SHIVAJI UNIVERSITY, KOLHAPUR

CENTRE FOR DISTANCE EDUCATION

Field Theory

(Mathematics)

For

M. Sc. Part-II : Semester-III

Paper (MT 302)

(Academic Year 2021-22 onwards)

UNIT - I

ALGEBRAIC EXTENSIONS OF FIELDS

1. INTRODUCTION

We have studied so far groups and rings in some detail and just touched fields as a special class of rings. Let us recall the definition of field, "A field is a commutative ring with unity in which every non-zero element has a multiplicative inverse". Now in this section we recall some basic definitions and results which are studied earlier.

Definition : A polynomial $P(x) \in F[x]$ is said to be irreduible over F, if $P(x)$ cannot be expressed as a product of two non-constant polynomials over F.

A polynomial $P(x) \in F[x]$ which is not irreduicible over F is called reducible over F.

Example : A polynomial $P(x) = x^2 + 1 \in \mathbb{R}[x]$ ($\mathbb{R}$ is field of reals) is irreducible over $\mathbb{R}$ but not over $\mathbb{C}$ ($\mathbb{C}$ is field of complex numbers) because $P(x) = x^2 + 1 = (x+i)(x-i)$ and $(x+i),(x-i) \notin \mathbb{R}[x]$ but $(x+i),(x-i) \in \mathbb{C}[x]$.

Definition : The polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$ in $\mathbb{Z}[x]$ ($\mathbb{Z}$ is set of integers) is said to be primitive if the greatest common divisor (g.c.d.) of $a_0, a_1, ..., a_n$ is 1.

Definition : A polynomial $a_0 + a_1x + ... + a_nx^n$ over a ring is called monic if $a_n = 1$.

Remark : By the definition of primitive polynomial it is obvious that every monic polynomial $f(x) \in \mathbb{Z}[x]$ is primitive.

Definition : Let F, E be fields such that $F \subseteq E$ and let $f(x) \in F[x]$. An element $\alpha \in E$ is said to be a root or a zero of $f(x)$ if $f(\alpha) = 0$.

We know that if F be a field and $F[x]$ be a ring of polynomials in x over F, then $F[x]$ has the following properties.

(i) $F[x]$ is an integral domain with unity and $F \subset F[x]$.

(ii) The division algorithm holds in $F[x]$.

i.e. if $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then $\exists$ unique $q(x), r(x) \in F[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

(iii) $F[x]$ is PID (Principal Ideal Domain).

(iv) $F[x]$ is UFD (Unique Factorization Domain).

(v) The units of $F[x]$ are non-zero elements of F.

(vi) A polynomial $P(x) \in F[x]$ is irreducible iff $\frac{F[x]}{\langle P(x) \rangle}$ is a field.

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

Proposition : Let $f(x) \in F[x]$ be a polynomial of degree greater than or equal to 2. Then $f(x)$ is reducible iff $f(x)$ has a root in F.

Lemma : If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive polynomials, then their product $f(x) \cdot g(x)$ is also primitive.

Lemma (Gauss) : Let $f(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x)$ is reducible over Q iff $f(x)$ is reducible over $\mathbb{Z}$.

Lemma : If $f(x) \in \mathbb{Z}[x]$ is reducible over Q, then it is also reducible over $\mathbb{Z}$.

Theorem (Eisenstein Criterion) : Let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, $n \geq 1$. If there is a prime 'P' such that $P^2 \nmid a_0$, $P \mid a_0$, $P \mid a_1, ..., P \mid a_{n-1}$ and $P \nmid a_n$, then $f(x)$ is irreducible over Q.

Example : $f(x) = x^2 - 2 \in \mathbb{Z}[x]$ is irreducible over Q. Because if we write $f(x) = 1 \cdot x^2 + 0 \cdot x - 2 = a_2 x^2 + a_1 x + a_0$ then $a_0 = -2$, $a_1 = 0$ and $a_2 = 1$.

If we choose prime P = 2, then $P^2 \nmid a_0$, $P \mid a_0$, $P \mid a_1$ and $P \nmid a_2$.

i.e. Eisenstein criterion holds for $f(x)$.

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

2. ADJUNCTION OF ROOTS

Definition : Extension Field :

If F is subfield of a field E, then E is called an extension of F.

Remarks :

1. If there is an embedding σ of a field F into a field E, then $F \cong \sigma(F)$ and hence we can regard F as a subfield of E or E is an extension of F.
2. We write $F \subseteq E$ when E is an extension of F.
3. Any field E can be considered as a vector space over any of its subfield.

Example : 1) The field Q of rationals is a subfield of the field $\mathbb{R}$ of reals and we say that $\mathbb{R}$ is an extension of Q.

2) The field $\mathbb{C}$ of complex numbers is an extension of the field $\mathbb{R}$ of reals.

Definition : If E is an extension of F, then the dimension of the vector space E over F is called the degree of E over F and is denoted by [E : F].

Note : If $[E:F] < \infty$ i.e. degree of E over F is finite, then E is called finite extension of F, otherwise E is called an infinite extension of F.

Example : $[\mathbb{C}:\mathbb{R}] = 2$ because the set $\{1, i\}$ forms a basis of $\mathbb{C}$ over $\mathbb{R}$.

Example : Let F be any field and $F[x]$ be a polynomial ring over F. Let E be the field of quotient of $F[x]$. Then E is field extension of F and an infinite set $\{1, x, x^2, ...\}$ is linearly independent subset of E which spans E.

$\therefore$ E is an infinite extension of F.

Example : For any field F; [F : F] = 1.

Since $F = \{1 \cdot a \mid a \in F\}$.

$\therefore$ $\{1\}$ will be the basis for F over F. Infact for $a \neq 0$ in F the singleton set $\{a\}$ will be the basis for F over F.

Conversely, if E is an extension of degree 1 of F then [E : F] = 1 = [F : F] and hence E = F.

Theorem (2.1) : Let $F \subseteq E \subseteq K$ be fields. If $[K:E] < \infty$ and $[E:F] < \infty$, then

1) $[K:F] < \infty$ and

2) $[K:F] = [K:E][E:F]$

Proof : Suppose that $[K:E]=m$ and $[E:F]=n$ let $\{v_1, v_2, ..., v_m\}$ be a basis of K over E and let $\{w_1, w_2, ..., w_n\}$ be a basis of E over F. Consider the set $B=\{v_i w_j \mid 1 \le i \le m, 1 \le j \le n\}$ of mn number of elements.

Claim : B is a basis of K over F.

i) B spans K over F :

For let $u \in K$ be any element.

Since $\{v_1, v_2, ..., v_m\}$ be a basis of K over E we write

$$u = \sum_{i=1}^{m} a_i v_i \; ; \; a_i \in E \text{ for each } i \qquad \text{.... (1)}$$

Now, since $\{w_1, w_2, ..., w_n\}$ be a basis of E over F and because $a_i \in E$, $1 \le i \le m$ we write

$$a_i = \sum_{j=1}^{n} b_{ij} w_j \; , \; b_{ij} \in F \; , \; 1 \le i \le m \qquad \text{..... (2)}$$

Substituting the expressions (2) into (1) we get

$$u = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} v_i w_j \; , \; b_{ij} \in F$$

i.e. $u = b_{11}v_1w_1 + b_{12}v_1w_2 + ... + b_{1n}v_1w_n + b_{21}v_2w_1 + b_{22}v_2w_2 + ... + b_{2n}v_2w_n$

$$+ ..... + b_{m1}v_mw_1 + b_{m2}v_mw_2 + ... + b_{mn}v_mw_n$$

But this shows that any element $u \in K$ can be written as a linear combination of elements of B with the elements $b_{ij} \in F$, $1 \le i \le m$, $1 \le j \le n$.

i.e. B spans K over F.

ii) B is linearly independent set over F :

Suppose that

$$c_{11}v_1w_1 + c_{12}v_1w_2 + ... + c_{1n}v_1w_n$$

$$+c_{21}v_2w_1 + c_{22}v_2w_2 + ... + c_{2n}v_2w_n + ...$$

$$+c_{m1}v_mw_1 + c_{m2}v_mw_2 + ... + c_{mn}v_mw_n = 0\ ,\ c_{ij} \in F$$

We write above expression by rearranging the terms as

$$\left(c_{11}w_1 + ... + c_{1n}w_n\right)v_1 + \left(c_{21}w_1 + ... + c_{2n}w_n\right)v_2 + ...$$

$$+\left(c_{m1}w_1 + ... + c_{mn}w_n\right)v_m = 0\ .$$

i.e. $\lambda_1v_1 + \lambda_2v_2 + ... + \lambda_mv_m = 0$

where $\lambda_i = c_{i1}w_1 + c_{i2}w_2 + ... + c_{in}w_n \in E$ for each $1 \le i \le m$, because $\{w_1, w_2, ..., w_n\}$ be a basis of E over F and $c_{ij} \in F$.

Now since $\{v_1, v_2, ..., v_m\}$ be a basis of K over E we must have $\lambda_i = 0$ for each $1 \le i \le m$.

i.e. $\lambda_i = c_{i1}w_1 + c_{i2}w_2 + ... + c_{in}w_n = 0$ for each $1 \le i \le m$

$\Rightarrow c_{ij} = 0\ ,\ 1 \le i \le m$ and $1 \le j \le n$.

($\because \{w_1, w_2, ..., w_n\}$ be a basis of E over F and $c_{ij} \in F$)

But this shows that B is linearly independent set over F.

Thus from (i) and (ii) the set $B = \{v_iw_j \mid 1 \le i \le m, 1 \le j \le n\}$, form a basis of K over F.

$\therefore$ 1) $[K : F] = mn < \infty$ and

2) $[K : F] = [K : E] \cdot [E : F]$

Example (2.6) : If $F \subseteq E \subseteq K$ be fields and $[K : F]$ is finite then $[K : E]$ and $[E : F]$ are divisors of $[K : F]$ since by theorem (2.1) $[K : F] = [K : E] \cdot [E : F]$.

Example 2.7 : If E is an extension field of F and $[E:F]$ is prime, prove that there are no fields properly between E and F.

Ans. : Let [E : F] = P (P is a prime number).

Suppose there is a field K such that $F \subseteq K \subseteq E$ then by theorem (2.1) $[E:F]=[E:K]\cdot[K:F]$.

$$\Rightarrow P=[E:K]\cdot[K:F] \qquad \text{..... (1)}$$

$\Rightarrow [E:K]$ divides P.

But P is a prime.

$\therefore [E:K]=1$ or P

i) If $[E:K]$ = 1 then E = K

ii) If [E : K] = P then [K : F] = 1 ($\because$ by (1))

$\Rightarrow K = F$

Thus if $F \subseteq K \subseteq E$ then either E = K or K = F i.e. there are no fields properly between F and E.

Theorem 2.2 : Let E and F be fields and let $\sigma : F \longrightarrow E$ 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 : Given that $\sigma : F \longrightarrow E$ be an embedding consider the set 'S' such that $|S| = |E - \sigma(F)|$ and $S \cap F = \phi$.

i.e. cardinality of S is same as cardinality of the compliment of σ (F) in E and S is disjoint with F.

Now, let $f : S \longrightarrow E - \sigma(F)$ be a one-one map and let $K = F \cup S$.

Define $\sigma^* : K \longrightarrow E$ by $\sigma^*(a) = \sigma(a)$ if $a \in F$ and $\sigma^*(a) = f(a)$ if $a \in S$.

Then σ^* is an extension of σ.

Since σ and f are 1 – 1 and $S \cap F = \phi$.

$\therefore$ σ^* is well defined, 1 – 1 and onto mapping.

Now for $x, y \in K$ define

$$x + y = (\sigma^*)^{-1}\left(\sigma^*(x) + \sigma^*(y)\right) \text{ and}$$

$$x \cdot y = (\sigma^*)^{-1}\left(\sigma^*(x) \cdot \sigma^*(y)\right)$$

Then above definitions of addition and multiplication coincide with the given addition and multiplication of elements of the field.

$\therefore$ F is a subfield of K and K is the desired field.

Theorem 2.3 : Let P (x) be an irreducible polynomial in F [x]. Then $\exists$ an extension E of F in which P (x) has a root.

Proof : Since $P(x) \in F[x]$ is irreducible polynomial.

$\therefore$ The ideal generated by P (x) i.e. $\langle P(x) \rangle$ in $F[x]$ is maximal ideal.

$\Rightarrow$ the quotient ring $\dfrac{F[x]}{\langle P(x) \rangle}$ is a field.

Let $E = \dfrac{F[x]}{\langle p(x) \rangle}$

Now define, $\sigma : F \longrightarrow \dfrac{F[x]}{\langle P(x) \rangle} = E$ by

$$\sigma(a) = a + \langle P(x) \rangle \text{ for } a \in F$$

Then σ is an embedding of F into $\dfrac{F[x]}{\langle P(x) \rangle}$ (prove it)

Thus we can regard $E = \dfrac{F[x]}{\langle P(x) \rangle}$ as an extension of F.

Let $P(x) = a_0 + a_1 x + ... + a_n x^n$, $n > 0$ and $a_i \in F$ then $x + \langle P(x) \rangle$ is a root of $P(x)$ in E.

(Since $P\left(x+\langle P(x)\rangle\right)=\sum_{i=0}^{n} a_i\left(x+\langle P(x)\rangle\right)^i$

$$=\sum_{i=0}^{n} a_i\left(x^i+\langle P(x)\rangle\right)$$

$$=\sum_{i=0}^{n} a_i x^i+\langle P(x)\rangle$$

$$=P(x)+\langle P(x)\rangle=\langle P(x)\rangle=0 \text{ in E.)}$$

Thus E is an extensionof F containing a root of $P(x)$.

Theorem 2.4 : 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

i) If $f(x)\in F[x]$ has a root in F then we take E = F.

ii) Suppose $f(x)\in F[x]$ has no root in F.

Let $P(x)$ be an irreducible factor of $f(x)$ in $F[x]$.

Define $E=\dfrac{F[x]}{\langle P(x)\rangle}$.

Then E is a field and it is an extension of F contains a root of $P(x)$.

($\because$ by theorem (2.3))

$\therefore$ E is an extension of F contains a root of $f(x)$ ($\because P(x)$ is a factor of $f(x)$. $\therefore$ root of $P(x)$ is also root of $f(x)$).

Thus $\exists$ an extension E of F that contains a root of non constant polynomial $f(x)\in F[x]$.

Remark : Let $P(x) \in F[x]$ be an irreducible polynomial having a root say 'u' in an extension E of F. The subfield denoted by $F(u)$ of E is the smallest subfield of E containing F and u and we call $F(u)$ the subfield of E generated by F and u.

Theorem 2.5 : 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

$$F[u] = \left\{ b_0 + b_1 u + ... + b_m u^m \in E \mid b_0 + b_1 x + ... + b_m x^m \in F[x] \right\}$$

(ii) If the degree of $P(x)$ is n, the set $\left\{1, u, ..., u^{n-1}\right\}$ forms a basis of $F(u)$ over F, i.e. each element of $F(u)$ can be written unuquely as $c_0 + c_1 u + ... + c_{n-1} u^{n-1}$ where $c_i \in F$ and $[F(u) : F] = n$.

Proof : Let $P(x) \in F[x]$ be an irreducible polynomial and let u be a root of $P(x)$ in an extension E of F.

Define a mapping,

$$\phi : F[x] \longrightarrow E \text{ by}$$

$$\phi\left(b_0 + b_1 x + ... + b_m x^m\right) = b_0 + b_1 u + ... + b_m u^m$$

$$\forall b_0 + b_1 x + ... + b_m x^m \in F[x]$$

Then ϕ is a homomorphism.

(Since for $f(x) = b_0 + b_1 x + ... + b_m x^m$, $g(x) = c_0 + c_1 x + ... + c_n x^n$ in $F[x]$ and assume that $m > n$.

