no element a of K which is not in S is algebraic over S.

Proof: For $\alpha \in F, x - \alpha$ is a minimal polynomial of α over F.

α is algebraic over F

$\Rightarrow \alpha \in S; \; F \subseteq S$.

Let $a, b \in S$

$\Rightarrow a$ and b are algebraic elements of K over F.

$\Rightarrow [F(a): F]$ and $[F(b): F]$ are both finite.

Since b is algebraic over F

$\Rightarrow b$ is algebraic over $F(a)$

$\Rightarrow [F(a)(b): F(a)]$ is finite.

$\Rightarrow [F(a, b): F(a)]$ is finite.

Now, $a, b \in F(a, b)$ and $F(a, b)$ is a field.

$$\Rightarrow a - b, ab^{-1} \in F(a, b)$$

Also, $[F(a, b): F] = [F(a, b): F(a)][F(a): F]$ is finite hence, $F(a, b)$ is algebraic over F implies $a - b, ab^{-1}$ both are algebraic over F.

$$a - b, ab^{-1} \in S$$

$\Rightarrow S$ **is a subfield of** K**.**

If in the above discussion, we replace F by S, then the set S_1 which contains all those elements of K which are algebraic over S form a subfield of K containing S. Thus S_1 is an algebraic extension of S and S is an algebraic extension of F. So, S_1 is an algebraic extension of F (By Theorem 3.4.3). Consequently, $S_1 \subseteq S$ and hence, $S = S_1$. If any $a \in K$ is algebraic over S then by definition of $S_1, a \in S_1$. So, $a \in S$ as $S_1 = S$. Hence, no element of K not in S is algebraic over S.

1) Let K be a field extension of field F. Then for $a, b \in K$, if a, b are algebraic over F then $a \pm b, ab$ are algebraic over F. Moreover, if $b \neq 0, ab^{-1}$ is algebraic over F.
2) S defined above is the largest possible algebraic extension of F in K, S is algebraically closed with respect to K, S is also called algebraic closure of F relative to K.

1) Prove that R is not an algebraic extension over Q.

2) Find algebraic extensions of Q and R. Observe that the two are the same.

3.5 Factor Theorem

A polynomial of degree n over a field F cannot have more than n roots in any field extension of F

Theorem 3.5.1: (Factor Theorem): Any element $a \in K$ is a root of a polynomial $f(x)$ over F of positive degree if and only if $x - a$ divides $f(x)$ in $K[x]$.

Proof:

Let $x - a$ divides $f(x)$ in $K[x]$.

This implies, there exists $g(x) \in K[x]$ such that $f(x) = (x - a)g(x)$

At $x = a, f(a) = (a - a)g(a) = 0$

This implies that a is a root of $f(x)$.

Conversely, let a is a root of $f(x)$ in K.

Divide $f(x)$ by $x - a$, there exist $q(x), r(x) \in K[x]$ such that $f(x) = (x - a)q(x) + r(x) \ldots (1)$ where $r(x) = 0;\ deg\ r(x) < deg\ deg\ (x - a) = 1$.

This implies, $r(x) = c$; where c is an element of K.

Put $x = a$ in (1)

$$f(a) = (a - a)q(a) + r(a) = r(a)$$

This implies, $r(a) = 0$

But $r(x) = c\ \forall\ x$

This implies, $r(x) = 0\ \forall\ x$

Put in (1)

We get, $f(x) = (x - a)q(x)$

This implies, $x - a$ divides $f(x)$.

Multiplicity of a root: Let $f(x) \in F[x]$ be a non-zero polynomial then if $f(x)$ has a root $x = a$, then the number of times it is appearing as a root of $f(x)$ is called multiplicity of a.

For example, let $F = C, f(x) = (x + 1)^2(x^2 + 1)$ then $f(x)$ has four roots $-1, -1, i, -i$. Therefore, -1 is a root of $f(x)$ with multiplicity 2 whereas, i and $-i$ are roots with multiplicity 1.

Theorem 3.5.2: Let a is a root of $f(x)$ of multiplicity m then $f(x) = (x - a)^m g(x)$ such that $g(a)$ is non-zero.

Proof: Let a be a root of $f(x)$ of multiplicity m. This implies, $(x - a)^m$ divides $f(x)$ but $(x - a)^{m+1}$ does not divide $f(x)$.

Since, $(x - a)^m$ divides $f(x)$

Therefore, there exists $g(x) \in F[x]$ such that $f(x) = (x - a)^m g(x) \ldots (1)$

If possible, let $g(a) = 0$

This implies that $x - a$ divides $g(x)$

or, $g(x) = (x - a)h(x); h(x) \in F[x]$

From (1), $f(x) = (x - a)^m(x - a)h(x) = (x - a)^{m+1}h(x)$

which is in contradiction to the choice of m. So, our supposition was wrong. That is, $g(a) \neq 0$.

Theorem 3.5.3: A polynomial of degree n, where n is positive, over a field F cannot have more than n roots in any field extension of F.

Proof: Let $f(x)$ be a polynomial of degree n. We will prove this result using the principle of mathematical induction on n.

For $n = 1$

Let $f(x) = \alpha x + \beta;\ \alpha, \beta \in F$

Since $deg\ deg\ f(x) = 1 \Rightarrow \alpha \neq 0$

Therefore, $\alpha^{-1} \in F$

Consider $x = -\alpha^{-1}\beta \in F$

$$f(-\alpha^{-1}\beta) = \alpha(-\alpha^{-1}\beta) + \beta = 0$$

Therefore, the result is true for all polynomials with degree $< n; n \geq 1$

For n; let $f(x)$ be a polynomial of degree n.

Let K is any extension of F.

If $f(x)$ has no root in K then we are through.

If $f(x)$ has at least one root a in K that is, $f(x) = (x-a)^m g(x);\ g(a) \neq 0; m \geq 1$

$$deg\ deg\ g(x) = n - m < n$$

By the induction hypothesis, $g(x)$ has at the most $n - m$ roots in K.

Therefore, $f(x)$ has maximum $n - m + m = n$ roots in K.

So, any polynomial of degree n can have maximum n roots in any field extension of F.

Task: 1) Give an example of a polynomial over a field F with a positive degree but no root.

2) Give an example of a polynomial over a field F with a degree more than 1 but only one root.

3.6 Kronecker's Result

Theorem 3.6.1: (Kronecker's result) If $p(x)$ is an irreducible polynomial over a field F then there exists an extension E of F such that $[E:F] = deg\ p(x)$ and $p(x)$ has a root in E.

Proof: $p(x)$ is irreducible polynomial.

This implies that $< p(x) >$ is a maximal ideal of $F[x]$.

$F[x]$ is integral domain

Therefore, $\frac{F[x]}{<p(x)>}$ is a field.

Let $E = \frac{F[x]}{<p(x)>}$

$$F \subseteq F[x] \subseteq E \Rightarrow F \subseteq E$$

Define $\sigma: F \to E = \frac{F[x]}{<p(x)>}$ as $\sigma(\alpha) = \alpha + < p(x) >\ \forall\ \alpha \in F$

Let $\alpha, \beta \in F$

$$\sigma(\alpha + \beta) = (\alpha + \beta) + < p(x) > = (\alpha + < p(x) >) + (\beta + < p(x) >) = \sigma(\alpha) + \sigma(\beta)$$

$$\sigma(\alpha\beta) = \alpha\beta + < p(x) > = (\alpha + < p(x) >)(\beta + < p(x) >) = \sigma(\alpha)\sigma(\beta)$$

Hence, σ **is a homomorphism.**

Let $\alpha \in ker\ ker\ \sigma$

$$\Rightarrow \alpha \in F; \sigma(\alpha) = < p(x) >$$

$$\Rightarrow \alpha + < p(x) \geq < p(x) >$$

$$\Rightarrow \alpha \in < p(x) >$$

That is, $ker\ ker\ \sigma = \{< p(x) >\}$

This implies, σ **is one-one.**

Therefore, $\sigma: F \to E$ is a monomorphism and $F \subseteq E$

$\Rightarrow E$ **is a field extension of** F**.**

Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$

Now, $p(x) \in < p(x) >$

$$\Rightarrow p(x) + < p(x) > = < p(x) >$$

Now, $< p(x) > = p(x) + < p(x) >$

$$= (\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n) + < p(x) >$$

$$= \alpha_0 + \alpha_1(x + < p(x) >) + \cdots + \alpha_n(x^n + < p(x) >)$$

$$= \alpha_0 + \alpha_1(\underline{x}) + \cdots + \alpha_n(\underline{x})^n;\ \underline{x} = x + < p(x) > = p(\underline{x})$$

That is, $p(\underline{x}) = < p(x) >$

$\underline{x} \in E$ **is a root of** $p(x)$.

Claim: $\{1, \underline{x}, \underline{x}^2, \ldots, \underline{x}^{n-1}\}$ is a basis for $[E: F]$

$$E = \frac{F[x]}{< p(x)}>$$

Let $f(x) + < p(x) > \in E$

Now, divide $f(x)$ by $p(x)$, there exist unique $q(x)$ and $r(x)$ such that $f(x) = p(x)q(x) + r(x)$ ... (1) where $r(x) = 0$ or $deg\ deg\ r(x) < deg\ deg\ p(x) = n$

Then $r(x) = \beta_0 + \beta_1 x + \cdots \beta_{n-1} x^{n-1}; \beta_i \in F$

$$f(x) = p(x)q(x) + r(x)$$

$$\Rightarrow f(\underline{x}) = p(\pi)q(\underline{x}) + r(\underline{x}) = < p(x) > q(\underline{x}) + r(\underline{x})$$

$\Rightarrow f(\underline{x}) = r(\underline{x})$ in E

$$\Rightarrow f(x) + < p(x) \geq \beta_0 + \beta_1 \underline{x} + \cdots + \beta_{n-1} \underline{x}^{n-1}$$

Therefore, $\{1, \underline{x}, \underline{x}^2, \ldots, \underline{x}^{n-1}\}$ **generates** E **over** F**.**

Let $\gamma_0, \gamma_1, \ldots, \gamma_{n-1} \in F$ such that

$$\gamma_0 + \gamma_1 \underline{x} + \gamma_2 \underline{x}^2 + \cdots + \gamma_{n-1} \underline{x}^{n-1} = < p(x) >$$

$$\Rightarrow \gamma_0 + \gamma_1(x + < p(x) >) + \gamma_2(x + < p(x) >)^2 + \cdots + \gamma_{n-1}(x + < p(x) >)^{n-1} = < p(x) >$$

$$\Rightarrow \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_{n-1} x^{n-1} + < p(x) > = < p(x) >$$

$$\Rightarrow \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_{n-1} x^{n-1} \in < p(x) >$$

$$\Rightarrow \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_{n-1} x^{n-1} = p(x)g(x); g(x) \in F[x]$$

That is, $deg\ deg\ \big(p(x)g(x)\big) = n - 1$

$$\Rightarrow deg\ deg\ p(x) + deg\ deg\ g(x) = n - 1$$

But $deg\ deg\ p(x) = n$ and $deg\ deg\ g(x) \geq 0$

$$\Rightarrow deg\ deg\ p(x) + deg\ deg\ g(x) \geq n$$

$\Rightarrow n - 1 \geq n$ which is absurd unless $\gamma_i = 0\ \forall\ i$

$\Rightarrow \{1, \underline{x}, \underline{x}^2, \ldots, \underline{x}^{n-1}\}$ **is linearly independent.**

Therefore, $[E: F] = n = deg\ deg\ p(x)$

Theorem 3.6.2: If $f(x)$ is any polynomial over a field F with a positive degree n then there exists an extension E of F such that $f(x)$ has n roots in E and $[E: F]$ is maximum $n!$

Proof: We prove this result by the principle of mathematical induction

For $n = 1$

Consider $f(x) = \alpha x + \beta;\ \alpha \neq 0, \alpha, \beta \in F$

Since $\alpha \neq 0, \alpha^{-1} \in F$

Therefore, $-\alpha^{-1}\beta \in F$

and $f(-\alpha^{-1}\beta) = \alpha(-\alpha^{-1}\beta) + \beta = 0$

Therefore $E = F$.

So, the result is true for $n = 1$.

Let the result be true for all polynomials with a degree less than n.

Let $f(x)$ be the polynomial with degree n.

Let $p(x)$ be the irreducible polynomial such that $p(x)$ divides $f(x)$ in $F[x]$.

So, by Theorem 3.6.1, there exists a field extension E' of F such that $p(x)$ has a root a in E' and $[E': F] = deg\ deg\ p(x) \leq n$

Now, a is the root of $p(x)$ and hence of $f(x)$.

Therefore, $f(x) = (x - a)g(x)$

So that $deg\ deg\ g(x) = n - 1 < n$

By the induction hypothesis, $g(x)$ has $n - 1$ roots in some extension E of E'

Therefore, $f(x)$ has $n - 1$ roots in extension E of E'; $[[E: E'] \leq (n - 1)!$

That is, E has n roots of $f(x)$ and $[E: F] = [E: E'][E': F] \leq n \cdot (n - 1)! = n!$

Task: 1) Find the field E containing all the roots of polynomial $x^2 + x + 1 \in Q[x]$.

2) Find the field E containing all the roots of polynomial $x^3 + 3 \in Q[x]$.

3) Prove that the field E containing all the roots of $x^2 + 1 \in R[x]$ is C.

Summary

- The algebraic structures rings and fields are defined.
- A field extension is defined and analyzed as a vector space. Further degree and basis of this extension are discussed.
- Monic and Minimal polynomials are defined and related results are discussed.
- Multiplicity of a root of a polynomial is defined and the Factor theorem is proved.
- It is proved that any field extension E of F contains at the most n roots of polynomial $f(x)$; where $f(x)$ is polynomial over F and $deg\ deg\ f(x) = n$.

Keywords

- Fields
- Field Extensions
- Algebraic Extension
- Minimal Polynomial
- Finite Extension
- Factor Theorem
- Kronecker's result

Self-assessment

Choose the most suitable answer from the options given with each question.

Question 1: Which of the following is NOT a field?

A: The ring of integers

B**:** The ring of real numbers

C: The ring of rational numbers

D: The ring of complex numbers

Question 2: Choose the correct statement

A: Every field is an integral domain

B: Every integral domain is a field

C: Every division ring is a field

D: Every commutative ring is a field

Question 3: Units of the ring Z_4 are

A: 1

B**:** 3

C: 1, 3

D: 1, 2, 3

Question 4: Degree of extension of $Q(\sqrt{3})$ over Q is

A: 1

B: 2

C: 3

D: Infinite

Question 5: Degree of extension of $Q(\sqrt{2},\sqrt{3})$ over Q is

A: 2

B: 3

C: 6

D: 1

Question 6: Which of the following is an algebraic extension of the field of rational numbers?

A: R

B: C

C: Both R and C

D: None of R and C

Question 7: Degree of the minimal polynomial of $x = i \in C$ over R is

A: 1

B: 2

C: 3

D: 4

Question 8: Degree of the minimal polynomial of $\omega = \sqrt[3]{1}, \omega \neq 1$ over the field of real numbers is

A: 4

B: 3

C: 2

D: 1

Question 9: True/ False Let K be a field extension of a field F.Then minimal polynomial of an element $a \in K$ is unique.

A: True

B: False

Question 10: Consider the polynomial $f(x) = (x^3 - 1)(x^2 - 1) \in R[x]$. Then multiplicity of 1 as a root of $f(x)$ is

A: 2

B: 3

C: 4

D: 5

Question 11: Let K be a field extension of a field F. Then

Statement I: $[K:F]=1$

Statement II: $K=F$

A: Both the statements are equivalent.

B: Statement I is necessary for II but not sufficient.

C: Statement I is sufficient for II but not necessary

D: Both the statements are independent.

Question 12: Basis of C over R is

A: $\{1,i,-1\}$

B: $\{1,i,-i\}$

C: $\{1,i\}$

D: $\{1,-1,i,-i\}$

Question 13: Let K is a finite extension of F and L is a finite extension of K such that $[K:F]=2$ and $[L:K]=3$. Then $[L:F]$ is

A: 2

B: 6

C: 3

D: Infinite

Question 14: Which of the following is a simple extension of Q

A: $Q(\sqrt{2},2)$

B: $Q(\sqrt{3},\ i)$

C: R

D: C

Question 15: Which of the following is not an algebraic extension of Q?

A: $Q(\sqrt{2})$

B: $Q(\sqrt{3},i)$

C: R

D: C

Question 16: Which of the following is a monic polynomial over Z_{11}?

A: $(4x^2+3x+1)(3x^2+4x+1)$

B: $(2x+5)(5x+1)$

C: $(x^3+3x^2+1)(2x+5)$

D: $(7x^2+3)(x^2+1)$

Question 17: Minimal polynomial of $1+i$ over the field of real numbers is

A: x^2+2x+1

B: x^2-2x+1

C: x^2-2x-2

D: x^2-2x+2

Question 18: Minimal polynomial of an element $a \in F$ over F

A: always exists and is of degree 1

B: May or may not exist

C: Never exists

D: Always exists and is of degree 2

Question 19: Minimal polynomial of $\omega = \frac{1+\sqrt{3}i}{2}$ over the field of real numbers is

A: $x^2 + x + 1$

B: $x^2 - x + 1$

C: $x^3 - 1$

D: $x^3 + 1$

Question 20: Which of these is not algebraic over Q?

A: π

B: $\sqrt{5}$

C: i

D: ω

Answers:

1)	A	2)	A	3)	C	4)	B	5)	C
6)	B	7)	B	8)	C	9)	A	10)	A
11)	A	12)	C	13)	B	14)	C	15)	A
16)	A	17)	D	18)	A	19)	A	20)	A

Review Questions

1) Let K be a field extension of F. Prove that $[K:F] = 1$ if and only if $K = F$.
2) Find a basis and degree of $Q(\sqrt{2}, \sqrt{3})$ over Q.
3) Prove that a cubic polynomial over a field F is reducible over F if and only if it has a root in F.
4) Prove that $F(\sqrt{2} + \sqrt{3}) = F(\sqrt{2}, \sqrt{3})$
5) Find the smallest extension of Q having a root of $x^4 - 2 \in Q[x]$.
6) Find the smallest extension of Q having a root of $x^2 + 4 \in Q[x]$.
7) Prove that $\sqrt{p}$ is algebraic over Q where p is a prime number.
8) Determine the minimal polynomial of $\sqrt{2} + 5$ over Q.
9) Let $f(x) \in F[x]$ has a root a of multiplicity 2. Then prove that a is a root of derivative of $f(x)$.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal, Cambridge university press

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 04: Splitting Fields

CONTENTS

Objectives

After studying this unit, you will be able to

- define and find the splitting field of a polynomial of degree n over some field F
- prove that two splitting fields of a polynomial are isomorphic
- find basis and degree of extension of splitting field of a polynomial over a field
- define conjugate elements and algebraically closed fields with example
- find the degree of the minimal polynomial of an algebraic element over some field
- relate the concept of differentiability with multiple roots
- define separable/inseparable polynomials, elements, and extensions over a field F
- prove that any algebraic extension of a finite field F is a separable extension.

Introduction

Let F be a field and $f(x)$ is a polynomial of degree $n \geq 1$ over the field F. Then in this unit, we will observe that in any field extension K of F, $f(x)$ can have maximum n roots. Further, we will see that there will be a field E called splitting field of polynomial $f(x)$ containing exactly n roots, i.e., all the roots. Further, we will see that two splitting fields of a polynomial are isomorphic.

The minimal polynomial will be defined corresponding to an algebraic element a of K over F. Algebraic and separable extensions will be defined and explained.

4.1 Splitting Fields

Definition 4.1.1: Let F be a field and $f(x) \in F[x]$ is of degree $n \geq 1$. Then a field E is called splitting field of $f(x)$ if

1. $f(x)$ can be factorized into n linear factors over E.
2. There does not exist any field E' such that $f(x)$ can be factorized into n linear factors in E' and $E' \subset E$.

For example, consider $f(x) = x^2 - 2 \in \mathbb{Q}[x]$

Then $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ has two roots $\sqrt{2}, -\sqrt{2}$ neither of which is a rational number.

Consider $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$

Then $\mathbb{Q}(\sqrt{2})$ contains both the roots of $f(x)$.

That is, $f(x)$ is factorized in 2 linear factors over $\mathbb{Q}$.

Note that, the field of real numbers $\mathbb{R}$ also contains both the roots of $f(x)$. However, $\mathbb{R}$ is not the smallest such field as $\mathbb{Q}(\sqrt{2})$ is properly contained in $\mathbb{R}$.

However, if there exists some field extension K of $\mathbb{Q}$ containing both the roots of $f(x)$ and contained in $\mathbb{Q}(\sqrt{2})$.

Since K contains both the roots of $f(x)$ this implies $\sqrt{2} \in K$. Also, $Q \subseteq K, \Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq K$

which implies that $K = \mathbb{Q}(\sqrt{2})$.

That is, $\mathbb{Q}(\sqrt{2})$ is the smallest field extension of $\mathbb{Q}$ containing all the roots of $f(x)$, hence $\mathbb{Q}(\sqrt{2})$ is the splitting field of $f(x)$.

The next theorem ensures the existence of a splitting field.

Theorem 4.1.2: If $f(x)$ is any polynomial over a field F with a positive degree then there exists an extension E of F such that $f(x)$ has n roots in E and $[E:F]$ is maximum $n!$

Proof:

We prove this result by the principle of mathematical induction

For $n = 1$

Consider $f(x) = \alpha x + \beta;\ \alpha \neq 0, \alpha, \beta \in F$

Since $\alpha \neq 0, \alpha^{-1} \in F$

Therefore, $-\alpha^{-1}\beta \in F$

and $f(-\alpha^{-1}\beta) = \alpha(-\alpha^{-1}\beta) + \beta = 0$

Therefore $E = F$.

So, the result is true for $n = 1$.

Let the result be true for all polynomials with degree less than n.

Let $f(x)$ be the polynomial with degree n.

Let $p(x)$ be the irreducible polynomial such that $p(x)$ divides $f(x)$ in $F[x]$.

So, by Theorem 3.6.1, there exists a field extension E' of F such that $p(x)$ has a root a in E' and $[E':F] = \deg p(x) \leq n$

Now, a is root of $p(x)$ and hence of $f(x)$.

Therefore, $f(x) = (x - a)g(x)$

So that $\deg g(x) = n - 1 < n$

By the induction hypothesis, $g(x)$ has $n - 1$ roots in some extension E of E'

Therefore, $f(x)$ has $n - 1$ roots in extension E of E'; $[[E:E'] \leq (n-1)!$

That is, E has n roots of $f(x)$ and $[E:F] = [E:E'][E':F] \leq n \cdot (n-1)! = n!$

From the above theorem, it is evident that any polynomial over a field F has some splitting field E with $[E:F\} \leq n!$.

Remark: An isomorphism σ between two fields F and F' can be extended to an isomorphism between their quotient fields as follows

$\sigma: F \to F'$ is an isomorphism. Let us consider $F[x]$ and $F'[t]$.

Define $\eta: F[x] \to F'[t]$ as

$$\eta(f(x)) = \quad \eta(\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n)$$

$$= \quad \sigma(\alpha_0) + \sigma(\alpha_1)t + \cdots + \sigma(\alpha_n)t^n$$

$$\alpha_i \in F \ \forall \ i \ \Rightarrow \sigma(\alpha_i) \in F'$$

$\eta: F[x] \to F'[t]$ is an isomorphism.

Let $p(x)$ be an irreducible polynomial over the field F. Let us denote $\eta\big(p(x)\big) = p'(t)$ and $\sigma(\alpha) = \alpha' \ \forall \ \alpha \in F$.

Claim:$p'(t)$ is an irreducible polynomial of $F'[t]$.

Let there exist polynomials $r'(t), s'(t) \in F'[t]$ such that

$$p'(t) = r'(t)s'(t)$$

Now, $\eta: F[x] \to F'[t]$ is an isomorphism.

That is, there exist $r(x), s(x) \in F[x]$ such that

$$\eta\big(r(x)\big) = r'(t)$$

and

$$\eta\big(s(x)\big) = s'(t)$$

Consider $p'(t) = r'(t)s'(t)$

$\Rightarrow \eta\big(p(x)\big) = \eta\big(r(x)\big)\eta\big(s(x)\big) = \eta\big(r(x)s(x)\big)$

$\Rightarrow p(x) = r(x)s(x)$

Since $p(x)$ is an irreducible polynomial over F, therefore, either $\deg r(x) = 0$ or $\deg s\,(x) = 0$.

Also, η being isomorphism preserves degree, that is,

$r'(t)$ or $s'(t)$ is constant polynomial.

This implies, $p'(t)$ is irreducible polynomial in $F'[t]$.

$< p(x) >$ and $< p'(t) >$ are both maximal ideals of $F[x]$ and $F'[t]$ respectively.

We know that for a ring R and an ideal I of R, R/I is a field if I is a maximal ideal of R.

Therefore, $F[x]/< p(x) >$ and $F'[t]/< p'(t) >$ are both fields.

We define a map

$$\mu: F[x]/< p(x) > \to F'[t]/< p'(t) >$$

as

$$\mu(f(x)+< p(x) >) = f'(t) + < p'(t) > \ \forall \ f(x) \in F[x]$$

then μ is the desired isomorphism between $F[x]/< p(x) >$ and $F'[t]/< p'(t) >$.

Theorem 4.1.3: Let $p(x)$ be an irreducible polynomial in $F[x]$and $p'(t)$ the corresponding polynomial in $F'(t)$. Suppose u and v are the roots of $p(x)$ and $p'(t)$ in some field extensions E and E' of F and F' respectively, then there exists an isomorphism μ of $F[u]$ onto $F'[v]$ such that $\mu(\alpha) = \alpha'$ for all $\alpha \in F$ and $\mu(u) = v$.

Proof: Define $\sigma: F[x] \to F[u]$ as $\sigma\big(f(x)\big) = f(u) \ \forall \ f(x) \in F[x]$

Then σ is onto homomorphism.

Let $f(x) \in \ker \sigma$

$\Rightarrow f(u) = 0$

$\Rightarrow p(x)$ divides $f(x)$

$\Rightarrow \ker \sigma =< p(x) >$

By the Fundamental theorem of Homomorphism,

$F[x]/< p(x) > \cong F[u] = F(u)$

Since u is algebraic over F, therefore, $F[u] = F(u)$.

$$F[x]/< p(x) > \cong F(u)$$

and

$$F'[t]/< p'(t) > \cong F'(v)$$

There exist functions $\sigma_1 : F[x]/< p(x) > \to F(u)$ as $\sigma_1(f(x)+< p(x) >) = f(u)$

and

$\sigma_2 : F'[t]/< p'(t) > \to F'(v)$as $\sigma_2(f'(t) +< p'(t) >) = f'(v)$

By remark, there exists a map $\eta : F[x]/< p(x) > \to F'[t]/< p'(t) >$ as

$$\eta(f(x)+< p(x) >) = f'(t) +< p'(t) >$$

Also,

$$\sigma_1(f(x)+< p(x) >) = f(u)$$
$$\sigma_2(f'(t) +< p'(t) >) = f'(v) \ldots (1)$$

If $f(x) = x, f'(t) = t$

$$\sigma_1(x+< p(x) >) = u$$
$$\sigma_2(t+< p'(t) >) = v$$
$$\eta(x+< p(x) >) = t +< p'(t) >$$

Let $\mu = \sigma_2 \eta \sigma_1^{-1}$

If $f(x) = \alpha, f'(t) = \alpha'$

Then

$$\begin{aligned} \mu(\alpha) &= \sigma_2 \eta \sigma_1^{-1}(\alpha) \\ &= \sigma_2 \eta(\alpha+< p(x) >) \\ &= \sigma_2(\alpha' +< p'(t) >) \\ &= \alpha' \end{aligned}$$

Again,

$$\begin{aligned} \mu(u) &= \sigma_2 \eta \sigma_1^{-1}(u) \\ &= \sigma_2 \eta(x+< p(x) >) \\ &= \sigma_2(t +< p'(t) >) \\ &= v \end{aligned}$$

$\mu : F[u] \to F'(v)$ is an isomorphism such that $\mu(u) = v$ and $\mu(\alpha) = \alpha' \ \forall \ \alpha \in F$.

Note: Taking $F = F', \eta$ as identity map, $u = \alpha, v = \beta$, we get an important result . Let $F \subset K$ be two fields. If $\alpha, \beta \in K$ have same minimal polynomial p(x) over F, then there exists an isomorphism μ of $F(\alpha)$ onto $F(\beta)$ such that $\mu(\alpha) = \beta$ and $\mu(a) = a$ for all $a \in F$.

Theorem 4.1.4: Let $F \cong F'$ and let $f(x)$ be any polynomial of degree ≥ 1 over F and $f'(t)$ be the corresponding polynomial over F'. If E and E' are splitting fields of $f(x)$ and $f'(t)$ over F and F' respectively, then there exists an isomorphism ϕ of E onto E' such that $\phi(\alpha) = \alpha' \forall \ \alpha \in F$.

Proof:

Let $\deg f(x) = n$

We know that in this case $[E : F] \leq n!$, that is finite.

We apply the Principle of Mathematical Induction on $[E : F]$.

Let $[E:F] = 1$

This implies, $E = F$

That is all n roots of $f(x)$ are in F, further

$f(x) = \alpha(x - a_1)(x - a_2) \ldots \cdot (x - a_n)$ for some $0 \neq \alpha \in F$

so that $f'(t) = \alpha'(t - a_1')(t - a_2') \cdots (t - a_n')$ and $a_1', a_{2,\ldots}', a_n' \in F'$

this Implies $E' = F'$

Then Ψ can be taken as isomorphism from F onto F'.

Therefore, the result holds for $[E:F] = 1$.

Let $[E:F] > 1$.

Let result holds for all splitting fields E over any field F of degree less than $[E:F]$.

Since $[E:F] > 1$

Therefore, at least one root u of $f(x)$ is not in F.

Let $p(x)$ be the minimal polynomial of u over F then $\deg p(x) > 1$. Let $p'(t)$ be the corresponding polynomial over F'.

Then by definition of minimal polynomial, $p(x)$ is irreducible and hence $p'(t)$ is irreducible.

As $p(x)$ divides $f(x)$

This implies that there exists some $q(x) \in F[x]$ such that $f(x) = p(x)q(x)$

$\Rightarrow f'(t) = p'(t)q'(t)$

Let v be a root of $p'(t)$ in E'.

There exists an isomorphism $\theta: F[u] \to F'[v]$ in which $\theta(\alpha) = \sigma(\alpha) = \alpha' \; \forall \; \alpha \in F$ and $\theta(u) = v$.

Now, $f(x) = (x - u)f_1(x)$ and $f'(t) = (t - v)g_1(t)$ for some $f_1(x) \in F(u)[x]$ and $g_1(t) \in F'(v)[t]$

If ρ_1 denotes the isomorphism of $F(u)[x]$ onto $F'(v)[t]$ such that ρ_1 is an extension of θ and $\theta_1(x) = t$ then $f'(t) = \theta_1\big(f(x)\big) = \theta_1\big((x - u)f_1(x)\big) = (t - v)\theta_1\big(f_1(x)\big)$

This implies, $\theta_1\big(f_1(x)\big) = g_1(t)$ as $f'(t) = (t - v)g_1(t)$

Further, as E contains all the n roots of $f(x)$, E contains all $n - 1$ roots of $f_1(x)$.

If E_1 is the splitting field of $f_1(x)$ over $F[u]$ contained in E, then E_1 contains not only roots of $f_1(x)$but also u.

E_1 contains all the roots of $f(x)$ so, by definition of the splitting field, we get that $E \subseteq E_1 \Rightarrow E = E_1$.

Therefore, E is splitting field of $f_1(x)$ over $F(u)$. Similarly, E' is the splitting field of $g_1(t)$ over $F'(v)$.

Now, $[E:F] = [E:F(u)][F(u):F]$ but $[F(u):F] = \deg p(x) > 1$

$\Rightarrow [E:F(u)] < [E:F]$

Hence by the induction hypothesis, there exists an isomorphism ψ of E onto E' which extends the isomorphism.

$\theta: F(u) \to F'(v)$. However, θ extends σ, hence $\psi(\alpha) = \theta(\alpha) = \alpha' \; \forall \; \alpha \in F$.

Corollary: In particular, taking $F = F'$ and σ as identity map, we can conclude that if $f(x)$ is a polynomial of positive degree over a field F with two splitting fields E and E' then $E \cong E'$. Moreover, if $\psi: E \to E'$ is the isomorphism then $\psi(\alpha) = \alpha \; \forall \; \alpha \in F$.

Task: Find the splitting field of polynomial $f(x) = \left(x - \sqrt{2}\right)^2$ over the field of complex numbers and real numbers.

4.2 Degree of Extension of Splitting Fields

Theorem 4.2.1: Let $F \subseteq K$ be a field extension. Let $a, b \in K$ be algebraic over F of degrees m and n respectively where m and n are relatively prime positive integers. Then $F(a,b)$ is a field extension of F of degree mn.

Proof:

An element $a \in K$is algebraic over F of degree m. That is, $[F(a):F] = m$.

Similarly, $b \in K$ is algebraic over F of degree n. That is, $[F(b):F] = n$.

Let $p(x)$ and $q(x)$ be the minimal polynomial of b over F and $F(a)$ respectively.

This implies, $\deg p(x) = n, p(x) \in F[x], F \subset F(a)$

$$\Rightarrow \deg q(x) \leq \deg p(x) = n$$

$$\Rightarrow [F(a)(b):F(a)] \leq n$$

$$\Rightarrow [F(a,b):F(a)] \leq n$$

Now, $[F(a,b):F] = [F(a,b):F(a)][F(a):F] \leq nm$ ... (1)

Again, $[F(a,b):F] = [F(a,b):F(a)][F(a):F]$

$[F(a):F]$ divides $[F(a,b):F]$

$\Rightarrow m$ divides $[F(a,b):F]$

Similarly, n divides $[F(a,b):F]$.

$$\Rightarrow mn \leq [F(a,b):F] \ldots (2)$$

From (1) and (2)

$$[F(a,b):F] = mn$$

Theorem 4.2.2: An element $a \in K$ is algebraic over the field F of odd degree then $F(a) = F(a^2)$.

Proof:

$$a^2 \in F(a)$$

$$\Rightarrow F(a^2) \subset F(a) \cdots (1)$$

Let $[F(a):F] = 2n+1; n \in \mathbb{Z}$

Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{2n} x^{2n} + x^{2n+1}$ is the minimal polynomial of a over F.

Putting $x = a, p(a) = 0$ we get

$$\begin{aligned} p(a) &= \alpha_0 + \alpha_1 a + \cdots + \alpha_{2n} a^{2n} + a^{2n+1} \\ 0 &= \alpha_0 + \alpha_1 a + \cdots + \alpha_{2n} a^{2n} + a^{2n+1} \\ &= (\alpha_0 + \alpha_2 a^2 + \cdots + \alpha_{2n} a^{2n}) + (\alpha_1 a + \alpha_3 a^3 + \cdots + a^{2n+1}) \\ &= (\alpha_0 + \alpha_2 a^2 + \cdots + \alpha_{2n} a^{2n}) + a(\alpha_1 + \alpha_3 a^2 + \cdots + a^{2n}) \end{aligned}$$

Since $[F(a):F] = 2n+1$ and $\alpha_1 + \alpha_3 x^2 + \cdots + x^{2n}$ is of degree $2n$ which is less than $2n+1$.

Therefore, $\alpha_1 + \alpha_3 a^2 + \cdots + a^{2n} \neq 0$

Let $\beta = \alpha_1 + \alpha_3 a^2 + \cdots + a^{2n} \neq 0$

$$\Rightarrow \beta^{-1} \in F$$

From (1)

$$0 = (\alpha_0 + \alpha_2 a^2 + \cdots + \alpha_{2n} a^{2n}) + a\beta$$

$$0 = (\alpha_0 + \alpha_2 a^2 + \cdots + \alpha_{2n} a^{2n})\beta^{-1} + a$$

or

$$a = -(\alpha_0 + \alpha_2 a^2 + \cdots \alpha_{2n} a^{2n})\beta^{-1} \in F(a^2)$$

$$\Rightarrow F(a) \subseteq F(a^2)$$

Also, $F(a^2) \subseteq F(a)$

Therefore, $F(a) = F(a^2)$

Example 4.2.3: Let E is the splitting field of the polynomial $x^5 - 3x^3 + x^2 - 3$ over $\mathbb{Q}$. Find E and $[E: \mathbb{Q}]$.

Solution:

Let $f(x) = x^5 - 3x^3 + x^2 - 3$

Putting $f(x) = 0$

$$x^5 - 3x^3 + x^2 - 3 = 0$$

$$x^3(x^2 - 3) + 1(x^2 - 3) = 0$$

$$(x^3 + 1)(x^2 - 3) = 0$$

$$x = \frac{1 \pm \sqrt{3}i}{2}, -1, \pm\sqrt{3}$$

Let $E = \mathbb{Q}(\sqrt{3}, i)$

Then all the roots of $f(x)$ are in E.

That is E contains a splitting field of $f(x)$.

Let K is splitting field of $f(x)$. Then $K \subseteq E$.

Also, K is a field extension of $\mathbb{Q}$. K contains $\sqrt{3}$ and $\frac{1+\sqrt{3}i}{2}$, which implies that $\mathbb{Q}(\sqrt{3}, i) \subseteq K$

This implies. $K = E$

That is, E is required splitting field of $f(x)$.

Now, we find $[E: F]$

$$\sqrt{3} \notin \mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{3}): \mathbb{Q}] \geq 2$$

Also, the polynomial $x^2 - 3$ is the monic polynomial with $\sqrt{3}$ as a root.

This implies, $[\mathbb{Q}(\sqrt{3}): \mathbb{Q}] \leq 2$

That is, $[\mathbb{Q}(\sqrt{3}): \mathbb{Q}] = 2$ ... (1)

Clearly, $i \notin \mathbb{Q}(\sqrt{3})$

$$[\mathbb{Q}(\sqrt{3}, i): \mathbb{Q}(\sqrt{3})] \geq 2$$

Also, the polynomial $x^2 + 1 \in \mathbb{Q}(\sqrt{3})[x]$is a monic polynomial with i as a root.

$$[\mathbb{Q}(\sqrt{3}, i): \mathbb{Q}(\sqrt{3})] \leq 2$$

That is,

$$[\mathbb{Q}(\sqrt{3}, i): \mathbb{Q}(\sqrt{3})] = 2$$

We know that

$$[F(a, b): F] = [F(a, b): F(a)][F(a): F]$$

That is,

$$[\mathbb{Q}(\sqrt{3}, i): \mathbb{Q}] = [Q(\sqrt{3}, i): \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}): \mathbb{Q}] = 2 \times 2 = 4$$

Therefore, $[E: \mathbb{Q}] = 4$.

Example 4.2.4: Let E is the splitting field of the polynomial $x^p - 1$ over $\mathbb{Q}$, where p is a prime number. Find E and $[E: \mathbb{Q}]$.

Solution:

Let $f(x) = x^p - 1$

To find the roots of $f(x)$, put $f(x) = 0$

$$x^p - 1 = 0$$

$$\Rightarrow x^p = 1$$

$$\Rightarrow x = (1)^{1/p}$$

$$= (\cos 2n\pi + i sin\ 2n\pi)^{\frac{1}{p}}$$

$$= e^{\frac{2n\pi i}{p}}; n = 0, 1, 2, \dots, p-1$$

Let $\xi = e^{\frac{2\pi i}{p}}$

$x = 1, \xi, \xi^2, \dots, \xi^{p-1}$ are roots of $f(x)$.

Consider $E = \mathbb{Q}(\xi)$; then E is splitting field of $f(x)$.

Again, $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$

$$\Rightarrow \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 = f(x)$$

$f(x)$ has roots $\xi, \xi^2, \dots, \xi^{p-1}$ and by Eisenstein's criteria, $f(x)$is an irreducible polynomial over $\mathbb{Q}$.

Therefore, $f(x)$ is the minimal polynomial of ξ over $\mathbb{Q}$ of degree $p-1$.

So, $[\mathbb{Q}(\xi): \mathbb{Q}] = p - 1$.

Definition 4.2.5: (Algebraically Closed Fields) Let F be a field. Then F is called algebraically closed if every non-zero, non-constant polynomial has all the roots in F. For example, $x^2 + 1 \in \mathbb{R}[x]$ but its roots $i, -i \notin \mathbb{R}$ hence $\mathbb{R}$ is not algebraically closed. The field $\mathbb{C}$ is algebraically closed.

Theorem 4.2.6: Algebraically closed fields are never finite fields.

Proof: Let F be an algebraically closed field.

Suppose $F = \{a_1, a_2, \dots, a_n\}$ is finite.

