GALOIS THEORY

M.Sc., MATHEMATICS First Year
Semester –II, Paper-I

Lesson Writers

Prof. R. Srinivasa Rao
Department of Mathematics
University College of Science
Acharya Nagarjuna University

Prof. P. Vijaya Saradhi
Department of Mathematics
Bapatla Engineering College
Bapatla

Dr. K. Siva Prasad
Department of Mathematics
University College of Science
Acharya Nagarjuna University

Dr. J L Rama Prasad
Department of Mathematics
P. B. Siddhartha College of
Arts & Science,Vijayawada

Editor

Prof. R. Srinivasa Rao
Department of Mathematics
University College of Science
Acharya Nagarjuna University

.

Academic Advisor

Prof. R Srinivasa Rao
Department of Mathematics
Acharya Nagarjuna University

Director I/c
Prof. V.VENKATESWARLU
MA., M.P.S., M.S.W., M.Phil., Ph.D.
CENTRE FOR DISTANCE EDUCATION
ACHARAYANAGARJUNAUNIVERSITY
NAGARJUNANAGAR – 522510
Ph:0863-2346222,2346208,
0863-2346259(Study Material)
Website: www.anucde.info
e-mail:anucdedirector@gmail.com

M.Sc., MATHEMATICS – GALOIS THEORY

First Edition 2025

No. of Copies :

Published by:
Prof. V.VENKATESWARLU,
Director, I/C
Centre for Distance Education,
Acharya Nagarjuna University

Printed at:

FOREWORD

Since its establishment in 1976, Acharya Nagarjuna University has been forging ahead in the path of progress and dynamism, offering a variety of courses and research contributions. I am extremely happy that by gaining 'A^{+}' grade from the NAAC in the year 2024, Acharya Nagarjuna University is offering educational opportunities at the UG, PG levels apart from research degrees to students from over 221 affiliated colleges spread over the two districts of Guntur and Prakasam.

The University has also started the Centre for Distance Education in 2003-04 with the aim of taking higher education to the doorstep of all the sectors of the society. The centre will be a great help to those who cannot join in colleges, those who cannot afford the exorbitant fees as regular students, and even to housewives desirous of pursuing higher studies. Acharya Nagarjuna University has started offering B.Sc., B.A., B.B.A., and B.Com courses at the Degree level and M.A., M.Com., M.Sc., M.B.A., and L.L.M., courses at the PG level from the academic year 2003-2004 onwards.

To facilitate easier understanding by students studying through the distance mode, these self-instruction materials have been prepared by eminent and experienced teachers. The lessons have been drafted with great care and expertise in the stipulated time by these teachers. Constructive ideas and scholarly suggestions are welcome from students and teachers involved respectively. Such ideas will be incorporated for the greater efficacy of this distance mode of education. For clarification of doubts and feedback, weekly classes and contact classes will be arranged at the UG and PG levels respectively.

It is my aim that students getting higher education through the Centre for Distance Education should improve their qualification, have better employment opportunities and in turn be part of country's progress. It is my fond desire that in the years to come, the Centre for Distance Education will go from strength to strength in the form of new courses and by catering to larger number of people. My congratulations to all the Directors, Academic Coordinators, Editors and Lesson-writers of the Centre who have helped in these endeavors.

Prof. K.GangadharaRao

M.Tech., Ph.D.,
Vice-Chancellor I/c
Acharya Nagarjuna University

M.Sc. – Mathematics

SEMESTER-II

201MA24: GALOIS THEORY

SYLLABUS

Unit-I

Algebraic extensions of fields: Irreducible polynomials and Eisenstein criterion-Adjunction of roots - Algebraic extensions.

(Sections 15.1 to 15. 3 of Chapter15 of the Prescribed book)

Unit-II

Algebraically closed fields; Normal and Separable extensions: Splitting fields - Normal extensions - Multiple roots.

(Section 15.4 of Chapter 15 and Sections 16.1 to 16.3 of Chapter16 of the prescribed book)

Unit-III

Finite fields - Separable extensions-Automorphism groups and fixed fields.

(Sections 16.4 to 16.5 of Chapter 16 and Section 17.1 of Chapter 17 of the prescribed book)

Unit-IV

Galois Theory: Fundamental theorem of Galois theory - Fundamental theorem of Algebra; Applications of Galois theory to classical problems: Roots of unity and cyclotomic polynomials - Cyclic extensions.

(Sections 17.2 to 17.3 of Chapter 17 and Sections 18.1 to 18.2 of Chapter 18 of the prescribed book).

Unit-V

Polynomials solvable by radicals -Symmetric functions – Ruler and Compass constructions

(Sections 18.3 to 18.5 of Chapter 18 of the prescribed text book)

PRISCRIBED BOOK:

P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.

REFERENCE BOOKS:

1. I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley &Sons, 1999.
2. Thomas W. Hungerford , 'Algebra', Springer-Verlag, New York, 1974.
3. Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

CODE: 201MA24

M.Sc DEGREE EXAMINATION
Second Semester
Mathematics:: Paper I – GALOIS THEORY

MODEL QUESTION PAPER

Time : Three hours **Maximum : 70 marks**

Answer ONE question from each Unit. **(5 x 14 = 70)**

UNIT - I

1. (a) Let $F \subseteq E \subseteq K$ be field. If $[K : E] < \infty$ and $[E : F] < \infty$, then show that
(i) $[K : F] < \infty$
(ii) $[K : F] = [K : E][E : F]$
(b) State and Prove Gauss Lemma.

(OR)

2. (a) If E is an extension of F and $u \in E$ is algebraic over F, then prove that $F(u)$ is an algebraic expansion of F.
(b) State and Prove Kronecker theorem.

UNIT – II

3. Prove that for any field K the following are equivalent.
(a) K is algebraically closed,
(b) Every irreducible polynomial in $K[x]$ is of degree 1,
(c) Every polynomial in $K[x]$ of positive degree factor completely in $K[x]$ into linear factors,
(d) Every polynomial in $K[x]$ of positive degree has atleast one root in K.

(OR)

4. (a) If $f(x) \in F[x]$ is irreducible over F, then show that all roots of $f(x)$ have the same multiplicity.
(b) State and prove uniqueness of splitting field theorem.

UNIT – III

5. Show that if E is a finite separable extension of a field F, then E is a simple extension of F.

(OR)

6. (a) State and prove Dedekind lemma.
(b) Let H be a finite subgroup of the group of automorphisms of a field E. Then show that $[E : E_H] = |H|$.

UNIT – IV

7. State and prove fundamental theorem of algebra.

(OR)

8. (a) Let F be a field let U be a finite subgroup of the multiplicative group $F^* = F - \{0\}$. Then show that U is cyclic.

   (b) Show that $\emptyset_n(x) = \pi_\omega(x - \omega)$, ω is primitive n^{th} root in C, is an irreducible polynomial of degree $\emptyset(n)$ in $Z[x]$.

UNIT – V

9. (a) Show that $f(x) \in F[x]$ is solvable by radicals over F if and only if its splitting field E over F has solvable Galois group $G(E/F)$.

   (b) Show that the polynomial $x^5 - 9x + 3$ is not solvable by radicals over Q.

(OR)

10. (a) Solve the problem of trisecting an angle.

    (b) Prove that it is impossible to construct a cube with a volume equal to twice the volume of a given cube by using ruler and compass only.

CONTENTS

LESSON- 1

IRREDUCIBLE POLYNOMIALS & EISENSTEIN CRITERION

OBJECTIVES:

- To define and identify irreducible polynomials over various rings, especially over fields like $\mathbb{Q}$, $\mathbb{R}$, and finite fields.
- To understand the relationship between irreducibility and factorization in polynomial rings.
- To determine irreducibility of polynomials using known theorems and tests.
- To state and apply Eisenstein's Criterion to test the irreducibility of a given polynomial in $\mathbb{Q}[x]$ or other relevant polynomial rings.

STRUCTURE:

1.1 INTRODUCTION:

Polynomials play a central role in abstract algebra, particularly in understanding the structure of rings and fields. An important concept in this context is the *irreducibility* of polynomials, analogous to primeness in integers. Irreducible polynomials cannot be factored into non-unit polynomials of lower degree over a given ring. Identifying irreducible polynomials is crucial in constructing field extensions and understanding algebraic equations.

One of the most powerful tools is Eisenstein's Criterion, which provides a sufficient condition for irreducibility. This criterion uses the divisibility properties of the coefficients relative to a prime number. Though not universally applicable, it simplifies many problems and reveals deep algebraic structure. In this lesson, we will study irreducibility, understand Eisenstein's Criterion, and learn to apply it effectively. We start with irreducible polynomials, primitive polynomials and finally we provide the proof for the theorem namely Eisenstein criterion.

1.2 IRREDUCIBLE POLYNOMIALS:

Let us recollect some important definitions and examples which are essential in the study of this Lesson.

1.2.1 Definition: A commutative ring R is said to be an integral domain if $xy = 0, x, y \in R$ $implies$ $x = 0$ or $y = 0$.

Note: Let R be a commutative integral domain with unity. $a \in R$ is a unit in R if there is a $b \in R$ such that $ab = 1$. For $0 \neq a, b \in R$, we say that a divides b, written $a|b$, if b = ac for some $c \in R$. Let $a \in R$. For $0 \neq b, c \in R$ if $a = bc$ then b is divisor of a. We say that a divisor b of a is improper if $a = bc$ then either b is a unit or c is a unit, where $b, c \in R$.

1.2.2 Definition: A non-zero element a of a commutative integral domain R with unity is called an irreducible element if it is not a unit and every divisor of a is improper.

1.2.3 Definition: A non-zero element p of a commutative integral domain R with unity is called a prime element if

(i) it is not a unit

(ii) p divides ab then either p divides a (or) p divides b, where $a, b \in R$.

1.2.4 Definition: A commutative Integral domain R with unity is called a unique factorization domain if (i) every non-zero non-unit of R is a finite product of irreducible elements and

(ii) every irreducible element in R is prime.

Note: Let F be a field and let $F[x]$be the ring of the polynomials in x over F. Then $F[x]$ is a commutative integral domain with unity and contains F as a proper subring.

1.2.5 Definition: A polynomial $f(x)$ in $F[x]$ is called irreducible polynomial if the degree of $f(x) \geqslant 1$ and whenever $f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in F[x]$, then either $g(x) \in F$ (or) $h(x) \in F$. If a polynomial is not irreducible, then it is a called reducible.

1.2.6 Example: $x^2 + 1$ is irreducible over $\mathbb{R}$, but it is reducible over C.

1.2.7 Properties of $F[x]$, F is field:

- The division algorithm holds in $F[x]$.This means if $f(x) \in F[x]$ and $0 \neq g(x) \in F[x]$ then there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < deg(g(x))$.
- $F[x]$ is a principal Ideal domain.
- $F[x]$ is a U.F.D.
- The units of $F[x]$ are the non-zero elements of F.
- If $p(x)$ is irreducible in $F[x]$, then $\frac{F[x]}{\langle p(x) \rangle}$ is a field and conversely.

1.2.8 Proposition: Let F be a field and $f(x) \in F[x]$ be a polynomial of degree > 1. If $f(\alpha) = 0$ for some $\alpha \in F$, then$f(x)$ is reducible over F.

Proof: let F be a field and let $f(x) \in F[x]$ be a polynomial such that $\deg f(x) > 1$ and $f(\alpha) = 0$ for some $\alpha \in F$.

Then $(x - \alpha)$ is a factor of $f(x)$. Here $f(x), (x - \alpha)$ are in $F[x]$. So by division algorithm, there exists $g(x), r(x) \in F[x]$ &$f(x) = (x - \alpha)g(x) + r(x)$ where $r(x) = 0$ (or) $\deg\ r(x) < \deg\ (x - \alpha) = 1$. If $\deg\ r(x) < \deg\ (x - \alpha)$, then $r(x)$ is a constant polynomial

Therefore $\mathrm{r}(x) = a$ where $a \in F$.

Here $0 = f(\alpha) = (\alpha - \alpha)g(\alpha) + r(\alpha) = r(\alpha)$. So, a = 0 and hence $\mathrm{r}(x) = 0$.

$\Rightarrow f(x) = (x - \alpha)g(x) + 0$

$\Rightarrow f(x) = (x - \alpha)g(x)$

Since deg $f(x) > 1$, we must have $f(x)$ is the product of two non-constant polynomials. Therefore $f(x)$ is reducible over F.

1.2.9 Definition: Let E be a field and F be a subfield of F, and let $f(x) \in F[x]$. An element $\alpha \in E$ is called a root (or) zero of $f(x)$ if $f(\alpha) = 0$.
Note:
1 If $f(x) = a_0 + a_1x + \cdots + a_kx^k$, then $f(\alpha)$ stands for the element $a_0 + a_1\alpha + \cdots + a_k\alpha^k$ in E
2. If $f_1(x)$ is a polynomial of degree one, then $f_1(x) = ax + b$, where $a, b \in F, a_0 \neq 0$ and $-ba^{-1}$ is a root of $f_1(x)$. So we can conclude that if a polynomial $f(x)$ in $F(x)$ has a factor of degree one in $F[x]$, then $f(x)$ has a root in F.

1.2.10 Proposition: let $f(x) \in F[x]$ be a polynomial of degree 2 or 3 , then $f(x)$ is reducible in $F[x]$ if and only if $f(x)$ has a root in F.

Proof: Let $f(x) \in F[x]$ be a polynomial of deg $f(x) = 2$ or 3.
Suppose that $f(x)$ is reducible over F. Then $f(x)$ can be expressed as the product of two non-constant polynomials. i.e. $f(x) = f_1(x).f_2(x)$ where $f_1(x), f_2(x) \in F[x]$ and deg $f_1(x) < 3$ and deg $f_2(x) < 3$.
Since $f_1(x), f_2(x)$ are non-constant polynomials, we have deg $f_1(x) \geqslant 1$ and deg $f_2(x) \geqslant 1$
So we must have deg $f_1(x) = 1$ (or) deg $f_2(x) = 1$($\because$ deg $f(x) = 2$ or 3)
If deg $f_1(x) = 1$, $f_1(x) = ax + b$, where $a, b \in F$ & $a \neq 0$
Since $a \neq 0$ and F is a field, we have $-ba^{-1} \in F$ and $f_1(-ba^{-1}) = a(-ba^{-1}) + b = 0$
Also $f(-ba^{-1}) = f_1(-ba^{-1})f_2(-ba^{-1}) = 0 \cdot f_2(-ba^{-1}) = 0$
So, f(x) has a root in F.
If deg $f_1(x) > 1$, then deg $f_1(x) = 2$.
Also if deg $f_2(x) = 2$, then deg $f(x) =$ deg $f_1(x) +$ deg $f_2(x) = 2 + 2 = 4$, which is a contradiction. Therefore deg $f_2(x) = 1$.
So , by the above proof $f(x)$ has a root in F.
Conversely, Suppose that $f(x)$ has a root in F, say 'α' i.e.$f(\alpha) = 0$.
Then $(x - \alpha)$ is a factor of $f(x)$, that is, $f(x) = (x - \alpha)g(x)$ for some $g(x) \in F[x]$.
Since deg$f(x) > 1$, we must have deg $g(x) \geqslant 1$
i.e. $f(x)$ is the product of two non-constant polynomials.i.e. $f(x)$ is reducible over F.

1.2.11 Definition: A polynomial $f(x) \in Z[x]$ is called a primitive polynomial if the greatest common divisor of the coefficients of $f(x)$ is 1. The g.c.d of the coefficients of $f(x)$ is called content of $f(x)$ and it is denoted by $c(f)$.
Note: 1. $c(f) = 1$ if and only if $f(x)$ is a primitive polynomial.

1.2.12 Definition: A polynomial $a_0 + a_1x + \cdots + a_nx^n$ over a ring R is called a monic polynomial if $a_n = 1$.
Note: Every monic polynomial $f(x) \in Z[x]$ is primitive.

1.2.13 Proposition: If $f(x), g(x) \in Z[x]$ are two primitive polynomials, then the product $f(x) \cdot g(x)$ is also primitive.
Proof: Given $f(x), g(x)$ are two primitive polynomials in$Z[x]$.

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$; where $a_i, b_j \in$ Z; $i = 0,1, \ldots, n, j = 0, 1, 2, \ldots, m$.
Suppose if possible, $f(x) \cdot g(x)$ is not primitive.

Then the g.c.d. of all coefficients of $f(x) \cdot g(x)$ is not a unit. There exist a prime number p, which divides all the coefficients of $f(x) \cdot g(x)$. Since $f(x)$ is primitive, p does not divides all the coefficients of $f(x)$. So let ' a_j ' be the first co-efficient, which is not divisible by ' p '. Since $g(x)$ is primitive, p does not divides all the co-efficients of $g(x)$. So, let ' b_k ' be the first coefficient of $g(x)$, which is not divisible by p.
Now, $c_{j+k} = a_jb_k + \left(a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0\right) + \cdots + \left(a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{j+\mathrm{k}}\right)$

Since $p|a_i$ for $i = 0,1, \ldots, j-1$, we have $p \mid a_0b_{j+k} + \cdots + a_{j-1}b_{k+1}$

Also, $p|b_{\mathrm{i}}$ for $i = 0,1, \ldots, k-1$, we have $p \mid \left(a_{j+k}b_0 + \cdots + a_{j+1}b_{k-1}\right)$

and p divides all the co-efficients of $f(x) \cdot g(x)$.
so $p|c_{j+k}$
,that is, $p|a_{\mathrm{j}}\, b_k$
Since p is a prime number, we have, $p|a_{\mathrm{j}}$ or $p|b_{\mathrm{k}}$ which is a contradiction to selection of a_j& b_k So, Our supposition is wrong.
Hence $f(x) \cdot g(x)$ is a primitive polynomial.

1.2.14 Definition: A polynomial $f(x) \in Z[x]$ is called irreducible over Z, if $f(x)$ is an irreducible element in $Z[x]$.
Note: An irreducible polynomial over Z must be primitive.

1.2.15 Gauss Lemma: Let $f(x) \in Z[x]$ be a primitive polynomial. Then $f(x)$ is reducible over Q if and only if $f(x)$ is reducible over Z.
Proof: Let $f(x) \in Z[x]$ be a primitive polynomial.
Assume that $f(x)$ is reducible over Z.
Then $f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in Z[x]$ and deg $g(x) \geqslant 1$&deg $h(x) \geqslant 1$ as $f(x) \in Z[x]$ is primitive.
Since $Z \subset Q$, we have $g(x), h(x) \in Q[x]$.
This implies $f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in Q[x]$ and deg $g(x) \geqslant 1$; deg $h(x) \geqslant 1$.
i.e. $f(x)$ is expressed as the product of two non-constant polynomials in $Q[x]$.
Therefore $f(x)$ is reducible over Q.
Conversely, suppose that, $f(x)$ is reducible over Q.
Then $f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in Q[x]$ and deg $g(x) \geqslant 1$; deg $h(x) \geqslant 1$.
$= \frac{a}{b} g_1(x)h_1(x)$ where $g_1(x), h_1(x) \in Z[x]$ and $g_1(x), h_1(x)$ are primitive, $a,b \in Z$, deg $g(x) =$ deg $g_1(x)$, and deg $h(x) =$ deg $h_1(x)$
$\Rightarrow bf(x) = a(g_1(x) \cdot h_1(x))$
$\Rightarrow c\big(b(f(x)) = c\big(a(g_1(x) \cdot h_1(x))\big)$
Since $f(x)$ is a primitive polynomial, $\mathrm{c}(f) = 1$. Therefore $c\left(b\big(f(x)\big)\right) = b$.
Since $g_1(x).\, h_1(x)$is primitive, we have $c\big(a(g_1(x) \cdot h_1(x))\big) = a$. So a = b.
This implies $f(x) = g_1(x) \cdot h_1(x)$ where $g_1(x) \cdot h_1(x) \in Z[x]$, deg $h_1(x) =$ deg $h(x) \geqslant 1$ and deg $g_1(x) =$ deg $g(x) \geqslant 1$.

i.e. $f(x)$ is the product of two positive degree polynomials in $Z[x]$.
Therefore $f(x)$ is reducible over Z.

1.2.16 Lemma: If $f(x) \in Z[x]$ is reducible over Q, then it is also reducible over Z.
Proof: Let $f(x) \in Z[x]$.
We know that any polynomial $f(x)$ in $Z[x]$ can be written as $f(x) = df_1(x)$, where $d = c(f)$ and $f_1(x)$ is a primitive polynomial in $Z[x]$.
Suppose $f(x)$ is reducible over Q. Then $df_1(x)$ is reducible over Q.
So $f_1(x)$ is reducible over Q & $f_1(x)$ is primitive in $Z[x]$.
Then by 1.2.15, we have $f_1(x)$ is reducible over Z.
So $df_1(x)$ is reducible over Z. Hence $f(x)$ is reducible over Z.

1.2.17 Proposition: Let $f(x) = a_0 + a_1x + a_2x + \cdots + a_{n-1}x^{n-1} + x^n \in Z[x]$ be a monic polynomial. If $f(x)$ has a root $a \in Q$, then $a \in Z$ & a divides a_0.
Proof: Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in Z[x]$ be a monic polynomial.
Let $0 \neq a \in Q$ be a root of $f(x)$.
Since $a \in Q$, we have $a = \frac{\alpha}{\beta}$, where $\alpha, \beta \in \mathbb{Z}$ & $\beta \neq 0$, $(\alpha, \beta) = 1$. Also since $a = \frac{\alpha}{\beta}$ is root

of $f(x)$, we have $f\left(\frac{\alpha}{\beta}\right) = a_0 + a_1\left(\frac{\alpha}{\beta}\right) + \cdots + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \left(\frac{\alpha}{\beta}\right)^n = 0$

$= a_0 + a_1 \cdot \frac{\alpha}{\beta} + \cdots + a_{n-1}\frac{\alpha^{n-1}}{\beta^{n-1}} + \frac{\alpha^n}{\beta^n} = 0 \ldots\ldots\ldots (*)$

Now multiplying the above with β^{n-1}, we get

$a_0\beta^{n-1} + a_1 \cdot \frac{\alpha}{\beta} \cdot \beta^{n-1} + \cdots + a_{n-1}\frac{\alpha^{n-1}}{\beta^{n-1}} \cdot \beta^{n-1} + \frac{\alpha^n}{\beta^n} \cdot \beta^{n-1} = 0.$

So $a_0\beta^{n-1} + a_1\alpha\beta^{n-2} + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n \cdot \beta^{-1} = 0.$

Now $a_0\beta^{n-1} + a_1\alpha\beta^{n-2} + \cdots + a_{n-1}\alpha^{n-1} = \frac{-\alpha^n}{\beta}$ is an integer.

Since $g.c.d\ of\ \alpha, \beta\ is\ 1$ & $\beta \in Z$, we have $\beta = \pm 1$.
Therefore $a = \pm\alpha$ where $\alpha \in Z$. so $a \in$ Z.

From (*), we have, $a_0 + a_1 \cdot \frac{\alpha}{\beta} + \cdots + a_{n-1}\frac{\alpha^{n-1}}{\beta^{n-1}} + \frac{\alpha^n}{\beta^n} = 0$

$So\ a_0 + a_1 \cdot \frac{\alpha}{\beta} + \cdots + a_{n-1} \cdot \frac{\alpha^{n-1}}{\beta^{n-1}} = -\frac{\alpha^n}{\beta^n}$ and that

$a_0\beta^n + a_1\alpha\beta^{n-1} + \cdots + a_{n-1}\alpha^{n-1} \cdot \beta = -\alpha^n$, that is,

$a_0\beta^n = -\alpha^n - a_1\alpha\beta^{n-1} \cdots - a_{n-1}\alpha^{n-1}\beta$

$= -\alpha(a_1\beta^{n-1} + \cdots + a_{n-1}\alpha^{n-2}\beta) - \alpha^n$

$So\ a_0\beta^n = -\alpha[a_1\beta^{n-1} + \cdots + a_{n-1}\alpha^{n-2}\beta + \alpha^{n-1}]$ and that

$\alpha \mid a_0\beta^n$

Now $\alpha \mid a_0$, since $(\alpha, \beta) = 1$. Hence α divides a_0.

1.2.18 Proposition: (Eisenstein Criterion): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z[x]$ with $n \geqslant 1$. If there is a prime number p such that $p|a_0, p|a_1, p|a_2, \ldots, p|_{a_{n-1}}, p \nmid a_n, p^2 \nmid a_0$, then $f(x)$ is irreducible over Q.
Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z[x]$ with $n \geqslant 1$ and let p be a prime number such that $p|a_0, p|a_1, p|a_2, \ldots, p|_{a_{n-1}}, p \nmid a_n, p^2 \nmid a_0$.
Claim: $f(x)$ is irreducible over Q.

First we show that $f(x)$ is irreducible in $Z[x]$.
If possible, Suppose that $f(x)$ is reducible over Z. Then $f(x) = g(x) \cdot h(x)$,
where $g(x) = b_0 + b_1x + \cdots + b_rx^r$ and $b_i, c_i \in \mathbb{Z}, r < n, s < n \ \& r + s = n$
$h(x) = c_0 + c_1x + \cdots + c_sx^s$
Therefore $a_0 = b_0c_0, a_n = b_nc_s \& a_i = b_0c_i + b_ic_{i-1} + \cdots + b_ic_0$ for all i
Since $p|a_0$, we have $p|b_0c_0$ so $p|b_0$ (or) $p|c_0$ (since p is prime).
[If $p|b_0 \& p|c_0 \Rightarrow p^2|b_0c_0 = a_0$, which is a contradiction]

Case (i) : Suppose $p|b_0$ and $p \nmid c_0$
If all the coefficients b_i are divisible by 'p' Then p divides all a_k' ($0 \le k \le n$)
and $p|a_n$, which is a contradiction.
So p does not divides all the coefficients b_i.
Let 'm' be the least positive integer such that $p \nmid b_m$.
This means that p divides $b_1, b_2, \ldots, b_{m-1}$.
Now $a_m = b_mc_0 + b_{m-1}c_1 + \cdots + b_0c_m$ so $b_mc_0 = a_m - (b_{m-1}c_1 + \cdots + b_0c_m)$
Since p divides $a_m, b_{m-1}, \ldots, b_0c_m$, we have, so $p \mid b_mc_0$
$p|b_m$ (or) $p|c_0$ ($\because p$ is prime)
But $p \nmid c_0$. So we must have $p|b_m$ which is a contradiction.
So our assumption is wrong.

Case (ii) : Suppose $p|c_0 \& p \nmid b_0$
Similarly, as in case(i), we get that our assumption is wrong.
Therefore f(x) is irreducible over Q.

1.3 SUMMARY:

An irreducible polynomial over a field F is a non-constant polynomial that cannot be factored into polynomials of lower degree over F. This lesson explores conditions under which a polynomial is irreducible over F. Eisenstein's Criterion provides a powerful tool for establishing the irreducibility of polynomials over Q.

1.4 TECHNICAL TERMS:

Field: A commutative ring with unity where every non-zero element has a multiplicative inverse.
Unit: An invertible element in a ring.
Prime element: A non-zero, non-unit element p such that p|ab implies p|a or p|b .
Irreducible element: An element (or polynomial) that is a non-zero non-unit and cannot be factored into two non-unit factors.
Leading coefficient: The coefficient of the highest-degree term in a polynomial.
Content of a polynomial: The greatest common divisor (g.c.d) of its coefficients.
Primitive polynomial: A polynomial whose content is 1.
Monic polynomial: A polynomial whose leading coefficient is 1.

1.5 SELF-ASSESSMENT QUESTIONS:

Question 1: Why Eisenstein's Criterion is useful and what are its limitations?
Answer: Eisenstein's Criterion provides a sufficient (but not necessary) condition to establish the irreducibility of a polynomial over $\mathbb{Q}$. It is useful because it offers a

straightforward test when applicable. However, its limitation is that it does not apply to all irreducible polynomials. Some irreducible polynomials do not satisfy the criterion, and some polynomials may need to be transformed (e.g., via a change of variable) before the criterion can be applied.

Question 2: Can Eisenstein's Criterion be used over arbitrary rings or only over $\mathbb{Z}$ and $\mathbb{Q}$? Explain.

Answer: Eisenstein's Criterion is primarily stated for polynomials in $\mathbb{Z}$[x] to test irreducibility over $\mathbb{Q}$. However, generalized forms of the criterion exist for unique factorization domains, where similar conditions involving prime elements can be applied. But its standard and most practical usage remains in the context of $\mathbb{Z}$ and $\mathbb{Q}$**.**

Question 3: Test whether the polynomial $x^3 + 3x + 2 \in \frac{Z}{\langle 7 \rangle}[x]$ (or) $Z_7[x]$ is irreducible Over the field $\frac{z}{\langle 7 \rangle}$ or not ?

Solution :

Let $f(x) = x^3 + 3x + 2$ be a polynomial in $\frac{z}{\langle 7 \rangle}[x]$.

Here $\deg f(x) = 3$.

By proposition 1.2.10, we have that $f(x)$ is reducible over $\frac{z}{\langle 7 \rangle}$, if $f(x)$ has a root in $\frac{z}{\langle 7 \rangle}$. Let us check whether $f(x)$ has a root in $\frac{z}{\langle 7 \rangle}$ or not.

Since $f(3) = 38,\ 0 \neq 3 \in \frac{z}{\langle 7 \rangle}$ is not a root of $f(x)$. Similarly one can easily verify that no element of $\frac{z}{\langle 7 \rangle}$ is a root of $f(x)$. Then by proposition 1.2.10, we have that $f(x)$ is irreducible over $\frac{z}{\langle 7 \rangle}$.

Question 4: Test whether the polynomial $f(x) = 1 + x + \cdots + x^{p-1}$, where p is prime number is irreducible over Q or not ?

Solution: Given $f(x) = 1 + x + \cdots + x^{p-1}$, where p is a prime number.

$$(x-1)f(x) = (x-1)[1 + x + \cdots + x^{p-1}]$$
$$= x - 1 + x^2 - x + \cdots + x^p - x^{p-1}$$

So $(x-1)f(x) = x^p - 1$

Put $y = x - 1$ so $x = 1 + y$.

Now $yf(x) = (y+1)^p - 1$

$$= \left(1 + py + \frac{p(p-1)}{2!}y^2 + \cdots\right) - 1$$
$$= py + \frac{p(p-1)}{2!}y^2 + \cdots$$

So $\Rightarrow f(x+y) = p + \frac{p(p-1)}{2!}y + \cdots + y^p$

From equation (1), clearly $p | p_{c_r}$, where $0 < r \leqslant p-1$ and $p^2 \nmid p_{c_{p-1}}$ and $p \nmid 1$

Therefore by Eisenstein criterion, $f(x)$ is irreducible over Q.

Question 5. Determine which of the following polynomials are irreducible over Q.

a) $x^3 - 5x + 10$

b) $x^4 - 3x^2 + 9$

c) $2x^5 - 5x^4 + 5$

Solution :

a) Let $f(x) = 10 - 5x + 0 \cdot x^2 + x^3$. Take $p = 5$

Note that $p|10\,, p|5\,, p|0, p \nmid 1$ & $p^2 \nmid 10$

Then by Eisenstein criterion, $f(x)$ is irreducible over Q.

Similarly, we can solve (b) and (c) by taking appropriate 'p'

1.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul, 1997, Basic Abstract Algebra, 2nd edition, UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York.
3. Khanna, V. K. and S. K. Bhambari, A Course in Abstract Algebra, 3rd edition, New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition, Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Prof. R. Srinivasa Rao**

LESSON- 2

ADJUNCTION OF ROOTS

OBJECTIVES:

- To construct field extensions by adjoining roots of irreducible polynomials to a base field.
- To analyze the properties of the extended field such as its degree and structure.
- To study the concept of minimal polynomials of the adjoined roots.
- To provide a foundation for Galois Theory and the study of finite extensions.

STRUCTURE:

2.1 INTRODUCTION:

Adjunction of roots involves creating field extensions by adding roots of a polynomial that are not in the given field. This process enriches the field structure and is fundamental in understanding algebraic extensions. For a field F and an irreducible polynomial f(x) over F, we adjoin a root α to form F(α). The extension F(α) is the smallest field containing both F and α, and α satisfying f(x). This concept is crucial for constructing fields which are finite extensions of the given field. Kronecker's theorem asserts that for any non-constant polynomial f(x) ∈ F[x], there exists an extension field, in which f(x) has a root.

2.2 EXTENSION OF FIELDS:

2.2.1. Definition: If F is a subfield of a field E, then E is called an extension field of F (or) simply an extension of F.

Note that it E is a field and F is a non-empty subset of E. then F is a subfield of E if $a = b, ab, a^{-1}(a \neq 0)$ are in F for all $a, b \in F$

Note: If E is an extension of F, then trivially E is a vector space over F. The dimension of E over F is usually written as [E: F].

2.2.2 Definition: Let E be an extension of F. Then the dimension of E considered as a vector space over F is called the degree of E over F and is denoted by [E: F].

Note: The degree of E over F is written as $[E : F]$. If $[E : F] < \infty$, then E is called a finite extension of F. If E is not a finite extension of F, then E is called an infinite extension of F.

2.2.3 Theorem: Let $F \subseteq E \subseteq K$ be fields. If $[K : E] < \infty$ and $[E : F] < \infty$, then (i)$[K : F] < \infty$ (ii) $[K : F] = [K : E][E : F]$

Proof: Let F, E, K be three fields such that $F \subseteq E \subseteq K$.

Given that $[K : E] < \infty$ and $[E : F] < \infty$.

Suppose $[K : E] = m$ and $[E : F] = n$

So, let $\{v_1, v_2, \dots, v_m\}$ be a basis of K over E and $\{\omega_1, \omega_2, \dots, \omega_n\}$ be a basis of E over F.

Write $S = \left\{ v_i\omega_j / \begin{matrix} 1 \le i \le m, \\ 1 \le j \le n \end{matrix} \right\}$

Now we show that $[K : F] < \infty$, that is, the dimension of K over F is finite.

Let $u \in K$.

Since $\{v_1, v_2, \dots, v_m\}$ is a basis of K over E, we have $u = a_1v_1 + a_2v_2 + \cdots + a_mv_m$ (1),

where $a_i \in$ E; $1 \le i \le m$.

Since $a_i \in E$, $1 \le i \le m$ and $\{\omega_1, \dots \omega_n\}$ is a basis of E over F, a_i can be written as

$$a_i = b_{i1}\omega_1 + b_{i2}\omega_2 + \cdots + b_{in}\omega_n, \text{ where } b_{i_j} \in F, 1 \le i \le m,$$

Substituting a_i in (1), we have for $1 \le j \le n$

$$\begin{aligned} u =& (b_{11}w_1 + b_{12}\omega_2 + \cdots + b_{1n}\omega_n)v_1 + (b_{21}\omega_1 + b_{22}\omega_2 + \cdots + b_{2n}\omega_n)v_2 \\ &+ \cdots + \left(b_{m1}\omega_1 + b_{m_2}\omega_2 + \cdots + b_{mn}\omega_n\right)v_m \\ =& b_{11}\omega_1v_1 + b_{12}\omega_2v_1 + \cdots + b_{1n}w_nv_1 + b_{21}w_1v_2 + \cdots + b_{2n}\omega_nv_2 \\ &+ \cdots + b_{m1}w_1v_m + b_{m2}w_2v_m + \cdots + b_{mn}\omega_nv_m \end{aligned}$$

So, u is the linear combination of the vectors $\left\{ v_i\omega_j \middle| \begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix} \right\}$

Therefore every element in K can be expressed as the linear combination of the set of vectors $\left\{ v_i\omega_j \middle| \begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix} \right\}$.

We show that the set $S = \left\{ v_i\omega_j \middle| \begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix} \right\}$ is linearly independent over F.

Suppose that

$$c_{11}v_1\omega_1 + c_{12}v_1\omega_2 + \cdots + c_{1n}v_1\omega_n + c_{21}v_2\omega_1 + c_{22}v_2\omega_1 + \cdots + c_{2n}v_2\omega_n + \cdots +$$

$c_{m1}v_m\omega_1 + \cdots + c_{mn}v_m\omega_n = 0$, where $c_{ij} \in F; 1 \le i \le m; 1 \le j \le n$.

we have $(c_{11}\omega_1 + c_{12}\omega_2 + \cdots + c_{1n}\omega_n)v_1 + (c_{21}\omega_1 + c_{22}\omega_2 + \cdots + c_{2n}\omega_n)v_2) +$

$$\cdots + \left(c_{m1}\omega_1 + c_{m_2}\omega_2 + \cdots + c_{mn}\omega_n\right)v_m = 0.$$

Since the set $\{v_1, v_2, \dots, v_m\}$ is linearly independent in K over the field E, we have

$$c_{11}\omega_1 + c_{12}\omega_2 + \cdots + c_{1n}\omega_n = 0$$
$$c_{21}\omega_1 + c_{22}\omega_2 + \cdots + c_{2n}\omega_n = 0$$

… … … … … … … … … … … … … … … … ….

$c_{m1}\omega_1 + c_{m_2}\omega_2 + \cdots + c_{mn}\omega_n = 0$

Since $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is linearly independent in E over F, we have

$c_{ij} = 0$ for $1 \leq i \leq m, 1 \leq j \leq n$

Hence S = $\left\{v_i\omega_j \middle| \begin{matrix}1 \leq i \leq m \\ 1 \leq j \leq n\end{matrix}\right\}$ is a linearly independent set over F with mn elements.

Therefore $[K : F] < \infty$ and the no. of elements in the basis of K over F is mn

So, $[K : F] = mn = [K : E\,][E : F]$

Hence $[K : F] = [K : E\,][E : F]$

Note: A one-to-one homomorphism of a field F into a field E is called an embedding of F into E.

Note that if E and F are fields then a mapping h: $F \to E$ is a homomorphism if

(i) $h(a + b) = h(a) + h(b)$ and

(ii) $h(ab) = h(a)h(b)$ for all $a, b \in E$

2.2.4 Proposition: Let E and F be fields and let $\sigma: F \to E$ be an embedding of F into E, then there exists a field K such that F is a subfield of K and σ can be extended to an isomorphism of K onto E.

Proof: let F and E be fields and $\sigma: F \to E$ be an embedding.

that is, $\sigma: F \to E$ is a monomorphism, that is, $\sigma: F \to E$ is a homomorphism and one-one.

Let S be the set whose cardinality is same as that of $E - \sigma(F)$ and it is disjoint from F.

Consider $f: S \to E - \sigma(\mathrm{F})$ be a one-to-one correspondence between S and $E - \sigma(\mathrm{F})$.

Write $K = F \cup S$.

Define a mapping $\sigma^*: K \to E$ as follows:

Let $a \in K$.

If $a \in F$, then define $\sigma^*(a) = \sigma(a)$.

If $a \in S$, then define $\sigma^*(a) = f(a)$.

By the above definition, σ^* is clearly well-defined and onto.

Let $a, b \in K$ and $\sigma^*(a) = \sigma^*(b)$

If $a, b \in$ F, then $\sigma^*(a) = \sigma^*(b)$ and that

$\sigma(a) = \sigma(b)$ and that

$a = b$($\because \sigma: F \to E$ is one-one)

If $a, b \in S$, then $f(a) = f(b)$and that $a = b$

Let $a \in$ F and $b \in S$.

So, $\sigma(a) = f(b) \in \sigma(F) \cap (E - \sigma(F))$

But we know that $\sigma(F) \cap E - \sigma(F) = \phi$, which is a contradiction.

Therefore both $a, b \in F$ (or) both $a, b \in S$.

So $\sigma^*: K \to E$ is one-one and hence a bijection and clearly $\sigma^*: K \to E$ is an extension of σ.

For any two elements $x, y \in K$, define

$$x + y = \sigma^{*^{-1}}(\sigma^*(x) + \sigma^*(y))$$
$$xy = \sigma^{*^{-1}}(\sigma^*(x) \cdot \sigma^*(y))$$

Under the above defined operations, it is clear that K is a field.

Also, the definitions defined here coincide with the given addition and multiplications of the elements of the original field F.

Let $a, b \in F$.

$$a + b = \sigma^{*^{-1}}[\sigma^*(a) + \sigma^*(b)]$$
$$= \sigma^{*^{-1}}[\sigma(a) + \sigma(b)]$$
$$= \sigma^{*^{-1}}[\sigma(a + b)] = \sigma^{*-1}[\sigma^*(a + b)] = a + b$$

Therefore F is a subfield of K (or) in other words K is the extension of F.

Note: If σ is an embedding of a field F into a field E, then we identify F with its homomorphic image $\sigma(F)$. So, we can write ' a ' in place of $\sigma(a)$ for each $a \in F$ and this E can be regarded as an extension of F. Hence, whenever there is an embedding of an field F into a field E, we say that E is an extension of F.

2.2.5 Theorem: Let $p(x)$ be an irreducible polynomial in $F[x]$, then there exists an extension E of F in which $p(x)$ has a root.

Proof: Let $p(x)$ be an irreducible polynomial in $F[x]$.

So, $\langle p(x) \rangle$ is a maximal ideal in $F[x]$. $< p(x) >$ is the ideal of $F[x]$ generated by $p(x)$

Then by known result, $\frac{F[x]}{\langle p(x) \rangle}$ is a field.

Put $E = \frac{F[x]}{\langle p(x) \rangle}$

Now we show that E is an extension of F.

Define $\phi: F \to E$ by $\phi(a) = \bar{a}$ where $\bar{a} = a + < p(x) >$.

Now we prove that the mapping $\phi: F \to E$ is an embedding.

Let $a, b \in F$ such that $\phi(a) = \phi(b)$.

So $\bar{a} = \bar{b}$, that is,

$a + \langle p(x) \rangle = b + \langle p(x) \rangle$, that is,

$a - b \in \langle p(x) \rangle$, that is,

$a - b = f(x)p(x)$ for some $f(x) \in F[x]$. This is possible only when

$f(x) = 0$ as $\deg\ p(x) \geq 1$

Now $a - b = 0$, that is,

$a = b$

Therefore ϕ is one-one.

We prove now that ϕ is a homomorphism.

Let $a, b \in F$.

Then $\phi(a + b) = \overline{a + b} = \bar{a} + \bar{b}$= $\phi(a) + \phi(b)$ and $\phi(ab) = \overline{ab} = \bar{a}\bar{b} = \phi(a) \cdot \phi(b)$

So $\phi: F \to E$ is a monomorphism, that is,$\phi: F \to E$ is an embedding.

Then by known result, E can be regarded as an extension of F and also we can also identify F as the homomorphic image $\phi(F)$.

So we can write a in place of $\bar{a}$.

Now we prove $p(x)$ has a root in E .

Let $p(x) = a_0 + a_1x + \cdots + a_nx^n; a_n \neq 0, n \geq 1$

Then $\overline{p(x)} = p(x) + \langle p(x)\rangle = \langle p(x)\rangle = \overline{0}$

$So\ \overline{a_0 + a_1x + \cdots + a_nx^n} = \overline{0}$, that is,

$\bar{a}_0 + \bar{a}_1\bar{x} + \cdots + \bar{a}_n\bar{x}^n = \overline{0}$, that is,

$\Rightarrow a_0 + a_4\bar{x} + \cdots + a_n\bar{x}^n = \bar{0}$

So $p(\bar{x}) = \bar{0}$, where $\bar{x} = x + \langle p(x)\rangle \in \dfrac{F[x]}{\langle p(x)\rangle} = E$

Therefore $\mathrm{p}(x)$ has a root in E .

2.3 KRONECKER THEOREM AND ITS APPLICATIONS:

2.3.1 Kronecker Theorem: Let $f(x) \in F[x]$ be a non-constant polynomial, then there exists an extension E of F in which $f(x)$ has a root.

Proof: Let$f(x) \in F[x]$ be a non-constant polynomial.

Case(i):If $f(x)$ has a root in F then put $E = F$.

Then clearly E is an extension of F and $f(x)$ has a root in E .

Case(ii): If $f(x)$ has no root in F, then let $p(x)$ be an irreducible factor of $f(x)$.

Then, by Theorem 2.2.5, corresponding to the irreducible polynomial $p(x)$, there exists an extension E of F in which $p(x)$ has a root and hence $f(x)$ has a root in E .

2.3.2 Corollary: Let $f_1(x), f_2(x), \ldots, f_m(x)$ be a set of non-constant polynomials over F. Then there exists an extension E of F in which each $f_i(x)$ has a root.

Proof: Let $f_1(x), f_2(x), \ldots, f_m(x)$ be a set of non-constant polynomials over the field F.

Consider $f_1(x)$ be a non-constant polynomial in $F[x]$.

Then by Kronecker theorem, there exists an extension K_1 of F such that $f_1(x)$ has a root in K_1.

Clearly $f_2(x) \in K_1[x]$ is a non-constant polynomial.