Then

$$f(x) + g(x) = \left(b_0 + c_0\right) + \left(b_1 + c_1\right) x + ... + \left(b_n + c_n\right) x^n + b_{n+1} x^{n+1} + ... + b_m x^m \in F[x]$$

and

$$f(x) \cdot g(x) = \left(b_0 c_0\right) + \left(b_0 c_1 + b_1 c_0\right) x + \left(b_0 c_2 + b_1 c_1 + b_2 c_0\right) x^2 + ... + \left(b_m c_n\right) x^{m+n} \in F[x]$$

$\therefore$ (i) $\phi\big(f(x)+g(x)\big)=\big(b_0+c_0\big)+\big(b_1+c_1\big)u+....+\big(b_n+c_n\big)u^n+b_{n+1}u^{n+1}+....+b_mu^m$

$$=\big(b_0+b_1u+.....+b_mu^m\big)+\big(c_0+c_1u+.....+c_nu^n\big)$$

$$=\phi\big(f(x)\big)+\phi\big(g(x)\big)$$

and (ii) $\phi\big(f(x)\cdot g(x)\big)=\big(b_0c_0\big)+\big(b_0c_1+b_1c_0\big)u+\big(b_0c_2+b_1c_1+b_2c_0\big)u^2+....+\big(b_mc_n\big)u^{m+n}$

$$=\big(b_0+b_1u_1+....+b_mu^m\big)\cdot\big(c_0+c_1u+....+c_nu^n\big)$$

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

$\therefore$ By fundamental theorem of homomorphism.

$$\frac{F[x]}{\text{Ker }\phi}\cong \text{Im}\,\phi \qquad \text{..... (1)}$$

Now since u is root of $p(x)$.

$$\therefore p(u)=0\Rightarrow\phi\big(p(x)\big)=p(u)=0$$

$$\Rightarrow p(x)\in \text{Ker }\phi$$

$\therefore$ Ker ϕ is non-empty.

Claim : Ker $\phi=\langle p(x)\rangle$

Since $F[x]$ is a PID and as Ker ϕ is an ideal of $F[x]$.

$\therefore$ Ker $\phi=\langle g(x)\rangle$ for some $g(x)\in F[x]$.

But since $p(x)\in$ Ker ϕ.

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

$\Rightarrow h(x)\in F$; because $p(x)\in F[x]$ is an irreducible polynomial.

$\Rightarrow\langle g(x)\rangle=\langle p(x)\rangle$

$\therefore$ Ker $\phi=\langle p(x)\rangle$

$\therefore$ From (1)

$$\frac{F[x]}{\langle p(x)\rangle} \cong \text{Im}\,\phi = \left\{b_0 + b_1 u + ... + b_m u^m \in E \mid b_0 + b_1 x + ... + b_m x^m \in F[x]\right\}$$

$$= F[u]$$

$$\therefore \frac{F[x]}{\langle p(x)\rangle} \cong F[u]$$

But since $p(x)$ is an irreducible polynomial

$\therefore \dfrac{F[x]}{\langle p(x)\rangle}$ is a field.

$\therefore F[u]$ is a field and it is the smallest subfield of E containing F and u.

$\therefore F[u] = F(u)$ and

$$F[u] = \left\{b_0 + b_1 u + ... + b_m u^m \in E \mid b_0 + b_1 x + ... + b_m x^m \in F[x]\right\}$$

Now if $\deg\left(p(x)\right) = n$.

Let $p(x) = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n$; $b_n \neq 0$

Then $0 = p(u) = b_0 + b_1 u + b_2 u^2 + ... + b_n u^n$

(Since u is root of $p(x)$)

$\Rightarrow$ each of u^n, u^{n+1}, ... can be expressed in the form $b_0 + b_1 u + ... + b_{n-1} u^{n-1}$ with $b_i \in F$.

$$\therefore F[u] = F(u) = \left\{b_0 + b_1 u + ... + b_{n-1} u^{n-1} \mid b_i \in F\right\}$$

$\therefore$ The set $\left\{1, u, u^2, ... u^{n-1}\right\}$ forms a basis for $F(u)$ over F.

$$\therefore [F(u) : F] = n$$

Example 2.8 : Consider the irreducible polynomial $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

If u is a root of $p(x)$ in some extension K of $\mathbb{Z}_2$. Show that the subfield $\mathbb{Z}_2(u)$ of K has four elements.

Ans. : $\mathbb{Z}_2 = \{0,1\}$

By theorem (2.5)

$$\mathbb{Z}_2(u) = \{b_0 + b_1 u \mid b_i \in \mathbb{Z}_2\}$$

$$= \{0, u, 1, 1+u\}$$

The field $\mathbb{Z}_2(u)$ is the smallest subfield of K generated by $\mathbb{Z}_2$ and u and having four elements.

Example 2.9 : Show that $p(x) = x^2 - x - 1 \in \mathbb{Z}_3[x]$ is irreducible over $\mathbb{Z}_3$ and $\exists$ an extension K of $\mathbb{Z}_3$ with nine elements having all roots of $p(x)$.

Ans. : $\mathbb{Z}_3 = \{0,1,2\}$

Since $p(0) \neq 0$, $p(1) \neq 0$ and $p(2) \neq 0$.

$\therefore p(x) = x^2 - x - 1$ is irreducible over $\mathbb{Z}_3$.

$\therefore$ by theorem (2.5).

If u is root of $p(x)$ in some extension K of $\mathbb{Z}_3$ then

$$K = \{b_0 + b_1 u \mid b_i \in \mathbb{Z}_3\} = \{0,1,2,u,1+u,2+u,2u,1+2u,2+2u\}$$

is an extension of $\mathbb{Z}_3$ having nine elements and containing all the roots of $p(x)$.

3. Algebraic Extensions

Definition (3.1) : Let E be an extension of F. An element $\alpha \in E$ is said to be algebraic over F if α is a root of a non constant polynomial $p(x) \in F[x]$. i.e. an element $\alpha \in E$ is algebraic over F if $\exists$ a non constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Remarks :

1. If $\alpha \in E$ is not algebraic over F, then α is called transcendental over F.

2. For any field F, every element $\alpha \in F$ is algebraic over F, since $\exists$ a non constant polynomial $p(x) = (x - \alpha)$ in $F[x]$ such that $p(\alpha) = 0$.

Example 3.1 : (a) An element $\sqrt{3} \in \mathbb{R}$ (field of reals) is algebraic over Q (field of rationals) because $\exists$ a non constant polynomial $p(x) = x^2 - 3 \in Q[x]$ such that $p(\sqrt{3}) = 0$.

(b) The complex number $i = \sqrt{-1}$ is algebraic over Q, since $\exists$ a non constant polynomial $(x^2 + 1) \in Q[x]$ such that *i* is a root of $(x^2 + 1)$.

Theorem 3.1 : Let $F \subseteq E$ be fields and let $u \in E$ be algebraic 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 : (i) Suppose on the contrary $p(x) \in F[x]$ is reducible over F.

$\therefore p(x) = p_1(x) \cdot p_2(x)$ for some non constant polynomials $p_1(x)$, $p_2(x) \in F[x]$ and $\deg p_1(x) < \deg p(x)$, $\deg p_2(x) < \deg p(x)$.

Then $0 = p(u) = p_1(u) \cdot p_2(u)$.

$\Rightarrow p_1(u) = 0$ or $p_2(u) = 0$

$\Rightarrow u$ satisfies a polynomial of degree less than $\deg p(x)$.

a contradiction to the fact that $p(x) \in F[x]$ be a polynomial of least degree such that $p(u) = 0$.

$\therefore p(x)$ must be irreducible over F.

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

Then by division algorithm.

$g(x) = p(x) \cdot q(x) + r(x)$ for some $q(x)$, $r(x) \in F[x]$ where $r(x) = 0$ or $\deg r(x) < \deg p(x)$.

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

$\Rightarrow 0 = r(u)$ ..... $(\because p(u) = 0)$

But since $p(x) \in F[x]$ be a polynomial of least degree such that $p(u) = 0$.

$\therefore$ there does not exists $r(x) \in F[x]$ such that $\deg r(x) < \deg p(x)$ and $r(u) = 0$.

$\therefore r(x) = 0$

$\Rightarrow g(x) = p(x) \cdot q(x)$

$\Rightarrow p(x) \mid g(x)$

(iii) Let $g(x) \in F[x]$ be a monic polynomialof least degree such that $g(u) = 0$.

Then by (i) $g(x)$ is irreducible polynomial over F and by (ii) $p(x) \mid g(x)$ and $g(x) \mid p(x)$.

Since $p(x)$, $g(x) \in F[x]$ are monic and irreducible polynomials, we must have $p(x) = g(x)$.

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

Theorem 3.2 : Let $F \subseteq E$ be fields and $u \in E$ be algebraic over F, then $\exists$ a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(u) = 0$.

Proof : Consider the set $I = \{f(x) \in F[x] \mid f(u) = 0\}$

Then I is an ideal of the ring $F[x]$.

Since for $f(x) \in I$ and $g(x) \in F[x]$; $f(u) \cdot g(u) = 0$.

$\Rightarrow f(x) \cdot g(x) \in I$

Now since $F[x]$ is a PID

$\therefore I$ is principal ideal.

$\therefore \exists\, p(x) \in I$ such that

$I = \langle p(x) \rangle = \{ p(x) \cdot g(x) \mid g(x) \in F[x] \}$

We assume that $p(x)$ is monic polynomial in $F[x]$.

(Since if $p(x)$ is not monic i.e. $p(x) = a_0 + a_1 x + ... + a_n x^n$ with $a_n \neq 0$ and let $g(x) = a_n^{-1} a_0 + a_n^{-1} a_1 x + ... + a_n^{-1} a_n x^n$ then $p(x) = a_n g(x)$. This shows that $p(x)$ and $g(x)$ are associates in $F[x]$ hence $\langle p(x) \rangle = \langle g(x) \rangle$.)

$\therefore \langle p(x) \rangle = I = \{ f(x) \in F[x] \mid f(u) = 0 \}$

Since $u \in E$ is algebraic over F.

$\therefore \exists$ a nonconstant polynomial $f(x) \in F[x]$ such that $f(u) = 0$.

$\Rightarrow f(x) \in I = \langle p(x) \rangle$

$f(x) = p(x) \cdot g(x)$ for some $g(x) \in F[x]$.

$\therefore p(x)$ is a non constant polynomial with

$\deg(p(x)) \leq \deg(f(x))$, $\forall f(x) \in I$ and $f(x) \neq 0$ ..... (1)

$\Rightarrow p(x)$ is irreducible.

(If $p(x)$ is reducible then $p(x) = g(x) \cdot h(x)$ for some non constant polynomials $g(x), h(x) \in F[x]$ and

$0 = p(u) = g(u) \cdot h(u)$

$\Rightarrow g(u) = 0$ or $h(u) = 0$

$\Rightarrow g(x) \in I$ or $h(x) \in I$

But since $\deg\big(p(x)\big) = \deg\big(g(x)\big) + \deg\big(h(x)\big)$

and $\deg\big(g(x)\big) > 0$, $\deg\big(h(x)\big) > 0$

$\Rightarrow \deg\big(g(x)\big) < \deg\big(p(x)\big)$ and $\deg\big(h(x)\big) < \deg\big(p(x)\big)$

a contradiction to (1).)

Thus $\exists$ monic irreducible polynomial $p(x) \in F[x]$ such that $p(u) = 0$.

Uniqueness :

Let $p(x) = a_0 + a_1 x + \ldots\ldots + a_{n-1} x^{n-1} + x^n$ and

$q(x) = b_0 + b_1 x + \ldots\ldots + b_{m-1} x^{m-1} + x^m$ be two irreducible monic polynomials in $F[x]$ such that $p(u) = q(u) = 0$.

Then $q(x) \in I = \langle p(x) \rangle$.

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

But $q(x)$ is irreducible.

$\Rightarrow g(x)$ is a unit (i.e. $g(x) \in F$)

and hence $\deg\big(q(x)\big) = \deg\big(p(x)\big) = n$. i.e. $m = n$

Now $p(u) - q(u) = 0$

$\Rightarrow p(x) - q(x) \in I$

$\Rightarrow p(x) - q(x) = 0$ $\quad (\because \deg\big(p(x) - q(x)\big) < n$, $\deg p(x) = n$ and by (1))

$\Rightarrow p(x) = q(x)$.

Definition 3.2 : The monic irreducble polynomial in $F[x]$ of which u is a root will be called the minimal polynomial of u over F.

Example 3.2 : $Q \subseteq \mathbb{R}$ and $\sqrt{3} \in \mathbb{R}$ the polynomial $x^2 - 3 \in Q[x]$ is the minimal polynomial of $\sqrt{3}$.

Definition 3.3 : An extension field E of F is called algebraic if each element of E is algebraic over F.

Theorem 3.3 : If E is finite extension of F, then E is an algebraic extension of F.

Proof : Suppose E is finite extension of F.

Let $[E : F] = n$.

To prove that E is an algebraic extension of F.

Let $u \in E$ be any element.

$\therefore$ The set $\{1, u, ...u^n\}$ must be linearly dependent set of elements of E over F.

$\therefore \exists$ elements a_0, a_1,....., a_n (not all zero) in F such that

$$a_0 + a_1 u + a_2 u^2 + ... + a_n u^n = 0$$

$\Rightarrow u$ is root of a non constant polynomial

$$p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in F[x]$$

$\Rightarrow u$ is algebraic over F.

$\Rightarrow$ every element of E is algebraic over F.

Thus E is an algebraic extension of F.

Note : Converse of theorem (3.3) is not true i.e. an algebraic extension of a field F need not be a finite extension of F.

Example 3.3 : Let P_1, P_2, ..., P_r, ... be all distinct primes. Then for each $r \geq 0$ define $E_0 = Q$ and $E_r = E_{r-1}\left(\sqrt{P_r}\right)$ for all $r > 0$.

(i.e. $E_0 = Q$, $E_1 = E_0\left(\sqrt{P_1}\right) = Q\left(\sqrt{P_1}\right)$, $E_2 = E_1\left(\sqrt{P_2}\right) = Q\left(\sqrt{P_1}\right)\left(\sqrt{P_2}\right)$

$\therefore E_2 = Q\left(\sqrt{P_1}, \sqrt{P_2}\right)$, $E_3 = Q\left(\sqrt{P_1}, \sqrt{P_2}, \sqrt{P_3}\right)$, ...)

Then $E_r = Q\left(\sqrt{P_1}, \sqrt{P_2}, ..., \sqrt{P_r}\right)$ is the smallest subfield of $\mathbb{R}$ containing $Q \cup \left\{\sqrt{P_1}, \sqrt{P_2}, ..., \sqrt{P_r}\right\}$.

Now, we prove that $\sqrt{P_{r+1}} \notin E_r$, $\forall r \geq 0$ using induction on 'r'.

Since $\sqrt{P_1}$ is irrational $\Rightarrow \sqrt{P_1} \notin Q = E_0$

So for $r = 0$ result holds.

Assume that result is true for $r - 1$

i.e. assume that $\sqrt{P_r} \notin E_{r-1}$.

We prove that $\sqrt{P_{r+1}} \notin E_r$.

Let if possible $\sqrt{P_{r+1}} \in E_r$ then $\sqrt{P_{r+1}} = a + b\sqrt{P_r}$ for some $a, b \in E_{r-1}$.

$(\because E_r = E_{r-1}\left(\sqrt{P_r}\right))$

$\Rightarrow P_{r+1} = a^2 + 2ab\sqrt{P_r} + P_r b^2$

$\Rightarrow \sqrt{P_r} = \frac{1}{2ab}\left(P_{r+1} - a^2 - P_r b^2\right) \in E_{r-1}$

a contradiction to the assumption $\sqrt{P_r} \notin E_{r-1}$.

$\therefore \sqrt{P_{r+1}} \notin E_r$ for all r.

Hence $\left[E_{r+1} : E_r\right] = 2$ for all r.

and we get $Q = E_0 \subset E_1 \subset .... \subset E_r \subset ....$ is strictly ascending chain of subfields of $\mathbb{R}$.

Let $E = \bigcup_{i=0}^{\infty} E_i$, then $E = Q\left(\sqrt{P_1}, \sqrt{P_2}, ...\right)$ is the smallest subfield of $\mathbb{R}$ containing

$Q \cup \left\{\sqrt{P_1}, \sqrt{P_2}, ...\right\}$ and

$$\left[E_r : Q\right] = \left[E_r : E_0\right]$$

$$= \left[E_r : E_{r-1}\right] \cdot \left[E_{r-1} : E_{r-2}\right] ..... \left[E_1 : E_0\right]$$

$$= 2 \cdot 2 \cdot .....2 \quad (r \text{ times})$$

$$= 2^r$$

Also since each E_r is a subfield of E.