Consider $f(x) = 1 + (x - a_1)(x - a_2) \cdots (x - a_n) \in F[x]$

For $1 \leq i \leq n;\ f(a_i) = 1 \neq 0$

Therefore, we arrive at a contradiction. So, F is never finite.

Example 4.2.7:$\sqrt{2} + \sqrt[3]{5}$is algebraic over $\mathbb{Q}$ of degree 6.

Solution:

Let $\alpha = \sqrt{2} + \sqrt[3]{5}$

$\Rightarrow \alpha - \sqrt{2} = \sqrt[3]{5}$

$\Rightarrow \alpha^3 - 2\sqrt{2} - 3\alpha\sqrt[3]{2} + 6\alpha = 5$

$\Rightarrow \alpha^3 + 6\alpha - 5 = \sqrt{2}(2 + 3\alpha^2)$

$\Rightarrow \alpha^6 + 36\alpha^2 + 25 + 12\alpha^4 - 60\alpha - 10\alpha^3 = 8 + 18\alpha^4 + 24\alpha^2$

$\Rightarrow \alpha^6 - 6\alpha^4 - 10\alpha^3 + 12\alpha^2 - 60\alpha + 17 = 0$

So, $f(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17 \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$

Therefore, α is algebraic over F.

Claim:$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$

$\alpha = \sqrt{2} + \sqrt[3]{5} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$

$\Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$

Again, $\alpha = \sqrt{2} + \sqrt[3]{5}$

$\alpha \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt{2} + \sqrt[3]{5} \in \mathbb{Q}(\alpha)$

$\Rightarrow 2 + \sqrt[3]{2}5 + 2\sqrt{2}\sqrt[3]{5} \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt[3]{25} + 2\sqrt{2}\sqrt[3]{5} \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt[3]{5}(\sqrt[3]{5} + 2\sqrt{2}) \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt[3]{5}(\sqrt[3]{5} + \sqrt{2} + \sqrt{2}) \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt[3]{5}(\sqrt{2} + \alpha) \in \mathbb{Q}(\alpha)$

$\Rightarrow 5(2\sqrt{2} + \alpha^3 + 6\alpha + \sqrt[3]{2}\alpha^2) \in \mathbb{Q}(\alpha)$

$\Rightarrow 2\sqrt{2} + 3\sqrt{2}\alpha^2 \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt{2}(2 + 3\alpha^2) \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt{2} \in \mathbb{Q}(\alpha)$

Also $\alpha \in \mathbb{Q}(\alpha)$

$\Rightarrow \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt[3]{5} \in \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) \subseteq \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\alpha)$

Now we find $[\mathbb{Q}(\alpha): \mathbb{Q}]$

Since $Q(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$

Consider the polynomial $x^3 - 5 \in \mathbb{Q}[x]$

This polynomial is monic over $\mathbb{Q}$, having $\sqrt[3]{5}$ as a root and by Eisenstein criteria, it is irreducible.

Therefore, it is minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$.

Hence, $[\mathbb{Q}(\sqrt[3]{5}): \mathbb{Q}] = 3$

Since $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{5})$

Therefore, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}): Q(\sqrt[3]{5})] \geq 2$

Also, $x^2 - 2$ is the monic polynomial with $\sqrt{2}$ as a root.

This implies, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}): \mathbb{Q}(\sqrt[3]{5})] \leq 2$

Therefore, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}): \mathbb{Q}(\sqrt[3]{5})] = 2$.

Hence, $[\mathbb{Q}(\alpha): \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}): \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}): \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}): \mathbb{Q}] = 2 \times 3 = 6$.

Task: Find the degree of extension of E over $F = \mathbb{Q}$ where E is the splitting field of the polynomial $(x - \sqrt{2})(x - \sqrt{3})$ over F.

4.3 Separable Polynomials

Definition 4.3.1: (Derivative of a polynomial over a field *F*) Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n \in F[x]$ be a polynomial of degree n over a field F.

That is, $\alpha_i \in F \; \forall \; 0 \leq i \leq n$

If $\deg f(x) = n \Rightarrow \alpha_n \neq 0$

$f'(x) = \alpha_1 + 2\alpha_2 x + \cdots + n\alpha_n x^{n-1}$ is derivative of $f(x)$ with respect to x.

Note: In general, if $\deg f(x) = n$, then $\deg f'(x) = n - 1$ but over a field, this is not true. Over a field, $\deg f'(x) \leq n - 1$. For example, consider the field $F = Z_7$ and $f(x) = 2x^7 + 3x^5 + 1 \in F[x]$ is a polynomial of degree 7. However, it's derivative $f'(x) = 14x^6 + 15x^4 = x^4$ in Z_7 is of degree 4. However, if the field is of characteristic 0 then $\deg f'(x) = \deg f(x) - 1$.

Rest properties are the same. That is for $f(x), g(x) \in F[x]$ and $\alpha \in F$

1) $\big(f(x) + g(x)\big)' = \big(f(x)\big)' + \big(g(x)\big)'$
2) $\big(\alpha f(x)\big)' = \alpha f'(x)$
3) $\big(f(x)g(x)\big)' = f(x)\big(g(x)\big)' + \big(f(x)\big)'g(x)$

Lemma 4.3.2: Let $f(x) \in F[x]$ be a non-constant polynomial, then an element α of a field extension K of F is multiple roots of $f(x)$ if and only if α is a common root of $f(x)$ and $f'(x)$.

Proof:

Let $\alpha \in K$ is a multiple root of $f(x)$.

Let $f(x) = (x - \alpha)^m g(x);\ m > 1, g(\alpha) \neq 0$

Differentiating both sides with respect to x, we get,

$$f'(x) = (x - \alpha)^m g'(x) + m(x - \alpha)^{m-1} g(x)$$

At $x = \alpha$,

$$f'(\alpha) = 0 + m(0)g(\alpha) = 0$$

This implies that α is a common root of $f(x)$ and $f'(x)$.

Conversely, let α is a common root of $f(x)$ and $f'(x)$.

That is, $f(\alpha) = 0$

and

$$f'(\alpha) = 0 \ldots (1)$$

Suppose α is a root of $f(x)$ with multiplicity 1.

That is, $f(x) = (x - \alpha)g(x);\ g(\alpha) \neq 0$

Differentiating both sides with respect to x, we get,

$$f'(x) = (x - \alpha)g'(x) + g(x)$$

At $x = \alpha$,

$$f'(\alpha) = 0 + g(\alpha)$$

That is,

$$f'(\alpha) = g(\alpha) \neq 0$$

α is not a root of $f'(x)$. So, we arrive at a contradiction.

Therefore, our supposition was wrong.

α is a multiple root of $f(x)$.

Theorem 4.3.3: Let $f(x)$ be an irreducible polynomial over F. Then $f(x)$ has a multiple root in some field extension if and only if $f'(x) = 0$.

Proof: Let $f(x)$ has a multiple root α in some field extension K of F. Also $f(x)$ is irreducible polynomial.

This implies $f(x)$ is the minimal polynomial of α in F.

So, if there exists any polynomial $g(x) \in F[x]$ such that $g(\alpha) = 0$ then $f(x)$ divides $g(x) \cdots (1)$

Since α is a multiple root of $f(x)$ in K.

This implies, $f'(\alpha) = 0$

By (1), $f(x)$ divides $f'(x)$

This implies, $\deg f(x) \leq \deg f'(x)$ which is not possible unless $f'(x) = 0$.

$$\Rightarrow f'(x) = 0$$

Conversely, $f(x)$ is an irreducible polynomial over F.

Let K be the splitting field of $f(x)$. Let $\alpha \in K$ be a root of $f(x) \Rightarrow f(\alpha) = 0$

Also, $f'(x) = 0 \; \forall \; x$

In particular, $f'(\alpha) = 0$

That is, α is a common root of $f(x)$ and $f'(x)$.

So, α is a multiple root of $f(x)$ in a field extension K of F.

Theorem 4.3.4: No irreducible polynomial over a field of characteristic zero has a multiple root in any field extension.

Proof: Let $f(x) \in F[x]$ is an irreducible polynomial with some multipleroot where F is a field of characteristic 0.

This implies $f'(x) = 0 \; \forall \; x$.

But we know that if $\deg f\,(x) = n$and F is a field of characteristic 0 then $\deg f'(x) = n - 1$

That is, $f'(x) \neq 0$

So, we arrive at a contradiction.

Hence, no such polynomial exists.

Example 4.3.5: The polynomial $x^2 - t$ in $F = Z_2(t)$ is irreducible over F having a multiple root in some field extension of F. Moreover,$f'(x) = 0$.

Solution:$f(x) = x^2 - t \in Z_2[t]$ is irreducible over F.

Let K be the splitting field of $f(x)$ and $f(x)$ has roots α and β.

$x^2 - t = (x - \alpha)(x - \beta)$

$\Rightarrow x^2 - t = x^2 - (\alpha + \beta)x + \alpha\beta$

$\Rightarrow 0 = -(\alpha + \beta)$

$\Rightarrow \alpha = -\beta$

Also, $\beta \in Z_2$

$\Rightarrow 2\beta = 0$

$\Rightarrow \beta + \beta = 0$

$\Rightarrow \beta = -\beta$

$\Rightarrow \alpha = \beta$

Therefore, $f(x)$ has a multiple root in K.

$f'(x) = 2x = 0$ in F.

Definition 4.3.6: (Separable and Inseparable Irreducible Polynomials) Let F be a field and $f(x) \in F[x]$ is an irreducible polynomial. Then $f(x)$ is called separable polynomial if $f(x)$ has all the roots distinct in its splitting field otherwise, it is called an inseparable polynomial**.** For example, $x^2 + 1 \in \mathbb{R}[x]$is a separable polynomial. The polynomial$x^2 + x + 1 \in \mathbb{Q}[x]$ is a separable polynomial.

Theorem 4.3.7: An irreducible polynomial $f(x)$ is separable if and only if $f'(x) \neq 0$.

Proof: The polynomial $f(x)$ is a separable irreducible polynomial

$\Leftrightarrow f(x)$ is irreducible and in any field extension of F, $f(x)$ has all roots distinct.

$\Leftrightarrow f(x)$ is an irreducible polynomial having no multiple roots.

$\Leftrightarrow f'(x) \neq 0$.

Every non-zero polynomial over a field of characteristic zero is separable. If the characteristic is non-zero then an irreducible polynomial may exist which is inseparable

Definition 4.3.8: (Separable and Inseparable Polynomials) For a general polynomial $f(x)$ is any polynomial then $f(x)$ is called separable polynomial if all its irreducible factors are separable. In case, the irreducible factors of $f(x)$ are not separable, then $f(x)$ is called inseparable polynomial over the field F.

For example, $f(x) = (x-1)^2(x^2+1) \in \mathbb{Q}[x]$ has irreducible factors $x-1, x^2+1$ and both are separable polynomials and hence $f(x)$ is separable polynomial.

A reducible separable polynomial may have multiple roots but an irreducible separable polynomial never has a multiple root.

Theorem 4.3.9: An irreducible polynomial $f(x)$ over a field F of characteristic $p>0$ is inseparable if and only if $f(x) \in F[x^p]$

Proof: Let $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ be an irreducible polynomial over the field F. Now characteristic $F \neq 0$ and $f(x)$ is inseparable.

This implies, $f'(x) = 0$

$\Rightarrow \alpha_1 + 2\alpha_2 x + 3\alpha_3 x^2 + \cdots + n\alpha_n x^{n-1} = 0$

$\Rightarrow k\alpha_k = 0 \; \forall \; k$

$\Rightarrow k = 0$ or $\alpha_k = 0$

Since characteristic $F = p$

$\Rightarrow p$ divides k or $\alpha_k = 0$

$\Rightarrow f(x) = \alpha_0 + \alpha_p x^p + \alpha_{2p} x^{2p} + \cdots + \alpha_{mp} x^{mp} \in F[x^p]$

Conversely, let $f(x) \in F[x^p]$

$\Rightarrow f(x) = \alpha_0 + \alpha_1 x^p + \alpha_2 x^{2p} + \cdots + \alpha_m x^{mp}$

$\Rightarrow f'(x) = p\alpha_1 x^{p-1} + 2p\alpha_2 x^{2p-1} + \cdots + mp\alpha_m x^{mp-1}$

Since characteristic $F = p$

$\Rightarrow px = 0 \; \forall \; x \in F$

$\Rightarrow p\alpha_i = 0 \; \forall \; i$

$\Rightarrow f'(x) = 0$

$\Rightarrow f(x)$ is inseparable polynomial.

Task: Which of the following polynomials are separable over $\mathbb{Q}$?

a) $f(x) = x^2 - 2$

b) $f(x) = (x-2)^2(x-3)$

4.4 Separable and Inseparable Extensions

Definition 4.4.1:(Separable Element) Let $F \subseteq K$ be any field extension. An algebraic element $a \in K$is called a separable element if its minimal polynomial over F is separable.

For example, $i \in \mathbb{C}$ has minimal polynomial $x^2 + 1 \in \mathbb{Q}[x]$ which is a separable polynomial and hence i is a separable element over $\mathbb{Q}$.

Definition 4.4.2: (Separable Extension) Let $F \subseteq K$ be an algebraic extension. If $\forall \; a \in K, a$ is a separable element over F then K is called a separable extension of F.

Example 4.4.3: Infinite field with finite characteristic may be inseparable.

Solution:$\boldsymbol{F = Z_2(t)}$is an infinite field with finite characteristic.

Consider $f(x) = x^2 - t \in Z_2[t]$ is an irreducible polynomial over F.

and by Example 4.3.5, $f(x)$ has a multiple root in K and hence it is inseparable.

Theorem 4.4.4: Let D be an integral domain of characteristic p, a prime number. Then (i) The mapping $\sigma: D \to D$ such that $\sigma(a) = a^p$ for $a \in D$ is a monomorphism.
(ii) For any positive integer n, the mapping $\sigma_n: D \to D$ such that $\sigma_n(a) = a^{p^n}$ for $a \in D$ is a monomorphism

Proof: Let $a, b \in D$

$$\begin{aligned}\sigma(a+b) &= (a+b)^p \\ &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + b^p\end{aligned}$$

We know that p divides $\binom{p}{r}$ $\forall\ 1 \le r \le p-1$

Since characteristic $F = p$

Therefore, $\binom{p}{r} = 0\ \forall\ 1 \le r \le p-1$

$(a+b)^p = a^p + b^p$

$\Rightarrow \sigma(a+b) = \sigma(a) + \sigma(b)$

Again,

$$\begin{aligned}\sigma(ab) &= (ab)^p \\ &= a^p b^p \\ &= \sigma(a)\sigma(b)\end{aligned}$$

Therefore, σ is a homomorphism.

Let $a \in \ker\sigma$

$\Rightarrow \sigma(a) = 0$

$\Rightarrow a^p = 0$

$\Rightarrow a = 0$

$\Rightarrow \ker\sigma = \{0\}$

Therefore, σ is one- one.

Hence, σ is a monomorphism.

(ii) $\sigma_n: D \to D$ is defined as $\sigma_n(a) = a^{p^n}\ \forall\ a \in D$

Clearly, $\sigma_n = \sigma \circ \sigma \circ \ldots \circ \sigma$

Since σ is a monomorphism.

$\Rightarrow \sigma_n$ is a monomorphism on D.

Theorem 4.4.5: If F is a finite field with characteristic p then $a \to a^p$ is an automorphism on F.

Proof: From Theorem 4.4.4, the function $\sigma(a) = a^p$ is a monomorphism.

$\Rightarrow \sigma: F \to F$ is one-one and F is finite.

We know that if S is a finite set then a function $f: S \to S$ is one-one if and only if it is onto.

Therefore, σ is onto and hence it is an automorphism.

Theorem 4.4.6: Any algebraic extension of a finite field F is a separable extension.

Proof: Let F be a finite field.

Let K be an algebraic extension of F.

Let $f(x)$ be an irreducible polynomial over F.

Suppose $f(x)$ is separable.

$\Rightarrow f(x) \in F[x^p]$

$\Rightarrow f(x) = \alpha_0 + \alpha_1 x^p + \alpha_2 x^{2p} + \cdots + \alpha_m x^{mp}$

Now, $\alpha_i \in F \; \forall \; i$

$\Rightarrow \sigma: F \to F$ as $\sigma(a) = a^p$ is an automorphism.

This implies, σ is onto.

There exist some $\beta_i \in F$ such that $\sigma(\beta_i) = \alpha_i$

That is, $\beta_i^p = \alpha_i$

$$\begin{aligned} f(x) &= \alpha_0 + \alpha_1 x^p + \cdots + \alpha_m x^{mp} \\ &= \beta_0^p + \beta_1^p x^p + \cdots \beta_m^p x^{mp} \\ &= (\beta_0 + \beta_1 x + \cdots + \beta_m x^m)^p \end{aligned}$$

This implies, $f(x) = \big(g(x)\big)^p$ where $g(x) \in F[x]$.

Thus $f(x)$ is reducible over F.

So, we arrive at a contradiction.

Therefore, $f(x)$ is separable.

So, this is a separable extension.

Task: Which of the following is separable element over $\mathbb{Q}$?

a) $i \in \mathbb{C}$

b) $\sqrt{2} \in \mathbb{R}$

c) $\pi \in \mathbb{R}$

d) $3 \in \mathbb{Q}$

Summary

- The splitting field of a polynomial of degree n over some field F is defined and explained with the help of examples.
- Isomorphism of two splitting fields of a polynomial is explained.
- Basis and degree of extension of splitting field of a polynomial over a field are defined.
- Algebraically closed fields are explained with examples.
- The degree of the minimal polynomial of an algebraic element over some field is defined.
- The concept of differentiability is related to multiple roots.
- Separable/inseparable polynomials, elements, and extensions over a field F are explained.

Keywords

- Splitting field of a polynomial
- Isomorphism of splitting fields
- Basis and degree of extension of splitting field
- Algebraically closed fields
- The minimal polynomial of an algebraic element
- Degree of the minimal polynomial
- Separable/inseparable polynomials, elements and extensions

Self-Assessment

Choose the most suitable answer from the options given with each question.

Question 1: Let $f(x)$ be a polynomial of degree n over a field F. Then the number of roots of $f(x)$ in F are

A: Exactly n

B: Maximum n

C: Minimum n

D: Maximum $n-1$

Question 2: Let $f(x) = xg(x)$ be a polynomial over a field F. Then $f(x)$ has a minimum ... number of roots in F.

A: 0

B: 1

C: 2

D: 3

Question 3: Splitting field of the polynomial $x^2 + x + 1 \in \mathbb{Q}[x]$ is

A: $\mathbb{C}$

B: $\mathbb{Q}(\sqrt{3})$

C: $\mathbb{Q}(\sqrt{3}, i)$

D: $\mathbb{Q}(\omega)$

Question 4: Let $f(x)$ be a polynomial of degree 4 over a field F and E be the splitting field of $f(x)$ over F. Then degree $[E:F]$ is maximum

A: 2

B: 4

C: 12

D: 24

Question 5: Let $f(x)$ be a polynomial of degree 1 over a field F and E is splitting field of $f(x)$ then

A: $E = F$

B: $[E:F] = 1$

C: F contains all the roots of $f(x)$

D: All the options are correct

Question 6: True/False: Every isomorphism between two fields can be extended to an isomorphism between their quotient fields

A: True

B: False

Question 7: Consider $\sqrt{5}, i \in \mathbb{C}$. Then

A: Both are algebraic over $\mathbb{R}$

B: Only $\sqrt{5}$ is algebraic over $\mathbb{R}$

C: Only i is algebraic over $\mathbb{R}$

D: Both are not algebraic over $\mathbb{R}$

Question 8: Consider $\pi i \in \mathbb{C}$, Then

A: it is algebraic over both $\mathbb{Q}$ and $\mathbb{R}$

B: it is algebraic over $\mathbb{Q}$ but not over $\mathbb{R}$

C: it is algebraic over $\mathbb{R}$ but not over $\mathbb{Q}$

D: it is algebraic neither over $\mathbb{Q}$ nor over $\mathbb{R}$

Question 9: Degree of extension of $[\mathbb{Q}(\sqrt{3}, i)]$ over $\mathbb{Q}$ is

A: 1

B: 2

C: 4

D: 8

Question 10: For any element $a \in K$ is algebraic over F then the necessary condition for $F(a) = F(a^2)$ is that minimal polynomial of a over F has degree n where n is

A: odd

B: Even

C: prime number

D: perfect square

Question 11: Splitting field of the polynomial $x^4 - 1 \in \mathbb{Q}$ is

A: $\mathbb{C}$

B: $\mathbb{Q}(\sqrt{3})$

C: $\mathbb{Q}(\sqrt{3}, i)$

D: $\mathbb{R}$

Question 12: Which of the following is an algebraically closed field?

A: $\mathbb{Z}_7$

B: $\mathbb{Q}$

C: $\mathbb{R}$

D: $\mathbb{C}$

Question 13: Statement I: Algebraically closed fields are always infinite.

Statement II: All infinite fields are algebraically closed

A: Statement I is true but II is false

B: Statement II is true but I is false

C: Statement I and II both are false

D: Statement I and II both are true

Question 14: Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{6})$ and $F = \mathbb{Q}$ be two fields. Then $[K: F]$ is

A: 2

B: 6

C: 3

D: 4

Question 15: Which of the following statements is correct?

A: $[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] = 2$

B: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}): \mathbb{Q}] = 2$

C: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}): \mathbb{Q}(\sqrt{2} + \sqrt{3})] = 2$

D: None of above

Question 16: If $\sqrt{a} + \sqrt{b} \neq 0$ where $a, b > 0, a, b \in \mathbb{Q}$ then $[\mathbb{Q}(\sqrt{a} + \sqrt{b}): \mathbb{Q}(\sqrt{a}, \sqrt{b})]$ is equal to

A: 1

B: 2

C: 4

D: 3

Question 17: Let a be a root of $f(x) \in F[x]$ such that $f'(a) = 0$. Then a is a root with multiplicity

A: 1

B: >1

C: < 2

D: ≥ 1

Question 18: Let $f(x) \in F[x]$ be a non-constant polynomial with degree n. If characteristic $F \neq 0$, then the degree of $f'(x)$ is

A: $= n$

B: $\leq n$

C: $= n - 1$

D: $\leq n - 1$

Question 19: Let $f(x) \in F[x]$ be a non-constant polynomial with degree n. If characteristic $F = 0$, then the degree of $f'(x)$ is

A: $= n$

B: $\leq n$

C: $= n - 1$

D: $\leq n - 1$

Question 20: Let $f(x) = c$ be a constant polynomial over the field of rational numbers. Then the number of roots of $f(x)$ is

A: 0

B: Infinite

C: 0 or infinite

D: Non-zero and finite

Answers for Self Assessment

1)	**B**	**2)**	**B**	**3)**	**D**	**4)**	**D**	**5)**	**D**
6)	**A**	**7)**	**A**	**8)**	**D**	**9)**	**C**	**10)**	**A**
11)	**D**	**12)**	**D**	**13)**	**A**	**14)**	**D**	**15)**	**A**
16)	**A**	**17)**	**B**	**18)**	**D**	**19)**	**C**	**20)**	**C**

Review Questions

1) Find the splitting field over $\mathbb{Q}$ for the polynomial $x^4 + 4$.

2) Let p be a prime number. Find the splitting field for $x^p - 1$ over $\mathbb{Q}$ and $\mathbb{R}$.

3) Find the splitting field for $x^3 + x + 1$ over $\mathbb{Z}_2$.

4) Find the degree of the splitting field over $\mathbb{Z}_2$ for the polynomial $(x^3 + x + 1)(x^2 + x + 1)$.

5) Find the degree $[F: \mathbb{Q}]$, where F is the splitting field of the polynomial $x^3 - 11$ over the field of rational numbers.

6) Determine the splitting field over $\mathbb{Q}$ for $x^3 + 2$.

7) Determine the splitting field over $\mathbb{Q}$ for $x^4 + x + 2$.

8) Determine the splitting field over $\mathbb{Z}_7$ for $x^6 - 1$.

9) Determine the splitting field over $\mathbb{Z}_7$ for $x^5 - 1$.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge university press

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 05: Normal Extension

CONTENTS

Objectives:

After studying this unit, you will be able to

- define normal extensions and relate normal extension with splitting fields
- define perfect field and relate it to separable extensions
- prove Lagrange's theorem for primitive elements
- prove that a prime field is isomorphic either to $\mathbb{Q}$ or some Z/pZ, where p is a prime number
- find the relation between the number of elements and characteristic of a field
- understand multiplicative groups of finite fields
- understand the relation between separable and simple extensions
- prove that finite separable field extension of a field F is a simple extension

Introduction

In this unit, an important field extension called normal extension will be studied. Some results about perfect fields and separable extensions will be done. Further, the relationship between separable, simple, and normal extensions will be discussed.

5.1 Normal Extension

Let F be a field and K be an algebraic extension of F then if for irreducible polynomial $p(x)$ over F having a root in K, $p(x)$ has all the roots in K then K is called normal extension.

K is an algebraic extension of F means $\forall\ \alpha \in K$, there exists a minimal polynomial $p(x)$ of α over F. By definition of normal extension,K is normal extension if and only if K contains a splitting field of $p(x)$.

Definition 5.1.1: (Conjugate Elements) Let $F \subseteq K$ be such that K is a field extension of F then for $\alpha, \beta \in K$, if α, β have same minimal polynomial over F then they are called conjugate elements.

$F = \mathbb{Q}, K = \mathbb{R}, \sqrt{2}, -\sqrt{2}$ have same minimal polynomial $x^2 - 2$ over F and hence they are conjugates.

Theorem 5.1.2: If K is a field extension of field F such that $[K: F] = 2$, then K is a normal extension.

Proof: Let K is a field extension of F such that $[K: F] = 2$.

Let $p(x)$ be an irreducible polynomial having one root $\alpha \in K$.

Then consider $F(\alpha)$;

$$F \subseteq F(\alpha) \subseteq K$$

This implies that $[F(\alpha): F]$ divides $[K: F]$.

But $[K: F] = 2$

This implies that $[F(\alpha): F] = 1$ or 2

$\Rightarrow \deg p(x) = 1$ or 2

In case, $\deg p(x) = 1, p(x)$ has only one root $\alpha \in K$.

In case, $\deg p(x) = 2$

$$p(x) = ax^2 + bx + c;\ a, b, c \in F, a \neq 0$$

If $p(x)$ has two roots α, β

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

$$\Rightarrow \beta = -\frac{b}{a} - \alpha = -ba^{-1} - \alpha$$

Since $b, a^{-1}, \alpha \in K$, therefore, $\beta \in K$.

In both cases, all roots of $p(x)$ are in K.

Therefore, K is a normal extension of F.

Theorem 5.1.3: Let K be a finite algebraic extension of a field F. Then K is a normal extension of the field$F$ if and only if K is the splitting field over F of some non-zero polynomial over F.

Proof: Let K be a finite algebraic extension of F.

$$K = F(a_1, a_2, \ldots, a_n)$$

Let K is a normal extension of F.

Therefore, every a_i has a minimal polynomial $f_i(x)$ over F.

Consider $f(x) = f_1(x) f_2(x) \ldots f_n(x)$

One root a_i of $f_i(x)$ is in K and K is a normal extension.

$\Rightarrow$ All roots of $f_i(x)$ are in K

$\Rightarrow$All roots of $f(x)$ are in K

That is, splitting field of $f(x) \subseteq K$

$K = F(a_1, a_2, \ldots, a_n)$ is generated by elements of F and roots of polynomial $f(x)$

$\Rightarrow K$ is contained in splitting field of $f(x)$.

Conversely, let K be a splitting field of some polynomial $f(x)$ over F.

Let $a_1, a_2, \ldots, a_n$ be the roots of $f(x)$ in K then $K = F(a_1, a_2, \ldots, a_n)$.

Let $p(x)$be an irreducible polynomial over F having a root $\beta \in K$.

$$p(x) \in F[x] \subseteq K[x]$$

Let L be the splitting field of $p(x)$ over K.

Claim: $\boldsymbol{K = L}$

Clearly, $K \subseteq L$

Let β' is a root of $p(x)$ such that $\beta' \notin K$

By choice of β'; $\beta' \in L$

β and β' being roots of the same minimal polynomial are conjugates.

There exists some $F-$ isomorphism $\sigma: F(\beta) \to F(\beta')$ such that $\sigma(\beta) = \beta'$ and $\sigma(\alpha) = \alpha \; \forall \; \alpha \in F$

Now $F \subseteq F(\beta) \subseteq K$ i.e., K is splitting field of $f(x)$ over $F(\beta)$.

Further $K(\beta') = F(a_1, a_2, \dots, a_n, \beta') = F(\beta')(a_1, a_2, \dots, a_n)$

$\Rightarrow K(\beta')$ is the splitting field of $f(x)$ over $F(\beta')$.

Therefore, there exists an isomorphism τ of K onto $K(\beta')$ such that $\sigma(x) = \tau(x) \; \forall \; x \in F(\beta)$.

Since σ is $F-$isomorphism, therefore, τ is $F-$ isomorphism.

Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n; \; \alpha_n \neq 0, \alpha_i \in F \; \forall \; i$

Since $a_1, a_2, \dots, a_n$ are roots of $f(x)$.

Therefore, $f(x) = \alpha_n (x - a_1)(x - a_2) \cdots (x - a_n) \cdots (1)$

Then τ can be extended to τ', the isomorphism of $K[x]$ onto $K(\beta')[x]$.

Now,

$$\tau'\big(f(x)\big) = \tau'(\alpha_0) + \tau'(\alpha_1)x + \cdots + \tau'(\alpha_n)x^n$$

$= \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$

Since $\tau'(\alpha_i) = \tau(\alpha_i) = \sigma(\alpha_i) = \alpha_i \; \forall \; i$

This gives, $\tau'\big(f(x)\big) = f(x)$

Also, $\tau'\big(f(x)\big) = \alpha_n \big(x - \tau(a_1)\big)\big(x - \tau(a_2)\big) \cdots \big(x - \tau(a_n)\big)$

Hence $f(x) = \alpha_n \big(x - \tau(a_1)\big)\big(x - \tau(a_2)\big) \dots \big(x - \tau(a_n)\big) \dots (2)$

From (1) and (2) we get that

$\{\tau(a_1), \tau(a_2), \dots, \tau(a_n)\} = \{a_1, a_2, \dots, a_n\}$

That is, $F(a_1, a_2, \dots, a_n) = F\big(\tau(a_1), \tau(a_2), \dots, \tau(a_n)\big)$

However,

$K(\beta') = \tau(K) = \tau\big(F(a_1, a_2, \dots, a_n)\big)$

$= F\big(\tau(a_1), \tau(a_2), \dots, \tau(a_n)\big)$

$= F(a_1, a_2, \dots, a_n) = K$

This implies, $\beta' \in K$

So, we arrive at a contradiction i.e., $p(x)$ splits completely over K

$\Rightarrow K$ is a normal extension of F.

Theorem 5.1.4: Let K be a finite normal extension of F. If E is any subfield of K containing F then K is also a normal extension of E.

Proof: K is a finite normal extension of F.

So, there exists some polynomial $f(x) \in F[x]$ such that K is splitting field of $f(x)$.

Now, $F \subseteq E \subseteq K$

$\Rightarrow f(x) \in F[x] \subset E[x]$ i.e., K is splitting field of $f(x)$ over E.

$\Rightarrow K$ is a normal extension of E.

Theorem 5.1.5: Let K be a finite normal extension of a field F. If $\alpha_1, \alpha_2 \in K$ are conjugates over F then there exists an $F-$ isomorphism σ on K such that $\sigma(\alpha_1) = \alpha_2$.

Proof: K is a finite normal extension of F.

Since $\alpha_1, \alpha_2 \in K$ are conjugates over F.

This implies, there exists an $F-$ isomorphism $\tau: F(\alpha_1) \to F(\alpha_2)$ such that $\tau(\alpha_1) = \alpha_2, \tau(\alpha) = \alpha \; \forall \; \alpha \in F$.

Also, $F \subseteq F(\alpha_1), F \subseteq F(\alpha_2)$

Since α_1 and α_2 are having the same minimal polynomial over F.

Let $p(x)$ be that minimal polynomial.

$$p(x) \in F[x] \subseteq F(\alpha)[x] \subseteq F(\beta)[x]$$

In that case, τ can be extended to an $F-$ isomorphism σ on K such that $\tau(\alpha_1) = \sigma(\alpha_1) = \alpha_2$

Theorem 5.1.6: Let $F \subseteq K \subseteq L$ such that K is a finite normal extension of F and L is a finite normal extension of K. Then L need not be a normal extension of F.

Proof: Let $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt[4]{2})$

Then $x^2 - 2$ is minimal polynomial of $\sqrt{2}$ over F; $[K:F] = 2$

$\Rightarrow K$ is a normal extension over F.

Similarly, $x^2 - \sqrt{2}$ is minimal polynomial of $\sqrt[4]{2}$ over K.

$$[L:K] = 2$$

So, $L$is a normal extension of K.

Again $F = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2})$

The minimal polynomial of $\sqrt[4]{2}$ over F is $f(x) = x^4 - 2$. Only roots of $f(x)$ that belong to L are $\sqrt[4]{2}$ and $-\sqrt[4]{2}$. The other two roots are $\sqrt[4]{2}i, -\sqrt[4]{2}i \notin L$. Hence L is not a normal extension over F.

Task:

1) Find a normal extension of $\mathbb{R}$ with the degree of extension 2.

2) Give an example of a normal extension $F \subseteq K$ such that $[K:F] > 2$.

5.2 Perfect Fields

Definition 5.2.1:(Perfect Field) Let F be a field. Then F is called a perfect field if every finite extension of F is separable.

Recall that $F \subseteq K$ is a finite extension if $[K:F]$ is finite. It is called a separable extension if $\forall \; a \in K, a$ is a separable element over F.

Theorem 5.2.2: Any algebraic field extension of a perfect field is a separable extension.

Proof: Let $F \subseteq K$ be an algebraic field extension.

Let F be a perfect field.

Let $a \in K$; a is algebraic element over F.

$\Rightarrow [F(a):F]$ is finite.

$\Rightarrow a$ is separable over F.

$\Rightarrow K$ is a separable extension.

Theorem 5.2.3: Let F be a field of characteristic $p \neq 0$, and K be a field extension of F. Then an element $a \in K$ algebraic over F is separable over F if and only if $F(a^p) = F(a)$

Proof: Let $a \in K$ be an algebraic element over F such that it is separable over F.

Since a is separable over F, this implies, minimal polynomial $f(x)$ of a over F is separable.

Let $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} + x^n$ be the minimal polynomial of a over F so that $[F(a):F] = n$.

Consider $g(x) = \alpha_0^p + \alpha_1^p x + \cdots + \alpha_{n-1}^p x^{n-1} + x^n$

$\Rightarrow g(x^p) = \alpha_0^p + \alpha_1^p x^p + \cdots + x^{np}$.

Since characteristic $F = p$

$\Rightarrow g(x^p) = (\alpha_0 + \alpha_1 x + \cdots + x^n)^p = \big(f(x)\big)^p$

Claim:$g(x)$ is minimal polynomial of a^p over F

Clearly, $g(x)$ is monic polynomial

$g(x^p) = \big(f(x)\big)^p$

So that $g(a^p) = \big(f(a)\big)^p = 0$

$\Rightarrow a^p$ is a root of $g(x)$

Let there exists $h(x) \in F[x]$ such that $h(x)$ divides $g(x)$

$\Rightarrow h(x^p)$ divides $g(x^p)$

Consider $g(x^p) = \big(f(x)\big)^p$

$\Rightarrow h(x^p)$ divides $\big(f(x)\big)^p$

$\Rightarrow h(x^p) = \big(f(x)\big)^k; 0 \le k \le p$

Differentiating both sides with respect to x, we get

$h'(x^p)px^{p-1} = k\big(f(x)\big)^{k-1} f'(x)$

Since $h(x^p) \in F[x^p] \Rightarrow h(x^p)$ is inseparable $\Rightarrow h'(x^p) = 0$

$\Rightarrow k\big(f(x)\big)^{k-1} f'(x) = 0$

$\Rightarrow k = 0$ or $k = p$

If $k = 0, h(x^p) = \big(f(x)\big)^0 = 1$

If $k = p, h(x^p) = \big(f(x)\big)^p = g(x^p)$

$\Rightarrow h(x) = g(x)$

So, $h(x)$ divides $g(x)$ in $F[x] \Rightarrow h(x) = 1$ or $g(x)$.

$\Rightarrow g(x)$ is irreducible polynomial.

$\Rightarrow g(x)$ is the minimal polynomial of a^p over F

$\Rightarrow [F(a^p):F] = \deg g(x) = n = [F(a):F]$

$a^p \in F(a) \Rightarrow F(a^p) \subseteq F(a)$

$\Rightarrow F(a^p) = F(a)$

Conversely, let $F(a^p) = F(a)$

Let a is not separable over F

This implies that the minimal polynomial $f(x)$ of a over F is not separable

$\Rightarrow f(x) \in F[x^p]$

$\Rightarrow f(x) = g(x^p)$

$\Rightarrow \deg f(x) = \deg g(x^p)$

Let $\deg f(x) = n$ and $\deg g(x) = m$

$m = n/p$

Since $p > 1 \Rightarrow m < n$ ... (1)

Also, $f(x) = g(x^p)$

Since $f(a) = 0 \Rightarrow g(a^p) = 0$

That is, $g(x)$ has a root a^p.

This implies, the minimal polynomial of a^p divides $g(x)$.

$\Rightarrow [F(a^p):F] \leq m$

$\Rightarrow [F(a):F] = [F(a):F(a^p)][F(a^p):F]$

$\Rightarrow n \leq m$ which is a contradiction to (1)

This implies, a is separable over F.

Theorem 5.2.4: Let F be a field of characteristic $p \neq 0$, and K be a field extension of F. If $a \in K$ is separable over F, then $F(a)$ is a separable field extension of F.

Proof: Let $b \in F(a)$

As a is algebraic over $F \Rightarrow [F(a):F]$ is finite.

Let $[F(b):F] = m$,

$[F(a):F(b)] = n$,

$[F(a):F(b^p)] = q$,

and $[F(b^p):F] = s$

then

$$\begin{aligned} nm &= [F(a):F(b)][F(b):F] \\ &= [F(a):F] \\ &= [F(a):F(b^p)][F(b^p):F] \\ &= qs \end{aligned}$$

Again, $b^p \in F(b)$

$\Rightarrow F(b^p) \subseteq F(b)$

Therefore, $F(b^p)$ is a subfield of $F(b)$.

$\Rightarrow [F(b^p):F] \leq [F(b):F]$

$\Rightarrow s \leq m$

But $nm = qs \Rightarrow n \leq q$

Let $f(x) = \alpha_0 + \alpha_1 x + \cdots + x^n$ be the minimal polynomial of a over $F(b)$.

As $\{1, b, b^2, \ldots, b^{m-1}\}$ is a basis of $F(b)$ over F;

For each $0 \leq i \leq n-1$,

$\alpha_i = \lambda_{i,0} + \lambda_{i,1} b + \cdots + \lambda_{i,m-1} b^{m-1}$ with $\lambda_{i,j} \in F \; \forall \; 0 \leq j \leq m-1$

Further, $f(x)$ is minimal polynomial of a over $F(b) \Rightarrow f(a) = 0$.

$\Rightarrow a^p$ is a root of $g(x)$ where $g(x) = \alpha_0^p + \alpha_1^p x + \cdots + x^n$

For each i, $0 \leq i \leq n-1$,

$$\begin{aligned} \alpha_i^p &= \left(\lambda_{i,0} + \lambda_{i,1} b + \cdots + \lambda_{i,m-1} b^{m-1}\right)^p \\ &= \lambda_{i,0}^p + \lambda_{i,1}^p b^p + \cdots + \lambda_{i,m-1}^p b^{(m-1)p} \\ &\in F(b^p) \end{aligned}$$

Since each $\alpha_i^p \in F(b^p)$

$\Rightarrow g(x) \in F(b^p)[x]$ and $g(a^p) = 0$

$\Rightarrow [F(b^p)(a^p):F(b^p)] \leq n$

But a is separable over F

$\Rightarrow F(a^p) = F(a)$

So, $[F(a):F(b^p)] \leq n$

$\Rightarrow q \leq n$

This implies, $q = n$

$\Rightarrow [F(a):F(b^p)] = [F(a):F(b)]$

$\Rightarrow F(b^p) = F(b)$

$\Rightarrow b$ is separable over F.

This implies that every element of $F(a)$ is separable over F.

$\Rightarrow F(a)$ is a separable extension of F.

Definition 5.2.5: (Primitive Element and Simple Extension): Let $K = F(a)$ be an extension of F generated by elements of F and singleton set $\{a\}$. Then K is called a simple extension of F and a is called primitive element over the field F.

The extension $\mathbb{Q}(\sqrt{2})$ is a simple extension of Q and $\sqrt{2}$ is a primitive element.