By Kronecker theorem, there exists an extension K_2 of K_1 such that $f_2(x)$ has a root in K_2.

If we continue the same process, we get successive fields $K_1 \subset K_2 \subset \cdots \subset K_m$ such that each K_i contains root of $f_i(x), 1 \leqslant i \leqslant m$.

Therefore K_m is the required extension of F in which each $f_i(x)$ has a root.

2.3.3 Definition: Let $p(x)$ be an irreducible polynomial in $F[x]$ and u be the root of $p(x)$ in an extension field E of F. Then we denote $F(u)$ to be the subfield of E generated by $F \cup \{u\}$, that is, $F(u)$ is the subfield of E generated by $F \cup \{u\}$, that is, smallest subfield of E containing F and u , that is, intersection of all subfields of E containing F and u . In general, if S is the subset of E , then we denote $F(S)$ to be the smallest subfield of E containing F and S.

2.3.4 Theorem: Let $p(x)$ be an irreducible polynomial in $F[x]$ and let u be a root of $p(x)$ in an extension E of F. Then

(i) $F(u)$, the subfield of E generated by F and u, is the set

$$F[u] = \{b_0 + b_1u + \cdots + b_mu^m / b_0 + b_1x + \cdots + b_mx^m \in F[x]\}$$

(ii) If the degree of $p(x)$ is n, the set $\{1, u, \ldots, u^{n-1}\}$ forms a basis of $F(u)$ over F, i.e each element of $F(u)$ can be written uniquely as $c_0 + c_1u + \cdots + c_nu^{n-1}$, where $c_i \in F$ and $[F(u): F] = n$.

Proof: let F, E be two fields such that E is an extension of F.

Let $p(x)$ be an irreducible polynomial in $F[x]$. Also let u be a root of $p(x)$ in E .

i) Define a mapping $\phi: F[x] \to E$ by

$\phi(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1u + \cdots + a_nu^n$ where $a_0 + a_1x + \cdots + a_nx^n \in F[x]$

Clearly ϕ is well-defined.

Let $f(x),\ g(x) \in F[x]$.

Then $\phi(f(x) + g(x)) = f(u) + g(u) = \phi(f(x)) + \phi(g(x))$

$\phi(f(x) \cdot g(x)) = f(u) \cdot g(u) = \phi(f(x)) \cdot \phi(g(x))$

Therefore ϕ is a homomorphism.

Then by fundamental theorem of homomorphism, we have that $\frac{F[x]}{ker\phi} \cong \phi(F[x]) = F[u]$….

(1)

Now we prove that ker $\phi = \langle p(x) \rangle$

Here ker $\phi = \{f(x) \in F[x] / \phi(f(x)) = 0\} = \{f(x) \in F[x] / f(u) = 0\}$

Since $p(u) = 0$, we have $p(x) \in$ ker ϕ.

We know that $F[x]$ is a principal ideal domain.

So, ker ϕ is principal ideal of $F[x]$ and ker $\phi = \langle g(x) \rangle$ for some $g(x) \in F[x]$

Therefore $p(x) \in \ker\phi = \langle g(x) \rangle$.

$\Rightarrow p(x) = h(x) \cdot g(x)$ for some $h(x) \in F[x]$

Since $p(x)$ is irreducible in $F[x], h(x)$ is a constant polynomial and hence

$< p(x) > = < g(x) >$

Therefore ker $\phi = \langle p(x) \rangle$

So, from (1), $\frac{F[x]}{\langle p(x) \rangle} \cong F[u]$

We know that $\frac{F[x]}{\langle p(x) \rangle}$ is a field as $p(x)$ is irreducible in $F[x]$

This implies $F[u]$ is a field and it is the smallest subfield of E containing F & $u, F[u]$

Therefore $F[u] = F(u)$

(ii) Let deg $p(x) = n$.

Then u is not a root of any polynomial in $F[x]$ whose degree is less than ' n '.

Now we show that the set $\{1, u, \dots, u^{n-1}\}$ is linearly independent.

Consider, $b_0 + b_1 \cdot u + \cdots + b_{n-1}u^{n-1} = 0; b_i \in F$.

Suppose that $g(x) = b_0 + b_1 \cdot x + \cdots + b_{n-1}x^{n-1} \neq 0$.

Now $g(x) \in F[x]$ and deg g$(x) < n$ and $g(u) = 0$, a contradiction to the irreducibility of p(x).

So $g(x) = 0$ and that $b_i = 0$ for all $i = 0,1, \dots, n-1$.

Therefore $\{1, u, \dots, u^{n-1}\}$ is linearly independent over F.

Now we show that the set $\{1, u, \dots, u^{n-1}\}$ generates $F[u]$ over F.

That is, every element in $F[u]$ can be written uniquely as the linear combination of the set of vectors $\{1, u, \dots, u^{n-1}\}$.

Let f(u) ∈ F[u] where $f(x) \in F[x]$.

By division algorithm there exists $t(x), r(x) \in F[x]$ such that $f(x) = p(x) \cdot t(x) + r(x)$ where $r(x) = 0$ (or) $\deg\ r(x) < \deg\ p(x) = n$.

Now $f(u) = p(u)t(u) + r(u)$. Since $p(u) = 0$,

$f(u) = r(u)$

Since deg $r(x) <$ deg$f(x) = n$, we can write $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, $a_i \in F$.

Therefore $f(u) = r(u) = a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$

i.e. $f(u)$ is linear combination of vectors $\{1, u, \ldots, u^{n-1}\}$

Therefore $\{1, u, \ldots, u^{n-1}\}$ generates $F(u)$ over F. Therefore it is a basis for $F(u)$ over F.

Hence $[F(u):F] = n$

2.4 SUMMARY:

Adjunction of roots refers to the process of extending a field F by adjoining a root α of an irreducible polynomial f(x) ∈ F[x]. The extended field F(α) contains all elements expressible as rational expressions in α with coefficients from F. This construction allows us to form new fields. The degree of the extension [F(α):F] equals to the degree of the minimal polynomial of α over F. Kronecker's theorem states that for any non-constant polynomial f(x) ∈ F[x], there exists an extension field of F where f(x) has at least one root.

2.5 TECHNICAL TERMS:

- Root of a polynomial $\boldsymbol{f(x)}$: An element α in some extension field such that f(α)=0.
- Adjunction of a root: The process of constructing a field extension by adding a root α of a polynomial f(x) ∈ F[x] to F.
- Minimal Polynomial of u over F: The monic irreducible polynomial in F[x] for which u is a root.
- Algebraic Element over $\boldsymbol{F}$: An element α in an extension field E of F that satisfies a polynomial equation with coefficients in F.
- Algebraic Extension of $\boldsymbol{F}$: An extension E of F where every element of E is algebraic over F.
- Degree of Extension: The dimension of E as a vector space over F and it is denoted by [E:F]

2.6 SELF-ASSESSMENT QUESTIONS:

Question 1: What is meant by the adjunction of a root to a field?

Answer: The adjunction of a root to a field refers to the process of extending a field F by including an element α that is a root of a given polynomial f(x) ∈ F[x], which does not already have a root in F. The resulting extension is denoted F(α), which is the smallest field containing F and α.

Question 2: Why is the concept of adjunction important in the theory of field extensions?

Answer: Adjunction is fundamental in building larger fields that contain roots of polynomials that are not in the base field. This process allows the construction of algebraic extensions and eventually leads to algebraic closures. It helps in understanding how fields can be systematically extended and analyzed using the roots of irreducible polynomials, laying the foundation for Galois theory.

Question 3: Let K be a finite extension of F and E be the subfield of K containing F. Does[E: F] divides $[K : F]$?

Solution: Let F, E, K be three fields such that $F \subseteq E \subseteq K$.

Given that the dimension of K over F is finite i.e.$[K : F] < \infty$.

Since K is finite dimensional over F and E is a subspace of K, we have E is finite dimensional over F.$i.e.[E : F] < \infty$.

We know that any set of elements in K, which are linearly independent over E are also linearly independent over F.

So, Dimension of K over $E = [K : \mathrm{E}]$

= Maximum no. of linearly independent vectors in K over F
$\leqslant$ Maximum no. of linearly independent vectors in K over F.

=The dimension of K over F = $[K : F]$

i.e.$[K : E] =$ dimension of K over $E \leq$ dimension of$K$ over F $= [K : F] < \infty$

By Theorem 2.2.3, we have that $[K : F] = [K : E][E : F]$.

$$\text{So } [E : F] | [K : F]$$

Question 4: Let K be an extension of F and $[K : F]$ is a prime number p. Can there be a field L such that $F \subset L \subset K$?

Solution: Let K be an extension of F.

Given that $[K : F] = p, p$ is a prime number.

Suppose, if possible, there is a field ' L 'such that $F \subset L \subset K$

By theorem 2.2.3. we have that $[K : F] = [K : L][L: F]$

$p = [K : L][L: F]$, where p is prime.

So, $[K : L] = 1$ (or) $[L: F] = 1$

$K = L$ (or) $L = F$, which is a contradiction.($\because F \subset \mathrm{L} \subset K$)

Therefore there is no field L such that $F \subset \mathrm{L} \subset K$.

2.7 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul, 1997, Basic Abstract Algebra, 2nd edition, UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York.
3. Khanna, V. K. and S. K. Bhambari, A Course in Abstract Algebra, 3rd edition, New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition, Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House, 2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Prof. R. Srinivasa Rao**

LESSON- 3

ALGEBRAIC EXTENSIONS

OBJECTIVES:

- To learn algebraic elements and minimal polynomials.
- To understand the concept of field extensions and field extensions which are generated by a single algebraic element.
- To distinguish between algebraic extensions and transcendental extensions.
- To explore the properties of finite extensions.

STRUCTURE:

3.1 INTRODUCTION:

In abstract algebra, the concept of an extension field arises naturally when considering how one field can be expanded to include roots of polynomials that might not exist in the given field. The study of algebraic extensions is fundamental in understanding how fields can be enlarged in a controlled way and is a stepping stone to more advanced topics such as Galois theory**.** An extension field E of a field F is a field containing F as a subfield. In this lesson, we discuss simple extension, degree of an extension, properties of algebraic elements, minimal polynomial of an algebraic element and related theorems.

3.2 ALGEBRAIC EXTENSIONS:

3.2.1 Definition: Let E be an extension of F. An element $\alpha \in E$ is said to be an algebraic element over F if there exists elements $a_0, a_1, \dots, a_n; n \geqslant 1$ of F, not all equal to zero such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. In other words, an element $\alpha \in E$ is said to be an algebraic element over F if there exists a non-constant polynomial $p(x) \in F[x]$ with $p(\alpha) = 0$.

3.2.2 Theorem: Let E be an extension field of F and let $u \in E$ be an algebraic element over F.
Let $p(x) \in F[x]$ be a polynomial of the least degree such that $p(u) = 0$. Then
(i) $p(x)$ is irreducible over F.

(ii) If $g(x) \in F[x]$ is such that $g(u) = 0$, then $p(x) \mid g(x)$.

(iii) There is exactly one monic polynomial $p(x) \in F[x]$ of least degree such that $p(u) = 0$.

Proof: Let E be an extension of F and $u \in E$ be an algebraic element over F. Let $p(x) \in F[x]$ be the least degree polynomial such that $p(u) = 0$.

(i) Suppose if possible $p(x)$ is not irreducible over F.

Then $p(x)$ is reducible over F.

So by definition $p(x) = p_1(x) \cdot p_2(x)$, where $p_1(x), p_2(x) \in F[x]$ and $0 < \deg p_1(x) < \deg p(x)$ and $0 < \deg p_2(x) < \deg p(x)$.

Now $p(u) = p_1(u) \cdot p_2(u) = 0$ $(\because p(u) = 0)$

This implies either $p_1(u) = 0$ (or) $p_2(u) = 0$, which is a contradiction

Therefore $p(x)$ is irreducible over F.

(ii) Let $g(x) \in F[x]$ be a polynomial in $F[x]$ such that $g(u) = 0$.

By division algorithm, there exists polynomials $q(x), r(x) \in F[x]$ such that $g(x) = q(x) \cdot p(x) + r(x)$, where $r(x) = 0$ (or) $\deg r(x) < \deg p(x)$

So, $g(u) = q(u) \cdot p(u) + r(u)$. Since $g(u) = 0$, and $p(u) = 0$, $r(u) = 0$

Now $r(x) = 0$ as p(x) is the least degree polynomial such that p(u)=0.

So $g(x) = g(x) \cdot p(x)$ and that $p(x) \mid g(x)$.

(iii) Suppose that $p(x)$ is monic polynomial.

[Otherwise, if c is the leading co-efficient of $p(x)$, then $c^{-1}p(x)$ is a monic polynomial of least degree & $c^{-1}p(u) = 0$.]

Let $g(x)$ be another least degree monic polynomial in F[x] with $g(u) = 0$.

Then by (ii), $p(x) | g(x)$ and $g(x) | p(x)$ Also $p(x), g(x)$ are monic. So $p(x) = g(x)$

Hence, there is exactly one monic polynomial of least degree such that $p(u) = 0$.

3.2.3 Definition: The monic irreducible polynomial in $F[x]$ of which u is a root is called the minimal polynomial of u over F.

3.2.4 Definition: An extension field E of F is called an Algebraic extension of F if each element of E is algebraic element over F. If E is not an algebraic extension, then E is called a transcendental extension.

3.2.5 Theorem: If E is a finite extension of F, then E is an algebraic extension of F (Or) Every finite extension of F is an algebraic extension of F.

Proof: Let E be a finite extension of F.

Suppose that $[E: F] = n$.

Now we show that E is an algebraic extension of F.

Let $u \in E$.

Then the set $\{1, u, u^2, \dots, u^n\}$ with $(n+1)$ number of elements is linearly dependent in E over F. So, there exists $a_0, a_1, \dots, a_n \in F$, not all zero such that $a_0 + a_1u + \cdots + a_nu^n = 0$ i.e. there exists a non-constant polynomial $a_0 + a_1x + \cdots + a_nx^n$ in $F[x]$ such that $a_0 + a_1u + \cdots + a_nu^n = 0$

This implies u is algebraic over F. So, every element of E is algebraic over F.

Therefore E is an algebraic extension of F.

Hence every finite extension is an algebraic extension of F.

Note: The converse of Theorem 3.2.5 need not be true. i.e. an algebraic extension need not be a finite extension.

3.2.6 Theorem: If E is an extension of F and $u \in E$ is algebraic over F, then $F(u)$ is an algebraic extension of F.

Proof: Let E be an extension of F and let $u \in E$ be an algebraic element over F.

By definition of algebraic element, there exists a non-constant polynomial $f(x)$ in F[x] such that $f(u) = 0$.

Since $f(x) \in F[x]$& $F[x]$ is a U.F.D, $f(x)$ can be written as, $f(x) = dp_1(x) \cdot p_2(x) \cdots p_n(x)$ where each $p_i(x)$ is an irreducible polynomial in $F[x]$.

Since u is a root of $f(x), u$ is root of the polynomial $p_i(x)$ for some i. So let $p_i(x)$ is an irreducible polynomial having u as a root.

Then by known theorem, we have $[F(u): F] = \deg \mathrm{p}(x) = n(say)$

i.e.$F(u)$ is a finite extension of F.

Then by Theorem 3.2.6, $F(u)$ is an algebraic extension of F.

3.2.7 Definition: An extension E of F is called finitely generated if there exists a finite number of elements $u_1, u_2, \dots, u_n$ in E such that the smallest subfield of E containing F and $\{u_1, u_2, \dots, u_n\}$ is E itself. i.e. $E = F(u_1, u_2, \dots, u_n)$

Note: A finitely generated extension need not be an algebraic extension.

Let $F[x]$ be a polynomial ring in the indeterminate x over the field F. Let E be the field of quotients of $F[x]$ i.e.,$E = \left\{ \frac{f(x)}{g(x)} / g(x) \neq 0 , f(x) \in F[x] \right\}$. Then E = F$(x)$ is finitely generated extension of F. Also we know that x is not an algebraic element over F. If x is an algebraic element over F, then there exists $a_0, a_1, \dots, a_n$ in F not all zero such that $a_0 + a_1x + \cdots + a_nx^n = 0$, which is a contradiction. So $E = F(x)$ is not an algebraic extension of F.

Hence a finitely generated extension need not be an algebraic extension.

3.2.8 Theorem: Let $E = F(u_1, u_2, \dots, u_r)$ be a finitely generated extension of F such that each u_i, $i = 1,2, \dots, r$ is algebraic over F. Then E is finite over F and hence an algebraic extension of F.

Proof: Let $E = F(u_1, u_2, \dots, u_r)$ be a finitely generated extension of F such that each u_i is algebraic over F.clearly $F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \cdots \subseteq F(u_1, u_2, \dots, u_r)$

Write $E_i = F(u_1, u_2, \dots, u_i)$ for all $i = 1,2, \dots, r$.Then $F \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_{r-1} \subseteq E_r = E$.

We know that if an element $\alpha \in E$ is algebraic over F, then ' α ' is algebraic over any field K such that $E \supseteq K \supseteq F$.

Given that $u_i \in E$ is algebraic over $F\ \forall i = 1,2, \dots, r$. So, $u_i \in E$ is algebraic over E_{i-1} for all $i = 1,2, \dots, r$ with $E_0 = F$.

This implies $E_{i-1}(u_i)$ is a finite extension of $E_{i-1} \forall i = 1,2, \dots$r

i. e, E_i is a finite extension of $E_{i-1} \forall i = 1,2, \dots, r$. So let, $[E_i : E_{i-1}] = n_i$ for all $i = 1,2, \dots,$ r

We know that $[E : F] = [E : E_{r-1}][E_{r-1} : E_{r-2}] \dots [E_1 : F] = n_r n_{r-1} \dots n_1 < \infty$

This implies E is a finite extension of F.

Hence E is an algebraic extension of F.

3.2.9 Theorem: Let E be an extension of F if K is the subset of E consisting of all the elements that are algebraic over F.Then K is a subfield of E and an algebraic extension of F.

Proof: Let E be an extension of F and $K = \{u \in \mathrm{E} / u$ is algebraic over $F\}$

First we show that K is a subfield of E and then K is an algebraic extension of F.

Let $a, b \in$ K. Then a, b are algebraic over F.

Since a is algebraic over F, we have $F(a)$ is a finite extension of F. So $[F(a) : F]$ is finite.

Since b is algebraic over F, we have b is algebraic over $F(a)$.

So, $F(a)(b)$ is a finite extension of $F(a)$.

Therefore $[F(a, b) : F(a)]$ is finite.

and hence $[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] < \infty$

$i. e, F(a, b)$is a finite extension of F.

Clearly, $a, b \in F(a, b) \& F(a, b)$ is a field

Then $a \pm b,\ ab,\ \frac{a}{b}$ (if $b \neq 0) \in F(a, b)$. So all the elements $a \pm b,\ ab,\ \frac{a}{b}$ are algebraic over F and that $a \pm b, ab, \frac{a}{b}$ (if $b \neq 0) \in K$

So ' K ' is a subfield of E & every element of K is algebraic over F.

Therefore K is an algebraic extension of F.

Note: Let E be an extension of F. An element $a \in E$ is algebraic over $F \Leftrightarrow F(a)$ is a finite extension of F.

3.2.10 Definition: let E be an extension of F. If K is the subset of E consisting of all the elements that are algebraic over$F$, then K is a subfield of E & K is an algebraic extension of F. This K is called an algebraic closure of F in E.

3.2.11 Definition: Let K & L be the extension fields of a field F. Then a non-zero homomorphism $\sigma: K \to L \ni \sigma(a) = a, \ \forall a \in F$, is called F-homomorphism of K into L (or) an embedding of K into L over F.

3.2.12 Theorem: Let E be an algebraic extension of F and let $\sigma: E \to E$ be an embedding of E into itself over F. Then σ is onto and hence an automorphism of E.

Proof: Let E be an algebraic extension of F and let $\sigma: E \to E$ be an embedding.

Then $\sigma: E \to E$ is a monomorphism.

First we show that $\sigma: E \to E$ is onto.

Let $a \in E$.

Then a is an algebraic element over F. So, there is a polynomial $f(x) \in F[x]$ for which a is a root.

Suppose $p(x)$is the minimal polynomial of a over F.

Let E' be the smallest subfield of E containing F and all the roots of $p(x)$ in E i.e .E' is a subfield of E generated over F with finite no of elements in E which are roots of $p(x)$.

Then E' is a finite algebraic extension of F. So, $[E': F] < \infty$.

Further σ maps every root of $p(x)$ onto the roots of $p(x)$.
So, $\sigma: E' \to E'$is one -one.

Since $\sigma: E' \to E'$is an isomorphism, we have $\sigma(E') \cong E'$.

$\sigma(E') \subseteq E'$ and $[\sigma(E'): F] = [E': F] < \infty$.

Since $F \subseteq \sigma(E') \subseteq E', [E': F] = [E': \sigma(E')][\sigma(E'): F]$.

Therefore $[E': \sigma(E')] = 1$ and that $E' = \sigma(E')$.

So there exists an element b in E' such that $\sigma(b) = a$.

Therefore σ is onto E.

Hence σ an automorphism of E.

3.3 SUMMARY:

Every algebraic element α over F has a unique minimal polynomial $\boldsymbol{p(x) \in F[x]}$ which divides any other polynomial in $\boldsymbol{F[x]}$ which is satisfied by α. Also F(α) is isomorphic to the quotient ring $\boldsymbol{F[x]/(p(x))}$. Finite extensions are algebraic, but an algebraic extension need not be finite. The Tower Law is a crucial tool for computing degrees of extensions in stages.

3.4 TECHNICAL TERMS:

- Field extension: A field E is called an extension field of F if F is a subfield of E.
- Degree of extension: [E:F] the dimension of E as a vector space over F if E is an extension field of F.
- Simple extension: An extension E generated by a single element α, written F(α) is a simple extension of F.
- Algebraic element: An element α ∈ E is algebraic over F if it is a root of a non-constant polynomial with coefficients in F.
- Minimal polynomial: The monic irreducible polynomial $p(x) \in F[x]$ such that p(α) = 0 is the minimal polynomial of α over F.
- Algebraic extension: A field extension E of F where every element of E is algebraic over F.

3.5 SELF-ASSESSMENT QUESTIONS:

Q1. What is an algebraic element? How is it different from a transcendental element?

Answer: An element α ∈ K is algebraic over F if it is a root of a non-constant polynomial with coefficients in F. If no such polynomial exists, α is transcendental over F.

Q2. What is the minimal polynomial of an algebraic element?

Answer: The minimal polynomial of an algebraic element α over a field F is the monic irreducible polynomial f(x) ∈ F[x] of least degree such that f(α) = 0. It is unique and divides every other polynomial in F[x] that has α as a root.

Q3. Is every finite extension algebraic? Justify.

Answer: Yes. Every finite extension K over F is algebraic.

Let $[K:F] = n$ and $u \in K$. $1, u, u^2, \ldots, u^n$ are linearly dependent over F and that $a_0 + a_1 u + \cdots + a_n u^n = 0$ for some $a_0, a_1, \ldots, a_n \in F$ *which are not all zero.*

So u is algebraic over F and that K is algebraic over F.

Q4. Can an algebraic extension be infinite?

Answer: Yes. An algebraic extension can have infinite degree.

3.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul, 1997, Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York.
3. Khanna, V. K. and S. K. Bhambari, A Course in Abstract Algebra, 3rd edition, New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993, Algebra, 3rd edition, Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House, 2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Prof. R. Srinivasa Rao**

LESSON- 4

ALGEBRAICALLY CLOSED FIELDS

OBJECTIVES:

- To understand the concept of algebraically closed field and related results.
- To understand the relationship between algebraically closed fields and field extensions**,** including how algebraic closures are minimal algebraic extensions.
- To understand the concept of the algebraic closure as the largest possible algebraic extension of a field that also contains all roots of all polynomials from that field.
- To understand the uniqueness of algebraic closures up to isomorphism.

STRUCTURE:

4.1 INTRODUCTION:

In the study of fields and polynomial equations, an essential question is whether a given field contains all roots of its polynomials**.** A field F is called algebraically closed if every non-constant polynomial with coefficients in F has a root in F. This means that every polynomial can be completely factored into linear factors over F. This concept generalizes the familiar property of the field of complex numbers **C**, where every polynomial over **C** has a complex root. However, many fields like R, or Q are not algebraically closed**.** The general problem is to determine whether an algebraically closed field containing a given field K exists. This leads to the notion of the algebraic closure of K, which is a minimal algebraically closed extension of K. In this lesson, we study the basic properties of algebraically closed fields, their existence and uniqueness (up to isomorphism), and their fundamental role in understanding field extensions.

4.2 ALGEBRAICALLY CLOSED FIELDS:

4.2.1 Definition: A field K is called an algebraically closed field if it possesses no proper algebraic extensions i.e. if every algebraic extension of K coincides with K.
Example: The field of complex numbers is an algebraically closed field.

4.2.2 Theorem: For any field K, the following are equivalent.

(i) K is algebraically closed.

(ii) Every irreducible polynomial in $K\ [x]$ is of degree 1.

(iii) Every polynomial in K$[x]$ of positive degree factors completely in K$[x]$ into linear factors. (iv) Every polynomial in K$[x]$ of positive degree has at least one root in K.

Proof: Let K be a field.

(i) ⇒(ii):-

Assume (i) i.e. K is algebraically closed.

Then by definition K has no proper algebraic extension.

Let p(x) be an irreducible polynomial in K$[x]$ of degree n.

Then by known theorem, there exists an extension E of K such that $[E: K\ ]$ =degree of p$(x) = n$. So E is a finite extension of K.

Therefore E is an algebraic extension of K.

By our assumption (i), we have$E =$ K.

$\Rightarrow\ [E:\mathrm{K}] = 1$

$\Rightarrow \deg\ p(x) = 1$

Therefore every irreducible polynomial in K$[x]$ is of degree 1.

(ii)⇒ (iii):-

Assume (ii) i.e.Every irreducible polynomial in K$[x]$ is of degree 1.

Let $f(x)$ be a polynomial in K$[x]$ of positive degree. Since K$[x]$ is a unique factorization, domain $f(x)$ can be uniquely written as the product of finite number of irreducible elements. i.e.,$f(x) = u_0\ p_1(x) \cdot \mathrm{p}_2(x) \cdot \ldots \mathrm{p}_n(x)$ where $u_0 \in K$ and each $p_i(x)$ is an irreducible polynomial in $K\ [x]$. By assumption, we have $p_i(x)$ is of degree 1.

So,$p_i(x) = x - u_i$, where $u_i \in k; 1 \leq i \leq n$

Therefore $f(x) = u_0(x - u_1)(x - u_2) \cdots (x - u_n)$

So, every polynomial of positive degree in $K\ [x]$ can be factored completely in $K\ [x]$ into linear factors.

(iii)⇒ (iv):-

Assume (iii) i.e.Every polynomial in K$[x]$ of positive degree can be factored completely in K$[x]$ into linear factors.

Let $f(x)$ be a polynomial of positive degree in K$[x]$. By assumption, $f(x)$ can be written as $f(x) = u_0(x-u_1)(x-u_2)-(x-u_n)$ where $u_i \in K$; $1 \leq i \leq n$. So each $u_i \in$ K is a root of $f(x)$. Hence$f(x)$ has atleast one root in K.

Therefore every polynomial of positive degree in K$[x]$ has atleast one root in K.

(iv) ⇒ (i):-

Assume (iv) i.e. Every polynomial in K$[x]$ of positive degree has atleast one root in K.

Let E be an algebraic extension of K. let $a \in E$. Then a is an algebraic element over K.

There exists a minimal polynomial f(x) of a in K[x]. By our assumption, this minimal polynomial has atleast one root in K, say b.

Then$f(x) = (x-b)f_1(x)$, where deg $f_1(x) <$ deg $f(x)$, $f_1(x) \in$ K$[x]$.

If $a \neq b$, then $f_1(a) = 0$ we get a contradiction due to the minimality of $f(x)$. So a = b.

Hence E = K.

This mean K doesnot possess any proper algebraic extension.

Therefore K is algebraically closed.

4.3 ALGEBRAIC CLOSURES:

4.3.1: Definition: If F is a subfield of a field E, then E is called an algebraic closure of F if E is an algebraic extension of F and E is algebraically closed.

4.3.2 Lemma : Let F be a field and let $\sigma: F \to L$ be an embedding of F into an algebraically closed field L. Let $E = F(\alpha)$ be an algebraic extension of F. Then σ can be extended to an embedding $\eta: E \to L$ and the number of such extensions is equal to the number of distinct roots of the minimal polynomial of α.

Proof: Let F be a field and L be an algebraically closed field.

Suppose that $\sigma: F \to L$ be an embedding.

Then L is an extension of $\dot{F}$ such that $\sigma(a) = a, \forall a \in F$.

Let $E =$ F(α) be an algebraic extension of F. Then $\alpha \in E$ is an algebraic element of F.

So, let $p(x) = a_0 + a_1x + \cdots + x^n$ be the minimal polynomial of α over F.

Let $p^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + x^n \epsilon$ L[x]

Since L is algebraically closed, $p^\sigma(x)$ has a root, say β in L.

Let us recall, if α is algebraic over F then every element in $F(\alpha)$ can be uniquely written as $b_0 + b_1\alpha + \cdots + b_k\alpha^k$, where $k+1$ is the degree of the minimal polynomial $p(x)$ of α over F and $b_i \in F; 1 \leq i \leqslant k$.

Define a mapping $\eta: F(\alpha) \to L$ by

$\eta(b_0 + b_1\alpha + \cdots + b_k\alpha^k) = \sigma(b_0) + \sigma(b_1)\beta) + \cdots + \sigma(b_k)\beta^k$.

Since each element of $F(\alpha)$ has a unique representation as $b_0 + b_1\alpha + \cdots + b_k\alpha^k$,

$b_0, b_1, \ldots, b_k \in F$,

η is well-defined.

Let $a = b_0 + b_1\alpha + \cdots + b_k\alpha^k$, $b = b_0' + b_k'\alpha + \cdots + b_k'\alpha^k \in F(\alpha)$

$$\eta\left((b_0 + b_1\alpha + \cdots + b_k\alpha^k) + \left(b_0' + b_1'\alpha + \cdots + b_k'\alpha^k\right)\right)$$
$$= \eta\left(\left(b_0 + b_0'\right) + \left(b_1 + b_1'\right)\alpha + \cdots + \left(b_k + b_k'\right)\alpha^k\right)$$
$$= \sigma\left(b_0 + b_0'\right) + \sigma\left(b_1 + b_1'\right)\beta + \cdots + \sigma\left(b_k + b_k'\right)\beta^k$$
$$= \sigma(b_0) + \sigma\left(b_0'\right) + \sigma(b_1)\beta + \sigma\left(b_1'\right)\beta + \cdots + \sigma(b_k)\beta^k + \sigma\left(b_k'\right)\beta^k$$
$$= (\sigma(b_0) + \sigma(b_1)\beta + \sigma + \sigma(b_k)\beta^k) + \left(\sigma\left(b_0'\right) + \sigma\left(b_1'\right)\beta + \cdots + \sigma\left(b_k'\right)\beta^k\right)$$
$$= \eta(b_0 + b_1\alpha + \cdots + b_k\alpha^k) + \eta\left(b_0' + b_1'\alpha + \cdots + b_k'\alpha^k\right)$$

We prove that $\eta(ab) = \eta(a) \cdot \eta(b)$

Let $f(x) = b_0 + b_1x + \cdots + b_kx^k$,

$g(x) = b_0' + b_1'x + \cdots + b_k'x^k \in F[x]$.

Now $f(x)g(x) = p(x)s(x) + r(x)$ for some $s(x), r(x) \in F[x]$ and $r(x) = 0$ or

$\deg\ r(x) < \deg\ p(x)$.

Let $h(x) = f(x)g(x)$

$h^\sigma(x) = p^\sigma(x)\, \mathrm{s}^\sigma(x) + \mathrm{r}^\sigma(x)$

$\eta(ab) = \eta(f(\alpha)g(\alpha)) = \eta(h(\alpha)) =$

$\eta(r(\alpha)) = r^\sigma(\beta) = p^\sigma(\beta)\, s^\sigma(\beta) + r^\sigma(\beta) = h^\sigma(\beta) = f^\sigma(\beta)g^\sigma(\beta) = \eta(a)\eta(b)$

Therefore $\eta: F(\alpha) \to L$ is a ring homomorphism and hence an embedding as $\eta \neq 0$.

So, $\eta: F(\alpha) \to L$ is an embedding and also an extension of σ.

Thus, with each root α of $p(x)$, we have an embedding $\eta: E \to L$, which is an extension of σ.Also, there is a one-to-one correspondence between the set of distinct roots of $p^\sigma(x)$ in Land the set of embeddings η of $F(\alpha)$ into L, that extends σ. Hence the number of such extensions is equal to the number of distinct roots of the minimal polynomial of α as distinct roots give distinct embeddings into L.

4.3.3Theorem: Let E be an algebraic extension of a field F and let $\sigma: F \to L$ be an embedding of F into an algebraically closed field L. Then σ can be extended to an embedding $\eta: E \to L$

Proof: Let E be an algebraic extension of a field F and let $\sigma: F \to L$ be an embedding of F into an algebraically closed field L.

Define S $=\{(K, \theta)$ / K is a subfield of E containing F and θ is an extension of σ to an embedding of K into L.$\}$

Since F is the subfield of E containing F and $\sigma: F \to L$ is an extension of σ itself, we have $(F, \sigma) \in S$. Therefore S is non-empty.

Define a relation '$\leqslant$' on S by$(K, \theta) \leqslant (K', \theta')$ if and only if $K \subset K'$ and θ' is an extension of θ.

Now we show that'$\leqslant$'is partial ordering on S.

Reflexive: Let $(K, \theta) \in S$

Since$K \subseteq K$ and $\theta: K \to L$ is an extension of $\theta: K \to L$, we have $(K, \theta) \leqslant (K, \theta), \forall (K, \theta) \in S$.

Therefore $\leq$ is reflexive on S.

Anti- Symmetric: Let $(K_1, \theta_1), (K_2, \theta_2) \in S$.

Suppose, $(K_1, \theta_1) \leq (K_2, \theta_2)$ and $(K_2, \theta_2) \leq (K_1, \theta_1)$

So $K_1 \subseteq K_2; \theta_2$ is an extension of θ_1 and$K_2 \subseteq K_1; \theta_1$ is an extension of θ_2.

$\Rightarrow K_1 = K_2 \& \ \theta_1 = \theta_2$
$\Rightarrow (K_1, \theta_1) = (K_2, \theta_2)$

Therefore' $\leqslant$ ' is antisymmetric on S.

Transitive: Let $(K_1, \theta_1), (K_2, \theta_2), (K_3, \theta_3) \in S$.

Suppose $(K_1, \theta_1) \leqslant (K_2, \theta_2)$ and $(K_2, \theta_2) \leqslant (K_3, \theta_3)$

$So \ K_1 \subseteq K_2; \theta_2$ is an extension of $\theta_1$and $K_2 \subseteq K_3; \theta_3$ is an extension of θ_2

$Now \quad K_1 \subseteq K_2; \ \theta_1(a) = \theta_2(a)$; for all $a \in K_1 \& K_2 \subseteq K_3; \ \theta_2(a) = \theta_3(a)$; for all $a \in K_2$

$therefore \ K_1 \subseteq K_3; \ \theta_1(a) = \theta_3(a)$ for all $a \in K_1 \ and \ that$

$K_1 \subseteq K_3$ & θ_3 is an extension of θ_1. So $(K_1, \theta_1) \leqslant (K_3, \theta_3)$

Therefore $\leqslant$ is transitive and hence $(S, \leqslant)$ is a poset.

Let $\{(K_i, \theta_i)\}$ be a chain in S.

Write $K = UK_i$; then K is a subfield of E containing F.

Define $\theta: K \to L$ as follows:

Let $a \in K$, then $a \in K_i$ for some i.

We define $\theta(a) = \theta_i(a)$

Now we show that "θ" is well-defined.

Let $a \in K_i \& a \in K_j$

Then either $K_i \subset K_j$ & $K_j \subset K_i$[Since$\{(K_i, \theta_i)\}$ is a chain]

So, we get $\theta_i(a) = \theta_j(a)$

Hence θ is well-defined.

Clearly θ is an embedding of K into L, which is an extension of θ_i for all i. Therefore $(K, \theta) \in S$ and it is an upper bound of the chain $\{(K_i, \theta_i)\}$. So, by Zorn's lemma 'S' has maximal element, Say (K, η). Therefore, η is an embedding of K into L, which is an extension of σ.

Now we claim $K = E$.

If possible, suppose that K $\neq$ E . Then there exists $\alpha \in E$ such that $\alpha \notin$ K.

Now α is algebraic over F. (Since E is an algebraic extension of F). Then by Lemma 4.3.2, the embedding $\eta: K \to$ L has an extension $\eta^*: K(\alpha) \to L$. Hence $(K(\alpha), \eta^*) \in S$ and $(K, \eta) < (K(\alpha), \eta^*)$, which is a contradiction(Since(K, η) is maximalelement in S.)

Therefore K = E. So, $\eta: E \to L$ is an embedding of E into L, which is an extension of σ.

4.3.4 Theorem: Let K and K′ be algebraic closures of a field F. Then K ≅ K′ under an isomorphism that is an identity on F.(Or) Any two algebraic closures of a field F are isomorphic.

Proof: Let F be a fieldand K, K′ be two algebraic closures of F.

Consider $\lambda: F \to$ K be an embedding, given by $\lambda(a) = a \; \forall \; a \in F$.

Since K' is an algebraic extension of F, and K is algebraically closed, by theorem 4.3.3 λ can be extended to an embedding $\lambda^*: K' \to K$. So $K' \cong \lambda^*(K')$

Since K' is algebraically closed, we have $\lambda^*(K')$ is also algebraically closed.Also K is an algebraic extension of F.

This implies K is an algebraic extension of $\lambda^*(K')$(Since $F \subset \lambda^*(K') \subset$ K)

So, $\lambda^*(K') = K$ i.e. $\lambda^*: K' \to$ K is onto.

Therefore $\lambda^*: K' \to$ K is an isomorphism.

Thus $K' \cong K$, under an isomorphism which acts as the identity on F.

Note: From the above Theorem 4.3.4, an algebraic closure of a field F is unique upto isomorphism and we denote the algebraic closure of F by $\bar{F}$.

4.3.5 Definition: let F be a field and let $S = (x_i)_{i \in \Delta}$ be an infinite set of commuting indeterminants (or) variables. Then the elements of the form $\sum_{\text{finite}} a_i x_{i_1} x_{i_2} \cdots x_{i_n}, a_i \in F, x_{ij} \in S$, with natural addition and multiplication form a ring $F[S]$, called the polynomial

ring over F in S. Note that for a polynomial $\sum_{\text{finite}} a_i x_{i_1} x_{i_2} \dots x_{i_n}$ to be zero, each coefficient a_i of each monomial $x_{i_1} x_{i_2} \dots x_{i_n}$must be zero.

4.3.6 Theorem: Let F be a field. Then there exists an algebraically closed field K containing F as a subfield.

Proof:

Part I: Let F be a field.

Let us first construct an extension K of F in which every polynomial $f(x) \in F[x]$ of degree $\geqslant 1$ has a root.

Let S be a set which is having one-to-one correspondence with the set of all polynomials in $F[x]$ of degree $\geqslant 1$.

We suppose that the element corresponding to a polynomial $f = f(x) \in F[x]$ of degree $\geqslant 1$ is $x_f \in S$.

Consider the polynomial ring $F[S]$.

Part II: Now we show that if A is an ideal in $F[S]$ generated by all polynomials $f(x_f)$ of degree $\geqslant 1$, then $A \neq F[S]$

Suppose if possible $A = F[S]$, where A is an ideal in $F[S]$ generated by all polynomials $f(x_f)$ in $F[S]$ are of degree $\geqslant 1$.

Since $A = F[S]$, we have $1 \in A$

$1 = g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots g_n f_n(x_{f_n}) - - -$ (1)where $g_i \in F[S], x_{f_1}, x_{f_2}, \dots x_{f_n} \in S$ and each $f_i(x_{f_i})$ is of degree $\geqslant 1$

Since each $g_i \in F[S]$ i.e., each g_i is a polynomial in a finite no. of variable in S.

Write $x_{f_i} = x_i$, for each $f_i \in F[x]$

After re-indexing we assume that $x_{f_1} = x_1, x_{f_2} = x_2, \dots \dots x_{f_n} = x_n$ and the variables occur in all $g_i; 1 \leq i \leq n$ are in the set$\{x_1, x_2, \dots, x_n, x_{n+1}, \dots, x_m\}$

Then we can write (1) as $\sum\ g_i(x_1, x_2, \dots, x_m) \cdot f_i(x_i)$---(2)

Now $f_1(x), f_2(x), \dots, f_n(x) \in F[x]$. Then there exists an extension E of F in which every polynomial has a root. So let α_i be the root of $f_i(x)$ in $E; i = 1, \dots n$.

Taking $x_i = \alpha_i; i = 1,2, \dots n$ and $x_i = 0, i = n+1, \dots m$,

we get $1 = \sum_{i=1}^{m} g_i(\alpha_1, \alpha_2, \dots, \alpha_n, 0, \dots, 0) f_i(\alpha_i)$

$\Rightarrow 1 = 0$, which is contradiction (Since α_i is a root of $f_i(x)\ and\ f_i(\alpha_i) = 0$)

Thus $A \neq F[S]$

So A is a proper ideal in $F[S]$.Then by Zorn's Lemma, A can be embedded in a maximal ideal say M of $F[S]$.

So, $\frac{F[S]}{M}$ is a field containing F.

Part III: let $f \in F[x]$ be a polynomial of degree $\geqslant 1$. Then clearly $f(x_f) \in A \subset M$

Let $f(x) = a_0 + a_1x + \cdots + a_mx^m, a_i \in F$. Let us denote the coset $g + M$ by $\bar{g}$ in $\frac{F[S]}{M}$.

Therefore $\bar{0} = \overline{f(x_f)}$

$$= \overline{a_0 + a_1x_f + \cdots + a_mx_f^m}$$
$$= \bar{a}_0 + \bar{a}_1\bar{x}_f + \cdots + \bar{a}_m\overline{x_f^m}$$
$$= a_0 + a_1\bar{x}_f + \cdots + a_m\bar{x}_f^m$$

Therefore $\bar{x}_f$ is a root of $f(x)$ in $\frac{F[S]}{M}$

Thus we have constructed a field K_1 named by $\frac{F[S]}{M}$ $i.e.$ an extension of F in which every polynomial $f(x) \in F[x]$ of degree $\geqslant 1$ has a root.

Inductively we can now form a chain of fields $K_1 \subset K_2 \subset K_3 \subset \cdots$ every polynomials in $K_n[x]$ of degree $\geqslant 1$ has a root in K_{n+1} . Let $K = \bigcup_{i=1}^{n} K_i$. Then clearly K is a field and every polynomial in $K[x]$ of positive degree has a root in K .

By known result, K is an algebraically closed field containing F as a subfield.

4.3.7 Theorem: Let F be a field. Then there exists an extension $\bar{F}$ that is algebraic over F and is algebraically closed, that is, each field has an algebraic closure.

Proof: By theorem 4.3.6, F has an extension K which is algebraically closed.

Let $\bar{F} = \{a \in K | a \text{ is algebraic over } F\}$.

Let $\bar{F}$ is a subfield of K and it is an algebraic extension of F ... ...(1)

Let $f(x) \in \bar{F}[x]$ be a polynomial of degree $\geqslant 1$.

Note that $f(x) \in \bar{F}[x] \subset K[x]$.

Since K is algebraically closed, we have $f(x)$ has a root say, $a \in K$.

Therefore $a \in K$ is algebraic over $\bar{F}$. So $a \in \bar{F}$.

Therefore every polynomial $f(x) \in \bar{F}[x]$ of positive degree has a root in $\bar{F}$.

Then by known result, $\bar{F}$ is algebraically closed---(2)

From (1) & (2), $\bar{F}$ is an algebraic closure of F.

Hence every field has an algebraic closure.

Note: Let $\sigma: F \to L$ be an embedding of F into L. Then the mapping from $F[x]$ to $L[x]$ given by $r_0 + r_1x + \cdots + r_mx^m = \sigma(r_0) + \sigma(r_1)x + \cdots + \sigma(r_n)x^n$ is a ring homomorphism.

Clearly this extends σ and we denote this extended mapping by σ^* so $\sigma^*: F[x] \to L[x]$ is a homomorphism and image of $f(x) \in F[x]$ under σ^* will be denoted by f^σ.