$\Rightarrow \left[E : Q\right]$ is infinite.

i.e. E is infinite extension of Q.

But E is an algebraic extension of Q for if $a \in E$ be any element.

Then $a \in E_r$ for some r.

i.e. $a \in E_r = Q\left(\sqrt{P_1}, \sqrt{P_2}, ..., \sqrt{P_r}\right)$ and $\left[E_r : Q\right] = 2^r$

$\therefore E_r$ is finite extension of Q.

$\therefore$ by theorem (3.3) E_r is an algebraic extension of Q.

$\therefore$ a is algebraic over Q.

$\therefore$ every element of E is algebraic over Q.

$\therefore$ E is an algebraic extension of Q.

Thus E is an algebraic extension of Q but not finite.

Remark : Extensions that are not algebraic are called transcendental extensions.

Theorem 3.4 : If E is an extension of F and $u \in E$ is algebraic over F, then $F(u)$ is an algebraic extension of F. x cannot be algebraic over F.

Proof : Let E is an extension of F and let $u \in E$ is algebraic over F, then by theorem (3.2) $\exists$ a minimal polynomial $p(x)$ of u over F.

Let $\deg\big(p(x)\big) = n$

Then by theorem (2.5) $\big[F(u) : F\big] = n$.

$\Rightarrow F(u)$ is finite extension of F.

$\therefore$ by theorem (3.3) $F(u)$ is an algebraic extension of F.

Definition 3.4 : An extension E of F is called finitely generated if $\exists$ a finite number of elements u_1, u_2, ..., u_r in E such that the smallest subfield of E containing F and $\{u_1, u_2, ..., u_r\}$ is E itself.

We then write $E = F\left(u_1, u_2, ..., u_r\right)$

Where $F\left(u_1, u_2, ..., u_i\right) = F\left(u_1, u_2, ..., u_{i-1}\right)\left(u_i\right)$

For each $1 < i \leq r$.

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

Example 3.4 : Let $F[x]$ be a polynomial ring over a field F in indeterminate x. Let E be the field of quotients of $F[x]$ then

$$E = \left\{ \frac{a_0 + a_1 x + ... + a_m x^m}{b_0 + b_1 x + ... + b_n x^n} / \, a_i, b_j \in F \text{ and not all } b_j\text{'s are zero} \right\}$$

i.e. $E = F(x)$.

Thus E is finitely generated extension of a field F but by definition of a polynomial ring x is algebraic over F.

$\therefore$ E is not an algebraic extension of F.

Theorem 3.5 : Let $E = F(u_1, u_2, ..., u_r)$ be a finitely generated extension of F such that each u_i; $i = 1, 2, ..., r$ is algebraic over F. Then E is finite over F and hence an algebraic extension of F.

Proof : We prove the theorem using induction on r. If $r = 1$ then by theorem (3.4) result holds.

Assume that the result is true for $r - 1$.

i.e. $\left[F(u_1, u_2, ..., u_{r-1}) : F\right]$ is finite.

Now since u_r is algebraic over F, it is algebraic over $F(u_1, u_2, ..., u_{r-1})$ also.

$\therefore$ by theorem (3.4).

$\left[F(u_1, u_2, ..., u_{r-1})(u_r) : F(u_1, u_2, ..., u_{r-1})\right]$ is finite.

i.e. $\left[F(u_1, u_2, ..., u_r) : F(u_1, u_2, ..., u_{r-1})\right]$ is finite.

$$\therefore [E : F] = \left[F(u_1, u_2, ..., u_r) : F\right]$$

$$= \left[F(u_1, u_2, ..., u_r) : F(u_1, u_2, ..., u_{r-1})\right] \cdot \left[F(u_1, u_2, ..., u_{r-1}) : F\right]$$

$$= (\text{finite}) \bullet (\text{finite})$$

$$= \text{finite}$$

Thus $[E : F]$ is finite.

i.e. E is finite extension of F and hence by theorem (3.3) an algebraic extension of F.

Theorem 3.6 : 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 : Here $K = \{u \in E / u \text{ is algebraic over F}\}$

Let $a, b \in K$ then by theorem (3.5) $F(a, b)$ is an algebraic extension of F.

Since $F(a, b)$ is a field, ab, $\frac{a}{b}$ (if $b \neq 0$) $\in F(a, b)$

$\therefore a \pm b$, ab, $\frac{a}{b}$ (if $b \neq 0$) are all algebraic over F.

$\Rightarrow a \pm b$, ab, $\frac{a}{b}$ $(b \neq 0) \in K$

$\Rightarrow K$ is subfield of E

and since every element of F is algebraic over F, every element of F is in K.

$\therefore$ K is an algebraic extension of F.

Definition 3.5 : Let K and L be extension fields of a field F. Then an embedding $\sigma : K \longrightarrow L$ such that $\sigma(a) = a$, $\forall a \in F$ is called an F-homomorphism of K into L or an embedding of K in L over F.

Theorem 3.7 : Let E be an algebraic extension of F and let $\sigma : E \longrightarrow E$ be an embedding of E into itself over F. Then σ is onto and hence an automorphism of E.

Proof : To prove σ is onto for let $a \in E$, we prove that $\exists$ an element $b \in E$ such that $\sigma(b) = a$.

Since E be an algebraic extension of F.

$\therefore$ a is algebraic over F.

Let $p(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} + x^n \in F[x]$ be the minimal polynomial of 'a' over F.

Let $a = u_1, u_2, ..., u_m \in E$ are roots of $p(x)$ then by theorem (3.5) $F(u_1, u_2, ..., u_m)$ is finite extension of F.

Since each u_i ; $1 \leq i \leq m$ is a root of $p(x)$ we have

$0 = p(u_i) = a_0 + a_1 u_i + ... + u_i^n$ for each i

$\Rightarrow \sigma(0) = \sigma\left(a_0 + a_1 u_i + ... + a_{n-1} u_i^{n-1} + u_i^n\right)$ for each i

$\Rightarrow 0 = \sigma(a_0) + \sigma(a_1)\cdot\sigma(u_i) + \ldots + \sigma(a_{n-1})\cdot\sigma(u_i^{n-1}) + \sigma(u_i^n)$ for each i

($\because \sigma$ is a homomorphism)

$\Rightarrow 0 = a_0 + a_1\sigma(u_i) + \ldots + a_{n-1}\left[\sigma(u_i)\right]^{n-1} + \left[\sigma(u_i)\right]^n$ for each i

[Since σ is F-homomorphism of E into itself

$\sigma(a_i) = a_i$, for each i.]

$\Rightarrow \sigma(u_i)$ is a root of $p(x)$ in E for each i, $1 \le i \le m$.

But since σ is $1-1$.

$\therefore \sigma(u_1)$, $\sigma(u_2)$, ..., $\sigma(u_m)$ must be same as u_1, u_2, ..., u_m in some order.

Now let $E' = F(u_1, u_2, \ldots, u_m)$

Then $\sigma(E') = \sigma\left(F(u_1, u_2, \ldots, u_m)\right)$

$\cong F\left(\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_m)\right)$

$= F(u_1, u_2, \ldots, u_m)$

$= E'$

i.e. $\sigma(E') \cong E'$

$\therefore [\sigma(E') : F] = [E' : F]$

$\Rightarrow \sigma(E') = E'$

and since $a = u_1 \in E'$, $\exists\ b \in E'$ such that $\sigma(b) = a \Rightarrow \sigma$ is onto.

$\therefore\ \sigma$ is an embedding (i.e. $1-1$, homomorphism) and onto.

$\therefore\ \sigma$ is an isomorpism of E onto E hence an automorphism of E.

Problem 3.1 : Let $F \subset K \subset E$ be three fields such that K is an algebraic extensionof F and $\alpha \in E$ is algebraic over K. Show that α is algebraic over F.

Ans. : $F \subset K \subset E$ be fields such that K is algebraic extension of F. $\alpha \in E$ is algebraic over K then $\exists$ a non-constant polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$ in $K[x]$ such that α is a root of $f(x)$.

Now let $L = F(a_0, a_1, ..., a_n)$, then $f(x) \in L[x]$ and hence α is algebraic over L.

Since K is algebraic extension of F.

$\therefore$ each a_i, $0 \le i \le n$ is algebraic over F.

$\therefore$ by theorem (3.5) L is finite and hence an algebraic extension of F.

i.e. $[L : F] < \infty$ ..... (1)

Since α is algebraic over L.

$\therefore$ by theorem (3.4) $L(\alpha)$ is a finite extension hence an algebraic extension of L.

$\therefore [L(\alpha) : L] < \infty$ ..... (2)

$\therefore$ By theorem (2.1)

$[L(\alpha) : F] = [L(\alpha) : L] \cdot [L : F] < \infty$ ($\because$ from (1) and (2))

$\therefore L(\alpha)$ is finite and hence an algebraic extension of F.

$\therefore \alpha \in L(\alpha)$ is algebraic over F.

Problem 3.2 : Prove that $\sqrt{2}$ is algebraic over Q. Find the degree of $Q(\sqrt{2})$ over Q.

Ans. : Since $p(x) = x^2 - 2$ be a non constant polynomial in $Q[x]$ such that $p(\sqrt{2}) = 0$.

$\therefore \sqrt{2}$ is algebraic over Q.

Now $p(x) = x^2 - 2 \in Q[x]$ be an irreducible polynomial such that $p(\sqrt{2}) = 0$ and $\sqrt{2} \in Q(\sqrt{2})$ an extension of Q.

$\therefore$ By theorem (2.5)

$\left[Q(\sqrt{2}):Q\right]=2$.

Problem 3.3 : Determine the minimal polynomial of $\sqrt{2}+5$ over Q.

Ans. : Let $u=\sqrt{2}+5$

$\Rightarrow (u-5)=\sqrt{2} \Rightarrow (u-5)^2=2$

$\Rightarrow u^2-10u+25=2$

$\Rightarrow u^2-10u+23=0$

The polynomial $p(x)=x^2-10x+23 \in Q[x]$ is monic irreducible polynomial such that $\sqrt{2}+5$ is the root of $p(x)$.

$\therefore p(x)=x^2-10x+23$ is the minimal polynomial of $\sqrt{2}+5$ over Q.

Problem 3.4 : Find a suitable number 'a' such that $Q\left(\sqrt{2},\sqrt{5}\right)=Q(a)$.

Ans. : Since $\sqrt{2}$, $\sqrt{5} \in Q\left(\sqrt{2},\sqrt{5}\right)$.

$\Rightarrow \sqrt{2}+\sqrt{5} \in Q\left(\sqrt{2},\sqrt{5}\right)$

$\Rightarrow Q\left(\sqrt{2}+\sqrt{5}\right) \subseteq Q\left(\sqrt{2},\sqrt{5}\right)$ ..... (1)

Now since $\left(\sqrt{2}+\sqrt{5}\right) \in Q\left(\sqrt{2}+\sqrt{5}\right)$

$\therefore \left(\sqrt{2}+\sqrt{5}\right)^3 \in Q\left(\sqrt{2}+\sqrt{5}\right)$

i.e. $2\sqrt{2}+5\sqrt{5}+6\sqrt{5}+15\sqrt{2} \in Q\left(\sqrt{2}+\sqrt{5}\right)$

i.e. $17\sqrt{2}+11\sqrt{5} \in Q\left(\sqrt{2}+\sqrt{5}\right)$

Now since $-11\left(\sqrt{2}+\sqrt{5}\right) \in Q\left(\sqrt{2}+\sqrt{5}\right)$

$$\therefore \frac{1}{6}\left[(17\sqrt{2}+11\sqrt{5})-11(\sqrt{2}+\sqrt{5})\right] \in Q(\sqrt{2}+\sqrt{5})$$

$$\Rightarrow \sqrt{2} \in Q(\sqrt{2}+\sqrt{5})$$

Now since $\sqrt{2}+\sqrt{5}$, $\sqrt{2} \in Q(\sqrt{2}+\sqrt{5})$

$$\therefore \ (\sqrt{2}+\sqrt{5})-\sqrt{2} \in Q(\sqrt{2}+\sqrt{5})$$

$$\Rightarrow \sqrt{5} \in Q(\sqrt{2}+\sqrt{5})$$

$\therefore$ both $\sqrt{2}, \sqrt{5} \in Q(\sqrt{2}+\sqrt{5})$

$$\Rightarrow Q(\sqrt{2},\sqrt{5}) \subseteq Q(\sqrt{2}+\sqrt{5}) \qquad \text{..... (2)}$$

Thus from (1) and (2) we write

$$Q(\sqrt{2},\sqrt{5}) = Q(\sqrt{2}+\sqrt{5})$$

$\therefore$ the suitable value of a is $(\sqrt{2}+\sqrt{5})$ so that $Q(\sqrt{2},\sqrt{5}) = Q(a)$.

Problem 3.5 : Let E be an extension of F and let $a, b \in E$ are algebraic over F. Suppose that the extensions $F(a)$ and $F(b)$ of F are of degree m and n respectively, where $(m,n)=1$ (i.e. m and n are relatively primes i.e. gcd (m,n) is 1). Then show that $\left[F(a,b):F\right] = m \cdot n$.

Ans. : Let $\left[F(a,b):F\right] = r$

$$r = \left[F(a,b):F\right] = \left[F(a,b):F(a)\right]\cdot\left[F(a):F\right]$$

$$\Rightarrow r = \left[F(a,b):F(a)\right]\cdot m \qquad \text{.....(1)}$$

$(\because \left[F(a):F\right] = m$ given)

$$\Rightarrow m / r$$

$\therefore r = pm$ for some positive integer p. ..... (i)

Similarly we can write

$$r = \left[F(a,b):F\right] = \left[F(a,b):F(b)\right]\cdot\left[F(b):F\right]$$

$\Rightarrow r = \left[F(a,b) : F(b)\right] \cdot n$ $\quad (\because \left[F(b) : F\right] = n$ given)

$\Rightarrow n / r$

$\therefore r = nq$ for some positive integer q. ..... (ii)

Since b is algebraic over F and $\left[F(b) : F\right] = n$.

$\therefore$ b satisfies an irreducible polynomialof degree n over F.

$\therefore$ b is algebraic over $F(a)$ and b may satisfy an irreducible polynomial of degree less than n over $F(a)$ i.e. $\left[F(a)(b) : F(a)\right]$ is atmost n.

i.e. b is algebraic over $F(a)$ and $\left[F(a,b) : F(a)\right] \leq n$.

$\therefore$ from (1)

$r \leq m \cdot n$ ..... (2)

If $r < m \cdot n$, then $r = pm < mn \Rightarrow p < n$ and $r = nq < mn \Rightarrow q < m$ (since from (i) and (ii)) and (i) $\div$ (ii) gives

$\frac{r}{r} = \frac{pm}{qn}$ with $p < n$ and $q < m$.

i.e. $\frac{q}{p} = \frac{m}{n}$ with $p < n$ and $q < m$.

$\Rightarrow m = q\alpha$ and $n = p\alpha$ for some positive integer $\alpha \neq 1$.

$\Rightarrow (m,n) = \alpha \neq 1$

a contradiction to $(m,n) = 1$.

$\therefore r < mn$ is not possible.

$\therefore r = mn$ $\quad (\because$ from (2))

$\therefore \left[F(a,b) : F\right] = m \cdot n$

Problem 3.6 : Let E be an extension field of F. If $a \in E$ has a minimal polynomial of odd degree over F, show that $F(a) = F(a^2)$.

Ans. : Since $a \in F(a)$

$\therefore a^2 \in F(a) \Rightarrow F(a^2) \subseteq F(a)$

$\therefore$ we write $F \subseteq F(a^2) \subseteq F(a)$

Let $\left[F(a^2) : F\right] = n$ and $\left[F(a) : F\right] = m$

Since the minimal polynomial of a over F is of odd degree.

$\therefore$ m is odd.

Now by theorem (2.1) $\left[F(a) : F\right] = \left[F(a) : F(a^2)\right] \cdot \left[F(a^2) : F\right]$

i.e. $m = \left[F(a) : F(a^2)\right] \cdot n$

$\Rightarrow n \leq m$ ..... (1)

Now let $f(x) = a_0 + a_1 x + ... + x^n$ be the minimal polynomial of a^2 over F

Then $a_0 + a_1 a^2 + ... + a^{2n} = 0$

$\Rightarrow a$ is root of the polynomial.