Theorem 5.2.6: (Lagrange's Theorem of Primitive Elements): Let F be an infinite field and E be some field extension of F. Let $a, b \in E$ be algebraic over F such that they are separable over F. Then there exists c in K such that $f(c) = F(a, b)$ and $c = a + \alpha b$ for some $\alpha \in F$.

Proof: Let $f(x)$ and $g(x)$ be minimal polynomials over F of a and b respectively.

Let deg $f(x) = m$ and deg $g(x) = n$.

Let K be the splitting field of $f(x)g(x)$ over E.

Then $a, b \in K$

Clearly, K contains a splitting field of $f(x)$ and one of $g(x)$.

Since a and b are separable over F.

$\Rightarrow f(x)$ has m distinct roots $a = a_1, a_2, \ldots, a_m$ in K and $g(x)$ has n distinct roots $b = b_1, b_{2,\ldots}, b_n$ in K.

For $2 \leq i \leq m, 2 \leq j \leq n$

Define

$$\lambda_{ij} = \frac{a_i - a}{b - b_j} \in K$$

λ_{ij} are finite in number but K is infinite. Therefore, we can choose $\alpha(\neq 0) \in F$ such that $\alpha \neq \lambda_{ij} \forall\, i, j \geq 2$.

Then $\alpha(b - b_j) \neq a_i - a \;\forall\, i, j \geq 2$

That is, $a_i + \alpha b_j \neq a + \alpha b$

Now put $c = a + \alpha b \in F(a, b)$

Therefore, $F(c) \subseteq F(a, b)$

Since $c \in F(c)$

and $f(x) \in F[x] \subseteq K[x]$

$\Rightarrow h(x) = f(c - \alpha x) \in K[x]$

Further deg $h(x) =$ deg $f(x) = m$

Now $h(b) = f(c - \alpha b) = f(a) = 0$

Suppose for some $j \geq 2, h(b_j) = 0$

$\Rightarrow f(c - \alpha b_j) = 0$

$\Rightarrow c - \alpha b_j = a_i$ for some i

Since only roots of $f(x)$ are$a = a_1, a_2, \ldots, a_m$

If $i = 1, a_i = a_1 = a$

$$\Rightarrow c = a + \alpha b_j$$

$$= a + \alpha b$$

$$\Rightarrow b = b_j$$

But $j \geq 2$ and $b \neq b_j$ for $j \geq 2$

This is not possible.

So, $i \geq 2, \alpha b + a = \alpha b_j + a_i$ which is again not possible.

Hence, $h(b_j) \neq 0$

For $j \geq 2, x - b_j$ does not divide $h(x)$.

Now $x - b$ is a factor of $h(x)$ over K.

As b is a root of $g(x)$ in K.

$x - b$ is a common factor of $h(x)$ and $g(x)$.

Claim: $\boldsymbol{x - b = HCF(h(x), g(x))}$

As $g(x)$ has no multiple roots, therefore, $(x - b)^2$ does not divide $g(x)$.

Since $g(x) = (x - b)(x - b_2)(x - b_3) \ldots (x - b_n)$

and each $x - b_j$ does not divide $h(x)$ for $j \geq 2$.

Therefore, $x - b = HCF(h(x), g(x))$.

Now, $h(x) \in F(c)[x]$ as $c \in F(c), \alpha \in F$

Also, $g(x) \in F(c)[x]$

Let $g_1(x)$ be the minimal polynomial of b over $F(c)$. Then $g_1(x)$ divides $g(x)$ and $h(x)$ both over the field $F(c)$ and hence over K.

So, $g_1(x)$ divides $x - b$ over K.

Since deg $g_1(x) > 0$ and $g_1(x)$ is monic, therefore, $x - b = g_1(x) \in F(c)[x]$

$\Rightarrow b \in F(c)$

$\Rightarrow a = c - \alpha b \in F(c)$

$\Rightarrow F(a, b) \subseteq F(c)$

$\Rightarrow F(c) = F(a, b)$.

Task:

Find a primitive element in the following fields over $\mathbb{Q}$

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
b) $\mathbb{Q}(\omega, \sqrt{2})$

5.3 Finite Fields

Theorem 5.3.1: Any prime field is either isomorphic to the field of rational numbers or to the field of integers modulo some prime number.

Proof: Let F be a prime field and e is the identity of F.

Let $f: \mathbb{Z} \to F$ as $f(n) = ne \; \forall \, n \in \mathbb{Z}$

Ker f is a subgroup of $\mathbb{Z}$. Also, Ker f is an ideal of $\mathbb{Z}$.

$\mathbb{Z}$ is a principal ideal domain.

Let ker $f =< q >; q \in \mathbb{Z}$

Case I:$q = 0$

Ker $f =< 0 >$

$\Rightarrow$ ker $f = \{0\}$

$\Rightarrow f$ is monomorphism from $\mathbb{Z} \to F$

or, f is an isomorphism from $\mathbb{Z} \to f(\mathbb{Z})$; where $f(\mathbb{Z}) \subseteq F$.

$\Rightarrow \mathbb{Z} \cong f(\mathbb{Z})$

Let $\mathbb{Q}'$ be the field of quotient of $f(\mathbb{Z})$

This implies, $\mathbb{Q}' = F$

Field of quotients of $\mathbb{Z} \cong \mathbb{Q}'$

That is, $\mathbb{Q} \cong \mathbb{Q}' = F$

$\Rightarrow F \cong \mathbb{Q}$

Case II: $q \neq 0$

Ker $f =< q >$

Assume that $q = rs$; $1 < r, s < q$

Then $f(q) = f(rs)$

That is, $0 = (rs)e$

$\Rightarrow (re)(se) = 0$

$\Rightarrow re = 0$ or $se = 0$

$\Rightarrow r \in$ ker $f =< q >$or $s \in$ ker $f =< q >$

$\Rightarrow q$ divides either r or s

$\Rightarrow q \leq r$ or $q \leq s$

We arrive at a contradiction. Hence our supposition was wrong. That is, q is a prime number.

Also, by the fundamental theorem of homomorphism,

$$\mathbb{Z}/_{< q >} \cong f(\mathbb{Z})$$

Since q is a prime element of a principal ideal domain $\mathbb{Z}$

This implies, $< q >$ is an irreducible ideal.

$\Rightarrow \mathbb{Z}/< q >$ is a field.

$\Rightarrow f(\mathbb{Z})$ is a field contained in F but F is a prime field.

$$F = f(\mathbb{Z}) \cong \mathbb{Z}/_{< q >}$$

Theorem 5.3.2: Let F be a field with q elements. Then characteristic $F = p$ where p is a prime number and $q = p^n$.

Proof: Let F be a field having $q$elements. Then e,$2e$,$3e$, ..., $(q + 1)e$ are not all distinct.

Otherwise, let $ke = le$; $1 \leq k, l \leq q$

$\Rightarrow (k - l)e = 0$

There exist some finite number p such that p is the smallest positive integer for which $pe = 0$.

Characteristic $F = p, p$ is a prime number.

Let P be the prime field of F.

$P \cong Z/< p >$ having p elements. Thus, P has p elements.

Therefore, $[F:P]$ is finite.

Let $[F:P] = n$

Let $\{\alpha_1, \alpha_{2,\dots}, \alpha_n\}$ is a basis of F over P.

$\Rightarrow \forall\ a \in F, a = \lambda_1\alpha_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n;\ \lambda_i \in P$

For each λ_i, we have p choices. This implies, a has p^n choices.

$\Rightarrow O(F) = p^n$

Theorem 5.3.3: Let F be a finite field with q elements, then F is the splitting field of $x^q - x$ over its prime subfield.

Proof:$O(F) = q$

Let $0 \neq a \in F$, we know that $F - \{0\}$ is a multiplicative group of order $q - 1$.

Therefore, $O(a)$ divides $O(G)$.

$\Rightarrow a^{q-1} = e$

$\Rightarrow a^q = a\ \forall\ 0 \neq a \in F$

If $a = 0, 0^q = 0$

Therefore, $\forall a \in F, a^q = a$

That is, a is a root of $x^q - x$.

F is contained in the splitting field of $x^q - x$.

Let P be the prime field then we know that $x^q - x$ has at most q roots in any field extension.

Thus, F contains all the roots of $x^q - x$.

This implies, F is the splitting field of $x^q - x$.

Theorem 5.3.4: (E. H. Moore) For every prime number p and $n \in \mathbb{N}$, there exist a field having p^n elements.

Proof: Consider $f(x) = x^{p^n} - x$.

Then $f(x) \in \mathbb{Z}_p[x]$

Let K be the splitting field of $f(x)$ over $\mathbb{Z}_p$.

Claim: K is a field having p^n elements.

Now, $f'(x) = p^n x^{p^n - 1} - 1 = -1 \neq 0$.

Therefore, $f(x)$ is separable polynomial.

$\Rightarrow f(x)$ has no multiple roots in K.

Thus, there are p^ndistinct roots of $f(x)$ in K.

Let L be the set of all roots of $f(x)$ in K.

$\Rightarrow L \subseteq K$ and L has p^n elements.

Clearly, $0,1 \in L$

Consider $a, b \in L$

$$\Rightarrow a^{p^n} = a, b^{p^n} = b$$

Therefore, there exists $\eta: K \to K$ such that $\eta(c) = c^{p^n}\ \forall\ c \in K$, is a monomorphism.

$\eta(a - b) = \eta(a) - \eta(b)$

$\Rightarrow (a - b)^{p^n} = a^{p^n} - b^{p^n} = a - b$

$\Rightarrow a - b \in L$

Suppose $b \neq 0$

Then

$$\eta(ab^{-1}) = \eta(a)\big(\eta(b)\big)^{-1}$$
$$= a^{p^n}\big(b^{p^n}\big)^{-1}$$
$$= ab^{-1}$$

$\Rightarrow ab^{-1} \in L$

$\Rightarrow L$ is a subfield of K.

Also, L contains all the roots of $f(x)$.

$\Rightarrow L$ is splitting field of $f(x)$.

$\Rightarrow L = K; K$ contains p^n elements.

Task:

Prove that the order of a finite field is never divisible by two distinct prime numbers.

Prove that a field with infinite characteristic is always isomorphic to the field of rational numbers.

5.4 Multiplicative Group of Finite Fields

Theorem 5.4.1: Finite fields having the same number of elements are isomorphic.

Proof: Let K_1 and K_2 be two finite fields such that $O(K_1) = q = O(K_2)$.

Then by Theorem 5.3.2, $q = p^n$ for some prime number p and thus $O(K_1) = p^n = O(K_2)$.

Let P_1 and P_2 be the prime subfields of K_1 and K_2 respectively.

Then

$$P_1 \cong \mathbb{Z}/< p >$$

and

$$P_2 \cong \mathbb{Z}/< p >$$

This implies, $P_1 \cong P_2$

Now by Theorem 5.3.3, K_1 is the splitting field of $x^q - x$ over P_1 and K_2 is the splitting field of $y^q - y$ over P_2.

Hence these are splitting fields of the same polynomial. Therefore, $K_1 \cong K_2$.

Theorem 5.4.2:A field is finite if and only if its multiplicative group is cyclic.

Proof: Let F be a finite field. Let $O(F) = q$.

Consider$F - \{0\}$; $O(F - \{0\}) = q - 1$.

Let $S = \{n |\ 0(a) = n, a \in F - \{0\}\}$

Then S has some maximum element say n, n is called exponent of $F - \{0\}$.

That is, $n = 0(a)$ for some $a \in F - \{0\} = G$.

This implies, $0(a)$ divides $O(G)$.

$\Rightarrow n$ divides $q - 1$.

$$\Rightarrow n \leq q - 1$$

Also, $x^n - x$ has at the most n roots in any field extension of F.

$\Rightarrow q - 1 \leq n$

$\Rightarrow n = q - 1$

$\Rightarrow 0(a) = q - 1 = 0(G)$

$\Rightarrow G =< a >$ is cyclic.

Conversely,let $G = F - \{0\}, G =< a >$ for some $a \in G$ be a cyclic group.

Case I: If $a = 1$

Then $G =< 1 >= \{1\}$

$\Rightarrow O(G) = 1$ and hence $O(F) = 2$

Hence, F is finite.

Case II: If $a \neq 1$

Subcase I: If characteristic $F = \mathbf{0}$

For $0 \neq a \in G$

$1, -1 \in G =< a >$

There exist some $n \in \mathbb{Z}$ such that $-1 = a^n$

$\Rightarrow 1 = a^{2n}$

$\Rightarrow o(a) \leq 2n$ and hence $0(G) \leq 2n$

So, $O(G)$ is finite this implies, $O(F)$ is finite but a field with characteristic 0 is never finite. This case is not possible.

Subcase II: Characteristic $F = p; p$ is a prime number.

The prime field P of F being isomorphic to $\mathbb{Z}_p$ has p elements.

Since $a \neq 1$

$\Rightarrow a - 1 \neq 0$

$\Rightarrow a - 1 \in G =< a >$

$\Rightarrow a - 1 = a^n; n \in \mathbb{Z}$

Thus, a satisfies $x^n - x + 1 \in F[x]$

$\Rightarrow a$ is algebraic over P.

Therefore, $[P(a): P] = r$ for some $r \in \mathbb{N}$.

As P has p elements, therefore, $P(a)$ has p^r elements.

Now $0 \in P(a)$ and every non-zero element of F, being the power of a also belong to $P(a)$.

$\Rightarrow F \subseteq P(a)$

But $P(a) \subseteq F$

$\Rightarrow F = P(a)$ and F is finite.

Theorem 5.4.3: Let two elements a, b in a field extension K of a field F be separable over F. Then $F(a, b)$ is a simple, separable extension of F.

Proof: If F is finite then $F(a, b)$ is also finite.

$F(a, b) = \{\alpha + \beta a + \gamma b | \alpha, \beta, \gamma \in F\}$.

$\Rightarrow F(a, b) - \{0\}$ is cyclic.

There exists c such that $F(a, b) - \{0\} =< c >$

$\Rightarrow F(a, b) = F(c)$; a simple extension.

If F is infinite then $F(a, b) = F(c);\ c = a + \lambda b; \lambda \in F$ that is, a simple extension.

If characteristic $F = 0$

$\Rightarrow F(a, b)$ is a separable extension.

If characteristic $F = p, p$ is a prime number.

Let $[F(c): F] = m$

Basis of $F(c)$ over F is $\{1, c, c^2, \ldots, c^{m-1}\}$.

Let $a, b \in F(c)$

Then

$$a = \alpha_0 + \alpha_1 c + \cdots + \alpha_{m-1} c^{m-1}$$

and

$$b = \beta_0 + \beta_1 c + \cdots + \beta_{m-1} c^{m-1}$$

$\alpha_i, \beta_i \in F \; \forall \; i$

Since characteristic $F = p$

So that,

$$\begin{aligned} a^p &= (\alpha_0 + \alpha_1 c + \cdots + \alpha_{m-1} c^{m-1})^p \\ &= \alpha_0^p + \alpha_1^p c^p + \cdots + \alpha_{m-1}^p c^{(m-1)p} \\ &\in F(c^p) \end{aligned}$$

Similarly, $b^p \in F(c^p)$

Since a, b are separable over F

So, $F(a^p) = F(a)$ and $F(b^p) = F(b)$

$F(a) = F(a^p) \subseteq F(c^p)$

$F(b) \subseteq F(c^p)$

That is, $F(a, b) \subseteq F(c^p)$ or $F(c) \subseteq F(c^p)$

Also, $c^p \in F(c)$

$\Rightarrow F(c^p) \subseteq F(c)$

$\Rightarrow F(c^p) = F(c)$

$\Rightarrow c$ is separable over F.

$F(a, b) = F(c)$ is a separable extension over F.

Task:

Prove that for any prime p, Z_p is a field whose multiplicative group is cyclic with $p - 1$ generators.

5.5 Steinitz Theorem

Theorem 5.5.1: Let K be a field extension of a field F. Then the set $L = \{a \in K | a$ is separable over $F\}$ is a subfield of K containing F.

Proof: Let $c \in F$

Then $x - c$ is a polynomial over F such that it is a minimal polynomial of c over F.

Therefore, the minimal polynomial of c over F is separable.

$\forall c \in F, c \in L \Rightarrow F \subseteq L$

$0, 1 \in L$

$\Rightarrow L \neq \phi$

For $a, b \in L$

a and b are separable elements over F.

Hence, $F(a, b)$ is separable extension of F.

$a, b \in L$ and $F(a, b)$ is a field.

$\Rightarrow a - b \in F(a, b)$ and $ab^{-1} \in F(a, b); b \neq 0$

$\Rightarrow a - b, ab^{-1}$ are both separable over F.

$\Rightarrow a - b, ab^{-1} \in L$

$\Rightarrow L$ is a subfield of K.

Theorem 5.5.2: Any finite separable field extension of a field F is a simple extension.

Proof: Let F be a field and $K = F(a_1, a_2, \ldots, a_n)$ be a finite separable extension of F.

For $n = 2$, $K = F(a_1, a_2)$be a finite separable extension of F then there exists $c \in K$ such that $K = F(c)$

That is K is a simple extension.

Let us assume that if $K = F(a_1, a_2, \ldots, a_{n-1})$ is finite separable extension then $\exists\, c \in K$ such that $K = F(c)$.

Now let

$$K_1 = F(a_1, a_2, \ldots, a_n)$$

Then

$$\begin{aligned} K_1 &= F(a_1, a_2, \ldots, a_n) \\ &= K(a_n) \\ &= F(c, a_n) \\ &= F(d);\ d \in K_1 \end{aligned}$$

That is, K_1 is a simple extension. So, by Principle of Mathematical Induction, IfK is a finite separable extension of a field F then K is simple.

Theorem 5.5.3:(Steinitz Theorem) If K is a finite extension of F then K is a simple extension of F if and only if there are only a finite number of subfields of K containing F.

Proof: Suppose K is a finite extension of F such that K is a simple extension.

So, there exist $c \in K$ such that $K = F(c)$

Let $f(x) \in F[x]$ such that $f(x)$ is minimal polynomial of c over F.

Now $F \subseteq K$ and let L be a subfield of K containing F.

Again, $F \subseteq L \subseteq K$

So, $f(x) \in F[x] \subseteq L[x]$

$c \in K$, let $g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{m-1}x^{m-1} + x^m$be the minimal polynomial of c over L.

Since $f(x) \in L[x]$ such that $f(c) = 0$

This implies, $g(x)$ divides $f(x)$ in $L[x]$ and hence in $K[x]$.

Now, let $L_0 = F(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$

Then $F \subseteq L$

Also, $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in L$

$$\Rightarrow L_0 \subseteq L$$

and $g(x)$ is an irreducible polynomial over L such that $g(c) = 0$

$\Rightarrow g(x)$ is an irreducible polynomial over L_0 such that $g(c) = 0$.

$\Rightarrow g(x)$ is minimal polynomial of c over L_0.

Again $K = F(c) \subseteq L(c); K \subseteq L(c)$

Also, $L \subseteq K, c \in K \Rightarrow L(c) \subseteq K$

$\Rightarrow K = L(c)$

Similarly, $K = L_0(c)$ and $\deg g(x) = m$

$\Rightarrow [K: L] = m = [K: L_0]$

$\Rightarrow L = L_0 = F(\alpha_0, \alpha_1, \dots, \alpha_{m-1})$

Therefore, any subfield of K containing F is $F(\beta_0, \beta_1, \dots, \beta_{m-1})$ such that the polynomial $\beta_0 + \beta_1 x + \cdots + \beta_{m-1}x^{m-1} + x^m$ divides $f(x)$ and monic polynomial dividing $f(x)$ will be finite in number.

$\Rightarrow$The number of subfields of K containing F is finite.

Conversely, let the number of subfields of K containing F is finite.

Case I:If F is finite

Then K is also a finite field.

$\Rightarrow K - \{0\}$ is a cyclic group.

So, there exists $c \in K - \{0\}$ such that $K - \{0\} = < c >$ or $K = F(c)$ i.e., a simple extension.

Case II: If F is infinite

For some $a \in K$,

Consider $F(a)$ is a subfield of Kcontaining F.

We can choose $b \in K$ such that $[F(b): F] = n$ and $[F(a): F] \leq n \; \forall \; a \in K$.

Claim: $K = F(b)$

If possible, let $K \neq F(b)$

There exist $c \in K$ such that $c \notin F(b)$

By the hypothesis of the set of fields $F(cd + b); d \in F$ is finite.

As F is infinite, therefore, there exist $r, s \in F$ such that $F(cr + b) = F(cs + b)$

Let $z = cr + b$

$\Rightarrow F(z) = F(cs + b)$

$\Rightarrow cr + b, cs + b \in F(z)$

Consider $c(r - s) = (cr + b) - (cs + b) \in F(z)$

$r \neq s \Rightarrow c \in F(z)$

Further $b = (cr + b) - cr \; \in F(z)$

$\Rightarrow F(b) \subseteq F(z)$

But $c \in F(z), c \notin F(b)$

$\Rightarrow F(b) \neq F(z)$

$\Rightarrow [F(z): F(b)] > 1$

But $[F(z): F] = [F(z): F(b)][F(b): F] > 1 \cdot n = n$

So, we arrive at a contradiction to the choice of n.

Therefore, $K = F(b); b \in K$ is a simple extension.

Summary

- Normal extensions and relation of normal extension with splitting fields are discussed
- The perfect field is defined and related to the separable extensions
- Lagrange's theorem for primitive elements is proved
- It is proved that a prime field is isomorphic either to $\mathbb{Q}$ or some Z/pZ, where p is a prime number
- The number of elements and characteristic of a field are related

- Multiplicative groups of finite fields are studied

Keywords

- Normal extension
- Perfect Fields
- Lagrange's theorem
- Finite fields
- Separable extension
- Simple extension

Self-assessment

Question 1: Let $f(x)$ be an irreducible polynomial of degree n over the field F having a root in the normal extension K of F, then

A: K contains only one root of $f(x)$

B: K contains at the most n roots of $f(x)$

C: K contains $n-1$ roots of $f(x)$

D: K contains all the n roots of $f(x)$

Question 2: Let K is an algebraic normal extension of F. Let $\alpha \in K$ and $p(x)$ is minimal polynomial of α over F. Then

A: K is the splitting field of $p(x)$

B: K contains a splitting field of $p(x)$

C: K is contained in some splitting field of $p(x)$

D: $K = F$

Question 3: Let $\mathbb{R} \subseteq \mathbb{C}$ be the field. Then conjugate element(s) of $i \in \mathbb{C}$ over $\mathbb{R}$ are

A: i

B: $i, -i, 1, -1$

C: $i, -i$

D: $-i$

Question 4: Let $\mathbb{R} \subseteq \mathbb{C}$ be the field. Then conjugate element(s) of $\omega = \frac{1+\sqrt{3}i}{2} \in \mathbb{C}$ over $\mathbb{R}$ are

A: ω

B: $\omega, \omega^2, 1$

C: ω, ω^2

D: $\omega^2, 1$

Question 5: Let K be a field extension of F such that $[K:F] = 2$. Then K is

A: Always a normal extension of F

B: Never a normal extension of F

C: May or may not be a normal extension of F

D: Never a simple extension of F

Question 6: Let F be a field. Then F is called a perfect field if

A: Every extension of F is separable

B: Every finite extension of F is separable

C: There exists some finite separable extension of F

D: Every infinite extension of F is separable

Question 7: Let K is a finite simple extension of a field F then the number of subfields of K containing F are

A: One

B: Two

C: Finite

D: Infinite

Question 8: Let $F = Z_3$ and K be a field extension of F. Then an element $a \in K$ is separable over F if and only if

A: $F(a^3) = F(a)$

B: $F(a^2) = F(a)$

C: $F(a^6) = F(a)$

D: $F(a^2) = F(a^3)$

Question 9: Let $F = Z_7$ and K is a field extension of F. Then for a separable element a over F, $F(a)$ is

A: Simple but not separable extension

B: Neither simple nor separable

C: Separable but not simple

D: Simple as well as separable

Question 10: The primitive root of the field $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ over $\mathbb{Q}$ is

A: $\sqrt{2}\mathrm{i}$

B: $\sqrt{2} + \mathrm{i}$

C: $-\sqrt{2}\mathrm{i}$

D: $\sqrt{2}$

Question 11: The field of quotients of $\mathbb{Z}$ is

A: $\mathbb{Z}$

B: $\mathbb{Q}$

C: $\mathbb{R}$

D: $\mathbb{C}$

Question 12: A prime field is isomorphic to $\mathbb{Z}/\langle q \rangle$ then q is

A: A prime number

B: A prime number or 0

C: A composite number

D: A composite number or 0

Question 13: Which of the following is not an order of a finite field?

A: 125

B: 49

C: 1331

D: 46

Question 14: Let F be a field of characteristic 5. Then the number of elements in F are

A: 5

B: 25

C: $5^n; n \in \mathbb{N}$

D: 120

Question 15: Let F be a field with 125 elements. F is splitting field of the polynomial $x^q - x$ over its prime subfield then $q =$

A: 1

B: 5

C: 25

D: 125

Question 16: Let F_1 and F_2 are two fields with the same number of elements. Then

A: $F_1 = F_2$

B: F_1 is a proper field extension of F_2

C: F_2 is a proper field extension of F_1

D: $F_1 \cong F_2$

Question 17: Let F be a field with 49 elements. Then its multiplicative group is

A: Not abelian

B: Abelian but not cyclic

C: Cyclic

D: Infinite group

Question 18: Multiplicative group of a field F is cyclic then

A: F is finite

B: F is infinite

C: $F \cong \mathbb{Q}$

D: $Ch.F = 0$

Question 19: For two elements a, b in a field extension K of a field F be separable over F. Then $F(a, b)$ is

A: Simple but not separable

B: Separable but not simple

C: Simple and separable

D: Neither simple nor separable

Question 20: The set of all separable elements of a field K over F is

A: A subfield of F

B: A subfield of K containing F

C: A field extension of K

D: Not a field

Answers for Self Assessment

1.	D	2.	B	3.	C	4.	C	5.	A
6.	B	7.	C	8.	B	9.	D	10.	B
11.	B	12.	B	13.	D	14.	C	15.	D
16.	D	17.	C	18.	A	19.	C	20	B

Review Questions

1) Prove or disprove: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is a normal extension.
2) Let K be any algebraic field extension of F. If F_1 and $F_2$are two non-empty subfields of K containing F, such that each F_i is a normal extension of F. Show that $F_1 \cap F_2$ is a normal extension of F.
3) Find a primitive element in the following fields over $\mathbb{Q}$
   a) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$
   b) $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$
4) Prove that any field which is either of characteristic zero or is finite is a perfect field.
5) Let $a, b \in K$, an extension of F, be algebraic over F. If one of a or b is separable over F, prove that $F(a, b)$ is a simple extension of F.

Further Readings

- Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
- Topics in algebra by I.N. Hartstein, Wiley
- Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 06: Introduction to Galois Theory

CONTENTS

Objectives

After studying this unit, you will be able to

- understand monomorphisms of some field E to some field K
- define fixed field and F- automorphisms
- prove that $\sigma(a)$ is conjugate of a over F for every F-automorphism σ
- analyze results about fixed fields with the help of examples
- state and prove Artin's theorem and understand some consequences of Artin's theorem
- define Galois extension and elaborate it with example
- relate normal and Galois extensions

Introduction

This unit provides a basic theory of Galois groups and extensions. In this unit, we will study monomorphisms between the fields. Fixed fields and F-automorphisms will be studied. It will be followed by Artin's theorem which relates fixed fields and degree of extension. Further Galois field will be defined and related to normal extensions.

6.1 Automorphism Groups

Linear Dependence/ Independence of Monomorphism: Let E be any set and K be any field. Let $S(E,K)$ be the set of all the mappings from E to K. Then $S(E,K)$is a vector space over K under the compositions

$$(\phi_1+\phi_2)(x)=\phi_1(x)+\phi_2(x)$$

$$(\alpha\phi_1)(x)=\alpha\phi_1(x);\ x\in E,\alpha\in K$$

Let $\phi_1,\phi_2,\dots,\phi_n\in S(E,K)$ then we call $\phi_1,\phi_2,\dots,\phi_n$ linearly independent if

$\alpha_1\phi_1+\alpha_2\phi_2+\cdots+\alpha_n\phi_n=\bar{0}$ where $\bar{0}$is the zero-map defined as $\bar{O}(x)=0\ \forall\ x\in E$

For $x\in E$,

$$(\alpha_1\phi_1+\alpha_2\phi_2+\cdots+\alpha_n\phi_n)(x)=0$$

$$\Rightarrow \alpha_1\phi_1(x)+\alpha_2\phi_2(x)+\cdots+\alpha_n\phi_n(x)=0$$

$$\Rightarrow \alpha_i=0\ \forall\ 1\le i\le n$$

Theorem 6.1.1: Let E and K be any two fields. If $\sigma_1, \sigma_2, \dots, \sigma_n$ are any n distinct monomorphisms of E into K, then they are linearly independent over K.

Proof: Let $S = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is the set of n distinct monomorphisms from E to K.

For $n = 1, S = \{\sigma_1\}, \sigma_1$ is monomorphism

If for some $\alpha \in K, \alpha\sigma_1 = \bar{0}$

$\Rightarrow \alpha\sigma_1(x) = 0 \; \forall \; x \in E$

$\Rightarrow \alpha(\sigma_1(x)) = 0 \; \forall \; x \in E$

$\Rightarrow \alpha = 0$

$\Rightarrow S$ is linearly independent in this case.

Let the result is true for S consisting of $n-1$ monomorphisms.

For n, let $\alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_n\sigma_n = \bar{O}; \; \alpha_i \in K \; \forall \; i$

$$\Rightarrow (\alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_n\sigma_n)(x) = 0 \; \forall \; x \in E$$

If $\alpha_n = 0 \; \Rightarrow \alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_{n-1}\sigma_{n-1} = \bar{0}$

By the induction hypothesis, $\{\sigma_1, \sigma_2, \dots, \sigma_{n-1}\}$ is linearly independent.

$$\Rightarrow \alpha_i = 0 \; \forall \; 1 \leq i \leq n-1$$

Also, $\alpha_n = 0$

$\Rightarrow \alpha_i = 0 \; \forall \; 1 \leq i \leq n$

If $\alpha_n \neq 0$

Then $\alpha_n^{-1} \in K$

$\Rightarrow \alpha_n^{-1}(\alpha, \sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_n\sigma_n) = \bar{O}$

$\Rightarrow \alpha_n^{-1}\alpha_1\sigma_1 + \alpha_n^{-1}\alpha_2\sigma_2 + \cdots + \sigma_n = \bar{O}$

$\Rightarrow \beta_1\sigma_1 + \beta_2\sigma_2 + \cdots + \sigma_n = \bar{O} \dots (1) \; ; \beta_i = \alpha_n^{-1}\alpha_i \; \forall \; 1 \leq i \leq n-1.$

$\sigma_1 \neq \sigma_n$

$\sigma_1(x) \neq \sigma_n(x_1)$ for at least one $x_1 \in E$

From (1)

$\beta_1\sigma_1(x_1x) + \beta_2\sigma_2(x_1x) + \cdots + \sigma_n(x_1x) = 0$

$\Rightarrow \beta_1\sigma_1(x_1)\sigma_1(x) + \beta_2\sigma_2(x_1)\sigma_2(x) + \cdots + \sigma_n(x_1)\sigma_n(x) = 0$

$$\Rightarrow \beta_1 \frac{\sigma_1(x_1)}{\sigma_n(x_1)}\sigma_1(x) + \beta_2 \frac{\sigma_2(x_1)}{\sigma_n(x_1)}\sigma_2(x) + \cdots + \beta_{n-1} \frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}\sigma_{n-1}(x) + \sigma_n(x) = 0 \dots (2)$$

From (1)

$\beta_1\sigma_1 + \beta_2\sigma_2 + \cdots + \beta_{n-1}\sigma_{n-1} + \sigma_n = 0$

$\Rightarrow (\beta_1\sigma_1 + \beta_2\sigma_2 + \cdots + \beta_{n-1}\sigma_{n-1} + \sigma_n)(x) = 0$

$\Rightarrow \beta_1\sigma_1(x) + \beta_2\sigma_2(x) + \cdots + \beta_{n-1}\sigma_{n-1}(x) + \sigma_n(x) = 0 \dots (3)$

From (2)

$$\sum_{i=1}^{n-1} \beta_i \frac{\sigma_i(x_1)}{\sigma_n(x_1)}\sigma_i(x) + \sigma_n(x) = 0$$

From (3)

$$\sum_{i=1}^{n-1} \beta_i\sigma_i(x) + \sigma_n(x) = 0$$

$(3) - (2)$

$$\sum_{i=1}^{n-1} \beta_i \left(\frac{\sigma_i(x_1)}{\sigma_n(x_1)} - 1 \right) \sigma_i(x) = 0$$

which is a linear combination of $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$.

By the induction hypothesis,

$$\beta_i\left(\frac{\sigma_i(x_1)}{\sigma_n(x_1)} - 1\right) = 0 \dots (4)$$

Consider, $i = 1$,

$$\beta_i\left(\frac{\sigma_i(x_1)}{\sigma_n(x_1)} - 1\right) \neq 0$$

Because $\sigma_1(x_1) \neq \sigma_n(x_1)$

Also, $\beta_1 \neq 0$

So, we arrive at a contradiction.

Our supposition was wrong.

Therefore, $\alpha_n = 0$

This implies $\alpha_i = 0 \; \forall \; 1 \leq i \leq n$

$\Rightarrow \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is always linearly independent.

Theorem 6.1.2: Any set of automorphism of K is linearly independent over K.

Proof:E and K are two fields.

Consider $S = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ such that $\sigma_i: E \to K$ is a monomorphism then this set is always linearly independent.

Let $E = K$ and consider the set of automorphisms on E then this set being subset of the set of monomorphisms is a linearly independent set.

Theorem 6.1.3: The set of all automorphisms of a field form a group under the resultant composition.

Proof: Let K be a field.

Let S be the set of all automorphisms on K.

Let $\sigma_1, \sigma_2 \in S$

$\Rightarrow \sigma_1$and σ_2 both are one-one, onto, homomorphism from K to itself.

$\Rightarrow \sigma_1 \circ \sigma_2$ is again one-one, onto, homomorphism from K to itself.

Define $\eta: K \to K$ as $\eta(y) = x \Leftrightarrow \sigma(x) = y$

Again, for $x_1, x_2 \in K$,

$\sigma(x_1 + x_2) = \sigma(x_1) + \sigma(x_2)$

$\Rightarrow \sigma(x_1 + x_2) = y_1 + y_2$

$\Rightarrow \eta(y_1 + y_2) = x_1 + x_2 = \eta(y_1) + \eta(y_2)$

$\Rightarrow \eta \in S$ and $\eta = \sigma^{-1}$

Therefore, σ^{-1} exists for all $\sigma \in S$

So, S is a group under the resultant composition.

:By taking different examples observe that set of all automorphisms on a field K is not a group under the composition of

a) Sum of automorphisms
b) Product of automorphisms
c) Subtraction of automorphisms

6.2 Fixed Field

Definition 6.2.1: Let K be a field extension of a field F. Let σ be any automorphism on K. Then σ is called $F-$automorphism if $\sigma(a) = a \; \forall \; a \in F$.

For example, let $\sigma = I: K \to K$ be identity map then $\sigma(x) = x \; \forall \; x \in K$.

Since $F \subseteq K, \sigma(x) = x \; \forall \; x \in F$

Therefore, I map is $F-$automorphism.

Theorem 6.2.2: Set of all $F-$automorphisms of K is a subgroup of the group of all automorphisms on K.

Proof: Let S be the set of all $F-$automorphisms of K over F then I is an $F-$automorphism.

This implies, $S \neq \phi$

Let $\sigma_1, \sigma_2 \in S$

$$\sigma_1(x) = x \; \forall \; x \in F$$

and

$$\sigma_2(x) = x \; \forall \; x \in F$$

$$\Rightarrow \sigma_2^{-1}(x) = x \; \forall \; x \in F$$

Now consider $x \in F$

$$\sigma_1\sigma_2^{-1}(x) = \sigma_1(x) = x$$

Therefore, $\sigma_1\sigma_2^{-1} \in S$

That is, S is a subgroup of $Aut(K)$ or G.

Definition 6.2.3:(Galois Group) Let K be a field extension of a field F. Then $S = \{\sigma | \sigma \in Aut(k); \; \sigma(x) = x \; \forall \; x \in F\}$ is a subgroup of $Aut(K)$ and hence S is itself a group under the composition of composite maps. The group S is known as the Galois group. We denote it as $G(K, F)$.

Theorem 6.2.4: Let Kbe any field extension of F and $a \in K$ be algebraic over F. Then for every $F-$ automorphism σ of $K, \sigma(a)$ is conjugate to a over F.

Proof: Since $a \in K$ is algebraic over F.

Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n-1}x^{n-1} + x^n$ is the minimal polynomial of a over F.

Put $x = a, p(a) = 0$

$\Rightarrow \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1}a^{n-1} + a^n = 0$

$\Rightarrow \sigma(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1}a^{n-1} + a^n) = 0$

$\Rightarrow \sigma(\alpha_0) + \sigma(\alpha_1)\sigma(a) + \sigma(\alpha_2)\sigma(a^2) + \cdots + \sigma(\alpha_{n-1})\sigma(a^{n-1}) + \sigma(a^n) = 0$

Now σ is $F-$homomorphism.

$\alpha_i \in F \; \forall \; 0 \leq i \leq n-1$

$\sigma(\alpha_i) = \alpha_i \; \forall \; 0 \leq i \leq n-1$

$$\sigma(a^k) = \big(\sigma(a)\big)^k$$

$\Rightarrow \alpha_0 + a_1\sigma(a) + \cdots + \alpha_{n-1}\big(\sigma(a)\big)^{n-1} + \big(\sigma(a)\big)^n = 0$

which proves that $\sigma(a)$ is a root of the minimal polynomial of a.

Therefore, a and $\sigma(a)$ are having the same minimal polynomial.

$\Rightarrow a$ and $\sigma(a)$ are conjugates over F.

Theorem 6.2.5: Let K be a finitely generated field extension of F such that $\{a_1, a_2, \ldots, a_n\}$ be the set of generators of K over F i.e., $K = F(a_1, a_2, \ldots, a_n)$ then any $F-$ automorphism σ on K is determined by $\{\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)\}$.

Proof: $K = F(a_1, a_2, \ldots, a_n)$.

For $a \in K$,

$a = \alpha_0 + \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n; \alpha_i \in F \; \forall \; i$

Then

$$\begin{aligned}\sigma(a) &= \sigma(\alpha_0 + \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n)\\ &= \sigma(\alpha_0) + \sigma(\alpha_1)\sigma(a_1) + \sigma(\alpha_2)\sigma(a_2) + \cdots + \sigma(\alpha_n)\sigma(a_n)\end{aligned}$$

$\alpha_i \in F\ \forall\ i$ and σ is F −automorphism

$\Rightarrow \sigma(\alpha_i) = \alpha_i\ \forall\ i$

Then

$\sigma(a) = \alpha_0 + \alpha_1\sigma(a_1) + \alpha_2\sigma(a_2) + \cdots + \alpha_n\sigma(a_n)$

Thus, any $F-$ automorphism σ on K is determined by $\{\sigma(a_1),\ \sigma(a_2), \ldots,\ \sigma(a_n)\}$.

Theorem 6.2.6: Let Gbe a group of automorphisms of a field K. Then the set $F_o = \{x \in K | \sigma(x) = x\ \forall\ \sigma \in G\}$ is a subfield of K.

Proof: Since G is a group of automorphisms of a field K.

$\forall\ \sigma \in G,$

$\sigma(0) = 0, \sigma(1) = 1$

$\Rightarrow 0,1 \in F_0$

$\Rightarrow F_0 \neq \emptyset$

Let $x, y \in F_0$

$\Rightarrow \sigma(x) = x\ \forall\ \sigma \in G$ and $\sigma(y) = y\ \forall\ \sigma \in G$

Also, $\sigma(x - y) = \sigma(x) - \sigma(y) = x - y$

$\Rightarrow x - y \in F_0\ \forall\ x, y \in F_0$

Again $x \in F_0, 0 \neq y \in F_0$

$0 \neq y \in K\ \Rightarrow y^{-1} \in K$

$\sigma(y^{-1}) = \big(\sigma(y)\big)^{-1} = y^{-1}$

$\Rightarrow y^{-1} \in F_0$

Consider $\sigma(xy^{-1}) = \sigma(x)\sigma(y^{-1}) = xy^{-1}$

$\Rightarrow xy^{-1} \in F_0$

$\Rightarrow F_0$ is a field contained in K.

1) Prime field is contained in F_0.

Proof: Prime field is the smallest subfield contained in K.

Prime field P is the intersection of all subfields of K.