4.4 SUMMARY:

An algebraically closed field is defined as a field in which every non-constant polynomial has at least one root within the field itself. This implies that every polynomial over such a field can be factored completely into linear factors. For instance, the field of complex numbers $\mathbb{C}$ is algebraically closed because every polynomial with complex coefficients has all its roots in $\mathbb{C}$. This lesson emphasizes several equivalent characterizations of algebraically closed fields.

An algebraic closure of a field F is an algebraic extension of F that is also algebraically closed. This means it contains all roots of all polynomials with coefficients in F. Any two algebraic closures are unique up to isomorphism. The construction of an algebraic closure of F involves extending the field F by successively adjoining roots of polynomials over F, ensuring that the resulting field is both an algebraic extension and algebraically closed.

4.5 TECHNICAL TERMS:

- Algebraically Closed Field: A field K is called an algebraically closed field if it possesses no proper algebraic extensions i.e. if every algebraic extension of K coincides with K.
- Irreducible Polynomial over F: This is a polynomial $f(x) \in F[x]$ that cannot be broken down into simpler (non-trivial) polynomials in $F[x]$ using multiplication.
- Algebraic Element of F: This refers to an element u is an extension E of F that is a solution of some polynomial with coefficients F. In other words, it satisfies a polynomial with coefficients only numbers from the field F.
- Algebraic Extension E of F: This is a bigger field E built from a smaller one F, where every element of E is algebraic over the smaller field F. i.e, each element of E comes from solving a polynomial whose coefficients lie in the original field F.
- Algebraic Closure of F: This is the largest possible algebraic extension of a field F that also contains all roots of all polynomials from the field F.

4.6 SELF-ASSESSMENT QUESTIONS:

Q1. Is the field R of real numbers, algebraically closed? Justify.
Answer: No, R is **not** algebraically closed because polynomials like $x^2+1 \in R[x]$ do not have real roots. Hence, not every non-constant polynomial over R has a root in R.

Q2. Prove or disprove: "If a field is algebraically closed, then every irreducible polynomial over it is linear."

Answer: True**.** If a field F is algebraically closed, then every non-constant polynomial in F[x] splits completely into linear factors. Hence, irreducible polynomials must is of degree one.

Q3. Let $K \subseteq L$ and L be a field extension of K. If L is algebraically closed, what can be said about the algebraic closure of K?

Answer: The algebraic closure of K is contained in L. Since L is algebraically closed, it contains all roots of algebraic polynomials over K, so the algebraic closure of K lies inside L.

Q4. Is it true that every algebraic extension of an algebraically closed field is trivial? Explain.

Answer: Yes**.** If F is algebraically closed and K is an algebraic extension of F, then K=F. Since all algebraic elements over F already lie in F, there are no proper algebraic extensions of an algebraically closed field.

Q5. Can a finite field be algebraically closed? Explain.
Answer: No. A finite field cannot be algebraically closed because not all polynomials over it can have all their roots within the field.

Q6: If F is a subfield of an algebraically closed field K , then is it true that the algebraic closure $\bar{F}$ of F in K is also algebraically closed.

Answer: Let F be a subfield of an algebraically closed field K and let $\bar{F}$ be an algebraic closure of F in K . So $F \subseteq \bar{F} \subseteq K$

Let $f(x) \in \bar{F}[x]$ be any polynomial of positive degree.

Let us recall, $\bar{F} = \{u \in \mathrm{K} / \ u$ is algebraic over $F\}$. Then $\bar{F}$ is subfield of K and is an algebraic extension of F.

For $f(x) \in \bar{F}[x]$, we have $f(x) \in K\ [x]$. Let $deg\ f(x) \geq 1$

Therefore $f(x) \in K\ [x]$ is a polynomial of positive degree. Since K is algebraically closed, by theorem 4.2.2, we have $f(x)$ has a root, say u in K .

So $u \in K$ is algebraic over F [Since $F \subset \bar{F} \subset K$ such that $\bar{F}$ is an algebraic extension of F.] $and\ that\ u \in \bar{F}$

Therefore by theorem 4.2.2, $\bar{F}$ is algebraically closed.

4.7 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House ,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

-

- **Prof. R. Srinvasa Rao**

LESSON- 5

SPLITTING FIELDS

OBJECTIVE:

- To determine the extension K of F for a polynomial over a given field F: splitting field.
- To investigate the existence and uniqueness of a splitting field of a polynomial over a given field.
- To learn and study the construction of a splitting field for the polynomial over a given field.

STRUCTURE:

5.1 INTRODUCTION:

The idea of splitting fields arose from the necessity to find roots of polynomials, especially those that do not have roots in the base field, and the first usage can be traced to Galois work in 1830's specially in the context of solving congruences modulo a prime. For example, some polynomials, like x^2+1 over the real numbers R, have no roots with the base field R. However, it splits in the field of complex numbers C where $x^2+1=(x+i)(x-i)$. Therefore, C is the splitting field of x^2+1 over R. Splitting fields provide a way to extend the field to include these roots.

5.2 SPLITTING FIELDS:

We now give the definition of a splitting field and some examples on it.

5.2.1: Definition: Let F be any field and $f(x) \in F[x]$ be a polynomial of degree ≥ 1. Then an extension K of F is called a splitting field of $f(x)$ over F, if
$i) f(x)$ can be factorized into linear factors in $K[x]$ that is,

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n),\ \alpha_1,\alpha_2,\alpha_3,\dots,\alpha_n \in K \text{ and } a \in F.$$

$ii)\ K = F(\alpha_1,\alpha_2,\alpha_3,\ \dots,\alpha_n)$, that is K is generated by F and the roots $\alpha_1,\alpha_2,\alpha_3,\dots,\alpha_n$ of $f(x)$ in K.

5.2.2: Examples:

i) Consider $f(x) = x^2 - 2 \in Q[x]$. Then the field $Q(\sqrt{2}) = \{a + b\sqrt{2} \,|a, b \in 2|\}$ is a splitting field of $x^2 - 2 \in Q[x]$ over Q.

ii)Consider $g(x) = x^2 + 1 \in \mathrm{R}[x]$ Then $C = \mathrm{R}[i]$ is a splitting field of $g(x)$ over R.

5.2.3: Note: For a polynomial $f(x)$ in $F[x]$ of degree ≥ 1, a splitting field of $f(x)$ over F always exists. This is because, for a field F, since $f(x) \in F[x] \subseteq \bar{F}\,[x]$, $f(x)$ has all its roots say $\beta_1, \beta_2, \beta_3 \ldots . \beta_k$ in $\bar{F}$ and that $F(\beta_1, \beta_2, \beta_3 \ldots . \beta_k)$ is a splitting field of $f(x)$ over F.

5.2.4: Theorem: Let F be a field and $f(x)$ be a polynomial in $F[x]$ of degree ≥ 1. Then the degree of the splitting field K of $f(x)$ over F is finite and hence K is an algebraic extension of F.

Proof: Let F be a field and $f(x) \in F[x]$ be a polynomial of degree ≥ 1.

Let $\bar{F}$ be the algebraic closure of F.

Now $f(x) \in F[x]$ has all its roots say $\alpha_1, \alpha_2, \alpha_3 \ldots . \alpha_n \in \bar{F}$

Then $K = F(\alpha_1, \alpha_2, \alpha_3 \ldots . \alpha_n)$ is a splitting field of $f(x)$ over F.

Since, each of $\alpha_1, \alpha_2, \alpha_3 \ldots . \alpha_n$ are algebraic over F, the degree of K over F is finite and hence K is an algebraic extension of F.

5.2.5: Theorem (Uniqueness of the splitting field): Let K be a splitting field of a polynomial $f(x)$ over a field F. If E is another splitting field of $f(x)$ over F then $\exists$ an isomorphism $\sigma: E \to K$ which is an identity on F.

Proof: Let $f(x) \in F[x]$ be a polynomial over F.

Also, let K be a splitting field of $f(x)$ over F and E be another splitting field $f(x)$ over F.

Obviously, F is a subfield of E and K.

Let $\bar{K}$ be the algebraic closure of K.

Let $\sigma: F \to F$ be an identity mapping.

Now $\sigma: F \to \bar{K}$ defined by $\sigma(\alpha) = \alpha$ for all $\alpha \in F$ is an embedding of F into $\bar{K}$.

Since E is an algebraic extension of F, by known theorem, σ can be extended to an embedding $\lambda: E \to \overline{K}$ of E into $\overline{K}$.

Now $f(x)$ can be factorized into linear factors in $E[x]$ as

$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n), a_n \in F$ and $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n \in E$

So, $E = F(\alpha_1, \alpha_2, \alpha_3 \ldots . \alpha_n)$

Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + a_nx^n$ where $a_0, a_1, a_2, \ldots, a_n \neq 0 \in F$.

Let us set $f(x) = f^{\lambda}(x) = f^{\sigma}(x) = a_n\big(x-\lambda(\alpha_1)\big)\big(x-\lambda(\alpha_2)\big)\ldots\big(x-\lambda(\alpha_n)\big)$

$= f^{\lambda}(x)\ \overline{K}[x]$

So, $\lambda(\alpha_1), \lambda(\alpha_2) \ldots . \lambda(\alpha_n)$ are the roots of $f(x)$ in $\overline{K}$.

Then $F\big(\lambda(\alpha_1), \lambda(\alpha_2) \ldots . \lambda(\alpha_n)\big) = K$ as K is a splitting field of $f(x)$ over F.

We have $K = F\big(\lambda(\alpha_1), \lambda(\alpha_2), \ldots . , \lambda(\alpha_n)\big)$

$= \lambda\big(F(\alpha_1, \alpha_2, \alpha_3, \ldots . , \alpha_n)\big)$

$= \lambda(E)$.

Hence E is isomorphic to K by λ which is an identity on F.

5.2.6: Examples:

i) The degree of extension of the splitting field of $x^3 - 2 \in Q[x]$ is 6

Solution: Let $f(x) = x^3 - 2 \in Q[x]$.

Then $f(x)$ is irreducible over Q by Einstein's criterion.

Also $x^3 - 2$ is the minimal polynomial of $2^{1/3}$.

Therefore, $\frac{Q[x]}{x^3-2} \cong Q\left(2^{1/3}\right)$ with $\left[Q\left(2^{1/3}\right) : Q\right] = \deg f(x) = 3$.

But $Q\left(2^{1/3}\right)$ is not the splitting field of $x^3 - 2 \in Q[x]$.

Now, $f(x) = x^3 - 2$

$$= \left(x - 2^{1/3}\right)\left(x^2 + 2^{1/3}x + 2^{2/3}\right)$$

So, $f(x) = x^3 - 2$ has two complex roots say α and $\bar{\alpha}$.

The roots are $\alpha = \frac{-2^{1/3} + i\sqrt{3 \times 2^{2/3}}}{2}$, $\bar{\alpha} = \frac{-2^{1/3} - i\sqrt{3 \times 2^{2/3}}}{2}$

Thus, $p(x) = x^2 + 2^{1/3}x + 2^{2/3} \in Q\left(2^{1/3}\right)[x]$ is irreducible over $Q\left(2^{1/3}\right)$

and is of degree 2.

Hence $\frac{Q\left(2^{1/3}\right)[x]}{(p(x))} \cong Q\left(2^{1/3}\right)(\alpha) = Q\left(2^{1/3}, \alpha\right)$.

Since $p(x) \in Q\left(2^{1/3}\right)(x)$ has degree 2 and its roots α and $\bar{\alpha}$ are not in

$Q\left(2^{1/3}\right)$, $\left[Q\left(2^{1/3}, \alpha\right) : Q\left(2^{1/3}\right)\right] = deg(p(x)) = 2$

Now all the roots of $f(x)$, viz., $2^{1/3}, \alpha, \bar{\alpha} \in Q\left(2^{1/3}, \alpha\right)$.

Hence, $Q\left(2^{1/3}, \alpha\right)$ is a splitting field of $f(x) = x^3 - 2 \in 2[x]$ over Q.

Also, $\left[Q\left(2^{1/3}, \alpha\right) : Q\right] = \left[Q\left(2^{1/3}, \alpha\right) : Q\left(2^{1/3}\right)\right]\left[Q\left(2^{1/3}\right) : Q\right]$ = (2)(3) =6.

Thus, the solution is completed.

ii) Let p be a prime. Then $f(x) = x^p - 1 \in Q[x]$ has a splitting field $Q(\alpha)$ where $\alpha \neq 1$ and $\alpha^p = 1$. Also $[Q(\alpha): Q] = p - 1$.

Solution: we have $f(x) = x^p - 1 \in Q[x]$ where p is prime.

Now $f(x) = x^p - 1$

$= (x - 1)(1 + x + x^2 + \ldots + x^{p-1}) \in Q[x]$ is an irreducible polynomial over Q.

We get an extension field E of Q such that E contains a root α of

$g(x) = 1 + x + x^2 + \ldots + x^{p-1} \in Q[x]$ and $g(x)$ is irreducible over Q.

Now $[Q(\alpha): Q] = deg\ g(x) = p - 1$.

So $\alpha \neq 1$ and $\alpha^p = 1$ as α is a root of $f(x)$.

Now we assert that $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$ are the p distinct roots of $f(x)$.

Clearly $\alpha^p = 1 \Rightarrow (\alpha^i)^p = 1 \; \forall$ the integer i.

Thus, we need to show that all these roots are distinct.

Suppose that $\alpha^i = \alpha^j, 0 \leq i < j \leq p-1$.

Then $\alpha^{i-j} = 1$.

Since p is prime and $0 < j - i < p$, we have $(p,\ j-i) = 1$.

$\Rightarrow 1 = px_0 + (j-i)y_0$ for some integers x_0 and y_0.

Now $\alpha = \alpha^1 = \alpha^{px_0+(j-i)y_0}$

$= \alpha^{px_0} . \alpha^{(j-i)y_0}$

$= (\alpha^p)^{x_0} . (\alpha^{j-i})^{y_0}$

$= (1)^{x_0} . (1)^{y_0} = 1$

$\therefore \alpha = 1$, which is a contradiction.

So, $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$ are the p distinct roots of $f(x) = x^p - 1$.

Hence, the splitting field of $f(x) = x^{p-1} \in Q[x]$ is $Q(\alpha)$.

Since, the minimal polynomial of α is $g(x)$ and $deg(g(x)) = p-1$,

We have $[Q(\alpha): Q] = deg\ g(x) = p-1$.

This completes the solution.

iii) Let $F = {}^{Z}/_{(2)}$. The splitting field of $x^3 + x^2 + 1 \in F[x]$ is a finite field with 8 elements.

Solution: Let $f(x) = x^3 + x^2 + 1 \in F[x]$ where $F = {}^{Z}/_{(2)}$ (or) Z_2.

Clearly $degf(x) = 3$.

Also $0,1 \in Z_2$ are not the roots of $f(x)$.

Thus, $f(x) = x^3 + x^2 + 1$ is irreducible over F.

So, we get an extension $E\ of\ F = Z_2$ that contains a root α of $f(x)$.

$Z_2(\alpha)$ is a subfield of E.

We now prove that $Z_2(\alpha)$ or $F(\alpha)$ is a splitting field of $f(x)$ over $F = Z_2$.

Since α is a root of $f(x)$, we have $f(\alpha) = 0$.

$\Rightarrow \alpha^3 + \alpha^2 + 1 = 0$.

Now $f(x) = (x - \alpha)(x^2 + (\alpha + 1)x + \alpha(\alpha + 1))$

$= (x - \alpha)(x - \alpha^2)(x + \alpha^2 + \alpha + 1)$

So, all the roots of $f(x)$ are in $Z_2(\alpha)$ and hence $Z_2(\alpha)$ is a splitting field of $f(x)$ over Z_2.

Now $Z_2(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 / a_0, a_1, a_2 \in Z_2\}$

$\Rightarrow Z_2(\alpha) = \{0,1, \alpha, \alpha^2, 1 + \alpha, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}$ Where $\alpha^3 + \alpha^2 + 1 = 0$

So, $Z_2(\alpha)$ is a splitting field of $x^3 + x^2 + 1 \in F[x]$ which contains 8 elements.

iv) The splitting field of $f(x) = x^4 - 2 \in Q[x]$ over Q is $Q\left(2^{1/4}, i\right)$ and its degree of extension is 8.

Solution: we have $f(x) = x^4 - 2 \in Q[x]$

Clearly $f(x)$ is irreducible over Q by Einstein's Criterion and $degf(x) = 4$.

Thus $f(x)$ is the minimal polynomial of $2^{1/4}$ over Q.

So $\left[Q\left(2^{1/4}\right) : Q\right] = degf(x) = 4$

Now $f(x) = x^4 - 2 = x^4 - \left(2^{1/4}\right)^4 = \left(x^2 - 2^{1/2}\right)\left(x^2 + 2^{1/2}\right)$

$= \left(x - 2^{1/4}\right)\left(x + 2^{1/4}\right)\left(x^2 + \left(2^{1/4}\right)^2\right)$

$= \left(x - 2^{1/4}\right)\left(x + 2^{1/4}\right)\left(x - i2^{1/4}\right)\left(x + i2^{1/4}\right)$.

Clearly $g(x) = x^2 + 2^{1/2}$ is irreducible over $Q\left(2^{1/4}\right)$.

Thus, the root $2^{1/4}i$ has $x^2 + 2^{1/2}$ as its minimal polynomial over $Q\left(2^{1/4}\right)$.

So $\left[Q\left(2^{1/4}\right)\left(2^{1/4}i\right) : Q\left(2^{1/4}\right)\right] = deg\ g(x) = 2$.

Now clearly $Q\left(2^{1/4}\right)\left(2^{1/4}i\right) = Q\left(2^{1/4}, i\right)$ is the splitting field of $f(x) = x^4 - 2 \in Q[x]$

and $\left[Q\left(2^{1/4}, i\right) : Q\right] = \left[Q\left(2^{1/4}, i\right) : Q\left(2^{1/4}\right)\right]\left[Q\left(2^{1/4}\right) : Q\right]$

$= 2 \times 4 = 8.$

This completes the solution.

5.3 SUMMARY:

This lesson presented the fundamental concept of constructing the splitting field of a given polynomial $f(x) \in F[x]$ over a field F. In summary, a splitting field of a polynomial $f(x)$ over a field F is the smallest extension $E\ of\ F$ where $f(x)$ splits into linear factors. From uniqueness theorem, the reader can easily understand that, the splitting field of a polynomial is unique (up to isomorphism). Few examples of constructing a splitting field for a given polynomial and their corresponding degrees were also included for better understanding of the reader. While the concept of splitting fields might seem abstract, its underlying principles, particularly in Galois theory have real-world applications in areas like coding theory and cryptography, where they are applied to construct error-correcting codes and secure communication protocols.

5.4 TECHNICAL TERMS:

Splitting Field: Let F be any field and $f(x) \in F[x]$ be a polynomial of degree ≥ 1. Then an extension K of F is called a splitting field of $f(x)$ over F, if

i) $f(x)$ can be factorized into linear factors in $K[x]$. That is,

$f(x) = a(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)\ \alpha_1, \alpha_2, \alpha_3 \ldots . \alpha_n\ and\ a \in F$.

ii) $K = F(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$, that is K is generated by F and the roots $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ of $f(x)$ in K.

Irreducible polynomial: A polynomial $f(x) \in F[x]$ is called irreducible if the degree of $f(x) \geq 1$ and whenever $f(x) = g(x)h(x)$, where $g(x),\ h(x) \in F[x]$ then $g(x) \in F$ (or) $h(x) \in F$. If a polynomial is not irreducible, it is called reducible.

Einstein criterion: Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + a_nx^n \in Z[x]$, $n \geq 1$.

If there is a prime p such that $p^2 \nmid a_0$, $p|a_0$, $p|a_1, p|a_2, \ldots, p|a_{n-1}$ and $p \nmid a_n$ then $f(x)$ is irreducible over Q.

Algebraic element: Let E be an extension of a field F. An element $\alpha \in E$ is said to be algebraic over F if there exists a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Minimal polynomial: The monic irreducible polynomial in $F[x]$ for which u is a root will be called the minimal polynomial of u over F.

Algebraic extension: An extension field E of F is called algebraic if each element of E is algebraic over F.

Algebraically Closed Field: A field K is algebraically closed if it possesses no proper algebraic extensions, that is, if every algebraic extension of K coincides with K.

Algebraic closure: If F is a subfield of E, then E is called an algebraic closure of F if

$i)$ E is an algebraic extension of F.

$ii)$ E is algebraically closed.

5.5 SELF- ASSESSMENT QUESTIONS:

1. Find the splitting field of $x^4 + 4$ over Q.

Ans: $x^4 + 4 = (x^2 + 2)^2 - 4x^2$

$= (x^2 - 2x + 2)(x^2 + 2x + 2)$ in $Q[x]$

By Eisenstein's criterion, $(x^2 - 2x + 2)$ and $(x^2 + 2x + 2)$ are irreducible over Q. Their roots in C are $1 \pm i$ and $-1 \pm i$.

Thus, the splitting field of $x^4 + 4$ over Q is $Q(1 + i, 1 - i, -1 + i, -1 - i) = Q(i)$.

Here, clearly $[Q(i):Q] = 2$.

2. Find the splitting field of $x^6 + 1$ over Z_2.

Ans: Over Z_2, $x^6 + 1 = x^6 - 1 = (x^3 - 1)^2 = (x + 1)^2(x^2 + x + 1)^2$

The roots are $1, 1, \alpha, \alpha, 1 + \alpha, 1 + \alpha$, where α is the root of the irreducible polynomial $x^2 + x + 1$ over Z_2.

Hence, the splitting field of $f(x)$ over Z_2 is $Z_2(\alpha)$.

Also, $[Z_2(\alpha) : Z_2] = 2$.

3. Find the splitting field of $f(x) = x^4 + x^2 + 1$ over Q.

Ans: Given $f(x) = x^4 + x^2 + 1$

Then, $f(x) = (x^2+1)^2 - x^2$

$= (x^2 - x + 1)(x^2 + x + 1)$ in $Q[x]$.

So, the roots of $f(x)$ are $\pm\omega, \pm\omega^2$ where $\omega = \frac{-1+\sqrt{3}i}{2}$.

Hence, the splitting field of $x^4 + x^2 + 1$ over Q is $Q(\omega, \omega^2) = Q(\omega)$ and

$[Q(\omega):Q] = 2$ ($\because \omega$ satisfies the irreducible polynomial $x^2 + x + 1$ over Q).

4. Construct the splitting field of $x^3 - 1$ over Q.

Ans: Let $f(x) = x^3 - 1 \in Q[x]$

$f(x) = x^3 - 1 = (x-1)(x^2 + x + 1)$

Let $\omega \neq 1$ be a cube root of 1.

So, the roots of $f(x)$ are $1, \omega, \omega^2$ where $\omega = \frac{-1}{2} + \frac{\sqrt{3}i}{2}$

Hence, splitting field of $x^3 - 1$ over Q is

$Q(1, \omega, \omega^2) = Q(\omega) = Q\left(\frac{-1}{2} \pm \frac{\sqrt{3}i}{2}\right) = Q(\sqrt{3}i)$.

Thus, splitting field $x^3 - 1$ over Q is $Q(\omega)(or)Q(\sqrt{3}i)$

Also, the degree $Q(\omega)$ over Q is

$[Q(\omega):Q] = 2$ ($\because x^2 + x + 1$ is irreducible over Q which satisfies ω)

5. Find a splitting field of $x^3 - 2 \in Z_3[x]$

Ans: Let $f(x) = x^3 - 2 \in Z_3[x]$

Now $f(x) = x^3 - \bar{2} = x^3 + \bar{1} = (x + \bar{1})^3$ in $Z_3[x]$

Thus, a splitting field of $x^3 - 2 \in Z_3[x]$ is

$Z_3(-\bar{1}, -\bar{1}, -\bar{1}) = Z_3$.

6. Identify the splitting field of $f(x) = x^2 - x + 1$ over $Q(\omega)$.

Ans: Let $f(x) = x^2 - x + 1 \in Q(\omega)[x]$.

The roots of $f(x)$ are $1 + \omega, 1 + \omega^2 \in Q(\omega)$.

Hence $Q(\omega)$ is the splitting field over itself.

7. Define splitting field of a polynomial $f(x)$ over a field F with 2 examples.

Ans: (Refer: Definition 5.2.1 and Examples 5.2.2).

8. State and prove uniqueness theorem on splitting fields of a polynomial $f(x)$ over a field F.

Ans: (Refer: Theorem 5.2.5).

5.6 SUGGESTED READINGS:

1. P. B. Bhattacharya, S. K. Jain and S. R. Nag Paul, Basic Abstract Algebra, Second Edition, Cambridge University Press,1995.
2. I. N. Herstein, Topics in Algebra, Second Edition, John Wiley & sons, Inc,1975.
3. Thomas W. Hungerford, Algebra, Springer-Verlag, New York.

- Dr. P. Vijaya Saradhi

LESSON- 6

NORMAL EXTENSIONS

OBJECTIVE:

- To know the splitting field of a family of polynomials of over a given field
- To provide equivalent conditions for an extension E of F to be a splitting field of a family of polynomials over F: Normal extension of a field F.
- To give illustrative examples which help us to understand how to exhibit an extension of a given field is either normal or not.

STRUCTURE:

6.1 INTRODUCTION:

The concept of normal extension of a field was developed by Evariste Galois in the 1830's as a part of his work on Galois theory, which he introduced to solve the problem of finding general solutions to polynomial equations. In field theory, a normal extension is an algebraic field extension where every irreducible polynomial over the base field that has a root in the extension splits completely into linear factors within the extension. For example, the extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is normal because the minimal polynomial $x^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$. A normal extension is also charecterised as the splitting field of a family of polynomials over the base field. This means that the extension contains all the roots of polynomials in that family.

6.2 NORMAL EXTENSIONS:

In lesson 5, we have defined the splitting field of a polynomial over a given field. Now we define the splitting field of a family of polynomials over a field F. Also, the proof of uniqueness (up to isomorphism) can be extended to prove the uniqueness of a splitting field of a family of polynomials over a given field.

6.2.1 Definition:

Let F be any field and $\{f_i(x)/i \in I\}$ be a family of polynomials of degree ≥ 1 over F. An extension E or F is said to be the splitting field of the family of polynomials $\{f_i(x)|i \in I\}$, if

i) Each $f_i(x)$ splits into linear factors in $E[x]$.

ii) E is generated over F by all the roots of the polynomials $f_i(x), i \in I$.

6.2.2 Theorem: Let E be an algebraic extension of a field F contained in algebraic closure $\bar{F}$ of F. Then the following conditions are equivalent.

i) Every irreducible polynomial in $F[x]$ that has a root in E splits into linear factors in E.

ii) E is the splitting field of a family of polynomial in $F[x]$.

iii) Every embedding σ of E into $\bar{F}$ that keeps each element of F fixed maps E onto E (or, σ may be regarded as an automorphism of E).

Proof: Let E be an algebraic extension of a field F contained in an algebraic closure $\bar{F}$ of F.

(i) $\Rightarrow$ (ii): Assume that every irreducible polynomial in $F[x]$ that has a root in E splits into linear facors in E.

Let $\alpha \in E$. Since E is an algebraic extension of F, α has a minimal polynomial $P_\alpha(x) \in F[x]$ such that $P_\alpha(\alpha) = 0$, where $P_\alpha(x)$ is an irreducible polynomial over a field F.

By hypothesis, $P_\alpha(x)$ splits into linear factors in $E[x]$. Thus E is an algebraic extension of F such that the family of polynomials $\{P_\alpha(x) \mid \alpha \in E\}$ splits into linear factors in E.

Moreover, E is generated over F by all roots of the family of polynomials $\{P_\alpha(x) \mid \alpha \in E\}$.

Hence E is the splitting field of the family of polynomials $\{P_\alpha(x) \mid \alpha \in E\}$, $P_\alpha(x) \in F[x]$.

This proves condition (ii).

Thus, (i) $\Rightarrow$ (ii). ------ (1).

(ii) $\Rightarrow$ (iii): Assume that E is a splitting field of a family of polynomials $\{f_i(x) \mid i \in I\}$ in $F[x]$.

Let $\sigma: E \to \bar{F}$ be any embedding of E into $\bar{F}$ such that $\sigma(a) = a \ \forall \ a \in F$.

Note that if α is a root of $f_i(x)$, $i \in I$ then $\sigma(\alpha)$ is also a root of $f_i(x) \in F[x]$.

Thus σ maps E into E as E is generated over F by the roots of the family of polynomials $\{f_i(x) \mid i \in I\}$ in $F[x]$.

Therefore $\sigma: E \to E$ is an embedding of E into E such that $\sigma(a) = a \ \forall \ a \in F$.

Now since E is an algebraic extension of F, $\sigma: E \to E$ is an embedding of E into E (i.e., $\sigma(E) = E$) and σ is an identity on F, by known theorem σ is an automorphism of E.

This Proves condition(iii).

Hence (ii) $\Rightarrow$ (iii). ------ (2).

(iii) $\Rightarrow$ (i): Assume that every embedding $\sigma: E \to \bar{F}$ which is an identity on F maps E onto E.

Let $f(x) \in F[x]$ be an irreducible polynomial over F and $f(x)$ has a root $\alpha \in E$.

Since all the roots of $f(x)$ are in $\bar{F}$, let $\beta \in \bar{F}$ be another root of $f(x)$.

Since $f(x)$ is irreducible over F, we have F- isomorphisms

$$\frac{F[x]}{(f(x))} \cong F(\alpha) \text{ and } \frac{F[x]}{(f(x))} \cong F(\beta)$$

Therefore, $F(\alpha) \cong F(\beta)$.

Let $\sigma: F(\alpha) \to F(\beta)$ be the above isomorphism. Then $\sigma(a) = a \; \forall \; a \in F$ and $\sigma(\alpha) = \beta$.

Note that $\sigma: F(\alpha) \to \bar{F}$ is an embedding of $F(\alpha)$ into an algebraically closed field $\bar{F}$.

Now since E is an algebraic extension of F, E is also an algebraic extension of $F(\alpha)$.

Thus σ can be extended to an embedding $\sigma^*: E \to \bar{F}$ such that $\sigma^*(\alpha) = \sigma(\alpha) = \alpha$ for all

$\alpha \in F$.

By hypothesis σ^* is an automorphism of E. i.e., $\sigma^*(E) = E$.

Also $\sigma^*(\alpha) = \sigma(\alpha) = \beta \in E$.

Thus, all the roots of $f(x)$ are in E and hence $f(x)$ splits into linear factors in E.

Hence every irreducible polynomial that has a root in E splits into linear factors in E.

This proves condition (i).

Hence (iii) ⇒ (i). ------ (3).

From (1), (2) and (3) we have, $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

Thus, the conditions (i), (ii) and (iii) are all equivalent.

6.2.3: Note: The above theorem proves a set of equivalent conditions for an extension E of F to be a splitting field of a family of polynomials over a given field F.

6.2.4: Definition: An extension E of a field F is called normal if E satisifies any one of the equivalent conditions of Theorem 6.2.2

6.2.5: Examples of normal extensions:

i) C is a normal extension of R.

Solution: We know that every irreducible polynomial over R have either a real root or a complex root or both.

Hence any irreducible polynomial in $\mathrm{R}[x]$ can split into linear factors in C.

Therefore, C is a normal extension of R.

ii) R is not a normal extension of Q.

Solution: Consider a polynomial $x^3 - 2 \in Q[x]$.

$$Let\ P(x) = x^3 - 2$$

$$= x^3 - (2^{1/3})^3$$

$$= \left(x - 2^{1/3}\right)\left(x^2 + 2^{1/3}x + 2^{2/3}\right)$$

$$= (x - 2^{1/3})(x - \alpha)(x + \alpha)\ where\ \alpha = \frac{-2^{1/3} \pm 2^{1/3} \times \sqrt{3}i}{2}$$

Thus, $P(x)$ cannot split into linear factors in R as it has complex roots.

Hence R is not a normal extension of Q.

iii) Let E be an extension of a field F such that $[E: F] = 2$. Then E is a normal extension of F.

Solution: Let E be an extension of a field F such that $[E: F] = 2$.

$\Rightarrow$ E is a finite extension of F.

Hence E is an algebraic extension.

Let $\alpha \in E\ and\ \alpha \notin F$.

$\Rightarrow$ There exists a minimal polynomial $P(x) \in F[x]$ such that $P(\alpha) = 0$ and $degP(x) \geq 1$.

$\Rightarrow [F(\alpha): F] = degP(x)$

$$Consider\ [E: F] = [E: F(\alpha)][F(\alpha): F]$$

$$\Rightarrow 2 = [E: F(\alpha)][F(\alpha): F]$$

$$\Rightarrow [E: F(\alpha)] = 1\ and\ [F(\alpha): F] = 2 = degP(x).$$

Therefore, $E = F(\alpha)$.

Thus E is a splitting field of the polynomial $P(x)$.

Hence E is a normal Extension of F.

iv) If $\alpha = \cos\left(\frac{\Pi}{4}\right) + i\sin\left(\frac{\Pi}{4}\right)$, then $Q(\alpha)$ is a normal extension of Q.

Solution: Let $\alpha = \cos\left(\frac{\Pi}{4}\right) + i\sin\left(\frac{\Pi}{4}\right) = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} = \frac{1+i}{\sqrt{2}}$.

The polynomial in $Q(\alpha)$ having α as a root is $x - \alpha = 0$.

$$\Rightarrow x = \alpha = \frac{1+i}{\sqrt{2}}$$

$$\Rightarrow \sqrt{2}x = 1 + i$$

$$\Rightarrow \sqrt{2}x - 1 = i$$

$$\Rightarrow \left(\sqrt{2}x - 1\right)^2 = i^2$$

$$\Rightarrow 2x^2 + 1 - 2\sqrt{2}x = -1$$

$$\Rightarrow 2\left(x^2 + 1 - \sqrt{2}x\right) = 0$$

$$\Rightarrow x^2 + 1 - \sqrt{2}x = 0$$

$$\Rightarrow (x^2 + 1)^2 = \left(\sqrt{2}x\right)^2$$

$$\Rightarrow x^4 + 2x^2 + 1 = 2x^2 \Rightarrow x^4 + 1 = 0$$

Thus, the polynomial in $Q[x]$ having α as a root is $x^4 + 1$

Now $x^4 + 1 = (x^2)^2 + 1 - 2x^2 + 2x^2$

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

Thus, the roots of $x^4 + 1 = 0$ are $\frac{1\pm i}{\sqrt{2}}, \frac{-1\pm i}{\sqrt{2}}$.

Since $\alpha = \frac{1+i}{\sqrt{2}}$, all the roots of $x^4 + 1 = 0$ are in Q(α).

(In terms of α, these roots are $\alpha, \alpha^3, \alpha^5 \text{ and } \alpha^7$).

Therefore, $Q(\alpha)$ is a splitting field of $x^4 + 1$ in $Q[x]$.

Hence $Q(\alpha)$ is a normal extension of Q.

v) Let E be a finite extension of F. Then E is a normal extension of F if and only if E is a splitting field of a polynomial $f(x) \in F[x]$.

Solution: Let E be a finite extension of F.

Then $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$.

Note that each α_i is algebraic over F.

Let $P_i(x)$ be the minimal polynomial for α_i over F for all i = 1, 2, ……, n.

Let E be a normal extension of F.

Then we have for each i, $P_i(x)$ is an irreducible polynomial over F with one root $\alpha_i \in E$.

Also $P_i(x)$ has all its roots in E as E is the normal extension of F.

Let $f(x) = P_1(x)P_2(x).P_2(x)\ldots\ldots P_n(x)$.

Clearly $f(x) \in F[x]$ as $P_i(x) \in F[x]$ for all i =1, 2, ..., n.

So, all the roots of $f(x)$ are in E and E is the smallest extension of F containing all the roots of $f(x)$.

Thus $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the splitting field of the polynomial $f(x) \in F[x]$.

Conversely, suppose that E is a splitting field of a polynomial $f(x) \in F[x]$.

Then E is a normal extension of F by the definition of normal extension.

6.3 SUMMARY:

This lecture imparted the basic concept of the splitting field of a family of polynomials over the base field namely the normal extension. In short normal extension contains all the roots of polynomials in that family. Some equivalent conditions were also given for an extension E of the base field F to be a splitting field of a family of polynomials over F. Few illustrative examples were also given in this lesson for showing whether the given extension is normal or not for the benefit of reader. Normal extensions have applications in coding theory, cryptography and network security, primarily through their use in constructing and analysing error-correcting codes, building secure cryptographic systems and designing robust network protocols. In particular normal extensions are crucial in constructing algebraic codes, which are used for error detection and correction in data transmission and storage.

6.4 TECHNICAL TERMS:

Splitting field: Let F be any field and $f(x) \in F[x]$ be any polynomial of degree ≥ 1. Then an extension K of F is called a splitting field of $f(x)$ over F, if

i) $f(x)$ can be factorized into liner factors in $K[x]$. That is,

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\ldots\ldots(x-\alpha_n),\ \alpha_1,\alpha_2,\ldots.\alpha_n \in K \text{ and } a \in F.$$

ii) $K = F(\alpha_1,\alpha_2,\ldots,\alpha_n)$. i.e., K is generated by F and the roots $\alpha_1,\alpha_2,\ldots,\alpha_n$ of $f(x)$ in K.

Irreducible polynomial: A polynomial $f(x) \in F[x]$ is called irreducible if the degree of $f(x) \geq 1$ and whenever $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x]$ then $g(x) \in F$ or $h(x) \in F$. If a polynomial is not irreducible, it is called reducible.

Algebraic element: Let E be an extension of a field F. An element $\alpha \in E$ is called algebraic over F if there exists a non-constant polynomial $P(x) \in F[x]$ such that $P(\alpha) = 0$.

Minimal polynomial: The monic irreducible polynomial in $F[x]$ for which a will be a root is called the minimal polynomial of a over F.

Algebraic Extension: An extension E of a field F is called algebraic if each element of E is algebraic over F.

Algebraically closed field: A field K is algebraically closed if it possesses no proper algebraic extensions. That is, if every algebraic extension of K coincides with K.

Normal extension: An extension E of a field F is called normal if E satisfies any one of the equivalent conditions of theorem 6.2.2 in this lesson.

Splitting field of a family of polynomials: Let F be any field and $\{f_i(x)|i \in I\}$ be a family of polynomials of degree ≥ 1 over F. An extension E of F is said to be the splitting field of the family of polynomials $\{f_i(x)|i \in I\}$, if

(i) Each $f_i(x)$ splits into linear factors in $E[x]$.

(ii) E is generated over F by all the roots of the polynomials $f_i(x), i \in I$.

6.5 SELF- ASSESSMENT QUESTIONS:

1. Show that $Q(\sqrt{2})$ is a normal extension of Q.

Ans: The minimal polynomial of $\sqrt{2}$ over Q is $x^2 - 2$.

The polynomial splits completely in Q as

$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Therefore, $Q(\sqrt{2})$ is a normal extension of Q.

2. Show that $Q(\sqrt{2}, i)$ is a normal extension of Q.

Ans: The polynomial $x^2 + 1$ has a root namely $i = \sqrt{-1}$ in $Q(\sqrt{2}, i)$ and it splits completely $Q(\sqrt{2}, i)$ as $x^2 + 1 = (x + i)(x - i)$.

Also, the polynomial $x^2 - 2$ has a root namely $\sqrt{2}$ in $Q(\sqrt{2}, i)$ and it splits completely in $Q(\sqrt{2}, i)$ as $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$.

Thus $Q(\sqrt{2}, i)$ is a normal extension of Q.

3. Show that $Q(\sqrt[3]{2})$ is not a normal extension of Q.

Ans: The minimal polynomial of $\sqrt[3]{2}$ over Q is $x^3 - 2$.

Also $x^3 - 2 = x^3 - \left(2^{1/3}\right)^3 = x^3 - \left(\sqrt[3]{2}\right)^3$

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

This polynomial $x^3 - 2$ has one real root $\sqrt[3]{2}$ in $Q(\sqrt[3]{2})$ and two complex roots.

Since the complex roots are not in $Q(\sqrt[3]{2})$, $Q(\sqrt[3]{2})$ is not a normal extension.

4. Show that $Q(\sqrt[4]{2})$ is not a normal extension of Q.

Ans: The minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$.

Also $x^4 - 2 = x^4 - \left(\sqrt[4]{2}\right)^4$

$= \left[x^2 - \left(\sqrt[4]{2}\right)^2\right]\left[x^2 + \left(\sqrt[4]{2}\right)^2\right]$

Thus, the roots of x^4-2 are $\pm\sqrt[4]{2}$ *and* $\pm i\sqrt[4]{2}$

Clearly $\pm\sqrt[4]{2} \in Q(\sqrt[4]{2})$ but the other two complex roots are not in $Q(\sqrt[4]{2})$.

Therefore, $Q(\sqrt[4]{2})$ is not a normal extension of Q.

5. Show that $Q(\sqrt{-2})$ is a normal extension of Q.

Ans: The minimal polynomial of $\sqrt{-2}$ over Q is $x^2 + 2$

The roots of $x^2 + 2$ in C are $\sqrt{-2}$, - $\sqrt{-2}$ and both of these two roots $\in Q(\sqrt{-2})$.

Hence $Q(\sqrt{-2})$ is a normal extension of Q.

6. If x is not algebraic over Q then show that $Q(x)$ is not a normal extension of Q.

Ans: Given x is not algebraic over Q.

Then $Q(x)$ is not an algebraic extension of Q.

Hence $Q(x)$ is not a normal extension of Q.

7. Find the smallest normal extension (up to isomorphism) of $Q(2^{1/4}, 3^{1/4})$ in Q.

Ans: The minimal polynomial of $2^{1/4}$ is $x^4 - 2$ and

the minimal polynomial of $3^{1/4}$ is $x^4 - 3$.

Thus, the smallest normal extension of $Q(2^{1/4}, 3^{1/4})$ is the splitting field of

$(x^4 - 2)(x^4 - 3)$.

The splitting field of $(x^4 - 2)(x^4 - 3)$ is $Q(2^{1/4}, 3^{1/4}, i)$.

Thus, $Q(2^{1/4}, 3^{1/4}, i)$ is the smallest normal extension of $Q(2^{1/4}, 3^{1/4})$ in Q.

8. Define normal extension of a field F and give two examples.

Ans: (Refer: Definition 6.2.4 and Examples 6.2.5)

6.6 SUGGESTED READINGS:

1. P. B. Bhattacharya, S. K. Jain and S. R. Nag Paul, Basic Abstract Algebra, Second Edition, Cambridge University Press,1995.
2. I. N. Herstein, Topics in Algebra, Second Edition, John Wiley & sons, Inc,1975.
3. Thomas W. Hungerford, Algebra, Springer-Verlag, New York.

- **Dr. P. Vijaya Saradhi**

LESSON- 7

MULTIPLE ROOTS

OBJECTIVE:

- To find the multiplicity of the roots of a polynomial over a given field.
- To construct some simple characterizations for an irreducible polynomial over a given field to have multiple roots.
- To prove that over any given field all the roots of an irreducible polynomial have the same multiplicity.

STRUCTURE:

7.1 INTRODUCTION:

A multiple root (also called a repeated root) of a polynomial is a root that occur more than once in its factorization. For example, in the polynomial $f(x) = (x-2)^2(x+5)$, $x = 2$ is a double root (multiplicity 2) while $x = -5$ is a simple root (multiplicity 1). Mathematically a root r of a polynomial $f(x)$ is a multiple root if both $f(r) = 0$ and $f'(r) = 0$, where f' is the derivative of f. Even through the study of polynomial equations started much earlier, it gained a formal algebraic structure through the works of Giralamo Cardino (solution of cubic equations) and Lodovico Ferrari (solution of quadratic equations). In the early 19th century, Evariste Galois developed a revolutionary frame work that connected field theory with group theory to explain the solvability of polynomial equations. One fundamental concept emerged in this context is the discriminant of a polynomial which closely relates to multiple roots. The discriminant of a polynomial is zero if and only if the polynomial has a multiple root. If the discriminant is not equal to zero, then the polynomial is separable. A polynomial is separable if it has no multiple roots. Multiple roots in Galois theory serve as a gateway to understand deeper structural properties of field extensions and the behaviour of polynomial equations. Practically this concept bridges abstract algebra with applications across modern mathematics, computer science and other fields.

7.2 MULTIPLE ROOTS:

In this lesson we discuss about the multiplicity of roots of a polynomial over a given field. First, we define the derivative of a polynomial.

7.2.1: Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{i=0}^{n} a_ix^i$ be a polynomial over a field *F*. We define the derivative of $f(x)$ denoted by $f'(x)$ as $f'(x) = \sum_{i=1}^{n} ia_ix^{i-1}$.

7.2.2: Remarks:

1) We may have $f'(x) = 0$ but $f(x)$ need not be a constant always. For example, let $f(x) = x^2$ in a field of characteristic 2 then $f'(x) = 2x = 0$.

2) The operation of derivative is a linear operation.