$g(x) = a_0 + a_1 x^2 + ... + x^{2n} \in F[x]$

$\Rightarrow m / 2n$ ($\because$ by theorem (3.1))

$\Rightarrow m / n$ ($\because$ m is odd)

$\Rightarrow m \leq n$ ..... (2)

$\therefore$ from (1) and (2)

$m = n$

$\therefore \left[F(a) : F\right] = m = n = \left[F(a^2) : F\right]$

$\therefore F(a) = F(a^2)$ ($\because F(a^2) \subseteq F(a)$)

4. Algebraically Closed Fields

Definition 4.1 : A field K is called algebraically closed if it possesses no proper algebraic extensions.

Theorem 4.1 : For any field K the following statements are all 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 atleast one root in K.

Proof : (i) $\Rightarrow$ (ii)

Suppose K is algebraically closed.

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

$\therefore$ by theorem (2.4) and (3.3) $\exists$ a finite and hence algebraic extension E of K such that $[E : K] = n$.

Since K is algebraically closed.

$\therefore E = K$, so $n = 1$.

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

(ii) $\Rightarrow$ (i)

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

To prove that K is algebraically closed.

For let E be any algebraic extension of K. ..... (1)

Let $a \in E$ be any element, then a is algebraic over K.

Let $p(x) \in K[x]$ be the minimal polynomialof a.

Since the minimal polynomial $p(x)$ of 'a' is monic and irreducible.

$\therefore p(x) = x - a$ ($\because$ by assumption)

$\Rightarrow a \in K$

$\Rightarrow E \subseteq K$

$\therefore$ E = K ($\because$ by (1))

$\Rightarrow K$ is algebraically closed field.

(ii) $\Rightarrow$ (iii)

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

$\therefore$ by (ii) $\Rightarrow$ (i) K is algebraically closed field.

Let $f(x) \in K[x]$ be any polynomial of positive degree.

Since K is algebraically closed field,

$\therefore$ K contains all the roots of $f(x)$.

$\therefore f(x)$ factors completely in $K[x]$ into linear factors.

(iii) $\Rightarrow$ (iv)

Suppose every polynomial in $K[x]$ of positive degree factors completely in $K[x]$ into linear factors.

Let $f(x) \in K[x]$ be any polynomial of positive degree.

$\Rightarrow f(x)$ factors completely in $K[x]$ into linear factors.

$\Rightarrow K$ contains all the roots of $f(x)$.

$\therefore$ K contains atleast one root of $f(x)$.

(iv) $\Rightarrow$ (i)

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

To prove that K is algebraically closed field.

Let E be an algebraic extension of K. ..... (2)

Let $a \in E$ be any element.

Then *a* is algebraic over K.

Let $p(x)$ be the minimal polynomial of '*a*' over K then $p(x) \in K[x]$.

and by assumption $p(x)$ has a root say '*b*' in K.

$\Rightarrow (x-b)$ is a factor of $p(x)$ in $K[x]$.

But since $p(x)$ is minimal polynomial of *a* over K.

$\therefore p(x)$ is monic, irreducible polynomial in $K[x]$.

Such that $p(a) = 0$.

$\Rightarrow p(x) = x - b$

and $p(a) = 0 = a - b \Rightarrow a = b \in K$

$\Rightarrow a \in K$

Thus K contains all elements of E.

i.e. $E \subseteq K$ ..... (3)

$\therefore$ from (2) and (3) K = E

Thus every algebraic extension of K coincides with K.

$\Rightarrow K$ is algebraically closed.

Definition 4.2 : If F is a subfield of a field E, then E is called an algebraic closure of F if,

(i) E is an algebraic extension of F.

(ii) E is algebraically closed.

Theorem 4.2 : Let F be a field and let $\sigma : F \longrightarrow L$ 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 $\eta : E \longrightarrow L$ and the number of such extensions is equal to the number of distinct roots of the minimal polynomial of α.

Proof : Let $p(x) = a_0 + a_1 x + ... + x^n$ be the minimal polynomial of α over F.

Let $p^{\sigma}(x) = \sigma(a_0) + \sigma(a_1)x + ... + x^n$

Then $p^{\sigma}(x) \in L[x]$

Since L is algebraically closed field.

$\therefore$ L contains all the roots of $p^{\sigma}(x)$.

Let $\beta \in L$ be a root of $p^{\sigma}(x)$.

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

$\therefore$ by theorem (2.5)

$E = F(\alpha) = \{b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} \mid b_i \in F\}$

Now, define $\eta_\beta : E \longrightarrow L$ by

$\eta_\beta(b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}) = \sigma(b_0) + \sigma(b_1)\beta + ... + \sigma(b_{n-1})\beta^{n-1}$

Since any element of $E = F(\alpha)$ can be written uniquely in the form

$b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1};\ b_i \in F$.

$\therefore \eta_\beta$ is well defined mapping. η_β is $1-1$ ($\because$ σ is 1–1)

Also it is easy to show that η_β is a homomosphism (prove it ?)

Thus η_β is an embedding of $F(\alpha)$ into L and it is an extension of σ .

($\because$ for $s \in F$; $\eta_\beta(s) = \sigma(s)$)

Further $\beta \longrightarrow \eta_\beta$ is a bijective correspondance between the distinct roots of $p^\sigma(x)$ and the extension of σ to E.

$\therefore$ The number of extensions of σ to E is equal to the number of distinct roots of $p^\sigma(x)$ in L.

Also if α is a root of $p(x)$ then $\sigma(\alpha)$ is a root of $p^\sigma(x)$. Thus number of distinct root of $p^\sigma(x)$ is same as number of distinct roots of $p(x)$. Here number of extensions of σ to E is equal to the number of distinct roots of $p(x)$.

Theorem 4.3 : Let E be an algebraic extension of a field F, and let $\sigma : F \longrightarrow L$ be an embedding of F into an algebraically closed field L. Then σ can be extended to an embedding $\eta : E \longrightarrow L$.

Proof : Consider the set

$S = \{(K, \theta) \mid F \subseteq K \subseteq E, \theta : K \to L$ is an embedding and $\theta|_F = \sigma\}$

Then $S \neq \phi$ ($\because (F, \sigma) \in S$)

Define a binary operation $\leq$ on S by

$(K_1,\theta_1) \le (K_2,\theta_2)$ if $K_1 \subset K_2$ and θ_2 restricted to K_1 is θ_1 i.e. $\theta_2|_{K_1} = \theta_1$.

Then $\le$ is a partial ordering on S.

Claim : $(S,\le)$ satisfies the hypothesis of the Zorn's lemma.

For let $\{(K_i,\theta_i)\}$ is a chain in S.

Define $K = \bigcup K_i$ and $\theta : K \longrightarrow L$ by

$\theta(a) = \theta_i(a)$ if $a \in K_i$

Also if $a \in K_i \bigcap K_j$ then $\theta_i(a) = \theta_j(a)$

($\because$ either $K_i \subset K_j$ or $K_j \subset K_i$)

$\therefore \theta$ is well defined map on K.

Clearly K is a subfield of E containing F and $\theta : K \longrightarrow L$ is an embedding.

And (K,θ) is an upper bound for the chain $\{(K_i,\theta_i)\}$.

Thus every chain $\{(K_i,\theta_i)\}$ in S has an upper bound.

i.e. $(S,\le)$ satisfy the hypothesis of Zorn's lemma.

$\therefore$ by Zorn's lemma.

$\exists$ a maximal element (K,η) in S.

Then η is an extension of σ.

Claim : K = E

Let if possible $K \neq E$.

$\therefore \exists a \in E$ such that $a \notin K$.

Since E is an algebraic extension of F, 'a' is algebraic over F and hence over K.

$\therefore$ by theorem (4.2), $\exists$ an embedding $\eta' : K(a) \longrightarrow L$ such that $\eta'|_K = \eta$.

But then $(K,\eta) < (K(a),\eta')$ and $(K(a),\eta') \in S$

a contradiction to the maximality of (K,η)

$\therefore K = E$

And $\eta : E \longrightarrow L$ is an embedding and is an extension of σ.

Theorem 4.4 : Let K and K' be algebraic closures of a field F. Then $K \cong K'$ under an isomorphism that is an identity on F.

Proof : Let K and K' be algebraic closures of a field F.

Then by definition of algebraic closure K and K' are algberaic extensions of F and are algebraically closed fields.

Define $\lambda : F \longrightarrow K$ by

$\lambda(a) = a, \ \forall a \in F$

Then λ is an embedding of F into algebraically closed field K (prove it ?)

$\therefore$ by theorem (4.3) λ can be extended to an embedding $\lambda^* : K' \longrightarrow K$.

$\therefore K' \cong \lambda^*(K') \subseteq K$

Since K' is algebraically closed field containing F.

$\therefore \lambda^*(K')$ is also algebraically closed field containing F.

And since K is algebraic extensionof F and $F \subseteq \lambda^*(K')$.

$\therefore K$ is also algebraic extension of $\lambda^*(K')$.

$\Rightarrow \lambda^*(K') = K$ ($\because \lambda^*(K')$ is algebraically closed field and K is algebraic extension of $\lambda^*(K')$. $\therefore$ by definition of algebraically closed field $\lambda^*(K') = K$)

This shows that an embedding $\lambda^* : K' \longrightarrow K$ is onto.

$\therefore \lambda^*$ is an isomorphism of K' onto K and $\lambda^*(a) = a, \ \forall a \in F$ ($\because \lambda^*|_F = \lambda$)

Remarks :

1) Any field F has a unique (upto isomorphism) algebraic closure.

2) The algebraic closure of a field F is denoted by $\overline{F}$.

3) Let F be a field and let $S = \{x_\alpha\}_{\alpha \in \Delta}$ be an infiite set of commuting indeterminates.

Define $F[S] = \left\{ \sum_{\text{finite}} a_i x_{i1} x_{i2} \ldots x_{in} / a_i \in F, x_{ij} \in S \right\}$

Then $F[S]$ is a polynomial ring over F in S w.r.t. natural addition and multiplication.

Theorem 4.5 : Let F be a field. Then there exists an algebraically closed field K containing F as a subfield.

Proof : Let F be a field.

We construct an extension K_1 of F in which every nonconstant polynomial has a root.

For each nonconstant polynomial $f = f(x) \in F[x]$ we correspond an indeterminate x_f and let $S = \{x_f \mid f = f(x) \in F[x] \text{ and degree of } f(x) \geq 1\}$.

Consider the polynomial ring $F[S]$ which is an integral domain.

Let A be an ideal in $F[S]$ generated by all polynomials $f(x_f)$ of positive degree in $F[S]$.

Claim : A is proper ideal of $F[S]$.

Let if possible A is not proper ideal in $F[S]$.

i.e. $A = F[S]$.

As $1 \in A \Rightarrow 1 = g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \ldots\ldots + g_n f(x_{f_n})$

where $g_1, g_2, \ldots\ldots, g_n \in F[S]$

($g_1, g_2, \ldots\ldots, g_n$ involves only a finite number of indeterminates)

We write $x_{f_i} = x_i$ for each $f_i \in F[x]$ then

$x_{f_1} = x_1$, $x_{f_2} = x_2$, ..., $x_{f_n} = x_n$.

And the indeterminates occuring in all the g_i, $1 \le i \le n$ are in the set $\{x_1, x_2, ..., x_n, ...x_m\}$.

$$\therefore 1 = \sum_{i=1}^{n} g_i(x_1, x_2, ..., x_m) f_i(x_i) \qquad \text{..... (1)}$$

Let E be an extensionof F in which each of the polynomials f_1, f_2 ,...., f_n has a root and let a_i be a root of f_i in E, for each $1 \le i \le n$.

If we substitute $x_i = a_i$, $1 \le i \le n$ and $x_{n+1} = ... = x_m = 0$ in (1) we get $1 = 0$ whichis absurd #

Thus A is a proper ideal of $F[S]$.

$\therefore$ by Zorn's Lemma, let M be a maximal ideal of $F[S]$ containing A.

Then there is $\sigma : F \longrightarrow \dfrac{F[S]}{M}$ defined by $\sigma(a) = a + M$ is an embedding.

Thus we can regard $\dfrac{F[S]}{M}$ is a field extension of F.

Also each nonconstant polynomial $f = f(x) = F[x]$ has a root in $\dfrac{F[S]}{M}$.

Thus we have constructed the extension field $K_1 = \dfrac{F[S]}{M}$ of F in which every nonconstruct polynomial in $F[x]$ has a root.

Now inductively we can form a chain of fields $F = K_0 \subset K_1 \subset K_2 \subset K_3 \subset .....$such that any nonconstant polynomial over K_n has a root in K_{n+1}, $\forall n \ge 0$.

Define $K = \bigcup_{n=1}^{\infty} K_n$.

Then K is a field extension of F.

If $g(x) = b_0 + b_1x + ... + b_mx^m$, $b_m \neq 0$, $m > 0$ is a polynomial over K, then $\exists$ 'n' such that $b_0, b_1, ..., b_m \in K_n \Rightarrow g(x) \in K_n[x]$ and $g(x)$ has a root in $K_{n+1} \subseteq K$.

Thus F has an algebraically closed extension.

Theorem 4.6 : Let F be a field. Then there exists an extension $\overline{F}$ that is algebraic over F and is algebraically closed i.e. each field has an algebraic closure.

Proof : Let F be a field, then by theorem (4.5) $\exists$ an extension K of F which is algebraically closed.

Let $\overline{F} = \{a \in K / a \text{ is algebraic over } F\}$ then $F \subseteq \overline{F} \subseteq K$

and by theorem (3.6) $\overline{F}$ is an algebraic extension of F. ..... (1)

Now we prove that $\overline{F}$ is algebraically closed.

For let $f(x) \in \overline{F}[x]$. Then $f(x)$ has a root $a \in K$ ($\because$ K is algebraically closed)

$\Rightarrow a \in K$ is algebraic over $\overline{F}$.

Now since $\overline{F}$ is algebraic extensionof F (by (1))

$\therefore$ a is algebraic over F (see problem (3.1)).

$\Rightarrow a \in \overline{F}$ ($\because$ by definition of $\overline{F}$)

$\therefore$ every root of any polynomial $f(x) \in \overline{F}[x]$ is in $\overline{F}$.

But this shows that $\overline{F}$ is algebraically closed field. ..... (2)

Thus from (1) and (2) $\overline{F}$ is an algebraic closure of F.

EXAMPLES :

4.1 $\overline{\mathbb{C}} = \mathbb{C}$

4.2 $\overline{\mathbb{R}} = \mathbb{C}$

4.3 $\overline{Q} \subset \mathbb{C}$ ($\because \overline{Q}$ is a countable set)

EXERCISE :

1. Show that $x^3 - 2 \in Q[x]$ is irreducible over Q. Find an extension K of Q having all roots of $x^3 - 2$ such that $[K : Q] = 6$.

2. Find the smallest extension of Q having a root of $x^4 - 2 \in Q[x]$.

3. Find a suitable number '*a*' such that $Q(\sqrt{3}, i) = Q(a)$.

4. Find the degree of $Q(\sqrt{2}, \sqrt{3})$ over Q.

5. Determine the minimal polynomials of the folowing numbers over Q.

(a) $3\sqrt{2} + 5$ (b) $\sqrt{-1} + \sqrt{2}$ (c) $\sqrt{2} - 3\sqrt{3}$

6. Let $F \subseteq K \subseteq E$ be fields such that K is algebraic extension of F and E is an algebraic extension of K then show that E is an algebraic extension of F.

7. If F is a subfield of an algebraically closed field K, then show that the algebraic closure $\overline{F}$ of F in K is also algebraically closed.

8. Prove that $Q(\sqrt{2}, \sqrt{5}) = Q(\sqrt{2} + \sqrt{5})$.

9. Prove that $\exists\ a \in \mathbb{R}$ such that $Q(\sqrt{2}, \sqrt[3]{5}) = Q(a)$.

REFERENCES :

1. P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul, "Basic Abstract Algebra", Second Edition, Cambridge University Press, UK (Asian Edition), 2005.