F_0 is a subfield of K.

$$P \subseteq F_0 = \{x \in K | \sigma(x) = x\ \forall\ \sigma \in G\}$$

$$\Rightarrow \forall\ \sigma \in G, x \in P, \sigma(x) = x$$

2) Every member of Gcan be regarded as F_0 −automorphism on G.

Let $\sigma \in G$

$$F_0 = \{x \in K | \sigma(x) = x\ \forall\ \sigma \in G\}$$

For $\sigma \in G, x \in F_0$

$\sigma(x) = x$

Therefore, σ can be treated as F_0 −automorphism on G.

Theorem 6.2.7: If K is a field extension of a field F and G is a group of F −automorphisms of K then $F \subseteq F_0$.

Proof: G is a group of $F-$ automorphisms of K.

This implies every automorphism σ is $F-$automorphism.

$\Rightarrow \sigma(x) = x \; \forall \; x \in F, \sigma \in G$

$\Rightarrow x \in F_0 \; \forall \; x \in F$

$\Rightarrow F \subseteq F_0$

6.2.8: $K = Q(\sqrt{2})$then $Aut(K)$ consists of two automorphisms and its fixed field is $\mathbb{Q}$.

Solution: Let $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt{2})$

Let σ be any $F-$automorphism

$B = \{1, \sqrt{2}\}$ is a basis of K over F.

$\sigma(x) = x \; \forall \; x \in F$

For $x \in K, x = \alpha_1 + \sqrt{2}\alpha_2; \alpha_1, \alpha_2 \in F$

Then

$$\begin{aligned} \sigma(x) &= \sigma(\alpha_1) + \sigma(\sqrt{2})\sigma(\alpha_2) \\ &= \alpha_1 + \sigma(\sqrt{2})\alpha_2 \end{aligned}$$

Now $\sigma(\sqrt{2})$ is a conjugate of $\sqrt{2}$

$$\Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$$

Case I: $\boldsymbol{\sigma(\sqrt{2}) = \sqrt{2}}$

$\sigma(x) = \alpha_1 + \sqrt{2}\alpha_2 = x$

$\Rightarrow \sigma = I$

Case II: $\boldsymbol{\sigma(\sqrt{2}) = -\sqrt{2}}$

$\sigma(x) = \alpha_1 - \sqrt{2}\alpha_2$

So, we get two isomorphisms $\{I, \sigma\}$; $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$

$F_0 = \{x \in k | \sigma(x) = x \; \forall \; x \in F\}$

Let $a + b\sqrt{2} \in F_0$

Then

$$I(a + b\sqrt{2}) = a + b\sqrt{2}$$

and

$\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$

$\Rightarrow a - b\sqrt{2} = a + b\sqrt{2}$

$\Rightarrow b = 0$

Therefore, $F_0 = \{a | a \in \mathbb{Q}\} = \mathbb{Q}$.

1) Let $K = Q(\sqrt{5})$then find the order of group $Aut(K)$ and its fixed field.

2) Let $K = Q(\sqrt{3}i)$then find the order of group $Aut(K)$ and its fixed field.

6.3 Artin Theorem

Theorem 6.3.1: (Artin) Let G be a finite group of automorphisms of a field K; F_0 the fixed field under G. Then the degree of K over F_0 is equal to the order of the group G.

Proof: $G = Aut(K)$ and $F_0 = \{x \in K | \sigma(x) = x \; \forall \; x \in G\}$

Let $[K : F_0] = m$ and $0(G) = n$

Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$

Let $B = \{x_1, x_2, \dots, x_m\}$ is a basis of K over F_0.

Let $m < n$

Consider m linear homogeneous equations in n unknowns given by

$$\sigma_1(x_j)u_1 + \sigma_2(x_j)u_2 + \cdots + \sigma_n(x_j)u_n = 0 \dots (1)$$

Since $m < n$ that is, the system of equations has at least one non-trivial solution. Let $\{y_1, y_2, \dots, y_n\}$ is that solution.

$$\sigma_1(x_j)y_1 + \sigma_2(x_j)y_2 + \cdots + \sigma_n(x_j)y_n = 0 \dots (2)$$

Now, $\forall\, x \in K$

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m; \alpha_i \in F_0$$

In (2), multiply jth equation by α_j

$$\alpha_j\sigma_1(x_j)y_1 + \alpha_j\sigma_2(x_j)y_2 + \cdots + \alpha_j\sigma_n(x_j)y_n = 0$$

Since $\sigma_j(\alpha_i) = \alpha_i\ \forall\ i, j$

Therefore,

$$\sigma_1(\alpha_j x_j)y_1 + \sigma_2(\alpha_j x_j)y_2 + \cdots + \sigma_n(\alpha_j x_j)y_n = 0$$

Adding these equations, we get,

$$\sigma_1(x)y_1 + \sigma_2(x)y_2 + \cdots + \sigma_n(x)y_n = 0$$

$$\Rightarrow y_1\sigma_1 + y_2\sigma_2 + \cdots + y_n\sigma_n = \bar{0}$$

Since $\sigma_1, \sigma_2, \dots, \sigma_n \in Aut(K)$ therefore, $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$is always linearly independent.

$$\Rightarrow y_i = 0\ \forall\ i$$

But $\{y_1, y_2, \dots, y_n\}$is a system of non-trivial solution. This implies, $y_i \neq 0$ for some i.

Thus, we arrive at a contradiction.

So, m is not less than n.

$\Rightarrow m \geq n$

Assume that $m > n$

$\Rightarrow m \geq n + 1$

Since a subset of a linearly independent set is linearly independent.

Hence, $\{x_1, x_2, \dots, x_{n+1}\}$ is a linearly independent subset of K over F_0.

Consider $n + 1$ equations in m unknowns,

$\sigma_j(x_1)u_1 + \sigma_j(x_2)u_2 + \cdots + \sigma_j(x_m)u_m = 0 \dots (3)$

Let $(z_1, z_2, \dots, z_m)$ be that non-trivial solution such that r is the minimum number of non-zero components in $(z_1, z_2, \dots, z_m)$.

Rearranging we can take

$z_i = 0\ \forall\ i > r$

From (3) we have,

$$\sigma_j(x_1)z_1 + \sigma_j(x_2)z_2 + \cdots + \sigma_j(x_r)z_r = 0 \dots (4)$$

$z_r \neq 0$; z_r^{-1} exists.

$$\sigma_j(x_1)\frac{z_1}{z_r} + \sigma_j(x_2)\frac{z_2}{z_r} + \cdots + \sigma_j(x_r)\frac{z_r}{z_r} = 0$$

Put

$$\frac{z_i}{z_r} = z_i'$$

$$\sigma_j(x_1)z_1' + \sigma_j(x_2)z_2' + \cdots + \sigma_j(x_{r-1})z'_{r-1} + \sigma_j(x_r) = 0 \dots (5)$$

If $r = 1$, from (5) we get,

$$\sigma_j(x_r) = 0$$

which is not possible. Hence, $r \neq 1$.

Also, if $z_1', z_2', \ldots, z_{r-1}' \in F_0$

Since $\sigma(\alpha) = \alpha \; \forall \; \alpha \in G$

Therefore, $\sigma(z_i') = z_i' \; \forall \; \sigma \in G$

From (5), $\sigma_j(x_1)z_1' + \sigma_j(x_2)z_2' + \cdots + \sigma_j(x_r) = 0$

Taking $\sigma_j = I$

$$x_1z_1' + x_2z_2' + \cdots + x_rz_r' = 0$$

If $z_i' \in F_0$

$\{x_1, x_2, \ldots, x_r\}$ being a subset of B is linearly independent.

$\Rightarrow z_1', z_2', \ldots, z_r'$ may not all belong to F_0.

That is, there exist i such that $z_i' \notin F_0$

Without loss of generality, we may take $i = 1$

$$\Rightarrow z_1' \in F_0$$

$\sigma_i(z_1') \neq z_1'$ for some $\sigma_i \in G$

Apply σ_i to (5), we get,

$$\sigma_i\big(\sigma_j(x_1)z_1'\big) + \sigma_i\big(\sigma_j(x_2)z_2'\big) + \cdots + \sigma_i\big(\sigma_j(x_{r-1})z_{r-1}'\big) + \sigma_i\left(\sigma_j(x_r)\right) = 0 \ldots (6)$$

Also, $\sigma_i G = G$ and $\sigma_i\sigma_j = \sigma_j$.

$$\sigma_j(x_1)z_1' + \sigma_j(x_2)z_2' + \cdots + \sigma_j(x_{r-1})z_{r-1}' + \sigma_j(x_r) = 0 \ldots (7)$$

Subtracting (7) from (6)

$$\sigma_j(x_1)\big(z'_1 - \sigma_i(z_1')\big) + \sigma_j(x_2)\big(z'_2 - \sigma_i(z_2')\big) + \cdots + \sigma_j(x_{r-1})\big(z'_{r-1} - \sigma_i(z_{r-1}')\big) = 0$$

Put $t_k = z_k' - \sigma_i(z_k') \; \forall \; 1 \leq k \leq r$

$$\sigma_j(x_1)(t_1) + \sigma_j(x_2)(t_2) + \cdots + \sigma_j(x_m)t_m = 0$$

by allowing $t_i = 0 \; \forall \; i \geq r$

$$\sigma_i(z_1') \neq z_1'$$

$$\Rightarrow t_1 \neq 0$$

$\{t_1, t_2, \ldots, t_m\}$ is a non-trivial solution of (3) having $r - 1$ non-zero entries.

So, we arrive at a contradiction.

Our supposition was wrong.

$$\Rightarrow m = n$$

That is, $O(G) = [K : F_0]$.

Note: In the first part of the proof, $[K : F_0] \geq O(G)$ without using that $O(G)$ is finite.

This implies that if $[K : F_0] = m$ is finite then $O(G)$ is the number of automorphisms on K is also finite.

Note: $F \subseteq F_0$

$$\Rightarrow [K : F] \leq [K : F_0] = O(G)$$

6.4 Introduction to Galois Theory

Definition 6.4.1: A finite extension K of a field F is called Galois extension if F is fixed subfield of K under the group $G(K, F)$.

Theorem 6.4.2: Let $K = F(\alpha)$ be a simple finite separable extension of F. Then K is the splitting field of the minimal polynomial of α over F if and only if F is the fixed field under the group of all F −automorphisms of K.

Proof: Let $f(x)$ be the minimal polynomial of α over F. Let $\deg f(x) = m$.

Therefore, $[K:F] = m$

Let $\alpha = \alpha_1, \alpha_{2,\dots}, \alpha_r$ be the distinct conjugates of α.

α_i is a root of $f(x)\ \forall\ 1 \le i \le r$

$\Rightarrow K = F(\alpha_i)$

There exist an F −automorphism σ_i on K such that $\sigma_i(\alpha_1) = \alpha_i$

Since α_1 is a generator of a field extension. That is, it is uniquely determined. Therefore, σ_i is uniquely determined.

Again, for any F −automorphism σ of $K, \sigma(\alpha_1) = \alpha_i$ for some i.

Therefore, $\sigma = \sigma_i$

Hence $G(K,F)$ consists of $\sigma_1, \sigma_2, \dots, \sigma_r$.

That is, $o\big(G(K,F)\big) = r$

$\Rightarrow [K:F_0] = r$

$F = F_0$

$\Leftrightarrow [K:F] = [K:F_0]$

$\Leftrightarrow\ m = r$

Hence F is a fixed field under G if and only if $f(x)$ has all m roots in K that is, if and only if K is splitting field of $f(x)$ over F.

Let $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, where p is any prime number. Find the group of all automorphisms of splitting field of $f(x)$.

Solution:

$$\begin{aligned} f(x) &= \frac{x^p - 1}{x - 1} \\ f(x+1) &= \frac{(x+1)^p - 1}{x + 1 - 1} \\ &= \frac{(x+1)^p - 1}{x} \\ &= \frac{(\binom{p}{0} + \binom{p}{1}x + \binom{p}{2}x^2 + \cdots + \binom{p}{p-1}x^{p-1} + \binom{p}{p}x^p) - 1}{x} \\ &= \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p-1}x^{p-2} + x^{p-1} \end{aligned}$$

Since p divides $\binom{p}{r}\ \forall\ 1 \le r \le p-1$

p divides all the coefficients of this polynomial except the leading coefficient.

Also, p^2 does not divide $\binom{p}{1} = p$

By Eisenstein criteria, $f(x+1)$ is an irreducible polynomial over $\mathbb{Q}$.

Hence, $f(x)$ is an irreducible polynomial over $\mathbb{Q}$.

$$\begin{aligned} f(x) &= x^{p-1} + x^{p-2} + \cdots + x + 1 \\ &= \frac{x^p - 1}{x - 1} \end{aligned}$$

That is, $x^p - 1 = (x-1)f(x)$

Therefore, roots of $f(x)$ are roots of $x^p - 1$ except 1 but roots of $x^p - 1$ are n −th roots of unity.

Except 1, all the roots of $x^p - 1$ are given by $\xi, \xi^2, \ldots, \xi^{p-1}$ where $\xi = e^{\frac{2\pi i}{p}}$

Therefore, $K = \mathbb{Q}(\xi)$ is the splitting field of $f(x)$.

Thus, the fixed field of group G of all $\mathbb{Q}$ −automorphisms of K is $\mathbb{Q}$.

$\Rightarrow \mathbb{Q}$ is a fixed field under the group of all automorphisms of K.

$\Rightarrow K$ is Galois extension of $\mathbb{Q}$.

 Let $f(x) = (x^2+3)(x^3-2)$. Find the group of all automorphisms of splitting field of $f(x)$.

Solution: $f(x) = (x^2+3)(x^3-2)$

Roots of $f(x)$ are $\pm\sqrt{3}i, \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2;\ \omega = \frac{-1\pm\sqrt{3}i}{2}$

Note. that $K = \mathbb{Q}\left(\sqrt{3}i, \sqrt[3]{2}\right)$ contains all the roots of $f(x)$.

Also, if L is splitting field of $f(x)$ then $K \subseteq L$ hence, K is splitting field of $f(x)$.

By Eisenstein criteria, $x^3 - 2$ is an irreducible polynomial over $\mathbb{Q}$.

Also, it is monic with $\sqrt[3]{2}$ as a root.

Hence, it is minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

$$\Rightarrow \left[\mathbb{Q}\left(\sqrt[3]{2}\right): \mathbb{Q}\right] = 3.$$

Since $\sqrt{3}i \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$

Therefore, $\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right] \geq 2$

Also, $x^2 + 3$ is a polynomial of degree 2 over $\mathbb{Q}\left(\sqrt[3]{2}\right)$ with $\sqrt{3}i$ as a root.

$$\Rightarrow \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right] \leq 2$$

$$\Rightarrow \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$$

This implies

$$\begin{aligned}[\mathrm{K}: \mathbb{Q}] = [\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}] &= \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right): \mathbb{Q}\right] \\ &= 3 \times 2 \\ &= 6\end{aligned}$$

If G is a group of all $\mathbb{Q}$ −automorphisms of K then

$$O(G) \leq [K: \mathbb{Q}] = 6$$

Claim: $x^3 - 2$ is irreducible over $F = \mathbb{Q}(\sqrt{3}i)$

If possible, suppose $x^3 - 2$ is not irreducible over $F = \mathbb{Q}(\sqrt{3}i)$

This implies, there exist at least one root β of $x^3 - 2$ in F

Then

$$\beta \in F$$

$$\mathbb{Q}(\beta) \subseteq \mathbb{Q}\left(\sqrt{3}i\right)$$

$\Rightarrow [\mathbb{Q}(\beta): \mathbb{Q}]$ divides $\left[\mathbb{Q}\left(\sqrt{3}i\right): \mathbb{Q}\right]$

$\Rightarrow 3$ divides 2, which is absurd.

Therefore, $x^3 - 2$ is irreducible over $F = \mathbb{Q}\left(\sqrt{3}i\right)$.

$K = \mathbb{Q}\left(\sqrt{3}i, \sqrt[3]{2}\right) = F\left(\sqrt[3]{2}\right)$ is a simple extension of F and K is splitting field of $x^3 - 2$ over F which is minimal polynomial of $\sqrt[3]{2}$.

Thus, the group G_1, of all $F-$automorphisms of K is such that F is fixed under G_1.

Therefore, $3 = [K:F] = O(G_1)$

But, G_1 is a subgroup of G. This implies 3 divides $O(G)$.

Similarly, by taking $F_1 = \mathbb{Q}(\sqrt[3]{2})$ and $K = F_1(\sqrt{3}i)$

We get that, 2 divides $O(G)$.

Combining both, we see that 6 divides $O(G)$.

$$\Rightarrow 6 \leq O(G)$$

Therefore, $O(G) = 6 = [K:\mathbb{Q}]$

Hence, $\mathbb{Q}$ is a fixed field under G and K over $\mathbb{Q}$ is Galois extension.

Theorem 6.4.4: Let K be a finite, separable field extension of a field F. Then K is the normal extension of F if and only if the fixed field under the Galois group $G(K,F)$ is F itself. In case,K is normal extension of F, $[K:F] = O(G(K,F))$.

Proof: Since K is a finite separable extension of F. Hence, it is a simple extension.

Let $K = F(\alpha)$ for some $\alpha \in K$.

Let K be the normal extension of F.

Therefore, every irreducible polynomial having a root in K, has all roots in K.

If K' is splitting field of the minimal polynomial of α over F then $K' \subseteq K$.

Also. $\alpha \in K'$

$$\Rightarrow F(\alpha) \subset K'$$

$$\Rightarrow K \subseteq K'$$

Hence, $K = K'$

$\Rightarrow F$ is a fixed field under $G(K,F)$.

Conversely, let F be the fixed field under $G(K,F)$.

$\Rightarrow K$ is the splitting field of the minimal polynomial of α over F.

$\Rightarrow K$ is a normal extension of F.

$$\Rightarrow [K:F] = O(G(K,F))$$

Summary

- Monomorphisms between two fields are defined and it is proved that the set consisting of the monomorphisms is linearly independent.
- Fixed field and F- automorphisms are defined.
- For every F-automorphism $\sigma, \sigma(a)$ and a are related.
- Results about fixed fields are analyzed with the help of examples.
- Artin's theorem and its consequences are studied.
- Galois extensionis defined and elaborated with the help of examples.
- Normal and Galois extensions are related.

Keywords

- Monomorphisms between the fields
- Fixed field
- F - automorphism
- Artin's theorem
- Galois extension

Self Assessment

1: The set of all automorphisms of a field

A: Is a group

B: Is an abelian group

C: Is a cyclic group

D: Is a finite group

2: The set of all automorphisms on a field is a group under the composition of

A: Addition of functions

B: Composite functions

C: Multiplication of functions

D: Subtraction of functions

3: Let K be a field. Which of the following statement is correct?

A: Every set of Monomorphisms from K to K is linearly independent

B: Every set of Monomorphisms from K to K is linearly independent

C: Every set of Monomorphisms from K to K is linearly independent

D: All the options are correct

4: Any set of automorphisms of K is

A: Always linearly independent over K

B: Always linearly dependent

C: May or may not be linearly independent

D: Never linearly independent

5: Let K be a field extension of a field F. Let σ be any automorphism on K. Then σ is $F-$automorphism if and only if

A: $\sigma(x) = 0 \; \forall \; x \in F$

B: $\sigma(x) = 1 \; \forall \; x \in F$

C: $\sigma(x) = x \; \forall \; x \in F$

D: $\sigma(x) = x \; \forall \; x \in K$

6: Let $K = \mathbb{Q}(\sqrt{2})$. Then the fixed field under $Aut\ (K);\ a$ group of all $\mathbb{Q}-$automorphisms on K is

A: $\mathbb{Q}(\sqrt{2})$

B: $\mathbb{Q}$

C: $\mathbb{R} - \mathbb{Q}$

D: $\mathbb{Z}$

7: Consider the field extension $\mathbb{R} \subseteq \mathbb{C}$. Then for every $\mathbb{R} -$ automorphism σ of $\mathbb{C},\ \sigma(i)$ is

A: i

B: $-i$

C: 1

D: $ior - i$

8: Let $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ be a field extension of $\mathbb{Q}$. Then any F −automorphism σ on $\mathbb{Q}(\sqrt{2})$ is determined by

A: $\sigma(\sqrt{2})$

B: $\sigma(\sqrt{3})$

C: $\sigma(\sqrt{2}), \sigma(\sqrt{3})$

D: $\sigma(\sqrt{6})$

9: Let $F \subseteq K$ be a field extension. Then for $F_0 = \{x \in K | \sigma(x) = x \; \forall \; \sigma \in G\}$

A: Prime subfield of K is contained in F_0.

B: F_0 is a subfield of K.

C: $F \subseteq F_0$

D: All options are correct

10: Let G be a finite group of automorphisms of a field K; F_0 the fixed field under G. Then the degree of K over F_0 is

A: $> O(G)$

B: $< O(G)$

C: $= O(G)$

D: $\leq O(G)$

11: Let G be the group of automorphisms of a field K; F_0 the fixed field under G. Then $O(G)$

A: $\leq [K:F]$

B: $\geq [K:F]$

C: $> [K:F]$

D: $= [K:F]$

12: A system of m linear homogeneous equations in n unknowns where $m < n$ has

A: A unique solution

B: Infinitely many solutions

C: No solutions

D: Two solutions

13: Let G be the group of automorphisms of a field K; F_0 the fixed field under G such that $[K:F_0]$ is finite then $[K:F]$

A: Is always finite

B: Is zero

C: Is never finite

D: May be finite or infinite

14: Let G be a finite group of automorphisms of a field K; F_0 the fixed field under G. Then the degree of K over F_0 is

A: $> O(G)$

B: $< O(G)$

C: $= O(G)$

D: $\leq O(G)$

15: Let G be the group of automorphisms of a field K; F_0 the fixed field under G. Then $O(G)$

A: $\leq [K:F]$

B: $\geq [K:F]$

C: $> [K:F]$

D: $= [K:F]$

16: A system of m linear homogeneous equations in n unknowns where $m < n$ has

A: A unique solution

B: Infinitely many solutions

C: No solutions

D: Two solutions

17: Let G be the group of automorphisms of a field K; F_0 the fixed field under G such that $[K:F_0]$ is finite then $[K:F]$

A: Is always finite

B: Is zero

C: Is never finite

D: May be finite or infinite

Answers for Self Assessment

1.	A	2.	B	3.	D	4.	A	5.	C
6.	B	7.	D	8.	C	9.	D	10.	C
11.	B	12.	B	13.	D	14.	C	15.	B
16.	B	17.	A						

Review Questions

1) Let $K = \mathbb{Q}(\sqrt[3]{2})$. Prove that $Aut\ (K) = \{I\}$.
2) Let $K = F(a)$be a simple algebraic extension of degree n of a field F of characteristic zero. Show that number of conjugates of a in K divides $[K:F]$.
3) Show that identity automorphism is the only automorphism of a field having p elements, where p is a prime number.
4) Let $K = \mathbb{Q}(i)$. Find the set of all the automorphisms on K.
5) Prove that the set of automorphisms on a field K is always linearly independent.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 7: Fundamental Theorem of Galois Theory

CONTENTS

Objective

After studying this unit, you will be able to

- state and prove the Fundamental Theorem of Galois theory
- understand important results based on the theorem
- understand Fundamental theorem of Galois theory with the help of examples
- observe the 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K, F)$

Introduction

In this unit, we will study the important result given by the Fundamental Theorem of Galois theory. Further, we will study its applications.

7.1 Fundamental Theorem of Galois Theory

Theorem 7.1.1: (Fundamental Theorem of Galois Theory): Let K be a finite, normal, separable field extension of a field F and let $G(K, F)$ be the Galois group of K over F. Then the correspondence $E \Leftrightarrow G(K, E)$ where E is a subfield of K containing F is 1-1 between the family of subfields of K containing F and the family of all subgroups of $G(K, F)$, satisfying the following conditions

Given any subfield E of K containing F and subgroup H of $G(K, F)$

1. $E = K_{G(K,E)}$
2. $H = G(K, K_H)$
3. $[K:E] = O(G(K, E))$ and $[E:F]$ is the index of $G(K, E)$ in $G(K, F)$
4. E is a normal extension of F if and only if $G(K, E)$ is a normal subgroup of $G(K, F)$
5. When E is a normal extension of F, then $G(E, F)$ is isomorphic to $\frac{G(K,F)}{G(K,E)}$.

Proof: Since K is a finite, normal, separable extension of F and $F \subseteq E \subseteq K$

Again, K is a finite, normal, separable extension of E

$$\Rightarrow E = K_{G(K,E)}$$

$$K_H = \{x \in K | \sigma(x) = x \; \forall \; \sigma \in H\}$$

Each $\sigma \in H$ is a K_H automorphism of K.

$$\Rightarrow H \subseteq G(K, K_H)$$

Also,

$$O(H) = [K: K_H]$$

So, K is a normal extension of K_H.

K_H is a fixed field under $G(K, K_H)$

$$[K: K_H] = O\big(G(K, K_H)\big)$$

$$\Rightarrow O(H) = O\big(G(K, K_H)\big)$$

$$\Rightarrow H = G(K, K_H)$$

Now, K is a normal separable extension of E

$$[K: E] = O\big(G(K, E)\big)$$

and

$$[K: F] = [K: E][E: F]$$

This implies,

$$O\big(G(K, F)\big) = [K: E][E: F]$$

That is,

$$O\big(G(K, F)\big) = O\big(G(K, E)\big)[E: F]$$

$$\Rightarrow [E: F] = \frac{O\big(G(K, F)\big)}{O\big(G(K, E)\big)}$$

Which is the index of $G(K, F)$ in $G(K, E)$.

Let E be the normal extension of F.

Consider $a \in E$, then the splitting field of the minimal polynomial of a over F is contained in E.

Since for any $\sigma \in G(K, F)$

$\sigma(a)$ is a conjugate of a

Therefore, $\sigma(a) \in E$

Thus, for any $\eta \in G(K, E)$

$\eta\big(\sigma(a)\big) = \sigma(a)$

$\Rightarrow \sigma^{-1}\eta\sigma(a) = a$

$\Rightarrow \sigma^{-1}\eta\sigma \in G(K, E)$

So, $G(K, E)$is a normal subgroup of $G(K, F)$.

Conversely, let $G(K, E)$is a normal subgroup of $G(K, F)$

Let $a \in E$. 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 b of $p(x)$ in L. Then b is a conjugate of a over F. Therefore, there exists an $F-$automorphism σ of K such that $\sigma(a) = b$.

For any $\eta \in G(K, E)$

$\sigma^{-1}\eta\sigma \in G(K, E)$

$\Rightarrow \sigma^{-1}\eta\sigma(a) = a$

$\Rightarrow \eta\sigma(a) = \sigma(a)\ \forall\ \eta \in G(K, E)$

However, E is fixed field under $G(K, E)$

$\Rightarrow b = \sigma(a) \in E$

$\Rightarrow L \subseteq E$

$\Rightarrow E$ is a normal extension of F.

Let E is a normal extension of F

$\Rightarrow E = F(a); a \in E$

For any $\sigma \in G(K, F)$

Let σ_E denote the restriction of σ to E

Since $\sigma(a) \in E$

$\Rightarrow \sigma(E) \subseteq E.$

As $[\sigma(E): F] = [E: F]$

$\Rightarrow \sigma(E) = E$

Hence, σ_E is an F −automorphism of F and so

$\sigma_E \in G(E, F)$

Define a map

$\lambda: G(K, F) \to G(E, F)$ as

$\lambda(\sigma) = \sigma_E \; \forall \; \sigma \in G(K, F)$

For $\sigma, \eta \in G(K, F)$

$$\begin{aligned} \lambda(\sigma\eta) &= (\sigma\eta)_E \\ &= \sigma_E \eta_E \\ &= \lambda(\sigma)\lambda(\eta) \end{aligned}$$

Therefore, λ is a homomorphism.

Given any $\gamma \in G(E, F)$

Now $\gamma(a)$ is a conjugate of a over F.

Therefore, there exists an $F -$ automorphism σ of K such that $\sigma(a) = \gamma(a)$.

Also, γ and σ are both $F -$ automorphisms.

$\sigma(x) = r(x) \; \forall \; x \in F(a) = E.$

$\Rightarrow \gamma = \sigma_E = \lambda(\sigma)$

Thus, λ is onto homomorphism.

By the Fundamental theorem of Homomorphism,

$$G(E, F) \cong G(K, F)/\ker \lambda \ldots (1)$$

Consider $\sigma \in \ker \lambda$

$\Leftrightarrow \sigma_E$ is identity map on E.

$\Leftrightarrow \sigma(x) = x \; \forall \; x \in E$

$\Leftrightarrow \sigma \in G(K, E)$

So, $\ker \lambda = G(K, E)$

From (1),

$$G(E, F) \cong G(K, F) \; / \; G(K, E)$$

:(1) Number of subfields of K containing F is finite and, is equal to the number of subgroups of $G(K, F)$.

(2) Since every subgroup of an abelian group is abelian, therefore, $G(K, F)$ is abelian. So, every subfield E of K containing F is a normal extension of F.

Consider $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ has roots $\xi, \xi^2, \ldots, \xi^{p-1}$ where $\xi = e^{\frac{2\pi i}{p}}$

Let $\xi = a = e^{\frac{2\pi i}{p}}$

Then for $\sigma, \eta \in G(K, F); F = \mathbb{Q}, K = F(a)$

$\sigma(a) = a^i,\ \eta(a) = a^j$ for some i, j

$$\eta(\sigma(a)) = \eta(a^i) = a^{ij}$$

$$\sigma(\eta(a)) = \sigma(a^j) = a^{ij}$$

Therefore, $\eta\sigma = \sigma\eta$

This implies, $G(K, F)$ is an abelian group.

7.2 Applications of Fundamental Theorem of Galois Theory

Galois group $G(K,\ F)$ of $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ is isomorphic to Klein's 4 group. Illustration of 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K,\ F)$ where K is splitting field of $f(x)$ over $\mathbb{Q}$ and $F = \mathbb{Q}$.

Solution:

$$\begin{aligned} f(x) &= x^4 - 5x^2 + 6 \\ &= x^4 - 3x^2 - 2x^2 + 6 \\ &= x^2(x^2 - 3) - 2(x^2 - 3) \\ &= (x^2 - 2)(x^2 - 3) \end{aligned}$$

So, $f(x)$ has 4 roots given by $\pm\sqrt{2}, \pm\sqrt{3}$

Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

K is consisting of all the roots of $f(x)$. K is the splitting field of $f(x)$.

Claim: $\{\mathbf{1}, \sqrt{\mathbf{2}}, \sqrt{\mathbf{3}}, \sqrt{\mathbf{6}}\}$ is a basis of $\boldsymbol{K}$ over $\mathbb{Q}$ and $[\boldsymbol{K}: \mathbb{Q}] = \mathbf{4}$

K is splitting field of a non-zero polynomial

$\Rightarrow K$ is a normal extension of $\mathbb{Q}$. Also, K is a separable extension of F.

Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

We know that $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$.

Hence, $[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] = 2$

Again if $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$

$\Rightarrow \sqrt{3} = a + b\sqrt{2};\ a, b \in \mathbb{Q}$

Squaring both sides, we get,

$3 = a^2 + 2b^2 + 2\sqrt{2}ab$

$\Rightarrow (a^2 + 2b^2 - 3) \cdot 1 + 2ab(\sqrt{2}) = 0$

Since the set $\{1, \sqrt{2}\}$ is linearly independent.

$\Rightarrow 2ab = 0$

$\Rightarrow a$ or b is 0

If $a = 0, \sqrt{3} = b\sqrt{2}; b \in \mathbb{Q}$

$\Rightarrow 3 = 2b^2$

$\Rightarrow 3$ is a multiple of 2, which is absurd.

If $b = 0, \sqrt{3} = a; a \in \mathbb{Q}$

which is not possible.

So, our supposition was wrong.

$$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$$

$$\left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})\right] \geq 2$$

Again, x^2-3 is a polynomial over $\mathbb{Q}(\sqrt{2})$ having a root $\sqrt{3}$.

$$\left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})\right] \leq 2$$

This implies, $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})\right]=2$

$$\begin{aligned}[K:\mathbb{Q}] &= \left[K:\mathbb{Q}(\sqrt{2})\right]\left[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right] \\ &= 2\times 2 \\ &= 4\end{aligned}$$

So, $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a basis of K over F.

$G(K,F)\cong K_4$ or it is a cyclic group.

$K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ has two proper normal subgroups namely $\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3})$.

$G(K,F)$ has two proper normal subgroups.

$\left[K:\mathbb{Q}(\sqrt{2})\right]=2,\left[K:\mathbb{Q}(\sqrt{3})\right]=2$

If $G(K,F)$ is a cyclic group of order 4 then $G(K,F)$ cannot have a proper subgroup of order 2.

Hence, $G(K,F)\cong K_4$

Consider x^2-2 is an irreducible monic polynomial over $\mathbb{Q}$ and hence over $\mathbb{Q}(\sqrt{3})$.

Therefore, there exist, $\sigma_1,\sigma_2\in G\left(K,\mathbb{Q}(\sqrt{3})\right)$ such that $\sigma_1(\sqrt{2})=\sqrt{2},\sigma_2(\sqrt{2})=-\sqrt{2}$

Similarly, there exist σ_3,σ_4 such that $\sigma_3(\sqrt{3})=\sqrt{3},\sigma_4(\sqrt{3})=-\sqrt{3}$

We have four automorphisms η_1,η_2,n_3,η_4 in $G(K,\mathbb{Q})$ such that

$$\eta_1(\sqrt{2})=\sqrt{2} \qquad \eta_1(\sqrt{3})=\sqrt{3}$$

$$\eta_2(\sqrt{2})=-\sqrt{2} \qquad \eta_2(\sqrt{3})=\sqrt{3}$$

$$\eta_3(\sqrt{2})=\sqrt{2} \qquad \eta_3(\sqrt{3})=-\sqrt{3}$$

$$\eta_4(\sqrt{2})=-\sqrt{2} \qquad \eta_4(\sqrt{3})=-\sqrt{3}$$

Also, $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a basis of K over $\mathbb{Q}$.

For all $a\in K,\exists\ \alpha_0,\alpha_{13}\alpha_2,\alpha_3\in\mathbb{Q}$ such that

$$a=\alpha_1\cdot 1+\alpha_2\sqrt{2}+\alpha_3\sqrt{3}+\alpha_4\sqrt{6}$$

$$\eta_i(a)=\alpha_1+\alpha_2\eta_i(\sqrt{2})+\alpha_3 n_i(\sqrt{3})+\alpha_4 n_i(\sqrt{6})$$

$$\eta_2^2(\sqrt{2})=\eta_2\left(\eta_2(\sqrt{2})\right)=\eta_2(-\sqrt{2})=-\eta_2(\sqrt{2})=-(-\sqrt{2})=\sqrt{2}$$

$$\eta_2^2(\sqrt{3})=\eta_2\left(\eta_2(\sqrt{3})\right)=\sqrt{3}$$

So, $\eta_2^2=I,\eta_3^2=I,n_1=I,\eta_4^2=I$

Therefore, $G(K,F)$ has 3 subgroups $\{I,\eta_2\},\{I,\eta_3\},\{I,\eta_4\}$.

Let $H_1=\{I,\eta_2\},H_2=\{I,\eta_3\},H_3=\{I,\eta_4\}$

Let K_{H_1} is fixed field of H_1.

$$K_{H_1}=\{x\in K|\sigma(x)=x\ \forall\ \sigma\in H_1\}$$

Let $x\in\mathbb{Q}(\sqrt{2}),x=\alpha+\beta\sqrt{2}$

$$I(x)=x$$

$$\eta_2(\alpha+\beta\sqrt{2})=\alpha+\beta\eta_2(\sqrt{2})$$

$$\Rightarrow \alpha + \beta\sqrt{2} = \alpha - \beta\sqrt{2}$$

$$\Rightarrow \beta = 0$$

Let $x \in \mathbb{Q}(\sqrt{3})$

$$\Rightarrow x = \alpha + \beta\sqrt{3}$$

$$\eta_1(x) = x$$

$$\eta_2(x) = \eta_2(\alpha + \beta\sqrt{3}) = \alpha + \beta\sqrt{3} = x$$

Thus, $\mathbb{Q}(\sqrt{3}) \subseteq K_{H_1}$

Also, for $x \in K_{H_1}$

$$\Rightarrow x \in K, \sigma(x) = x \; \forall \; \sigma \in H_1$$

$$\eta_2(x) = x$$

$$\Rightarrow \eta_2(\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6}) = \alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6}$$

$$\Rightarrow \alpha - \beta\sqrt{2} + \gamma\sqrt{3} - \delta\sqrt{6} = \alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6}$$

$$\Rightarrow \beta = \delta = 0$$

Therefore, $2 = \alpha + \gamma\sqrt{3} \in \mathbb{Q}(\sqrt{3})$

$$K_{H_1} = \mathbb{Q}(\sqrt{3})$$

$$K_{H_2} = \mathbb{Q}(\sqrt{2})$$

and

$$k_{H_3} = \mathbb{Q}(\sqrt{6})$$

Find the Galois group $G(K, F)$ of $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Illustrate of 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K, F)$ where K is splitting field of $f(x)$ over $\mathbb{Q}$ and $F = \mathbb{Q}$.

Solution: $f(x) = x^4 - 2$

Roots of $f(x)$ are given by $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$

Let $\sqrt[4]{2} = \alpha$

So, roots are $\alpha, -\alpha, \alpha i, -\alpha i$

The splitting field K of $f(x) = \mathbb{Q}(\alpha, i)$

$\alpha = \sqrt[4]{2}$ has minimal polynomial $x^4 - 2$ over $\mathbb{Q}$.

Then $[\mathbb{Q}(\alpha): \mathbb{Q}] = 4$.

Then $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

If $i \in \mathbb{Q}(\alpha)$

$$\Rightarrow i = a + b\alpha + c\alpha^2 + d\alpha^3, a, b, c, d \in \mathbb{Q}$$

which is not possible.

Therefore, $i \notin \mathbb{Q}(\alpha)$

$$[\mathbb{Q}(\alpha, i): \mathbb{Q}(\alpha)] \geq 2$$

But $x^2 + 1$ is the polynomial over $\mathbb{Q}(\alpha)$ having root i.

$$\Rightarrow [\mathbb{Q}(\alpha, i): \mathbb{Q}(\alpha)] \leq 2$$

Hence

$$\Rightarrow [\mathbb{Q}(\alpha, i): \mathbb{Q}(\alpha)] = 2$$

Therefore,

$$[K: \mathbb{Q}] = [K: \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha): \mathbb{Q}] = 4 \times 2 = 8$$

So, $\{1, \alpha, \alpha^2, \alpha^3, i\alpha, i\alpha^2, i\alpha^3, i\}$ is a basis of K over $\mathbb{Q}$.