7.2.3: Theorem: $(af(x) + bg(x))' = af'(x) + bg'(x)$ where $a, b \in F$.

Proof: Let $f(x) = \sum_{i=0}^{n} a_ix^i$ and $g(x) = \sum_{j=0}^{n} b_jx^j$ be polynomials over a field *F*.

Now $af(x) + bg(x) = a\sum_{i=0}^{n} a_ix^i + b\sum_{j=0}^{n} b_jx^j$ where $a, b \in F$. Then

$$(af(x) + bg(x))' = \left(a\sum_{i=0}^{n} a_ix^i + b\sum_{j=0}^{n} b_jx^j\right)' = \left(a\sum_{i=0}^{n} a_ix^i\right)' + \left(b\sum_{j=0}^{n} b_jx^j\right)'$$

$$= a\sum_{i=1}^{n} ia_ix^{i-1} + b\sum_{j=1}^{n} jb_jx^{j-1} = af'(x) + bg'(x)$$

7.2.4: Theorem: $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Proof: Let $f(x) = \sum_{i=0}^{n} a_ix^i$ and $g(x) = \sum_{j=0}^{n} b_jx^j$ be polynomials over a field *F*.

Now $f(x)g(x) = \sum_{i+j=0}^{m+n} a_ib_jx^{i+j}$.

$$Then,\ (f(x)g(x))' = \left(\sum_{i+j=0}^{m+n} a_ib_jx^{i+j}\right)' = \sum_{i+j=1}^{m+n} (i+j)a_ib_jx^{i+j-1}$$

$$= \sum_{i+j=1}^{m+n} ia_ib_jx^{i+j-1} + \sum_{i+j=1}^{m+n} ja_ib_jx^{i+j-1}$$

$$= \sum_{i=1}^{m} ia_ix^{i-1}\sum_{j=0}^{n} b_jx^j + \sum_{i=0}^{m} a_ix^i + \sum_{j=1}^{n} jb_jx^{j-1} = f'(x)g(x) + f(x)g'(x).$$

7.2.5: Definition: Let $f(x) \in F[x]$ be any polynomial over a field *F* and *K* be the splitting field of $f(x)$ over *F*. Let $\alpha \in K$ be a root of $f(x)$. Then $(x - \alpha)|f(x)$ in $K[x]$. If $(x - \alpha)^s$ is the highest power of $(x - \alpha)$ that divides $f(x)$, then s is called the multiplicity of α.

If $s = 1$, then s is called a simple root.

If $s > 1$, then s is called a multiple root.

7.2.6: Theorem: Let $f(x) \in F[x]$ be a polynomial of degree ≥ 1 with α as a root. Then α is a multiple root if and only if $f'(\alpha) = 0$.

Proof: Let $f(x) \in F[x]$ be a polynomial of degree ≥ 1 with α as a root.

Assume that α is a multiple root.

Then $f(x) = (x-\alpha)^k g(x)$ where $k > 1$ and $g(x) \neq 0$.

$\Rightarrow f'(x) = (x-\alpha)^k g'(x) + k(x-\alpha)^{k-1} g(x)$.

$\Rightarrow f'(\alpha) = (\alpha-\alpha)^k g'(x) + k(\alpha-\alpha)^{k-1} g(\alpha) = 0 + 0 = 0$.

Therefore, $f'(\alpha) = 0$.

Converse: Suppose that $f'(\alpha) = 0$.

Since α is a root of $f(x)$, we have $f(x) = (x-\alpha)g(x)$. (1)

$\Rightarrow f'(x) = g(x) + (x-\alpha)g'(x)$.

$\Rightarrow f'(\alpha) = g(\alpha) + (\alpha-\alpha)g'(\alpha)$.

$\Rightarrow 0 = g(\alpha) + 0$ ($\because f'(\alpha) = 0$ by hypothesis).

$\Rightarrow g(\alpha) = 0$.

Thus, α is a root of $g(x)$.

Then $g(x) = (x-\alpha)h(x)$, so that equation (1) becomes $f(x) = (x-\alpha)(x-\alpha)h(x)$.

$\Rightarrow f(x) = (x-\alpha)^2 h(x)$

Therefore, α is a multiple root.

7.2.7: Corollary1: Let $f(x)$ be an irreducible polynomial over *F*. Then $f(x)$ has a multiple root if and only if $f'(x) = 0$.

Proof: Let $f(x) \in F[x]$ be irreducible over *F*.

Assume that $f(x)$ has a multiple root, say α.

Then by above theorem 7.2.6, $f'(\alpha) = 0$.

So, α is a root of both $f(x)$ and $f'(x)$.

To prove that $f'(x) = 0$

If possible, suppose that $f'(x) \neq 0$

Now since $f(x)$ is irreducible over F, $a^{-1} f(x)$ is the minimal polynomial of α over F where a is the leading coefficient of $f(x)$.

$\Rightarrow \deg f'(x) \geq \deg a^{-1} f(x)$.

Which is a contradiction ($\because \deg f'(x) < \deg f(x)$, by definition of $f'(x)$).

So, our assumption that $f'(x) \neq 0$ is wrong.

Hence, $f'(x) = 0$.

Conversely, suppose that $f'(x) = 0$.

$\Rightarrow f'(\alpha) = 0$ for all α, a root of $f(x)$.

Then by the above theorem, 7.2.6, α is a multiple root.

7.2.8: Corollary 2: Any irreducible polynomial $f(x)$ over a field of characteristic zero has simple roots. Also, any irreducible polynomial over a field F of characteristic $p \neq 0$ has multiple roots if and only if there exists $g(x) \in F[x]$ such that $f(x) = g(x^p)$.

Proof: Let $f(x) \in F[x]$ be an irreducible polynomial over F.

Suppose that $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{i=0}^{n} a_i x^i$ where $a_i's \in$ F

To prove the corollary, we consider two cases.

Case1: Let F be a field of characteristic zero.

$\Rightarrow \exists$ no positive integer 'n' such that $na = 0$ for $a \in F$ (i.e., $na = 0 \Rightarrow a = 0$).

To prove that $f(x)$ has simple roots.

If possible, suppose that α is a multiple root of $f(x)$.

Then by the above corollary 7.2,7, $f'(x) = 0$.

$\Rightarrow \sum_{i=1}^{n} ia_i x^{i-1} = 0$

$\Rightarrow ia_i = 0$ for all $i = 1, 2, \ldots, n$.

$\Rightarrow a_i = 0$ for all $i = 1, 2, \ldots, n$. ($\because charF = 0$).

Then $f(x) = a_0$, a constant.

Which is a contradiction to $f(x) \in F[x]$ is irreducible over F.

So, $f(x)$ has no multiple roots when char $F = 0$.

Hence all the roots of $f(x) \in F[x]$ are simple when char $F = 0$.

Case 2: Let F be a field of characteristic $p \neq 0$.

Then p is a least positive integer such that $pa = 0 \ \forall \ a \in F$.

Now since $f(x) \in F[x]$ is irreducible over F, by corollary 7.2.7, we have that α is a multiple root of $f(x) \Leftrightarrow f'(x) = 0$.

$\Leftrightarrow \sum_{i=1}^{n} \ ia_i x^{i-1} = 0$.

$\Leftrightarrow ia_i = 0 \ \forall \, i = 1, 2, \ldots, n$.

$\Leftrightarrow$ either $a_i = 0$ (or) $p|i \ \forall \, i = 1, 2, \ldots, n$.

If $a_i = 0$, we get a contradiction.

So, $p|i \Rightarrow i = pk$ for some positive integer k.

$\therefore f(x) = \sum_{i=0}^{n} \ a_i x^i = \sum_{i=0}^{n} \ a_i x^{pk} = \sum_{i=0}^{n} \ a_i (x^p)^k = g(x^p)$.

So, α is a multiple root of $f(x) \Leftrightarrow f(x) = g(x^p)$ for some $g(x) \in F[x]$ when

char F = $p \neq 0$.

7.2.9: Theorem: If $f(x) \in F[x]$ is irreducible over F, then all roots of $f(x)$ have the same multiplicity.

Proof: Let $f(x) \in F[x]$ be an irreducible polynomial over F.

Let α, β be any two distinct roots of $f(x)$ with multiplicities $k \ and \ k'$ respectively.

We prove that $k = k'$.

Since α, β are the roots of an irreducible polynomial $f(x)$, we have

$$F(\alpha) \cong \frac{F[x]}{(f(x))} \cong F(\beta)$$

Let $\sigma: F(\alpha) \to F(\beta)$ be this isomorphism defined by

$\sigma(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = a_0 + a_1\beta + \ldots + a_n\beta^n$

Such that $\sigma(\alpha) = \beta$ and $\sigma(a) = a \ \forall \ a \in F$.

Note that $\sigma: F(\alpha) \to \bar{F}$ is an embedding and can be extended to an embedding $\sigma^*: \bar{F} \to \bar{F}$ such that $\sigma^*(\alpha) = \beta$ and $\sigma^*(a) = a \ \forall \ a \in F$.

Now F is fixed under σ^* and $\bar{F}$ is an algebraic extension of F.

So $\sigma^*: \bar{F} \to \bar{F}$ is an isomorphism.

This isomorphism induces a ring homomorphism $\eta: \bar{F}[x] \to \bar{F}[x]$.

given by $\eta(a_0 + a_1x + \ldots + a_rx^r) = \sigma^*(a_0) + \sigma^*(a_1)x + \ldots + \sigma^*(a_r)x^r$.

Now $\eta(x - \alpha) = \sigma^*(1).x - \sigma^*(\alpha) = 1.x - \beta = x - \beta$.

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \ where \ a_0, \ a_1, \ \ldots, a_n \in F$.

then $\eta(f(x)) = \eta(a_0 + a_1x + \ldots + a_nx^n)$

$= \sigma^*(a_0) + \sigma^*(a_1)x + \ldots + \sigma^*(a_n)x^n$

$= a_0 + a_1x + \ldots + a_nx^n = f(x)$.

So, $\eta(x - \alpha) = x - \beta$ and $\eta(f(x)) = f(x)$.

Now since α is a root of $f(x)$ with multiplicity k, we have

$f(x) = (x - \alpha)^k g(x)$.

Now $f(x) = \eta(f(x))$.

$$\Rightarrow f(x) = \eta((x - \alpha)^k g(x))$$

$$= \eta(x - \alpha)^k \eta(g(x))$$

$$= \eta(x - \alpha)\eta(x - \alpha)\ldots\eta(x - \alpha)\,\eta(g(x))$$

$$= (x - \beta)(x - \beta)\ldots(x - \beta)g(x)$$

$$= (x-\beta)^k g(x).$$

$\Rightarrow k \leq k'$ ($\because$ multiplicity of β is k').

Similarly, we can prove that $k' \leq k$ by interchanging the roles of α and β

Therefore, $k = k'$.

Hence all the roots of $f(x)$ have the same multiplicity.

7.2.10: Corollary: If $f(x) \in F[x]$ is irreducible over F, then $f(x) = a\prod_{i=1}^{r}(x-\alpha_i)^k$, where α_i are the roots of $f(x)$ in its splitting field over F, and k is the multiplicity of each root.

Proof: Let $f(x) \in F[x]$ be irreducible over F.

Also let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the distinct roots of $f(x)$ in its splitting field over F and a be the leading coefficient of $f(x)$.

Then by the above theorem 7.2.9 all the roots of $f(x)$ have the same multiplicity say k.

$$Therefore, f(x) = a(x-\alpha_1)^k(x-\alpha_2)^k \ldots (x-\alpha_r)^k = a\prod_{i=1}^{r}(x-\alpha_i)^k.$$

7.2.11: Example: Let $K = F(x)$ be the field of rational functions in one variable x over a field F of characteristic 3. (Indeed, $F(x)$ is the field of fractions of the polynomial ring $F[x]$). Then the polynomial $y^3 - x$ in the polynomial ring $K[y]$ over K is irreducible over K and has multiple roots.

Solution: Let $K = F[x] = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \neq 0 \in F[x]\right\}$ and let char $F = 3$.

Consider the polynomial $y^3 - x \in K[y]$.

To show that $y^3 - x$ is irreducible over K and has multiple roots.

Now $deg(y^3 - x) = 3$.

So $y^3 - x$ is reducible over K if and only if it has a root in K.

Let $\alpha \in K$ be a root of $y^3 - x$.

Then $\alpha = \frac{f(x)}{g(x)}$ where $f(x), g(x) \neq 0 \in F[x]$ and $\alpha^3 - x = 0$.

$\Rightarrow \left(\frac{f(x)}{g(x)}\right)^3 - x = 0$

$\Rightarrow (f(x))^3 = x(g(x))^3$

$\Rightarrow 3degf(x) = 1 + 3deg\ g(x)$

$\Rightarrow 3n = 1 + 3m$. This is a contradiction.

$\Rightarrow \alpha$ is not a root of $y^3 - x\ \forall\ \alpha \in K$

$\Rightarrow y^3 - x$ has no root in K.

$\Rightarrow y^3 - x$ is irreducible over K.

Let $\alpha,\ \beta$ be any two roots of $y^3 - x$ in its splitting field over K.

Then we have $\alpha^3 - x = 0$ and $\beta^3 - x = 0$

$\Rightarrow \alpha^3 = \beta^3 \Rightarrow \alpha^3 - \beta^3 = 0 \Rightarrow (\alpha - \beta)^3 = 0 \Rightarrow \alpha - \beta = 0\ \Rightarrow \alpha = \beta$

Thus, all the roots of $y^3 - x$ are same.

Hence $y^3 - x$ has a multiple root of multiplicity 3.

Therefore, $y^3 - x$ has multiple roots.

7.3 SUMMARY:

This lesson provided the concept of multiplicity of the roots of a polynomial over any given field. If the multiplicity of a root is one then it is called a simple root and if it is greater than one it is called a multiple root. The derivative of a polynomial is also defined, which plays a key role in the theory of multiple roots of a given polynomial. Some characterizations were also developed to decide whether a root α is a multiple root of the given polynomial or not based on the concept of a derivative of a polynomial. It was also shown that multiplicity of all the roots of an irreducible polynomial over a given field is same. Multiple roots have several significant applications in real life areas like cryptography, computer science and error correction especially when it intersects with the structure of polynomials over finite fields. Particularly in error correcting codes multiple roots affect the structure and decoding of certain codes. The codes like BCH and Reed-Solomon codes are constructed using polynomials over finite fields. If a generator polynomial has multiple roots, some algorithms fail or behave unpredictably. Ensuring distinct roots (i.e., square free polynomials) guarantees error detection and correction strength.

7.4 TECHNICAL TERMS:

Derivative of a polynomial: Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial over a field. We define the derivative of $f(x)$ denoted by $f'(x)$ as $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

Splitting field: Let F be any field and $f(x) \in F[x]$ be any polynomial of degree≥ 1. Then an extension K of F is called a splitting field of $f(x)$ over F, if

$i)$ $f(x)$ can be factorized into linear factors in $K[x]$. That is,

$f(x) = a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$, $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ and $a \in F$.

$ii)$ $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, that is K is generated by F and the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $f(x)$ in K.

Multiplicity of a root of a polynomial: Let $f(x) \in F[x]$ be any polynomial over a field F and K be the splitting field of $f(x)$ over F. Let $\alpha \in K$ be a root of $f(x)$. Then $(x-\alpha) \mid f(x)$ in $K[x]$. If $(x-\alpha)^s$ is the highest power of $(x-\alpha)$ that divides $f(x)$ then s is called the multiplicity of α.

If $s = 1$, the s is called a simple root.

If $s > 1$, then s is called a multiple root.

Characteristic of a field: Let F be any field. If there exists a positive integer 'n' such that $na = 0 \; \forall \; a \in F$, the smallest such positive integer is called the characteristic of a field F. If no such positive integer exists, then the characteristic of field F is zero.

Irreducible polynomial: A polynomial $f(x) \in F[x]$ is called irreducible if the degree of $f(x) \geq 1$ and whenever $f(x) = g(x)h(x)$, where $g(x), \; h(x) \in F[x]$ then $g(x) \in F$ or $h(x) \in F$. If a polynomial is not irreducible, it is called reducible.

Minimal polynomial: The monic irreducible polynomial in $F[x]$ for which u will be a root is called the minimal polynomial of u over F.

Algebraic element: Let E be an extension of F. An element $\alpha \in E$ is called algebraic over F if there exists a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Algebraic Extension: An extension E of a field F is called algebraic if each element of E is algebraic over F.

7.5 SELF- ASSESSMENT QUESTIONS:

1) Verify that $(f(x)+g(x))' = f'(x)+g'(x)$

Ans: Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots.$

Then $f(x)+g(x) = (a_0+b_0) + (a_1+b_1)x + \ldots + (a_i+b_i)x^i + \ldots$

$= \sum_{i=0}^{r}(a_i+b_i)x^i$ (where r= max {deg $f(x)$, deg $g(x)$ })

By definition of the derivative,

$(f(x)+g(x))' = \sum_{i=1}^{r} i(a_i+b_i)x^{i-1}$

$= \sum_{i=1}^{r} ia_ix^{i-1} + \sum_{i=1}^{r} ib_ix^{i-1}$

$= f'(x)+g'(x)$

2) Show that $x^3 - x^2 - x + 1 = 0$ has a repeated root and solve it.

Ans: Let $f(x) = x^3 - x^2 - x + 1.$

$\Rightarrow f'(x) = 3x^2 - 2x - 1.$

Now $f'(x) = 0 \Rightarrow 3x^2 - 2x - 1 = 0.$

$\Rightarrow (3x+1)(x-1) = 0.$

$\Rightarrow x = 1, {}^{-1}/_{3}$.

Thus $1, {}^{-1}/_{3}$ are the roots of $f'(x)$.

Now $f(1) = 1^3 - 1^2 - 1 + 1 = 1 - 1 - 1 + 1 = 0$

$\Rightarrow$ 1is a root of $f(x)$.

Thus 1 is a common root of $f(x)$ and $f'(x)$.

$\Rightarrow$ 1 is a repeated root (or multiple root) of $f(x)$.

Therefore, roots of $f(x)$ are 1, 1, α.

$\Rightarrow (x-1)^2$ is a factor of $f(x)$.

$\Rightarrow (x-1)^2$ divides $f(x)$.

Thus $f(x) = (x-1)^2(x+1)$.

Hence the roots of $f(x)$ are 1, 1, and -1 and out of which 1 is a repeated root of $f(x)$.

3) Show that $x^3 - 3x^2 - 4 = 0$ has no multiple roots.

Ans: Let $f(x) = x^3 - 3x^2 - 4$.
$\Rightarrow f'(x) = 3x^2 - 6x$.

Now $f'(x) = 0 \Rightarrow 3x^2 - 6x = 0. \Rightarrow x(x-2) = 0. \Rightarrow x = 0, 2.$

Thus 0, 2 are the roots of $f'(x)$.

Now $f(0) = 0^3 - 30^2 - 4 = -4 \neq 0.$

$f(2) = 2^3 - 3(2)^2 - 4 = 8 - 12 - 4 = -8 \neq 0.$

So, 0, 2 are not the roots of $f(x)$.

$\Rightarrow f(x)$ and $f'(x)$ have no common root.

Hence $f(x) = x^3 - 3x^2 - 4 = 0$ has no multiple roots.

4) Solve the equation $f(x) = x^4 + 4x^3 - 6x^2 - 36x - 27 = 0$. given that it has a repeated root.

Ans: Let $f(x) = x^4 + 4x^3 - 6x^2 - 36x - 27.$

$\Rightarrow f'(x) = 4x^3 + 12x^2 - 12x - 36.$

Given that $f(x)$ has a repeated root.

Therefore, $f(x)$ and $f'(x)$ has at least one common root.

Now $f'(x) = 0 \Rightarrow 4x^3 + 12x^2 - 12x - 36 = 0.$

$\Rightarrow x^3 + 3x^2 - 3x - 9 = 0.$

$\Rightarrow x^2(x+3) - 3(x+3) = 0.$

$\Rightarrow (x+3)(x^2 - 3) = 0.$

$\Rightarrow x = -3, \pm\sqrt{3}$ are the roots of $f'(x)$.

Now $f(-3) = (-3)^4 + 4(-3)^3 - 6(-3)^2 - 36(-3) - 27$

$= 81 - 108 - 54 + 108 - 27 = 0.$

Thus -3 is a root of $f(x)$.

$\Rightarrow -3$ is a common root of $f(x)$ and $f'(x)$.

$\Rightarrow -3$ is a multiple root of $f(x)$.

$\Rightarrow (x+3)^2$ is a factor of $f(x)$ (or) $(x+3)^2$ divides $f(x)$.

Thus, by ordinary method of division (or short division), we have

$$f(x) = (x+3)^2(x^2-2x-3) = (x+3)^2(x-3)(x+1).$$

Hence the roots of $f(x)$ are $-3, -3, -1$ and 3. Also, -3 is a multiple root of $f(x)$.

5) Define the derivative of a polynomial over a field F and prove that

i) $\big(af(x)+bg(x)\big)' = af'(x)+bg'(x)$.

ii) $(f(x)g(x))' = f'(x)g(x)+f(x)g'(x)$.

Ans: (Refer theorem 7.2.3 and theorem 7.2.4)

6) If $f(x)$ is a polynomial of degree ≥ 1 over a field F with α as a root, then prove that α is a multiple root if and only if $f'(\alpha) = 0$.

Ans: (Refer theorem 7.2.6).

7) If $f(x)$ is an irreducible polynomial over a field F, then show that all the roots of $f(x)$ have the same multiplicity.

Ans: (Refer theorem 7.2.9).

8) If $f(x)$ is an irreducible polynomial over a field F, then prove that $f(x)$ has a multiple root if and only if $f'(x) = 0$.

Ans: (Refer theorem 7.2.7).

7.6 SUGGESTED READINGS:

1. P. B. Bhattacharya, S. K. Jain and S. R. Nag Paul, Basic Abstract Algebra, Second Edition, Cambridge University Press,1995.
2. I. N. Herstein, Topics in Algebra, Second Edition, John Wiley & sons, Inc,1975.
3. Thomas W. Hungerford, Algebra, Springer-Verlag, New York.

- Dr. P. Vijaya Saradhi

LESSON- 8

FINITE FIELDS

OBJECTIVE:

- To understand the concepts of a prime field and a Galois field.
- To show that finite fields (or Galois fields) are splitting fields of suitable polynomials over F_p.
- To prove the existence of a field with p^n elements for any prime p and a positive integer n.

STRUCTURE:

8.1 INTRODUCTION:

It is quite interesting to study finite fields rather than infinite fields. Around 1830's, Galois introduced finite fields implicitly in his work on solving polynomial equations. At that time, he didn't call them as "fields" or "Galois fields". The terminology and formal Structure came later in the 19th century. Ferdinand Frobenius (1879) formally described the structure of finite fields. A finite field or a Galois field is a field with a finite number of elements. Every finite field has p^n elements where p is a prime number and n is a positive integer. For example, $F_2 = \{0,1\}$ is the simplest prime field with arithmetic mod 2. when $n > 1$, the field F_{p^n} is constructed as an extension of F_p. It is built by using irreducible polynomial of degree n over F_p. Finite fields have applications in various fields like Coding Theory, Cryptography and Computer Science etc.

8.2 FINITE FIELDS:

In this lesson we show that an irreducible polynomial over a finite field has only simple roots. We first define the concept of prime field for this purpose.

8.2.1 Definition:

A field F is called a prime field if it has no proper sub field.

8.2.2: Examples

i. Q is a prime field.

ii. $Z/_{(p)}$ or Z_p is a prime field where p is prime.

8.2.3 Remark: Every field F contains a prime field.

Proof: Let F be any field.

Case1: Suppose F has no proper sub field.

Then F itself is a prime field.

Case2: Suppose F has proper sub fields say F_1, F_2, …., F_k, ….

Let K be the intersection of the family of sub fields of F.

That is, $K = F_1 \cap F_2 \cap \ldots \cap F_k \cap \ldots$

Then K is the smallest sub field of F.

Also K does not contain any proper sub field.

So, K is a prime field of F.

8.2.4: Theorem: The prime field of a field F is either isomorphic to Q or to Z_p where p is a prime.

Proof: Let F be a field.

Define a mapping $f: Z \to F$ by $f(n) = ne, e$ is the unity of F.

Now for any $m, n \in Z$,

$f(m+n) = (m+n)e = me + ne = f(m) + f(n)$

$f(mn) = (mn)e = (me)(ne) = f(m)f(n)$.

Then f is a homomorphism of rings and

$kerf = \{n \in Z | f(n) = 0\} = \{n \in Z | ne = 0\}$.

Case1: Suppose that $kerf = 0 \Rightarrow ne = 0 \Rightarrow n = 0$

So, char $F = (0)$

We know that $kerf = 0$ if and only if f is one-one.

Then f is an embedding of Z into F.

This embedding of f can be extended to an embedding

$f^*: Q \to F$ by defining $f^*\left(\frac{m}{n}\right) = \frac{me}{ne}$, $0 \neq n \in Z$

Thus Q embeds in F and the prime field of F is isomorphic to Q.

Case2: Suppose that $kerf \neq \{0\}$.

Then $kerf$ is an ideal of Z.

Since Z is a PID, every ideal in Z is a principal ideal.

$\Rightarrow kerf$ is a non-zero principal ideal in Z.

$\therefore$ By fundamental theorem of homomorphism, $\frac{Z}{kerf} \simeq Imf \subseteq Z$

$\Rightarrow \frac{Z}{(m)} \simeq f(Z) \subseteq F$.

As $f(Z) \subseteq F, f(Z)$ has nonzero divisors.

$\Rightarrow \frac{Z}{(m)}$ has no nonzero divisors

$\Rightarrow m$ is a prime number $= p$, say.

$\Rightarrow \frac{Z}{(m)} = \frac{Z}{(p)} = Z_p$ is a prime field.

Therefore, $f(Z)$ is a sub field of F and $f(Z) \simeq Z_p$.

$\Rightarrow f(Z)$ is also a prime field of F.

Hence the prime field of a field F is isomorphic to $\frac{Z}{(p)}$ where p is a prime.

8.2.5: Theorem: Let F be a finite field. Then

i) The characteristic of F is a prime number p and F contains a sub field $F_p \simeq \frac{Z}{(p)}$.

ii) The no. of elements in F is p^n for some positive integer n.

Proof: Let F be a finite field.

i) We know that for any field F, either char $F = 0$ or $char\ F = p$, where p is a prime number.

Since F is a finite field, char $F = p$.

We know that every field contains a prime field.

So, F contains a prime field denoted by F_p.

By Theorem 8.2.4 above $F_p \simeq \frac{Z}{(p)}$

Hence the characteristic of F is a prime number p and F contains a sub field $F_p \simeq \frac{Z}{(p)}$

This proves part (i)

ii) By part(i), we have that $F_p \simeq \frac{Z}{(p)}$.

So, the number of elements in F_p is p.

To prove(ii), we regard F as a vector space over its prime field F_p.

Since F is finite, F is a finite dimensional vector space over F_p.

Then $[F: F_p] = n$ for some positive integer n.

Let $\{e_1, e_2, \ldots, e_n\}$ be a basis of F over Fp.

Any element $x \in F$ can be uniquely expressed as

$x = a_1e_1 + a_2e_2 + \ldots + a_ne_n$ where $a_i \in F_p$, $i = 1, 2, \ldots, n$.

Here each a_i in this expression for x can be chosen in p ways and there are n such a_i's in this expression.
Hence the no. of elements in F is p^n for some positive integer n.

8.2.6: Notation: A finite field F is also called a Galois field. A Galois field with p^n elements is usually written as GF (p^n)

8.2.7: Theorem: A finite field F with p^n elements is the splitting field of $x^{p^n} - x \in F_p[x]$. Consequently, any two finite fields with p^n elements are isomorphic.

Proof: Let F be a finite field with p^n elements.
Then $F^* = F\backslash\{0\}$ is a multiplicative group of order $p^n - 1$.

$\Rightarrow \forall 0 \neq \lambda \in F,\ \lambda^{p^n-1} = 1 \left(\because \forall a \in G, a^{|G|} = e\right)$.

$\Rightarrow \lambda^{p^n} = \lambda$ (or) $\lambda^{p^n} - \lambda = 0$.

$\Rightarrow \lambda$ satisfies the equation $x^{p^n} - x = 0 \,\forall\, 0 \neq \lambda \in F$ and also $\lambda = 0$ satisfies the equation $x^{p^n} - x = 0$

Now because $x^{p^n} - x \in F_p[x]$ has only p^n roots, it follows that F coincides with the set of roots of $x^{p^n} - x$.

$\Rightarrow$ F is the splitting field of $x^{p^n} - x$ over F_p.

As a consequence of this now we will now prove that any two finite fields with p^n elements are isomorphic.

Let E and F be two finite fields with p^n elements.

By Theorem 8.2.5., E and F contains sub fields E_p and F_p such that

$E_p \simeq \frac{Z}{(p)}$ and $F_p \simeq \frac{Z}{(p)}$.

This implies $E_p \simeq F_p$.

Moreover, by the above part, E is the splitting field of $x^{p^n} - x \in E_p[x]$ and F is the splitting field of $x^{p^n} - x \in F_p[x]$

But since $E_p \simeq F_p$, it follows that $E \simeq F$ by uniqueness of splitting fields.

Hence any two finite fields with p^n elements are isomorphic.

8.2.8: Theorem: For each prime p and each positive integer $n \geq 1$, the roots of $x^{p^n} - x \in Z_p[x]$ in its splitting field over Z_p are all distinct and form a field F with p^n elements. Also F is the splitting field of $x^{p^n} - x$ over Z_p.

Proof: Let p be any prime number and $n \geq 1$ be a positive integer.

Consider the polynomial $f(x) = x^{p^n} - x \in Z_p[x]$.

Then $f'(x) = p^n . x^{p^n-1}$

Let α be any root of $f(x) = 0 \Rightarrow f(\alpha) = 0$ and $f'(\alpha) = p^n.\alpha^{p^n-1} \neq 0$

$\Rightarrow f'(\alpha) \neq 0$.

$\Rightarrow \alpha$ is a simple root of $f(x)$.

Thus, all the p^n roots of $f(x)$ are distinct.

Let $F = \{\alpha: \alpha \text{ is a root of } f(x) = x^{p^n} - x \text{ in its splitting field over } Z_p\}$.

Since $f(x)$ has p^n distinct roots, F contains p^n elements. i.e, $|F| = p^n$.

Now we will show that F forms a field with p^n elements.

For this it is enough to show that $\alpha \pm \beta,\ \alpha\beta^{-1} \in F\ \forall\ \alpha, \beta \in F\ \&\ \beta \neq 0$.

Let $\alpha, \beta \in F$ and $\beta \neq 0 \Rightarrow \alpha^{p^n} - \alpha = 0$ and $\beta^{p^n} - \beta = 0$

$$\Rightarrow \alpha^{p^n} = \alpha \text{ and } \beta^{p^n} = \beta.$$

Now since, α, β are the roots of $x^{p^n} - x \in Z_p[x]$, we have $charZ_p = p$.

Consider $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}\ (\because charZ_p = p)$.

$$= \alpha \pm \beta\ (\because \alpha^{p^n} = \alpha\ and\ \beta^{p^n} = \beta).$$

$\Rightarrow (\alpha \pm \beta)^{p^n} - (\alpha \pm \beta) = 0.$ (1)

Also $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}.(\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}$.

$\Rightarrow (\alpha\beta^{-1})^{p^n} - (\alpha\beta^{-1}) = 0.$ (2)

From (1) and (2) $\alpha \pm \beta$ and $\alpha\beta$ are the roots of $f(x) = x^{p^n} - x \in Z_p[x]$ over Z_p.

$\Rightarrow \alpha \pm \beta \in F$ and $\alpha\beta^{-1} \in F$.

$\Rightarrow F$ is a field with p^n elements $(\because |F| = p^n)$.

Thus, all the roots of $x^{p^n} - x$ over Z_p forms a field F with p^n elements.

Hence, by above theorem 8.2.7, F is the splitting field of the polynomial $x^{p^n} - x$ over Z_p.

8.2.9: Theorem: If F is a field with p^n elements and m is a positive integer, then there exists an extension field E of F such that $[E: F] = m$, and all such extensions are isomorphic.

Proof: Let F be a finite field with p^n elements and m be any positive integer.

Consider the polynomial $f(x) = x^{p^{mn}} - x \in F[x]$.

Note that for any $0 \neq \alpha \in F, \alpha^{p^n-1} = 1$ because the multiplicative group of F is of order $p^n - 1$.

This implies $\alpha^{p^{mn}-1} = 1\ (\because n|mn, (p^n - 1)|(p^{mn} - 1))$

$\Rightarrow \alpha^{p^{mn}} = \alpha$ (or) $\alpha^{p^{mn}} - \alpha = 0$

$\Rightarrow \alpha$ satisfies the polynomial $f(x)\ \forall\ \alpha \in F$.

$\Rightarrow \alpha$ is a root of $f(x)$

Thus, every element of F is a root of $f(x)$.

Now let E be the set of all p^{mn} roots of $f(x) = x^{p^{mn}} - x \in F[x]$

Then by the above theorem 8.2.8, all the roots of E are distinct and forms a field.

Therefore, E is a field with p^{mn} elements.

Hence E is an extension of F and $[E: F_P] = mn$.

Also, we have $[F: F_p] = n$

$\Rightarrow [E: F_P] = [E: F][F: F_P]$

$\Rightarrow mn = [E: F]n$

$\Rightarrow [E: F] = m$

Let K be another extension of F such that $[K: F] = m$.

Then K will be a field with p^{mn} elements.

Thus K, E are both finite fields with p^{mn} elements.

Therefore, $K \simeq E$

Hence all such extensions of F are isomorphic.

8.2.10: Note: Let a and b be the elements of a finite abelian group G of orders m and n respectively. Then there exists an element $c \in G$ whose order is the l.c.m of m and n.

8.2.11: Theorem: The multiplicative group of nonzero elements of a finite field is cyclic.

Proof: Let F be a finite field.

Consider the multiplicative group of nonzero elements of F namely, $F^* = F\backslash\{0\}$.

Now F^* is a finite group.

Let r be the l.c.m of the orders of all elements in F^*.

By the above note 4.2.10, $\exists$ an element $\alpha \in F^*$ such that $O(\alpha) = r$

Now by the choice of r, we have that $O(a)|r \ \forall\, a \in F^*$

$\Rightarrow a^r = 1 \ \forall\, a \in F^*$

$\Rightarrow$ Every element of F^* satisfies the polynomial $x^r - 1$.

Since the polynomial $x^r - 1$ has at most r distinct roots in F, it follows that the no.of elements in $F^* \leq r$ that is, $|F^*| \leq r$. (1)

Further note that as $O(\alpha) = r$, we have $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ are all distinct and belong to F^*

i.e., $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\} \subseteq F^*$

$\Rightarrow r \leq |F^*|$ ---------- (2).

From (1) and (2), $|F^*| = r$

$\therefore F^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\} = (\alpha)$ $(\because O(\alpha) = r)$

Hence F^* is a cyclic group.

8.2.12: Corollary: Let E be a finite extension of a finite field F. Then $E = F(\alpha)$ for some $\alpha \in E$.

Proof: Let E be a finite extension of a finite field F.

Then E is a finite field.

By the above theorem 8.2.11 the multiplicative group E^* is cyclic where $E^* = E\backslash\{0\}$.

i.e., $E^* = (\alpha)$ for some $\alpha \in E$.

Also $E = E^* \cup \{0\} = (\alpha) \cup \{0\} \subseteq F(\alpha) \subseteq E$.

$\Rightarrow E = F(\alpha)$ for some $\alpha \in E$.

8.2.13: Theorem: Let F be a finite field. Then there exists an irreducible polynomial of any given degree n over F.

Proof: Let F be a finite field and n be any positive integer.

Then $\exists$ an extension E of Fsuch that $[E: F] = n$.

Now since E is a finite extension of F, by the above corollary 8.2.12,

$E = F(\alpha)$ for some $\alpha \in E$.

Also, because E is a finite extension of F, $\alpha \in E$ is algebraic over F.

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

Then $[F(\alpha): F] = \deg\ p(x)$

But since $F(\alpha) = E$ and $[E: F] = n$, we have $n = [F(\alpha): F] = deg\ p(x)$

$\Rightarrow p(x)$ is an irreducible polynomial of degree n over F.

8.2.14: Examples:

1) Show that a finite field F of p^n elements has exactly one subfield with p^m elements for each divisor m of n.

Solution: First we state a result in group theory: A cyclic group of order n has a unique subgroup of order 'd' for each divisor d of n.

Let F be a finite field with p^n elements.

Then $F^* = F\backslash\{0\}$ is a cyclic group of order $p^n - 1$.Now for each divisor m of n,

$(p^m - 1)|(p^n - 1)$.

$\Rightarrow p^m - 1$ is a divisor of the order of the group F^* which is cyclic.

$\Rightarrow F^*$ has a unique subgroup of order $p^m - 1$ say H ($\because$ by the result stated above)

So, for all $\alpha \in H$, $\alpha^{p^m - 1} = 1 \Rightarrow \alpha^{p^m} = \alpha$ (or) $\alpha^{p^m} - \alpha = 0$.

$\Rightarrow \alpha$ is a root of $x^{p^m} = x\ \forall\ \alpha \in H$.

Hence $H \cup \{0\} = K$ (say) is the set of all roots of $x^{p^m} - x \in F_p[x]$, which forms a field contained in F.

$\Rightarrow K$ is a subfield of F with p^m elements i.e., $|K| = p^m$.

Now let L be any other subfield of F with p^m elements.

Then L^* is a subgroup F^* of order $p^m - 1$

$\Rightarrow L^* = H$ ($\because$ by the uniqueness of H)

$\Rightarrow L = L^* \cup \{0\} = H \cup \{0\} = K$.

Hence F has exactly one subfield with p^m elements for each divisor m of n.

2) If the multiplicative group F^* of nonzero elements of a field F is cyclic then F is finite.

Solution: Let the multiplicative group F^* of nonzero elements of a field F be cyclic.

Then $F^* = (\alpha)$ for some $\alpha \in F$.

If F^* is finite, then F is finite and the proof is complete.

So assume that F^* is an infinite cyclic group.

Case 1: $charF = p \neq 0 \ \ (or\ p > 0)$

Then we have $F = F_p(\alpha)$ where F_p is the subfield $\{0, 1, 2, \ldots, p-1\}$ of F.

Consider the element $1 + \alpha \in F$

Then $1 + \alpha = 0$ or $1 + \alpha \neq 0$

If $1 + \alpha = 0$ the $\alpha = -1 \Rightarrow \alpha^2 = 1 \Rightarrow (\alpha)$ is finite

Which is a contradiction to F^* is infinite.

If $1 + \alpha \neq 0$ then $1 + \alpha \in F^* = (\alpha)$

$\Rightarrow 1 + \alpha = \alpha^r$ where r is some positive or negative integer.

If r is positive then α satisfies the polynomial $x^r - x - 1$.

If r is negative, i.e., $r = -s, s > 0$.

Then $1 + \alpha = \alpha^{-s} \Rightarrow \alpha^s(1 + \alpha) = 1 \Rightarrow \alpha^{s+1} + \alpha^s = 1$.

$\Rightarrow \alpha$ satisfies the polynomial $x^{s+1} + x^s - 1$.

Thus, in both cases, either r is positive or negative, we have that the minimal polynomial of α over F_p is of finite degree.

$\Rightarrow [F:F_p] = [F_p(\alpha):F_p]$ = degree of minimal polynomial of α over F_p = finite.

$\Rightarrow [F:F_p]$ is finite.

$\Rightarrow F$ is a finite field.

$\Rightarrow F^*$ is finite, which is a contradiction to F^* is infinite.

So, either the characteristic of F is zero or F^* must be finite.

Case2: $charF = 0$.

Then we have $0 \neq 1 \in F$.

So, we have $-1 \in F^* = (\alpha)$.

$\Rightarrow \alpha^r = -1$ where r is some positive or negative integer.

$\Rightarrow \alpha^{2r} = 1$.

$\Rightarrow O(\alpha)$ is finite.

$\Rightarrow (\alpha)$ is finite.

$\Rightarrow F^*$ is finite, which is a contradiction to F^* is infinite.

So, our assumption that F^* is infinite is wrong.

$\Rightarrow F^*$ is finite.

$\Rightarrow F = F^* \cup \{0\}$ is finite.

Hence F is a finite field whenever F^* is cyclic.

3) If $f(x) \in F[x]$ is an irreducible polynomial over a finite field F, then all the roots of $f(x)$ are distinct.

Solution: Let F be a finite field with p^n elements.

Also let $f(x) \in F[x]$ be an irreducible polynomial over F.

To prove that all the roots of $f(x)$ are distinct.

If possible, suppose that $f(x)$ has multiple roots.

We know that $f(x)$ has multiple roots if and only if

$$f(x) = g(x^p) = \sum_{i=0}^{m} a_i (x^p)^i, a_i \in F \qquad (*)$$

Since $a_i \in F$, $a_i{}^{p^n} = a_i$ ($\because a_i$ satisfies the polynomial $x^{p^n} - x$ over F)

Set $a_i{}^{p^{n-1}} = b_i$ then $a_i{}^{p^n} = a_i$

$$\Rightarrow \left(a_i{}^{p^{n-1}}\right)^p = a_i$$

$$\Rightarrow b_i{}^p = a_i$$

Substituting $a_i = b_i{}^p$ in (*), we have

$$f(x) = g(x^p) = \sum_{i=0}^{m} b_i{}^p (x^p)^i = \sum_{i=0}^{m} \left(b_i x^i\right)^p = \left(\sum_{i=0}^{m} b_i x^i\right)^p$$

which is a contradiction, because $f(x)$ is irreducible.

Hence, $f(x)$ must have distinct roots.

4) The group of automorphisms of a field F with p^n elements is cyclic of order n and generated by ϕ, where $\phi(x) = x^p, x \in F$ (ϕ is called the frobenius endomorphism).

Solution: Let F be a finite field with p^n elements.

Also let $Aut(F)$ denote the group of automorphisms of F.

Define $\phi: F \to F$ as $\phi(\alpha) = \alpha^p \ \forall \ \alpha \in F$.

ϕ is a homomorphism: For any $\alpha, \beta \in F$,

$\phi(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \phi(\alpha) + \phi(\beta)$ $(\because charF = p)$

Similarly, $\phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p.\beta^p = \phi(\alpha).\phi(\beta)$

$\therefore \phi$ is a homomorphism.

ϕ is one-one: For every $\alpha, \beta \in F$,

$\phi(\alpha) = \phi(\beta) \Rightarrow \alpha^p = \beta^p \Rightarrow \alpha^p - \beta^p = 0$

$\Rightarrow (\alpha - \beta)^p = 0 (\because charF = p)$

$\Rightarrow \alpha - \beta = 0$

$\Rightarrow \alpha = \beta$

$\therefore \phi$ is one-one.

ϕ is onto: since $\phi: F \to F$, ϕ is one-one and F is finite, we have ϕ is onto.

Thus $\phi \in Aut(F)$.

Now consider $\phi^n(a) = \phi^{n-1}\big(\phi(a)\big)$

$= \phi^{n-1}(a^p)$

$= \phi^{n-2}\big(\phi(a^p)\big)$

$= \phi^{n-2}\big(a^{p^2}\big)$

$\vdots$

$= \phi^{n-n}(a^{p^n}) = a^{p^n} = a.$

$\Rightarrow \phi^n = I$

$\Rightarrow O(\phi) = n$

Now we will show that $|Aut(F)| = n$.

Note that as F is a finite field, the multiplicative group F^* of F is cyclic where $F^* = F\backslash\{0\}$.

Let $F^* = (\alpha)$ and we have $F = F_p(\alpha)$ where F_p is a subfield of F with p elements.

Let $f(x)$ be the minimal polynomial of α over F_p.

Then $\lambda: F_p \to F$ is an embedding and may be extended to an embedding $\lambda^*: F_p(\alpha) \to F$ (or) $\lambda^*: F \to F$ $(\because F_p(\alpha) = F)$.

Now since $F_p(\alpha) = F$ is a splitting field of $x^{p^n} - x$ over F_p, we have that $F_p(\alpha)$ is a normal extension of F_p.

Hence, the embedding $\lambda^*: F_p(\alpha) \to F$ that fixes F_p is an automorphism of F.

This will then give us all the automorphisms of F, because any automorphism of F keeps each element of F_p fixed.

Also, the number of such extensions of $\lambda \; to \; \lambda^*$ is equal to the number of distinct roots of the minimal polynomial.

Note that as $F = F_p(\alpha)$ and $|F| = p^n$, we have

$n = [F: F_p] = [F_p(\alpha): F_p] = degf(x)$ ($\because f(x)$ is the minimal polynomial of α over F_p).

$\Rightarrow$ The number of distinct roots of $f(x) = degf(x) = n$.