2. U. M. Swamy, A.V.S.N. Murthy, "Algebra : Abstract and Modern", Pearson Education, 2012.

3. Michael Artin, "Algebra", Second Edition, Pearson Education, 2015.

4. I. N. Herstein, "Topics in Algebra", Wiley Eastern Ltd.

UNIT - II

NORMAL AND SEPARABLE EXTENSION

Finding roots of polynomials has been an important problem since the time of the ancient Greeks. Some polynomials, however, x^2+1 over $\mathbb{R}$, the real numbers, have no roots in $\mathbb{R}$. By constructing the splitting field for such a polynomial one can find the roots of the polynomial in the new field.

1. SPLITTING FIELDS

The first step in finding the Galois group of a polynomial over a field is to find the smallest extension of the field that contains all of the roots of the polynomial. Beginning with a field F, and a polynomial $f(x) \in F[x]$, we need to construct the smallest possible extension field K of F that contains all of the roots of $f(x)$.

Definition 1.1 : Let $f(x)$ be a polynomial in $F[x]$ of degree ≥ 1. Then an extension K of F is called a splitting field of $f(x)$ over F if

(i) $f(x)$ factors into linear factors in $K[x]$; that is $f(x) = c(x-\alpha_1)\ldots(x-\alpha_n), \quad \alpha_i \in K.$

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

Note :

1. The splitting field is the smallest field that containing all roots.
2. $\mathbb{Q}(\sqrt{3}) = \left\{a+b\sqrt{3} \mid a,b \in \mathbb{Q}\right\}$ is a splitting field of $x^2-3 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

3. Splitting field of $x^4 - 1 \in \mathbb{R}[x]$ over $\mathbb{R}$ is the field $\mathbb{C}$.

4. We note that a polynomial $f(x) \in F[x]$ always has a splitting field, namely, the field generated by its roots in a given algebraic closure $\overline{F}$ of F.

Theorem 1.1 : If K is a splitting field of $f(x) \in F[x]$ over F, then K is a finite extension and, hence, an algebraic extension of F.

Proof. Since K is a splitting field of $f(x) \in F[x]$ over F, $K = F(\alpha_1, \ldots \alpha_n)$; that is, K is generated over F by the roots $\alpha_1, \ldots \alpha_n$ of $f(x)$ in K. That is, $K = F(\alpha_1, \ldots \alpha_n)$ is a finitely generated extension of F such that $\alpha_1, \ldots \alpha_n$ are algebraic over F. Hence by theorem, K is a finite extension and, hence, an algebraic extension of F.

Theorem 1.2 (uniqueness of splitting field) : Let K be a splitting field of the polynomial $f(x) \in F[x]$ over a field F. If E is another splitting field of $f(x)$ over F, then there exists an isomorphism $\sigma : E \to K$ that is identity on F.

Proof. Let K be a splitting field of the polynomial $f(x) \in F[x]$ over a field F and $\overline{K}$ be an algebraic closure of K.

Then $\overline{K}$ is algebraic over K. Since K is algebraic over F, $\overline{K}$ is algebraic over F.

Hence $\overline{K} = \overline{F}$.

Since E is an algebraic extension of F, by theorem the identity mapping $\lambda : F \to F$ can be extended to an embedding $\sigma : E \to \overline{K}$.

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$ and

$f^{\sigma}(x) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n \in F[x]$.

Since σ is identity on F, $f^{\sigma}(x) = f(x)$.

Let $f(x)=c(x-\alpha_1) \quad \ldots \quad (x-\alpha_n),\ \alpha_i \in E,\ i=1,\ldots,n,\ c \in F$.

Then $f(x)=c(x-\sigma(\alpha_1)) \quad \ldots \quad (x-\sigma(\alpha_n))$ be unique factorization in $\overline{K}[x]$.

But since $f(x)$ has a factorization in $K[x]$, say $f(x)=c(x-\beta_1)\ldots(x-\beta_n)$, where $\beta_i \in K,\ i=1,\ldots,n,$ it follows that the sets $\{\sigma(\alpha_1),\ldots,\sigma(\alpha_n)\}$ and $\{\beta_1,\ldots,\beta_n\}$ are equal.

Thus, $K=F(\beta_1,\ldots,\beta_n)=F(\sigma(\alpha_1),\ldots,\sigma(\alpha_n))=\sigma(F(\alpha_1,\ldots,\alpha_n))=\sigma(E)$.

Hence, σ is an isomorphism of E onto K.

Note : Theorem 1.2 proves that the splitting field of a polynomial over a given field is unique (up to isomorphism) if it exists. But recall that any field F has an algebraic closure $\overline{F}$ that contains roots of all polynomials over F .Thus, the intersection of all subfields of $\overline{F}$ containing all the roots of a given polynomial $f(x) \in F[x]$ is the splitting field of $f(x)$ over F.

Example 1.1 : Show that degree of the extension of the splitting field of $x^3-2 \in \mathbb{Q}[x]$ is 6.

Solution : By Eisenstein's criterion $x^3-2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and it is the minimal polynomial of $2^{1/3}$.

Thus $\mathbb{Q}[x]/(x^3-2) \simeq \mathbb{Q}(2^{1/3})$ with $[\mathbb{Q}(2^{1/3}):\mathbb{Q}]=3$.

Since $x^3-2=(x-2^{1/3})(x^2+2^{1/3}x+2^{2/3})$, x^3-2 has two complex roots, say α and $\overline{\alpha}$.

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

Hence, $\mathbb{Q}(2^{1/3})[x]/(p(x)) \simeq \mathbb{Q}(2^{1/3})(\alpha)=\mathbb{Q}(2^{1/3},\alpha)$ and $[\mathbb{Q}(2^{1/3},\alpha):\mathbb{Q}(2^{1/3})]=$ degree of $p(x)=2$.

Because $\mathbb{Q}(2^{1/3},\alpha)$ contains one root α of $p(x)$, it will also contain the other root $\bar{\alpha}$.

Hence, $\mathbb{Q}(2^{1/3},\alpha)$ is the splitting field of $x^3-2\in\mathbb{Q}[x]$ over $\mathbb{Q}$. Finally,

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

Example 1.2 : Let p be prime. Then show that $f(x)=x^p-1\in\mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\alpha)$, where $\alpha\neq 1$ and $\alpha^p=1$. Also, $\left[\mathbb{Q}(\alpha):\mathbb{Q}\right]=p-1$.

Solution : Let $f(x)=x^p-1=(x-1)\left(x^{p-1}+x^{p-2}+\ldots+x+1\right)$.

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

Let α be a root of $p(x)$ in the splitting field of $f(x)$ over $\mathbb{Q}$. Then, clearly $\alpha^p=1$ and $\alpha\neq 1$.

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

Clearly, $\alpha^p=1$ implies $\left(\alpha^i\right)^p=1$ for all positive integers i.

Thus, we need to show that $1,\alpha,\alpha^2,\ldots,\alpha^{p-1}$ are distinct roots.

Note that if m is the smallest positive integer such that $\alpha^m=1$, then $m\mid p$. Thus, $m=p$.

Hence, no two roots in the list $1,\alpha,\alpha^2,\ldots,\alpha^{p-1}$ can be equal, whence these are all the p roots of x^p-1.

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

Since, the minimal polynomial of a is $p(x)$, which is of degree $p-1$.

Hence $\left[\mathbb{Q}(\alpha):\mathbb{Q}\right]=$ degree of $p(x)=p-1$.

Example 1.3 : Let $F = \mathbb{Z}_2$. Then show that splitting field of $x^3 + x^2 + 1 \in F[x]$ is a finite field with eight elements.

Solution : Let $p(x) = x^3 + x^2 + 1$.

Since $p(0) = 1 \neq 0$ and $p(1) = 1 \neq 0$, $x^3 + x^2 + 1$ is irreducible over F.

Let α be a root of this polynomial in its splitting field. Then,

$$\begin{aligned} x^3 + x^2 + 1 &= (x + \alpha)(x^2 + (1+\alpha)x + (\alpha + \alpha^2)) \\ &= (x + \alpha)(x + \alpha^2)(x + 1 + \alpha + \alpha^2). \end{aligned}$$

Therefore, $F(\alpha)$ is the splitting field of $p(x) = x^3 + x^2 + 1$ over F, and $[F(\alpha) : F] = 3$, the degree of the minimal polynomial $p(x) = x^3 + x^2 + 1$ of α. Furthermore, $F(\alpha)$ has a basis $\{1, \alpha, \alpha^2\}$ over F.

Therefore, $F(\alpha) = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$, where $\alpha^3 + \alpha^2 + 1 = 0$.

Example 1.4 : Show that the splitting field of $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/4}, i)$ and its degree of extension is 8.

Solution : Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, then by Eisenstein criterion $f(x)$ irreducible over $\mathbb{Q}$.

Also $2^{1/4}$ is one root of $f(x)$. Therefore $f(x)$ is the minimal polynomial of $2^{1/4}$ over $\mathbb{Q}$.

Thus, $\left[\mathbb{Q}(2^{1/4}) : \mathbb{Q}\right] =$ degree of $f(x) = 4$.

Now $f(x) = \left(x - 2^{1/4}\right)\left(x + 2^{1/4}\right)(x^2 + 2^{1/2})$ and the factor $p(x) = x^2 + 2^{1/2}$ is irreducible over $\mathbb{Q}(2^{1/4})$.

Thus, $p(x) = x^2 + 2^{1/2}$ is the minimal polynomial of $2^{1/4} i$ over $\mathbb{Q}(2^{1/4})$,

Hence $\left[\mathbb{Q}(2^{1/4})(2^{1/4}i):\mathbb{Q}(2^{1/4})\right]=$ degree of $p(x)=2.$

Since $\mathbb{Q}(2^{1/4})(2^{1/4}i)=\mathbb{Q}(2^{1/4},i),$ contains all roots of $f(x)$, $\mathbb{Q}(2^{1/4},i)$ is the splitting field of $f(x)=x^4-2\in\mathbb{Q}[x].$

Therefore,

$$\left[\mathbb{Q}(2^{1/4},i):\mathbb{Q}\right]=\left[\mathbb{Q}(2^{1/4},i):\mathbb{Q}(2^{1/4})\right]\left[\mathbb{Q}(2^{1/4}):\mathbb{Q}\right]=2.4=8.$$

Example 1.5 : Find splitting field of $f(x)=x^4+4$ over $\mathbb{Q}$.

Solution : Let $f(x)=x^4+4$ is not irreducible over $\mathbb{Q}$.

Since $f(x)=x^4+4=(x^2+2x+2)(x^2-2x+2)$ is reducible over $\mathbb{Q}$. But two factors are irreducible over $\mathbb{Q}$.

By using quadratic formula, we find four roots $1+i,1-i,-1+i$ and $-1-i$. Thus splitting of this polynomial is $\mathbb{Q}(i)$ and $\left[\mathbb{Q}(i):\mathbb{Q}\right]=2.$

Example 1.6 : If K is an extension field of F of degree 2, then prove that K is the splitting field over F for some polynomial.

Solution : Let K be an extension field of F of degree 2. Since $[K:F]>1,$ we can choose $\alpha\in K$ such that $\alpha\notin F$.

Then α is algebraic over F. Let $p(x)$ be minimal polynomial of α over F.

Since $[K:F(\alpha)][F(\alpha):F]=[K:F]=2$ and $[F(\alpha):F]>1,$ we have

$$[F(\alpha):F]=2 \text{ and } [K:F(\alpha)]=1.$$

Therefore $F(\alpha)=K$.

Thus minimal polynomial $p(x)$ has degree 2.

Let $p(x)=x^2+ax+b,\quad a,b\in F$. Therefore $p(x)=(x-\alpha)(x-\beta)$, where $\beta\in\mathbb{C}$.

Then $F(\alpha,\beta)$ be splitting field for $p(x)$ over F.

Since $K = F(\alpha)$, K is subfield of $F(\alpha, \beta)$.

Since, $p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta = x^2 + ax + b$, we have

$\alpha + \beta = -a$ and $\alpha\beta = b$.

Therefore $\beta = -\alpha - a \in F(\alpha)$.

Thus $F(\alpha, \beta)$ is subfield of K.

Hence $K = F(\alpha, \beta)$.

Thus K is splitting field for some polynomial $p(x)$ over F.

Example 1.7 : Let $f(x) = x^2 + 3, \quad g(x) = x^2 + x + 1 \in \mathbb{Q}[x]$. Show that their splitting fields are equal and find its degree over $\mathbb{Q}$.

Solution : Let $f(x) = x^2 + 3, \quad g(x) = x^2 + x + 1 \in \mathbb{Q}[x]$.

Then $\pm\sqrt{3}\,i$ are roots of $f(x)$ and $\frac{-1 \pm \sqrt{3}\,i}{2}$ are roots of $g(x)$.

Therefore, $\mathbb{Q}\left(\sqrt{3}\,i\right)$ is the splitting field of $f(x)$ and $\mathbb{Q}\left(\frac{-1 \pm \sqrt{3}\,i}{2}\right)$ is the splitting field of $g(x)$.

Since $\mathbb{Q}\left(\sqrt{3}\,i\right) = \mathbb{Q}\left(\frac{-1 \pm \sqrt{3}\,i}{2}\right)$, splitting field of $f(x)$ and $g(x)$ are equal.

Also $\left[\mathbb{Q}\left(\sqrt{3}\,i\right) : \mathbb{Q}\right]$ = degree of $f(x) = 2$.

Example 1.8 : Find condition on a and b such that the splitting field of $x^3+ax+b\in\mathbb{Q}[x]$ has degree 3 over $\mathbb{Q}$.

Solution : Let $f(x)=x^3+ax+b\in\mathbb{Q}[x]$, then $f(x)$ must be irreducible over $\mathbb{Q}$, otherwise degree of extension is either 1 or 2.

Let $E=\mathbb{Q}(\alpha,\beta,\gamma)$ be splitting field of $f(x)$ over $\mathbb{Q}$.

Therefore $f(x)=x^3+ax+b=(x-\alpha)(x-\beta)(x-\gamma)$ implies that

$\alpha+\beta+\gamma=0,\ \alpha\beta+\beta\gamma+\gamma\alpha=a$ and $\alpha\beta\gamma=-b$

Therefore $\beta+\gamma=-\alpha$ and $\beta\gamma=-b/\alpha=\alpha^2+a$.

Thus β and γ are roots of second degree polynomial,

$$g(x)=x^2+\alpha x+\alpha^2+a\in\mathbb{Q}(\alpha).$$

Hence if β and γ are in $\mathbb{Q}(\alpha)$ then $E=\mathbb{Q}(\alpha,\beta,\delta)=\mathbb{Q}(\alpha)$ and $[E:\mathbb{Q}]=3$ as desired.

But roots β and γ are in $\mathbb{Q}(\alpha)$ if and only if discriminant $\Delta=-3\alpha^2-4a$ of $g(x)$ must be a square in $\mathbb{Q}$ otherwise other two roots are in $\mathbb{Q}\left(\alpha,\sqrt{\Delta}\right)$ which is of degree 6 over $\mathbb{Q}$.

Hence the splitting field of $x^3+ax+b\in\mathbb{Q}[x]$ has degree 3 over $\mathbb{Q}$ if $\sqrt{\Delta}\in\mathbb{Q}(\alpha)$.

2. NORMAL EXTENSIONS

Let $\left(f_i(x)\right)_{i\in\Lambda}$ be a family of polynomials of degree ≥ 1 over a field F. Splitting field of a family $\left(f_i(x)\right)_{i\in\Lambda}$ of polynomials is an extension E of F such that every $f_i(x)$ splits into linear factors in $E[x]$, and E is generated over F by all the roots of the polynomials $f_i(x), i\in\Lambda$. If Λ is finite and our polynomials are $f_1(x),\ldots, f_n(x)$, then their splitting field is a splitting field of the single polynomial $f(x) = f_1(x)\ldots f_n(x)$, obtained by taking the product. The proof of uniqueness (up to isomorphism) of a splitting field of a single polynomial can be extended to prove the uniqueness (up to isomorphism) of a splitting field of a family of polynomials over a given field.

The next theorem proves a set of equivalent statements for an extension E of F to be a splitting field of a family of polynomials over F.

Theorem 2.1 : Let E bean algebraic extension of a field F contained in an algebraic closure $\overline{F}$ 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 polynomials in $F[x]$.