For all $a \in K$

$$a = \alpha_1 \cdot 1 + \alpha_2 \cdot \alpha + \alpha_3 \cdot \alpha^2 + \alpha_4 \cdot \alpha^3 + \alpha_5(i) + \alpha_6(i\alpha) + \alpha_7(i\alpha^2) + \alpha_8(i\alpha^3), \alpha_i \in \mathbb{Q}$$

Now for any $\sigma \in G(K, \mathbb{Q})$

$$\sigma(a) = \alpha_1 + \alpha_2\sigma(\alpha) + \alpha_3\big(\sigma(\alpha)\big)^2 + \alpha_4\big(\sigma(\alpha)\big)^3 + \alpha_5\big(\sigma(i)\big) + \alpha_6\sigma(i)\sigma(\alpha) + \alpha_7\left(\sigma(i)\big(\sigma(\alpha)\big)^2\right) + \alpha_8\sigma(i)\big(\sigma(\alpha)\big)^3$$

σ depends only on $\sigma(i)$ and $\sigma(\alpha)$

$\sigma(i)$ is a conjugate to $i, \sigma(i) = \pm i$

Similarly, $\sigma(\alpha) = \alpha, -\alpha, \alpha i, -\alpha i$

So, we get

$$\sigma_1(\alpha) = \alpha \qquad \sigma_1(i) = i$$
$$\sigma_2(\alpha) = i\alpha \qquad \sigma_2(i) = i$$
$$\sigma_3(\alpha) = -\alpha \qquad \sigma_3(i) = i$$
$$\sigma_4(\alpha) = -i\alpha \qquad \sigma_4(i) = i$$
$$\sigma_5(\alpha) = \alpha \qquad \sigma_5(i) = -i$$
$$\sigma_6(\alpha) = i\alpha \qquad \sigma_6(i) = -i$$
$$\sigma_7(\alpha) = -\alpha \qquad \sigma_7(i) = -i$$
$$\sigma_8(\alpha) = -i\alpha \qquad \sigma_8(\alpha) = -i$$

Then

$$\sigma_2^2(\alpha) = -\alpha = \sigma_3(\alpha) \qquad \sigma_2^2(i) = \sigma_3(i)$$

This implies, $\sigma_2^2 = \sigma_3$

Similarly, $\sigma_3^2 = \sigma_4$

$$\sigma_2^4 = I \qquad \sigma_5^2 = I$$
$$\sigma_6 = \sigma_2\sigma_5 \qquad \sigma_7 = \sigma_2^2\sigma_5$$
$$\sigma_8 = \sigma_2^3\sigma_5$$

If $\sigma_2 = \sigma$ and $\sigma_5 = \eta$

Then

$$\sigma_3 = \sigma^2 \qquad \sigma_4 = \sigma^3$$
$$\sigma_6 = \sigma\eta \qquad \sigma_7 = \sigma^2\eta$$
$$\sigma_8 = \sigma^3\eta \qquad \eta\sigma = \sigma^3\eta$$

So, G has 4 proper normal subgroups given by

$$N_1 = \{I, \sigma\eta, \sigma^2, \sigma^3\eta\}$$
$$N_2 = \{I, \sigma, \sigma^2, \sigma^3\}$$
$$N_3 = \{I, \eta, \sigma^2, \sigma^2\eta\}$$
$$N_4 = \{I, \sigma^2\}$$

and 4 non-normal subgroups

$$H_1 = \{I, \sigma^3\eta\}$$
$$H_2 = \{I, \sigma^2\eta\}$$
$$H_3 = \{I, \sigma\eta\}$$
$$H_4 = \{I, \eta\}$$

$$\sigma(a) = \alpha_1 + \alpha_2\sigma(\alpha) + \alpha_3\big(\sigma(\alpha)\big)^2 + \alpha_4\big(\sigma(\alpha)\big)^3 + \alpha_5\sigma(i) + \alpha_6\sigma(i)\sigma(\alpha) + \alpha_7\sigma(i)\big(\sigma(\alpha)\big)^2 + \alpha_8\sigma(i)\big(\sigma(\alpha)\big)^3$$

Then

$$x \in K_{N_4}$$
$$\Leftrightarrow \sigma^2(x) = x$$
$$\Leftrightarrow \alpha_2 = \alpha_u = \alpha_6 = \alpha_8 = 0$$
$$\Leftrightarrow x = \alpha_1 + \alpha_3\alpha^2 + \alpha_5 i + \alpha_7 i\alpha^2$$
$$\Leftrightarrow K_{N_4} = \mathbb{Q}\big(\sqrt{2}, i\big)$$

Similarly,

$$K_{N_3} = \mathbb{Q}\big(\sqrt{2}\big)$$
$$K_{N_1} = \mathbb{Q}\big(\sqrt{2}i\big)$$
$$K_{N_2} = \mathbb{Q}(i)$$
$$K_{H_1} = \mathbb{Q}\big((1-i)\alpha\big)$$
$$K_{H_2} = \mathbb{Q}\big((1+i)\alpha\big)$$
$$K_{H_3} = \mathbb{Q}(\alpha)$$
$$K_{H_4} = \mathbb{Q}(\alpha);\ \alpha = \sqrt[4]{2}$$

Summary

- The Fundamental Theorem of Galois theory is proved.
- Important results based on the theorem are discussed.
- The Fundamental Theorem of Galois theory is explained with the help of examples.
- 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K,\ F)$ is established.

Keywords

- Galois theory
- Fundamental Theorem of Galois Theory
- Applications of Fundamental theorem of Galois theory

Self Assessment

1: Let K be a finite, normal, separable field extension of a field F and let $G(K,\ F)$ be the Galois group of K over F. Let n be the number of subfields of K containing F and m be the number of subgroups of $G(K, F)$. Then

A. A: $m = n$

B. B: $m < n$

C. C: $m > n$

D. D: $m \geq n$

2: Let K be a finite, normal, separable field extension of a field F and let $G(K,\ F)$ be the Galois group of K over F. Let E be a subfield of K containing F and H is a subgroup of $G(K,F)$ then

A: $E = K_{G(K,F)}$

B: $E = G(K,E)$

C: $E = G(K,F)$

D: $E = K_{G(K,E)}$

3: Let K be a finite, normal, separable field extension of a field F and let $G(K,\ F)$ be the Galois group of K over F. Let E be a subfield of K containing F and H is a subgroup of $G(K,F)$ then

A: $H = G(K,H)$

B: $H = G(K,K_H)$

C: $H = G(K,E)$

D: $H = G(K,F)$

4: Let K be a finite, normal, separable field extension of a field F and let $G(K,\ F)$ be the Galois group of K over F. Let E be a subfield of K containing F and H is a subgroup of $G(K,F)$ then E is a normal extension of F

A: If and only if $G(K,E)$ is a normal subgroup of $G(K,F)$

B: If and only if $G(K,E)$ is an abelian subgroup of $G(K,F)$

C: If and only if $G(K,E)$ is a cyclic subgroup of $G(K,F)$

D: If and only if $G(K,E)$ is a subgroup of $G(K,F)$

5: Let K be a finite, normal, separable field extension of a field F and let $G(K,\ F)$ be the Galois group of K over F. Let E is a normal extension of F, then

A: $G(E,F) = \frac{G(K,F)}{G(K,E)}$

B: $G(E,F)$ is a subgroup of $\frac{G(K,F)}{G(K,E)}$

C: $G(E,F)$ contains $\frac{G(K,F)}{G(K,E)}$

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

6: True/ False Every subfield E of K containing F is a normal extension of F.

A: True

B: False

7: Every subgroup of an abelian group is

A: Abelian and normal

B: Abelian but not normal

C: Normal but not abelian

D: Neither normal nor abelian

8: Let $f(x) = x^2 + x + 1 \in \mathbb{Q}[x]$ and $K = \mathbb{Q}(\omega)$ where $\omega = \frac{1+\sqrt{3}i}{2}$. Then for $\sigma, \eta \in G(K,\mathbb{Q})$

A: σ and η never commute

B: σ and η may or may not commute

C: σ and η are identical

D: σ and η always commute

9: Galois group $G(K,F)$ of $f(x) = x^4 - 7x^2 + 8 \in \mathbb{Q}[x]$ is

A: Infinite

B: Finite

C: Non-abelian

D: Cyclic

10: Let $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Then Galois group of $f(x)$ contains

A: 1 element

B: 2 elements

C: 4 elements

D: 6 elements

11: Let $F = \mathbb{Q}$. Then for any $\sigma \in G(K,F)$ where $G(K,F)$ is Galois group of polynomials $x^2 - 2 \in \mathbb{Q}[x]$, $\sigma(\sqrt{2}) =$

A: $\sqrt{2}$

B: $-\sqrt{2}$

C: $2, \sqrt{2}$

D: $\sqrt{2}, -\sqrt{2}$

12: Let $F = \mathbb{Q}$. Then for any $\sigma \in G(K,F)$ where $G(K,F)$ is Galois group of polynomials $x^2 + 4 \in \mathbb{Q}[x]$, $\sigma(2i) =$

A: $2, -2$

B: $2i, -2i$

C: $2, -2, 2i, -2i$

D: $-2i$

13: Let $F = \mathbb{Q}$. Then for any $\sigma \in G(K,F)$ where $G(K,F)$ is Galois group of polynomials $x^3 - 1 \in \mathbb{Q}[x]$, $\sigma(\omega) =$

A: $1, \omega, \omega^2$

B: $1, \omega$

C: $1, \omega^2$

D: ω, ω^2

14: Let $F = \mathbb{Q}$. Then for any $G(K,F)$ where $G(K,F)$ is Galois group of polynomials $x^2 + 1 \in \mathbb{Q}[x]$ consists of two elements $\{I, \sigma\}$, then for any $a + bi \in K; \sigma(a + bi) =$……

A: $a - b$i

B: $a + bi$

C: $-a + bi$

D: $-a-bi$

15: Let $f(x)=x^4-5x^2+6\in\mathbb{Q}[x]$. Then the number of proper subgroups of $G(K,F)$ is

A: 1

B: 2

C: 3

D: 4

Answers for Self Assessment

1.	A	2.	D	3.	B	4.	A	5.	D
6.	A	7.	A	8.	D	9.	B	10.	C
11.	D	12.	B	13.	D	14.	A	15.	C

Review Questions

1) Find the Galois group $G(K,\ F)$ of $f(x)=x^2-2\in\mathbb{Q}[x]$. Illustrate of 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K,\ F)$ where K is splitting field of $f(x)$ over $\mathbb{Q}$ and $F=\mathbb{Q}$.
2) Find the Galois group $G(K,\ F)$ of $f(x)=x^4-2x^2+1\in\mathbb{Q}[x]$. Illustrate of 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K,\ F)$ where K is splitting field of $f(x)$ over $\mathbb{Q}$ and $F=\mathbb{Q}$.
3) Find the Galois group $G(K,\ F)$ of $f(x)=x^3-2\in\mathbb{Q}[x]$. Illustrate of 1-1 correspondence between the family of subfields of K containing F and the family of all subgroups of $G(K,\ F)$ where K is splitting field of $f(x)$ over $\mathbb{Q}$ and $F=\mathbb{Q}$.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 08: Galois Group of Polynomials

CONTENTS

Objective

After studying this unit, you will be able to

- define Galois group of polynomials
- find Galois group of polynomials
- find the degree of extension of Galois group of polynomials

Introduction

In this unit, we will define the Galois group of polynomials, how to find the Galois group of polynomials, degree of extension of the Galois group of polynomials. We will understand the concept with the help of various examples.

8.1 Galois Group of Polynomials

Definition 8.1.1: Let F be a field. Let $p(x)$ be any non-zero polynomial over the field F and E is the splitting field of $p(x)$ over F. The group of all F −automorphisms of E is called Galois group of $p(x)$ over F.

Let $f(x) = x^4 - x^2 + 1 \in \mathbb{Q}[x]$. Find Galois group of $f(x)$.

Solution:

$$\begin{aligned} f(x) &= x^4 - x^2 + 1 \\ &= \left(x^2 - \sqrt{3}x + 1\right)\left(x^2 + \sqrt{3}x + 1\right) \end{aligned}$$

$f(x)$ has 4 roots given by

$$\frac{\sqrt{3}+i}{2}, \frac{\sqrt{3}-i}{2}, \frac{-\sqrt{3}+i}{2}, \frac{-\sqrt{3}-i}{2}$$

Splitting field K of $f(x)$ is $\mathbb{Q}(\sqrt{3}, i)$.

Consider $B = \{1, \sqrt{3}, i, \sqrt{3}i\}$

Let $a, b, c, d \in \mathbb{Q}$ such that

$$a \cdot 1 + b\sqrt{3} + c \cdot i + d\sqrt{3}i = 0$$

$$\Rightarrow a + b\sqrt{3} = 0$$

and

$$c + d\sqrt{3} = 0$$

Since $\{1, \sqrt{3}\}$ is linearly independent over $\mathbb{Q}$ therefore, $a = b = c = d = 0$

$\Rightarrow$ ***B* is linearly independent.**

Also, for all $\alpha \in K = \mathbb{Q}(\sqrt{3}, i)$

$$\alpha = ak + b\sqrt{3} + c \cdot i + d\sqrt{3}i;\ k \in \mathbb{Q}$$

$$\Rightarrow \alpha = d' \cdot 1 + b\sqrt{3} + c \cdot i + d\sqrt{3}i;\ d' = ak \in \mathbb{Q}$$

That is,

$$\alpha \in L(B)$$

$$\Rightarrow \boldsymbol{K = L(B)}$$

B is the basis of K over F having 4 elements.

Let $\sigma \in G(K, F), F = \mathbb{Q}$

Then $\sigma(a) = a\ \forall\ a \in \mathbb{Q}$

For any $x \in K$

$$x = \alpha_0 \cdot 1 + \alpha_1 \cdot \sqrt{3} + \alpha_2 i + \alpha_3 \cdot \sqrt{3}i$$

$$\Rightarrow \sigma(x) = \alpha_0 + \alpha_1\sigma(\sqrt{3}) + \alpha_2\sigma(i) + \alpha_3\sigma(\sqrt{3})\sigma(i)$$

Since $\sigma(a)$ is a conjugate of a, therefore, $\sigma(\sqrt{3}) = \pm\sqrt{3}, \sigma(i) = \pm i$

Thus $G(K, F) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ such that

$$\sigma_1 = I$$

$$\sigma_2(\sqrt{3}) = \sqrt{3}, \sigma_2(i) = -i$$

$$\sigma_3(\sqrt{3}) = -\sqrt{3}, \sigma_3(i) = i$$

$$\sigma_4(\sqrt{3}) = -\sqrt{3}, \sigma_4(i) = -i$$

Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Find the Galois group of $f(x)$.

Solution:

Let $f(x) = x^3 - 2$

Roots of $f(x) = \sqrt[3]{2}, \sqrt[3]{2}\omega \cdot \sqrt[3]{2}\omega^2$

Splitting field K of $f(x) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$x^2 + x + 1$ is the monic irreducible polynomial over $\mathbb{Q}$ having root ω.

$$\Rightarrow [\mathbb{Q}(\omega): \mathbb{Q}] = 2$$

Again, $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}(\omega)$.

$$\Rightarrow \left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right): \mathbb{Q}(\omega)\right] = 3$$

Therefore, $[K: \mathbb{Q}] = \left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right): \mathbb{Q}(\omega)\right][\mathbb{Q}(\omega): \mathbb{Q}] = 3 \times 2 = 6$

K is generated by $\left\{1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2, \omega\right\}$

So, $G(K, \mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

$$\sigma_1\left(\sqrt[3]{2}\right) = \sqrt[3]{2} \qquad \sigma_1(\omega) = \omega$$

$$\sigma_2\left(\sqrt[3]{2}\right) = \sqrt[3]{2}\omega \qquad \sigma_2(\omega) = \omega$$

$$\sigma_3\left(\sqrt[3]{2}\right) = \sqrt[3]{2}\omega^2 \qquad \sigma_3(\omega) = \omega$$

$$\sigma_4\left(\sqrt[3]{2}\right) = \sqrt[3]{2} \qquad \sigma_4(\omega) = \omega^2$$

$$\sigma_5\left(\sqrt[3]{2}\right) = \sqrt[3]{2}\omega \qquad \sigma_5(\omega) = \omega^2$$

$$\sigma_6\left(\sqrt[3]{2}\right) = \sqrt[3]{2}\omega^2 \qquad \sigma_6(\omega) = \omega^2$$

Let F be a field such that characteristic F is not equal to 2. If $f(x) = x^2 - a$ be an irreducible polynomial over F, then the order of Galois group of $f(x)$ is 2.

Solution:

Given $f(x) = x^2 - a$

Let α be a root of $f(x)$ in some field extension K

$$\Rightarrow \alpha^2 - a = 0$$

$$\Rightarrow (-\alpha)^2 - a = 0$$

$\Rightarrow -\alpha$ is also a root of $f(x)$ in K.

So, splitting field of $f(x) = F(\alpha)$

That is, splitting field K of $f(x)$ over F is a finite, separable, and normal extension of F.

$$[K: F] = 2$$

Characteristic $F \neq 2$

$$\Rightarrow \alpha \neq -\alpha$$

$f(x)$ has two distinct roots α and $-\alpha$.

Therefore, the Galois group of $f(x)$ is $G(K, F) = \{\sigma_1, \sigma_2\}$ where $\sigma_1 = I$ and $\sigma_2(\alpha) = -\alpha$.

If $f(x)$ is a polynomial over F such that $f(x)$ has r distinct roots then Galois group $G(K, F)$ of $f(x)$ is a subgroup of S_r.

Solution:

Let $f(x) = \alpha_0 + x_1 x + \cdots + \alpha_n x^n \in F[x]$ be such that $f(x)$ has r distinct roots $a_1, a_2, \ldots, a_r \in K$.

Then

$\alpha_0 + \alpha_1 a_i + \alpha_2 a_i^2 + \cdots + \alpha_n a_i^n = 0$ for all $1 \leq i \leq r$

Now for $\sigma \in G(K, F)$

$$\alpha_0 + \alpha_1 \sigma(a_i) + \alpha_2 \big(\sigma(a_i)\big)^2 + \cdots + \alpha_n \big(\sigma(a_i)\big)^n = 0$$

$\Rightarrow \sigma(a_i)$ is a root of $f(x)$.

Also, $a_i \neq a_j$

$$\Rightarrow \sigma(a_i) \neq \sigma(a_j)$$

Therefore, $\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_r)$ are r distinct roots of $f(x)$.

That is, $\{\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_r)\} = \{a_1, a_2, \ldots, a_r\}$

$\Rightarrow \sigma(a_i) = a_j$ for some $1 \leq j \leq r$

If $\sigma(a_i) = a_j$ then $\sigma(a_k) \neq a_j$ for any $k \neq i$

$\Rightarrow \phi_\sigma(a_i) = \sigma(a_i)$.

$\Rightarrow \phi_\sigma \in S_r$.

Define a function $f: G(K, F) \to S_r$ as $f(\sigma) = \phi_\sigma$

f is homomorphism

For $\sigma, \eta \in G(K, F)$

$$\begin{aligned} \phi_{\sigma\eta}(a_i) &= (\sigma\eta)(a_i) \\ &= \sigma\big(\eta(a_i)\big) \\ &= \phi_\sigma\big(\eta(a_i)\big) \\ &= \phi_\sigma \circ \phi_\eta(a_i) \end{aligned}$$

So, f is a homomorphism.

f is one-one

Let $\phi_\sigma = \phi_\eta$

$$\Rightarrow \sigma(a_i) = \eta(a_i)$$

$$\Rightarrow \sigma = \eta$$

This implies, f is one-one.

So, $f: G(K, F) \to S_r$ is one-one and homomorphism.

$f\big(G(K, F)\big) \subseteq S_r$ and is an embedding of $G(K, F)$ in S_r but $f\big(G(K, F)\big)$ is a subgroup of S_r.

$\Rightarrow G(K, F)$ is isomorphic to a subgroup of S_r.

Let F be a field such that Ch F is not equal to 2, 3. Let $f(x) = x^3 + bx + c$ be a separable polynomial over F, if $f(x)$ is irreducible, then the Galois group of $f(x)$ is of order 3 or 6. Also Galois group of $f(x)$ is S_3 if and only if $\Delta = -4b^3 - 27c^2$ is not a square in F.

Solution:

Let $f(x)$ has a root $\alpha \in F$

$\Rightarrow f(x) = (x - \alpha)g(x);\ g(x) \in F[x]$ then if $g(x)$ has a root in F, this implies, $f(x)$ has all the roots in F.

Therefore, F is splitting field of $f(x)$. Hence, $[K: F] = 1$.

If $g(x)$ has no root in F, $g(x)$ is irreducible over F and K is splitting field of $f(x)$.

$$[K: F] = 2 \Rightarrow O\big(G(K, F)\big) = 2.$$

If $f(x)$ is irreducible over F then $O\big(G(K, F)\big) \neq 1\ or\ 2$

Also, $G(K,F)$is a subgroup of S_3.

$$O\big(G(K,F)\big) = 3 \text{ or } 6$$

Let α, β, γ be distinct roots of $f(x)$ in K.

Let $\delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\delta)$

$$\Delta = \delta^2 = -4b^3 - 27c^2$$

Then for $\sigma \in G(K,F)$

$$\sigma(\delta) = \pm\delta$$

$$\begin{aligned} \Rightarrow \sigma(\Delta) &= \big(\sigma(\delta)\big)^2 \\ &= (\pm\delta)^2 \\ &= \delta^2 \\ &= \Delta \end{aligned}$$

$\Rightarrow \Delta$ belongs to the fixed field of $G \Rightarrow \Delta \in F$.

Now, $\delta \in F$

$$\Rightarrow \sigma(\delta) = \delta \ \forall\ \sigma \in G(K,F)$$

$\Rightarrow \sigma$ cannot be an odd permutation.

$$\Rightarrow \sigma \in A_3$$

Again, $\sigma \in A_3$

$$\Rightarrow \sigma(\delta) = \delta$$

Therefore, $G(K,F) = A_3$ if and only if $\delta \in F$

If and only if $x^2 - \Delta$ is irreducible over F

If and only if $\Delta \neq x^2$ for any $x \in F$

$\Rightarrow \Delta$ is not a square in F

Let $f(x) = x^3 - 10 \in \mathbb{Q}\big(\sqrt{3}i\big)$. Find the order of the Galois group of its splitting field.

Solution:

Since $f(x)$ hasno roots in F.

Therefore, $f(x)$ is an irreducible polynomial over F.

So, Galois group of $f(x)$ is of order 3 or 6.

$$\Delta = -4(0)^3 - 27(-10)^2 = -2700 = \big(30\sqrt{3}i\big)^2$$

Hence, $0\big(G(K,F)\big) = 3$.

Summary

- Galois group of a polynomial is defined.
- The method to find the Galois group of polynomials is explained with examples.
- The degree of extension of the Galois group of polynomials is defined and explained.

Keywords

- Galois group
- Galois group of a polynomial
- Degree of extension of a Galois group

Self-assessment

1: Let $p(x)$ be a non-zero polynomial over a field F and E be the splitting field of $p(x)$. Then Galois group of $p(x)$ is

A: Group of all monomorphisms on E
B: Group of all automorphisms on E
C: Group of all $F-$ automorphisms on E
D: Group of all homomorphisms on E

2: Let $p(x)$ be a non-zero constant polynomial. Then

A: Splitting field of $p(x) = F$
B: Galois group of $p(x)$ is a singleton set
C: Galois group of $p(x)$ contains at least one non-identity automorphism.
D: None of the above is true

3: Let $p(x)$ be a polynomial of degree 1. Then

A: Splitting field of $p(x) = F$
B: Galois group of $p(x)$ is a singleton set
C: Galois group of $p(x)$ contains only identity automorphism.
D: All above are true

4: Let $p(x) = x^2 + 4x + 4 \in \mathbb{Q}[x]$. Then

A: Splitting field of $p(x)$ is $\mathbb{Q}$
B: $p(x)$ is reducible over $\mathbb{Q}$
C: $p(x)$ has no repeated roots
D: Splitting field of $p(x)$ is a proper extension of $\mathbb{Q}$

5: Let $p(x)$ be a polynomial of degree 3 over $\mathbb{R}$. Then

A: $p(x)$ is always irreducible over $\mathbb{R}$

B: $p(x)$ may or may not be reducible over $\mathbb{R}$

C: $p(x)$ is always reducible over $\mathbb{R}$

D: $p(x)$ has exactly one complex root

6: Minimum number of elements in the Galois group of a polynomial of degree $n \geq 1$ is

A: 0

B: 1

C: 2

D: 3

7: Let $f(x) = x^4 - 3x^2 + 1 \in \mathbb{Q}[x]$. Then Galois group of $f(x)$ contains

A: Only identity element

B: Exactly one non-identity element

C: At least one non-identity element

D: At the most one non-identity element

8: Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Then splitting field of $f(x)$ is

A: $\mathbb{Q}(\sqrt{2}, \mathrm{i})$

B: $\mathbb{Q}(2, \mathrm{i})$

C: $\mathbb{Q}(\pm 2\mathrm{i})$

D: $\mathbb{Q}(\pm \mathrm{i})$

9: Let $f(x) = x^3 - 1 \in \mathbb{Q}[x]$. Then Galois group of $f(x)$ contains …... number of elements

A: 0

B: 1

C: 2

D: 3

10: Let $f(x) = x^4 - 2x^2 + 1 \in \mathbb{Q}[x]$. Then the number of roots of $f(x)$ in $\mathbb{Q}$ is

A: 1

B: 2

C: 3

D: 4

11: Let $f(x) = x^2 - 55 \in \mathbb{Q}[x]$. Then the order of the Galois group of $f(x)$ is

A: 0

B: 1

C: 2

D: 3

12: Galois group of a polynomial over a field F is

A: Always unique

B: May or may not be unique

C: Never unique

D: Always infinite

13: Let $f(x) = (x^2 - 2)(x^2 - 3)(x + 1)^2 \in \mathbb{Q}[x]$ is a polynomial. Then Galois group $G(K, \mathbb{Q})$ of $f(x)$ is a subgroup of

A: S_4

B: S_5

C: S_6

D: S_7

14: Let $f(x) = x^3 - 3 \in \mathbb{Q}[x]$. Then $O(G(K, F)) =$

A: 1

B: 3

C: 6

D: 18

15: Let $f(x) = x^3 - 10 \in \mathbb{Q}[x]$. Then $O(G(K, F)) =$

A: 1

B: 3

C: 6

D: 18

Answers for Self Assessment

1.	C	2.	D	3.	D	4.	A	5.	C
6.	B	7.	B	8.	A	9.	C	10.	D
11.	C	12.	A	13.	B	14.	C	15.	B

Review Questions

1) Let $f(x) = x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$. Find Galois group of $f(x)$.
2) Let $f(x) = x^3 - 12 \in \mathbb{Q}[x]$. Find the Galois group of $f(x)$.
3) Let $F = \mathbb{Q}$ and$f(x) = x^2 - 11$then find the order of Galois group of $f(x)$.
4) If $f(x) = x^3 - 3x^2 + 2x$ is a polynomial over $F = \mathbb{Q}$ then prove that Galois group $G(K, F)$ of $f(x)$ is a subgroup of S_3.
5) Let $f(x) = x^3 - 10 \in \mathbb{Q}(\sqrt{3}i)$. Find the order of the Galois group of its splitting field.

Further Readings

1) Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
2) Topics in algebra by I.N. Hartstein, Wiley
3) Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 09: Cyclotomic and Abelian Extensions

CONTENTS

Objective

After studying this unit, you will be able to

- define cyclotomic polynomials and extensions
- express cyclotomic polynomials explicitly
- prove that cyclotomic polynomials are irreducible over $\mathbb{Q}$
- define abelian field extension
- prove that the splitting field K of $x^n - \alpha$ for $\alpha \in F$ is an abelian extension

Introduction

In this unit, we will define cyclotomic polynomials and extensions. We will express these extensions and prove that the cyclotomic polynomials are irreducible over the field of rational numbers. Further, we will study abelian extensions.

9.1 Cyclotomic Polynomials and Extensions

Definition 9.1.1: Let F be any field. Then the roots of polynomial $x^n - 1 \in F[x]$ are called $n-th$ roots of unity. For example, $n = 2, x^2 - 1 \in \mathbb{Q}[x]$ has 2 roots 1 and -1. For $n = 3, x^3 - 1$has 3 roots $1, \omega, \omega^2$; $\omega = \frac{1 \pm \sqrt{3}i}{2}$. For $n = 4$, roots are $1, -1, i, -i$.

Theorem 9.1.2: The $n - th$ roots of unity form a cyclic group under multiplication.

Proof: Let G be the set of $n - th$ roots of unity.

$$G = \{a | a^n = 1\}$$

Then $1^n = 1$ implies $1 \in G$

$$\Rightarrow G \neq \phi$$

Also, if K is splitting field of $x^n - 1$ then $G \subseteq K$.

Let $a, b \in G$

$$a^n = 1, b^n = 1$$

Consider

$$(ab^{-1})^n \quad = a^n b^{-n}$$

$$= (1)(1)$$

$$= 1$$

Therefore, $ab^{-1} \in G \; \forall \; a, b \in G$

Thus, G is a subgroup of the multiplicative group of K, hence G is a group.

Let exponent of $G = m$

$\Rightarrow m \leq n$ ... (1)

Also, there exists $a \in G$ such that $a^m = 1$

For all $b \in G, b^m = 1$

$\Rightarrow x^m - 1 = 0$ has at least n roots.

Therefore, $n \leq m$ ... (2)

From (1) and (2), we get,

$$n = m$$

So, there exist $a \in G$ such that $a^n = 1$

$$\Rightarrow 0(a) = 0(G)$$

Hence, $G = < a >$ is the cyclic group.

Definition 9.1.3: (Primitive nth root of unity): Let ξ be the generator of nth root of unity. Then ξ is called the primitive nth root of unity.

1. If ξ is a generator of G then ξ^k is also a generator of G for all $k \in \mathbb{N}$ such that $k < n$ and $GCD\ (k, n) = 1$. Hence G has $\phi(n)$ number of generators. In other words, for all n, there are $\phi(n)$ primitive nth roots of unity.
2. If a field F has a primitive nth root of unity ξ

   $$\xi \in F$$

   $$\Rightarrow \xi^k \in F \; \forall \; k$$

   For all $x \in G =< \xi >$

   $$x = \xi^m; m \in \mathbb{Z}$$

   $$\Rightarrow x \in F$$

   $\Rightarrow F$ contains all nth roots of unity.
3. If ξ is a generator of G then ξ^k is also a generator of G for all $k \in \mathbb{N}$ such that $k < n$ and $GCD\ (k, n) = 1$. Hence G has $\phi(n)$ number of generators. In other words, for all n, there are $\phi(n)$ primitive nth roots of unity.
4. If a field F has a primitive nth root of unity ξ

   $$\xi \in F$$

   $$\Rightarrow \xi^k \in F \; \forall \; k$$

   For all $x \in G =< \xi >$

   $$x = \xi^m; m \in \mathbb{Z}$$

   $$\Rightarrow x \in F$$

   $\Rightarrow F$ contains all nth roots of unity.

Definition 9.1.4: (nth cyclotomic polynomial): Let ω be the primitive nth root of unity. Let S be the collection of all such ω. then

$$\phi_n(x) = \prod_{\omega \in S} (x - \omega)$$

is called nth cyclotomic polynomial.

For $n = 2, \omega = -1, \phi_2(x) = x + 1$

For $n = 3, \omega = \omega, \omega^2, \phi_3(x) = (x - \omega)(x - \omega^2) = x^2 + x + 1$

Theorem 9.1.5:

$$\boldsymbol{x^n - 1 = \prod_{d|n} \phi_d(x)\,, 1 \le d \le n}$$

Proof: Let α_i is the nth root of unity for $1 \le i \le n$

Then $x^n - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$

Let us re-arrange $\alpha_i's$ such that we put together those $\alpha_i's$ whose orders are the same.

Since G is cyclic, therefore, there are $\alpha_i's$ for each divisor d of n.

Let P is the product of all $(x - \alpha_i)$, factors of $x^n - 1$ such that $O(\alpha_i) = d, d|n$

Claim: $\boldsymbol{P = \phi_d(x)}$

Let α is dth root of unity.

$$\alpha^d = 1$$

Since $d|n, n = dn_1; n_1 \in \mathbb{Z}$

$$\alpha^n = \alpha^{dn_1} = (\alpha^d)^{n_1} = 1$$

$\Rightarrow \alpha$ is nth root of unity.

In particular, primitive dth root of unity is nth roots of unity

Therefore, each of the primitive dth roots of unity must give rise to a factor in P.

$$P = \phi_d(x)$$

$$\Rightarrow x^n - 1 = \prod_{d|n} \phi_d(x)\,;\ 1 \le d \le n$$

Determination of $\boldsymbol{\phi_1(x), \phi_2(x)}$, ...

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

For $n = 1$

$$x - 1 = \phi_1(x)$$

For $n = 2$

$$\begin{aligned} x^2 - 1 &= \phi_1(x)\phi_2(x) \\ &= (x - 1)\phi_2(x) \end{aligned}$$

This implies, $x + 1 = \phi_2(x)$

For $n = 3$

$$\begin{aligned} x^3 - 1 &= \phi_1(x)\phi_3(x) \\ &= (x - 1)\phi_3(x) \end{aligned}$$

This implies, $\phi_3(x) = x^2 + x + 1$

For $n = 4$

$$\begin{aligned} x^4 - 1 &= \prod_{d|4} \phi_d(x) \\ &= \phi_1(x)\phi_2(x)\phi_4(x) \\ &= (x - 1)(x + 1)\phi_4(x) \end{aligned}$$

$$(x^2-1)(x^2+1) = (x^2-1)\phi_4(x)$$

$$\Rightarrow \phi_4(x) = x^2+1$$

……

Theorem 9.1.6: $\boldsymbol{\phi_n(x) \in \mathbb{Z}[x]}$

Proof: We will use the Principle of Mathematical Induction on n

For $n = 1$,

$$\phi_1(x) = x - 1 \in \mathbb{Z}[x]$$

Therefore, the result is true for $n = 1$

Let the result is true for some $1 \leq m < n, n > 1$

By the result,

$$x^n - 1 = \prod_{d|n} \phi_d(x)\,;\ 1 \leq d \leq n$$

$$x^n - 1 = q(x)\phi_n(x);\ q(x) = \prod_{d|n} \phi_d(x)\,;\ 1 \leq d < n$$

By the Induction hypothesis,

$$\phi_d(x) \in \mathbb{Z}[x]\ \forall\ d < n$$

$$\Rightarrow q(x) \in \mathbb{Z}[x]$$

Since $q(x)$ is monic polynomial in $\mathbb{Z}[x]$

By division algorithm, there exist $r(x), s(x) \in \mathbb{Z}[x]$ such that

$$x^n - 1 = q(x)r(x) + s(x);\ s(x) = 0\ or\ \deg s\,(x) < \deg q(x)$$

As $\mathbb{Z} \subseteq \mathbb{Q}(\xi)$

ξ is primitive nth root of unity

$$\Rightarrow x^n - 1 = q(x)r(x) + s(x) \in \mathbb{Q}(\xi)[x]$$

But in $\mathbb{Q}(\xi)[x]$

$$x^n - 1 = q(x)\phi_n(x)$$

By uniqueness of quotient and remainder,

$$r(x) = \phi_n(x), s(x) = 0$$

Since $r(x) \in \mathbb{Z}[x]$

$$r(x) = \phi_n(x)$$

Thus, $\phi_n(x) \in \mathbb{Z}[x]$

Corollary 9.1.7: $\phi_n(x) \in \mathbb{Z}[x]$

Also, $\mathbb{Z} \subseteq \mathbb{Q}$

$\phi_n(x)$ can also be treated as a polynomial over $\mathbb{Q}$.

Theorem 9.1.8: $\phi_n(x)$is irreducible over $\mathbb{Q}$.

Proof: First we prove that $\phi_n(x)$ is irreducible over $\mathbb{Z}$.

Let $h(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ such that

$$\phi_n(x) = h(x)g(x); g(x) \in \mathbb{Z}[x]$$

Since ϕ_n is monic. Therefore, we can choose $g(x), h(x)$ as monic polynomials

Now any root of $h(x)$ is a root of $\phi_n(x)$ that is, primitive nthroot of unity

Let ξ be the primitive nth root of unity so that $h(\xi) = 0$

Let p be a prime number such that $p < n$ and $p \nmid n$

Claim: ξ^p is a root of $h(x)$

Assume that $h(\xi^p) \neq 0$

$$\Rightarrow g(\xi^p) = 0$$

$\Rightarrow \xi^p$ is a root of $g(x)$.

$\Rightarrow \xi$ is a root of $g(x^p)$

But $h(x)$is an irreducible monic polynomial satisfied by ξ so, it is a minimal polynomial of ξ over $\mathbb{Q}$.

Hence, $h(x)$ divides $g(x^p)$ in $\mathbb{Q}[x]$

$$\Rightarrow g(x^p) = h(x)l(x); l(x) \in \mathbb{Q}[x]$$

Since $g(x^p), h(x) \in \mathbb{Z}[x]$

$$\Rightarrow l(x) \in \mathbb{Z}[x]$$

Now, $x^n - 1 = q(x)\phi_n(x)$ where $q(x) = \prod_{d|n} \phi_d(x)\,;\ 1 \leq d \leq n$

$$\Rightarrow x^n - 1 = q(x)h(x)g(x)$$

Now define,

$\theta: \mathbb{Z} \to \mathbb{Z}/\langle p\rangle$ by $\theta(n) = n + \langle p\rangle = \bar{n}$

θ is onto homomorphism

Therefore, θ induces an onto homomorphism. $\psi: \mathbb{Z}[x] \to \mathbb{Z}\,/\,\langle p\rangle[x]$ given by

$$\psi\left(\sum_{i=1}^{t} \alpha_i x^i\right) = \sum_{i=1}^{t} \bar{\alpha_i} x^i$$

Let $f(x) = \sum_{i=1}^{t} \alpha_i x^i$

and $\bar{f}(x) = \sum_{i=1}^{t} \bar{\alpha_i} x^i$

$$\psi(x^n - 1) = \psi\big(q(x)h(x)g(x)\big)$$

$$\Rightarrow x^n - \bar{1} = \bar{q}(x)\bar{h}(x)\bar{g}(x) \cdots (1)$$

Let $g(x) = \beta_0 + \beta_1 x + \cdots + \beta_r x^r$

By Fermat's theorem,

For $a \in \mathbb{Z}, \bar{a}^p = \bar{a}$

$$\begin{aligned} \Rightarrow \bar{g}(x^p) &= \left(\bar{\beta}_0 + \bar{\beta}_1 x^p + \cdots + \bar{\beta}_r x^{rp}\right) \\ &= \bar{\beta}_0^p + \bar{\beta}_1^p x^p + \cdots + \bar{\beta}_r^p x^{rp} \\ &= \big(\bar{g}(x)\big)^p \end{aligned}$$

Now, $g(x^p) = h(x)l(x)$

$$\Rightarrow \bar{g}(x^p) = \bar{h}(x)\bar{l}(x)$$

$$\Rightarrow \big(\bar{g}(x)\big)^p = \bar{h}(x)\bar{l}(x)$$

If $\bar{\imath}(x)$ is irreducible factor of $\bar{h}(x)$ in ${}^{\mathbb{Z}}/_{\langle p\rangle}[x]$.

$\Rightarrow \bar{\imath}(x)\ |(\bar{g}(x))^p$ in ${}^{\mathbb{Z}}/_{\langle p\rangle}[x]$

$\Rightarrow \bar{\imath}(x)|\bar{g}(x)$ in ${}^{\mathbb{Z}}/_{\langle p\rangle}[x]$.

Using (1)

$\left(\bar{i}(x)\right)^2 | \, x^n - \bar{1}$ in $\mathbb{Z}/\langle p \rangle [x]$.

Consequently, $x^n - \bar{1}$ has multiple roots in $\mathbb{Z}/\langle p \rangle$

But $f(x) = x^n - \bar{1}$

$\Rightarrow \left(\bar{f}(x)\right)' = nx^{n-1} \neq 0$ as $p \nmid n$ which is a contradiction

$\Rightarrow \xi^p$ is a root of $h(x)$.

Let a be any root of $\phi_n(x)$

$\Rightarrow a$ is primitive nth root of unity.

Since ξ is also a primitive nth root of unity.

$\Rightarrow a = \xi^k$ for some $k \in \mathbb{N}$

Let $k = p_1 p_2 \ldots p_s$; $p_i's$ are all prime numbers such that $p_i < n \forall \, i$

None of the p_i is a factor of n, otherwise, $GCD(k, n) \neq 1$

$p_i | n$ Since $p_i | k$

Therefore, $p_i | GCD(k, n)$, that is, $p_i | 1$ but p_i is a prime number.

So, $p_i \nmid n$ for any i

That is, $a = \xi^k$ cannot be primitive nth root of unity.

By successive application of what we did, $\xi^{p_1}, \xi^{p_1 p_2}, \ldots, \xi^{p_1 p_2 \ldots p_s} = a$ are roots of $h(x)$.

$\Rightarrow$ Every root of $\phi_n(x)$ is a root of $h(x)$.

$\Rightarrow \phi_n(x) = h(x)$.

Since $h(x)$ is irreducible, therefore, $\phi_n(x)$ is an irreducible polynomial over $\mathbb{Z}$, hence over $\mathbb{Q}$.

Corollary 9.1.9: Degree of splitting field of $x^n - 1$ over $\mathbb{Q}$ is $\phi(n)$.

Let K be the splitting field of $x^n - 1$ over $\mathbb{Q}$, then if ξ is primitive nth root then $K = \mathbb{Q}(\xi)$.

Note: K defined above is called a cyclotomic extension of $\mathbb{Q}$.

1) Find the primitive 5th root of unity.
2) For a prime number p, find the primitive $p - th$ roots.

9.2 Abelian Extension

Theorem 9.2.1: Any finite subgroup of the multiplicative group of a field is cyclic and hence a multiplicative group of a Galois field is cyclic.

Proof: Let F be any field and S be a finite subgroup of $F - \{0\}$.

Now, S is finite. Therefore, we can choose $y \in S$ such that $O(y) \geq O(z) \; \forall \, z \in S$

Let $O(y) = n$

For $z \in S$, $O(y)$ is a multiple of $O(z)$.

$$O(z) | O(y) \; \forall \, z \in S$$

Therefore,

$$z^n = e \; \forall \, z \in S$$

That is, every element in S is a root of the polynomial $x^n - e$ and S contains elements of type $e, y, y^2, \ldots$, as $y \in S$.

For all $z \in S, z$ is a root of $x^n - e$ over F but $x^n - e$ can have maximum n number of roots.

Therefore, $O(S) \leq n$

Also, $O(y) = n$

So, $e, y, y^2, \ldots, y^{n-1}$ are all distinct elements in S.