Now since $f(x)$ is an irreducible polynomial over the finite field F, $f(x)$ has all simple roots.

Hence, the number of extensions of $\lambda \; to \; \lambda^*$ is equal to n and each of these λ^* are automorphisms of F.

Thus, the order of the group $Aut(F)$ is n. i.e., $|Aut(F)| = n$.

In the beginning, we have showed that $\exists$ an element $\phi \in Aut(F)$ such that $O(\phi) = n$.

Hence, $Aut(F)$ is a cyclic group generated by ϕ.i.e., $Aut(F) = < \phi >$.

8.3 SUMMARY:

This lesson provided the basic idea of prime fields and some properties of finite fields. We have shown that the number of elements in a finite field is p^n where p is a prime number and n is a positive integer. A finite field (or Galois field) with p^n elements is denoted by $GF(p^n)$. It was proved that a finite field F with p^n elements is the splitting field of $x^{p^n} - x \in F_p[x]$ and hence any two finite fields with p^n elements are isomorphic. We have also established the existence of a finite field with p^n elements for any given prime p and any positive integer n. It was also verified that the multiplicative group of nonzero elements of a finite field is cyclic. Finite fields have useful applications in various fields like Cryptography, Coding theory and Computer networks, Digital signal processing, Random number Generation and Quantum computing etc. In particular, these are fundamental in the design and analysis of error-correcting codes, which are used to ensure reliable data transmission. They also play a crucial role in various cryptographic algorithms, including elliptic curve cryptography and RSA, due to their unique properties.

8.4 TECHNICAL TERMS:

Prime field: A field F is called a prime field if it has no proper subfield.

Notation: A finite field or Galois field with p^n elements is denoted by $GF(p^n)$.

Irreducible polynomial: A polynomial $f(x) \in F[x]$ is called irreducible if $degf(x) \geq 1$ and whenever $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x]$ then $g(x) \in F$ or $h(x) \in F$.

If a polynomial is not irreducible, it is called reducible.

Splitting field: Let F be any field and $f(x) \in F[x]$ be any polynomial of $degree \geq 1$.

Then an extension K of F is called a splitting field of $f(x)$ over F, if

i) $f(x)$ can be factorized into linear factors in $K[x]$. That is

$f(x) = a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n), \alpha_1, \alpha_2, \ldots, \alpha_n \in K$ and $a \in F$.

ii) $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, that is K is generated by F and the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $f(x)$ in K.

Minimal polynomial: The monic irreducible polynomial in $F[x]$ for which u will be a root is called the minimal polynomial of u over F.

Algebraic element: Let E be an extension of F. An element $\alpha \in E$ is called algebraic over F if there exists a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Algebraic extension: An extension E of a field F is called algebraic if each element of E is algebraic over F.

Normal extension: An extension E of a field F is called normal extension if E satisfies any one of the following equivalent conditions.

i) Every irreducible polynomial in $F[x]$ that has a root in E splits into linear factors in E.

$ii)$ E is the splitting field of a family of polynomial in $F[x]$.

iii) Every embedding σ of E into $\bar{F}$ that keeps each element of F fixed maps E onto E (or, σ may be regarded as an automorphism of E).

Simple and multiple roots: Let $f(x) \in F[x]$ be any polynomial over a field F and K be the splitting field of $f(x)$ over F. Let $\alpha \in K$ be a root of $f(x)$. Then $(x-\alpha)|f(x)$ in $K[x]$.

If $(x-\alpha)^s$ is the highest power of $(x-\alpha)$ that divides $f(x)$ then s is called the multiplicity of α. If $s = 1$, then s is called a simple root. If $s > 1$, then s is called a multiple root.

8.5 SELF- ASSESSMENT QUESTIONS:

1) If F is a finite field of characteristic p, show that each element a of F has a unique p[th] root, $\sqrt[p]{a}$ in F.

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

So, assume that $F = GF(p^n)$ for some $n \geq 1$.

Let $a \in F$.

If $a = 0$, then $a^p = 0$

If $a \neq 0$, then $a^p \neq 0$ since F is a field.

Since $F^* = F \setminus \{0\}$ is a multiplicative group with $p^n - 1$ elements, we have $a^{p^n-1} = 1$.

This implies $a^{p^n} = a$.

Let $b = a^{p^{n-1}}$

$\Rightarrow b^p = \left(a^{p^{n-1}}\right)^p = a^{p^n} = a$

$\Rightarrow b$ is a p[th] root of a in F.

Moreover, this b is unique p[th] root of a in F.

For, let $c \in F$ be any other element such that $c^p = a$.

Then $c = c^{p^n} = (c^p)^{p^{n-1}} = a^{p^{n-1}} = b$.

Thus b is the unique p[th] root $\sqrt[p]{a}$ in F.

Since, $a \in F$ was arbitrary, every element $a \in F$ has a unique p[th] root $\sqrt[p]{a}$ in F.

2) Show that $x^p - x - 1$ is irreducible over Z_p.

Ans: Let $f(x) = x^p - x - 1 \in Z_p[x]$

$\Rightarrow f'(x) = px^{p-1} - 1 = -1 \neq 0.$

So, the roots of $f(x)$ are distinct.

Let α be a root of $f(x)$ in the algebraic closure of Z_p.

Then $(\alpha + 1)$ is also a root of $f(x)$.

For, $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - 1 = \alpha^p + 1 - \alpha - 1 - 1 = \alpha^p - \alpha - 1 = 0.$

So, if α is a root of $f(x)$, then $(\alpha + 1)$ is also a root of $f(x)$.

Thus the p roots of $f(x)$ may be written as $\alpha,\ \alpha + 1,\ \alpha + 2,\ \ldots,\ \alpha + (p-1)$.

To prove that $f(x) = x^p - x - 1$ is irreducible over Z_p.

Let $\alpha \in Z_p$.

Then all the roots $\alpha,\ \alpha + 1,\ \alpha + 2,\ \ldots,\ \alpha + (p-1)$ lie in Z_p.

$\Rightarrow 0$ must be a root of $p(x)$ which is not true.

Thus $\alpha \notin Z_p$.

This shows that $Z_p(\alpha)\ (\neq Z_p)$ is a splitting field of f over Z_p and $[Z_p(\alpha): Z_p] = p$

Hence $f(x) = x^p - x - 1$ is irreducible over Z_p.

3) Find the generator for the multiplicative group of a field with 8 elements.

Ans: By theorem 8.2.7, the Galois field with 8 elements is the splitting field of $x^8 - x$ over $GF(2)$.

Let $F = GF(2^3)$. Then $|F| = 8$.

Clearly $F^* = F \setminus \{0\}$ is a multiplicative group of order 7 which is cyclic and is generated by any element $\alpha \neq 1$ (clearly $\alpha \neq 0$ since $\alpha \in F^* = F \setminus \{0\}$).

So, $\alpha \neq 1$ is a generator for the multiplicative group $F^* = F\setminus\{0\}$ of a field $F = GF(2^3)$ with 8 elements where $F = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$ with $1 + \alpha + \alpha^2 + \ldots + \alpha^6 = 0$ and $\alpha^8 = \alpha$.

4) Construct a field with 4 elements.

Ans: Consider the polynomial $f(x) = x^2 + x + 1 \in Z_2[x]$

Clearly $f(x)$ has no root in Z_2.

So, $f(x) = x^2 + x + 1$ is irreducible over Z_2.

Hence the required field is $F = \frac{Z_2[x]}{(x^2+x+1)}$

$$= \{a + b\alpha / a, b \in Z_2, \alpha^2 + \alpha + 1 = 0\}.$$

$= \{0, 1, \alpha, 1 + \alpha\}$ where $\alpha^2 = \alpha + 1$.

5) Define a prime field and give two examples.

Ans: (Refer Definition 8.2.1 and Examples 8.2.2).

6) Prove that the prime field of a field F is either isomorphic to Q or to Z_p where p is a prime.

Ans: (Refer theorem 8.2.4).

7) Prove that any finite field F with p^n elements is the splitting field of $x^{p^n} - x \in F_p[x]$

Ans: (Refer theorem 8.2.7).

8) Show that there exists a field with p^n elements for any prime p and positive integer n.

Ans: (Refer theorem 8.2.8).

9) Show that there exists an irreducible polynomial of any given degree n over F.

Ans: (Refer theorem 8.2.13).

10) Prove that the multiplicative group of non-zero elements of a finite field is cyclic.

Ans: (Refer theorem 8.2.11).

8.6 SUGGESTED READINGS:

1. P. B. Bhattacharya, S. K. Jain and S. R. Nag Paul, Basic Abstract Algebra, Second Edition, Cambridge University Press,1995.
2. I. N. Herstein, Topics in Algebra, Second Edition, John Wiley & sons, Inc,1975.
3. Thomas W. Hungerford, Algebra, Springer-Verlag, New York.

Dr. P. Vijaya Saradhi

LESSON- 9

SEPARABLE EXTENSIONS

OBJECTIVE:

- To know the concepts of separable extension and simple extension.
- To get the idea of a perfect field.
- To establish a necessary and sufficient condition for the finite extension to be a simple extension.

STRUCTURE:

9.1 INTRODUCTION:

The concept of separable extensions appeared indirectly during the time of Evariste Galois in 1830 while studying the roots of polynomial equations. At that time, the formal term "separable" was not introduced. Later Steinitz around 1910 formally introduced separable elements and separable extensions in the study of field theory. An interesting question in solving polynomial equations is when do polynomials will have distinct roots. A separable polynomial is one whose roots are all distinct (i.e., no repeated roots) in its splitting field. An extension E of a field F is a separable extension if every element of E is a root of a separable polynomial over F. In fields of characteristic zero (like $Q, \mathbb{R}, \mathbb{C}$) all extensions are separable. For example, $Q(\sqrt{2})$ is a separable extension of Q. Separable extensions are used in the real-world areas like Cryptography, Algebraic Geometry, Coding theory, Data Storage and Quantum Computing etc.

9.2 SEPARABLE EXTENSIONS:

9.2.1: Definition: An irreducible polynomial $f(x) \in F[x]$ is called a separable polynomial if all its roots are simple. Any polynomial $f(x) \in F[x]$ is called separable if all its irreducible factors are separable. A polynomial that is not separable is called inseparable.

9.2.2: Definition: Let E be an extension of a field F. An element $\alpha \in E$ that is algebraic over F is called separable over F if its minimal polynomial over F is separable.

9.2.3 Definition: An algebraic extension of a field F is called a separable extension if each element of E is separable over F.

9.2.4: Remarks:

1) Any polynomial over a field of characteristic zero is separable.

Proof: Let $f(x)$ be a polynomial over a field F of characteristic zero.

$\Rightarrow f(x) = f_1(x)f_2(x)\dots f_n(x)$ where each $f_i(x)$ is an irreducible polynomial over F.

If char $F = 0$, then any irreducible polynomial over F has simple roots.

$\Rightarrow$ Each $f_i(x)$ has simple roots.

$\Rightarrow$ Each $f_i(x)$ is a separable irreducible polynomial.

$\Rightarrow f(x)$ is a separable polynomial.

Hence any polynomial over a field of characteristic zero is separable.

2) If F is a field of characteristic zero then any algebraic extension of F is separable.

Proof: Let F be a field with char $F = 0$ and E be an algebraic extension of F.

$\Rightarrow$ Every element of E is algebraic over F.

Let $\alpha \in E$

$\Rightarrow \alpha$ is algebraic over F.

$\Rightarrow \exists$ a minimal polynomial $f(x) \in F[x]$ with α as a root.

$\Rightarrow f(x)$ is a separable polynomial.

$\Rightarrow \alpha$ is a separable element.

$\Rightarrow E$ is a separable extension of F.

Hence any algebraic extension of F is separable when char F = 0.

3) Any algebraic extension of a finite field is separable.

Proof: Let E be an algebraic extension of a finite field F and let $\alpha \in E$.

$\Rightarrow \alpha$ is algebraic over F.

$\Rightarrow \exists$ a minimal polynomial $f(x) \in F[x]$ with α as a root.

We know that all the roots of an irreducible polynomial over a finite field are distinct.

$\Rightarrow$ All the roots of $f(x)$ are simple.

$\Rightarrow f(x)$ is a separable polynomial.

$\Rightarrow \alpha \in E$ is a separable.

Hence E is a separable extension.

Thus, any algebraic extension of a finite field is separable.

9.2.5: Example: If $K = F[x]$ is the field of rational functions over a field F of characteristic 3, then the polynomial $y^3 - x \in K[y]$ is irreducible over K. Also $y^3 - x$ has all its roots equal, each being α, say. Hence $K[\alpha]$ is not a separable extension of K.

9.2.6: Definition: A field F is called perfect if each of its algebraic extensions is separable.

9.2.7: Example: $F = Q$ is a perfect field.

For, if E is any algebraic extension of Q, then for every $\alpha \in E$, α is separable over Q.

$\Rightarrow E$ is a separable extension of Q for every algebraic extension E of Q.

Hence Q is perfect.

9.2.8: Note: Any field of characteristic zero is perfect and any finite field is also perfect.

9.2.9: Definition: An extension E of a field F is called a simple extension if $E = F(\alpha)$ for some $\alpha \in E$.

9.2.10: Note: Any finite extension of a finite field is a simple extension.

i.e., if F is a finite field and E be any finite extension of F then $E = F(\alpha)$ for some $\alpha \in E$.

9.2.11: Theorem: If E is a finite separable extension of field F then E is a simple extension of F.

Proof: Let F be a finite field and E be a finite separable extension of F.

First note that if F is a finite field then any finite extension E of F is simple.

So, consider the case when F is infinite.

Now as E is a finite extension, we have $E = F(a_1, a_2, a_3, \ldots, a_n)$ where $a_i \in E$ are algebraic over F, for each $i = 1, 2, \ldots, n$.

Now we prove the result for $n = 2$ and then the result will follow by induction.

So, let $E = F(\alpha, \beta)$ where $\alpha, \beta \in E$.

Let $p(x)$ and $q(x)$ be the minimal polynomials for α and β, respectively, over F.

Let the roots of $p(x)$ be $\alpha_1, \alpha_2, \ldots, \alpha_n$ and the roots of $q(x)$ be $\beta_1, \beta_2, \ldots, \beta_m$.

Since E is a separable extension of F, all the roots of $p(x)$ and $q(x)$ are distinct.

$\Rightarrow \alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct and $\beta_1, \beta_2, \ldots, \beta_m$ are distinct.

Since F is infinite, $\exists a \in F$ such that $a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$ $for\ 1 \leq i \leq n\ and\ 2 \leq j \leq m.$

$\Rightarrow a(\beta - \beta_j) \neq \alpha_i - \alpha$ for $i = 1,2,\ldots,n$ and $j = 2,3,\ldots,m$.

$\Rightarrow \alpha + a\beta \neq \alpha_i + a\beta_j$ for $i = 1,2,\ldots,n$ and $j = 2,3,\ldots,m$.

Now $set\ \theta = \alpha + a\beta$ and $\theta \neq \alpha_i + a\beta_j$.

$\Rightarrow \theta - a\beta_j \neq \alpha_i$ for $i = 1,2,\ldots,n$ and $j = 2,3,\ldots,m$.

Now we prove that $F(\alpha, \beta) = F(\theta)$.

For this we define $h(x) = p(\theta - ax) \in F(\theta)[x]$.

Then $h(\beta) = p(\theta - a\beta) = p(\alpha) = 0 \Rightarrow \beta$ is a root of $h(x)$.

Consider $h(\beta_j) = p(\theta - a\beta_j) \neq 0$ for $j \neq 1$ and $j = 2,3,\ldots,m$.

Hence β is a root of $h(x)$ and no $\beta_j (j \neq 1)$ is a root of $h(x)$.

Also, we have $h(x) \in F(\theta)[x]$ and $q(x) \in F[x] \subseteq F(\theta)[x]$ with β as the common root.

Let $A(x) \in F(\theta)[x]$ be the minimal polynomial of β over $F(\theta)$ then $A(x)|h(x)$ and $A(x)|q(x)$.

Thus, any root of $A(x)$ is a root of $h(x)$ as well as a root of $q(x)$.

But the only common root of $q(x)$ and $h(x)$ is β.

Therefore, $A(x) = x - \beta \in F(\theta)[x]$

$\Rightarrow \beta \in F(\theta)$

$\Rightarrow -a\beta \in F(\theta)$ and $\theta \in F(\theta)$

$\Rightarrow -a\beta \in F(\theta)$ and $\alpha + a\beta \in F(\theta)$

$\Rightarrow \alpha \in F(\theta)$ and $\beta \in F(\theta)$

$\Rightarrow F(\alpha, \beta) \subseteq F(\theta)$

By definition of θ, we have $F(\theta) = F(\alpha + a\beta) \subseteq F(\alpha, \beta)$.

Therefore, $F(\alpha, \beta) = F(\theta)$.

By the above argument, we have proved the result for $n = 2$.

i.e., if $E = F(a_1, a_2)$ then $E = F(\alpha)$ for some $\alpha \in E$.

Thus, by induction, we have that if $E = F(a_1, a_2, \ldots, a_n)$ then $E = F(\alpha)$ for some $\alpha \in E$.

Hence, E is a simple extension of F.

9.2.12: Theorem: Let E be a finite extension of a field F, then the following are equivalent.

$i)$ $E = F(\alpha)$ for some $\alpha \in E$.

ii) There are only a finite number of intermediate fields between F and E.

Proof: Let E be a finite extension of a field F.

(i) $\Rightarrow$ (ii) : Assume (i). i.e., $E = F(\alpha)$ for some $\alpha \in E$.

$\Rightarrow$ E is a finite extension of F.

$\Rightarrow \alpha \in E$ is algebra over F.

$\Rightarrow$ $\exists$ a minimal polynomial $f(x) \in F[x]$ of α over F with α as a root (i.e., $f(\alpha) = 0$).

Now let K be the subfield of E containing F.

i.e., K is the intermediate field between F and E.

Let $g(x)$ be the minimal polynomial of α over K.

Then since $g(x) \in K[x]$ and $f(\alpha) = 0$, $g(x)|f(x)$.

Let K' be the subfield of K containing F and the coefficients of the polynomial $g(x)$ then $g(x) \in K'[x]$, being irreducible over K, is also reducible over K'.

$\Rightarrow g(x)$ is the minimal polynomial of α over K'.

Since $E = F(\alpha)$, we get $E = K(\alpha) = K'(\alpha)$.

Consider $[E:K] = [K(\alpha):K] = \deg\ g(x)$

Also $[E:K'] = [K'(\alpha):K'] = \deg\ g(x)$

$\Rightarrow [E:K] = [E:K']$

$\Rightarrow K = K'$

Now let $I = \{K:K$ is a subfield of E containing F i.e., $F \subseteq K \subseteq E\}$.

That is, I is the set of all intermediate fields between F and E.

Also let D be the set of all divisors of $f(x) \in F[x]$. i.e., $D = \{g(x) \in E[x]: g(x)|f(x)\}$.

Because there are only finitely many divisors of $f(x)$, the set D is finite. i.e., $|D|$ is finite.

Define a mapping $\sigma: I \to D$ by $\sigma(K) = g(x)$, the minimal polynomial of α over K in D.

Then by the above argument σ is one-one. i.e., $\forall K_1, K_2 \in I$, $\sigma(K_1) = \sigma(K_2) \Rightarrow K_1 = K_2$

Now since $\sigma: I \to D$ is one-one, we have $|I| \leq |D|$ and hence $|I|$ is finite as $|D|$ is finite.

Hence there are only a finite number of intermediate fields between F and E when $E = F(\alpha)$.

Thus $(i) \Rightarrow (ii)$. (1)

$(ii) \Rightarrow (i)$: Assume that there are only a finite number of intermediate fields between F and E.

Then as E is a finite extension of F, $E = F(\alpha)$ for some $\alpha \in E$ by note 9.2.10.

So, assume that F is infinite.

We first prove that for any 2 elements $\alpha, \beta \in E$ there exists $r \in E$ such that $F(\alpha, \beta) = F(r)$.

For each $a \in F$, define $r_a = \alpha + a\beta$.

Then for each of these r_a, the fields $F(r_a)$ are the intermediate fields between F and E. i.e., $F \subseteq F(r_a) \subseteq E$.

Now as F is infinite, we have infinitely many such $F(r_a)$.

Because there are only a finite number of intermediate fields between F and E(by hypothesis), so all the fields $F(r_a)$ need not be distinct.

$\Rightarrow \exists\, a, b \in F \ni a \neq b\ F(r_a) = F(r_b)$

$\Rightarrow r_a, r_b \in F(r_b)$

$\Rightarrow r_a - r_b \in F(r_b)$

$\Rightarrow (a - b)\beta \in F(r_b)$

$\Rightarrow \beta \in F(r_b)$

Thus, $r_b = \alpha + b\beta \in F(r_b) \Rightarrow \alpha \in F(r_b)$

$$\Rightarrow F(\alpha, \beta) \subseteq F(r_b)$$

By definition of r_b, $F(r_b) \subseteq F(\alpha, \beta)$

Therefore, $F(\alpha, \beta) = F(r_b)$ and hence our assertion is proved.

We now choose $u \in E$ such that $[F(u) : F]$ is as large as possible.

Then we claim that $E = F(u)$.

Otherwise, let $x \in E$ but $x \notin F(u)$.

Then we can find an element $t \in E$ such that $F(t)$ contains both u and x with $F(t) \supsetneq F(u)$.

This contradicts the choice of u.

Hence $E = F(u)$.

Therefore, $(ii) \Rightarrow (i)$. (2)

Thus from (1) and (2), the conditions (i) and (ii) in the theorem are equivalent.

9.2.13: Examples:

1) Let E be an extension of a field F and let $\alpha \in E$ be algebraic over F. Then α is separable over F if and only if $F(\alpha)$ is a separable extension of F.

Solution: Let E be an extension of F and $\alpha \in E$ be algebraic over F.

Assume that $F(\alpha)$ is a separable extension of F.

Then as $\alpha \in F(\alpha)$, we have α is separable over F.

Conversely, suppose that α is separable over F.

To show that $F(\alpha)$ is a separable extension of F.

i.e., to show that $\forall\ \beta \in F(\alpha)$, β is separable over F.

Now let $\beta \in F(\alpha)$

We show that β is separable over F.

We have $F \subseteq F(\beta) \subseteq F(\alpha)$.

Let $p_1(x)$ be the minimal polynomial of β over F that has m distinct roots.

Let L be an algebraically closed field and $\sigma: F \to L$ be an embedding

Note that σ can be extended from F to $F(\beta)$ and no. of such extensions of σ to $F(\beta) = m$, the no. of distinct roots of $p_1(x)$ over F.

So, there are m distinct extensions, say $\sigma_1, \sigma_2, \ldots, \sigma_m$ of σ to $F(\beta)$.

Now α is algebraic over $F(\alpha)$ and hence α is algebraic over $F(\beta)$.

$\Rightarrow \exists$ a minimal polynomial $p_2(x)$ of α over $F(\beta)$ such that $[F(\alpha): F(\beta)] = \deg\ p_2(x)$.

Suppose $p_2(x)$ has n distinct roots i.e., $\deg\ p_2(x) = n$.

Then by the same argument as above, each $\sigma_i (i = 1\ to\ m)$ has exactly n extensions $\sigma_{ij}, 1 \leq j \leq n$ to $F(\alpha)$.

So clearly, the set of mn embeddings $(\sigma_{ij}), 1 \leq i \leq m, 1 \leq j \leq n$ are the only possible embeddings from $F(\alpha)$ to L that extend $\sigma: F \to L$.

Now since α is algebraic over F, $\exists$ a minimal polynomial $p_3(x)$ of α over F such that

$[F(\alpha): F] = degp_3(x)$ = no. of distinct roots of $p_3(x)$ = no. of extensions of σ to $F(\alpha)$.$= mn$.

$\Rightarrow mn = [F(\alpha): F] = [F(\alpha): F(\beta)][F(\beta): F] = degp_2(x).degp_1(x) = n.degp_1(x)$.

$\Rightarrow m = degp_1(x)$= no. of distinct roots of $p_1(x)$.

Thus $p_1(x)$ is a separable polynomial.

Hence, β is separable over F.

$\Rightarrow \beta$ is separable over $F\ \ \forall\ \beta \in F(\alpha)$.

$\Rightarrow F(\alpha)$ is a separable extension of F.

2) If K is a field of characteristic $p \neq 0$, then K is perfect if and only if $K^p = K$ (i.e., if and only if every element of K has pth root in K).

Solution: Let K be a field of characteristic $p \neq 0$.

Assume that K is perfect.

$\Rightarrow$ Every algebraic extension of K is a separable extension of K.

To prove that $K^p = K$.

It is enough to prove that $\forall\ a \in K,\ \ \exists\ b \in K$, such that $a = b^p$.

Let $a \in K$ and consider $f(x) = x^p - a \in K[x]$.

Let b be a root of $f(x)$ in some extension field K' of K.

Then $b \in K'$ and $b^p - a = 0$ i.e., $b \in K'$ and $a = b^p$.

Since b is a root of $f(x) = x^p - a \in K[x]$, $p(x)$ is a factor of $f(x)$ in $K[x]$. i.e., $p(x)|f(x)$.

In $K[x]$, we have $f(x) = x^p - a = x^p - b^p = (x-b)^p$ $(\because char\ K = p)$

$\Rightarrow p(x)|(x-b)^p$ and hence $p(x) = (x-b)^r$.

Since $K' = K(b)$, K' is an algebraic extension of K.

$\Rightarrow K'$ is a separable extension of K and $b \in K'$.

$\Rightarrow b$ is a separable element over K in K'.

$\Rightarrow p(x)$ has no multiple roots.

$\Rightarrow r = 1$ and $p(x) = x - b$.

Since $p(x) \in K[x]$, it follows that $b \in K$.

So, $\exists$ an element $b \in K$ such that $a = b^p$.

Thus $\forall\ a \in K,\ \exists\ b \in K$ such that $a = b^p$.

Hence $K^p = K$.

Conversely, suppose that $K^p = K$.

To prove that K is perfect.

Let E be an algebraic extension of K and $\alpha \in E$

$\Rightarrow \alpha$ is algebraic over K.

$\Rightarrow \exists$ a minimal polynomial $f(x)$ of α over K

It is enough to prove that all the roots of $f(x)$ are simple.

Suppose $f(x)$ has a multiple root.

$\Rightarrow f(x) = g(x^p)$ for some polynomial $g(x) \in K[x]$, i.e., $f(x) = \sum_{i=0}^{n} a_i (x^p)^i, a_i \in K$.

From hypothesis, for all $a_i \in K \ \exists \ b_i \in K$ such that $a_i = {b_i}^p$

$\Rightarrow f(x) = \sum_{i=0}^{n} {b_i}^p (x^p)^i = \sum_{i=0}^{n} {b_i}^p (x^i)^p = \sum_{i=0}^{n} \left(b_i x^i\right)^p = \left(\sum_{i=0}^{n} b_i x^i\right)^p (\because charK = p)$

$\Rightarrow f(x)$ is reducible, a contradiction to the minimality of $f(x)$.

Thus, all the roots of $f(x)$ are simple.

$\Rightarrow \alpha$ is a separable element over K for all $\alpha \in E$.

$\Rightarrow E$ is a separable extension of K.

Hence, K is perfect.

3) Let $F \subset E \subset K$ be three fields such that E is a finite separable extension of F, and K is a finite separable extension of E. Then K is a finite separable extension of F.

Solution: Let $F \subset E \subset K$ be three fields such that E is a finite separable extension of F, and K is a finite separable extension of E.

$\Rightarrow$ K is a finite extension of F.

To prove that K is a finite separable extension of F.

Now since E is a finite separable extension of F, $\exists \ \alpha \in E$ such that $E = F(\alpha)$.

Similarly, since K is a finite separable extension of E, $\exists \ \beta \in K$ such that $K = E(\beta)$.

$\Rightarrow \mathrm{K} = F(\alpha)(\beta) = F(\alpha, \beta)$.

Let $r \in F(\alpha, \beta) = K$ but $r \notin F(\alpha)$.

We prove that r is separable over F.

Let $p_1(x)$ = the minimal polynomial of α over F with degree m.

$p_2(x)$ = the minimal polynomial of r over $F(\alpha)$ with degree n.

$p_3(x)$ = the minimal polynomial of r over F with degree s.

$p_4(x)$ = the minimal polynomial of α over $F(r)$ with degree t.

Let $\sigma: F \to L$ be an embedding of F into an algebraically closed field L.

Because α is separable over F there are exactly m extensions (α_i), $1 \leq i \leq m$ of σ to $F(\alpha)$.

i.e., $[F(\alpha): F] = deg\ p_1(x) = m$.

Also, since r is separable over $F(\alpha)$, there are exactly n extensions of each σ_i to $F(\alpha, r)$.

i.e., $[F(\alpha, r): F(\alpha)] = deg\ p_2(x) = n$.

Let us call these extensions as $\sigma_{i1}, \sigma_{i2}, \ldots, \sigma_{in}$ where $1 \leq i \leq m$.

Thus, there are precisely mn extensions of $\sigma: F \to L$ to $\sigma_{ij}: F(\alpha, r) \to L$ Where $1 \leq i \leq m$, $1 \leq j \leq n$ (these are via $F(\alpha)$). i.e., $[F(\alpha, r): F] = [F(\alpha, r): F(\alpha)][F(\alpha): F] = mn$------ (1)

Now by considering extensions $\sigma: F \to L$ to $F(\alpha, r)$ via $F(r)$ we obtain similarly that there are precisely st extensions to $F(\alpha, r)$. i.e., $[F(\alpha, r): F] = [F(\alpha, r): F(r)][F(r): F] = st$ --- (2)

From (1) and (2), $mn = st$.

Suppose r is not separable over F.

Then the no. of elements of σ to $F(r)$ is $< s$

$\Rightarrow$ the no. of extensions of σ to $F(\alpha, r)$ is $< st = mn$, a contradiction.

Thus r is separable over F.

Hence K is a finite separable extension of F.

9.3 SUMMARY:

This lesson gives the basic idea of a separable polynomial over a field F and hence the concept of a separable extension of a given field F. It was shown that any algebraic extension of a finite field is separable. The concept of a perfect field and a simple extension of a field F are also given. It was also understood that perfect fields are fields of characteristic zero and finite fields. We have also remarked that infinite fields of characteristic $p > 0$have inseparable extensions and hence such fields are not perfect in general. A necessary and sufficient condition was also provided for a finite extension to be a simple extension. Some examples of separable and non-separable extensions are also given for better understanding of the reader. Even though field extensions and separability sound abstract, separable extensions matter a lot in the real-world areas like Cryptography, Error-Correcting Codes, Algebraic Geometry, Robotics, Coding Theory, Data Storage and Quantum computing etc. In

particular separable extensions are used in the construction of error correcting codes which are essential for reliable data transmission and storage. They also play a role in the development of secure communication protocols and algorithms ensuring confidentiality and integrity of data.

9.4 TECHNICAL TERMS:

Irreducible polynomial: A polynomial $f(x) \in F[x]$ is called irreducible if $degf(x) \geq 1$ and whenever $f(x) = g(x)h(x)$, where $g(x),\ h(x) \in F[x]$ then $g(x) \in F$ or $h(x) \in F$. If a polynomial is not irreducible, it is called reducible.

Minimal polynomial: The monic irreducible polynomial in $F[x]$ for which u will be a root is called the minimal polynomial of u over F.

Algebraic element: Let E be an extension of a field F. An element $\alpha \in E$ is called algebraic over F if there exists a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Algebraic Extension: An extension E of a field F is called algebraic if each element of E is algebraic over F.

Separable polynomial: An irreducible polynomial $f(x) \in F[x]$ is called a separable polynomial if all its roots are simple. Any polynomial $f(x) \in F[x]$ is called separable if all its irreducible factors are separable. A polynomial that is not separable is called inseparable.

Separable element: Let E be an extension of a field F. An element $\alpha \in E$ that is algebraic over F is called separable over F if its minimal polynomial over F is separable.

Separable Extension: An algebraic extension of a field F is called a separable extension if each element of E is separable over F.

Perfect field: A field F is called perfect if each of its algebraic extensions is separable.

Simple Extension: An extension E of a field F is called a simple extension if $E = F(\alpha)$ for some $\alpha \in E$.

Algebraically closed field: A field K is algebraically closed if it possesses no algebraic extensions. That is if every algebraic extension of K coincides with K.

9.5 SELF -ASSESSMENT QUESTIONS:

1) Prove that $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.

Ans: clearly $Q(\sqrt{2} + \sqrt{3}) \subset Q(\sqrt{2}, \sqrt{3})$. (1)

So, it is enough to show that $Q(\sqrt{2}, \sqrt{3}) \subset Q(\sqrt{2} + \sqrt{3})$.

Consider $\sqrt{3} + \sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$.

$\Rightarrow \sqrt{3}-\sqrt{2}=\frac{1}{\sqrt{3}+\sqrt{2}} \in Q(\sqrt{2}+\sqrt{3})$.

So $\sqrt{3}+\sqrt{2}, \sqrt{3}-\sqrt{2} \in Q(\sqrt{2}+\sqrt{3})$.

$\Rightarrow (\sqrt{3}+\sqrt{2})+(\sqrt{3}-\sqrt{2}) \in Q(\sqrt{2}+\sqrt{3})$ and $(\sqrt{3}+\sqrt{2})-(\sqrt{3}+\sqrt{2}) \in Q(\sqrt{2}+\sqrt{3})$.

$\Rightarrow 2\sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$ and $2\sqrt{2} \in Q(\sqrt{2}+\sqrt{3})$.

$\Rightarrow \sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$ and $\sqrt{2} \in Q(\sqrt{2}+\sqrt{3})$ and hence $Q(\sqrt{2},\sqrt{3}) \subset Q(\sqrt{2}+\sqrt{3})$. (2)

From (1) and (2), $Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$.

2)Prove that every extension of Q is separable.

Ans: We know that Q is a field of characteristic zero and every irreducible polynomial over a field of characteristic zero is separable.

Let E be any extension of Q.

To prove that E is separable.

Let $\alpha \in E$

Then α has a minimal polynomial $p(x)$ over Q.

Since Q has characteristic zero, every irreducible polynomial, including the minimal polynomial $p(x)$ of α is separable.

Because the minimal polynomial of every element in E is separable, every element in E is separable over Q.

Therefore, every extension of Q is a separable extension.

3)Define perfect field and give an example

Ans: (Refer Definition 9.2.6 and Example 9.2.7)

4)Give an example of a non-separable extension of a field.

Ans: (Refer Example 9.2.5)

5)If E is a finite separable extension of a field F, show that E is a simple extension of F.

Ans: (Refer Theorem 9.2.11)

6)Define (i) Separable Extension (ii) Simple Extension

Ans: (Refer Definition 9.2.3 and Definition 9.2.9)

7)Prove that a finite extension of a finite field is separable

Ans: Let F be a finite field and E be the finite extension of F

$\Rightarrow E$ is an algebraic extension of F.

To show that E is a separable extension of F.

Let $\alpha \in E$ and $f(x)$ be the minimal polynomial of α over F.

Then $f(x)$ is irreducible over F.

We know that every irreducible polynomial over a finite field has all its roots distinct.

Since, F is a finite field, all the roots of $f(x)$ are simple.

Thus $f(x)$ is separable and hence α is separable over F.

8)Let α be a root of $x^p - x - 1$ over a field F of characteristic p. Then show that $F(\alpha)$ is a separable extension of F.

Ans: Let $f(x) = x^p - x - 1 \in F[x]$ and let α be a root of $f(x)$.

To show that that $F(\alpha)$ is a separable extension of F.

For this, it is enough to show that α is separable over F.

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

Then $p(x)|f(x) = x^p - x - 1 \in F[x]$.

Now to show that $p(x)$is separable, it is enough to show that $f(x) = x^p - x - 1$ does not have multiple roots.

Let β be a root of $f(x)$ with multiplicity m_β then $1 \leq m_\beta \leq$ p.

If $m_\beta = p$ then $f(x) = x^p - x - 1 = (x - \beta)^p = x^p - \beta^p$ which gives a contradiction.

Hence m_β < p.

Then by known result, m_β = the smallest number k such that $f^{(K)}(\beta) \neq 0$.

But note that $f'(x) = px^{p-1} - 1 = -1 \neq 0$.

Therefore, k = 1 = m_β.

Hence every root of $f(x)$ is simple as required.

So, $p(x)$is a separable polynomial.

Thus, α is separable over F.

Hence F(α) is a separable extension of F.

9.6 SUGGESTED READINGS:

1. P. B. Bhattacharya, S. K. Jain and S. R. Nag Paul, Basic Abstract Algebra, Second Edition, Cambridge University Press,1995.
2. I. N. Herstein, Topics in Algebra, Second Edition, John Wiley & sons, Inc,1975.
3. Thomas W. Hungerford, Algebra, Springer-Verlag, New York.

- **Dr. P. Vijaya Saradhi**

LESSON- 10

AUTOMORPHISM GROUPS AND FIXED FIELDS

OBJECTIVES:

- To define the fixed field of a group of automorphism of a field.
- To introduce the group $G(\mathrm{E/F})$
- To compare $O\big(G(\mathrm{E/F})\big)$ and $[E:F]$ under certain conditions
- To introduce Dedekind Lemma
- To obtain necessary and sufficient conditions under which $O\big(G(\mathrm{E/F})\big) = [E:F]$ where E is a finite separable extension of F.

STRUCTURE:

10.1 INTRODUCTION:

In this lesson some basic results of Galois theory are presented. These results are used in proving the fundamental theorem of Galois theory. The results of this section and the fundamental theorem of Galois theory are used to give a simple algebraic proof for the fundamental theorem of algebra.

10.2 AUTOMORPHISM GROUPS AND FIXED FIELDS:

10.2.1 Definition: Let F be a filed and E be an extension field of F. Then the set of automorphisms of E each of which fixes each element of F, is denoted by $G(\mathrm{E/F})$ that is $G(\mathrm{E/F}) = \{T \,/\, T$ is an automorphism of E and $T(\alpha) = \alpha$ for all $\alpha \in F\}$. Here each element of $G(\mathrm{E/F})$ is also called an F-automorphism of E.

10.2.2 Result: $G(\mathrm{E/F})$ is a group under composition of mappings, where E is an extension of the field F.

Proof: Let $T_1,\ T_2 \in G(\mathrm{E/F})$

(i) $T_1 o T_2 \in G(\mathrm{E/F})$

(ii) $(T_1 o T_2) o T_3 = T_1 o (T_2 o T_3)$

(iii) $I \in G(\mathrm{E/F})$ and $T_1 o I = T_1 = I o T_1$, I is the identity automorphism of E.

(iv) Given $T \in G(\mathrm{E/F})$ there is a $S \in G(\mathrm{E/F})$ such that $ST = TS = I_E;\ T^{-1} = S$

To prove (iv)

Let $T \in G(\mathrm{E/F})$.

$\Rightarrow$T is an automorphism of E.

$\Rightarrow$T is one-to-one and onto E.

Therefore, T has inverse mapping $T^{-1}: E \to E$ which is also a bijection of E onto E where $T^{-1}(v) = u$ if and only if $T(u) = v$.

Let $a,\ b \in E$. Then we get $c,\ d \in E$ such that $T(c) = a$ and $T(d) = b$

Now $a + b = T(c) + T(d) = T(c + d)$

So $T^{-1}(a + b) = c + d = T^{-1}(a) + T^{-1}(b)$

Also we have $ab = T(c).T(d) = T(cd)$. So $T^{-1}(ab) = cd = T^{-1}(a)T^{-1}(b)$

Therefore T^{-1} is a homomorphism of E onto E.

That is, T^{-1} is an automorphism of E.

Let $u \in E$ and $T(u) = v$

$(ToT^{-1})v = T\big(T^{-1}(v)\big) = T(u) = v = I(u) \quad \forall\ u \in E$

So, $T^{-1}oT = I$. Similarly $ToT^{-1} = I$.

Therefore, $T^{-1} \in G(\mathrm{E/F})$ is the inverse of T.

Hence $G(\mathrm{E/F})$ is a group under composition of mappings.

10.2.3 Definition: If F is a field and E is an extension field of F, then $G(\mathrm{E/F})$ is called the group of F-automorphism of E.

10.2.4 Theorem: Let E be a finite simple extension of the field F. Then $O\big(G(\mathrm{E/F})\big) \leq [E:F]$

Proof: Let E be a finite simple (separable) extension of the field F.

Since E is a simple extension of F we have $E = F(u)$ for some $u \in E$

Let $P(x)$ be the minimal polynomial of u over F and $\deg\ p(x) = n$

Now $[E:F] = [F(u):F] = \deg\ p(x) = n$.

Let k be the number of distinct roots of $p(x)$. Let $\sigma: F \to \bar{E}$ be the identity map of $F[\sigma(\alpha) = \alpha \quad \forall \quad \alpha \in F]$

σ can be extended to exactly k embeddings of E into $\bar{E}$ namely $\sigma_1, \sigma_2, \ldots, \sigma_K$.

Note that each element of $G(\mathrm{E/F})$ is an extension of σ from E into $\bar{E}$. So

therefore $O\big(G(\mathrm{E/F})\big) \leq k \leq n = [E:F]$.

Hence the Result.

10.2.5 Example: We find the automorphism group $G(\mathbb{C}/\mathbb{R})$

Let $T \in G(\mathbb{C}/\mathbb{R})$.

Let $c \in \mathbb{C}$

Now $c = a + ib \quad a,\ b \in \mathbb{R}$

Now $T(c) = T(a + ib) = T(a) + T(i)T(b) = a + T(i)b$

$(T(i))^2 = T(i)T(i) = T(i^2) = T(-1) = -1$

So $T(i) = i$ or $-i$

$T_1(a + ib) = a + ib \ \forall \ \ a + ib \in \mathbb{C}$ is identity automorphism

$T_2(a + ib) = a + (-i)b \ \ \forall \ a + ib \in \mathbb{C}$ is also an automorphism

Therefore $G(\mathbb{C}/\mathbb{R}) = \{(I = T_1),\ T_2\}$

Since $f(x) = x^2 + 1 \in R[x]$ is an irreducible polynomial over $\mathbb{R}$ and i is a root of $f(x)$, $[R(i): R] = 2$ that is $[\mathbb{C}: R] = 2$. So $O(G(\mathbb{C}/\mathbb{R})) = [\mathbb{C}: R] = 2$.

10.2.6 Example: Let Q be the field of rational numbers

Consider the field of $Q\left(2^{1/3}\right)$. We have that

$g(x) = x^3 - 2 \in Q[x]$ is irreducible over Q and

$2^{1/3}$ is a root of $g(x)$. So $\left[Q\left(2^{1/3}\right): Q\right] = 3$

The roots of $g(x) = x^3 - 2$ are $2^{1/3},\ 2^{1/3}\omega,\ 2^{1/3}\omega^2$, where ω is a primitive 3rd root of unity.

Let $a \in Q\left(2^{1/3}\right)$. Now $a = \alpha_0 + \alpha_1 2^{1/3} + \alpha_2\left(2^{1/3}\right)^2$

Let $T \in G\left(Q\left(2^{1/3}\right) / Q\right)$

Now $T(a) = T\left[\alpha_0 + \alpha_1 2^{1/3} + \alpha_2\left(2^{1/3}\right)^2\right]$

$= T(\alpha_0) + T(\alpha_1)2^{1/3} + T(\alpha_2)T\left(2^{1/3}\right)^2$

$= \alpha_0 + \alpha_1 T(2^{1/3}) + \alpha_2 T\left(2^{1/3}\right)^2$

$T\left(2^{1/3}\right)^3 = T(2) = 2$

So $T\left(2^{1/3}\right) = 2^{1/3}\ (or)\ 2^{1/3}\omega \ \ (or)\ \ 2^{1/3}\omega^2$

Since $2^{1/3}\omega,\ 2^{1/3}\omega^2 \notin Q\left(2^{1/3}\right)$, we have $T\left(2^{1/3}\right) = 2^{1/3}$

Therefore $T = I$, that is, $G\left(Q\left(2^{1/3}\right) / Q\right) = \{I\}$.

So $O\left(G\left(Q\left(2^{1/3}\right)/Q\right)\right) = 1 < 3 = \left[Q\left(2^{1/3}\right): Q\right]$.

10.2.7 Definition: Let E be a field and H be a subgroup of the group of automorphisms of E. Then $E_H := \{a \in E \,/\, h(a) = a \text{ for all } h \in H\}$ is called the fixed field of H in E.

Note: Note that E_H is always a subfield of E.

10.2.8 Lemma: (Dedekind lemma)

Let E and F be fields, and $\sigma_1, \sigma_2, \ldots, \sigma_n$ be distinct embeddings of F into E.