(iii) Every embedding σ of E in $\overline{F}$ that keeps each element of F fixed maps E onto E. (In other words, σ may be regarded as an automorphism of E.

Proof : (i) $\Rightarrow$ (ii)

Let $\alpha\in E$, and let $p_\alpha(x)$ be its minimal polynomial over F. By (i), $p_\alpha(x)$ splits into linear factors in E. Thus, it follows immediately that E is the splitting field of the family $\left\{p_\alpha(x)\right\}_{\alpha\in E}$ of polynomial over F.

(ii) $\Rightarrow$ **(iii)**

Let $\{f_i(x)\}_{i\in\Lambda}$, be a family of polynomials of which E is the splitting field.

If α is a root of some $f_i(x)$ in E, then for any embedding σ of E into $\overline{F}$ that keeps each element of F fixed, $\sigma(\alpha)$ is also root of $f_i(x)$.

Since E is generated by the roots of all the polynomials $f_i(x)$, it follows that σ maps E into itself. That is $\sigma: E \to E$ be an embedding of E into itself over F. Then, by Theorem, σ is an automorphism of E.

(iii) $\Rightarrow$ **(i)**

Let $p(x) \in F[x]$ be an irreducible polynomial over F that has a root $\alpha \in E$. Let $\beta \in \overline{F}$ be another root of $p(x)$. Now we claim that $\beta \in E$.

Since α and β are roots of the same irreducible polynomial $p(x)$, we have F-isomorphisms

$$F(\alpha) \simeq F[x]/(p(x)) \simeq F(\beta)$$

under the isomorphism,

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n \to a_0 + a_1x + \ldots + a_nx^n + (f(x)) \to a_0 + a_1\beta + \ldots + a_n\beta^n.$$

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

By Theorem, σ can be extended to an embedding $\sigma^*: E \to \overline{F}$. But then, by (iii), σ^* is an automorphism of E;

Therefore, $\beta = \sigma(\alpha) = \sigma^*(\alpha) \in \mathrm{E}$. Hence the proof.

Definition 2.1 : An extension E of a field F is called normal 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 polynomials in $F[x]$.

(iii) Every embedding σ of E in $\overline{F}$ that keeps each element of F fixed maps E onto E. (In other words, σ may be regarded as an automorphism of E.)

Note :

1. The Field of complex numbers $\mathbb{C}$ is a normal extension of the field of real numbers $\mathbb{R}$ and $[\mathbb{C}:\mathbb{R}]=2$.
2. $\mathbb{R}$ is not a normal extension of the field $\mathbb{Q}$ of rational numbers, for $x^3-2\in\mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and has a root $\sqrt[3]{2}$ in $\mathbb{R}$, but it does not split into linear factors in $\mathbb{R}$ because it has complex roots.
3. If $\alpha=\cos(\pi/4)+i\sin(\pi/4),$ then $\mathbb{Q}(\alpha)$ is a normal extension of $\mathbb{Q}$. As $\mathbb{Q}(\alpha)$ is the splitting field of $x^4+1\in\mathbb{Q}[x]$.

Example 2.1 : 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 over F.

Solution : Let E be a finite extension of F and $E=F(\alpha_1,\ldots,\alpha_n),$ where $\alpha_i\in E$ are algebraic over F.

Let $p_i(x)$ be the minimal polynomial of α_i, over F.

Assume first that E is a normal extension of F. Then $p_i(x)$ splits in E because it has one root $\alpha_i\in E$.

Thus, $p(x) = p_1(x)\dots p_n(x) \in F[x]$ has all roots in E.

Since $E = F(\alpha_1,\dots,\alpha_n)$, and $\alpha_1,\dots,\alpha_n$, are some of the roots of $p(x)$, E must be the splitting field of $p(x)$.

Conversely suppose that E is splitting field of $f(x) \in F[x]$. If $\alpha_1,\dots,\alpha_n$ are all roots of $p(x)$, then $E = F(\alpha_1,\dots,\alpha_n)$.

If $\sigma : E \to \overline{F}$ is an embedding that keeps each element of F fixed, then $\sigma(\alpha_i)$ is also root of $f(x)$.

Therefore $\sigma(\alpha_i) = \alpha_j$ for some j and $\sigma(\alpha_i) \in E$ for all $1 \le i \le n$.

Hence $\sigma(E) \subseteq E$ and σ is an automorphism of E.

Thus by Theorem 2.1, E is a normal extension of F.

Example 2.2 : Show that any extension K of a field F, such that $[K : F] = 2$, is a normal extension.

Solution : In example 1.6 we have shown that K is the splitting field $p(x) \in F[x]$. Then by definition , K is normal extension of F.

Example 2.3 : Show that $\mathbb{Q}\left(\sqrt{-2}\right)$ and $\mathbb{Q}\left(2\sqrt{7}\right)$ are normal extension of $\mathbb{Q}$.

Solution : Let $\alpha = \sqrt{-2}$ then α is algebraic over $\mathbb{Q}$ and minimal polynomial is $p(x) = x^2 + 2 \in \mathbb{Q}[x]$.

Therefore $\left[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\alpha) : \mathbb{Q}\right] =$ degree of $p(x) = 2$.

Hence $\mathbb{Q}(\sqrt{-2})$ is normal extension of $\mathbb{Q}$.

Similarly $\mathbb{Q}\left(2\sqrt{7}\right)$ is normal extension of $\mathbb{Q}$.

Example 2.4 : Let E be normal extension of F and let be K a subfield of E containing F. Show that E is a normal extension of K. Give an example to show that K need not be a normal extension of F.

Solution : Let E be normal extension of F. Then by definition E is splitting field of a family of polynomials over F.

Since $F \subset K$, E is splitting field of a family of polynomials over K.

Hence E is a normal extension of K.

Let $E = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ and $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ where ω is cube root of unity.

Then $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$.

Here $E = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ is normal extension of $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ but $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ is not normal extension of $\mathbb{Q}$.

Example 2.5 : Let $F = \mathbb{Q}\left(\sqrt{2}\right)$ and $E = \mathbb{Q}\left(\sqrt[4]{2}\right)$. Show that E is normal extension of F and F is normal extension of $\mathbb{Q}$, but E is not a normal extension of $\mathbb{Q}$.

Solution : Since $x^2 - 2 \in \mathbb{Q}[x]$ be minimal polynomial of $\sqrt{2}$, $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$.

Therefore $F = \mathbb{Q}\left(\sqrt{2}\right)$ is normal extension of $\mathbb{Q}$.

Also $x^2 - \sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)[x]$ is minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}\left(\sqrt{2}\right)$.

Therefore $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$.

Hence $E = \mathbb{Q}\left(\sqrt[4]{2}\right)$ is normal extension of $F = \mathbb{Q}\left(\sqrt{2}\right)$.

Also $x^4 - 2 \in \mathbb{Q}[x]$ is minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ and roots $\pm\sqrt[4]{2}\, i$ of $x^4 - 2 \in \mathbb{Q}[x]$ are does not belong to $E = \mathbb{Q}\left(\sqrt[4]{2}\right)$.

Therefore $E = \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not splitting field of $x^4 - 2 \in \mathbb{Q}[x]$.

Hence $E = \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not a normal extension of $\mathbb{Q}$.

3. MULTIPLE ROOTS

In this section we discuss the multiplicity of roots of a polynomial over a field. For this purpose, we introduce the concept of the derivative of a polynomial.

Definition 3.1 : Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial over a field F. Then derivative of $f(x)$ is defined as $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$.

Note :

1. Properties of derivatives that are familiar from calculus are not necessarily valid here. For example, $f'(x) = 0$ does not always imply that $f(x)$ is a constant: for example, if we set $f(x) = x^3$ in a field of characteristic 3 then $f'(x) = 3x^2 = 0.$
2. Derivative of a polynomial is a linear operation; that is $\left(af(x) + bg(x)\right)' = af'(x) + bg'(x)$, where $a, b \in F.$
3. For the derivative of a product we have the usual rule $\left(f(x)g(x)\right)' = f'(x)g(x) + f(x)g'(x).$
4. If $Char(F) = 0$ and degree of $f(x) = n > 0$, then degree of $f'(x) = n - 1.$
5. If $Char(F) = p$ and degree of $f(x) = x^p$, then $f'(x) = 0.$

Definition 3.2 : Let K be a splitting field of a polynomial $f(x) \in F[x]$. Let α 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 $f(x)$ in $K[x]$, then s is called the multiplicity of α.

If $s=1$, then α is called a simple root; if $s>1$, then α is called a multiple root.

Theorem 3.1 : 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 α is a root of $f(x) \in F[x]$,

By division algorithm we can write $f(x)=(x-\alpha)g(x)$.

Therefore $f'(x)=(x-\alpha)g'(x)+g(x)$.

Thus α is a multiple root of $f(x)$ if and only if $g(\alpha)=0$.

Since $f'(\alpha)=g(\alpha)$, α is a multiple root if and only if $f'(\alpha)=0$.

Corollary 3.2 : Let $f(x) \in F[x]$ 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 an irreducible polynomial over F and α is root of $f(x)$. Suppose $f'(x)=0$. Therefore $f'(\alpha)=0$.

Hence by Theorem 3.1, α is a multiple root of $f(x)$.

On the other hand, suppose $f(x)$ has a multiple root α. Then by Theorem 3.1, α is a root of $f'(x)$.

Since $f(x)$ is irreducible, $a^{-1}f(x)$ is the minimal polynomial of α over F, where a is the leading coefficient of $f(x)$.

Now suppose $f'(x) \neq 0$, then $f'(x)$ is a non constant polynomial satisfied by α. Since $a^{-1}f(x)$ is the minimal polynomial of α over F, degree of $f'(x) \geq$ degree of $a^{-1}f(x)$. Which is a contradiction.

Hence, $f'(x) = 0$.

Corollary 3.3 : Any irreducible polynomial $f(x)$ over a field of characteristic 0 has simple roots. Also any irreducible polynomial $f(x)$ over afield 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 $f(x) = \sum_{i=0}^{n} a_i x^i$ be an irreducible polynomial over a field F.

Then by Corollary 3.2 $f(x)$ has multiple roots if and only if $f'(x) = \sum_{i=0}^{n} i a_i x^{i-1} = 0$. Therefore $f(x)$ has multiple roots if and only if $i\, a_i = 0, 1 \leq i \leq n$.

Thus in a field of characteristic 0, if $f'(x) = 0$ then $a_i = 0, 1 \leq i \leq n$.

But then $f(x) = a_0 \in F$, which is a contradiction.

Hence in a field of characteristic 0, all roots of $f(x)$ are simple.

Now if F is of characteristic $p \neq 0$, and if $a_i \neq 0$, we must have $p \mid i$.

Thus $f(x)$ has multiple roots if and only if, either $a_i = 0$, or $p \mid i$.

Therefore $f(x) = g(x^p)$, for a suitable polynomial $g(x) \in F[x]$.

Theorem 3.4 : If $f(x) \in F[x]$ is irreducible over F, then all roots of $f(x)$ have the same multiplicity.

Proof : Let $\overline{F}$ be the algebraic closure of F, and let α and β be roots of $f(x)$ in $\overline{F}$ with multiplicities k and k', respectively.

We know that

$$F(\alpha) \simeq F[x]/(f(x)) \simeq F(\beta),$$

under the isomorphism,

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n \to a_0 + a_1x + \ldots + a_nx^n + (f(x)) \to a_0 + a_1\beta + \ldots + a_n\beta^n.$$

Let $\sigma : F(\alpha) \to F(\beta)$ be an isomorphism.

Clearly, $\sigma(\alpha) = \beta$ and $\sigma(s) = s,$ for all $s \in F$.

We know $\sigma : F(\alpha) \to F(\beta)$ can be extended to an isomorphism $\sigma^* : \overline{F} \to \overline{F(\beta)} = \overline{F}$. Then we define a ring homomorphism $\eta : \overline{F}[x] \to \overline{F}[x]$ by

$$\eta(a_0 + a_1x + \ldots + a_rx^r) = \sigma^*(a_0) + a_1x + \ldots + \sigma^*(a_r)x^r.$$

Clearly $\eta(f(x)) = f(x),\ f(x) \in F[x]$.

Therefore if α is roots of $f(x)$ with multiplicity k, then

$$f(x) = (x-\alpha)^k g(x),\ g(x) \in \overline{F}[x]$$

and

$$\eta(f(x)) = (x-\beta)^k\ \eta(g(x)) \Rightarrow f(x) = (x-\beta)^k\ \eta(g(x)).$$

Thus $(x-\beta)^k$ is also factor of $f(x)$ and hence $k' \geq k$.

By interchanging roles of α and β, we get $k \geq k'$.

Hence $k = k'$.

Corollary 3.5 : 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 $\alpha_1, \alpha_2, \ldots, \alpha_r$ be roots of polynomial $f(x) \in F[x]$ with multiplicities $k_1, k_2, \ldots, k_r$ respectively.

Then $f(x) = a\prod_{i=1}^{r}(x-\alpha_i)^{k_i}$.

Since, $f(x)$ is irreducible over F, by Theorem 3.4, all roots of $f(x)$ have the same multiplicity.

Therefore $k = k_1 = k_2 = \ldots = k_r$.

Hence $f(x) = a\prod_{i=1}^{r}(x-\alpha_i)^k$.

Example 3.1 : Prove that a polynomial $f(x) \in F[x]$ has multiple root if and only if $f(x)$ and $f'(x)$ has a non-constant common factor.

Solution : Let a be multiple root of $f(x)$ in an extension E of F.

Then $f(x) = (x-a)^m g(x), \quad m > 1, \; g(x) \in E[x]$.

Therefore

$$\begin{aligned} f'(x) &= m(x-a)^{m-1} g(x) + (x-a)^m g'(x) \\ &= (x-a)^{m-1}\left[m\, g(x) + (x-a) g'(x)\right], \quad m-1 > 0. \end{aligned}$$

Therefore $(x-a)^{m-1}$ is non-constant common factor of $f(x)$ and $f'(x)$.

Conversely suppose that $f(x)$ and $f'(x)$ has a non-constant common factor.

Now if all roots of $f(x)$ are distinct, then $f(x) = a\prod_{i=1}^{n}(x-a_i)$, for some $a \in F$

and $f'(x) = a\sum_{i=1}^{n}\left(\prod_{j\neq i}(x-a_j)\right)$.

Therefore, $f'(a_i) = a\prod_{j\neq i}(a_i - a_j) \neq 0, \quad 1 \le i \le n$.

Hence no root of $f(x)$ is a root of $f'(x)$, which is a contradiction.

Therefore all roots of $f(x)$ are not distinct.

Hence $f(x)$ has multiple roots.

Example 3.2 : Let $f(x)$ be a polynomial of degree n over F of characteristic p. Suppose $f'(x)=0$. Show that $p \mid n$ and that $f(x)$ has atmost $\frac{n}{p}$ distinct roots.

Solution : Let $f(x)$ be a polynomial of degree n over F and $f'(x)=0$.

Then by corollary 3.2 $f(x)$ has multiple roots.

Also by corollary 3.3 $f(x)$ has multiple roots if and only if there exists $g(x) \in F[x]$ such that $f(x)=g(x^p)$.

Therefore $n=pm$

Also by theorem 3.4, since each root is of same multiplicity, $f(x)$ has atmost $\frac{n}{p}$ distinct roots.

Example 3.3 : 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 : If y^3-x has a root in K, then there $g(x)/h(x)$ in K with $h(x) \neq 0$ such that $\left(g(x)/h(x)\right)^3 = x$; that is, $g^3(x)=xh^3(x)$.

But this implies that $3\left(\text{degree of } h(x)\right)+1=3\left(\text{degree of } g(x)\right)$, which is impossible. Thus, $y^3-x \in K[y]$ is irreducible over K.

Now if β_1 and β_2 are two roots of y^3-x in its splitting field, then $\beta_1^3 = x = \beta_2^3$.

But then $\left(\beta_1 - \beta_2\right)^3 = \beta_1^3 + (-1)^3\beta_2^3 = 0$, and, hence $\beta_1 - \beta_2 = 0$.

This shows that $y^3 - x$ has only one distinct root whose multiplicity is 3. This completes the solution.