$S = \{e, y, y^2, \ldots, y^{n-1}\} = < y >$ is a cyclic group.

Since Galois field is always finite.

Therefore, its multiplicative group is always finite and hence cyclic.

Theorem 9.2.2: If K is splitting field of $f(x) = x^n - e$ over some field F of characteristic p such that p does not divide n, then K contains n distinct roots of $f(x)$.

Proof: $f(x) = x^n - e$

$$\Rightarrow f'(x) = nx^{n-1}$$

Therefore, $f'(x) = 0$ if and only if $n = 0$ or $p|n$ or $x = 0$

But $n \neq 0$ and $p \nmid n \Rightarrow f'(x) = 0$ only if $x = 0$.

So, $f'(x) \neq 0$

$\Rightarrow f(x)$ has no multiple roots in any field extension of F.

Also, splitting field of $f(x)$ contains all the roots of $f(x)$.

Since $\deg f(x) = n$and all roots are distinct, therefore, K contains n distinct roots of $f(x)$.

Theorem 9.2.3: Let F be a field of characteristic zero and K be the splitting field of polynomial $x^n - e$ over F, then the set of all roots of $f(x)$ form a cyclic group of order n with respect to multiplication.

Proof: Let $f(x) = x^n - e$

K is splitting field of $f(x)$.

Let S be the set of all roots of $f(x)$.

Since $e^n - e = 0$, therefore, $e \in S$.

$\Rightarrow S \neq \phi$

Also, for $a, b \in S$

$a^n = e, \quad b^n = e$

Consider

$$\begin{aligned}(ab^{-1})^n &= a^n(b^{-1})^n \\ &= a^n(b^n)^{-1} \\ &= e \cdot e^{-1} \\ &= e\end{aligned}$$

Thus, S is a subgroup of the multiplicative group of K and S is finite.

This implies S is a cyclic group.

Theorem 9.2.4: Let F be a field of characteristic zero and K be the splitting field of polynomial $x^n - e$ over F, the Galois group $G(K, F)$ is isomorphic to a subgroup of the residue class group M of integers relatively prime to n. Consequently, $G(K, F)$ is cyclic.

Proof: Let $G(K, F)$ be the Galois group of K over F and we have proved that the set $S = \{a | a^n = e\}$ is a cyclic group. Let $S = < \theta >$

Then$\theta^n = e$, i.e., θ is a root of $x^n = e$ then all other roots of this polynomial are of the form $\theta^i; i \in \mathbb{Z}$ and splitting field of $x^n - e$ is $F(\theta) = K$.

Let $\sigma \in G(K, F)$

Then for $\xi^n = e$,

$$\begin{aligned} e &= \sigma(e) \\ &= \sigma(\xi^n) \\ &= \big(\sigma(\xi)\big)^n \end{aligned}$$

So, $\big(\sigma(\xi)\big)^n = e$

That is, $\sigma(\xi)$ is also a root of $x^n - e$ if ξ is a root of $x^n - e$.

Now, θ is a root of $x^n - e \Rightarrow \sigma(\theta) \in S = < \theta >$.

$\Rightarrow \exists\, t \in \mathbb{Z}$ such that $\sigma(\theta) = \theta^t$

Now, $\sigma(\theta) = \theta^t; t \in \mathbb{Z}$ such that $GCD\ (n, t) = 1$

Let $\bar{t}$ be the residue class modulo n in which t belongs. Then $\bar{t} \in M$.

Define a map $g: G(K, F) \to M$ as $g(\sigma) = \bar{t}; \sigma(\theta) = \theta^t$

g is well defined:

Let $\sigma(\theta) = \theta^u$

Also, $\sigma(\theta) = \theta^t$

$$\Rightarrow \theta^t = \theta^u$$

$$\Rightarrow \theta^{t-u} = e$$

But the order of $\theta = n$

$$\Rightarrow n | t - u$$

$$\Rightarrow \bar{t} = \bar{u}$$

$\Rightarrow g(\sigma)$ is unique.

Hence, g is well defined.

g is homomorphism

Let $\sigma, \eta \in G(K, F)$ such that $g(\sigma) = \bar{t}_1;\ \sigma(\theta) = \theta^{t_1}$

and

$$g(\eta) = \bar{t}_2; \eta(\theta) = \theta^{t_2}$$

Then

$$\begin{aligned} \sigma\eta(\theta) &= \sigma(\theta^{t_2}) \\ &= (\theta^{t_2})^{t_1} \\ &= \theta^{t_2 t_1} \end{aligned}$$

Also,

$$\begin{aligned} g(\sigma\eta) &= \overline{t_2 t_1} \\ &= \overline{t_1 t_2} \\ &= \bar{t}_1 \bar{t}_2 \\ &= g(\sigma) g(\eta) \end{aligned}$$

g is one-one

Let $\sigma \in 0$

$$\Rightarrow g(\sigma) = \bar{1}$$

$$\Rightarrow \sigma(\theta) = \theta' = \theta$$

σ is identity on $F(\theta) = K$

$$\Rightarrow \sigma = I$$

So, $\ker g = \{I\}$

$\Rightarrow g$ is one-one.

Since both $G(K,F)$ and M are consisting of n elements. Then g is one-one and hence g is onto.

Therefore, $g: G(K,F) \to M$ is one-one, onto and homomorphism.

Hence, $g: G(K,F) \to M$ is an isomorphism.

$$\Rightarrow G(K,F) \cong M$$

Theorem 9.2.5: If F is a field with ch. 0 such that it contains a primitive nth root of unity then for any $0 \neq \alpha \in F$, the splitting field L of $x^n - \alpha$ over F is $F(a)$ where a is the arbitrary root of $x^n - \alpha$. Further $G(L,F)$ is abelian.

Proof: $a$is a root of $x^n - \alpha$.

Also, let θ be a primitive nth root of unity then we know that all the nth roots of unity are represented as $\theta, \theta^2, \theta^3, \ldots, \theta^n = e$.

Consider

$$\begin{aligned}(\theta a)^n - \alpha &= \theta^n a^n - \alpha \\ &= e \cdot \alpha - \alpha \\ &= \alpha - \alpha \\ &= 0\end{aligned}$$

Thus, θa is a root of $x^n - \alpha$.

Moreover, $\theta a, \theta^2 a, \theta^3 a, \ldots, \theta^{n-1} a, a$ are all roots of $x^n - \alpha$ over F.

Let K be any field containing a splitting field of $x^n - \alpha$ over $F \Rightarrow a \in K$.

Also, $a, \theta a, \theta^2 a, \ldots, \theta^{n-1} a \in K$.

If L is splitting field of $x^n - \alpha$

$$\Rightarrow a, \theta a, \theta^2 a, \ldots, \theta^{n-1} a \in L$$

$$\Rightarrow F(\theta, a) \subseteq L$$

But $L = F(a, \theta a, \theta^2 a, \ldots, \theta^{n-1} a) \subseteq F(\theta, a)$

Hence, $L = F(\theta, a)$

If θ is that primitive root in F such that $F(\theta) = F$

$$\Rightarrow F(\theta, a) = F(a)$$

$$\Rightarrow L = F(a)$$

Let $\sigma, \eta \in G(L,F)$

$\sigma(a), \eta(a)$ both are roots of $x^n - \alpha$.

$$\sigma(a) = \theta^i a$$

and

$$\eta(a) = \theta^j a$$

Then

$$\begin{aligned}\sigma\eta(a) &= \sigma\left(\theta^j a\right) \\ &= \theta^i\left(\theta^j a\right) \\ &= \theta^{i+j}(a)\end{aligned}$$

$$\begin{aligned}\eta\sigma(a) &= \eta\left(\theta^i a\right) \\ &= \theta^j\left(\theta^i a\right)\end{aligned}$$

$$= \theta^{j+i}(a)$$

$$= \sigma\eta(a)$$

Hence $\eta\sigma = \sigma\eta \; \forall \; \sigma, \eta \in G(L, F)$

Therefore, $G(L, F)$ is an abelian group.

Definition 9.2.6: (Abelian Field Extension): Let $F \subseteq K$ be a field extension such that $G(K, F)$ is an abelian group then this extension is called abelian field extension. For example, K is splitting field of $x^n - e \in F[x]$ such that F contains a primitive nth root of unity then $G(K, F)$ is abelian and hence it is an abelian field extension.

Summary

- Cyclotomic polynomials and extensions are defined.
- Cyclotomic polynomials are explained.
- It has been observed that Cyclotomic polynomials are irreducible over $\mathbb{Q}$
- Abelian field extensions are defined.

Keywords

- Cyclotomic polynomial
- Cyclotomic extensions
- The primitive $n - th$ root of unity
- Abelian field extension
- Irreducibility of Cyclotomic polynomial

Self Assessment

1: The set of 4th roots of unity over the field $\mathbb{Q}$ are given by

A: $\{1, -1\}$

B: $\{1, -1, i\}$

C: $\{1, i\}$

D: $\{1, -1, i, -i\}$

Question 2: The $n - th$ roots of unity

A: Does not form a group

B: Form a cyclic group under multiplication

C: Form a group under addition

D: Form a non-abelian group under multiplication

3: If the set $\{a | a^n = 1\}$ contains 2 elements. Then

A: $n = 2$

B: $n > 2$

C: $n < 2$

D: $n = 3$

4: If n is even positive integer then the set of nth root of unity contains exactly …… real numbers

A: 0

B: 1

C: 2

D: 4

5: If n is an odd positive integer then the set of nth root of unity contains exactly …… complex (non-real) numbers

A: 0

B: 1

C: 2

D: 4

6: Exponent of a group G is

A: The highest positive integer m such that $a^m = e$

B: The least positive integer m such that $a^m = e$

C: Order of the group G

D: $n - 1$; where n is the order of group G.

7: The exponent of a cyclic group G is

A: $\leq O(G)$

B: $< O(G)$

C: $> O(G)$

D: $= O(G)$

8: Primitive root(s) of nth root of unity

A: Is unique always

B: Unique only if $n = 2$

C: Is $\phi(n)$ in number

D: All options are correct

9: The number of primitive 16th root of unity is

A: 2

B: 4

C: 6

D: 8

10: Number of primitive pth roots of unity, where p is any prime, is

A: p

B: $p - 1$

C: $p - 2$

D: $2p$

11: Multiplicative group of a Galois group is always

A: Infinite

B: Non-abelian

C: Cyclic

D: Abelian but not cyclic

12: Let K is the splitting field of $f(x) = x^7 - 1 \in \mathbb{Z}_5[x]$ then K

A: Contains 7 distinct roots of $f(x)$

B: Contains at least one root with a multiplicity greater than 1

C: Contains at least two roots with multiplicity greater than 1

D: Contains all the roots with multiplicity greater than 1

13: Let K is the splitting field of the polynomial $x^9 - 1 \in \mathbb{Q}[x]$. Then the Galois group $G(K, F)$

A: Is isomorphic to a subgroup of the residue class group M of integers relatively prime to 9

B: $G(K, F)$ is abelian

C: $G(K, F)$ is cyclic

D: All options are correct

14: Let K is the splitting field of the polynomial $x^{24} - 1 \in \mathbb{Q}[x]$. Then the Galois group $G(K, F)$

A: Is isomorphic to a subgroup of the residue class group M of integers relatively prime to 6

B: Is isomorphic to a subgroup of the residue class group M of integers relatively prime to 12

C: Is isomorphic to a subgroup of the residue class group M of integers relatively prime to 18

D: Is isomorphic to a subgroup of the residue class group M of integers relatively prime to 24

15: Let F is a field with ch. 0 such that it contains a primitive nth root of unity then for any $0 \neq \alpha \in F$, the splitting field L of $x^n - \alpha$ over F is a simple extension

A: True

B: False

Answers for Self Assessment

1.	D	2.	B	3.	A	4.	C	5.	B
6.	A	7.	D	8.	D	9.	D	10.	B
11.	C	12.	A	13.	D	14.	D	15.	A

Review Questions

1) Check that $\frac{-1+\sqrt{3}i}{2}$ is a primitive cube root of unity and $\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$ is the primitive 5^{th} root of unity.
2) Prove that the 7^{th} roots of unity form a cyclic group under multiplication.

3) Prove

$$x^n - 1 = \prod_{d|n} \phi_d(x), 1 \leq d \leq n$$

for $n = 4$.

4) Prove/Disprove: Multiplicative group of a Galois field is cyclic.

Further Readings

1) Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
2) Topics in algebra by I.N. Hartstein, Wiley
3) Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 10: Fundamental Theorem of Algebra and Composite Extension

CONTENTS

Objective

After studying this unit, you will be able to

- understand the theory of roots of polynomials
- prove that the square root of every complex number exists in the field of complex numbers
- state and prove the fundamental theorem of algebra
- understand the importance of the theorem
- define composite extension
- understand results about composite Galois extension

Introduction

In this unit, we will first understand the theory of the roots of polynomials. Then we will state and prove the fundamental theorem of algebra. Composite extension of field will be defined and explained.

10.1 Basics of Fundamental theorem of algebra

Theorem 10.1.1: Intermediate Value Theorem: Let $f(x)$ be a continuous, real-valued function defined on a closed interval $[a, b]$ such that $f(a) < 0$ and $f(b) > 0$ then there exists at least one $c \in (a, b)$ such that $f(c) = 0$. Moreover, for any real number $b, \sqrt{b}$ is always a complex number. If $b \geq 0, b \in \mathbb{R}$.

For example, let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$

Then $f(1) = 1^2 - 2 = 1 - 2 = -1 < 0$

and $f(2) = 2^2 - 2 = 4 - 2 = 2 > 0$

So, $f(1) < 0, f(2) > 0$ but there does not exist any $x \in \mathbb{Q}, x \in (1, 2)$ and $f(x) = 0$ but if we consider $f(x)$ over the field of real numbers then there exists $\sqrt{2} \in \mathbb{R}, f(\sqrt{2}) = 0$ and $\sqrt{2} \in (1,2)$.

Theorem 10.1.2: Every polynomial $f(x) \in \mathbb{R}[x]$ of odd degree has at least one real root.

Proof: Let $f(x)$ be a polynomial over $\mathbb{R}$ with odd degree n.

Without loss of generality, we may assume that $f(x)$ is a monic polynomial.

Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n;\ a_i \in \mathbb{R}, 1 \le i \le n$

Choose $c > 1$ and

$$c > \sum_{l=1}^{n} |a_i|$$

Consider

$$\left|\sum_{i=1}^{n} a_i c^{n-i}\right| \le \sum_{i=j}^{n} \left|a_i c^{n-i}\right|$$

$$\le \sum_{i=1}^{n} |a_i| c^{n-i}$$

Also,

$$c > 1$$

$$\Rightarrow c \le c^i;\ 1 \le i \le n$$

$$\Rightarrow \frac{1}{c^i} \le \frac{1}{c}$$

$$\Rightarrow c^{-i} \le c^{-1}$$

$$\Rightarrow c^{n-i} \le c^{n-1}\ \ \forall\ 1 \le i \le n$$

Therefore, we have

$$\left|\sum_{i=1}^{n} a_i c^{n-i}\right| \le \sum_{i=1}^{n} |a_i| c^{n-1}$$

$$= c^{n-1} \sum_{i=1}^{n} |a_i| \ldots (1)$$

Again,

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

$$= x^n + \sum_{i=1}^{n} a_i x^{n-i}$$

$$f(c) = c^n + \sum_{i=1}^{n} a_i c^{n-i}$$

$$\ge c^n - \left|\sum_{i=1}^{n} a_i c^{n-i}\right| \ldots\ldots (2)$$

From (1)

$$\left|\sum_{i=1}^{n} a_i c^{n-i}\right| \le c^{n-1} \sum_{1=1}^{n} |a_i|$$

$$\Rightarrow -\left|\sum_{i=1}^{n} a_i c^{n-i}\right| \ge -c^{n-1} \sum_{i=j}^{n} |a_i|$$

$$\Rightarrow c^n - \left|\sum_{i=1}^{n} a_i c^{n-i}\right| \geq c^n - c^{n-1}\sum_{i=1}^{n}|a_i|$$

From (2)

$$f(c) \geq c^n - \left|\sum_{i=1}^{n} a_i c^{n-i}\right|$$

$$\geq c^n - c^{n-1}\sum_{i=J}^{n}|a_i|$$

$$= c^n\left(1 - \frac{\sum_{i=1}^{n}|a_i|}{c}\right) \ldots (3)$$

Since

$$c > \sum_{i=1}^{n}|a_i|$$

$$\Rightarrow \frac{\sum_{i=1}^{n}|a_i|}{c} < 1$$

$$\Rightarrow 1 - \frac{\sum_{i=1}^{n}|a_i|}{c} > 0$$

Also, $c > 1, c^n > 1 > 0$

$$\Rightarrow c^n\left(1 - \frac{\sum_{i=1}^{n}|a_i|}{c}\right) > 0$$

From (3)

$$f(c) > 0$$

Again,

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

Since n is odd

$$= -x^n + a_1x^{n-1} + \cdots - a_{n-1}x + a_n$$

$$= -g(x)$$

where $g(x)$ is a monic polynomial given by

$$g(x) = x^n - a_1x^{n-1} + \cdots + (-a_{n-1}x) + a_n$$

Also,

$$f(c) > 0$$

$$\Rightarrow f\big(-(-c)\big) > 0$$

$$\Rightarrow -g(-c) > 0$$

$$\Rightarrow g(-c) < 0$$

and

$$g(c) > 0$$

By intermediate value theorem, there exists $b \in (-c, c)$ such that $f(b) = 0$

Therefore, f has a root in the interval $(-c, c)$ that is, f has at least one real root.

Theorem 10.1.3: Any quadratic equation over $\mathbb{C}$ has a root in $\mathbb{C}$.

Proof: Quadratic equation over the field of complex numbers is given by $f(x) = ax^2 + bx + c$ where $a, b, c \in \mathbb{C}$.

We know that roots of $f(x)$ are given by

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

That is,

$$-\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}$$

$$= -\frac{b}{2a} \pm \frac{\sqrt{D}}{2a};\ D = b^2 - 4ac$$

Claim: $\forall\ \boldsymbol{D} \in \mathbb{C}, \sqrt{\boldsymbol{D}} \in \mathbb{C}$

Since $D \in \mathbb{C}$

Let $D = u + iv$

Let $D = E^2;\ E = \alpha + i\beta$

$$\begin{aligned} u + iv &= (\alpha + i\beta)^2 \\ &= \alpha^2 - \beta^2 + 2i\alpha\beta \end{aligned}$$

Comparing real and imaginary parts

$$u = \alpha^2 - \beta^2, v = 2\alpha\beta$$

Consider

$$\begin{aligned} 4\alpha^4 - 4\alpha^2 u - v^2 &= 4\alpha^4 - 4\alpha^2(\alpha^2 - \beta^2) - (2\alpha\beta)^2 \\ &= 4\alpha^4 - 4\alpha^4 + 4\alpha^2\beta^2 - 4\alpha^2\beta^2 \\ &= 0 \end{aligned}$$

Therefore,

$$4\alpha^4 - 4\alpha^2 u - v^2 = 0$$

$$\alpha^2 = \frac{4u \pm \sqrt{16u^2 + 16}v^2}{8}$$

$$= \frac{1}{2}\left(u + \sqrt{u^2 + v^2}\right) \in \mathbb{R}$$

As $\alpha^2 > 0 \Rightarrow \alpha \in \mathbb{R}$

$$\Rightarrow \beta = \frac{v}{2\alpha} \in \mathbb{R}$$

$$\Rightarrow \sqrt{D} \in \mathbb{C}$$

$$\Rightarrow \alpha + i\beta \in \mathbb{C}$$

Therefore, we can observe that $\frac{-b \pm \sqrt{D}}{2a} \in \mathbb{C}$

Remark: Given $z = u + iv\ ; u, v \in \mathbb{R}$

$\bar{z} = u - iv$ is called conjugate of z and $|z| = \sqrt{u^2 + v^2}$ is called modulus of z.

$$\begin{aligned} z\bar{z} &= (u + iv)(u - iv) \\ &= u^2 + v^2 \end{aligned}$$

$$= |z|^2 > 0$$

$$z\bar{z} = 0 \quad \Leftrightarrow u^2 + v^2 = 0$$
$$\Leftrightarrow u = v = 0$$
$$\Leftrightarrow z = 0$$

Consider $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in \mathbb{C}[x]$

Then conjugate of $f(x)$ is defined as

$$\bar{f}(x) = \overline{\alpha_0} + \overline{\alpha_1} x + \cdots + \overline{\alpha_n} x^n \in \mathbb{C}[x]$$

Remark: If $z = \alpha + i\beta \in \mathbb{C}$

$$\bar{z} = \alpha - i\beta$$
$$\Rightarrow z + \bar{z} = 2\alpha \in \mathbb{R}$$

and

$z - \bar{z} = 2i\beta$ is always a purely imaginary number.

Let $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$

$\Rightarrow \bar{f}(x) = \overline{\alpha_0} + \bar{\alpha}_1 x + \cdots + \bar{\alpha}_n x^n$

$\Rightarrow f(x) + \bar{f}(x) = (\alpha_0 + \overline{\alpha_0}) + (\alpha_1 + \bar{\alpha}_1)x + \cdots + (\alpha_n + \bar{\alpha}_n)x^n \in \mathbb{R}[x]$

For any $z \in \mathbb{C}, \overline{f(z)} = \bar{f}(\bar{z})$

Theorem 10.1.4: For any non-constant polynomial $f(x) \in \mathbb{C}[x]$, the polynomial $g(x) = f(x)\bar{f}(x)$ has a root in $\mathbb{C}$ if and only if $f(x)$ has a root in $\mathbb{C}$.

Proof: For any non-zero polynomial $f(x) \in \mathbb{C}[x]$, the polynomial $g(x) = f(x)\bar{f}(x)$ has a root in $\mathbb{C}$

if and only if there exists $d \in \mathbb{C}$ such that $g(d) = 0$

$\Leftrightarrow f(d)\bar{f}(d) = 0$

$\Leftrightarrow f(d) = 0$ or $\bar{f}(d) = 0$

If $f(d) = 0 \Rightarrow d$ is a root of $f(x)$

If $\bar{f}(d) = 0$

$\Rightarrow \bar{f}(d) = \overline{\bar{f}(d)} = \bar{0} = 0$

$\Rightarrow f(\bar{d}) = 0$

$\Rightarrow \bar{d}$ is a root of $f(x)$.

Conversely, let $f(x)$ has a root $z \in \mathbb{C}$

That is, $f(z) = 0$

$g(z) = f(z)\bar{f}(z) = 0.\bar{f}(z) = 0$

$\Rightarrow z$ is a root of $g(z)$.

Hence, $g(z) = f(z)\bar{f}(z)$ has a root in $\mathbb{C}$ if and only if $f(z)$ has a root in $\mathbb{C}$.

Theorem 10.1.5: For any non-constant polynomial $f(x) \in \mathbb{C}[x]$, the polynomial $g(x) = f(x)\bar{f}(x) \in \mathbb{R}[x]$

Proof: Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$ be a polynomial of degree n over $\mathbb{C}$, then

$\bar{f}(x) = \overline{\alpha_0} + \overline{\alpha_1} x + \overline{\alpha_2} x^2 + \cdots + \overline{\alpha_n} x^n$

$$\Rightarrow f(x)\bar{f}(x) = (\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n)(\overline{\alpha_0} + \overline{\alpha_1} x + \cdots + \overline{\alpha_n} x^n)$$
$$= \alpha_0\overline{\alpha_0} + (\alpha_0\overline{\alpha_1} + \alpha_1\bar{\alpha}_0)x + (\alpha_0\bar{\alpha}_2 + \alpha, \overline{\alpha_1} + \alpha_2\overline{\alpha_0})x^2 + \cdots + \alpha_n\overline{\alpha_n}x^{2n} \cdots (1)$$

Also,

$$\begin{aligned}\alpha_0\overline{\alpha_0} &= |\overline{\alpha_0}|^2 \in \mathbb{R}\\ \alpha_0\overline{\alpha_1} + \alpha_1\overline{\alpha_0} &= \alpha_0\bar{\alpha}_1 + \overline{\alpha_0\overline{\alpha_1}}\\ &= |\alpha_0\overline{\alpha_1}|^2 \in \mathbb{R}\\ \alpha_0\overline{\alpha_2} + \alpha_1\overline{\alpha_1} + \alpha_2\overline{\alpha_0} &= (\alpha_0\overline{\alpha_2} + \overline{\alpha_0\overline{\alpha_2}}) + |\alpha_1|^2\\ &= |\alpha_0\overline{\alpha_2}|^2 + |\alpha_1|^2 \in \mathbb{R}\end{aligned}$$

Continuing so on, we get all the coefficients of $f(x)\bar{f}(x)$ are from $\mathbb{R}$ and hence $f(x)\bar{f}(x) \in \mathbb{R}[x]$.

1) Find the value of $\sqrt{4+5i}$.
2) Prove that a polynomial of degree 3 over the field of real numbers has at leastone real root.

10.2 Fundamental theorem of algebra

Theorem 10.2.1 (Fundamental Theorem of Algebra): Every polynomial $f(x) \in \mathbb{C}[x]$ with a positive degree has all the roots in $\mathbb{C}$.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$ such that $\deg f(x) = n \geq 1$

For $n = 1$

$$f(x) = a_0 + a_1x, a_1 \neq 0, a_1 \in \mathbb{C}$$

Then $x = a_1^{-1}a_0 \in \mathbb{C}$ is a root of $a_0 + a_1x$. Therefore, $a_0 + a_1x$ has all the roots in $\mathbb{C}$.

For $n > 1$

Let $g(x) = (x^2 + 1)f(x)\bar{f}(x)$ is a polynomial over the field of real numbers.

That is, $g(x) \in \mathbb{R}[x]$

Let E be the splitting field of $g(x)$ over $\mathbb{R}$.

Also, $\mathbb{R} \subseteq \mathbb{C} = \mathbb{R}(i) \subseteq E$

As, E is the splitting field of $g(x)$ over $\mathbb{R}$. Therefore, $\mathbb{R} \subseteq E$.

Also, i is the root of $g(x)$. i belong to the splitting field of $g(x)$ that is E.

Claim: There does not exist a subfield K of E containing $\mathbb{C}$ such that $[K: \mathbb{C}] = 2$.

Hence K is a finite, separable extension of $\mathbb{C}$. Therefore, K is a simple extension of $\mathbb{C}$. So, there exists $\alpha \in K$ such that $K = \mathbb{C}(\alpha)$.

If $p(x) \in \mathbb{C}[x]$ is minimal polynomial of α over $\mathbb{C}$ then $\deg p(x) = [K: \mathbb{C}] = 2$.

Suppose $p(x) = x^2 + 2ax + b;\ a, b \in \mathbb{C}$

Then

$$\begin{aligned}p(x) &= (x + a)^2 - (a^2 - b)\\ &= \left(x + a - \sqrt{a^2 - b}\right)\left(x + a + \sqrt{a^2 - b}\right)\end{aligned}$$

Since $a, b \in \mathbb{C}$

$\Rightarrow a^2 - b \in \mathbb{C} \Rightarrow \sqrt{a^2 - b} \in \mathbb{C}$

Again, $\pm\sqrt{a^2 - b}, a, 1 \in \mathbb{C}$

So, $x + a + \sqrt{a^2 - b}, x + a - \sqrt{a^2 - b} \in \mathbb{C}[x]$

$\Rightarrow p(x)$ is a reducible polynomial over $\mathbb{C}$ but $p(x)$ is a minimal polynomial and hence irreducible over $\mathbb{C}$.

Therefore, our supposition was wrong and hence the claim is established.

Let $G = G(E, \mathbb{R})$ be the Galois group of $g(x)$ over $\mathbb{R}$.

Let $O(G) = 2^m q, q$ is odd integer.

If $m = 0 \Rightarrow O(G) = q$ is odd but $G = G(E, \mathbb{R})$

$$\begin{aligned} O(G) &= [E: \mathbb{R}] \\ &= [E: \mathbb{C}][\mathbb{C}: \mathbb{R}];\ \mathbb{C} = \mathbb{R}(i) \\ &= 2[E: \mathbb{C}] \end{aligned}$$

This implies, $O(G)$ is even.

So, we arrive at a contradiction.

Hence $m \neq 0$.

2 divides $O(G) \Rightarrow O(G) = 2^m q; q$ is odd.

Let H be the Sylow 2- subgroup of G and $O(H) = 2^m$

Let L be the corresponding subfield of E.

Moreover, $O(H) = [E: L]$

Therefore, $[E: L] = 2^m$

Consider $[E: \mathbb{R}] = 2^m q$

$\Rightarrow [E: L][L: \mathbb{R}] = 2^m q$

$\Rightarrow 2^m [L: \mathbb{R}] = 2^m$

$\Rightarrow [L: \mathbb{R}] = q$

L is a finite, separable extension of $\mathbb{R}$. Therefore, there exists $\beta \in L$ such that $L = R(\beta)$.

The minimal polynomial $q(x)$ of $\mathbb{R}(\beta)$ over $\mathbb{R}$ is of degree q and q is odd.

$\Rightarrow q(x)$ has at least one real root

$\Rightarrow \exists$ some $\gamma \in \mathbb{R}$ such that $q(\gamma) = 0$.

$q(x) = (x - \gamma) q_1(x),\ q_1(x) \in \mathbb{R}[x]$ that is, $q(x)$ is a reducible polynomial over $\mathbb{R}$ but $q(x)$ being minimal polynomial is irreducible.

So, we arrive at a contradiction unless $q = 1$.

$[E: \mathbb{R}] = 2^m$

$\Rightarrow [E: \mathbb{C}][\mathbb{C}: \mathbb{R}] = 2^m$

$\Rightarrow [E: \mathbb{C}] = \dfrac{2^m}{2} = 2^{m-1}$

Then the subgroup $G(E, \mathbb{C})$ of $G(E, \mathbb{R})$ is of order 2^{m-1}.

If $m > 1$, let H' be the subgroup of E containing $\mathbb{C}$.

$\Rightarrow [E: L'] = 2^{m-2}$

$[E: \mathbb{C}] = 2^{m-1}, [E: L'] = 2^{m-2}$

$\Rightarrow [E: L'][L': \mathbb{C}] = [E: \mathbb{C}]$

$\Rightarrow 2^{m-2}[L': \mathbb{C}] = 2^{m-1}$

$\Rightarrow [L': \mathbb{C}] = 2$

So, we arrive at a contradiction to the claim we established.

Therefore, $m = 1$

and $[E:\mathbb{R}] = 2^m = 2 = [\mathbb{C}:\mathbb{R}]$

$\Rightarrow \mathbb{C} \subseteq E \Rightarrow \mathbb{C} = E$

So, $\mathbb{C}$ itself is splitting field of $g(x) = (x^2+1)f(x)\bar{f}(x)$

Therefore, $\mathbb{C}$ is the splitting field of $f(x)$.

Such fields F; all the roots of polynomials $f(x) \in F[x]$ are in F, are called algebraically closed.

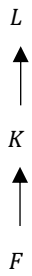
Let $F = \mathbb{R}$, then $x^2 + 1$ has both roots $\pm i \notin \mathbb{R}$, $\mathbb{R}$ is not algebraically closed.

10.3 Composite Field Extension

Definition 10.3.1 (Composite Extension): Let K_1 and K_2 are two extensions of a field F both contained in some field extension $\bar{F}$ of F then the composite extension of K_1 and K_2 is denoted as K_1K_2 and K_1K_2 is the smallest field extension of F such that it is generated by F and $K_1 \cup K_2$ that is,

$$K_1K_2 = F(K_1 \cup K_2) = K_2K_1$$

For field extension $F \subseteq K \subseteq L$



Composite field extension is given by

Result: Let K_1 be Galois extension of F and K_2 be a finite extension of F then K_1K_2 is Galois extension of K_2 and $G(K_1K_2, K_2)$ is isomorphic to a subgroup of $G(K_1, F)$.

Proof: K_1 is a finite, separable extension of field F and hence K_1 is a simple extension of F.

So, there exists some $a \in K_1$ such that $K_1 = F(a)$.

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

$a \in K_1$ is a root of $p(x) \in F[x]$ and $F \subseteq K_1$ is a normal extension.

Thus, $p(x)$ has all the roots in $K_1 = F(a) \subseteq K_2(a)$

Therefore, $K_2(a)$ is the splitting field of $p(x)$ over K_2 and

$$\begin{aligned} K_2(a) &= K_2\big(F(a)\big)(F \subseteq K_2) \\ &= K_2K_1 \\ &= K_1K_2 \end{aligned}$$

$\Rightarrow K_1K_2$ is the splitting field of $p(x)$ over K_2

$\Rightarrow$ K_1K_2 is a normal extension of K_2

Again, $p(x)$ has distinct roots as K_1 is a separable extension of F.

$\Rightarrow$ K_1K_2 is a Galois extension of K_2.

Define $\theta: G(K_1K_2, K_2) \to G(K, F)$ by $\theta(\sigma) = \sigma|K_1$ where $\sigma|K_1$ denotes the restriction of σ on K_1.

θ is a homomorphism

For $\sigma, \eta \in G(K_1K_2, K_2)$

$$\begin{aligned}\theta(\sigma\eta) &= \sigma\eta|K_1\\ &= (\sigma|K_1)(\eta|K_1)\\ &= \theta(\sigma)\theta(\eta)\end{aligned}$$

Therefore, θ is a homomorphism.

θ is one-one

Let $\sigma \in \ker\theta$

$\Leftrightarrow \theta(\sigma) = I$ where $I: K_1 \to K_1$ is the identity map.

$\Leftrightarrow \sigma(x) = x \; \forall \; x \in K_1$ and by definition of $G(K_1, F)$, we have $\sigma(x) = x \; \forall \; x \in F$

The domain of θ is $G(K_1K_2, K_2)$ and identity of D is σ such that $\sigma(x) = x \; \forall \; x \in K_1K_2$ but by definition of $G(K_1K_2, K_2)$; $\sigma(x) = x \; \forall \; x \in K_2$.

In particular, $\sigma \in \ker\theta$

$\Leftrightarrow \sigma(x) = x \; \forall \; x \in K_1$

For some $x \in K_1K_2$

$$\begin{aligned}\sigma(x) &= \sigma(k_1k_2);\, k_1 \in K_1,\; k_2 \in K_2\\ &= \sigma(k_1)\sigma(k_2)\\ &= k_1k_2\\ &= x\end{aligned}$$

Therefore, σ is identity map on K_1K_2.

Thus, $\ker\theta = \{I\}$

Hence, θ is one-one.

By Fundamental Theorem of Homomorphism

$$G(K_1K_2, K_2) \cong f\left(G(K_1K_2, K_2)\right)$$

Therefore, $f\left(G(K_1K_2, K_2)\right)$ is a subgroup of codomain $G(K, F)$.

$\Rightarrow G(K_1K_2, K_2)$ is isomorphic to a subgroup of $G(K_1, F)$.

Theorem 10.3.2: Let K_1 be a Galois extension of F and K_2 be any finite extension of F. Then $[K_1K_2: K_2]$ divides $[K_1: F]$.

Proof: K_1 is a Galois extension of F and K_2 is any finite extension of F

In this case, $G(K_1K_2, K_2)$ is isomorphic to a subgroup of $G(K_1, F)$.

$\Rightarrow O\left(G(K_1K_2, K_2)\right)$ divides $O\left(G(K_1, F)\right)$ ... ... (1)

Since K_1 is Galois extension of F therefore, K_1K_2 is also a Galois extension of K_2.

By the Fundamental theorem of Galois extension,

$O\left(G(K_1K_2, K_2)\right) = [K_1K_2: K_2]$ and $O\left(G(K_1, F)\right) = [K_1: F]$ ... ... (2)

Using (1) and (2), we have, $[K_1K_2: K_2]$ divides $[K_1: F]$.

If $K_1$is not Galois extension of F then $[K_1K_2: K_2]$ need not divide $[K_1: F]$.

Solution: Consider $K_1 = \mathbb{Q}(\sqrt[3]{2}\omega), F = \mathbb{Q}$

ω is the primitive cube root of unity

Consider $x^3 - 2 \in \mathbb{Q}[x]$ then roots of $x^3 - 2$ are $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$.

Now $\sqrt[3]{2}\omega \in K_1$

If possible, let $\sqrt[3]{2}\omega^2 \in K_1$

$\Rightarrow \omega \in K_1$

$\Rightarrow K_1 = F(\sqrt[3]{2}, \omega)$ and $[K_1: F] = 6$

If $K_1 = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$f(x) = x^3 - 2$, by Eisenstein criteria is an irreducible monic polynomial over $\mathbb{Q}$ having a root $\sqrt[3]{2}$. Therefore, $x^3 - 2$ is minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

Thus, $[\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}] = 3$

If possible, let $\omega \in \mathbb{Q}(\sqrt[3]{2})$

$\Rightarrow \omega = \alpha + \beta\sqrt[3]{2}\ ;\ \alpha, \beta \in \mathbb{Q}$

$\Rightarrow \omega - \beta\sqrt[3]{2} = \alpha$

$\Rightarrow \omega^3 - 2\beta^3 - 3\omega^2\beta\sqrt[3]{2} + 3\sqrt[3]{4}\beta\omega = \alpha^3$

$\Rightarrow 1 - 2\beta^3 - \alpha^3 = \sqrt[3]{2}(3\omega^2\beta - 3\sqrt[3]{2}\omega\beta)$

$\Rightarrow 1 - 2\beta^3 - \alpha^3 = 3\sqrt[3]{2}\omega\beta(\omega - 1)$

$\Rightarrow \omega \notin \mathbb{Q}(\sqrt[3]{2})$

So, $[\mathbb{Q}(\sqrt[3]{2}, \omega): \mathbb{Q}(\sqrt[3]{2})] \geq 2$

But $x^2 + x + 1$ is a monic polynomial over $\mathbb{Q}(\sqrt[3]{2})$ having a root ω.

$[\mathbb{Q}(\sqrt[3]{2}, \omega): \mathbb{Q}(\sqrt[3]{2})] \leq 2$

$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}, \omega): \mathbb{Q}(\sqrt[3]{2})] = 2$

Therefore, $[\mathbb{Q}(\sqrt[3]{2}, \omega): \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega): \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}] = 2 \times 3 = 6$

But $x^3 - 2$ is an irreducible polynomial of degree 3 over $\mathbb{Q}$ and hence it is minimal polynomial of $\sqrt[3]{2}\omega$ over $\mathbb{Q}$.

Therefore, $[K_1: \mathbb{Q}] = 3 \neq 6$

Thus, we arrive at a contradiction.

There exists a polynomial $x^3 - 2 \in \mathbb{Q}[x]$ such that it has one root $\sqrt[3]{2}\omega \in K_1$ but not all the roots are in K_1.

Therefore, K_1 is not a normal extension of F and hence not a Galois extension either.

Also, $[K_1: \mathbb{Q}] = 3$

Let $K_2 = \mathbb{Q}(\sqrt[3]{2})$ then K_2 is a finite extension of $\mathbb{Q}$.

$K_1K_2 = \mathbb{Q}(\sqrt[3]{2}\omega)\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$[K_1K_2: K_2] = 2$

$x^2 + \sqrt[3]{2}x + \sqrt[3]{2}$ is the minimal polynomial of $\sqrt[3]{2}\omega$ over K_2.

2 does not divide 3

That is, $[K_1K_2: K_2]$ need not divide $[K_1: F]$.

Summary

- The theory of roots of polynomials is discussed.
- The square root of every complex number exists in the field of complex numbers is proved.
- The Fundamental Theorem of Algebra is proved.
- The importance of the Fundamental Theorem of Algebra is discussed.
- The composite extension is defined.
- Composite Galois extension is explained with the help of an example.

Keywords

- Roots of polynomial
- Fundamental Theorem of Algebra
- Composite Galois Extension

Self Assessment

1: For every real number $b, \sqrt{b}$ is

A: A real number

B: A rational number

C: A complex number

D: A purely imaginary number

2: Let $f(x)$ is a polynomial of degree 3 over $\mathbb{R}$ then

A: $f(x)$ has no real root

B: $f(x)$ has exactly one real root

C: $f(x)$ has at least one real root

D: $f(x)$ has at least one positive real root.

3: Let $f(x)$ is a polynomial of degree 10 over $\mathbb{R}$ such that $f(x)$ has at least one real root. Then

A: $f(x)$ has 3 real roots

B: $f(x)$ has 2 real roots

C: $f(x)$ has an even number of real roots

D: $f(x)$ has an odd number of real roots.