If $a_1,\ a_2,\ \ldots,\ a_n \in E$ and $a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0 \quad \forall \quad x \in F$, then $0 = a_1 = a_2 = \cdots = a_n$.

Proof: Given that E and F are fields and $\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_n$ are distinct embeddings of F into E.

We prove that if $a_1,\ a_2,\ \ldots,\ a_n \in E$ and

$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0$ for all $x \in F$ then

$0 = a_1 = a_2 = \cdots = a_n$.

Suppose we have $a_1,\ a_2,\ \ldots,\ a_n \in E$ not all zero such that

$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0$ for all $x \in F$. Among all such equations we choose an equation having least number of non-zero terms, namely

$b_1\sigma_1(x) + b_2\sigma_2(x) + \ldots + b_k\sigma_k(x) = 0$ for all $x \in F$

and no $b_1,\ b_2,\ \ldots,\ b_k$ is 0. (1)

We have $\sigma_1 \neq \sigma_k$. So we get $y \in F$ such that $\sigma_1(y) \neq \sigma_k(y)$. Since $y \in F \ \forall \ x \in F$,

$b_1\sigma_1(xy) + b_2\sigma_2(xy) + \ldots + b_k\sigma_k(xy) = 0$ and that

$b_1\sigma_1(x)\sigma_1(y) + b_2\sigma_2(x)\sigma_2(y) + \ldots + b_k\sigma_k(x)\sigma_k(y) = 0$ (2)

(1) x $\sigma_1(y)$ gives $b_1\sigma_1(x)\sigma_1(y) + b_2\sigma_2(x)\sigma_1(y) + \ldots + b_k\sigma_k(x)\sigma_1(y) = 0 \quad \forall\, x \in F$ (3)

(3) - (2) gives $b_2\sigma_2(x)[\sigma_1(y) - \sigma_2(y)] + \ldots + b_k\sigma_k(x)[\sigma_1(y) - \sigma_k(y)] = 0 \quad \forall\, x \in F$ (4)

(4) is an equation with fewer terms than k as $b_k[\sigma_1(y) - \sigma_k(y)] \neq 0$

This is a contradiction to our assumption.

This establishes the lemma.

10.2.9 Theorem: Let E be a field and H be a finite subgroup of the group of automorphisms of E. Then $O(H) = [E: E_H]$.

Proof: Suppose E is a field and H is a finite subgroup of the group of automorphisms of E.

Let $O(H) = n$. We prove that $[E: E_H] = n$.

Let $H = \{g_1,\ g_2,\ \ldots,\ g_n\}$ where $e = g_1$

Case - I: Suppose that $[E: E_H] < n$

Let $[E: E_H] = m$ and

let $\{a_1,\ a_2,\ \ldots,\ a_m\}$ be the basis of E over E_H (A)

$$\left.\begin{array}{c} g_1(a_1)x_1 + g_2(a_1)x_2 + \cdots + g_n(a_1)x_n = 0 \\ g_1(a_2)x_1 + g_2(a_2)x_2 + \cdots + g_n(a_2)x_n = 0 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ g_1(a_m)x_1 + g_2(a_m)x_2 + \cdots + g_n(a_m)x_n = 0 \end{array}\right\} \quad (I)$$

(I) is a system of m equations in unknowns $x_1,\ x_2,\ \ldots,\ x_n$ over E.

Since $m < n$, the above system (I) has a non-trivial solution $y_1,\ y_2,\ \ldots,\ y_n \in E$

[not all $y_1,\ y_2,\ \ldots,\ y_n$ are zero′s]

So for $1 \leq j \leq m$, we have

$g_1(a_j)y_1 + g_2(a_j)y_2 + \ldots + g_n(a_j)y_n = 0$ (II)

Let $a \in E$, From (A), $a = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m$ for some $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m \in E_H$

Now $\sum_{i=1}^{n}\ g_i(a)y_i = \sum_{i=1}^{n}\ g_i(\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m)y_i$

$= \sum_{i=1}^{n}\ [g_i(\alpha_1 a_1) + g_i(\alpha_2 a_2) + \ldots + g_i(\alpha_m a_m)]y_i$

$= \sum_{i=1}^{n}\ [\alpha_1 g_i(a_1) + \alpha_2 g_i(a_2) + \ldots + \alpha_m g_i(a_m)]y_i$

$= \alpha_1[\sum_{i=1}^{n}\ g_i(a_1)y_i] + \alpha_2[\sum_{i=1}^{n}\ g_i(a_2)y_i] + \ldots + \alpha_m[\sum_{i=1}^{n}\ g_i(a_m)y_i]$

$= \alpha_1 . 0 + \alpha_2 . 0 + \ldots + \alpha_m . 0 = 0$ [from (II)]

By lemma 10.2.8, we have $0 = y_1 = y_2 = \ldots = y_n$ as $g_1,\ g_2,\ \ldots,\ g_m$ are distinct embeddings.

This is a contradiction to not all $y_1,\ y_2,\ \ldots,\ y_n$ are zero.

Therefore $m \not< n$.

Case II: Suppose that $n < m$

Since $[E: E_H] = m$, we get $n + 1$ linearly independent elements $a_1,\ a_2,\ \ldots,\ a_{n+1}$ of E over E_H.

$$\left.\begin{array}{c} g_1(a_1)x_1 + g_1(a_2)x_2 + \cdots + g_1(a_{n+1})x_{n+1} = 0 \\ g_2(a_1)x_1 + g_2(a_2)x_2 + \cdots + g_2(a_{n+1})x_{n+1} = 0 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ g_n(a_1)x_1 + g_n(a_2)x_2 + \cdots + g_n(a_{n+1})x_{n+1} = 0 \end{array}\right\} \quad (III)$$

(III) is a system of n linear equations in $n+1$ unknowns over E.

So (III) has non-trivial solution $y_1,\ y_2,\ \ldots,\ y_{n+1}$. Such that

$g_j(a_1)y_1 + g_j(a_2)y_2 + \cdots \ldots + g_j(a_{n+1})y_{n+1} = 0$ for $1 \leq j \leq n$, (IV)

w.l.g we may assume that $y_1,\ y_2,\ \ldots,\ y_r$ are all non-zero and

$0 = y_{r+1} = y_{r+2} = \ldots = y_{n+1}$ and $y_1,\ y_2,\ \ldots,\ y_r$ are least non-zero elements satisfying (IV)

Now (IV) becomes

$g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r = 0,\ 1 \le j \le n$ (V)

For $g \in H$, $g\left[g_j(a_1)y_1 + g_j(a_2)y_2 + \ldots + g_j(a_r)y_r = 0\right] = g(0) = 0$. As $gH = H$,

$g_j(a_1)g(y_1) + g_j(a_2)g(y_2) + \ldots + g_j(a_r)g(y_r) = 0,\ 1 \le j \le n$ (VI)

(V) x $g(y_1)$ – (VI) x y_1 gives

$g_j(a_2)[y_2g(y_1) - y_1g(y_2)] + \ldots + g_j(a_r)[y_rg(y_1) - y_1g(y_r)] = 0, \quad 1 \le j \le n$ (VII)

In view of our assumption, as (VII) consists of less than n terms,

$y_2g(y_1) - y_1g(y_2) = 0, \ldots, y_rg(y_1) - y_1g(y_r) = 0$

That is, $g(y_1{y_2}^{-1}) = y_1{y_2}^{-1}, \ldots, g(y_1{y_r}^{-1}) = y_1{y_r}^{-1}$

That is, $y_2{y_1}^{-1} \ldots y_r{y_1}^{-1} \in E_H$.

So $y_2{y_1}^{-1} = z_2, \ldots, y_r{y_1}^{-1} = z_r$ and that

$y_2 = y_1z_2, \ldots, y_r = y_1z_r$, where $z_2, \ldots, z_n \in E_H$.

Now from (V) $g_1(a_1)y_1 + g_1(a_2)y_1z_2 + \ldots + g_1(a_r)y_1z_r = 0$

That is $g_1[a_1 + z_2a_2 + \ldots + z_ra_r] = 0$

That is $1.a_1 + z_2a_2 + \ldots + z_ra_r = 0$. Since $a_1, a_2, \ldots, a_n$ are independent over E_H,

$0 = 1 = z_2 = z_3 = \ldots = z_r$

So $0 = y_2 = y_3 = \ldots = y_r$, a contradiction.

Therefore $n \not< m$

Hence $n = m$.

10.2.10 Theorem: Let E be a finite separable extension of F and H be a subgroup of $G(\mathrm{E/F})$. Then $G(\mathrm{E}/E_H) = H$ and $[E : E_H] = O\left(G(\mathrm{E}/E_H)\right)$.

Proof: Suppose E is a finite separable extension of F and H is a subgroup $G(\mathrm{E/F})$ and E_H is the fixed field of H. We have $H \subseteq G(\mathrm{E}/E_H)$ and

$O(H) = [E : E_H] \ge O\left(G(\mathrm{E}/E_H)\right) \ge O(H)$

Therefore $O\left(G(\mathrm{E}/E_H)\right) = O(H)$ and that $G(\mathrm{E}/E_H) = H$

Hence $[E : E_H] = O(H) = O\left(G(\mathrm{E}/E_H)\right)$.

10.2.11 Theorem: Let E be a finite separable extension of a field F.Then the following conditions are equivalent:

1. E is a normal extension of F.
2. F is the fixed field of $G(\mathrm{E/F})$
3. $[E : F] = O\left(G(\mathrm{E/F})\right)$

Proof: Given E is a finite separable extension of F.

So, $E = F(u)$ for some $u \in E$.

Let $p(x)$ be the minimal polynomial of u over F and let $\deg\ p(x) = n$

So, $p(x)$ has n distinct roots as u is separable over F.

Now $[E\colon \mathrm{F}] = [F(u)\colon F] = n$.

Let E_0 be the fixed field of $G(\mathrm{E/F})$.

So, $[E\colon E_0] = O\big(G(\mathrm{E/F})\big)$ (by Theorem 10.2.9)

$(\mathbf{1}) \Rightarrow (\mathbf{2})$: we have that E is a normal extension of F.

Let $\sigma\colon F \to \bar{E}$ be an identity mapping of F. $(\sigma(\alpha) = \alpha\ \forall\ \alpha \in F)$

Then σ is an embedding of F into the algebraically closed field $\bar{E}$. So, σ can be extended to n embeddings $\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_n$ of $E = F(u)$ into $\bar{E}$, where n is the number of distinct roots of $p(x)$. Since E is a normal extension of F, (by Theorem 1.1)

each of $\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_n$ is an automorphism of E. So $\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_n \in G(\mathrm{E/F})$.

More over, each $g \in G(\mathrm{E/F})$ is an extension of σ. So $G(\mathrm{E/F}) = \{\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_n\}$ and that $O\big(G(\mathrm{E/F})\big) = n$.

Now $[E\colon E_o][E_o\colon F] = [E\colon F] = n = O\big(G(\mathrm{E/F})\big) = [E\colon E_o]$

Therefore, $[E_o\colon F] = 1 \Rightarrow E_o = F$

$(\mathbf{2}) \Rightarrow (\mathbf{1})$: we have that F is the fixed field of $G(\mathrm{E/F})$.

Let $G(\mathrm{E/F}) = \ \{\sigma_1 = I,\ \sigma_2,\ \ldots,\ \sigma_n\}$

Now $O\big(G(\mathrm{E/F})\big) = [E\colon F] = n$ [By Theorem(10.2.10)]

Consider $f(x) = (x-u)(x-\sigma_2(u))\ldots\big(x-\sigma_n(u)\big)$

Note that $u = \sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u) \in E$

So, $f(x) \in E[x]$.

Now $\sigma^*\colon E[x] \to E[x]$ defined by

$\sigma^*(g(x) = b_0 + b_1x + \ldots + b_kx^k) = g^{\sigma^*}(x) = \sigma(b_0) + \sigma(b_1)x + \ldots + \sigma(b_k)x^k$

is an automorphism of $E[x]$ for all $\sigma \in G(\mathrm{E/F})$.

For $\sigma \in G(\mathrm{E/F})$,

$\sigma^*(f(x)) = \big(x - \sigma(\sigma_1(u))\big)\Big(x - \sigma\big(\sigma_2(u)\big)\Big)\ldots.\Big(x - \sigma\big(\sigma_n(u)\big)\Big)$

$= f(x)$ as $\{\sigma\sigma_1,\ \sigma\sigma_2,\ \ldots,\ \sigma\sigma_n\} = G(\mathrm{E/F})$.

So the coefficients of $f(x)$ are fixed by all elements of $G(\mathrm{E/F})$. So $f(x) \in F[x]$.

Splitting field of $f(x)$ over F is $F\big(\sigma_1(u) = u,\ \sigma_2(u),\ \ldots, \sigma_n(u)\big) = F(u) = E$ as

$\sigma_2(u),\ \sigma_3(u)\ldots\sigma_n(u) \in E$

Therefore E is a normal extension of F.

$(\mathbf{2}) \Rightarrow (\mathbf{3})$: we have that F is a fixed field of $G(\mathrm{E/F})$

By theorem 10.2.10, $O\big(G(\mathrm{E/F})\big) = [E:F]$

$(\mathbf{3}) \Rightarrow (\mathbf{2})$: we have that $[E:F] = O\big(G(\mathrm{E/F})\big)$

We have by theorem 10.2.10, $[E:E_o] = O\big(G(\mathrm{E/F})\big)$

$\Rightarrow [E:E_o] = O\big(G(\mathrm{E/F})\big) = [E:F] = [E:E_o][E_o:F]$

$\Rightarrow [E_o:F] = 1$, that is, $E_o = F$

Therefore, the fixed field of $G(\mathrm{E/F})$ is F.

10.2.12 Example: The group $G(Q(\alpha)/Q)$ where $\alpha^5 = 1,\ \alpha \neq 1$ is a cyclic group of order 4.

Solution: We have $\alpha^5 = 1$ and $\alpha \neq 1$. Consider the group $G(Q(\alpha)/Q)$

Let $p(x) = 1 + x + x^2 + x^3 + x^4 \in Q[x]. Then\ p(x)$ is an irreducible polynomial over Q. (By Eisenstein criterian).

Since $x^5 - 1 = (x-1)p(x)$, we have that α is a root of $p(x)$. Since $p(x)$ is irreducible over Q (which is also monic), $p(x)$ is the minimal polynomial of α over Q.

So, $[Q(\alpha):Q] = \deg\ p(x) = 4$

Now $Q(\alpha)$ is a finite separable extension of Q as Q is a field of characteristic '0'.

Now $1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ are roots of $x^5 - 1 = (x-1)p(x)$, and distinct as $\alpha \neq 1$ and $O(\alpha) = 5$

Here $\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ are the roots of $p(x)$.

So, $Q(\alpha)$ is the splitting field of $p(x)$ over Q and

$Q(\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4) = Q(\alpha)$

By theorem 10.2.11, $4 = [Q(\alpha):Q] = O\big(G(Q(\alpha)/Q)\big)$

We have that α is a root of

$p(x) = 1 + x + x^2 + x^3 + x^4$ and that $0 = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$

Let $\sigma \in G(Q(\alpha)/Q)$.

Now $0 = \sigma(0) = \sigma(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4)$

$= \sigma(1) + \sigma(\alpha) + \sigma(\alpha^2) + \sigma(\alpha^3) + \sigma(\alpha^4)$

$= 1 + \sigma(\alpha) + \big(\sigma(\alpha)\big)^2 + \big(\sigma(\alpha)\big)^3 + \big(\sigma(\alpha)\big)^4$

So, $\sigma(\alpha)$ is a root of $p(x)$ and that $\sigma(\alpha) = \alpha$ or α^2 or α^3 or α^4.

Note that σ is completely determined by $\sigma(\alpha)$.

Let $\sigma_1(\alpha) = \alpha,\ \sigma_2(\alpha) = \alpha^2,\ \sigma_3(\alpha) = \alpha^3,\ \sigma_4(\alpha) = \alpha^4$. Then $\sigma_1, \sigma_2, \sigma_3\ and\ \sigma_4$ are all distinct automorphisms of $Q(\alpha)$ as $\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ are distinct.

Therefore, $G(Q(\alpha)/Q) = \{\sigma_1 = I, \sigma_2, \sigma_3, \sigma_4\}$.

$$\sigma_2{}^2(\alpha) = \sigma_2\big(\sigma_2(\alpha)\big) = \sigma_2(\alpha^2) = \big(\sigma_2(\alpha)\big)^2 = (\alpha^2)^2 = \alpha^4$$

$\sigma_2{}^3(\alpha) = \sigma_2\big(\sigma_2{}^2(\alpha)\big) = \sigma_2(\alpha^4) = \big(\sigma_2(\alpha)\big)^4 = \alpha^8 = \alpha^3$

$\sigma_2{}^4(\alpha) = \sigma_2\big(\sigma_2{}^3(\alpha)\big) = \sigma_2(\alpha^3) = \big(\sigma_2(\alpha)\big)^3 = (\alpha^2)^3 = \alpha^6 = 2$

So $\sigma_2{}^4(\alpha) = I$ and that $O(\sigma_2) = 4$

Therefore, $G(Q(\alpha)/Q)$ is a cyclic group of order 4 generated by σ_2(also by σ_3).

10.3 SUMMARY:

In this lesson, comparison between $O\big(G(\mathrm{E/F})\big)$ and $[E:F]$ is studied, where E is a finite separable extension of F. Moreover the equality between $[E:E_H]$ and $O(H)$ was established, where H is a finite subgroup of the group of automorphism of E and E_H is the fixed field of H. Also if E is a finite separable extension of F then some equivalent conditions presented under which E is a normal extension of F. An example was presented to identify the group $G(\mathrm{E/F})$ for a given Galois extension E of F.

10.4 TECHNICAL TERMS:

1. F- automorphism
2. Fixed field
3. Dedekind lemma

10.5 SELF- ASSESSMENT QUESTIONS:

1. Show that $G(Q(\beta)/Q)$ is a group of order 2, where $\beta^3 = 1$ and $\beta \neq 1$.
2. Find $G\big(Q(\sqrt{2})/Q\big)$.

10.6 SUGGESTED READINGS:

1. Bhattacharya P.B, S.K.Jain, S.R. Nagpaul. “Basic Abstract Algebra”, second Edition 1997, Cambridge University press (Indian Edition).
2. Hungerford, Thomas W., Abstract algebra, 1974, Springer – Verlag, New York.
3. Lang S. Algebra third edition, Boston Addison-wesley Moss 1993.
4. Ian stewart, Galois Theory, Chapman and Hall, CRC 2004.
5. I.S.Luther and I.B.S.Passi, Algebra, Volume.IV- Field Theory, Narosa Publishing House 2012.

- **Dr. K. Siva Prasad**

LESSON- 11

FUNDAMENTAL THEOREM OF GALOIS THEORY

OBJECTIVES:

- To understand fundamental theorem of Galois theory.
- To establish one-to-one correspondence between the subgroups of $G(E/F)$ and the intermediate fields between F and E, E is a Galois extension of F.
- To identify how normal subgroups correspond to normal extensions of fields.

STRUCTURE:

11.1 INTRODUCTION:

The Fundamental Theorem of Galois Theory is a central result in abstract algebra that links field theory with group theory. It arises from the study of polynomial equations and their roots, first developed by Évariste Galois. The theorem applies to Galois extensions, which are both normal and separable. For such an extension, the group of automorphisms that fix the base field play a crucial role. The theorem sets up a one-to-one correspondence between the subgroups of the $G(E/F)$ and the intermediate fields lying between F and E, E is a Galois extension of F. This correspondence is inclusion-reversing, which means larger subgroups correspond to smaller fields. Normal subgroups of $G(E/F)$ correspond to normal extensions of F. Moreover, the index of a subgroup $G(E/K)$ of $G(E/F)$ is equal to the degree of K over F if K is a normal extension of F.

11.2 FUNDAMENTAL THEOREM OF GALOIS THEORY:

11.2.1 Definition: Let $f(x) \in F[x]$ be a polynomial and let K be its splitting field over F. Then the group $G(K/F)$ of F-automorphisms of K is called the Galois group of $f(x)$ over F.

11.2.2 Definition: A finite, normal and separable extension E of a field F is called a Galois extension of F.

11.2.3 Theorem (**Fundamental Theorem of Galois Theory):** Let E be a Galois extension of F. Let K be any subfield of E containing F. Then the mapping $K \mapsto G(E/K)$ sets up a one-to-one correspondence from the set of subfields of E containing F to the subgroups of

$G(E/F)$ such that
(i) $K = E_{G(E/K)}$

(ii) For any subgroup H of $G(E/F)$, $H = G(E/E_H)$

(iii) $[E: K] = O(G(E/K))$ and $[K: F]$ = index of $G(E/K)$ in $G(E/F)$

(iv) K is a normal extension of F if and only if $G(E/K)$ is a normal subgroup of $G(E/F)$.

(v) If K is a normal extension of F, then $G(K/F) \cong \frac{G(E/F)}{G(E/K)}$

Proof: Let E be a Galois extension of F.

Then E is a finite, normal and separable extension of F.

Let K be a subfield of E containing F.

Let $\mathbf{S} = \{K/\ K \text{ is a subfield of E containing } F\}$ and $\mathbf{S}' = \{H/H \text{ is a subgroup of } G(E/F)\}$.

Define a mapping $\psi: \mathbf{S} \to \mathbf{S}'$ as follows:

let $K \in \mathbf{S}$.

Then K is a subfield of E containing F.

Now we show that $G(E/K)$ is a subgroup of $G(E/F)$, where $G(E/F)$ is the Galois group of F-automorphisms of E.

let $\sigma \in G(E/K)$.

Then σ is an automorphism of E that keeps every element of K fixed.

This implies that σ is an automorphism of E that keeps every element of F fixed as $F \subset K$

So, $\sigma \in G(E/F)$.

Therefore, $G(E/K) \subset G(E/F)$ and hence $G(E/K)$ is a subgroup of $G(E/F)$.

Now define $\psi: \mathbf{S} \to \mathbf{S}'$ by $\psi(K) = G(E/K)$.

(i) Since E is a Galois extension of F and K is a subfield of E containing F, we have that E is also a Galois extension of K. So, by a known theorem (10.2.11), K is a fixed field of $G(E/K)$.

Therefore $K = E_{G(E/K)}$.

(ii) We show that for any subgroup H of $G(E/F)$, $H = G(E/E_H)$.

Let H be a subgroup of $G(E/F)$.

Since E is a Galois extension of F, we have E is a finite separable extension of F and H is a subgroup of G(E/F).

By known theorem, $H = G(E/E_H)$

From (i), the mapping $\emptyset$ is one-one.

From (ii), the mapping $\emptyset$ is onto.

Hence, $\emptyset$ is a bijection from $\boldsymbol{S}$ onto $\boldsymbol{S'}$

(iii) Since E is a normal extension of F, we have E is a normal extension of K

By a known Theorem (10.2.11), $[\mathrm{E}:\mathrm{F}] = \mathrm{O}(\mathrm{G}(\mathrm{E}/\mathrm{F}))$ and $[\mathrm{E}:\mathrm{K}] = \mathrm{O}(\mathrm{G}(\mathrm{E}/\mathrm{K}))$

We know that [E:F] = [E:K][K:F]

Therefore $\mathrm{O}(\mathrm{G}(\mathrm{E}/\mathrm{F})) = \mathrm{O}(\mathrm{G}(\mathrm{E}/\mathrm{K}))\ [\mathrm{K}:\mathrm{F}]$

So, $[\mathrm{K}:\mathrm{F}] = \frac{\mathrm{O}(\mathrm{G}(\mathrm{E}/\mathrm{F}))}{\mathrm{O}(\mathrm{G}(\mathrm{E}/\mathrm{K}))}$. that is, $[\mathrm{K}:\mathrm{F}]$ is the index of $\mathrm{G}(\mathrm{E}/\mathrm{K})$ in $\mathrm{G}(\mathrm{E}/\mathrm{F})$

(iv) First we show that K is a normal extension of F iff $\sigma(\mathrm{K}) \subseteq \mathrm{K}$ for all $\sigma \in \mathrm{G}(\mathrm{E}/\mathrm{F})$

Suppose that K is a normal extension of F.

Let $\sigma \in \mathrm{G}(\mathrm{E}/\mathrm{F})$.

Then $\sigma : \mathrm{E} \to \mathrm{E}$ is an automorphism that keeps every element of F fixed.

Let $\bar{\mathrm{F}}$ be the algebraic closure of F containing E.

That is, $\sigma : \mathrm{K} \to \bar{\mathrm{F}}$ is an embedding that keeps every element of F fixed.

Let σ^* be the restriction of σ to K. Now σ^* is an embedding of K into $\bar{\mathrm{F}}$ and $\sigma^* = I\ on\ F$

Since K is a normal extension of F, σ^* is an automorphism of K. So, $\sigma^*(K) = K$ and that $\sigma(K) = K$ as $\sigma^* = \sigma$ on K. On the other hand suppose that $\sigma(K) \subseteq K$ for all $\sigma \in \mathrm{G}(\mathrm{E}/\mathrm{F})$.

Let $T: \mathrm{K} \to \bar{\mathrm{F}}$ be an embedding and $T = I$ on F.

Since E is an algebraic extension of K, T can be extended to an embedding T^* of E into $\bar{\mathrm{F}}$.

Since E is a normal extension of F, we have T^* is an automorphism of E.

Since $\mathrm{T}^* = T = I\ on\ F$, $\mathrm{T}^* \in \mathrm{G}(\mathrm{E}/\mathrm{F})$.

By our assumption, $\mathrm{T}^*(K) \subseteq K$ and that $\mathrm{T}^*$is an automorphism of K as $\mathrm{T}^*(K) = K$ on K, T is an automorphism of K.

That is, K is a normal extension of F.

Suppose now that K is a normal extension of F.

We prove that G(E/K) is a normal subgroup of G(E/F). It is clear that G(E/K) is a subgroup

of G(E/F). Let $\sigma \in G(E/F)$ and $\mathrm{T} \in G(E/K)$.

$(\sigma^{-1}\ \mathrm{T}\ \sigma)(k) = \sigma^{-1}\left(T\left(\sigma(k)\right)\right) = \sigma^{-1}\left(\sigma(k)\right) = k\ \forall\ k \in K$ as $\sigma(k) \in K$

and $T = \text{I}$ on K.

Therefore, $\sigma^{-1}\,\text{T}\,\sigma \in G(E/K)$ and hence $G(E/K)$ is a normal subgroup of G(E/F).

On the other hand suppose that G(E/K) is a normal subgroup of G(E/F).

We prove that K is a normal extension of F, that is $\sigma(K) \subseteq K$ for all $\sigma \in G(E/F)$.

Let $\sigma \in G(E/F)$, and let $k \in K$.

We have $\sigma^{-1}\,\text{T}\,\sigma \in G(E/K)$ for all $\text{T} \in G(E/K)$.

Also we have $k = (\sigma^{-1}\,\text{T}\,\sigma)(k) = \sigma^{-1}\left(T\left(\sigma(k)\right)\right)$ for all $k \in K$.

So, $T\left(\sigma(k)\right) = \sigma(k)\ for\ all\ \text{T} \in G(E/K), k \in K$.

Since the fixed field of $G(E/K)$ is K, $\sigma(k) \in K\ as\ \sigma(k)$ is fixed by all $\text{T} \in G(E/K)$.

Therefore $\sigma(K) \subseteq K$, that is, K is a normal extension of F.

5) We have that K is a normal extension of F.

We prove that $G(K/F) \cong G(E/F)/G(E/K)$

Define $\psi: G(E/F) \to G(K/F)$ by $\psi(\sigma) = \sigma^*$, for all $\sigma \in G(E/F)$,

where σ^* is the restriction of $\sigma \in G(E/F)$ to K and $\sigma^* \in G(E/F)$

Let $\sigma_1, \sigma_2 \in G(E/F)$. $Then\ \sigma_1\ o\ \sigma_2 \in G(E/F). So,\ \psi(\sigma_1\ \text{o}\ \sigma_2) = (\sigma_1\ o\ \sigma_2)^*$.

Now $(\sigma_1\ o\ \sigma_2)^*(k) = (\sigma_1(\sigma_2(k)) = \sigma_1\left(\sigma_2^*(k)\right) = \sigma_1^*\left(\sigma_2^*(k)\right)$

$= (\sigma_1^*\ \text{o}\ \sigma_2^*)(k)$ for all $k \in K$.

This implies $(\sigma_1 \text{o}\ \sigma_2)^* = \sigma_1^*\ o\ \sigma_2^*$.

So, $\psi(\sigma_1\ o\ \sigma_2) = \sigma_1^*\ o\ \sigma_2^* = \psi(\sigma_1)\ \text{o}\ \psi(\sigma_2)$.

Therefore, ψ is a homomorphism of the group G(E/F) into the group G(K/F).

Consider Ker $\psi = \{\sigma \in G(E/F)/\psi(\sigma) = \text{I on K}\}$

$= \{\sigma \in G(E/F)/\sigma^* = \text{I on K}\}$

So, $\text{Ker}\psi \subseteq G(E/K)$. Also for $\sigma \in G(E/K), \sigma(k) = k$ for all $k \in K$.

This implies $\sigma \in \text{Ker}\ \psi$. So, $G(E/K) \subseteq \text{Ker}\ \psi$.

Hence, Ker $\psi = G(E/K)$.

Therefore, $G(E/F)/G(E/K) \cong \psi\left(G(E/F)\right)$ and $\psi\left(G(E/F)\right)$is a subgroup of $G(K/F)$.

We have $[E:F] = [E:K][K:F]$ and $[E:F] = O\left(G(E/F)\right)$

and $[E:K] = O\big(G(E/K)\big)$. So, $[K:F] = \frac{O\big(G(E/F)\big)}{O\big(G(E/K)\big)}$

Now $[K:F] = \frac{O\big(G(E/F)\big)}{O\big(G(E/K)\big)} = O\left(\frac{G(E/F)}{G(K/F)}\right) = O\left(\psi\big(G(E/F)\big)\right)$

Since K is a normal extension of F, we have

$[K:F] = O\big(G(K/F)\big)$

So, $O\big(G(K/F)\big) = O\left(\psi\big(G(E/F)\big)\right)$ and that $G(K/F) = \psi(G(E/F)))$

Therefore, $G(E/F)/G(E/K) \cong G(K/F)$

11.3 SUMMARY:

The Fundamental Theorem of Galois Theory describes the deep relationship between fields and groups. If E is a finite Galois extension of F, then there is a one-to-one correspondence between the subgroups of $G = G(E/F)$ and the intermediate fields lying between F and E. This correspondence is inclusion-reversing, meaning that larger subgroups correspond to smaller fields. Each subgroup H of G gives a fixed field E_H and each intermediate field K gives the subgroup G(E/K). Normal subgroups of $G(E/F)$ correspond to normal extensions of F. For a normal extension K of F, the index of the subgroup $G(E/K)$ equals the degree of the extension, of K over F. Thus, the subgroup structure of the $G(E/F)$ mirrors the lattice of intermediate fields. This correspondence allows field-theoretic problems to be translated into group-theoretic ones, and it explains why certain polynomials are solvable while others are not.

11.4 TECHNICAL TERMS:

- **Degree of Extension**: The dimension of E as a vector space over F and it is denoted by [E:F]
- **Splitting Field:** The smallest field in which a given polynomial splits completely into linear factors.
- **Separable Extension:** A field extension in which every element is the root of a separable polynomial over the base field.
- **Normal Extension:** An extension in which every irreducible polynomial over the base field that has one root in the extension splits completely in it.
- **Galois Extension:** A finite extension that is both normal and separable.
- **Intermediate Field:** A field K such that F⊆K⊆E, F is a subfield of K and K is a subfield of E.

11.5 SELF-ASSESSMENT QUESTIONS:

Question 1. What is a Galois extension?

Answer: A finite extension E of F is called a Galois extension if it is both normal and separable.

Question 2. State the Fundamental Theorem of Galois Theory.

Answer: If E/F is a finite Galois extension with Galois group G, then there is a one-to-one inclusion-reversing correspondence between the subgroups of G and the intermediate fields of E.

Question 3. What type of field extensions correspond to normal subgroups of the Galois group?
Answer: Normal subgroups of G correspond to intermediate fields that are normal over F.

Question 4. Why is the correspondence inclusion-reversing?
Answer: Because larger subgroups of $G(E/F)$ fix fewer elements, resulting in smaller fields, and vice versa.

Question 5. Give one application of the Fundamental Theorem of Galois Theory.
Answer: It explains why general equations of degree five or higher over Q cannot always be solved by radicals.

11.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Dr. K. Siva Prasad**

LESSON- 12

FUNDAMENTAL THEOREM OF ALGEBRA

OBJECTIVES:

- To understand the statement of the fundamental theorem of Algebra that every non-constant polynomial with complex coefficients has at least one root in the field of complex numbers.
- To realize the importance of the field of complex numbers as an algebraically closed field. i.e., every polynomial equation over $\mathbb{C}$ can be completely factorized into linear factors.

STRUCTURE:

12.1 INTRODUCTION:

The Fundamental Theorem of Algebra is a central result in Algebra which states that every non-constant polynomial with complex coefficients has at least one root in the field of complex numbers. This establishes that the field of complex numbers is algebraically closed. Consequently, any polynomial of degree *n* over $\mathbb{C}$ can be completely factorized into exactly *n* linear factors, counting multiplicities. The theorem highlights the distinction between $\mathbb{R}$ and $\mathbb{C}$, since real numbers are not algebraically closed. Various proofs exist, ranging from analytic approaches using Liouville's theorem to purely algebraic and topological methods. A direct outcome of the theorem is that over $\mathbb{C}$ the only irreducible polynomials are linear. It also guarantees the completeness of polynomial solutions in the complex plane.

12.2 FUNDAMENTAL THEOREM OF ALGEBRA:

12.2.1 Note: Any field of characteristic zero is a perfect field. Since the characteristic of $\mathbb{R}$ and $\mathbb{C}$ are zero, the fields $\mathbb{R}$ and $\mathbb{C}$ are perfect fields. So any algebraic extension over them is a separable extension.

12.2.2 Note: Let G be a finite group and let p be a prime number. If $p^m \mid o(G)$, then G has a subgroup of order p^m.

Theorem 12.2.3: (Fundamental Theorem of Algebra)
Let $f(x) \in \mathbb{C}[x]$ be a non-constant polynomial. Then $f(x)$ can be factored as linear factors in $\mathbb{C}[x]$.

Proof: Let $f(x) \in \mathbb{C}[x]$ be a non-constant polynomial.

We prove that the splitting field of $f(x)$ over $\mathbb{C}$ is $\mathbb{C}$, that is, all roots of $f(x)$ are in $\mathbb{C}$.

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_n \neq 0$.

Consider $g(x) = (x^2 + 1)(a_0 + a_1x + \cdots + a_nx^n)(\overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n)$

Clearly $g(x) \in \mathbb{R}[x]$. Let E be the splitting field of $g(x)$ over $\mathbb{R}$.

Clearly $\mathbb{C}$ is a subfield of E and that $\mathbb{R} \subseteq \mathbb{C} \subseteq E$.

We prove that $E = \mathbb{C}$ and that all roots of $f(x)$ will be in $\mathbb{C}$. We first prove that there is no subfield K of E containing $\mathbb{C}$ such that $[K:\mathbb{C}] = 2$. Suppose that K is a subfield of E and $\mathbb{C} \subseteq K$ and $[K:\mathbb{C}] = 2$. Since K is a finite separable extension of $\mathbb{C}$ such that $K = \mathbb{C}(u)$ for some $u \in K$.

Let $p(x)$ be the minimal polynomial of u over $\mathbb{C}$.

Now $deg\ p(x) = 2$ and $p(x)$ is irreducible monic polynomial in $\mathbb{C}[x]$.

Suppose $p(x) = x^2 + 2ax + b$, where $a, b \in \mathbb{C}$.

Now $p(x) = (x + a)^2 - (a^2 - b)$

$= (x + a)^2 - \left(\sqrt{a^2 - b}\right)^2$

$= ((x + a) - \sqrt{a^2 - b})\ ((x + a) + \sqrt{a^2 - b})$

$= \left(x - \left(\sqrt{a^2 - b} - a\right)\right)\left(x - \left(-a - \sqrt{a^2 - b}\right)\right)$

Since $a^2 - b \in \mathbb{C},\ we\ have\ that\ \sqrt{a^2 - b} \in \mathbb{C}$ and that both roots

$(\sqrt{a^2 - b} - a), \left(-\sqrt{a^2 - b} - a\right)$ are in $\mathbb{C}$.

This is a contradiction to $p(x)$ is irreducible over $\mathbb{C}$.

Therefore there is no subfield K of E containing $\mathbb{C}$ such that $[K:\mathbb{C}] = 2$.

Consider the Galois group $G(E/\mathbb{R})\ of\ g(x)$ over $\mathbb{R}$.

Now $O\big(G(E/\mathbb{R})\big) = 2^m q$, where m is a positive integer and q is an odd integer.

Let $G(E/\mathbb{R})$ has a 2-Sylow subgroup of H of order 2^m.

Now H = G(E/L) for some subfield L of E containing $\mathbb{R}$.

Now $2^m q = O\big(G(E/\mathbb{R})\big) = [E:\mathbb{R}] = [E:L][L:\mathbb{R}]$

$= O(H)[L:\mathbb{R}] = 2^m[L:\mathbb{R}]$

So, $[L:\mathbb{R}] = q$.

Since L is a finite separable extension of $\mathbb{R}$, we have that

$L = \mathbb{R}(v)$ for some $v \in L$.

Let $q(x)$ be the minimal polynomial of v over $\mathbb{R}$,

Now $q(x) \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$, and its degree is q, an odd integer.

We know that every equation of odd degree over the reals has a real root.

So, $q(x)$ has a root in $\mathbb{R}$. Since $q(x)$ is irreducible over $\mathbb{R}$, and has a root in $\mathbb{R}$, it follows that deg $q(x) = 1$ and that $q = 1$.

So, $L = \mathbb{R}$. Now $O\big(G(E/\mathbb{R})\big) = 2^m$ and $\mathbb{R} \subseteq \mathbb{C} \subseteq E$.

Since $2^m = [E:\mathbb{R}] = [E:\mathbb{C}][\mathbb{C}:\mathbb{R}] = [E:\mathbb{C}]$ x 2, we have that

$[E:\mathbb{C}] = 2^{m-1}$.

Since E is a Galois extension of $\mathbb{C}$, it follows that

$[E:\mathbb{C}] = O\big(G(E/\mathbb{C})\big) = 2^{m-1}$.

Suppose that $m > 1$. So, $m - 1 \geq 1$. So, $G(E/\mathbb{C})$ has a subgroup of order 2^{m-2} as $2^{m-2}/2^{m-1}$.

Now by the fundamental theorem of Galois theory,

we get a subfield E_0 of E containing $\mathbb{C}$ such that

$G(E/E_0) = T$ and $[E: E_0] = O\big(G(E/E_0)\big)$

Now $2^{m-1} = [E: \mathbb{C}] = [E: E_0][E_0: \mathbb{C}]$

$= O(T)[E_0: \mathbb{C}]$

$= 2^{m-2}[E_0: \mathbb{C}]$

Therefore, $[E_0: \mathbb{C}] = 2$. This is a contradiction to the fact that E has no subfield K containing

$\mathbb{C}$ such that $[K: \mathbb{C}] = 2$. Therefore $m \not> 1$, that is, $m = 1$.

So, $[E: \mathbb{C}] = 2^{m-1} = 2^{1-1} = 2^0 = 1$.

Hence, $E = \mathbb{C}$ as required.

12.3 SUMMARY:

The Fundamental Theorem of Algebra is one of the most celebrated results connecting algebra and analysis. It asserts that every non-constant polynomial with complex coefficients has at least one root in the field of complex numbers. This property makes the complex number system an algebraically closed field, a concept of fundamental importance in higher algebra. The necessity of the theorem arises from the fact that equations of degree higher than two cannot always be solved explicitly by radicals, yet we still require a guarantee of root existence. Without such a result, the theory of polynomial factorization would remain incomplete. The theorem provides the foundation for expressing any polynomial of degree *n* as a product of *n* linear factors over $\mathbb{C}$, ensuring completeness of algebraic equations.

12.4 TECHNICAL TERMS:

Fundamental theorem of algebra.

12.5 SELF-ASSESSMENT QUESTIONS:

Question 1. Why is the field of complex numbers called algebraically closed?

Answer: Because every non-constant polynomial in $\mathbb{C}$[x] has at least one root in $\mathbb{C}$, and hence every polynomial splits completely into linear factors over $\mathbb{C}$.

Question 2. What are the irreducible polynomials over $\mathbb{C}$?

Answer: Over $\mathbb{C}$, the only irreducible polynomials are linear.

Question 3. What is the necessity of the Fundamental Theorem of Algebra?

Answer: It guarantees the existence of roots for all complex polynomials, making factorization possible and ensuring completeness of algebraic equations.

Question 4. How does the Fundamental Theorem of Algebra relate to Galois Theory?

Answer: It ensures that the splitting field of a polynomials exists inside $\mathbb{C}$, which is essential for studying solvability of polynomials by radicals.

Question 5. Why is the theorem not true over the field of real numbers?

Answer: Because there exist real polynomials, like x^2+1 which have no real roots, $\mathbb{R}$ is not algebraically closed.

12.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

-

- **Dr. K. Siva Prasad**

LESSON- 13

ROOTS OF UNITY AND CYCLOTOMIC POLYNOMIALS

OBJECTIVES:

- To understand the concept of roots of unity and its properties.
- To derive the minimal polynomial of primitive roots of unity over the rationals.
- To construct the nth cyclotomic polynomial, which is the minimal polynomial of a primitive nth root of unity.
- To investigate the irreducibility and degree of cyclotomic polynomials.

STRUCTURE:

13.1 INTRODUCTION:

In algebra, one of the central theme is understanding the roots of polynomials over fields. This lesson on roots of unity and cyclotomic polynomials introduces the fundamental concepts that link algebra, number theory, and geometry. It focuses on the study of the nth roots of unity, which are precisely the solutions to the equation $x^n = 1$ in a suitable field. The concept of primitive roots of unity, construction and properties of cyclotomic polynomials is discussed. The elegant algebraic properties of cyclotomic polynomials including their irreducibility over Q is studied.

13.2 ROOTS OF UNITY:

13.2.1 Definition: Let E be a field and n be a positive integer. An element $\omega \in E$ is called a primitive n^{th} root of unity in E if $\omega^n = 1$ and $\omega^m \neq 1$, for any positive integer $m < n$.

13.2.2 Note: The set of complex numbers satisfying $x^n = 1$ form a finite subgroup H of the multiplicative group $\mathbb{C}^* = C - \{0\}$, where C is the field of complex numbers. Also this H is cyclic group generated by a primitive n^{th} root of unity. For any positive integer 'n', there are exactly $\varphi(n)$ primitive n^{th} roots of unity, where $\varphi(n)$ is the number of positive integers less than n and are relatively prime to n.

(i) If a finite group of order 'n' contains an element of order 'n', then it must be a cyclic group.

(ii) If A and B are cyclic groups of orders m and n respectively such that (m,n) =1, then A×B is a cyclic group.

(iii) Let A be a finite abelian group of order $p_1^{e_1}.p_2^{e_2}\ldots\ldots p_k^{e_k}$ where $p_1, p_2, \ldots\ldots p_k$ are distinct primes and $e_i>0$ then $A = S(p_1)\oplus S(p_2)\oplus\ldots\ldots\ldots\oplus S(p_K)$ where $|S(p_i)| = p_i^{e_i}$ $\forall i = 1,2,\ldots..,$ k and this decomposition of A is unique.

13.2.3 Theorem: Let F be a field and let U be a finite subgroup of the multiplicative group $F^* = F - \{0\}$. Then U is cyclic. In particular, roots of $x^n - 1 \in F[x]$ from a cyclic group.

Proof: Let F be a field and $F^* = F - \{0\}$ be the multiplicative group of non-zero elements, which is abelian.

Let U be a finite subgroup of F^*.

Suppose $|U| = n>1$ and $n = p_1^{r_1}.p_2^{r_2}\ldots\ldots p_k^{r}$, where $p_1, p_2, \ldots\ldots p_k$ are distinct prime numbers and $r_1, r_2, \ldots\ldots r_k$ are positive integers.

Let $S(p_i)$ be a p_i- sylow subgroup of U.

Since U is finite abelian group, we have $U = S(p_1)\times S(p_2)\times\ldots\ldots\ldots\times S(p_K)$ where $|S(p_i)|= p_i^{r_i}$; $1\leq i\leq k$.

Now we show that U is cyclic.

For this first we show that each $S(p_i)$ is a cyclic group.

Let $a\in S(p_i)$ be an element such that O(a) is maximal, say $p_i^{s_i}$.