4. FINITE FIELDS

In this section we show that an irreducible polynomial over a finite field has only simple roots. Hence, it will follow then that the only fields over which an irreducible polynomial may have multiple roots are infinite fields of characteristic $p \neq 0$.

Definition 4.1 : A field is called prime if it has no proper subfield.

Note :

1. Every field F contains a prime field F_p,which is precisely the intersection of the family of its subfields, called the prime field of F.
2. $\mathbb{Q}$ and $\mathbb{Z}_p$, where p is prime are prime fields.

Theorem 4.1 : The prime field of a field F is either isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$, where p is prime.

Proof : Define the mapping $f : \mathbb{Z} \to F$ given by $f(n) = ne$, e the unity of F. Then clearly f is a homomorphism.

Case 1 : Ker $f = (0)$ (or, equivalently, char F is 0).

Then f is an embedding of $\mathbb{Z}$ into F.

This embedding can be extended to an embedding $f^* : \mathbb{Q} \to F$ defined by $f^*(m/n) = me/ne$.

Thus, $\mathbb{Q}$ embeds in F, and hence, the prime field of F is isomorphic to $\mathbb{Q}$.

Case 2 : Ker $f \neq (0)$.

Since $\mathbb{Z}$ is a PID, Ker $f = (m)$, m a positive integer.

By the fundamental theorem of homomorphism of rings $\mathbb{Z}_m \simeq \text{Im } f$.

This shows that $\mathbb{Z}_m$, being isomorphic to a subring of the field F, has no proper divisors of zero, so m must be a prime number p.

Thus, $\mathbb{Z}_p$ embeds in F.

Hence, the prime field of F is isomorphic to $\mathbb{Z}_p$.

Theorem 4.2 : Let F be a finite field. Then

(i) The characteristic of F is a prime number p and F contains a subfield $F_p \simeq \mathbb{Z}_p$.

(ii) The number of elements of F is p^n for some positive integer n.

Proof : i) Let characteristic of F is a prime number p.

Since every field F contains a prime field F_p, by theorem 4.1, F contains a subfield $F_p \simeq \mathbb{Z}_p$.

To prove (ii), we regard F as a vector space over its prime field F_p.

Let $(e_1,\ldots,e_n)$ be a basis of F over F_p. Then any element $x \in F$ can be written uniquely as

$$x = a_1e_1 + \ldots + a_ne_n, \quad a_i \in F_p, i = 1,2,\ldots,n.$$

Since each a_i, in the above expression for x be chosen in p ways, the number of elements of F is thus p^n.

Definition 4.2 : A finite field is called a Galois field. A Galois field with p^n elements is denoted by $GF\left(p^n\right)$.

Theorem 4.3 : Any 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 : In the finite field F with p^n elements the nonzero elements form a multiplicative group of order $p^n - 1$.

Thus, if $0 \neq \lambda \in F,$ then $\lambda^{p^n-1} = 1,$ so $\lambda^{p^n} = \lambda.$

Also, if $\lambda = 0,$ then $\lambda^{p^n} = \lambda.$

Hence, all the p^n elements of F satisfy the equation $x^{p^n} - x = 0.$

Since $x^{p^n} - x \in F_p[x]$ has only p^n roots, every element of F is a root of $x^{p^n} - x.$

Hence finite field F with p^n elements is the splitting field of $x^{p^n} - x \in F_p[x].$

Let E and F be two finite fields with p^n elements. By Theorem 4.2, E and F contain subfields E_p and F_p, each of p elements.

Also, E and F are splitting fields of $x^{p^n} - x$ over E_p and F_p, respectively.

But since $E_p \simeq \mathbb{Z}_p \simeq F_p$, it follows by uniqueness of splitting fields (up to isomorphism) that $E \simeq F$. This proves the theorem.

Theorem 4.4 : For each prime p and each positive integer $n \geq 1$ the roots of $x^{p^n} - x \in \mathbb{Z}_p[x]$ in its splitting field over $\mathbb{Z}_p$ are all distinct and form a field F with p^n elements. Also, F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof : Let $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$.

Since $f'(x) = p^n x^{p^n-1} - 1 \neq 0$, by Corollary 3.2, $f(x)$ cannot have multiple roots.

Thus, $f(x)$ has all its p^n distinct roots.

We show that these roots form a field that is the splitting field of $f(x)$ over $\mathbb{Z}_p$.

Let α and β be roots, where β is different from zero.

Then

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta \text{ and } \left(\alpha\beta^{-1}\right)^{p^n} = \alpha^{p^n}\left(\beta^{p^n}\right)^{-1} = \alpha\beta^{-1}.$$

Thus, the set of roots of $f(x)$ forms a subfield of the splitting field $f(x)$ over $\mathbb{Z}_p$ with p^n elements and, therefore, coincides with the splitting field.

Theorem 4.5 : If F is a finite 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 $\overline{F}$ be the algebraic closure of F.

Consider the polynomial $f(x) = x^{p^{mn}} - x \in F[x]$.

Since the multiplicative group of F is of order $p^n - 1$, for $0 \neq u \in F$, $u^{p^n-1} = 1$,.

Also, since $(p^n - 1)(p^{n(m-1)} + p^{n(m-2)} + \ldots + 1) = p^{nm} - 1$, $\left(p^n - 1\right) \mid \left(p^{mn} - 1\right)$.

which gives $u^{p^{mn}-1} = 1$; that is, $u^{p^{mn}} = u$.

This shows that each element of F satisfies $f(x)$.

By Theorem 4.4 the p^{mn} roots of $f(x)$ are distinct and form a field E.

Therefore $\mathbb{Z}_p \simeq F_p \subset F \subset E \subset \overline{F}$ and $[F:F_p] = n$, $[E:F_p] = mn$.

Hence $[E:F] = m$.

Theorem 4.6 : The multiplicative group of nonzero elements of a finite field is cyclic.

Proof : Let F^* be the multiplicative group of nonzero elements of F.

Since F^* is finite abelian group, we can find an element $\alpha \in F^*$ whose order r is the l.c.m. of the orders of all the elements of F^*.

Then the order of each element of F^* divides r.

Hence, for all $a \in F^*$, $a^r = 1$.

Since the polynomial $x^r - 1$ has at most r roots in F, it follows that the number of elements in $F^* \leq r$.

However, $1, \alpha, \ldots, \alpha^{r-1}$ are all distinct and belong to F^*.

Thus, F^* is generated by α. Hence F^* is cyclic.

Corollary 4.7 : Let E be a finite extension of a finite field F. Then $E = F(\alpha)$ for some $\alpha \in E$.

Proof : Let E is a finite extension of a finite field F and $[E : F] = n$.

Then E is an n dimensional vector space over F and hence $|E| = |F|^n$.

Thus E is finite field. Then by above theorem, multiplicative group E^* of nonzero elements of E is a cyclic group generated by $\alpha \in E$.

Therefore E itself is the smallest subfield of E containing F and α. Hence $E = F(\alpha)$.

Theorem 4.8 : Let F be a finite field. Then there exists an irreducible polynomial of any given degree n over F.

Proof : F be a finite field. Then, by the Theorem 4.5, there exists an extension E of F of any given degree n.

Then by Corollary 4.7, $E = F(a)$, for some $\alpha \in E$.

Since E is a finite extension of F, $\alpha \in E$ is algebraic over F.

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

Then $\left[F(\alpha):F\right]=$ degree of $p(x)$.

But since $E=F(a)$, and $\left[E:F\right]=n$, we have an irreducible polynomial $p(x)$ of degree n over F.

Example 4.1 : Show that every finite extension of a finite field is normal.

Solution : Let E be finite extension of a finite field F and $\left[E:F\right]=n$.

Then E is also finite and E^*, the multiplicative group of E is cyclic and generated by u such that $u^{n-1}=1$.

Therefore u is a root of $x^n-x\in F\left[x\right]$.

All other roots of $x^n-x\in F\left[x\right]$ are zero and power of u.

Therefore all roots of $x^n-x\in F\left[x\right]$ are in E.

Hence E is splitting field of $x^n-x\in F\left[x\right]$.

Therefore E is normal extension of F.

Example 4.2 : 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 : We know that a cyclic group of order n has a unique subgroup of order d for each divisor d of n. Let m be divisor of n.

Now consider the cyclic group $F^*=F-\{0\}$ of order p^n-1.

Since $m\,|\,n$,

$$p^n-1=\left(p^m-1\right)\left(p^{m(d-1)}+p^{m(d-2)}+\ldots+p^m+1\right),\quad n=md.$$

Thus $p^m - 1$ divides $p^n - 1$.

Then there exists a unique subgroup H of F^* of order $p^m - 1$.

So for all $x \in H$, $x^{p^m - 1} = 1$.

Hence, $x^{p^m} = x$ for all $x \in H \cup \{0\}$.

Since the roots of $x^{p^m} = x$ form a field, $H \cup \{0\}$ is the unique subfield of F of order p^m.

Example 4.3 : 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.

By Corollary 3.3, $f(x)$ has multiple roots if and only if $f(x) = \sum_{i=0}^{m} a_i \left(x^p\right)^i$.

Because $a_i \in F, a_i^{p^n} = a_i$. Set $b_i = a_i^{p^{n-1}}$.

Thus, $f(x)$ has multiple roots if and only if $f(x) = \sum_{i=0}^{m} \left(b_i x^i\right)^p = \left(\sum_{i=0}^{m} b_i x^i\right)^p$,

a contradiction, because $f(x)$ is irreducible.

Thus, $f(x)$ must have distinct roots.

Example 4.4 : If the multiplicative group F^* of nonzero elements of a field F is cyclic, then F is finite.

Solution : Let $F^* = (\alpha)$, where α generates F^*. If F^* is finite, then F is finite. So assume F^* is an infinite cyclic group.

Case l : The characteristic of F is $p > 0$.

In this case $F = F_p(\alpha)$, where F_p is the subfield $\{0,1,2,\ldots, p-1\}$ of F.

If $1+\alpha=0$, then $\alpha^2=1$, a contradiction, because F^* is infinite.

If $1+\alpha\neq 0$, then $1+\alpha\in F^*$, so $1+\alpha=\alpha^r$, where r is some positive or negative integer.

In either case $1+\alpha=\alpha^r$ yields a polynomial over F_p with α as its root.

Thus, α is algebraic over F_p, so $[F_p(\alpha):F_p]=$degree of the minimal polynomial of α over $F_p=r$, say.

Then $F=F_p(\alpha)$ has p^r elements, a contradiction.

So either the characteristic of F is 0, or F^*must be finite.

Case 2 : The characteristic of F is 0.

Here $0\neq 1\in F$. So $-1=\alpha^r$, where r is some positive or integer.

This implies $\alpha^{2r}=1$; that is, $o(\alpha)$is finite, a contradiction.

Hence, F^* must be finite, so F must be a finite field.

Example 4.5 : 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 field with p^n elements.

Let $Aut(F)$ denote the group of automorphisms of F.

Clearly, the mapping $\phi: F\to F$, defined by $\phi(x)=x^p$, is a homomorphism.

Let $x^p=y^p \Rightarrow (x-y)^p=0\Rightarrow x=y$.

This shows that ϕ is 1-1 and, hence, onto.

Thus, $\phi\in Aut(F)$.

We note that $\phi^n=$ identity because $\phi^n(x)=x^{p^n}=x$for all $x\in F$.

Let d be the order of ϕ. We have $\phi^d(x) = x^{p^d}$ for all $x \in F$.

Hence, each $x \in F$ is a root of the equation $t^{p^d} - t = 0$.

This equation has p^d roots. It follows that $d \geq n$, hence $d = n$.

Let α be a generator of the multiplicative cyclic group F^*.

Then $F = F_p(\alpha)$, where F_p is the subfield of F with p elements.

Let $f(x)$ be the minimal polynomial of α over F_p.

Clearly, the degree of $f(x) = n$.

We are interested in counting the number of extensions of the identity mapping $\lambda : F_p \to F$ to an automorphism $\lambda^* : F \to F$.

This will then give us all the automorphisms of F, because, clearly, any automorphism of F keeps each element of F_p fixed.

By Lemma it follows that the number of automorphisms of F is equal to the distinct roots of $f(x)$.

However, by Example 4.3, $f(x)$ has all its roots distinct. Thus, the order of the group $Aut(F)$ is n.

We showed in the beginning that there exists an element $\phi \in Aut(F)$ such that the order of ϕ is n. Hence, $Aut(F)$ is a cyclic group generated by ϕ.

Example 4.6 : Let a and b be two elements of finite field F, then prove that there exists elements α and β in F such that $1 + a\alpha^2 + b\beta^2 = 0$.

Solution : Let F be finite field with characteristic $p = 2$.

Then F contains 2^n elements.

Therefore, every element of satisfies $x^{2^n} - x$.

Then,

$$a^{2^n} = a, \text{ for all } a \in F$$

$$\Rightarrow a^{2^{n-1}.2} = a, \text{ for all } a \in F$$

$$\Rightarrow \left(a^{2^{n-1}}\right)^2 = a, \text{ for all } a \in F .$$

Thus every element of F is a square.

Now if $a, b \in F$, $a^{-1} \in F \Rightarrow a^{-1} = \alpha^2$, for some $\alpha \in F$.

Then for $\beta = 0$ we have

$$1 + a\alpha^2 + b\beta^2 = 1 + a.a^{-1} + 0$$

$$= 1 + 1 = 0 \qquad (\text{char } F \ \ p = 2)$$

Thus $1 + a\alpha^2 + b\beta^2 = 0$ if F be finite field with characteristic $p = 2$.

Next if F be finite field with characteristic $p \neq 2$, then F has p^n elements.

Let $W_a = \left\{1 + ax^2 \mid x \in F\right\}$.

Then if $1 + ax^2 = 1 + ay^2$, for some $x, y \in F \quad \Rightarrow \quad x = \pm y$.

Thus for all $x, -x \in F, \quad 1 + ax^2 \in W_a$.

Also $0 \in F \Rightarrow 1 \in W_a$.

Therefore W_a contains $1 + \dfrac{p^n - 1}{2} = \dfrac{p^n + 1}{2}$ elements.

Similarly, $W_b = \left\{-bx^2 \mid x \in F\right\}$ contains $\dfrac{p^n + 1}{2}$ elements.

Since W_a and W_b more than half elements of F, $W_a \cap W_b \neq \phi$.

Let $c \in W_a \cap W_b$ then $c = 1 + a\alpha^2 = -b\beta^2 \Rightarrow 1 + a\alpha^2 + b\beta^2 = 0$ for some $\alpha, \beta \in F$.

5. SEPARABLE EXTENSIONS

Definition 5.1 : 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.

Definition 5.2 : 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.

Definition 5.3 : An algebraic extension E of a field F is called a separable extension if each element of E is separable over F.

Note :

1. By Corollary 3.4, any polynomial over a field of characteristic zero is separable. Thus, if F is a field of characteristic 0, then any algebraic extension of F is separable.
2. We know that, irreducible polynomials over finite fields have distinct roots. Hence, any algebraic extension ofa finite field is separable.
3. We know that, if $K = F(x)$ be the field of rational functions in one variable x over a field F of characteristic 3. Then the polynomial $y^3 - x$ in the polynomial ring $K[y]$ over K 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.

Definition 5.4 : A field F is called perfect if each of its algebraic extensions is separable.

Note.

1. Fields of characteristic zero and finite fields are perfect fields.
2. Infinite fields of characteristic $p > 0$ have inseparable extensions. Thus, such fields are not, in general, perfect.

Definition 5.5 : An extension E of a field F is called a simple extension if $E = F(\alpha)$ for some $\alpha \in E$.

Theorem 5.1 : If E is a finite separable extension of a field F, then E is a simple extension of F.

Proof : If F is a finite field, then by Corollary 4.7, each finite extension E of F is simple.

So suppose now that F is infinite.

Since E is a finite extension of F, $E = F(a_1,\ldots a_n)$, where $a_i \in E, 1 \le i \le n$, are algebraic over F.

We first show that if $E = F(\alpha,\beta)$, then there exists an element $\theta \in E$ such that $E = F(\theta)$. Then the result will follow by induction.

Let $p(x)$ and $q(x)$ be the minimal polynomials for α and β, respectively, over F. Let the roots of $p(x)$ be $\alpha = \alpha_1,\ldots,\alpha_n$, and let those of $q(x)$ be $\beta = \beta_1,\ldots,\beta_m$.