4: $\sqrt{9 + 40i} =$

A: $5 + 4i$

B: $5 - 4i$

C: $4 + 5i$

D: $4 - 5i$

5: Square of a purely imaginary number is

A: Always real and positive

B: Always real and negative

C: Never a real number

D: May or may not be real

6: For $f(x) \in \mathbb{C}[x]$, then $g(x) = f(x) + \bar{f}(x)$

A: has all roots real

B: has all roots imaginary

C: has all coefficients real

D: has all the coefficients purely imaginary

7: For $f(x) \in \mathbb{C}[x]$, then $g(x) = f(x)\bar{f}(x)$

A: has all roots real

B: has all coefficients real

C: has all roots imaginary

D: has all the coefficients purely imaginary

8: All the roots of a polynomial $f(x) \in \mathbb{C}[x]$ are

A: Real

B: Purely imaginary

C: Complex

D: Zero

9: $[\mathbb{R}(i): \mathbb{R}] =$

A: 1

B: 2

C: 3

D: 4

10: Composite extension of field extensions K_1 and K_2 of a field $F$is

A: Generated by F

B: Generated by $K_1 \cup K_2$

C: Generated by F and $K_1 \cup K_2$

D: Generated by K_1K_2

11: Let K_1 is Galois extension of F and K_2 is a finite extension of F then K_1K_2 is

A: Galois extension of K_1

B: Galois extension of K_2

C: Galois extension of K_1K_2

D: Galois extension of $K_1 \cup K_2$

12: Galois extension of a field F is

A: Finite

B: Separable

C: Simple

D: All are correct

13: Let K_1 is Galois extension of F and K_2 be any finite extension of F. Then

A: $[K_1K_2: K_2] \leq [K_1: F]$

B: $[K_1K_2: K_2] \geq [K_1: F]$

C: $[K_1K_2: K_2] = [K_1: F]$

D: $[K_1K_2: K_2] > [K_1: F]$

14: Let $K_1 = \mathbb{Q}(\sqrt[3]{2}\omega)$ and $F = \mathbb{Q}$ then $[K_1: F] =$

A: 2

B: 3

C: 4

D: 6

15: Let $K_1 = \mathbb{Q}(\sqrt[3]{2}\omega)$and $K_2 = \mathbb{Q}(\sqrt[3]{2})$ then $[K_1K_2: K_2]$

A: 1

B: 2

C: 3

D: 4

Answers for Self Assessment

1.	C	2.	C	3.	C	4.	A	5.	B
6.	C	7.	B	8.	C	9.	B	10.	C
11.	B	12.	D	13.	A	14.	B	15.	D

Review Questions

1) In $\mathbb{Q}(\sqrt{2})$ express the following elements as polynomials in $\sqrt{2}$
   a) $\frac{1}{2+\sqrt{2}}$
   b) $\frac{3+\sqrt{2}}{5+\sqrt{8}}$
2) Show that if a polynomial $f(x)$ over the field of real numbers has a root $a + ib$ then $a - ib$ is also a root of $f(x)$.
3) Let K_1 be a Galois extension of F and K_2 be any finite extension of F. Then prove that $[K_1: F]$is a multiple of $[K_1K_2: K_2]$.
4) Give an example of a polynomial over the field of real numbers with exactly two real and two complex roots.

5) Give an example of a polynomial over the field of real numbers with exactly two purely imaginary roots.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 11: Normal Closure of an Algebraic Extension

CONTENTS

Objective

After studying this unit, you will be able to

- define normal closure of a field extension
- understand normal closure with the help of examples

Introduction

In this unit, we will define the normal closure of a field extension and understand it with the help of various examples.

11.1 Definition and Examples

Definition 11.1.1: Let K is a field and L is an algebraic extension of K then there is some algebraic extension M of L such that M is a normal extension of K and up to isomorphism there is only one such extension which is minimal. The only subfield of M which contains L and which is a normal extension of K is M itself. This extension is called normal closure of algebraic extension L of K.

: Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ then splitting field of $f(x)$ is $\mathbb{Q}(\sqrt{2})$. Then its normal closure is $\mathbb{R}$.

: Let $f(x) = (x^2 - 2)(x^2 - 3)$ then roots of $f(x)$ are $\pm\sqrt{2}, \pm\sqrt{3}$.

Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a field extension such that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $f(x)$.

$\mathbb{Q}(\sqrt{2})$ is a field extension of $\mathbb{Q}$ and $\sqrt{2} \notin \mathbb{Q}$.

Therefore,

$$[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] \geq 2$$

Also, $x^2 - 2$ is the polynomial over $\mathbb{Q}$ having root $\sqrt{2}$that is,

$$[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] \leq 2$$

We can conclude that

$$[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] = 2 \ldots (1)$$

Now $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

Otherwise

If $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$

$$\begin{aligned} \sqrt{3} &= p + q\sqrt{2}; p, q \in \mathbb{Q} \\ \Rightarrow 3 &= p^2 + 2q^2 - 2\sqrt{2}pq \\ \Rightarrow 3 - p^2 - 2q^2 &= -2\sqrt{2}pq \end{aligned}$$

This is not possible as the left side is a rational number and the right side is purely irrational.

This implies, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

$$\Rightarrow [\mathbb{Q}(\sqrt{3}, \sqrt{2}): \mathbb{Q}(\sqrt{2})] \geq 2$$

Again, $x^2 - 3$ is the polynomial over $\mathbb{Q}(\sqrt{2})$ having a root $\sqrt{3}$.

$$\Rightarrow [\mathbb{Q}(\sqrt{3}, \sqrt{2}): \mathbb{Q}(\sqrt{2})] \leq 2$$

This implies,

$$[\mathbb{Q}(\sqrt{3}, \sqrt{2}): \mathbb{Q}(\sqrt{2})] = 2$$

Hence

$$\begin{aligned} [\mathbb{Q}(\sqrt{3}, \sqrt{2}): \mathbb{Q}] &= [\mathbb{Q}(\sqrt{3}, \sqrt{2}): \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}): \mathbb{Q}] \\ &= 2 \times 2 \\ &= 4 \end{aligned}$$

Then we have three extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Note that each of the three $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$is having the same degree of extension over $\mathbb{Q}$

:Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ then its roots are $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$where $\omega = \frac{-1+\sqrt{3}i}{2}$ and $\omega^2 = \frac{-1-\sqrt{3}i}{2}$

$\mathbb{Q}(\sqrt[3]{2}, \omega)$ and $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ both can be treated as splitting fields of $f(x)$.

Consider the field $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$

Then $x^3 - 2$ is an irreducible polynomial over $\mathbb{Q}$, it is monic and having $\sqrt[3]{2}$ as a root.

Therefore, the minimal polynomial of $\sqrt[3]{2}$ is a divisor of $x^3 - 2$. But the polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$. Hence, it cannot have a proper factor. Therefore, $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

$$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}] = 3$$

Again $\sqrt{3}i \notin \mathbb{Q}(\sqrt[3]{2})$

Therefore,

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i): \mathbb{Q}(\sqrt[3]{2})] \geq 2$$

Also, $x^2 + 3$is an irreducible polynomial over $\mathbb{Q}$, it is monic and having $\sqrt{3}i$ as a root.

Hence,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right] \leq 2$$

This implies,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$$

So,

$$\begin{aligned}\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\right] &= \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right): \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right): \mathbb{Q}\right] \\ &= 3 \times 2 \\ &= 6\end{aligned}$$

It can be in the following four ways

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{3}i\right) \subseteq \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right)$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\theta_1) \subseteq \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right)$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\theta_2) \subseteq \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right)$$

and

$$\mathbb{Q} \subseteq \mathbb{Q}(\theta_3) \subseteq \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}i\right)$$

Where $\theta_1 = \sqrt[3]{2}$,

$\theta_2 = \sqrt[3]{2}\omega$ and

$\theta_3 = \sqrt[3]{2}\omega^2$.

:

1) For any field F if $f(x)$ is a polynomial over the field F then there exists an extension K of F such that $f(x)$ splits completely in K which proves that a normal closure of an algebraic extension always exists.
2) If K is an algebraic extension of F which is splitting field over F for a collection of polynomials $f(x) \in F[x]$ then it is normal closure of F.
3) If $f(x) \in F[x]$ and $f(x)$ is of degree n then adjoining one root of $f(x)$ to F generates an extension F_1 of degree at the most n. This implies $f(x)$ has a root α in any field extension F_1 of F. Then

   $$F_1 = F(\alpha)$$

   Then α is a root of $f(x)$. Further, if $f(x)$ is the minimal polynomial of α over F, then

   $$[F(\alpha): F] = n$$

   But if it is not, then

   $$[F(\alpha): F] < n$$

   In general, we can say

   $$[F(\alpha): F] \leq n \ldots (1)$$

   Now in F_1,

   $$f(x) = (x - \alpha) f_1(x)$$

   $\Rightarrow \deg f(x) = \deg(x - \alpha) + \deg f_1(x)$

   $\Rightarrow \deg f(x) = 1 + \deg f_1(x)$

   $\Rightarrow \deg f_1(x) = n - 1$

   For a root β of $f_1(x)$, in the same way, we can find $F_2 = F_1(\beta)$

and

$$[F_2 : F_1] \leq n - 1 \cdots (2)$$

Continuing so on…

If K is the splitting field of $f(x)$.

$$\begin{aligned}[K : F] &= [K : F_n] \cdot \cdots [F_2 : F_1][F_1 : F] \\ &\leq 1 \times 2 \times 3 \times \cdots \times n - 1 \times n \\ &= n! \text{ (From (1) and (2))}\end{aligned}$$

Summary

- The normal closure of a field extension is defined.
- Normal closure is explained with the help of examples

Keywords

- Field extension
- Splitting field
- Normal closure of a field extension

Self Assessment

1: Let L be an algebraic extension of the field K. Then M is called normal closure of this algebraic extension if

A: M is a subfield of L containing K

B: M is a subfield of K

C: M is any field extension of L

D: M is the unique (up to isomorphism) field extension of L such that it is a normal extension of K.

2: Let $K \subseteq L$ be an algebraic extension such that M is the normal closure of this extension. Let $f(x) \in K[x]$ be a polynomial of degree 3 having at least one root in M. Then M contains …. number of roots of $f(x)$

A: 0

B: 1

C: 2

D: 3

3: Let $K \subseteq L$ be an algebraic extension such that M is the normal closure of this extension. Then the number of fields N properly contained in M such that N is a normal extension of K is

A: 0

B: 1

C: 2

D: 3

4: Splitting field of $f(x) = x^2 + 3 \in \mathbb{Q}[x]$ is

A: $\mathbb{Q}(\sqrt{3})$

B: $\mathbb{Q}(i)$

C: $\mathbb{Q}(\sqrt{3}, i)$

D: $\mathbb{C}$

5: Consider $f(x) = (x^2 - 5)(x^2 - 3) \in \mathbb{Q}[x]$. Then splitting field K of $f(x)$ and $[K: \mathbb{Q}]$ is

A: $K = \mathbb{Q}(\sqrt{5}, \sqrt{3})$ and $[K: \mathbb{Q}] = 4$

B: $K = \mathbb{Q}(\sqrt{5}, \sqrt{3})$ and $[K: \mathbb{Q}] = 6$

C: $K = \mathbb{Q}(\sqrt{5})$ and $[K: \mathbb{Q}] = 2$

D: $K = \mathbb{Q}(\sqrt{3})$ and $[K: \mathbb{Q}] = 2$

6: Let $F \subseteq K$ be a field extension then

A: $[K: F] = 1$ if and only if $K = F$

B: $[K: F] > 1$ if and only if $K \neq F$

C: $a \in F$ if and only if $F(a) = F$

D: All the options are correct

7: Let $F \subseteq K$ be a field extension and $f(x) \in F[x]$ is a polynomial such that $f(a) = 0$ for some $a \in K$ and $p(x)$ is the minimal polynomial of a over F then

A: $f(x) = p(x)$

B: $f(x)$ divides $p(x)$

C: $p(x)$ divides $f(x)$

D: $p(x)$ is never equal to $f(x)$

8: Degree of extension $[\mathbb{Q}(\omega): \mathbb{Q}]$ where $\omega = \frac{1+\sqrt{3}i}{2}$ is

A: 1

B: 2

C: 3

D: 4

9: A normal closure of an algebraic extension

A: may not exist

B: always exists and is unique

C: always exists but not unique

D: always exists but may or may not be unique

10: Normal closure of $\mathbb{Q} \subseteq \mathbb{R}$ is

A: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

B: $\mathbb{Q}(\sqrt{2}, i)$

C: $\mathbb{C}$

D: $\mathbb{Q}(i)$

11: Let $F \subseteq K$ is a field extension then for $a, b \in K$,

$Statement\ I$: $[F(a): F] = [F(b): F]$

$Statement\ II$: $a = b$

A: Statement I implies II

B: Statement II implies I

C: Statement I and II are equivalent

D: Statement I is always true for any $a, b \in K$

12: Which of the following is true?

A: $\left[\mathbb{Q}(\sqrt{2}): \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}\right]$

B: $[\mathbb{Q}(\mathrm{i}): \mathbb{Q}] = [\mathbb{C}: \mathbb{R}]$

C: $\left[\mathbb{Q}(\sqrt{5}): \mathbb{Q}\right] = 5$

D: $[\mathbb{C}: \mathbb{R}] = \infty$

13: Let $F \subseteq K$ be a field extension and $f(x) \in F[x]$ is a polynomial of degree 4 such that $f(a) = 0$ for some $a \in K$. Then the degree of the minimal polynomial of a over F is

A: $= 4$

B: < 4

C: ≤ 4

D: > 4

14: Splitting field of $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ is

A: $\mathbb{Q}$

B: $\mathbb{Q}(\mathrm{i})$

C: $\mathbb{R}$

D: $\mathbb{C}$

15: Splitting field of $f(x) = x^2 + 1 \in \mathbb{R}[x]$ is

A: $\mathbb{Q}$

B: $\mathbb{Q}(\mathrm{i})$

C: $\mathbb{R}$

D: $\mathbb{C}$

Answers for Self Assessment

1.	D	2.	D	3.	A	4.	C	5.	A
6.	D	7.	C	8.	B	9.	B	10.	C
11.	B	12.	B	13.	C	14.	B	15.	D

Review Questions

1) Find the normal closure of splitting field of the polynomial $f(x) = x^2 - 3 \in \mathbb{Q}[x]$.
2) Find the normal closure of splitting field of the polynomial$f(x) = (x^2 - 5)(x^2 - 7) \in \mathbb{Q}[x]$.

Further Readings

Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress

Topics in algebra by I.N. Hartstein, Wiley

Abstract algebra by David S Dummit and Richard M Foote, Wiley

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 12: Radical Extensions

CONTENTS

Objective

After studying this unit, you will be able to

- define radical and simple radical extension
- understand results about radical and simple radical extensions
- relate Galois radical extensions to its Galois group
- find radical extension corresponding to a Galois extension
- define polynomials solvable by radicals
- understand important results about polynomials solvable by radicals
- relate the concept to the symmetric group

Introduction

In this unit, radical and simple radical extensions are defined. Some important results about these extensions are discussed. The Galois radical extension is related to its Galois group. Further, polynomials solvable by radicals are defined and explained with the help of examples. A symmetric group is defined.

12.1 Radical Extension

Definition 12.1.1 (Simple Radical Extension): Let F be a field. A finite field extension K of F is called a simple radical extension if $K = F(\alpha)$; $\alpha \in K$ such that $\alpha^n \in F$ for some $n \in \mathbb{Z}$. If characteristic $F = p$ then $GCD\ (p, n) = 1$.

: Let $F = \mathbb{R}$ is the field of real numbers then $\mathbb{C} = \mathbb{R}(i)$; $i^2 = -1 \in \mathbb{R}$. Hence $\mathbb{C}$ over $\mathbb{R}$ is a simple radical extension.

Definition 12.1.2 (Radical Extension): A field extension $K$of a field F is said to be a radical extension if there exist subfields K_i of K containing $F(1 \leq i \leq m)$ such that

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$$

such that $K_{i+1} = K_i(\alpha_i)$; $\alpha_i \in K_{i+1}$ and $\alpha_i^{m_i} \in K_i$; $m_i \in \mathbb{Z}$.

That is, each K_{i+1} is a simple radical extension of K_i.

Theorem 12.1.3: A simple radical and a radical extension are always separable extensions.

Proof: We will consider two cases:

Case I: Let K is a simple radical extension of field F.

$\Rightarrow K = F(\alpha)$ for some $\alpha \in K$ such that $\alpha^n \in F$ for some natural number n.

$\Rightarrow \alpha$ is a root of the polynomial $x^n - \beta \in F[x];\ \beta = \alpha^n \in F$

Let $f(x) = x^n - \beta$

$\Rightarrow f'(x) = nx^{n-1}$.

Now either characteristic $F = 0$ or p and $GCD(n, p) = 1$

This implies, p does not divide n.

$\Rightarrow f'(x) \neq 0$

$\Rightarrow f(x)$ has no repeated roots in any field extension of F.

This implies, the minimal polynomial of α over F divides $f(x)$.

$\Rightarrow K$ is a separable extension over F.

Case II: Let K is a radical extension of F.

$\Rightarrow$ There exist $K_i;\ 0 \leq i \leq m$ such that

$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$ where $k_{i+1} = k_i(\beta_i);\ \beta_i^{m_i} \in K_i;\ 1 \leq i \leq m$

By case I, K_{i+1} is a separable extension of K_i for every i.

$$K_{i+1} = K_i(\beta_i)$$

$$K_{i+2} = K_{i+1}(\beta_{i+1}) = K_i(\beta_i, \beta_{i+1})$$

Since K_{i+1} is separable over K_i and K_{i+2} is separable over K_{i+1} and both β_i and β_{i+1} are separable over F.

$\Rightarrow K_{i+2} = K_i(\gamma_i)$ is a separable extension.

Continuing so on, we get that K_i is a separable extension of $F \forall\ 0 \leq i \leq m$.

$\Rightarrow K$ is a separable extension of F.

Theorem 12.1.4: Let K is a radical extension of L and L is a radical extension of F then K is a radical extension of F.

Proof: Since K is a radical extension of L.

This implies there exist subfields K_i of K containing F such that

$$L = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = K \ldots\ldots (1)$$

such that

$$K_{i+1} = K_i(\alpha_i);\ \alpha_i \in K_{i+1};\ \alpha_i^{n_i} \in K_i;\ n_i \geq 1$$

Moreover, if characteristic $L = p > 0$ then $GCD\ (p, n_i) = 1\ \forall\ 0 \leq i \leq m$.

Again, L is a radical extension of F, there exist subfields L_i of L such that

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_s = L \ldots\ldots (2)$$

such that

$$L_{j+1} = L_j(\beta_j);\ \beta_j \in L_{j+1};\ \beta_j^{m_j} \in L_j;\ m_j \geq 1$$

if characteristic $L = p > 0$ then $GCD\ (p, m_j) = 1\ \forall\ 0 \leq j \leq m$.

From (1) and (2)

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_s = L = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = K$$

and this series satisfies all the axioms of being a radical extension.

Therefore, K is a radical extension of the field F.

Theorem 12.1.5: Composite extension of two radical extensions is a radical extension of F.

Proof: Let K_1 and K_2 be two radical extensions of a field F.

Since K_2 is a radical extension of F therefore, there exist subfields N_i of K_2 such that

$$F = N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_m = K_2$$

Where $N_{i+1} = N_i(\alpha_i);\ \alpha_i^{n_i} \in N_i; n_i \geq 1$

Consider the series

$$K_1 = K_1F = K_1N_0 \subseteq K_1N_1 \subseteq \cdots \subseteq K_1N_m = K_1K_2$$

Note that

$$K_1N_{i+1} = K_1N_i(\alpha_i)$$

Since $\alpha_i^{n_i} \in N_i$ and $N_i \subseteq K_1N_i$. This implies $\alpha_i^{n_i} \in K_1N_i$

$\Rightarrow K_1K_2$ has the subfields such that K_1N_{i+1} is a simple radical extension of $K_1N_i\ \forall\ i$.

Also, $K_1N_m = K_1K_2$

Thus,

$K_1 = K_1F = K_1N_0 \subseteq K_1N_1 \subseteq \cdots \subseteq K_1N_m = K_1K_2$ is a series of subfields of K_1K_2 such that K_1N_{i+1} is a simple radical extension of K_1N_i.

Theorem 12.1.6: Let Kbe a radical extension of F then there exists a field $K \subseteq L$ such that L is a radical Galois extension of F.

Proof: Let K be a radical extension of F such that $[K:F] = n$

We will prove this result by using the Principle of Mathematical Induction on n

For $n = 1$

We have $[K:F] = 1$

$\Rightarrow K = F$

We can take $L = F$. Hence, we are thorough in this case.

For $n = 1$, the result is true.

Let us suppose that the result is true for field extension of degree less than n.

Since K is a radical extension of F, there exists a radical extension K_1 of F such that K is a simple radical extension of F.

$\Rightarrow K = K_1(\alpha), \alpha^m = \beta \in K_1$

Therefore, $[K_1:F] < [K:F] = n$

By the induction hypothesis, there exists a Galois radical extension L_1 of F such that $K_1 \subseteq L_1$.

Let $G = G(L_1, F)$

and

$$f(x) = \prod_{\sigma \in G}\left(x^m - \sigma(\beta)\right)$$

Then $\forall\ \tau \in G$

$$\tau\left(f(x)\right) = \tau\left(\prod_{\sigma \in G}\left(x^m - \sigma(\beta)\right)\right)$$

$$= \left(\prod_{\sigma \in G} \tau\left(x^m - \sigma(\beta)\right)\right)$$

$$= \left(\prod_{\sigma \in G} \left(x^m - \tau\left(\sigma(\beta)\right)\right)\right)$$

$$= \left(\prod_{\sigma \in G} \left(x^m - \left(\sigma(\beta)\right)\right)\right)$$

$$= f(x)$$

Therefore, $\tau\left(f(x)\right) = f(x)$

$f(x) \in F[x] \subseteq L_1[x]$

Let L be the splitting field of $f(x)$ over L_1.

Since for each σ, splitting field of $x^m - \sigma(\beta) \in L_1[x]$ is a radical extension of L_1.

Note that $\beta = \alpha^m \Rightarrow \sigma(\beta) = \left(\sigma(\alpha)\right)^m$

Therefore, splitting field L of $f(x)$ is also a radical extension of L_1.

$Also, L_1$ is a radical extension of F implies L is a radical extension of F.

Now, L_1 is the splitting field of some polynomial $g(x) \in F[x]$.

Also, L is the splitting field of some polynomial $f(x) \in L_1[x]$this implies, L is the splitting field of polynomial $f(x)g(x) \in F[x]$. Hence, L is a normal and Galois extension of F.

Also, L contains all the roots of $f(x)$, therefore, $K_1 \subseteq L_1$ can be extended to an $F-$ isomorphism of $K = K_1(\alpha)$ into L.

Therefore, L is Galois radical extension of F such that$K \subseteq L$.

1) Give an example of a field F having two different simple radical extensions with the same degree of extension.

2) Give an example of a field F having two different simple radical extensions with different degrees of extension.

12.2 Radical extension and Galois group

Theorem 12.2.1: Let K is Galois radical extension of F. Then $G(K, F)$ is a solvable group.

Proof: Since K is a radical extension of F, there exist subfields

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$$

Such that $K_{i+1} = K_i(\alpha_i);\ \alpha_i^{n_i} = \beta_i \in K_i, GCD(n_i, p) = 1\ \forall\ 1 \leq i \leq m$

Let $n = n_1 n_2 \ldots n_{m-1}$

Claim:$GCD(n, p) = 1$

Let $d = GCD(n, p)$

$\Rightarrow d|n$ and $d|p$

$\Rightarrow d|n_1 n_2 \ldots n_m$.

If $d > 1$ then there exists a prime number d_1 such that $d_1|d$

$\Rightarrow d_1|n_1 n_2 \ldots n_m$

$\Rightarrow d|n_i$ for at least one $1 \leq i \leq m$

Also, $d_1|p$

Therefore, $d_1|GCD(n_i, p) = 1$

$\Rightarrow d_1|1$ Which is contradictory to the fact that d_1 is a prime number.

So, our assumption was wrong.

$\Rightarrow d = 1$

Hence the claim is established.

Again as K is Galois extension of F, therefore, K is splitting field of separable polynomial $f(x) \in F[x]$.

Let $K \subseteq L$ is the splitting field of $\phi(x) = (x^n - 1)f(x) \in F[x]$.

Then L is a splitting field of $\phi(x)$ over K. $\phi(x)$ is a separable polynomial over F.

This implies that L is a separable extension of K.

Also, K is a separable extension of F.

Hence, L is a separable extension of F.

This further implies that L is a Galois extension of F.

Let L' be the subfield of L generated by F and roots of polynomial $x^n - 1$.

Let L_i be the subfield of L generated by L' and K_i; $0 \leq i \leq m$

Then $L_0 = L'F = L'$

and $L_m = L'K_m = L'K = L$

Note that

$$\begin{aligned} L_{i+1} &= L'K_{i+1} \\ &= L'K_i(\alpha_i) \\ &= L_i(\alpha_i);\ 0 \leq i \leq m-1 \end{aligned}$$

Since L' contains all the $n - th$ roots of unity, therefore, it contains all the $n_i - th$ roots of unity.

This is due to the fact that for any a such that a is the $n_i - th$ root of unity that is $a^{n_i} = 1$

$\Rightarrow (a^{n_i})^{n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_m} = 1$

$\Rightarrow a^n = 1$

This implies, a is $n - th$ root of unity.

Therefore, L_{i+1} is a cyclic extension of L_i $\forall\ 0 \leq i \leq m-1$ ... (1)

Claim: $G = G(L, F)$ is solvable.

Let G_i be the subgroups of G having L_i as fixed fields $\forall\ 0 \leq i \leq m$.

Then

$G_0 = G(L, L') \supseteq G_1 \supseteq \cdots \supseteq G_m = \{e\}$ ... (2)

$G_i = G(L, L_i)\ \forall\ 1 \leq i \leq m-1$

$G_m = G(L, L_m) = G(L, L)$

Since L_{i+1} is a cyclic and hence normal extension of L_i, therefore, G_{i+1} is a normal subgroup of G_i and

$$G_i/G_{i+1} \cong G(L_{i+1}, L_i)$$

$\Rightarrow G_i\ /\ G_{i+1}$ is cyclic and hence abelian.

(2) is a subnormal series with abelian factor groups.

$\Rightarrow G_0 = G(L, L')$ is a solvable group. Now $G(L', F)$ is abelian as it is isomorphic to a subgroup of the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$.

$\Rightarrow G(L', F)$ is a solvable group.

Also,

$$G(L,F)/G(L,L') \cong G(L',F)$$

Thus, $G(L,F)$ is solvable.

Again,

$$G(K,F) \cong G(L,F)/G(L,K)$$

Therefore, $G(K,F)$ is also a solvable group.

Theorem 12.2.2: Let K be a Galois extension of F of degree n such that n and p are coprime. If $G = G(K,F)$ is a solvable group, then there exists a radical extension L of F such that $K \subseteq L$.

Proof: We prove this result by using the Principle of Mathematical Induction on n.

For $n = 1$,

Taking $K = F = L$, we get that the result is true for $n = 1$.

Let $n > 1$

$G = G(K,F)$ is solvable and we know that a finite group is solvable if and only if for each composition series of G, the factor groups are cyclic of prime order. Therefore, there exists a normal subgroup G_1 of G such that G/G_1 is cyclic and

$$O\left(\frac{G}{G_1}\right) = m$$

Where m is a prime number.

Let K_1 be the fixed field of G_1. Then by the Fundamental Theorem of Galois theory, K_1 is Galois extension of F and

$$G(K_1,F) \cong G(K,F) \,/\, G(K,K_1)$$

That is,

$$G(K_1,F) \cong G/G_1$$

Therefore,

$$O\big(G(K_1,F)\big) = m$$

Let L_1 be the splitting field of $x^m - 1 \in K[x]$.

Since $m|n, x^m - 1$ is a separable polynomial.

Also, K is a Galois extension of F. Therefore, K is the splitting field of $f(x) \in F[x]$.

$\Rightarrow L_1$ is the splitting field of $f(x)(x^m - 1) \in F[x]$ and both $f(x)$ and $x^m - 1$ are separable polynomials.

$\Rightarrow L_1$ is a Galois extension of F.

Now,

$$F \subseteq F(\omega) \subseteq K_1(\omega) \subseteq K(\omega) = L_1$$

where ω is the $m - th$ root of unity and L_1 is a Galois extension of F.

$\Rightarrow L_1$ is Galois extension of $K_1(\omega)$.

$G\big(L_1, K_1(\omega)\big) = G\big(K(\omega), K_1(\omega)\big)$ is isomorphic to a subgroup of $G(K,K_1)$.

Also, G is solvable and $G(K,K_1)$ is a normal subgroup of G.

Therefore, $G(K,K_1)$ is solvable and hence $G\big(L_1, K_1(\omega)\big)$ is solvable.

Also, $O(G\big(L, K_1(\omega)\big) \leq O(G)$

By the Induction hypothesis, there exists a radical extension L of $K_1(\omega)$ such that $L_1 \subseteq L$ ... (1)

Now, $K_1(\omega)$ is a simple radical extension of $F(\omega)$ and $F(\omega)$ is a simple radical extension of F ... (2)

From (1) and (2)

L is a radical extension of F such that $K\ (\subseteq L_1) \subseteq L$.

12.3 Solution of polynomial equation by radicals

Definition 12.3.1 (Polynomials solvable by radicals): Let $f(x) \in F[x]$. Then $f(x)$ is said to be solvable by radicals if its splitting field is a subfield of some radical extension of F.

Remark 12.3.2: A polynomial $f(x)$ is solvable by radicals if and only if every irreducible factor of $f(x)$ is solvable by radicals.

Solution: It is sufficient to prove the result by taking two irreducible factors.

Let $f(x) = f_1(x)f_2(x)$ where $f_1(x), f_2(x)$ are irreducible factors of $f(x)$.

If $f(x)$ is solvable by radicals then splitting field of $f(x)$ lies in a radical extension L of F.

Therefore, all the roots of $f(x)$ are in L.

This implies, all the roots of $f_1(x)$ and $f_2(x)$ lie in L.

So, splitting field of $f_1(x)$ and $f_2(x)$ are contained in radical extension L of F.

Hence. $f_1(x)$ and $f_2(x)$are solvable by radicals.

Conversely, let $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ and $F(\beta_1, \beta_2, \dots, \beta_n)$ be two splitting fields of $f_1(x)$ and $f_2(x)$ respectively. So, there exist L_1 and L_2, the radical extensions of F such that

$$K_1 = F(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq L_1$$

and

$$K_2 = F(\beta_1, \beta_2, \dots, \beta_n) \subseteq L_2$$

This implies, $K_1K_2 \subseteq L_1L_2$

L_1L_2 being the composite extension is again a radical extension.

Also, if K is splitting field of $f(x)$ then

$$K \subseteq K_1K_2 \subseteq L_1L_2$$

Hence, $f(x)$ is solvable by radicals.

Theorem 12.3.3: Let $f(x) \in F[x], K$ is the splitting field of $f(x)$ such that $[K:F] = n$ and $GCD(n,p) = 1$ where $p = char\ (F)$. Then K is Galois extension of F. Also, $G(K,F)$ is solvable if and only if $f(x)$ is solvable by radicals.

Proof: Let $a \in K$ and $g(x)$ is the minimal polynomial of a over F.

Let $[F(a):F] = m$

Also, $F \subset F(a) \subset K$

This implies, $[F(a):F]$ divides $[K:F]$that is, m divides n.

Since $GCD(n,p) = 1$

$\Rightarrow GCD(m,p) = 1$

$\Rightarrow p$ does not divide m.

Also, $\deg g(x) = m$, this implies that $g'(x) \neq 0$.

Hence, $g(x)$ is a separable polynomial over F.

$\Rightarrow a$ is a separable element over F.

$\Rightarrow K$ is a separable extension of F.

Also, K is splitting field of $g(x)$ over F.

$\Rightarrow K$ is a normal extension of F and hence Galois extension of F.

Let $G(K,F)$ be a solvable group then there exists a radical extension L of F such that $K \subseteq L$.

$\Rightarrow f(x)$ is solvable by radicals.

Conversely, let $f(x)$ is solvable by radicals.

Therefore, there exists a radical extension L of F such that $K \subseteq L$.

So, there exists a radical Galois extension L_1 such that $L \subseteq L_1$.

Since K is also Galois extension of F, therefore, $G(L_1, K)$ is a normal subgroup of $G(L_1, F)$ and

$$G(K, F) \cong G(L_1, F) \,/\, G(L_1, K)$$

Now, $G(L_1, F)$ is solvable and hence $G(K, F)$ is solvable.

: When characteristic $F = p > 0$ then we are taking the condition that $GCD(n, p) = 1$ but when characteristic $F = p = 0$ then we can trivially assume that $GCD\ (n, p) = 1$ that is, all the results are true for Characteristic $F = 0$ also.

Theorem 12.3.4: Let characteristic $F = p$ such that $p \neq 2, 3$ and $f(x) \in F[x]$ with $\deg f(x) \leq 4$. Then $f(x)$ is solvable by radicals.

Proof: As a polynomial $f(x)$ is solvable by radicals if and only if its irreducible factors are all solvable by radicals, therefore, we may assume that $f(x)$ is an irreducible polynomial.

Claim:$GCD(4!, p) = 1$.

Let $GCD\ (4!, p) = d$

$\Rightarrow d|4!$ and $d|p$

Since $d|p$, and p is a prime number then $d = 1$ or p

Also, $d|4!$ and prime divisors of 4! are 2 or 3. Since $p \neq 2,3$, therefore, $d = 1$.

Hence, $GCD(4!, p) = 1$

Let K be the splitting field of $f(x)$ and $[K: F] = m$ so that $[K: F] = m \leq 4$ and $m|4!$

Now $GCD\ (m, p) = 1$

Therefore, K is Galois extension of F.

Thus $f(x)$ is separable polynomial. Also, $G(K, F)$ is isomorphic to a subgroup of $S_n;\ n \leq 4$.

Since S_n is solvable for all $n \leq 4$, therefore, $G(K, F)$ is solvable.

This proves that $f(x)$ is solvable by radicals.

Theorem 12.3.5: Let $f(x) \in \mathbb{Q}[x]$be an irreducible polynomial of degree $p; p$ is a prime number. If $f(x)$ has exactly two non-real roots over $\mathbb{C}$, then the Galois group of $f(x)$ is S_p.

Proof: Let K be the splitting field of $f(x) \in \mathbb{Q}[x]$.

Characteristic $\mathbb{Q} = 0$

If $\alpha \in K$ is a root of $f(x)$ then $[\mathbb{Q}(\alpha): \mathbb{Q}] = \deg f(x) = p$.

Also, $[K: \mathbb{Q}] = [K: \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha): \mathbb{Q}]$

This implies, $[\mathbb{Q}(\alpha): \mathbb{Q}]$ divides $[K: \mathbb{Q}]$.

$\Rightarrow p$ divides $[K: \mathbb{Q}]$.

Again, $O\big(G(K, \mathbb{Q})\big) = [K: \mathbb{Q}]$ implies that p divides $0\big(G(K, \mathbb{Q})\big)$.

By Cauchy's theorem, $G = G(K, \mathbb{Q})$ has at least one element say σ of order p.

Since $\deg f(x) = p$

Therefore, G is isomorphic to a subgroup of S_p. As $\sigma \in G$ and $0(\sigma) = p$

That is, σ is a $p-$cycle.

Claim: G contains a transposition.

Given that $f(x)$ has exactly two complex roots.

Let α_1 and α_2 be two non-real roots of $f(x)$.

$\Rightarrow \alpha_1$ and α_2 are conjugates to each other.

Let $\tau \in G(K, \mathbb{Q})$such that $\tau(\alpha_1) = \alpha_2$. Since τ is one-one and it takes every element to its conjugate. Therefore, $\tau(\alpha_2) = \alpha_1$.

All other roots are fixed under τ. Thus τ can be associated with a transposition $(1\ 2) \in G$.

Since G contains a transposition. Hence, G is isomorphic to S_p.

Summary

- Radical and simple radical extensionsare defined.
- Results about radical and simple radical extensions are proved.
- Galois radical extensions are related to its Galois group.
- Polynomials solvable by radicals are defined.
- Important results about polynomials solvable by radicals are explained.
- The concept of a symmetric group is described.

Keywords

- Radical extension
- Simple radical extension
- Galois radical extension
- Polynomials solvable by radicals
- Symmetric group

Self Assessment

1: A field extension $F \subseteq K$ is called simple radical extension if

A: $K = F(\alpha)$ for some $\alpha \in K$

B: $K = F(\alpha)$ for some $\alpha \in F$

C: $K = F(\alpha)$ for some $\alpha \in K$ such that $\alpha^n \in F$ for some integer n

D: None of the options is correct

2: Which of the following is a simple radical extension of $\mathbb{Q}$?

A: $\mathbb{R}$

B: $\mathbb{C}$

C: $\mathbb{Q}$(i)

D: $\mathbb{Z}$

3: The field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is

A: Simple but not simple radical

B: Simple radical but not simple

C: Neither simple radical nor simple

D: Both simple and simple radical

4: Composite of two radical extensions is again a radical extension.

A: True

B: False

5: Every radical extension $F \subseteq K$ gives rise to a radical Galois extension $K \subseteq L$

A: True

B: False

6: Let K be a Galois radical extension of F then

A: K is simple extension of F

B: K is contained in a simple extension of F

C: K contains a simple extension of F which is not radical

D: K contains a simple radical extension

7: Let $F \subseteq K_1 \subseteq K_2 \subseteq K$ be a radical extension such that $K_1 = F(\alpha), K_2 = K_1(\beta), K = K_2(\gamma)$ then

A: There exists some positive integer n, such that $\alpha^n \in F$

B: There exists some positive integer n, such that $\beta^n \in F$

C: There exists some positive integer n, such that $\gamma^n \in F$

D: All options are correct

8: Let K be a Galois radical extension of F. Then

A: $F \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$ where each K_i is a simple extension of K_{i-1}.

B: $F \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$ where each K_i is a radical extension of K_{i-1}.

C: $F \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$ where each K_i is a simple radical extension of K_{i-1}.

D: $F \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$ where each K_i is a separable extension of K_{i-1}.

9: Any 25th root of unity is also a nth root of unity, if and only if,

A: n is any multiple of 25

B: n is any divisor of 25

C: $n = 5$

D: $n = 10$

10: True/False Let K be a Galois extension of F of degree n such that n and p are coprime. If $G = G(K, F)$ is a solvable group, then there exists a radical extension L of F such that $K \subseteq L$.

A: True

B: False

11: Let $f(x)$ be a polynomial over a field F. Then its splitting field is

A: a radical extension of F

B: a simple radical extension of F

C: a subfield of some radical extension of F

D: a subfield of some simple radical extension of F

12: Let $f(x) = g(x)h(x); g(x), h(x) \in F[x]$. Let K be the splitting field of $f(x)$ and L be the splitting field of $g(x)$. Then $K = L$ if

A: $h(x)$ is a constant polynomial

B: $h(x)$ and $g(x)$ have same roots

C: All the roots of $h(x)$ are roots of $g(x)$ also

D: All options are correct

13: Let characteristic of a field $F = 5$ and $f(x)$ is a polynomial over F. Let K be the splitting field of $f(x)$ such that $[K:F] = 3$. Then $G(K,F)$ is solvable if and only if

A: $f(x)$ is reducible over F

B: $f(x)$ is solvable by radicals

C: $f(x)$ is irreducible over F

D: $f(x)$ has multiple roots in K

14: Let $F \subseteq K$ be a field extension. Let $a \in K$ be an element such that $a \notin F$. If $[K:F] = n$ and $[F(a):F] = m$, then

A: n is a divisor of m

B: m is a divisor of n

C: $n = m$

D: $m > n$

15: Let characteristic $F = 5$ and $f(x) \in F[x]$ is a polynomial of degree 4. Then

A: $f(x)$ is always solvable by radicals

B: $f(x)$ is not solvable by radicals

C: $f(x)$ may or may not be solvable by radicals

D: $f(x)$ is always irreducible

Answers for Self Assessment

1.	C	2.	B	3.	D	4.	A	5.	A
6.	D	7.	D	8.	C	9.	A	10.	A
11.	C	12.	D	13.	B	14.	B	15.	A

Review Questions

1) Let F be any field and let $F(x,y,z)$ be the field of rational functions in 3 indeterminates. Let S be the field of symmetric functions. Find $[F(x,y,z):S]$.
2) Prove that every polynomial over a field F with degree less than or equal to 4 is always solvable by radicals.
3) Prove that the polynomial $f(x) = x^8 + x^6 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$ is solvable by radicals.
4) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 7. If $f(x)$ has exactly two non-real roots over $\mathbb{C}$, then find the Galois group of $f(x)$.