Since $O(a)|\ O(S(p_i))$, we have $p_i^{s_i}|\ p_i^{r_i}$

This implies $s_i\leq r_i$ (1)

Let $x \in S(p_i)$ with $O(x) = p_i^{t_i}$

By the selection of the element 'a' in $S(p_i)$, we have that $p_i^{t_i} \leq p_i^{s_i}$

This implies $x^{p_i{}^{s_i}} = 1$.

Then every element of $S(p_i)$ is a root of the polynomial $x^{p_i{}^{s_i}} - 1$.

But we know that the number of roots of the polynomial $x^{p_i{}^{s_i}} - 1$ is $p_i^{s_i}$

$\Rightarrow |S(p_i)| \leq p_i^{s_i}$

$\Rightarrow\quad p_i^{r_i} \leq p_i^{s_i}$

$\Rightarrow r_i \leq s_i$ (2)

From (1) and (2), we have $r_i = s_i$

$\Rightarrow\quad p_i^{r_i} = p_i^{s_i}$

$\Rightarrow O(a) = p_i^{r_i}$

Therefore $|S(p_i)| = O(a)$.

So $S(p_i)$ is cyclic for all i =1,2,…..,k.

Therefore $S(p_1), S(p_2)\ldots\ldots\ldots S(p_K)$ are cyclic groups of orders $p_1^{r_1}, p_2^{r_2}, \ldots\ldots, p_k^{r}$

Thus $S(p_1)\times S(p_2)\times\ldots\ldots\ldots\times S(p_K)$ is cyclic and hence U is cyclic.

Let H be the set of roots of $x^n - 1 \in F[x]$. Let E be the splitting field of $x^n - 1$.

Then $E^* = E - \{0\}$ is a multiplicative group of non-zero elements.

Let $a,b\in H$. Then $a^n = 1$ and $b^n = 1$

Consider, $(ab)^n = a^n b^n = 1$. So, $ab \in H$

This shows that H is a finite subgroup of E^* and hence H is a cyclic group

Therefore the set of roots of $x^n - 1$ is a cyclic group.

13.2.4 Theorem: Let F be a field and let n be a positive integer. Then there exists a primitive n^{th} root of unity in some extension E of F if and only if either charF = 0 (or) charF$\nmid$n

Proof: Given that F is a field and n is a positive integer.

Consider the polynomial $f(x) = x^n - 1 \in F[x]$

Assume that char F = 0 or charF$\nmid$n

Let E be the splitting field of f(x) over F.

Let $\alpha \in E$ be a root of $f(x) \in F[x]$.

Then $f'(x) = nx^{n-1}$ (Since $f(x) = x^n - 1$)

This implies $f'(\alpha) = n\alpha^{n-1} \neq 0$ (charF$\nmid$n)

Since charF = 0 or charF$\nmid$n, we have $f'(\alpha) \neq 0$.

i.e, Each root of the polynomial f(x) is simple.

Therefore f(x) has n distinct roots.

Let H be the set of all these 'n' roots of f(x).

Then $H \subseteq E$, $|H| = n$ and we know that H is a cyclic group of $E^* = E - \{0\}$.

Therefore H = (a).

Here O(a) = n, $a^n = 1$ and $a^m \neq 1$ for any positive integer m<n.

So, a is primitive n^{th} root of unity in E, where E is extension of F.

Conversely, Assume that E is an extension of F and $a \in E$ is a primitive n^{th} root of unity.

Then $1, a, a^2, \ldots\ldots, a^{n-1}$ are n distinct roots of the polynomial $f(x) = x^n - 1 \in F[x]$

Therefore all the roots of f(x) are simple.

So, $f'(x) \neq 0$ i.e, $f'(x) = nx^{n-1} \neq 0$.

Hence charF = 0 (or) charF$\nmid$n

13.3 CYCLOTOMIC POLYNOMIALS:

13.3.1 Definition: Let n be a positive integer. Let F be a field of characteristic zero or characteristic p$\nmid$n. Then the polynomial $\varphi_n(x) = \pi_\omega(x - \omega)$ where the product runs over all the primitive n^{th} roots ω of unity is called the n^{th} cyclotomic polynomial.

Example: $\varphi_1(x) = x - 1$, $\varphi_2(x) = x + 1$, $\varphi_3(x) = x^2 + x + 1$, $\varphi_4(x) = x^2 + 1$ are cyclotomic polynomials over Q.

13.3.2 Theorem: $\varphi_n(x) = \pi_\omega(x - \omega)$, ω is primitive n^{th} root in C, is an irreducible polynomial of degree $\varphi(n)$ in Z[x]

Proof:

Let E be the splitting field of $x^n - 1$ over Q.

Then E is a finite, normal and separable extension of Q (Since char Q = 0)

Therefore the fixed field of G(E/Q) is Q.

Let ω be any primitive n^{th} root of unity.

Then for any $\sigma \in G(E/Q)$, $(\sigma(\omega))^n = \sigma(\omega^n) = \sigma(1) = 1$ & $(\sigma(\omega))^m = \sigma(\omega^m) \neq \sigma(1) = 1$ for positive integer m<n.

Therefore for any $\sigma \in G(E/Q)$, the induced mapping $\sigma^* : E[x] \to E[x]$ keeps $\varphi_n(x)$ unaltered.

i.e., $\sigma^*(\varphi_n(x)) = \varphi_n(x)\ \forall \sigma \in G(E/Q)$

i.e, each coefficient of $\varphi_n(x)$ remains unchanged for any $\sigma \in G(E/Q)$

This implies that all the coefficients of $\varphi_n(x)$ are in the fixed field of G(E/Q) and hence all the coefficients of $\varphi_n(x)$ are in Q. ($\because$ fixed field of G(E/Q) is Q)

Therefore $\varphi_n(x) \in Q[x]$

Since $\varphi_n(x)$ is a factor of $x^n - 1$ & $\varphi_n(x)$ is monic, we have $\varphi_n(x) \in Z[x]$ (1)

We know that for any positive integer n, the number of primitive n^{th} root of unity is $\varphi(n)$

So the degree of $\varphi_n(x)$ is $\varphi(n)$. (2)

Now we show that $\varphi_n(x)$ is irreducible over Z

Let $f(x) \in Z[x]$ be an irreducible factor of $\varphi_n(x)$ and ω be a root of f(x).

Here ω is also a primitive n^{th} root of unity.

We shall now prove that ω^p is also a root of f(x) for any prime number p such that $p \nmid n$.

Let p be any prime number such that $p \nmid n$.

Clearly ω^p is also generator of the cyclic group consisting of the roots of $x^n - 1$ ($\because (p,n) = 1$)

This implies that ω^p is also a primitive n^{th} root of unity.

Since $f(x) \in Z[x]$ is a factor of $\varphi_n(x)$, there exists a polynomial $h(x) \in Z[x]$ such that $\varphi_n(x) = f(x).h(x)$.

If possible suppose that ω^p is not a root of f(x).

Then ω^p is a root of h(x) ($\because \varphi_n(x) = f(x).h(x)$)

This implies $h(\omega^p) = 0$. So, ω is a root of $h(x^p)$

Therefore f(x) and $h(x^p)$ have a common factor over some extension of Q.

By Euclid's division algorithm, f(x) and $h(x^p)$ have a common factor over Q.

Since f(x) is irreducible in Z[x], we have f(x) is irreducible in Q[x]

Therefore $f(x)|h(x^p)$ in Q[x]. So, there exists $g(x) \in Z[x]$ such that $h(x^p) = f(x).g(x)$

Since $h(x^p)$ and f(x) are monic polynomials, it follows that g(x) is a monic polynomial over Z.

Let $\bar{f}(x)$ and $\bar{h}(x)$ be obtained by replacing the coefficients $a \in Z$ by $\bar{a}$ of $Z/(p)$

Since $a^p \equiv a(\text{mod}p)$ for all integers a, we have $(\bar{h}(x))^p = \bar{h}(x^p)$

So $\bar{h}(x^p) = \bar{f}(x).\bar{g}(x)$ and hence $\bar{h}(x)$ and $\bar{f}(x)$ have a common factor.

But we know that $\varphi_n(x) \mid x^n - 1$ and $\varphi_n(x) = f(x).h(x)$

This implies $x^n - 1$ has a multiple root, Say α.

Then the derivative of $x^n - 1$ must vanish at α.

$\Rightarrow n\alpha^{n-1} = 0$

$\Rightarrow \alpha^{n-1} = 0$ ($\because$ char p$\nmid$ n)

$\Rightarrow \alpha = 0$, which is contradiction ($\because$ 0 is not a root of $x^n - 1$)

Therefore ω^p is also a root of f(x).

Thus if ω is a root of f(x), then ω^p is also a root of f(x) for any prime p < n & p$\nmid$ n (*)

Since any primitive nth root of unity can be obtained by raising ω to a succession of prime powers with primes not dividing n, we have that all the primitive nth roots of unity are roots of f(x). So, $\varphi_n(x) = f(x)$

Therefore $\varphi_n(x)$ is irreducible over Z.

13.3.3 Theorem: Let ω be a primitive n^{th} root of unity in C, then Q(ω) is the splitting field of $\overline{\varphi_n}(x)$ and also of $x^n - 1 \in Q[x]$. Further $[Q(\omega):Q] = \varphi(n) = |G(Q(\omega)/Q)|$ and $G(Q(\omega)/Q) \cong \left(\frac{Z}{<n>}\right)^*$, the multiplicative group formed by the units of $\frac{Z}{<n>}$.

Proof: Given that ω is a primitive n^{th} root of unity in C.

Let $1, \omega, \omega^2, \ldots\ldots, \omega^{n-1}$ be the n distinct roots of the polynomial x^n-1.

So Q(ω) is the splitting field of the polynomial x^n-1.

Since Q(ω) contains ω and ω is a primitive n^{th} root of unity, we have that Q(ω) contains all n^{th} roots of unity. Hence Q(ω) is also the splitting field of $\overline{\varphi_n}(x)$.

Now $\overline{\varphi_n}(x) \in Q[x]$, and by Theorem 13.3.2, it is irreducible with leading coefficient 1 and ω is a root of $\overline{\varphi_n}(x)$. Also we have $\overline{\varphi_n}(x)$ is the minimal polynomial of ω over Q.

$\therefore [Q(\omega):Q] = \deg\overline{\varphi_n}(x) = \varphi(n)$ (1)

Since Q(ω) is a finite, normal and separable extension of Q, by known theorem, we have

$|G(Q(\omega)/Q)| = [Q(\omega):Q]$ (2)

Let $\sigma \in G(Q(\omega)/Q)$.

Since ω is a primitive n^{th} root of unity, we have $\sigma(\omega)$ is also a primitive n^{th} root of unity.

Therefore $\sigma(\omega) = \omega^k$ for $k < n$ and k is relatively prime to n.

Denote σ by σ_k.

From (1) and (2), we have $|G(Q(\omega)/Q)| = [Q(\omega):Q] = \varphi(n) = \deg\overline{\varphi_n}(x)$

The number of such k's are equal to $\varphi(n)$ and they are precisely the elements of $(Z/(n))^*$

Now we show that the galois group $G(Q(\omega)/Q)$ is isomorphic to $(Z/(n))^*$, where$(Z/(n))^*$ is the multiplicative group formed by the units of $Z/(n)$.

Define a mapping f: $(Z/(n))^* \to G(Q(\omega)/Q)$ as $f(k) = \sigma_k, \forall\, k \in (Z/(n))^*$

It is easy to verify that f is one-one and onto.

Now we show that f is a homomorphism.

Let $k_1, k_2 \in (Z/(n))^*$ .Then $k_1.k_2 = qn+r$ where $r < n$

So $k_1.k_2 + (n) = qn + r + (n) = r + (n)$ ($\because qn \in (n)$)

This implies $k_1.k_2 = r$. So $\omega^{k_1k_2} = \omega^{qn+r} = \omega^r$

Now $f(k_1k_2) = f(r) = \sigma_r = \sigma_{k_1k_2} = \sigma_{k_1}.\sigma_{k_2} = f(k_1).f(k_2)$

Therefore f is homomorphism.

Hence $\left(\frac{Z}{<n>}\right)^* \cong G(Q(\omega)/Q)$

13.4 SUMMARY:

The topic "Roots of Unity and Cyclotomic Polynomials" explores an essential area of algebra that links polynomial equations, field theory, and number theory. In particular the complex numbers that satisfying the equation $x^n = 1$ form a cyclic group under multiplication. A primitive n^{th} root of unity is one that generates all the n^{th} roots of unity. The study of these roots is extended through cyclotomic polynomials, which are minimal polynomials of primitive n^{th} roots of unity over the rationals. This polynomial denoted by $\varphi_n(x)$ have integer coefficients, degree equal to $\varphi(n)$ and are irreducible over Q. The cyclotomic polynomial $\varphi_n(x)$ captures the structure of roots of unity and provides a factorization of $x^n - 1$ into irreducible polynomials over Q. The construction of cyclotomic polynomials is recursive.

13.5 TECHNICAL TERMS:

Root of Unity: A solution to the equation $x^n = 1$.

Primitive n^{th} Root of Unity: The primitive nth roots of unity are those that generate all the nth roots through their powers.

Cyclotomic Polynomial: Let n be a positive integer. Let F be a field of characteristic zero or characteristic $p \nmid n$. Then the polynomial $\varphi_n(x) = \pi_\omega(x - \omega)$ where the product runs over all the primitive n^{th} roots ω of unity is called the n^{th} cyclotomic polynomial.

Euler's Totient Function $\varphi(n)$: The number of positive integers k less than n such that gcd(k,n)=1.

Irreducible Polynomial: A nonconstant polynomial that cannot be factored into the product of two nonconstant polynomials over the field.

13.6 SELF -ASSESSMENT QUESTIONS:

Q1. How many primitive nth roots of unity exist in C?
Answer:
There are $\phi(n)$ primitive nth roots of unity in C, where ϕ is Euler's totient function.

Q2. Are cyclotomic polynomials irreducible over Q?
Answer: Yes, $\varphi_n(x)$ is irreducible over Q for every positive integer n.

Q3. Compute $\Phi_3(x)$.
Answer:

We have $x^3-1=(x-1)(x^2+x+1)$

So $\Phi_3(x)=x^2+x+1$ which is the minimal polynomial of a primitive cube root of unity over Q.

Q4. What is the degree of $\varphi_n(x)$?
Answer:
The degree of $\varphi_n(x)$ is $\phi(n)$, where ϕ is Euler's totient function.

13.7 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Dr. J.L Rama Prasad**

LESSON- 14

CYCLIC EXTENSIONS

OBJECTIVES:

- To understand the structure and properties of cyclic extensions of fields.
- To analyze Galois extensions with cyclic Galois groups.
- To explore explicit examples and constructions of cyclic extensions.
- To learn how cyclic extensions contribute to solvability of polynomial by radicals.
- To apply cyclic extension theory to fundamental algebraic structures and their automorphisms.

STRUCTURE:

14.1 INTRODUCTION:

A cyclic extension of a field is a Galois extension whose Galois group is cyclic. This concept plays a crucial role in Galois theory**,** which connects field extensions with group theory. Cyclic extensions are particularly important for understanding the solvability of polynomials by radicals and the structure of field automorphisms. Cyclic extensions also illustrate the fundamental theorem of Galois theory, which describes a correspondence between subgroups of the Galois group and intermediate fields. In cyclic extensions, this correspondence is particularly simple because the Galois group is cyclic and its subgroups are easy to classify.

14.2 CYCLIC EXTENSIONS:

14.2.1 Definition: Let E be a Galois extension of F. Then E is called a cyclic extension of F if G(E/F) is a cyclic group.

Example: 1. Let ω be a primitive n^{th} root of unity in $\mathbb{C}$. Consider the polynomial $x^n - 1 \in Q[x]$. Then ω is a root of the polynomial $x^2 - 1 \in Q[x]$ which implies that $Q(\omega)$ is the splitting field of $x^n - 1$, If $E = Q(\omega)$, then E is a Galois extension of Q as $x^n - 1$ is a separable polynomial . Since G(E/Q) is a cyclic group by known theorem, we have E is cyclic extension of Q.

Example 2 : All finite extensions of finite fields are separable. Thus the splitting field E of a polynomial f(x) over a finite field F is a Galois extension. By known theorem, we have G(E/F) is cyclic. Thus all the splitting fields over finite fields are cyclic extensions.

14.2.2 Proposition: Let F be a field of non-zero characteristic p. Then for every positive integer k the mapping π_k of F into itself, defined by $\pi_k(x) = x^{p^k}$ for all elements $x \in F$ is an embedding of F into itself. (The mapping $\pi_k(x) = x^{p^k}$ is called Frobenius endomorphism).

Proof: Given that F is a field of characteristic $p \neq 0$.

Let k be a positive integer.

Define a mapping $\pi_k: F \to F$ by $\pi_k(x) = x^{p^k}$, $\forall\, x \in F$.

Now we show that π_k is an embedding.

Let $x, y \in F$.

Then $\pi_k(x + y) = (x + y)^{p^k} = x^{p^k} + y^{p^k} = \pi_k(x) + \pi_k(y)$ and

$\pi_k(x.\, y) = (x.y)^{p^k} = x^{p^k}.\, y^{p^k} = \pi_k(x)\, .\pi_k(y)$

Therefore $\pi_k: F \to F$ is homomorphism

Let $x, y \in F$ be such that $\pi_k(x) = \pi_k(y)$.

$\Longrightarrow x^{p^k} = y^{p^k}$

$\Longrightarrow (x - y)^{p^k} = x^{p^k} - y^{p^k} = 0$

$\Longrightarrow x = y$

Therefore π_k is one-one

Hence π_k is an embedding of F into itself.

14.2.3 Lemma: Let E be a finite extension of F. Suppose $f: G \to E^*$ where $E^* = E - \{0\}$ has the property that $f(\sigma\eta) = \sigma(f(\eta))\, f(\sigma)$, $\forall \sigma, \eta \in G$. Then there exists $\alpha \in E^*$ such that $f(\sigma) = \sigma(\alpha^{-1})\, \alpha$, $\forall \sigma \in G$ (The mapping f in the hypothesis of this lemma is called a crossed homomorphism).

Proof: Given that E is a finite extension of F and $E^* = E - \{0\}$ be the multiplicative group of non-zero elements and f is a mapping from G to E^* such that $f(\sigma\eta) = \sigma(f(\eta))\, f(\sigma)$, $\forall \sigma, \eta \in G$.

By known theorem, we have $|G(E/F)| \leq [E:F]$

Consider, $\sum_{\sigma \in G} f(\sigma)\sigma(a)$, $\forall a \in F$

If $\sum_{\sigma \in G} f(\sigma)\sigma(a) = 0$, $\forall a \in F$ then by a known theorem, $f(\sigma) = 0$, which is a contradiction to $f(\sigma) \in E^*$

Therefore $\sum_{\sigma \in G} f(\sigma)\sigma(a) \neq 0$, for some $a \in F$

Put $\alpha = \sum_{\sigma \in G} f(\sigma)\sigma(a)$. Let $\eta \in G$.

Now $\eta(\alpha)$

$= \eta(\sum_{\sigma \in G} f(\sigma)\sigma(a))$

$= \sum_{\sigma \in G} \eta\,(f(\sigma))\eta(\sigma(a))$ [$\because f(\sigma\eta) = \sigma(f(\eta))\, f(\sigma), f(\eta\sigma) = \eta(f(\sigma))\, f(\eta) \Rightarrow f(\eta\sigma)(f(\eta))^{-1} = \eta(f(\sigma))$]

$= \sum_{\sigma\in G} f(\eta\sigma)\,(f(\eta))^{-1}\,\eta(\sigma(a))$ $[\because \{\eta\sigma/\sigma \in G\} = \{\sigma/\sigma \in G\}]$

$= \sum_{\sigma\in G} f(\sigma)\,(f(\eta))^{-1}\sigma(a)$

$= (f(\eta))^{-1} \sum_{\sigma\in G} f(\sigma)\ \sigma(a)$

$= (f(\eta))^{-1}\,\alpha$

Thus $\eta(\alpha) = (f(\eta))^{-1}\,\alpha$

$\Rightarrow \eta(\alpha) f(\eta) = \alpha$

$\Rightarrow f(\eta) = (\eta(\alpha))^{-1}\,\alpha = \eta(\alpha^{-1})\alpha.$

Therefore $f(\eta) = \eta(\alpha^{-1})\alpha$, $\forall \eta \in G$

14.2.4 Lemma: (Special Case of Hilbert's Problem 90):

Let E be a finite extension of F and let G = G(E/F) be a cyclic group of order n generated by σ. If $\omega \in$ E is such that $\omega.\ \sigma(\omega).\ \sigma^2(\omega)\ldots\sigma^{n-1}(\omega) = 1$, then there exists $\alpha \in E^*$ such that $\omega = \sigma(\alpha)\alpha^{-1}$.

Proof: Given that E is a finite extension of F and G = G(E/F) is a cyclic group of order n generated by σ .

Let $\omega \in$ E be such that $\omega.\ \sigma(\omega).\ \sigma^2(\omega)\ldots\sigma^{n-1}(\omega) = 1$

Let $G = \{ I = \sigma^n, \sigma^{n-1}, \ldots\ldots..\sigma^2, \sigma\}$

Define a mapping $f: G \to E^*$ by $f(I) = 1$, $f(\sigma) = \omega$, $f(\sigma^i) = \sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots\ \sigma(\omega)\ \omega$ for i = 2,3….n-1.

Now we show that this mapping f is a crossed homomorphism.

Let $\sigma^i, \sigma^j \in G$ for $1 \le i, j \le n$

Case(i) : Suppose that $i + j \equiv 0 \bmod n$ i.e, $i + j = n\,q$ i.e., i + j is a multiple of n

Now $f(\sigma^i\sigma^j) = f(\sigma^{i+j}) = f(\sigma^n) = f(I) = 1$

Consider $f(\sigma^i)\sigma^i\,(f(\sigma^j))$

$= (\sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots\ \sigma(\omega)\ \omega)\sigma^i(\sigma^{j-1}(\omega)\sigma^{j-2}(\omega)\ldots\ldots\ldots\ \sigma(\omega)\ \omega)$

$= \sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots\ \sigma(\omega)\ \omega\sigma^{i+j-1}(\omega)\sigma^{i+j-2}(\omega)\ldots\ldots\ldots\ \sigma^{i+1}(\omega)\sigma^i(\omega)$

$= \sigma^{i+j-1}(\omega)\sigma^{i+j-2}(\omega)\ldots\ldots\ldots\ \sigma^{i+1}(\omega)\ \sigma^i(\omega)\sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots\ \sigma(\omega)\ \omega$

$= f(\sigma^{i+j})$

$= f(\sigma^n)$

$= f(I)$

$= 1$

Therefore $f(\sigma^i\sigma^j) = f(\sigma^i)\sigma^i\,(f(\sigma^j))$

Case (ii): Suppose $\sigma^i, \sigma^j \in G$ be such that i +j is not a multiple of n.

Then i + j = nq+r where r < n

Here $f(\sigma^i\sigma^j) = f(\sigma^{i+j}) = f(\sigma^{nq+r}) = f(\sigma^{nq}\ \sigma^r) = f((\sigma^n)^q\sigma^r) = f((I)^q\sigma^r) = f(\sigma^r)$

$= \sigma^{r-1}(\omega)\sigma^{r-2}(\omega)\ldots\ldots\ldots \sigma(\omega)\ \omega$

So $f(\sigma^i)\sigma^i\ (f(\sigma^j))$

$= (\sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots \sigma(\omega)\ \omega)\sigma^i(\sigma^{j-1}(\omega)\sigma^{j-2}(\omega)\ldots\ldots\ldots \sigma(\omega)\ \omega)$

$= \sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots \sigma(\omega)\ \omega\sigma^{i+j-1}(\omega)\sigma^{i+j-2}(\omega)\ldots\ldots\ldots \sigma^{i+1}(\omega)\ \sigma^i(\omega)$

$= \sigma^{i+j-1}(\omega)\sigma^{i+j-2}(\omega)\ldots\ldots\ldots \sigma^{i+1}(\omega)\ \sigma^i(\omega)\sigma^{i-1}(\omega)\sigma^{i-2}(\omega)\ldots\ldots\ldots \sigma(\omega)\ \omega$

$= \sigma^{r-1}(\omega)\sigma^{r-2}(\omega)\ldots\ldots\ldots \sigma(\omega)\ \omega$ as $\sigma^{i+j} = \sigma^{n\,q+r} = (\sigma^n)^q\sigma^r = (I)^q\sigma^r = \sigma^r$

Therefore $f(\sigma^i\sigma^j) = f(\sigma^i)\sigma^i\ (f(\sigma^j))$

Hence f is a crossed homomorphism.

By lemma 14.2.3, there exists $\alpha \in E^*$ such that $f(\sigma) = \sigma(\alpha^{-1})\ \alpha$

$\therefore \omega = \sigma(\alpha)\alpha^{-1}$ (By def $f(\sigma) = \omega$. Since $\alpha \in E^*$, E^* is a field, we have α^{-1}exists and we can replace α^{-1} by α & α by α^{-1})

Hence Proved.

14.2.5 Theorem: Let F contain a primitive n^{th} root ω of unity. Then the following are equivalent.

(i) E is a finite cyclic extension of degree n over F

(ii) E is the splitting field of a irreducible polynomial $x^n - b \in F[x]$. Further more note E = $F[\alpha]$ where α is a root of $x^n - b$

Proof: Given that the field F contains a primitive n^{th} root ω of unity.

Assume (i) i.e, Suppose that E is a finite cyclic extension of degree n over F

By def., of cyclic extension, we have E is a Galois Extension of F and G(E/F) is a cyclic group.

Since E is finite extension, it implies [E:F] = n(say).

Since G(E/F) is a cyclic group, we have G = G(E/F) = (σ) i.e., G is generated by $\sigma \in G$

By known theorem, we have $|G(E/F)|$ = [E:F] = n and F is the fixed field of G(E/F).

Since $\omega \in F$, $\sigma \in G$ we have $\sigma(\omega) = \omega$

Therefore $\omega.\ \sigma(\omega).\ \sigma^2(\omega)\ldots\ldots\sigma^{n-1}(\omega) = \omega.\ \omega\ldots\omega = \omega^n = 1$

By lemma 14.2.4, there exists $\alpha \in E^*$ such that $\omega = \sigma(\alpha)\alpha^{-1}$

Therefore $\sigma(\alpha) = \omega\alpha$

$\Rightarrow \sigma^i(\alpha) = \omega^i\alpha$ (1)

Now $\sigma(\alpha^n) = (\sigma(\alpha)^n) = (\omega\alpha)^n = \omega^n\alpha^n = \alpha^n$($\because\omega^n = 1$)

Therefore $\sigma^i(\alpha^n) = \alpha^n$; $\forall$i = 1,2,….n

So each element in G is fixing α^n $\therefore$ $\alpha^n \in$ F.

Put b = α^n.

Consider the polynomial f(x) = x^n – b$\in$ F[x].

Let g(x) be a monic irreducible factor of the polynomial f(x) in F[x]

Now α, ωα, $\omega^2\alpha$, ……$\omega^{n-1}(\alpha)$ are the n distinct roots of the polynomial f(x)

Suppose $\omega^i\alpha$ is a root of g(x), where i = 0, 1,…, n-1

Suppose 0 ≤ j ≤ n-1

Consider $\sigma^{j-i}(\omega^i\alpha) = \omega^i\omega^{j-i}\alpha$ (from(1))

$= \omega^j\alpha$ [we know that ω ∈ F . So $\omega^i \in$ F, $\sigma^{j-i}(\omega^i) = \omega$]

We have $\sigma^{j-i}(\omega^i\alpha) = \omega^j\alpha$; ∀ i = 0,1,2,….n-1.

i.e., If $\omega^i\alpha$ is a root of g(x) ∈ F[x] then $\sigma^{j-i}(\omega^i\alpha)$ is also a root of g(x).

Therefore α, ωα, $\omega^2\alpha$, ……$\omega^{n-1}(\alpha)$ are all the roots of g(x) and deg g(x) = deg f(x) = n

So, f(x) = g(x) .μ, where μ is a unit in F

Since g(x) is irreducible over F, we have f(x) is also irreducible over F

Therefore F(α, ωα, $\omega^2\alpha$, ……$\omega^{n-1}(\alpha)$) is the splitting field of f(x) over F

Clearly F ⊆F(α) ⊆ E and n = [E:F] = [E:F(α)][F(α):F] = [E:F(α)] n

⇒[E:F(α)] = 1.

Therefore E = F(α) .

So, E is the splitting filed of f(x) over F

Assume (ii) i.e., E is the splitting filed of an irreducible polynomial f(x) = x^n – b$\in$ F[x]

We show that E is a finite cyclic extension of F of degree n.

Let c ∈ E be a root of f(x). So, b = c^n

Then c, ωc, $\omega^2\alpha$, ……ω^{n-1}c are n-distinct roots of f(x) in E [$\because\omega$ is primitive n^{th} root of unity]. Since deg f(x) = n, we have f(x) is separable over F.

So F(c) = F(c, ωc, $\omega^2\alpha$, ……ω^{n-1}c) is the splitting field of f(x) over F and hence it is normal extension of F.

Therefore E = F(c) and [E:F] = [F(c):F] = n

Since the minimal polynomial of c is separable over F, we have c is separable over F

Therefore E is finite separable normal extension of F.

i.e, E is a Galois extension of F and $|G(E/F)|$ = [E:F] = n

Now it remains to show that G(E/F) is cyclic.

For this we show that $\phi : G(E/F) \longrightarrow Z/< n>$ is an isomorphism.

We know that $Z/< n>$ is cyclic group of order n under addition

Let $\sigma \in G(E/F)$.

Since c is a root of f(x), we have $\sigma(c)$ is also a root of f(x) and $\sigma(c) = \omega^i c$; $0 \leq i \leq n-1$

Define $\phi : G(E/F) \longrightarrow Z/< n> = \{0+(n), 1+(n),.....(n-1)+(n)\}$ by $\phi(\sigma) = i + (n)$ where $0 \leq i \leq n-1$

Now we show that ϕ is homomorphism, one-one and onto

Let $\sigma_1, \sigma_2 \in G(E/F)$ and $\sigma_1(c) = \omega^i c$, $\sigma_2(c) = \omega^j c$, $0 \leq i,j \leq n-1$ and $i + j = n\,q + r$;

where $q,r \in Z$ and $0 \leq r < n-1$

Then $(\sigma_1\sigma_2)(c) = \sigma_1(\sigma_2(c)) = \sigma_1(\omega^j c) = \omega^j \sigma_1(c) = \omega^j(\omega^i c) = \omega^{j+i} c$

Now $\phi(\sigma_1\sigma_2) = r + n = i+j+(n)$ $(\because\ i +j +(n) = nq +r +(n) = r +(n))$

$= (i +(n)) + (j +(n))$

$= \phi(\sigma_1) + \phi(\sigma_2)$

Therefore ϕ is homomorphism

Suppose $\phi(\sigma_1) = \phi(\sigma_2)$

$\Rightarrow i +(n) = j +(n)$

$\Rightarrow \quad i \quad = \quad j$

$\Rightarrow \omega^i c \quad = \omega^j c$

$\Rightarrow \sigma_1(c) \ = \sigma_2(c)$

$\Rightarrow \sigma_1 \quad = \sigma_2$

$\therefore$ ϕ is one – one

Since $|G(E/F)| = |Z/< n >| = n$, we have ϕ is onto.

Since $Z/< n >$ is cyclic group, we have $G(E/F)$ is cyclic.

Therefore E is cyclic extension of F

Hence (ii) $\Rightarrow$ (i) is proved.

14.3 SUMMARY:

A cyclic extension of fields is a special type of field extension where the associated Galois group is a cyclic group**,** meaning it is generated by a single automorphism. In such extensions, the group of automorphisms has a simple and well-understood structure, making cyclic extensions an important concept in Galois theory. Cyclic extensions help describe how fields can be expanded by adjoining roots of polynomials, with the symmetry of these extensions captured by the cyclic structure of their Galois groups. They also demonstrate the link between field extensions and group theory, which is central to modern algebra. The study of cyclic extensions focuses on their construction, properties, and how they relate to the

solvability of polynomial equations. They play a key role in understanding radical extensions and are fundamental in applications such as the classification of intermediate fields.

14.4 TECHNICAL TERMS:

- Galois Group: Let F be a field and f(x) ∈ F[x] and K be the splitting field of f(x) over F then $G(K/\mathrm{F})$ is called the Galois group of f(x) over F.
- Cyclic Group**:** A group G generated by a single element, denoted by ⟨g⟩.
- Cyclic Extension**:** A Galois extension whose Galois group is cyclic.
- Normal Extension: An extension E of F where every irreducible polynomial in F[x] that has a root in E splits into linear factors in E.
- Separable Extension: An extension E of a field F is a called a separable extension if each element of E is separable.
- Splitting Field: Let f(x) be a polynomial over a field F. A splitting field of f(x) over F is an extension field K of F such that f(x) splits into linear factors over K and K is generated over F by the roots of f(x).

14.5 SELF- ASSESSMENT QUESTIONS:

Q1. What is a cyclic extension?
Answer: A field extension E of a field F is called a cyclic extension if it is a Galois extension of F and G(E/F) is a cyclic group.
Q2. When is a polynomial solvable by radicals in terms of cyclic extensions?
Answer: A polynomial is solvable by radicals if its splitting field can be obtained by a tower of cyclic extensions, i.e., a sequence of field extensions where each intermediate extension is cyclic and corresponds to extracting radicals.
Q3. Is every Galois extension a cyclic extension? Justify.
Answer: No. A Galois extension E of F is cyclic only if G(E/F) is a cyclic group. Many Galois extensions E of F have the groups G(E/F) which are non-cyclic, such as the Klein four-group.
Q4. What condition must a finite field extension E of F satisfy to be a cyclic extension of degree n?
Answer: Extension field E of F must be a normal and separable extension (i.e., Galois), and the group G(E/F) must be cyclic of order n.

14.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Dr. J.L Rama Prasad**

LESSON- 15

POLYNOMIALS SOLVABLE BY RADICALS

OBJECTIVES:

- To understand the concept of solving polynomial equations using radicals.
- To explore conditions under which a polynomial is solvable by radicals.
- To learn about radical extensions and their relation to field extensions.
- To study the connection between solvability by radicals and the Galois group structure.
- To apply Galois theory to determine the solvability of polynomials.

STRUCTURE:

15.1 INTRODUCTION :

The study of polynomials solvable by radicals investigates the conditions under which the roots of a polynomial can be expressed using basic arithmetic operations and radical expressions involving nth roots. Historically, mathematicians sought general formulas for solving polynomial, succeeded for degrees two, three, and four. However, the general and higher-degree equations are not solvable by radicals in most cases. This realization led to the development of Galois theory, which examines how the symmetries of roots, encapsulated in the Galois group determine solvability. A key aspect of this topic is the concept of radical extensions, where a field is built by successively adjoining radical elements. Polynomials solvable by radicals correspond to extensions whose Galois groups are solvable, reflecting a deep interplay between group theory and field theory. In this lesson we find necessary and sufficient condition for a polynomial over a field F to be solvable by radicals using the fundamental theorem of Galois theory. Also, we construct a polynomial of degree 5 that is not solvable by radicals.

15.2 DEFINITIONS AND NOTATIONS:

15.2.1 Definition: An extension E of a field F is called an extension by radical or radical extension if there exists elements $\alpha_1, \alpha_2, \ldots\ldots\alpha_n \in E$ and positive integers $n_1, n_2, \ldots\ldots, n_r$ such that $E = F(\alpha_1, \alpha_2, \ldots\ldots\alpha_r)$; $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \alpha_2, \ldots\ldots\alpha_{i-1})$; $1 \leq i \leq r$.

Example: 1. $Q(2^{1/3})$ is a radical extension of Q. Also $Q(2^{1/3}, 3^{1/5})$ is a radical extension of Q.

Note: If E is a radical extension of F, then there exists a sequence of fields $F = E_0 \subseteq E_1 \subseteq \ldots\ldots\ldots \subseteq E_r = E$ such that for every i, $E_i = E_{i-1}(\alpha_i)$ for some $\alpha_i \in E_i$ with the property that $\alpha_i^{n_i} \in E_{i-1}$ for some positive integer $n_i \geq 1$

15.2.2 Result: If E_r is a radical extension of $F= E_0$ with intermediate fields $E_1, E_2, \ldots\ldots. E_{r-1}$(written in ascending order) then there exists radical extension E'_s of $F = E_0$ with intermediate fields $E'_1, E'_2, \ldots\ldots E'_{s-1}$,(written in ascending order) such that

(i) $E'_s \supseteq E_r$

(ii) E'_s is a normal extension of F and

(iii) E'_i is a splitting filed of a polynomial of the form $x^{m_i} - b_i \in E'_{i-1}[x]$ for all i = 1,2….s.

15.2.3 Note: If E is a radical extension of F, then E is a finite algebraic extension of F.

Verification: By definition, for each i, $E_i = E_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in E_{i-1}$ which implies that α_i is a root of the polynomial $x_i^{n_i} - \alpha_i^{n_i} \in E_{i-1}[x]$ and hence E_i is an algebraic extension of E_{i-1} and $[E_i:E_{i-1}]$ is finite for all i. Therefore $[E:F] = [E_r:E_{r-1}] \ldots\ldots..[E_2:E_1][E_1:F]$ is finite and E is a finite algebraic extension of F.

15.2.4 Note : A polynomial $f(x) \in F[x]$ is solvable by radicals if we can obtain every root of f(x) by using a finite sequence of operations of addition, subtraction, multiplication, division and taking n^{th} roots starting with elements of F.

Notation: In this section, we consider only the fields of characteristic zero unless otherwise stated.

15.2.5 Result: Suppose n is a positive integer, and the field F contains all the n^{th} roots of unity, and K is the splitting field of $x^n - a \in F[x]$, then

(i) $K = F(\lambda)$, λ is any root of $x^n - a$

(ii) The Galois group G(K/F) is abelian.

15.2.6 Defnition: The subgroup G' generated by the set of all commutators $aba^{-1}b^{-1}$ in a group G is called the derived group of G, $a, b \in G$. For any positive integer n, the n^{th} derived group of G is denoted by $G^{(n)}$ and is defined as follows $G^{(1)} = G', G^{(n)} = (G^{(n-1)})', n > 1$

15.2.7 Defnition: A group G is said to be solvable if $G^{(k)} = \{e\}$ for some positive integer, where $G^{(k)}$ is the k^{th} derived group of G.

Example: Every abelian group is solvable.

15.2.8 Normal Series: A sequence $\{ G_0, G_1, \ldots\ldots G_r\}$ of subgroups of a group G is called normal series of a group G if $\{e\} = G_0 \lhd G_1 \lhd \ldots\ldots \lhd G_r = G$. The factors of normal series are $G_i/G_{i-1} \forall\ i = 1,2,\ldots..r$.

15.2.9 Composition Series: A composition series of a group G is a normal series $G_0, G_1, \ldots\ldots G_r$ without repetition whose factors G_i/G_{i-1} are simple groups. The factors G_i/G_{i-1} are called composition factors of G.

15.2.10 Note:

1. Every finite group has a composition series
2. A group G is solvable $\Leftrightarrow$ G has a normal series with abelian factors.
3. A finite group is solvable $\Leftrightarrow$ its composition factors are cyclic groups of prime orders,
4. Any subgroup of a solvable group is solvable.

15.3 POLYNOMIALS SOLVABLE BY RADICALS:

15.3.1 Theorem: Let E be the splitting field of $x^n - a \in F[x]$, then G(E/F) is a solvable group.

Proof:

Case(i): Suppose F contains a primitive n^{th} root of unity.

Then we can take the primitive n^{th} root as a generator of the group of all the n^{th} roots of unity, and hence F contains all the n^{th} roots of unity.

Let α be a root of $x^n - a$.

Since E is the splitting field of $x^n - a$, we have $E = F(\alpha)$ and G(E/F) is abelian

So, G(E/F) is solvable. (Since Every abelian group is solvable)

Case(ii) :Suppose F does not contain any primitive n^{th} root of unity.

Let ω be a primitive n^{th} root of unity in $\bar{F}$, $\bar{E} = \bar{F}$.

Then $\omega \notin F$ which implies $F \subseteq F(\omega)$ and $F(\omega)$ is the splitting field of $x^n - 1$.

Let b be a root of $x^n - a$ (i.e., $b^n = a$).

This implies bω is also a root of $x^n - a$ and hence $b\omega \in E$

So $b^{-1}(b\omega) \in E$. i.e, $\omega \in E$.

Consider the sequence of fields $F \subseteq F(\omega) \subseteq E$.

Since $F(\omega)$ is the splitting filed of $x^n - 1 \in F[x]$, we have $F(\omega)$ is a normal extension of F.

So, $G(E/F(\omega))$ is a normal extension of G(E/F) (∵ By fundamental theorem of Galois Theory)

∴ $\{e\} \lhd G(E/F(\omega)) \lhd G(E/F)$ is a normal series of the group G(E/F)

Since F(ω) contains a primitive n^{th} root of unity, we have G(E/F(ω)) is abelian. (1)

By Fundamental Theorem of Galois Theory, we have $\frac{G(E/F)}{G(E/F(\omega))} \cong G(F(\omega)/F)$ and

By known theorem, we have $G(F(\omega)/F) \cong (Z/(n))^*$, which is abelian

Therefore $\frac{G(E/F)}{G(E/F(\omega))}$ is abelian. (2)

So the normal series $\{e\} \lhd G(E/F(\omega)) \lhd G(E/F)$ of the group G(E/F) has abelian factors. Hence the group G(E/F) is solvable.

15.3.2 Theorem: A polynomial $f(x) \in F[x]$ is solvable by radicals $\Leftrightarrow$ its splitting field E over F has solvable galois group G(E/F).

Proof: Let $f(x) \in F[x]$ be a polynomial and E be the splitting field of f(x)

Then G = G(E/F) is the Galois group of f(x).

Suppose that the Galois group G(E/F) is solvable.

Now we show that f(x) is solvable by radicals over F.

Since the characteristic of F is 0 and E is the splitting field of f(x) over F, we have that E is finite separable and normal extension of F.

Therefore |G(E/F)| = [E:F] = n (say) and G = G(E/F) is a finite solvable group.

Case-(i): Suppose F contains a primitive n^{th} root of unity.

Since G is a finite solvable group, there exists a sequence, $G = G_0 \supseteq G_1 \supseteq \ldots\ldots\ldots \supseteq G_r = \{e\}$ of subgroups of G such that $G_i \lhd G_{i-1}$ and $\frac{G_{i-1}}{G_i}$ is cyclic, for each i.

By Fundamental Theorem of Galois Theory, there exists subfields $F_0, F_1, \ldots\ldots\ldots F_r$ of E such that $F = E_0 \subseteq E_1 \subseteq \ldots\ldots\ldots \subseteq E_r = E$, $F_i = E_{G_i}$ and $G(E/F_i) = G_i \; \forall$ i

We know that $G_1 = G(E/F_1) \lhd G(E/F) = G$.

This implies that F_1 is a normal extension of F

Now E can be regarded as the splitting field of f(x) over F_1.

So E is a finite normal extension of F_1.

Then $G_2 \lhd G_1$ implies that F_2 is a normal extension of F_1.

Continuing this way, since G_i is a normal subgroup of G_{i-1}, we can show F_i is a normal extension of F_{i-1} and also $\frac{G(E/F_{i-1})}{G(E/F_i)} \cong G(F_i/F_{i-1})$ (By Fundamental Theorem of Galois Theory)

$\Rightarrow \frac{G_{i-1}}{G_i} \cong G(F_i/F_{i-1})$

$\Rightarrow G(F_i/F_{i-1})$ is a cyclic group $(\because \frac{G_{i-1}}{G_i}$ is a cyclic group)

Therefore F_i is a cyclic extension of $F_{i-1}$and we also know that F_{i-1} contains a primitive n^{th} root of unity.

By known result, F_i is the splitting filed of an irreducible polynomial $x^{n_i} - b_i$ i.e., $\alpha_i^{n_i} = b_i \in F_{i-1}$ This is true for every i =1,2,…..r

Thus there exists elements $\alpha_1, \alpha_2, \ldots\ldots\alpha_n \in E$ and positive integers $n_1,n_2,\ldots\ldots,n_r \ni E = F(\alpha_1, \alpha_2, \ldots\ldots\alpha_r)$; $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F_{i-1} = F(\alpha_1, \alpha_2, \ldots\ldots\alpha_{i-1})$

Therefore E is radical extension of F. So, the splitting field E of f(x) is contained in the radical extension of F.

So, f(x) is solvable by radicals over F.

Case-(ii): Suppose F contains no primitive n^{th} root of unity.

Let ω be a primitive n^{th} root of unity in $\overline{E}$.