Further Readings

1) Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
2) Topics in algebra by I.N. Hartstein, Wiley
3) Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Isha Garg, Lovely Professional University

Unit 13: Insolvability of the general equation of degree 5 by radicals

CONTENTS

Objective

After studying this unit, you will be able to

- observe that an equation of degree 2, 3, or 4 are always solvable by radicals over Q
- analyze that the equation with order more than 4 may not be solvable by radicals with the help of various examples

Introduction

In this unit, we will discuss that a polynomial of degree 4 or less is always solvable by radicals but a polynomial with a degree more than 4 may not be solvable by radicals. With the help of examples, we will prove these statements.

13.1 Insolvability of the general equation of degree 5 by radicals

Theorem 13.1.1: Any quadratic equation over $\mathbb{Q}$ is solvable by radicals.

Proof: Let $f(x) = x^2 + ax + b$ be a quadratic equation over $\mathbb{Q}$.

Now $a, b \in \mathbb{Q}$

Then roots of the polynomial $f(x)$ are given by

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2}$$

and

$$\beta = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

Now for rational numbers a and b,

Either $a^2 - 4b \geq 0$ or $a^2 - 4b < 0$

If $a^2 - 4b \geq 0$, then both the roots α and β of $f(x)$ are rational numbers hence the splitting field of $f(x)$ is $\mathbb{Q}$.

If $a^2 - 4b < 0$, then $f(x) = (x - \alpha)(x - \beta)$ is irreducible over $\mathbb{Q}$ but both the irreducible factors of $f(x)$ are solvable by radicals.

That is, if $\sqrt{a^2 - 4b} \notin \mathbb{Q}$

Then let $c = \sqrt{a^2 - 4b}$

Consider $K = \mathbb{Q}(c)$, then K is a proper extension of $\mathbb{Q}$ and it is a simple extension. Moreover,

$$c^2 = a^2 - 4b \in \mathbb{Q}$$

Thus, K is a simple radical extension of $\mathbb{Q}$ and hence $f(x)$ is solvable by radicals.

Theorem 13.1.2: Any cubic equation over Q is solvable by radicals.

Proof: Let $f(x) = x^3 + 3ax^2 + 3bx + c \in \mathbb{Q}[x]$ is a cubic polynomial.

Put $x = z - a$

Then

$$\begin{aligned} g(z) &= (z-a)^3 + 3a(z-a)^2 + 3b(z-a) + c \\ &= z^3 - a^3 - 3z^2a + 3a^2z + 3az^2 + 3a^3 - 6a^2z + 3bz - 3ba + c \\ &= z^3 + (-3a^2z + 3bz) + 3a^3 - a^3 - 3ba + c \\ &= z^3 + 3rz + s \end{aligned}$$

where $r = b - a^2$,

$s = 2a^3 - 3ab + c$.

Since $a, b, c \in \mathbb{Q} \Rightarrow r, s \in \mathbb{Q}$

Hence, $g(z) \in \mathbb{Q}[x]$

Also, $f(x)$ has same splitting field as $g(x)$.

By knowing the roots of $f(x)$, we get the roots of $g(x)$ and vice versa.

Put $z = p + q$

$$\begin{aligned} z^3 &= p^3 + q^3 + 3pq(p+q) \\ &= p^3 + q^3 + 3pqz \end{aligned}$$

This implies,

$$z^3 - 3pqz - (p^3 + q^3) = 0$$

That is,

$$pq = -r$$

$$p^3 + q^3 = -s$$

and

$$p^3q^3 = -r^3;$$

A quadratic equation with roots p^3, q^3 is given by $y^2 + sy - r^3$

So, we can take

$$p^3 = -\frac{s}{2} + \sqrt{r^3 + \frac{s}{2}}$$

and

$$q^3 = -\frac{s}{2} - \sqrt{r^3 + \frac{s}{2}}$$

Therefore,

$$p = \left(-\frac{s}{2} + \sqrt{r^3 + \frac{s}{2}}\right)^{\frac{1}{2}}$$

So, three roots of $g(z)$ are$p + q, p\omega + q\omega^2$ and $p\omega^2 + q\omega; \omega = \sqrt[3]{1}$ is the imaginary cube root of unity.

Consider

$$\alpha_1 = \sqrt{r^3 + \frac{S}{2}},$$

$$\alpha_2 = \left(-\frac{S}{2} + \alpha_1\right)^{\frac{1}{3}}$$

and

$$\alpha_3 = \sqrt{-3}$$

Set

$$F_0 = \mathbb{Q}$$

$$F_1 = F_0(\alpha_1)$$

$$F_2 = F_1(\alpha_2)$$

and

$$F_3 = F_2(\alpha_3)$$

Note that $F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3$

Also,

$$\alpha_1^2 = r^3 + \frac{S}{2} \in \mathbb{Q} = F_0$$

So, F_1 is a simple radical extension of F_0.

$$\alpha_2^3 = \alpha_1 - \frac{S}{2} \in F_1$$

So, F_2 is a simple radical extension of F_1.

$$\alpha_3^2 = -3 \in F_0 \subseteq F_2$$

So, F_3 is a simple radical extension of F_2.

Therefore, F_3 is a radical extension of $\mathbb{Q}$.

As F_3 contains all the roots of $f(x)$ that is, F_3 contains a splitting field of $f(x)$.

Hence, any cubic equation over $\mathbb{Q}$ is solvable by radicals.

Theorem 13.1.3: Any quartic equation over F is solvable by radicals.

Proof: Let $f(x) = a_0x^u + a_1x^3 + a_2x^2 + a_3x + a_4; a_0 \neq 0$ be any quartic equation over F.

Let E be its splitting field over F and $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be four roots of $f(x)$.

Then

$$E = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

Now for any $\sigma \in G(E, F)$

$\sigma(\alpha_i)$ is a root of $p(x)$ $\forall i$.

Therefore, σ induces a permutation of set $X = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$.

Now, $O(X) \leq 4$

Let $O(X) = m \leq 4$

The group $A(X)$ of all the permutations on X is isomorphic to S_m.

Since S_1, S_2, S_3, S_4 are all solvable groups hence $A(X)$ is solvable.

Define

$$f: G(E, F) \to A(X)$$

by

$$f(\sigma) = \sigma|X \text{ (Restriction of } \sigma \text{ on } X)$$

Then f is monomorphism and hence

$$G(E,F) \cong \text{Im}\, f$$

$Im\ (f)$ is a subgroup of solvable group $A(X)$. Since subgroup of a solvable group is always solvable, therefore, $G(E,F)$ is a solvable group.

This implies, $f(x)$ is solvable by radicals.

: The polynomial $x^7 - 10x^5 + 15x + 5$ is not solvable by radicals.

Solution: By Eisenstein Criteria of irreducible polynomials, taking $p = 5$, we get that $f(x) = x^7 - 10x^5 + 15x + 5$ is an irreducible polynomial over $\mathbb{Q}$.

Also, by Descartes's rule of signs

$$\begin{aligned} \text{Number of positive real roots of } f(x) &\leq \text{Number of changes in sign of } f(x) \\ &= 2 \end{aligned}$$

Also,

$$\begin{aligned} f(-x) &= (-x)^7 - 10(-x)^5 + 15(-x) + 5 \\ &= -x^7 + 10x^5 - 15x + 5 \end{aligned}$$

Again, by Descartes's rule of signs

$$\begin{aligned} \text{Number of negative real roots of } f(x) &\leq \text{Number of changes in sign of } f(-x) \\ &= 3 \end{aligned}$$

Therefore, the number of real roots of $f(x) \leq 5$.

Again,

$$\begin{aligned} f(-4) < 0, \quad & f(-3) > 0 \\ f(-2) > 0, \quad & f(-1) < 0 \\ f(-1) < 0, \quad & f(0) > 0 \\ f(1) > 0, \quad & f(2) < 0 \\ f(3) < 0, \quad & f(4) > 0 \end{aligned}$$

By Intermediate Value Theorem, $f(x)$ has exactly five real roots in intervals $(-4,-3)$, $(-2,-1)$, $(-1,0)$, $(1,2)$ and $(3,4)$.

Therefore, $f(x)$ has exactly two non-real roots.

Galois group of $f(x)$ is S_7 but S_7 is not a solvable group.

Hence, $f(x)$ is not solvable by radicals.

Theorem 13.1.5: The polynomial $x^5 - 6x + 3$ is not solvable by radicals.

Solution: Taking $p = 3$, and using Eisenstein criteria, we see that $f(x) = x^5 - 6x + 3$ is irreducible over $\mathbb{Q}$ and hence it has no root in $\mathbb{Q}$.

Also, $f'(x) = 0$

$\Rightarrow 5x^4 - 6 = 0$

$\Rightarrow x^2 = \sqrt{\frac{6}{5}}$

$\Rightarrow x = \pm\left(\frac{6}{5}\right)^{\frac{1}{4}}$

So, $f'(x) = 0$ at $x = \pm\left(\frac{6}{5}\right)^{\frac{1}{4}}$

Possible maxima or minima of $f(x)$ is at $\pm\left(\frac{6}{5}\right)^{\frac{1}{4}}$ only.

$$f(-\infty) = -\infty$$

$$f\left(-\left(\frac{6}{5}\right)^{\frac{1}{4}}\right) = \left(-\frac{6}{5}\right)^{\frac{5}{4}} - 6\left(-\left(\frac{6}{5}\right)^{\frac{1}{4}}\right) + 3 > 0$$

$$f\left(\left(\frac{6}{5}\right)^{\frac{1}{4}}\right) = \left(\frac{6}{5}\right)^{\frac{5}{4}} - 6\left(\left(\frac{6}{5}\right)^{\frac{1}{4}}\right) + 3 < 0$$

and

$$f(\infty) = \infty$$

Therefore, $f(x)$ has exactly three real roots in each of the intervals

$$\left(-\infty, -\left(\frac{6}{5}\right)^{\frac{1}{4}}\right), \left(-\left(\frac{6}{5}\right)^{\frac{1}{4}}, \left(\frac{6}{5}\right)^{\frac{1}{4}}\right), \left(\left(\frac{6}{5}\right)^{\frac{1}{4}}, \infty\right)$$

So, $f(x)$ is not solvable by radicals.

Every irreducible polynomial over $\mathbb{R}$ and $\mathbb{C}$ is solvable.

Let $f(x)$ be an irreducible polynomial over $\mathbb{R}$.

Then $f(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$

but $\mathbb{C}$ is algebraically closed.

Therefore, the splitting field of $f(x)$ is $\mathbb{C}$.

Since $[\mathbb{C}: \mathbb{R}] = 2, O\big(G(f(x), \mathbb{R})\big) = 2$

So, Galois group of $f(x)$ is S_2.

S_2 is solvable implies $f(x)$ is solvable by radicals.

Also, over $\mathbb{C}$, every polynomial is reducible in linear factors and hence solvable by radicals.

The polynomial $x^2 + x + 1$ is solvable by radicals over Z_2.

Solution: Since $0^2 + 0 + 1 = 1 \neq 0$ in $\mathbb{Z}_2$

$1^2 + 1 + 1 = 3 = 1 \neq 0$ in $\mathbb{Z}_2$.

Therefore, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$.

Let α be any root of $x^2 + x + 1$ in some field extension of $\mathbb{Z}_2$, then $\alpha^2 + \alpha + 1 = 0$.

$\Rightarrow \alpha^3 + \alpha^2 + \alpha = 0$

$\Rightarrow \alpha^3 - 1 = 0$

$\Rightarrow \alpha^3 = 1$ in $\mathbb{Z}_2$

$\Rightarrow \alpha^3 \in \mathbb{Z}_2$

Therefore, $\mathbb{Z}_2(\alpha)$ is a field extension of $\mathbb{Z}_2$, which is a simple extension and contains roots of $x^2 + x + 1$. Also, it is a simple radical extension of $\mathbb{Z}_2$. Hence, this polynomial is solvable by radicals.

Let characteristic $F = 0$. The polynomial $f(x) = ax^8 + bx^6 + cx^4 + dx^2 + e \in F[x]$ is solvable by radicals.

Solution: $f(x) = ax^8 + bx^6 + cx^4 + dx^2 + e$

Let $x^2 = y$

$g(y) = ay^4 + by^3 + cy^2 + dy + e$ is a quartic polynomial over F.

Since every quartic polynomial is solvable by radicals, therefore, $g(y)$ is solvable by radicals over F.

Let K be the splitting field of $g(y)$ over F then there exists a radical extension L of F such that $K \subseteq L$.

In $L, g(y) = a(y-\alpha_1)(y-\alpha_2)(y-\alpha_3)(y-\alpha_4)$ where $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are roots of $g(y)$ so, $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in L$.

$f(x) = a(x^2-\alpha_1)(x^2-\alpha_2)(x^2-\alpha_3)(x^2-\alpha_4)$ in L

The splitting field of $f(x)$ is $L\left(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \sqrt{\alpha_3}, \sqrt{\alpha_4}\right)$ and $\left(\sqrt{\alpha_i}\right)^2 \in L$

Therefore, each $x^2 - \alpha_i$ is solvable by radicals over L

So, $f(x)$ is solvable by radicals over L.

This implies that $f(x)$ is solvable by radicals over F

Summary

- Apolynomial of degrees 2, 3, or 4 are always solvable by radicals over Q is proved.
- A polynomial with order more than 4 may not be solvable by radicals is explained with the help of various examples

Keywords

- Field extensions
- Radical extension
- Solvability of polynomials by radicals

Self Assessment

1: Choose the incorrect statement

A: Any quadratic equation over $\mathbb{Q}$ is solvable by radicals

B: Any cubic equation over $\mathbb{Q}$ is solvable by radicals

C: Any quartic equation over $\mathbb{Q}$ is solvable by radicals

D: Any equation over $\mathbb{Q}$ is solvable by radicals

2: Let $f(x)$ be a quadratic polynomial over $\mathbb{Q}$, then roots of $f(x)$ are

A: Both rational numbers

B: Both complex numbers

C: Either both complex or rational numbers

D: One complex number and another rational number

3: Let $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$ have both roots real and distinct. Then

A: $a^2 > 4b$

B: $a^2 < 4b$

C: $a^2 \geq 4b$

D: $a^2 = 4b$

4: Any cubic equation over the field of rational numbers

A: Has at least one rational root

B: Has at the most two complex roots

C: Is always solvable by radicals

D: All options are correct

5: Let $f(x)$ is a monic polynomial with integral coefficients. Then by Descartes' rule of sign number of positive real roots of $f(x)$

A: = Number of changes in sign of $f(x)$

B: $\leq$ Number of changes in sign of $f(x)$

C: > Number of changes in sign of $f(x)$

D: $<$ Number of changes in sign of $f(x)$

6: Let $f(x) = x^5 - 5x^4 + 10x^3 + 5x^2 + 2x - 1$ then by Descartes' rule of sign number of positive real roots of $f(x)$ is

A: $= 3$

B: ≤ 3

C: ≥ 3

D: < 3

7: Let $f(x) = x^5 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$ then by Descartes' rule of sign number of negative real roots of $f(x)$ is

A: 0

B: 1

C: 2

D: 3

8: A polynomial having a root in the field of rational numbers is

A: Always reducible over $\mathbb{Q}$

B: Never reducible over $\mathbb{Q}$

C: Completely splits into linear factors over $\mathbb{Q}$

D: Completely splits into linear factors over $\mathbb{R}$

9: Let $f(x)$ be a polynomial over $\mathbb{Q}$ such that $f(a)$ is maxima and $f(b)$ is minima of $f(x)$. Then

A: $f(a) < f(b)$

B: $f(a) < 0$ and $f(b) > 0$

C: $f'(a) > 0$ and $f'(b) < 0$

D: $f'(a) = f'(b) = 0$

10: Let $f(x)$ be a polynomial of degree 7 over the field of rational numbers. Then

A: $f(x)$ is always solvable by radicals over $\mathbb{Q}$.

B:$f(x)$ has no real root

C: $f(x)$ is always solvable over $\mathbb{C}$

D: None of the above is correct

11: Let $f(x)$ be a polynomial of degree 7 over the field of real numbers. Then

A: The order of Galois field of $f(x)$ is 2 and it is always solvable by radicals

B: Order of Galois field of $f(x)$ is greater than 2 and it is always solvable by radicals

C: Order of Galois field of $f(x)$ is greater than 4 and it is not solvable by radicals

D: Order of Galois field of $f(x)$ is 7 and it is not solvable by radicals

12: The polynomial $x^2 + x + 1$ is

A: Solvable by radicals over $\mathbb{Q}$

B: Solvable by radicals over $\mathbb{C}$

C: Solvable by radicals over $\mathbb{Z}_2$

D: All options are correct

13: A polynomial $x^n - 1 \in \mathbb{Q}[x]$; n is any natural number, is

A: Never reducible over $\mathbb{Q}$

B: Has no root in $\mathbb{Q}$

C: Is always solvable by radicals

D: Is solvable by radicals only if $n \leq 4$

14: Splitting field of a polynomial $x^n - 1 \in \mathbb{Q}[x]$; n is any natural number is

A: Always algebraic over $\mathbb{Q}$

B: Always solvable by radicals over $\mathbb{Q}$

C: Having a splitting field which is a simple extension of $\mathbb{Q}$

D: All the options are correct

15: Let $f(x) = x^8 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$. Then

A: $f(x)$ is solvable by radicals

B: $f(x)$ is not solvable by radicals

C: $f(x)$ splits completely into linear factors over $\mathbb{Q}$

D: $f(x)$ splits completely into linear factors over $\mathbb{R}$

Answers for Self Assessment

1.	D	2.	C	3.	A	4.	D	5.	B
6.	B	7.	A	8.	A	9.	D	10.	C
11.	A	12.	D	13.	C	14.	D	15.	A

Review Questions

1) Prove that every polynomial over a field F with degree 2 is always solvable by radicals.
2) Prove that the polynomial $f(x) = x^6 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$ is solvable by radicals.
3) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. If $f(x)$ has exactly two non-real roots over $\mathbb{C}$, then find the Galois group of $f(x)$.

Further Readings

1) Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
2) Topics in algebra by I.N. Hartstein, Wiley
3) Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlinecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

Unit 14: Symmetric Functions and Cyclic Extensions

CONTENTS

Objective

After studying this unit, you will be able to

- define symmetric functions on n variables
- understand symmetric functions with the help of examples
- state and prove Abel's theorem
- define cyclic extensions
- relate cyclic and normal extension
- understand results about cyclic extensions

Introduction

In this unit, we will define symmetric functions on n variables and understand them with the help of examples. Further, we will state and prove Abel's theorem. The cyclic extension is defined and related to normal extensions.

14.1 Symmetric Functions

Let F be a field and $y_1, y_2, \dots, y_n$ be n indeterminates. Let $F(y_1, y_2, \dots, y_n)$ be the field of rational functions over F. Corresponding to any $\sigma \in S_n$, define $\bar{\sigma}: F(y_1, y_2, \dots, y_n) \to F(y_1, y_2, \dots, y_n)$ by

$$\bar{\sigma}\left(\frac{f(y_1, y_2, \dots, y_n)}{g(y_1, y_2, \dots, y_n)}\right) = \frac{f(y_{\sigma(1)}, y_{\sigma(2)}, \dots, y_{\sigma(n)})}{g(y_{\sigma(1)}, y_{\sigma(2)}, \dots, y_{\sigma(n)})}$$

where $f(y_1, y_2, \dots, y_n), g(y_1, y_2, \dots, y_n) \in F(y_1, y_2, \dots, y_n)$ and $g(y_1, y_2, \dots, y_n) \neq 0$.

Then $\bar{\sigma}$ is an automorphism of $F(y_1, y_2, \dots, y_n)$ which keeps elements of F fixed.

$$\frac{f(y_1, y_2, \dots, y_n)}{g(y_1, y_2, \dots, y_n)} \in F(y_1, y_2, \dots, y_n)$$

is called symmetric function in n indeterminates $y_1, y_2, \dots, y_n$ over F if it is fixed by all $\sigma \in S_n$.

Generic Polynomial

Let

$$f(x) = \prod_{l=1}^{n}(x - y_l) \in F(y_1, y_2, \dots, y_n)[x]$$

Then the mapping $F(y_1, y_2, \dots, y_n)[x] \to F(y_1, y_2, \dots, y_n)[x]$ induced by each $\bar{\sigma} \in \bar{S}_n$ keeps $f(x)$ fixed. Hence, if $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ then $(-1)^i a_i$, coefficient of x^{n-i} in $f(-x)$ are called elementary symmetric function and are denoted by s_i.

Hence,

$$s_1 = y_1 + y_2 + \cdots + y_n$$

$$s_2 = y_1y_2 + y_1y_3 + \cdots + y_1y_n + y_2y_3 + \cdots + y_2y_n + \cdots + y_{n-1}y_n = \sum_{i<j} y_iy_j$$

$$\vdots$$

$$s_n = y_1y_2 \cdots y_n$$

For $n = 3$,

$$s_1 = y_1 + y_2 + y_3$$

$$s_2 = y_1y_2 + y_1y_3 + y_2y_3$$

$$s_3 = y_1y_2y_3$$

$f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$ is $n - th$ generic polynomial.

Theorem 14.1.1: Every symmetric function in $y_1, y_2, \dots, y_n$ over field F is a rational function of the elementary symmetric functions $s_1, s_2, \dots, s_n$. Also $F(y_1, y_2, \dots, y_n)$ is a finite normal extension of $F(s_1, s_2, \dots, s_n)$ of degree n!and the Galois group of this extension is isomorphic to S_n.

Proof: Let $\overline{S_n}$ be the group of all automorphisms $\bar{\sigma}$ of $F(y_1, y_2, \dots, y_n)$ corresponding to $\sigma \in S_n$ so that $\overline{S_n} \cong S_n$.

Let $E = F(s_1, s_2, \dots, s_n)$ and K be the subfield of $F(y_1, y_2, \dots, y_n)$ which is a fixed field of $\overline{S_n}$, this implies $E \subseteq K$ ... (1).

Also, $F(y_1, y_2, \dots, y_n)$ is the splitting field of

$$f(x) = \prod_{i=1}^{n}(x - y_i)$$

of degree n over E.

Therefore, $[F(y_1, y_2, \dots, y_n) : E] \leq n!$ ... ... (2)

and $[F(y_1, y_2, \dots, y_n) : K] \geq O(\overline{S_n}) = O(S_n) = n!$ ... ... (3)

$From$ (1), (2) and (3), we get that $E = K$.

Therefore, every symmetric function can be expressed as a rational function of elementary symmetric functions. Now, $f(x)$is a separable polynomial over E and $F(y_1, y_2, \dots, y_n)$ is its splitting field. Hence $F(y_1, y_2, \dots, y_n)$ is a finite separable extension of E and hence

$$[F(y_1, y_2, \dots, y_n) : E] = O\big(G(F(y_1, y_2, \dots, y_n)), E\big) \dots \dots (4)$$

$$\Rightarrow O\big(G(F(y_1, y_2, \dots, y_n)), E\big) = [F(y_1, y_2, \dots, y_n) : E] = n!\,(By\ (3))$$

$\Rightarrow \big(G(F(y_1, y_2, \dots, y_n)), E\big) \cong S_n$ as $G(F(y_1, y_2, \dots, y_n)$ is embedded in S_n.

Theorem 14.1.2: (Abel's Theorem): The generic polynomial of degree $n \geq 5$ over a field F is not solvable by radicals where characteristic $F = 0$.

Proof: The $n - th$ generic polynomial over a field F is

$$f(x) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$$

Its Galois group over $F(s_1, s_2, \dots, s_n)$ is S_n and S_n is not solvable for $n \geq 5$.

This implies $f(x)$ is not solvable by radicals for $n \geq 5$.

: Express the symmetric polynomials as rational functions of the elementary symmetric functions

$(i)\ x_1^2 + x_2^2 + x_3^2$

$(ii)\ x_1^3 + x_2^3 + x_3^3$

$(iii)(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$

Solution: For $n = 3$

$s_1 = x_1 + x_2 + x_3$

$s_2 = x_1x_2 + x_1x_3 + x_2x_3$

$s_3 = x_1x_2x_3$

$(i)s_1 = x_1 + x_2 + x_3$

Squaring both sides, we get,

$$\begin{aligned} s_1^2 &= (x_1 + x_2 + x_3)^2 \\ &= x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x, x_3 + 2x_2x_3 \\ &= x_1^2 + x_2^2 + x_3^2 + 2(x_1x_2 + x_1x_3 + x_2x_3) \\ &= x_1^2 + x_2^2 + x_3^2 + 2s_2 \end{aligned}$$

$$x_1^2 + x_2^2 + x_3^2 = s_1^2 - 2s_2$$

$(ii)s_1 = x_1 + x_2 + x_3$

Cubing both sides,

$$\begin{aligned} s_1^3 &= (x_1 + x_2 + x_3)^3 \\ &= (x_1 + x_2)^3 + x_3^3 + 3(x, +x_2)^2x_3 + 3x_3^2(x_1 + x_2) \\ &= x_1^3 + x_2^3 + 3x_1x_2(x_1 + x_2) + x_3^2 + 3x_3(x_1^2 + x_2^2 + 2x_1x_2) + 3x_1x_2^2 + 3x_2^3 \\ &= x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3x_1^2x_2 + 3x_1x_2^2 + 3x_1^2x_3 + 3x_2^2x_3 + 3x_2^2x_1 + 3x_3^2x_2 \\ &= x_1^3 + x_2^3 + x_3^3 + 3s_1s_2 - 3s_3 \end{aligned}$$

This implies,

$x_1^3 + x_2^3 + x_3^3 = s_1^3 - 3s_1s_2 + 3s_3$

(iii) The equation whose roots are x_1, x_2 and x_3 is

$x^3 - s_1x^2 + s_2x - s_3 = 0 \ldots (1)$

Let

$$h = \frac{sum\ of\ roots}{number\ of\ roots} = \frac{s_1}{3}$$

and

$$y = x - h = x - \frac{s_1}{3}$$

Then (1) implies, $y^3 + 3\alpha y + \beta = 0 \ldots \ldots (2)$, where,

$$\alpha = \frac{-s_1^2}{3} + s_2$$

and

$$\beta = -s_3 - \frac{2s_1^3}{27} + \frac{s_1 s_2}{3}$$

Now roots of (2) are

$$y_1 = x_1 - \frac{s_1}{3},$$

$$y_2 = x_2 - \frac{s_1}{3},$$

and

$$y_3 = x_3 - \frac{s_1}{3}$$

Thus,

$$(y_1 - y_2)^2 \quad = (y_1 + y_2)^2 - 4y_1 y_2$$

Also,

$$y_1 + y_2 + y_3 = 0$$

So, we get,

$$(y_1 - y_2)^2 = y_3^2 - \frac{4\beta}{y_3}$$

Taking $z = y^2 - \frac{4\beta}{y}$, we get, $y^3 - zy - 4\beta = 0$ ... (3)

Subtracting (2) from (3), we get,

$$(3\alpha + z)y = 3\beta$$

$$\Rightarrow y = \frac{3\beta}{3\alpha + z}$$

Put in equation (2),

$\left(\frac{3\beta}{3\alpha + z}\right)^3 + 3\alpha\left(\frac{3\beta}{3\alpha + z}\right) + \beta = 0$

$\Rightarrow (3\alpha + z)^3 + 9\alpha(z + 3\alpha)^2 + 27\beta^2 = 0$

$\Rightarrow z^3 + 18\alpha z^2 + 81\alpha^2 z + 27 - (\beta^2 + 4\alpha^3) = 0$ ... ... (4)

Therefore,

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 \quad = (y_1 - y_2)^2(y_2 - y_3)^2(y_3 - y_1)^2$$

= Product of roots of (4)

$$= -27\ (\beta^2 + 4\alpha^3)$$

14.2 Cyclic Extension

Definition 14.2.1: A Galois extension K of F is said to be a cyclic extension if $G(K, F)$ is a cyclic group.

: If ω is a primitive $p - th$ root of unity where p is a prime number, then $\mathbb{Q}(\omega)$ is a cyclic extension of $\mathbb{Q}$.

Proof: $\mathbb{Z}\ /\ p\mathbb{Z}$ is a finite field with p elements.

Therefore, its multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

$\Rightarrow G(\mathbb{Q}(\omega), \mathbb{Q})$ is cyclic.

Also, $\mathbb{Q}(\omega)$ is Galois extension of $\mathbb{Q}$. Hence, $\mathbb{Q}(\omega)$ is a cyclic extension of $\mathbb{Q}$.

Theorem 14.2.3: Let F be a finite field and K be a finite extension of F then K is a cyclic extension of F.

Proof: Because F is a finite field, therefore, $O(F) = p^n$ for some prime number p and natural number n.

Let $[K:F] = m$

Then K is splitting field of $f(x) = x^{p^{mn}} - x \in \mathbb{Z}_p[x]$

Also, $f'(x) = p^{mn}x^{p^{mn}-1} - 1 = -1 \neq 0$

Thus, $f(x)$ is a separable polynomial.

Also, K is a Galois extension of F.

Now, let $G = G(K,F)$ so that $o(G) = [K:F] = m$

Define $\sigma: K \to K$ by $\sigma(a) = a^{p^n}\ \forall\ a \in K$

Then σ is a homomorphism and one-one.

$\sigma: K \to K$ and K is finite. This implies that σ is onto.

Thus, σ is an automorphism on K. Further, $a^{p^n} = a\ \forall\ a \in F$

$\Rightarrow \sigma(a) = a\ \forall\ a \in F$

Therefore, $\sigma \in G$

Now let $O(\sigma) = r$

$\Rightarrow \sigma^r = I$

$\Rightarrow \sigma^r(c) = c\ \forall\ c \in K$

$\Rightarrow \left(\sigma(c)\right)^r = c\ \forall\ c \in K$

$\Rightarrow \left(c^{p^n}\right)^r = c$

$\Rightarrow c^{q^r} = c\ \forall\ c \in K; q = p^n$

$\Rightarrow c^{q^r-1} = 1\ \forall\ c \in K$

$\Rightarrow q^r - 1 \geq q^m - 1$ (Because $O(K) = p^{mn} = q^m; O(K^*) = q^m - 1$)

$\Rightarrow r \geq m$

But $r \leq m$

$\Rightarrow r = m$

Therefore, $O(\sigma) = m = O(G)$

$\Rightarrow G = \langle\sigma\rangle$is a cyclic group.

$\Rightarrow K$ is a cyclic extension of F.

Theorem 14.2.3: Let K be a cyclic extension of F and L be a field such that $F \subseteq L \subseteq K$. Then K is a cyclic extension of L. Further, if L is a normal extension of F then L is a cyclic extension of F.

Proof: Since K is a cyclic extension of F therefore, $G(K,F)$ is a cyclic group.

Now, K is a Galois cyclic extension of L as K is a Galois extension of F.

Also, $G(K,L)$ being a subgroup of $G(K,F)$ is cyclic.

$\Rightarrow K$ is a cyclic extension of L.

Now, if L is a normal extension of F then it is Galois extension and

$$G(L,F) \cong G(K,F) \,/\, G(K,L)$$

Therefore, L is Galois extension of F and $G(L,F)$ is cyclic group, being quotient group of a cyclic group $G(K,F)$.

Hence, L is a cyclic extension of F.

Theorem 14.2.4: Let K be a cyclic extension of F. There is a unique field L such that $F \subseteq L \subseteq K$ and $[L:F] = d$ for each divisor d of $n = [K:F]$.

Proof:K is a cyclic extension of F of degree n. Therefore, $G(K,F)$ is a cyclic group of order n.

For each $d|n$, there exists a unique subgroup H of order $\frac{n}{d} = d'$

Let L be the fixed field of H. Then $[K:L] = d'$

Hence,

$$\begin{aligned}[L:F] &= [K:F]/[K:L] \\ &= \frac{n}{d'} \\ &= d\end{aligned}$$

Theorem 14.2.5: Let E be a normal extension of a field F of degree n and F contains a primitive nth root of unity. Then the Galois group $G(E,F)$ is cyclic if and only if there exists an element$b$ in F such that $x^n - b$ is an irreducible polynomial over F and E is its splitting field.

Proof: Let for some positive integer n and some $b \in F, x^n - b$ is an irreducible polynomial over F and let E is the splitting field of $x^n - b$ over F.

$\Rightarrow E = F(c)$ where c is a root of $x^n - b$.

$$[E:F] = n \Rightarrow O\big(G(E,F)\big) = n$$

Now, let ξ be a primitive nth root of unity in F. Then since F contains a primitive root of unity so it contains all the roots $c, \xi c, \xi^2 c, \dots, \xi^{n-1} c$ of $x^n - b$.

Since c and ξc are conjugates over F, there exists an F −automorphism σ of $F(c)$ onto $F(\xi c)$ such that $\sigma(c) = \xi c$.

However, $E = F(c) = F(\xi c)$

So, σ is an $F -$ automorphism of F.

Therefore, $\sigma \in G(E,F)$

Now,

$$\begin{aligned}\sigma^2(c) &= \sigma\big(\sigma(c)\big) \\ &= \sigma(\xi c) \\ &= \xi\big(\sigma(c)\big) \\ &= \xi^2 c\end{aligned}$$

$$\forall\, k \in \mathbb{N}, \qquad \sigma^k(c) = \xi^k c$$

As $\xi^n = 1$ and $c, \xi c, \xi^2 c, \dots, \xi^{n-1} c$ are all distinct. Thus, we get $I, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are all n distinct elements of $G(E,F)$.

$G(E,F) =< \sigma >$ is a cyclic group of order n.

Conversely,let $G(E,F)$ is a cyclic group of order n and its elements are $I, \sigma, \sigma^2, \dots, \sigma^{n-1}$.

$\{I, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ is linearly independent set over F.

Let ξ be a primitive nth root of unity in F.

Then $\xi \neq 0$

$I + \xi^{-1}\sigma + \xi^{-2}\sigma^2 + \cdots + +\xi^{-n+1}\sigma^{n-1}$ is a non-zero endomorphism of E as a vector space over F.

Thus, for $a \in E$,

$$c = I(a) + \xi^{-1}\sigma(a) + \xi^{-2}\sigma^2(a) + \cdots + +\xi^{-n+1}\sigma^{n-1}(a) \neq 0$$

Now

$$\begin{aligned}\sigma(c) &= \sigma(a) + \xi^{-1}\sigma^2(a) + \xi^{-2}\sigma^3(a) + \cdots + +\xi^{-n+1}\sigma^n(a)\\ &= \xi(\xi^{-1}\sigma(a) + \xi^{-2}\sigma^2(a) + \cdots + I(a))\\ &= \xi c \text{ since } \sigma^n = I, \xi^n = 1\end{aligned}$$

In general,

$$\sigma^k(c) = \xi^k(c)\ \forall\ k$$

$$\begin{aligned}\sigma^k(c^n) &= \left(\sigma^k(c)\right)^n\\ &= \xi^{kn}(c^n)\\ &= c^n\ \forall\ k\end{aligned}$$

So, c^n is in the fixed field under $G(E, K)$.

However, F is the fixed field under $G(E, F)$ so $c^n \in F$.

But $b = c^n$

Therefore, $x^n - b$ is a polynomial over F whose roots are $c, \xi c, \xi^2 c, \ldots, \xi^{n-1}c$.

Also, $\sigma^k(c) = \xi^k(c)$

$\Rightarrow c, \xi c, \xi^2 c, \ldots, \xi^{n-1}c$ are conjugates in F.

The minimal polynomial $f(x)$ of c over F is at least of degree n.

As $f(x)$ divides $x^n - b$

$$\Rightarrow f(x) = x^n - b$$

So, it is itself a minimal polynomial of c.

Therefore, $x^n - b$ is irreducible polynomial over F.

Now, $[F(c): F] = n$

$[E: F] = n, F(c) \subseteq E$

$\Rightarrow F(c) = E$

E is the splitting field of $x^n - b$ over F and $x^n - b$ is an irreducible polynomial over F.

Summary

- Symmetric functions on n variables are defined.
- Symmetric functions are explained with the help of examples.
- Abel's theorem is proved.
- Cyclic extensions are defined.
- Cyclic and normal extensions are related.
- Results about cyclic extensions are explained.

Keywords

- Symmetric Functions
- Abel's theorem
- Cyclic extensions

Self Assessment

1: A symmetric function in n indeterminates over a field F is fixed under

A: at least one $\sigma \in S_n$

B: Exactly one $\sigma \in S_n$

C: At the most one $\sigma \in S_n$

D: All the $\sigma \in S_n$

2: Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, then the corresponding generic polynomial is

A: $t^n - a_1t^{n-1} + \cdots + a_n$

B: $t^n + a_1t^{n-1} + \cdots + a_n$

C: $t^n - a_1t^{n-1} + \cdots + (-1)^n a_n$

D: $t^n - a_1t^{n-1} + \cdots - a_n$

3: The generic polynomial of degree 7 over $\mathbb{Q}$ is

A: Always solvable by radicals

B: Never solvable by radicals

C: May or may not be solvable by radicals

D: Has no real roots

4: Every symmetric function in n variables over a field F is a rational function of the …… number of elementary symmetric functions

A: n

B: $n - 1$

C: $n!$

D: $n/2$

5: The elementary symmetric function corresponding to the symmetric polynomial $x_1^2 + x_2^2 + x_3^2$ is

A: $S_1^2 + 2S_2$

B: $S_1^2 - 2S_2$

C: $S_1 + 2S_2^2$

D: $S_1 - 2S_2^2$

6: The elementary symmetric function corresponding to the symmetric polynomial $x_1x_2x_3$ is

A: $S_1S_2S_3$

B: $S_1^2S_2^2S_3^2$

C: S_1S_2

D: S_3

7: The elementary symmetric function corresponding to the symmetric polynomial $x_1^3 + x_2^3 + x_3^3$ is

A: $S_1^3 + 2S_1S_2 + 3S_3$

B: $S_1^3 - 2S_1S_2 - 3S_3$

C: $S_1^3 - 2S_1S_2 + 3S_3$

D: $S_1^3 + 2S_1S_2 - 3S_3$

8: The elementary symmetric function corresponding to the symmetric polynomial $(x_1 - x_2)^2$ is

A: $S_1^2 + 4S_2$

B: $S_1^2 - 4S_2$

C: $S_1 + 4S_2^2$

D: $S_1 - 4S_2^2$

9: If ω is primitive 5th root of unity then $\mathbb{Q}(\omega)$ is

A: Cyclic extension of $\mathbb{Q}$

B: Abelian but not a cyclic extension of $\mathbb{Q}$

C: Extension with an infinite degree

D: Inseparable extension

10: Multiplicative group of the field $\mathbb{Z} / p\mathbb{Z}$ is

A: Finite but not cyclic

B: Infinite and cyclic

C: Finite and cyclic

D: Infinite but not cyclic

11: Finite extension of a finite field is

A: Always cyclic

B: Abelian but not cyclic

C: Never abelian

D: Never cyclic

12: The order of a field is always

A: Divisible by at least two distinct prime numbers

B: Divisible by a single prime number only

C: Is a prime number

D: Is a composite number

13: Let F be a field such that $O(F) = 27$. Let K be a field extension of F such that $[K:F] = 4$. Then K is splitting field of

A: $f(x) = x^{3^{12}} - x \in \mathbb{Z}_3[x]$

B: $f(x) = x^{3^4} - x \in \mathbb{Z}_3[x]$

C: $f(x) = x^{3^3} - x \in \mathbb{Z}_3[x]$

D: $f(x) = x^{27} - x \in \mathbb{Z}_3[x]$

14: The polynomial $f(x) = x^{5^n} - x \in \mathbb{Z}_5[x]$ is

A: Always separable polynomial

B: Separable polynomial only if $n > 2$

C: Separable polynomial only if $n > 3$

D: Separable polynomial only if $n > 4$

15:Let $F \subseteq L \subseteq K$ is field extension such that K is a cyclic extension of F. Then

A: K is a cyclic extension of L

B: K is abelian but not a cyclic extension of L

C: K is not an abelian extension of L

D: L is a cyclic extension of F

Answers for Self Assessment

1.	B	2.	C	3.	B	4.	A	5.	B
6.	D	7.	C	8.	B	9.	A	10.	C
11.	A	12.	B	13.	A	14.	A	15.	A

Review Questions

1) Prove that every symmetric function in n variables over field F is a rational function of the elementary symmetric functions n variables.
2) Prove that the generic polynomial of degree 7 over a field of rational numbers is not solvable by radicals.
3) Prove that $\mathbb{Q}(i)$ is a cyclic extension of $\mathbb{Q}$.
4) Prove that finite extension of a finite field is always a cyclic extension.

Further Readings

1) Basic abstract algebra by P. B. Bhattacharya, S. K. Jain, S. R. Nagpal,Cambridge universitypress
2) Topics in algebra by I.N. Hartstein, Wiley
3) Abstract algebra by David S Dummit and Richard M Foote, Wiley

Web Links

https://onlin ecourses.nptel.ac.in/noc20_ma29/preview

https://nptel.ac.in/courses/111/105/111105112/#

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-521360
Fax.: +91-1824-506111
Email: odl@lpu.co.in