Then E(ω) is the splitting field of f(x), where f(x) is regarded as an element of F(ω)[x]

Define $\psi : G(E(\omega)/F(\omega)) \longrightarrow G(E/F)$ as follows:

Let $\sigma \in G(E(\omega)/F(\omega))$.

Then σ is an automorphism of E(ω) that keeps every element of F(ω) fixed.

Let σ_0 be the restriction of σ to E.

Since E is a normal extension of F, we have σ_0 is an automorphism of E that keeps every element of F fixed. So, $\sigma_0 \in G(E/F)$

Define $\psi : G(E(\omega)/F(\omega)) \longrightarrow G(E/F)$ as $\psi(\sigma_0) = \sigma_0$.

Then ψ is a monomorphism.

Therefore $G(E(\omega)/F(\omega)) \cong \psi(G(E(\omega)/F(\omega))) \subseteq G(E/F)$

This implies $G(E(\omega)/F(\omega)) \cong$ solvable group ($\because$ Any subgroup of a solvable group is solvable)

Therefore G(E(ω) /F(ω)) is solvable

i.e, E(ω) is the splitting field of $f(x) \in F(\omega)[x]$ and F(ω) contains a primitive n^{th} root of unity such that G(E(ω) /F(ω)) is solvable.

So by case-(i), E(ω) is a radical extension of F(ω), hence E(ω) is a radical extension of F.

In this case, the splitting field is contained in the radical extension E(ω) of F.

Therefore f(x) is solvable by radicals over F.

Converse:

Suppose that f(x) is solvable by radicals over F.

Then its splitting field E is contained in some radical extension E_r of F.

By Result 15.2.2, without loss of generality, we assume that $E \subseteq E_r$, E_r is a normal extension of F and there exists intermediate fields $E_0, E_1, \ldots\ldots, E_{r-1}$ such that each E_i is a splitting filed of a polynomial of the form $x^{n_i} - b_i \in E_{i-1}[x]$.

So E_i is a normal extension of E_{i-1} and $G(E_i/E_{i-1})$ is solvable for all i = 1 to r (*)

Since E_i is a normal extension of E_{i-1}, by fundamental theory of Galois theory, we have $G(E_r/E_i)$ is a normal subgroup of $G(E_i/E_{i-1})$ for all i

Therefore $\{e\} \subseteq G(E_r/E_{r-1}) \subseteq G(E_r/E_{r-2}) \subseteq \ldots\ldots\ldots\ldots \subseteq G(E_r/F)$ is a normal series of the group $G(E_r/F)$

Now we show that the factors of this normal series are solvable.

By Fundamental Theorem of Galois Theory, we have $\frac{G(E_r/E_{r-i})}{G(E_r/E_{r-i+1})} \cong G(E_{r-i+1})/E_{r-i})$

This implies $\frac{G(E_r/E_{r-i})}{G(E_r/E_{r-i+1})}$ is solvable for all i ($\because$ R.H.S is solvable by (*))

So $\{e\} \subseteq G(E_r/E_{r-1}) \subseteq G(E_r/E_{r-2}) \subseteq \ldots\ldots\ldots\ldots \subseteq G(E_r/F)$ is a normal series of the group $G(E_r/F)$ with solvable factors. i.e, $G(E_r/F)$ is solvable.

Further, $G(E/F) \cong \frac{G(E_r/F)}{G(E_r/E)}$, ($\because$ E is a normal extension of F) which implies that G(E/F) is the homomorphic image of $G(E_r/F)$.

Hence G(E/F) is solvable. (Since the homomorphic image of a solvable group is solvable)

15.3.3 Definition: A subgroup H of S_n is said to be a transitive permutation group if for all i,j $\in \{1,2,\ldots n\}$, there exists $\sigma \in H$ such that $\sigma(i) = j$.

Note: If p is a prime number and if a subgroup of S_p is a transitive group of permutations containing a transposition (a, b), then $G \cong S_p$

15.3.4 Theorem: Let f(x) be a polynomial over a field F with no multiple roots. Then f(x) is irreducible over F iff the Galois group G of F(x) is isomorphic to a transitive permutation group.

Proof : Suppose that $f(x) \in F[x]$ be a polynomial over a field F with no multiple roots and degree of f(x) is n.

Let $\alpha_1, \alpha_2, \ldots\ldots\ldots \alpha_n$ be the distinct roots of f(x) in some splitting field E and G be the Galois group of f(x).

For any $\sigma \in G$, we have $\sigma(\alpha_1), \sigma(\alpha_2), \ldots\ldots\ldots \sigma(\alpha_n)$ are also roots of f(x), which implies that $\{\alpha_1, \alpha_2, \ldots\ldots\ldots \alpha_n\} = \{\sigma(\alpha_1), \sigma(\alpha_2), \ldots\ldots\ldots \sigma(\alpha_n)$

So σ is a permutation on $\{\alpha_1, \alpha_2, \ldots\ldots\ldots \alpha_n\}$

Thus every element σ is a permutation on 'n' elements. So, we treat G as subgroup of S_n.

Suppose f(x) is irreducible over F

For each i = 1,2,……n; $F(\alpha_i) \cong \frac{F[x]}{<f(x)>}$ by an isomorphism which maps α_i to x +(f(x)) and $a \in F$ to a + (f(x)) .

So $F(\alpha_i)$ is isomorphic to $F(\alpha_j)$ by an isomorphism say η which maps α_i to α_j and $\eta(a) = a \; \forall \; a \; in$ F.

Since E is a normal extension of F, η can be extended to an F- automorphism η^*: E→E

Therefore $\eta^* \in G = G(E/F)$ and $\eta^*(\alpha_i) = \alpha_j$.

So for any α_i, α_j there exists $\sigma \in G$ such that $\sigma(\alpha_i) = \alpha_j$.

Therefore G is a transitive permutation group.

Converse:

Suppose that G is a transitive permutation group.

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

Now we show that all the roots of f(x) are roots of p(x).

Let α_i be a root of f(x).

Since G is a transitive permutation group, there exists $\sigma \in G$ such that $\sigma(\alpha_1) = \alpha_i$

Now $p(\alpha_i) = p(\sigma(\alpha_1)) = \sigma(p(\alpha_i)) = 0$ ($\because \sigma$is a homomorphism)

i.e, α_i is a root of p(x)

Therefore all the roots of f(x) are roots of p(x).

Since p(x) is a minimal polynomial of α_i, and $f(\alpha_1) = 0$, we have p(x)|f(x)

So f(x) = c p(x) for some c ∈ F

Therefore f(x) is irreducible.

15.3.5 Theorem: Let f(x) ∈ Q[x] be a monic irreducible polynomial over Q of degree p, where p is prime. If f(x) has exactly two non-real roots in ℂ, then the Galois group of f(x) is isomorphic to S_p.

Proof: Let E be the splitting field of f(x) over Q.

Then E ⊆ ℂ (Since f(x) has exactly two non real roots)

Since f(x) is irreducible, by Th. 15.3.4 the Galois group G(E/Q) of f(x) is isomorphic to a transitive permutation group which is a subgroup of S_p.

Let $\alpha_1, \alpha_2, \ldots\ldots\alpha_p$ be the roots of f(x).

Let α_i be a non-real root among these roots, which implies $\overline{\alpha_i}$ is also a root of f(x) ($\because$ f(x) ∈ Q[x])

So, $\overline{\alpha_i} = \alpha_j$ for some $j \neq i$; $1 \leq j \leq p$

Define $\sigma : E \to \overline{Q}$ as $\sigma(z) = \overline{z}$.

Then σ is an automorphism of E ($\because$ E is a normal extension of Q), which implies that $\sigma \in G(E/Q)$, $\sigma(\alpha_i) = \overline{\alpha_i} = \alpha_j$ and $\sigma(\alpha_j) = \overline{\alpha_j} = \alpha_i$.

Moreover $\sigma(\alpha_k) = \alpha_k \forall\ k \neq i, j$

Therefore σ is the transposition (α_i , α_j)

By using result after 15.3.3, we have $G \cong S_p$

15.4 SUMMARY:

This lesson focuses on determining when polynomial equation can be solved by expressing their roots using radicals and arithmetic operations. It explores radical extensions, fields created by adjoining successive roots, and examines how these connect to solvability. The key tool is Galois theory, which links the structure of the Galois group to the possibility of expressing roots in radicals. Specifically, a polynomial is solvable by radicals if and only if its Galois group is solvable. It also explains why general higher-degree polynomials are not solvable by radicals.

15.5 TECHNICAL TERMS:

- **Radicals**: Expressions involving roots (square roots, cube roots, etc.) used to represent solutions of polynomials.
- **Solvability by Radicals:** A property of a polynomial equation whose roots can be expressed using arithmetic operations and radical operations.
- **Radical Extension:** A field extension built by successively adjoining radicals.
- **Normal Extension**: An extension E of F where every irreducible polynomial in F[x] that has a root in E splits into linear factors in E.
- **Splitting Field:** Let f(x) be a polynomial over a field F. A splitting field of f(x) over F is an extension field K of F such that f(x) splits into linear factors over K and K is generated over F by the roots of f(x).

15.6 SELF-ASSESSMENT QUESTIONS:

Q1. What does it mean for a polynomial to be solvable by radicals?

Answer: A polynomial $f(x) \in F[x]$ is solvable by radicals if its roots can be expressed using a finite number of additions, subtractions, multiplications, divisions, and extractions of roots (radicals) starting from elements of the base field F.

Q2. How is solvability by radicals connected to Galois theory?

Answer: A polynomial is solvable by radicals if and only if its Galois group is a solvable group.

Q3. Give an example of a polynomial that is solvable by radicals.

Answer: The quadratic polynomial x^2-2 is solvable by radicals because its roots are $\pm\sqrt{2}$, which can be expressed using radicals over Q. Its Galois group over Q is of order 2 and hence solvable.

Q4. What role do radical extensions play in solving polynomials?

Answer: Radical extensions are field extensions formed by adjoining nth roots of elements. A polynomial is solvable by radicals if its splitting field can be obtained by a tower of radical extensions over the base field.

Q5: If an irreducible polynomial $p(x) \in F[x]$ over a field F has a root in a radical extension of F, then show that p(x) is solvable by radicals over F.

Answer: Suppose p(x) is an irreducible polynomial over a filed F and p(x) has a root in a radical extension E_r of F. By known result 15.2.2, there exists radical extension E_s^1 of F such that $E_r \subseteq E_s'$ and E_s' is a normal extension of F.

Given that p(x) has a root in E_r that implies p(x) has a root in E_s' and we know that E_s' is a normal extension of F. So, E_s' is the splitting field of p(x) ($\because$ By def. of normal extension)

Therefore the splitting field E_s' of p(x) is contained in some radical extension E_s' of F.

Hence p(x) is solvable by radicals.

Q6 : Show that polynomial $x^7 - 10x^5 + 15x + 5$ is not solvable by radicals over Q

Answer: Let $f(x) = x^7 - 10x^5 + 15x + 5$

By Eisenstein criterion, f(x) is irreducible over Q. Moreover by Descarte's rule of signs, we know that the number of positive real roots is $\leq$ the number of changes in signs in f(x) = 2 and the number of negative real roots is $\leq$ the number of changes in signs in f(-x) = 3

Therefore The number of real roots is ≤ 5

Moreover, by intermediate value theorem, f(x) has five real roots one in each of the intervals (-4,-3) (-2,-1) (-1,0) (1,2) and (3,4) . So f(x) has exactly two non-real roots.

By Theorem 15.3.5, the Galois group G of f(x) is isomorphic to S_7.

This implies that G is not solvable ($\because S_7$ is not solvable)

By Theorem 15.3.2, f(x) is not solvable by radicals over Q.

15.7 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- **Dr. J.L Rama Prasad**

LESSON- 16

SYMMETRIC FUNCTIONS

OBJECTIVES:

- To understand the definition and properties of symmetric functions
- To understand that every symmetric polynomial can be expressed as a polynomial in the elementary symmetric functions.
- To lay the groundwork for the study of Galois theory by examining the symmetries of the roots of polynomials.

STRUCTURE:

16.1 INTRODUCTION:

The concept of symmetric functions holds a central place in algebra, especially in the study of polynomial equations and field extensions. A symmetric function is a polynomial in several variables that remains unchanged under any permutation of those variables. This invariance property leads to rich algebraic structures and plays a pivotal role in understanding the relationships among the roots of a polynomial. Elementary symmetric functions, which sum products of variables taken a specific number at a time, form the backbone of this theory. Remarkably, any symmetric polynomial can be expressed as a polynomial in the elementary symmetric functions, a fact known as the fundamental theorem of symmetric functions. This result not only simplifies the study of polynomials but also connects algebraic properties to the roots of equations. The theory of symmetric functions provides a pathway which relate the coefficients of a polynomial to sums and products of its roots. This linkage serves as a bridge to field theory, where one explores how the symmetries of roots influence field extensions and automorphisms.

16.2 SYMMETRIC FUNCTIONS:

Let F be a field, and let $y_1 \dots \dots \dots \dots y_n$ be n indeterminates. Consider the field of rational functions $F(y_1, \dots \dots \dots \dots, y_n)$ over F. If σ is a permutation of {1, 2, 3, ……, n} i.e., $\sigma \in S_n$ then σ gives rise to a natural map $\bar{\sigma}$: $F(y_1 \dots \dots \dots \dots y_n) \rightarrow F(y_1 \dots \dots \dots \dots y_n)$ given by $\bar{\sigma}\left(\frac{f(y_1 \dots\dots\dots\dots y_n)}{g(y_1 \dots\dots\dots\dots y_n)}\right) = \frac{f(y_{\sigma(1)} \dots\dots\dots\dots y_{\sigma(1)})}{g(y_{\sigma(1)} \dots\dots\dots\dots y_{\sigma(1)})}$, where $f(y_1 \dots \dots \dots \dots y_n)$, $g(y_1 \dots \dots \dots \dots y_n) \in F[y_1 \dots \dots \dots \dots y_n]$ and $g(y_1 \dots \dots \dots y_n) \neq 0$.

Here $\bar{\sigma}$ is an automorphism of F($y_1 \dots \dots \dots \dots y_n$) having each element of F fixed.

16.2.1 Definition: An element f($y_1 \dots \dots \dots \dots y_n$) / g($y_1 \dots \dots \dots \dots y_n$) of F($y_1 \dots \dots \dots \dots y_n$) is called a symmetric function in $y_1, \dots \dots \dots \dots, y_n$ over F if it is left fixed by all permutations of 1,…..n, that is, $\forall \sigma \in S_n$, that is , $\bar{\sigma}\left(\frac{f(y_1 \dots\dots\dots y_n}{g(y_1 \dots\dots\dots y_n}\right) = \frac{f(y_1 \dots\dots\dots y_n)}{g(y_1 \dots\dots\dots y_n)}$ for all $\sigma \in S_n$.

Note: Let $\bar{S}_n$ be the group of all F-automorphisms $\bar{\sigma}$ of F($y_1 \dots \dots \dots \dots y_n$) corresponding to $\sigma \in S_n$. Clearly, $\bar{S}_n \simeq S_n$. Let K be the fixed field of $\bar{S}_n$.

Consider the polynomial f(x) $= \prod_{i=1}^{n}(x - y_i)$, Here f(x) $\in$F($y_1 \dots \dots \dots \dots y_n$)[x] .

Clearly the natural mapping F($y_1 \dots \dots \dots \dots y_n$)[x] $\rightarrow$F($y_1 \dots \dots \dots \dots y_n$)[x] induced by each $\bar{\sigma} \in \bar{S}_n$ leaves f(x) unaltered. Thus the coefficients are unaltered by each $\bar{\sigma} \in \bar{S}_n$. Hence, the coefficients lie in the fixed field K. Let us write the polynomial f(x) as $x^n + a_1x^{n-1} + a_2x^{n-2} +$ ……+ a_n, $a_i \in K$

16.2.2 Definition: If a_i is the coefficient of x^{n-i} in th polynomial f(x) = $\prod_{i=1}^{n}(x - y_i)$, then $(-1)^i a_i$ is called the i^{th} elementary symmetric function in $y_1 \dots \dots \dots \dots y_n$ and is denoted by s_i.

Thus $s_1 = y_1 + y_2 +$……+ y_n, $s_2 = y_1y_2 + y_1y_3 +$……+ $y_{n-1}y_n$, …….

… … … $s_n = y_1y_2 \dots \dots \dots \dots y_n$.

16.2.3 Theorem: Let s_1,……..s_n be the elementary symmetric functions in the indeterminates $y_1 \dots \dots \dots \dots y_n$. Then every symmetric function in $y_1 \dots \dots \dots \dots y_n$ over F is a rational function of the elementary symmetric functions. Also, F($y_1 \dots \dots \dots \dots y_n$) is a finite normal extension of F($s_1 \dots \dots \dots \dots s_n$) of degree n! and the Galois group of this extension is isomorphic to S_n.

Proof: Consider the field E = F($s_1 \dots \dots \dots \dots s_n$).

Since K is the field of all symmetric functions in $y_1 \dots \dots \dots \dots y_n$ over F, we have E $\subset$ K.

Since F($y_1 \dots \dots \dots \dots y_n$) is a splitting field of the polynomial f(x) = $\prod_{i=1}^{n}(x - y_i)$, of degree n over E, we have [F($y_1 \dots \dots \dots \dots y_n$): E] $\leq$ n! (1)

Also we have [F($y_1 \dots \dots \dots \dots y_n$): K] $\geq |\bar{S}_n|$ = n! (2)

Since E $\subset$ K, from (1) and (2) we have E = K.

Now F(x) is a separable polynomial over E, and F($y_1 \dots \dots \dots \dots y_n$) is its splitting field. Thus, F($y_1 \dots \dots \dots \dots y_n$) is a finite, separable, normal extension of E.

[F($y_1 \dots \dots \dots \dots y_n$): E] = |G(F($y_1 \dots \dots \dots \dots y_n$)/ E| (3)

Since G(F($y_1 \dots \dots \dots \dots y_n$)/ E) is embedded in S_n, and [F($y_1 \dots \dots \dots \dots y_n$): E] = n!, we have from(3), G(F($y_1 \dots \dots \dots \dots y_n$)/ E) $\simeq S_n$.

Finally, the fact K = E shows that every symmetric function can be expressed as a rational function of the elementary symmetric functions $s_1 \ldots\ldots\ldots\ldots s_n$.

16.2.4 Example: We express the following symmetric polynomials as rational functions of the elementary symmetric functions:

(a) $x_1^2 + x_2^2 + x_3^2$

(b) $(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$

Verification:

(a) $(x_1^2 + x_2^2 + x_3^2) = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = s_1^2 - 2s_2$,

where s_1 and s_2 are elementary symmetric functions of x_1, x_2 and x_3.

(b) By simple computation it can be checked that

$y_1 = x_1 - \frac{s_1}{3}$, $y_2 = x_2 - \frac{s_1}{3}$, $y_3 = x_3 - \frac{s_1}{3}$ are the roots of $x^3 + 3\alpha x + \beta = 0$,

Where $\alpha = -\frac{s_1^2}{3} + s_2$, $\beta = -s_3 - \frac{2s_1^3}{27} + \frac{s_1 s_2}{3}$

Then the cubic equation whose roots are $(y_1 - y_2)^2$, $(y_2 - y_3)^2$ and $(y_3 - y_1)^2$

is $(3\alpha + y)^3 + 9\alpha(3\alpha + y)^2 + 27\beta^2 = 0$ (1)

Here $(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = (y_1 - y_2)^2(y_2 - y_3)^2(y_3 - y_1)^2$

= product of all the roots of (1)

$= -27(\beta^2 + 4\alpha^3)$

where α and β are expressed in elementary symmetric functions

16.3 SUMMARY:

The topic of symmetric functions revolves around polynomials in several variables that remain unchanged under any permutation of these variables. These polynomials are called symmetric polynomials, and their study is crucial in understanding the relationship between a polynomial's coefficients and its roots. The elementary symmetric functions are constructed as sums of products of variables taken 1,2,…,n at a time. The fundamental theorem of symmetric polynomials states that any symmetric polynomial can be expressed as a polynomial in the elementary symmetric functions. This provides a powerful tool for rewriting complex symmetric expressions in a simpler, standardized form.

16.4 TECHNICAL TERMS:

- Symmetric Polynomial / Function: A polynomial $f(x_1,x_2,\ldots,x_n)$ that remains unchanged under any permutation of its variables.
- Degree of a Polynomial: The highest total degree of any term in the polynomial.
- Monic Polynomial: A polynomial where the leading coefficient (the coefficient of the highest degree term) is 1.
- Root of a Polynomial: A value of the variable that makes the polynomial equal to zero.

16.5 SELF-ASSESSMENT QUESTIONS:

Q1. Is the polynomial $x_1^2+x_2^2+x_3^2$ symmetric? Can it be expressed in terms of elementary symmetric polynomials?

Answer: Yes, $x_1^2+x_2^2+x_3^2$ is symmetric. It can be expressed in terms of elementary symmetric polynomials using the identity: $x_1^2+x_2^2+x_3^2 = s_1^2-2s_2$ where $s_1=x_1+x_2+x_3$ and $s_2=x_1x_2+x_1x_3+x_2x_3$.

Q2. What is the significance of symmetric functions in the theory of equations?

Answer: Symmetric functions play a crucial role in understanding the relationship between the roots and coefficients of a polynomial. According to Viète's formulas, the coefficients of a polynomial are (up to sign) the elementary symmetric functions of its roots. This helps in solving polynomials and studying their properties without explicitly finding the roots.

Q3. Is $x_1x_2+x_2x_3+x_3x_1$ a symmetric function?

Answer: Yes. The expression is symmetric because it remains unchanged under any permutation of x_1,x_2,x_3 . It is a symmetric polynomial of degree 2, and it equals the elementary symmetric function s_2 for 3 variables.

Q4. Can a non-symmetric polynomial be written in terms of elementary symmetric polynomials?

Answer: No, only symmetric polynomials can be expressed in terms of the elementary symmetric polynomials. Non-symmetric polynomials do not satisfy the invariance under variable permutations required for such a representation.

Q5. Give an example of a symmetric polynomial that is not elementary.

Answer: The polynomial $x_1^2x_2+x_2^2x_3+x_3^2x_1$ is symmetric in x_1,x_2,x_3, but it is not an elementary symmetric polynomial.

16.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

-

- **Dr. J.L Rama Prasad**

LESSON- 17

RULER AND COMPASS CONSTRUCTIONS

OBJECTIVES:

- To define constructible numbers as lengths that can be constructed from the unit segment using a finite sequence of ruler and compass operations.
- To explore the algebraic characterization of constructible numbers as elements of field extensions generated by square roots.
- To explain how each construction step corresponds to a quadratic field extension over the rationals.
- To demonstrate the limitations through the concept of irreducible polynomials and non-quadratic extensions.
- To understand how classical geometric constructions can be generalized using algebraic structures like fields and Galois theory.

STRUCTURE:

17.1 INTRODUCTION:

The study of geometric constructions using a ruler and compass dates back to the ancient Greeks, who sought to solve various problems using these simple tools. While these constructions appear purely geometric, they are deeply connected to algebra. By translating geometric steps into algebraic language, we can represent constructed points and lengths using algebraic numbers—specifically, numbers obtained by repeatedly taking square roots, starting from rational numbers. This algebraic approach reveals the limitations of ruler and compass constructions, explaining why certain classical problems, such as angle trisection and doubling the cube, are impossible with these tools. The theory of constructible numbers and field extensions provides a rigorous framework for understanding these limitations.This approach not only enhances our understanding of classical geometry but also bridges it with modern algebra and number theory, highlighting the power of algebra in solving geometrical problems. In this section, we see how to find the solutions to some geometric problems using the Galois Theory. Such problems are given below

(1) To construct by ruler and compass a square having the same area as that of a circle.
(2) To construct by ruler and compass a cube having twice the volume of a given cube.
(3) To trisect a given angle by ruler and compass.
(4) To construct by ruler and compass a regular polygon having n – sides.

Translation of the geometric problem into an algebraic problem:

Let R be the field of real numbers.

We consider the co-ordinate plane R^2. Suppose $P_0 \subset R^2$

Assume that P_0 has atleast two points then we construct an ascending chain of subsets P_i of R^2 for I = 0,1,….. inductively as follows.

Let A be the set of points obtained by intersection of

(i) two distinct circles each with its centre in P_i and passing through another point in P_i,

(or)

(ii) two distinct lines each passing through two distinct points in P_i, (or)

(iii) a line and a circle of the types described in (i) & (ii)

Let P_{i+1} be the union of P_i and A.

Suppose that the co-ordinates of points in P_0 belong to a subfield K of R.

Then the equation of the line passing through two distinct points in P_0 is $ax+by+ c = 0 \rightarrow (1)$; where a, b, c ∈ K and the equation of a circle with centre in P_0 and passing through another point in P_0 is $x^2 + y^2 +2gx + 2fy +d = 0 \longrightarrow (2)$, where g,f,d ∈ K

Therefore the co-ordinates of point of intersection of the two such lines of the form (1) lie in K. Also, the co-ordinates of point of intersection of line (1) and a circle (2) lie in $K(\sqrt{\alpha_1})$ where $\alpha_1>0$ and $\alpha_1 \in K$.

Again the co-ordinates of point of intersection of two distinct circles of the form (2) also lie in $K(\sqrt{\alpha_1})$ where $\alpha_1> 0$, $\alpha_1 \in K$.

In similar manner, the co-ordinates of the points in P_i lie in $K(\sqrt{\alpha_1} \ldots\ldots\ldots\ldots \sqrt{\alpha_i})$ where $\alpha_1, \alpha_2, \ldots\ldots\ldots\ldots \alpha_i > 0$, $\alpha_1 \in K$, $\alpha_2 \in K(\sqrt{\alpha_1})$, $\ldots\ldots\ldots\ldots \alpha_i \in K(\sqrt{\alpha_1} \ldots\ldots\ldots\ldots \sqrt{\alpha_{i-1}})$

So, A geometric problem can be translated into an algebraic problem.

17.2 CONSTRUCTIBLE NUMBERS:

17.2.1 Definition: A point x is constructible from P_0 if $x \in P_i$ for some $i \in \{0,1,2,\ldots..\}$

(a) A line L is constructible from P_0 if it passes through two distinct points in some P_i, $i \in \{0,1,2,\ldots..\}$

(b) A circle C is constructible from P_0, if its centre is in some P_i, and it passes through another point in P_i, $i \in \{0,1,2,\ldots..\}$

Note: If a point X or a line L or a circle C is constructible from Q×Q, then we say that the point X or the line L or the circle C is constructible.

17.2.2 Definition: A real number 'u' is constructible from Q if the point (u,0) is constructible from Q×Q, a subset of the plane R^2.

Note: If u ∈ R is constructible from Q, then there exists an ascending chain

$Q = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n$ of subfields $K_1, K_2, \ldots\ldots K_n$ of R such that

(i) $u \in K_n$

(ii) $K_i = K_{i-1}(\alpha_i)$; $0 \leq i \leq n$, $\alpha_i^2 \in K_{i-1}$

17.2.3 Theorem: Let u ∈ R be constructible from Q, then there exists a subfield K of R containing u such that $[K:Q] = 2^m$ for some positive integer m.

Proof: Since u∈ R is constructible from Q, we have (u,0) is constructible from Q×Q.

By definition, there exists an ascending chain $G = K_0 \subset K_1 \subset K_2 \subset \ldots\ldots\ldots \subset K_n$ such that u $\in K_n$ and $K_i = K_{i-1}(\alpha_i)$ for i = 1,2,…..n and $\alpha_i^2 \in K_{i-1}$ So, $[K_i : K_{i-1}] \leq 2$, i = 1, 2, ..., n

Therefore $[K:Q] = [K_n : Q] = [K_n : K_{n-1}]\,[K_{n-1} : K_{n-2}] \ldots\ldots\ldots [K_1 : K_0 = Q] = 2^m$; $m \leq n$

($\because$ $[K_i : K_{i-1}] \leq 2$) where m is some positive integer.

17.2.4 Lemma: The following are equivalent statements.

(i) $a \in R$ is a constructible from Q

(ii) $(a,0)$ is a constructible point from Q×Q

(iii) (a, a) is a constructible point from Q×Q

(iv) $(0, a)$ is a constructible point from Q×Q

Proof:

Assume (i) i.e., $a \in R$ is a constructible from Q

Then by def., we have $(a,0)$ is constructible from Q×Q.

Therefore (i) ⇒(ii)

Assume (ii) i.e., $(a,0)$ is a constructible point from Q×Q

Taking$(a,0)$ as centre and 'a' is radius, we can construct a circle $(x- a)^2 + y^2 = a^2$ and it passes through a constructible point (0,0).

Also the line x = y is constructible because it passes through the constructible points (0,0) and (1,1). Now the point (a, a) is a point of intersection of the circle and the line

So, (a, a) is a constructible point from Q×Q

Therefore (ii) ⇒(iii)

Assume (iii) i.e., (a, a) is a constructible point from Q×Q.

The circle $x^2 + y^2 = 2a^2$ is constructible because its centre (0,0) is constructible and the circle passing through constructible point (a, a).

Also the line y = -x is constructible, since it passes through two distinct constructible points (0,0) and (1,-1).

Now $(-a, a)$ is a point of intersection of the circle and the line.

Now $(0, a)$ is a constructible point which is the intersection of the line y = 1 which passes through two distinct constructible points $(-a, -a)$ and (a, a), x = 0

So, $(0, a)$ is a constructible point from Q×Q.

Therefore (iii) ⇒(iv)

Assume (iv) i.e., $(0, a)$ is a constructible point from Q×Q.

Then the line $y = a$ is constructible and the line x = 0 is constructible.

Now, the line y = -x is constructible, and hence we have the point $(a,0)$ is constructible .

So, the real number 'a' is constructible.

Therefore (iv) ⇒(i)

Note: A real number 'a' is constructible means that a is constructible from Q.

17.2.5 Lemma: If a is constructible number, then $x = a$ and $y = a$ are constructible lines.

Proof:

Case (i): Suppose $a = 0$.

Clearly x = 0 and y = 0 are constructible lines.

Case – (ii): Suppose $a \neq 0$

Then the line $x = a$ passes through two distinct constructible points $(a, 0)$ and $(-a, a)$.

Therefore $x = a$ is constructible.

Similarly $y = a$ is a line passing through two distinct constructible points (0, a) and (a, a) and hence y = a is a constructible line.

17.2.6 Lemma: If a and b are constructible numbers, then (a,b) is a constructible point.

Proof: By Lemma17.2.5, we have $x = a$ and y = b are constructible lines.

Clearly the point (a, b) is the intersection of the constructible lines $x = a$ and y = b.

Therefore the point (a, b) is constructible.

17.2.7 Lemma: If a and b are constructible numbers, then $a \pm b$ are also constructible.

Proof: Suppose a & b are constructible numbers.

Then by lemma 17.2.4, $(a, 0)$ is constructible.

So, the circle with centre $(a, 0)$ and radius 'b' i.e., $(x- a)^2 + y^2 = b^2$ is constructible.

Also, the line y = 0 is always constructible (∵ It is origin, it is always constructible).

Therefore the point of intersection of the line and the circle are $(a \pm b, 0)$ are constructible.

So, by lemma 17.2.4, we have $a \pm b$ are constructible numbers.

17.2.8 Lemma: If a and b are constructible numbers, then

(i) ab is constructible

(ii) a/b; $b \neq 0$ is constructible

Proof:

(i) Suppose a and b are constructible numbers.

Since b is constructible, by lemma 17.2.4, we have (0, b) is a constructible point.

Since b,1 are constructible numbers, by lemma 17.2.7, we have b-1 is constructible.

Since a, b-1 are constructible, we have $(a, b-1)$ is constructible (by lemma17.2.6)

The line passing through two constructible points (0, b) and $(a, b-1)$ is

$$y-b = \frac{b-1-b}{a-0}(x-0) \qquad \text{i.e.,} \quad ay - ab = -x$$

$$\text{i.e.,} \quad ay = -x + ab \longrightarrow (1) \text{ is constructible}$$

So, the intersection of constructible line (1) and the constructible line y = 0 is the point $(ab,0)$ which is also a constructible point.

Therefore by lemma 17.2.4, ab is constructible.

(ii) Suppose $b \neq 0$

Case-(i): If $a = 0$, then $\frac{a}{b} = 0$ which is always a constructible number.

Case-(ii): Suppose $a \neq 0$

Since b is constructible, we have 1 – b is constructible (by lemma 17.2.7)

So. $a(1 – b)$ is constructible (from part – i)

Now a is constructible which implies that (0, a) is a constructible (by lemma 17.2.4)

So a is constructible and $a(1 – b)$ is constructible.

This implies that (a, a(1-b)) is a constructible point (by lemma 17.2.6)

The line passing through two constructible points (0,b) and (a,b-1) is

$$y - a = \frac{a-ab-a}{a-0}(x - 0) \quad [\because \; y - y_1 = \frac{y_2-y_1}{x_2-x_1}(x - x_1)]$$

$$\text{i.e.,} \quad ay - a^2 = -abx$$

$$\text{i.e.,} \quad y - a = -bx \text{ (or) } bx = a - y \text{ is a constructible line} \qquad (2)$$

So, the intersection of the constructible line (2) with the constructible line y = 0 is the point $(\frac{a}{b}, 0)$ which is constructible.

Hence $\frac{a}{b}$ is constructible.

17.2.9 Lemma: If $a > 0$ is constructible, then $\sqrt{a}$ is constructible.

Proof:

Suppose a is constructible. Then $1 + a$ is constructible (by lemma 17.2.7)

Since $1+ a$ and $2 \neq 0$ are constructible numbers, we have by lemma 17.2.8, $\left(\frac{1+a}{2}\right)$ is a constructible number and by lemma 17.2.4 $\left(\frac{1+a}{2}, 0\right)$ is constructible point.

The circle with centre $\left(\frac{1+a}{2}, 0\right)$ and radius $\frac{1+a}{2}$ is $(x - \frac{1+a}{2})^2 + y^2 = (\frac{1+a}{2})^2$ is constructible (1)

But we know that x = 1 is a constructible line (by lemma 17.2.5)

Therefore the point of intersection of the constructible circle (1) and the constructible line x = 1 is $(1 \pm \sqrt{a})$

So, $(1 \pm \sqrt{a})$ is constructible point.

Since $(1, \sqrt{a})$ is constructible and a + 1 is constructible, the circle $(x-1)^2 + (y- \sqrt{a})^2 = a + 1$ is constructible. (2)

Clearly the point of intersection of constructible circle (2) and the constructible line x = 0 is $(-a,0)$ or $(0,2\sqrt{a})$ which is constructible point. So, by lemma 17.2.4 we have $2\sqrt{a}$ is constructible number.

Since $0 \neq 2$ is constructible, by lemma 17.2.8, $\frac{2\sqrt{a}}{2} = \sqrt{a}$ is constructible number.

17.2.10 Theorem: Let K be the subset of R consisting of numbers constructible from Q. Then K is a subfield containing square roots of all nonnegative numbers in K.

Proof: Let K be a subset of R consisting of numbers constructible from Q. Then by lemma 17.2.7 & 17.2.8 we have K is a subfield of constructible numbers. Also by lemma 17.2.9, K contains square roots of all non-negative numbers of K.

Therefore K is a subfield containing square roots of all non-negative numbers in K.

17.2.11: If $u \in K_m$, where $K_0 = Q \subset K_1 \subset K_2 \subset \ldots\ldots\ldots \subset K_m$ is an ascending chain of fields $K_i \ni [K_i : K_{i-1}] = 2$ then u is constructible. Equivalently if $[Q(u): Q] = 2^t$ for some $t > 0$ then u is constructible.

Proof: Let $u \in K_m$, and $K_0 = Q \subset K_1 \subset K_2 \subset \ldots\ldots\ldots \subset K_m$ is an ascending chain of fields K_i such that $[K_i : K_{i-1}] = 2$.

Since $K_0 \subset K_1 \subset K_2 \subset \ldots\ldots\ldots \subset K_n$, we have there exists $\alpha_1 \in K_1 - K_0$

So $K_1 = K_0(\alpha_1)$

Clearly $\alpha_1^2 \in K_0 = Q$

So, α_1^2 is constructible ($\because$ rationals are constructible)

By lemma 17.2.9, we have $\sqrt{\alpha_1^2} = \alpha_1$ is constructible.

Therefore $K_1 = K_0(\alpha_1)$ consists of constructible numbers.

Continuing this process we get K_m is a field of constructible numbers. Since $u \in K_m$, we have u is constructible.

17.2.12 Definition: An angle α is constructible by ruler and compass if the point (cosα, sinα) is constructible from Q×Q.

17.2.13 Proposition: The point (cosα, sinα) is constructible from Q×Q iff cosα is a constructible iff sinα is a constructible number

Proof :

Suppose that the point (cosα, sinα) is a constructible point.

First we show that cosα is a constructible number.

We know that the line y = 0 is always a constructible line and the circle $(x - \cos\alpha)^2 + (y - \sin\alpha)^2 = 1$ is constructible.

The point of intersection of this circle and the line y = 0 is (0,0) and (2cosα, 0) which are constructible points. So, (2cosα, 0) is constructible point.

By lemma 17.2.4, we have 2cosα is a constructible number.

Therefore $\frac{2\cos\alpha}{2}$ is a constructible number.

By lemma 17.2.8, cosα is constructible number.

Conversely, Suppose that cosα is a constructible number.

Then $\cos\alpha \cdot \cos\alpha = \cos^2\alpha$ is constructible.

Since 1 is a constructible number and $\cos^2\alpha$ is a constructible number, we have $(1 - \cos^2\alpha)$ is also constructible number.

By lemma 17.2.9, $\sqrt{(1 - \cos^2\alpha)} = \sin\alpha$ is constructible number, which implies (cosα,cosα), (sinα, sinα) are constructible points

Therefore x = cosα is a constructible line and y = sinα is a constructible line.

The point of intersection of these two constructible lines is (cosα, sinα) which is a constructible point.

17.3 SUMMARY:

The topic of Ruler and Compass Constructions explores how classical geometric constructions correspond to algebraic operations. Each construction using a straightedge and compass represents a point in the plane with coordinates satisfying certain algebraic equations. These constructed points correspond to numbers known as constructible numbers, which can be generated by starting with rational numbers and applying square roots successively. Algebraically, constructible numbers form a field extension of the rational numbers, built by adjoining square roots, and therefore correspond to extensions of degree a power of 2.This connection helps in understanding why some constructions, such as angle trisection or doubling the cube, are impossible: these involve solutions of cubic equations or higher degrees not solvable by square roots alone. Thus, constructions are limited to points whose coordinates can be expressed in terms of rational numbers and square roots.

17.4 TECHNICAL TERMS:

Constructible real numbers, Constructible line and Constructible circle.

17.5 SELF- ASSESSMENT QUESTIONS:

Problem of squaring a Circle: If we consider a circle with radius 1, then show that it is impossible to construct a square equal in area to the area of the circle.

Answer: Consider a circle with radius 1. Let 'a' be the side of a square whose area is equal to the area of the circle. So, $a^2 = \pi$

We know that π is not algebraic over Q.

Therefore a^2 is not algebraic over Q and hence a is not algebraic over Q.

So, $[Q(a) : Q] \neq 2^m$ for any $m \in Z^+$

By theorem 17.2.3, we have a is not constructible by ruler and compass.

Therefore we cannot construct a square whose area is π.

Problem of duplicating a Cube: Show that it is impossible to construct a cube with volume equal to twice the volume of a given cube by ruler and compass.

Answer : Assume that the side of the given cube is 1.

Let x be the side of the cube which should be constructed.

Let us suppose that $x^3 = 2.1^3$ i.e., $x^3 - 2 = 0$

Now $2^{1/3}$ is the real cube root of 2 which is a real root of the equation $x^3 - 2 = 0$

We know that the polynomial, $f(x) = x^3 - 2$ is irreducible over Q.

By known theorem, we have $[Q(2^{1/3}) : Q] = \deg f(x) = 3$, which is not a power of 2.

By Theorem 17.2.3, $2^{1/3}$ is not constructible from Q.

Therefore a cube with volume equal to twice the volume of a given cube cannot be constructed by ruler and compass.

Problem of Trisecting an Angle: Show that there exists an angle that cannot be trisected by ruler and compass.

Answer: Consider $\alpha = 60^0$ is the given angle.

Now we show that α cannot be trisected by ruler and compass.

Suppose if possible α is trisected by ruler and compass. i.e., the number $\cos 20^0$ is constructible number from Q. Put a = 2cos20.

We know that $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.

Therefore $(2\cos 20)^3 = 8\cos^3 20 = 2(4\cos^3 20) = 2(\cos 3.20 + 3\cos 20)$

i.e., $a^3 = 2\cos 60 + 3.2\cos 20$

$\Rightarrow a^3 = 2.\frac{1}{2} + 3a$

$\Rightarrow a^3 - 3a - 1 = 0$ (1)

So $f(x) = x^3 - 3x - 1 \in Q[x]$ and it is irreducible over Q.

From (1), a is a root of f(x).

Therefore $[Q(2^{1/3}) : Q] = \deg f(x) = 3 \neq 2^m$, for any positive integer.

By theorem 17.2.3, $a = 2\cos 20$ is not constructible.

Hence angle of 20^0 cannot be constructible by ruler and compass from Q

Problem of constructing a regular n-gon: Show that a regular n-gon is constructible (equivalently, the angle $\frac{2\pi}{n}$ is constructible) if and only if $\phi(n)$ is a power of 2.

Answer:

Let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, where ω is a primitive n^{th} root of unity.

Then $\bar{\omega} = \cos\frac{2\pi}{n} - i\sin\frac{2\pi}{n}$. So, $\omega + \bar{\omega} = 2\cos\frac{2\pi}{n}$.

Put $\cos\frac{2\pi}{n} = u$.

Since $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, we have $\omega - \cos\frac{2\pi}{n} = i\sin\frac{2\pi}{n}$

$\Rightarrow \left(\omega - \cos\frac{2\pi}{n}\right)^2 = -\sin^2\frac{2\pi}{n}$

$\Rightarrow \omega^2 - 2\omega\cos\frac{2\pi}{n} + \cos^2\frac{2\pi}{n} = -\sin^2\frac{2\pi}{n}$

$\Rightarrow \omega^2 - 2\omega\cos\frac{2\pi}{n} + \cos^2\frac{2\pi}{n} + \sin^2\frac{2\pi}{n} = 0$

$\Rightarrow \omega^2 - 2\omega\cos\frac{2\pi}{n} + 1 = 0$

Therefore ω satisfies the polynomial $f(x) = x^2 - \left(2\cos\frac{2\pi}{n}\right)x + 1 \in Q(u)[x]$.

Clearly the polynomial f(x) is irreducible over Q(u) and $[Q(\omega) : Q] = [Q(\omega) : Q(u)][Q(u) : Q]$

$\Rightarrow \phi(n) = 2.[Q(u) : Q]$

$\Rightarrow [Q(u) : Q] = \frac{\phi(n)}{2}$

Therefore u is constructible iff $\phi(n)$ is a power of 2

Question 1. What is the connection between ruler and compass constructions and field theory?

Answer: There is a deep algebraic connection: a point in the plane is constructible by ruler and compass if and only if its coordinates can be obtained from the rational numbers using a finite number of additions, subtractions, multiplications, divisions, and square roots. This means that constructible points lie in a field extension of Q of degree a power of 2.

Question 2. What does it mean for a number to be constructible?

Answer: A number is constructible if it can be represented as the coordinate (or distance) of a point that can be obtained through a finite sequence of ruler and compass constructions, starting from 0 on the real line.

Question 3. Can cube roots be obtained by ruler and compass constructions?

Answer: No. Cube roots generally cannot be obtained using only ruler and compass, because solving cubic equations requires constructing elements in field extensions of degree 3, which is not a power of 2.

Question 4. What is the field of constructible numbers?

Answer: The field of constructible numbers is the smallest subfield of R that contains Q and is closed under the operations of addition, subtraction, multiplication, division, and extraction of square roots. It contains all numbers that can be constructed using ruler and compass.

17.6 SUGGESTED READINGS:

1. Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. Basic Abstract Algebra, 2nd edition. UK: Cambridge University Press (Indian Edition).
2. Hungerford, Thomas W. Abstract Algebra, 1974, Springer-Verlag, New York
3. Khanna, V. K. and S. K. Bhambari. A Course in Abstract Algebra, 3rd edition. New Delhi: Vikas Publishing House Pvt. Ltd.
4. Lang, S. 1993. Algebra, 3rd edition. Boston: Addison-Wesley, Mass.
5. I.S. Luther and I.B.S.Passi, Algebra, Vol. IV-Field Theory, Narosa Publishing House,2012.
6. Ian Stewart, Galios Theory, Chapman and Hall/CRC, 2004.

- Dr. J.L Rama Prasad