Since E is a separable extension of F, all $\alpha_i, 1 \le i \le n,$, and all $\beta_j, 1 \le j \le m,$, are distinct.

Since F is infinite, there exists $a \in F$ such that $a \neq (\alpha_i - \alpha)/(\beta - \beta_j)$ for $1 \leq i \leq n, 2 \leq j \leq m.$

Then $a(\beta - \beta_j) \neq \alpha_i - \alpha.$ So $a\beta + \alpha \neq \alpha_i + a\beta_j$ for $j \neq 1.$

Set $\theta = a\beta + \alpha$. Then $\theta - a\beta_j \neq \alpha_i$ for all $1 \leq i \leq n$ and $2 \leq j \leq m.$

Define $h(x) = p(\theta - ax) \in F(\theta)[x].$

Then $h(\beta) = p(\alpha) = 0$ and $h(\beta_j) = p(\theta - a\beta_j) \neq 0$ for $j \neq 1.$

So β isa root of $h(x)$, but no $\beta_j, j \neq 1$ is a root of $h(x)$.

Also, β is a root of $q(x)$. Regard $q(x) \in F(\theta)[x].$

Let $A(x) \in F(\theta)[x]$ be the minimal polynomial of β over $F(\theta)$.

Therefore $A(x) \mid h(x)$ and $A(x) \mid q(x)$.

Then any root of $A(x)$ is a root of $q(x)$ as well as a root of $h(x)$.

But the only common root of $q(x)$ and $h(x)$ is β.

Therefore, $A(x) = x - \beta$. This implies that $\beta \in F(\theta)$.

Then since $\theta = a\beta + \alpha,\ \alpha \in F(\theta)$.

Hence, $F(\alpha, \beta) = F(\theta)$.

Theorem 5.2 : Let E be a finite extension of a field F. Then the following are equivalent.

(a) $E = F(\alpha)$ for some $\alpha \in E$.

(b) There are only a finite number of intermediate fields between F and E.

Proof : (a) $\Rightarrow$ (b) Let $f(x) \in F[x]$ be the minimal polynomial of α over F.

Let K be a subfield of E containing F, and let $g(x)$ be the minimal polynomial of α over K.

Then since $g(x)$ is in $K[x]$, and $f(\alpha) = 0,\ g(x) \mid f(x).$

If K' is 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 irreducible over K'.

Also, $E = F(\alpha)$ implies $K(\alpha) = K'(\alpha) = E$.

Thus, $[E:K] =$ degree of $g(x) = [E:K']$.

Hence, $K = K'$.

Consider the mapping σ from the family of intermediate fields to the divisors of $f(x)$ in $E[x]$, given by $\sigma(K) = g(x)$, the minimal polynomial of α over K.

Then σ is 1-1. Since there are only finitely many divisors of $f(x)$, the family of intermediate fields between F and E is also finite.

(b) $\Rightarrow$ (a) If F is a finite field, then E is a finite field, and the result follows from Corollary 4.7.

So assume F is infinite. We first prove that for any two elements $\alpha, \beta \in E$ there is an element $\gamma \in E$ such that $F(\alpha, \beta) = F(\gamma)$.

For each $a \in F$ consider the linear combination $\gamma_a = \alpha + \alpha\beta$ of α and β.

The fields $F(\gamma_a)$ are intermediate fields between F and E.

Because there are only a finite number of intermediate fields, there exist $a, b \in F, a \neq b$, such that $F(\gamma_a) = F(\gamma_b)$.

But then $\gamma_a, \gamma_b \in F(\gamma_b)$ implies $\gamma_a, \gamma_b \in F(\gamma_b)$.

Thus, $(a-b)\beta \in F(\gamma_b)$, and, hence, $\beta \in F(\gamma_b)$.

Then $\gamma_b = \alpha + b\beta \in F(\gamma_b)$ implies $\alpha \in F(\gamma_b)$.

Therefore, $F(\alpha, \beta) \subset F(\gamma_b)$.

Since $F(\gamma_b) \subset F(\alpha, \beta)$, our assertion is proved.

We now choose $u \in E$ such that $[F(u):F]$ is as large as possible.

Then we claim $E = F(u)$. Otherwise let $x \in E, x \notin F(u)$.

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, $E = F(u)$.

Example 5.1 : 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 $F(\alpha)$ is a separable extension of F.

Solution : Let $\beta \in F(\alpha)$. We show that β is separable over F.

We have $F \subseteq F(\beta) \subseteq F(\alpha)$.

Let L be an algebraically closed field, and let $\sigma : F \to L$ be an embedding.

Suppose $p_1(x)$ is the minimal polynomial of β over F that has m distinct roots.

Then by Lemma, there are m distinct extensions, say $\sigma_1, \ldots, \sigma_m$, of σ to $F(\beta)$.

Further, let $p_2(x)$ be the minimal polynomial of α over $F(\beta)$, and suppose $p_2(x)$ has n distinct roots.

Then again by the same lemma, for each $\sigma_i, 1 \le i \le m,$ there are exactly n extensions $\sigma_{ij}, 1 \le j \le n,$, to $F(\alpha)$.

It is clear that the set of mn embeddings $(\sigma_{ij}), 1 \le j \le n, 1 \le i \le m,$ are the only possible embeddings from $F(\alpha)$ to L that extend $\sigma : F \to L$.

Now let $p_3(x)$ be the minimal polynomial of α over F. Then

$[F(\alpha):F]$ = degree $p_3(x)$.

= number of distinct roots of $p_3(x)$, since α is separable over F.

= number of extensions of the embedding σ to $F(\alpha)$.

Moreover, α is separable over F implies α is separable over $F(\beta)$, and, hence, by the same reasoning as in the previous paragraph,

$[F(\alpha):F(\beta)]$ = degree $p_2(x)$.

= number of distinct roots of $p_2(x)$.

= number of extensions of each σ_i to $F(\alpha)$.

= n.

Also,

$[F(\beta):F]$ = degree $p_1(x)$.

= number of distinct roots of $p_1(x)$.

= number of extensions of the embedding σ to $F(\beta)$.

= m.

Thus, $mn = [F(\alpha):F] = [F(\alpha):F(\beta)][F(\beta):F] = n \cdot$ degree $p_1(x)$.

Hence, m = degree $p_1(x)$ = the number of distinct roots of $p_1(x)$. Thus, $p_1(x)$ is a separable polynomial. Hence, β is separable over F.

Example 5.2 : 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 : From Theorem 5.1 we know that $E = F(\alpha), K = E(\beta)$ for some $\alpha \in E, \beta \in K$. Let $\gamma \in F(\alpha,\beta), \gamma \notin F(\alpha)$.

Then $F(\alpha)$ is a finite separable extension of F, and γ is a separable element over $F(\alpha)$.

We prove that γ is separable over F.

Let

$p_1(x)$ = the minimal polynomial of α over F with m,

$p_2(x)$ = the minimal polynomial of γ over $F(\alpha)$ with degree n,

$p_3(x)$ = the minimal polynomial of γ over F with degree s,

$p_4(x)$ = the minimal polynomial of α over $F(\gamma)$ with degree t.

Let $\sigma : F \to L$ be an embedding of F into an algebraically closed field L. Since α is separable over F, there are exactly m extensions $(\sigma_i), 1 \le i \le m,$, of σ to $F(\alpha)$.

Also, since γ is separable over $F(\alpha)$, again by Lemma , there are exactly n extensions of each σ_i to $F(\alpha, \gamma)$.

Let us these n extensions $\sigma_{i1}, \ldots, \sigma_{in}$, where $1 \le i \le m$.

Therefore, there are precisely mn extensions of $\sigma : F \to L$ to $\sigma_{ij} : F(\alpha, \gamma) \to L$, $1 \le i \le m, 1 \le j \le n$.

By considering extensions of $\sigma : F \to L$ to $F(\alpha, \gamma)$ via $F(\gamma)$, we obtain similarly that there are precisely st extensions to $F(\alpha, \gamma)$. Hence, $mn = st$.

Suppose γ is not separable over F. Then the number of extensions of σ to $F(\gamma)$ is $< s$.

This implies that the number of extensions of σ to $F(\alpha, \gamma)$ is $< st = mn$, a contradiction. Hence, γ is separable over F.

Example 5.3 : 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 p^{th} root in K).

Solution : Suppose K is perfect. Let a be any element of K.

We claim that there is an element b in K such that $a = b^p$.

We must show that the polynomial $f(x) = x^p - a$ has a root in K.

Let b be a root of $f(x)$ in some extension field of K.

Since K is perfect, b is separable over $K = K(a) = K(b^p)$.

Let $p(x)$ be the minimal polynomial for b over K.

Since b is a root of $x^p - b^p$ in $K[x]$, $p(x)$ is a factor of $x^p - b^p$ in $K[x]$.

In $K[x]$ we have the decomposition $x^p - b^p = (x-b)^p$.

So $p(x)$ is a power of $x-b$. But b is separable over K, so $p(x)$ has no multiple roots. Hence, $p(x) = x - b$.

Because $p(x) \in K[x]$, it follows that $b \in K$.

Conversely, suppose that every element of K is the p^{th} power of an element of K. To show that K is perfect, we show that every irreducible polynomial of $K[x]$ has distinct roots.

Let $p(x) \in K[x]$ be irreducible.

Now if roots of $p(x)$ are not distinct.

Then by Corollary 3.4, $p(x)$ has the form $a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_n x^{np}$, where $a_0, \ldots, a_n \in K$.

By hypothesis there exist elements $b_0, \ldots, b_n \in K$ such that $a_i = b_i^p$ $(i = 0,1,\ldots,n)$. Then, since K has characteristic p, $p(x) = \left(b_0 + b_1 x + \ldots + b_n x^n\right)^p$, which is a contradiction.

Thus every irreducible polynomial of $K[x]$ has distinct roots. Hence, K is perfect.

EXERCISE :

1. Determine the splitting field of $x^4 + x^2 + 1$ over $\mathbb{Q}$.

2. Find the degree of splitting field over $\mathbb{Q}$ of $x^4 + 2$.

3. If $F = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$, find $[F : \mathbb{Q}]$ and prove that F is not normal over $\mathbb{Q}$.

4. Verify that $\left(f(x) + g(x)\right)' = f'(x) + g'(x)$.

5. Construct fields with 4, 8, 9 and 16 elements.

6. Prove that a finite extension of a finite field is separable.

7. Prove that every extension of $\mathbb{Q}$ is separable.

8. Show that the field generated by a root of $x^3 - x - 1$over $\mathbb{Q}$ is not normal over $\mathbb{Q}$.

9. Prove that every finite extension of a finite field is normal.

10. Prove that in any finite field any element can be written as the sum of two squares

UNIT - III

GALIOS THEORY

UNIT I : AUTOMORPHISM GROUPS AND FIXED FIELDS :

Recall :

(i) Any finite separable extension E of a field F is simple i.e. $E = F(a)$ for some $a \in E$.

(ii) For any field E, the set Aut (E) of all automorphisms of E forms a group under the composition of mappings.

Note : Throughout this section, we confine ourselves to finite separable extension and their groups of automorphisms.

Definition 1.1 : Let F be a field and E be an extension of F. An automorphism σ of E is called an F-automorphism if σ fixes all elements of F.

Then $G(E/F) = \{\sigma \in \text{Aut}(E) \mid \sigma(a) = a \ \forall a \in F\}$ is called the group of F-automorphisms of E. Note that $G(E/F)$ is a subgroup of Aut (E).

Theorem 1.1 : Let E be a finite separable extension of a field F. Then

$$|G(E/F)| \leq [E : F]$$

Proof : Any finite separable extension E of F is a simple extension of F.

i.e. $E = F(a)$ for some $a \in E$.

Let $p(x)$ be the minimal polynomial of a over F and $\deg\big(p(x)\big) = n$. Then,

$$[E : F] = [F(a) : E] = \deg\big(p(x)\big) = n$$

Now, we know that if $\sigma : F \longrightarrow L$ be an embedding of F into an algebraically closed field L. Then σ can be extended to an embedding $\eta : E \longrightarrow L$ and the nmber of such extensions is equal to the number of distinct roots of the minimal polynomial $p(x)$ of a over F.

Since the extension E of F is separable, the minimal polynomial $p(x)$ of a over F has distinct roots in L.

Here consider $\sigma : F \longrightarrow L$ to be the identity map of F. Then σ can be extended to an embedding $\eta : E \longrightarrow L$ ($\eta|_F$ is the identity map of F) and the number of such extensions which fix all elements of F is equal to the degree of $p(x)$.

$\therefore |G(E/F)| \leq n = [E : F]$

EXAMPLES :

1) Consider $G = G(\mathbb{C}/\mathbb{R})$

Let $a, b \in \mathbb{R}$ and $\sigma \in G$

Then $\sigma(a+ib) = \sigma(a) + \sigma(i)\sigma(b)$

$= a + \sigma(i)b$ (since σ fixes all elements of $\mathbb{R}$)

Also, $-1 = \sigma(-1) = \sigma(i^2) = \sigma(i) \cdot \sigma(i)$

i.e. $\sigma(i)^2 = -1$

$\Rightarrow \sigma(i) = \pm i$

Hence, $\sigma(a+ib) = a + \sigma(i)b = a \pm ib$

Thus, G contains only two $\mathbb{R}$-automorphisms of $\mathbb{C}$.

Hence, $|G| = 2$.

Therefore, G is a cyclic group (since 2 is a prime)

2) Consider $G = G\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)$

$\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right] = 3$ since $x^3 - 2$ is the minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$.

And $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$ is a basis of $\mathbb{Q}\left(\sqrt[3]{2}\right)$ over $\mathbb{Q}$.

Let $a,b,c \in \mathbb{Q}$ and $\sigma \in G$

Then $\sigma\left(a + \sqrt[3]{2}b + \sqrt[3]{4}c\right) = \sigma(a) + \sigma(b)\left(\sqrt[3]{2}\right) + \sigma(c)\left(\sqrt[3]{4}\right)$

$$= a + b\sigma\left(\sqrt[3]{2}\right) + c\sigma\left(\sqrt[3]{4}\right)$$

Also, $\left(\sigma\left(\sqrt[3]{2}\right)\right)^3 = \sigma\left(\sqrt[3]{2}\right)^3 = \sigma(2) = 2$

$\therefore \sigma\left(\sqrt[3]{2}\right)$ is a cube root of 2.

$\therefore \sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$, $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2$ where $\omega^3 = 1$.

But $\omega \neq 1$.

Since $\sigma\left(\sqrt[3]{2}\right) \in \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{R}$, $\sigma\left(\sqrt[3]{2}\right)$ is real.

$\therefore$ The only possibility is $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$.

$\therefore \sigma\left(a + \sqrt[3]{2}b + \sqrt[3]{4}c\right) = a + \sqrt[3]{2}b + \sqrt[3]{4}c$

Hence, σ is the identity and G is the trivial group.

Definition 1.2 : Let E be any field and let H be a subgroup of the group of automorphisms of E, Aut (E). Then the set $E_H = \left\{a \in E \mid \sigma(a) = a \ \ \forall \sigma \in H\right\}$ is called the fixed field of H.

Note that E_H is a subfield of E.

Suppose $a,b \in E_H$.

Then $\sigma(a) = a$ and $\sigma(b) = b$, $\forall \sigma \in H$.

$\therefore \sigma(a-b) = \sigma(a) - \sigma(b)$

$$= a - b \qquad \forall \sigma \in H$$

$\Rightarrow a - b \in E_H$

Now suppose $a, b(\neq 0) \in E_H$

Then $\sigma(ab^{-1}) = \sigma(a) \cdot \sigma(b)^{-1}$

$= ab^{-1} \qquad \forall \sigma \in H$

$\Rightarrow ab^{-1} \in E_H$

$\therefore E_H$ is a subfield of E.

Also note that if E is a field extension of F and $H < G(E/F)$ then,

$F \subseteq E_H \subseteq E$

Theorem 1.2 : (Dedekind theorem) : Let F and E be fields, and let $\sigma_1, \sigma_2, ..., \sigma_n$ be distinct embeddings of F into E. Suppose that, for

$a_1, a_2, ..., a_n \in E, \ \sum_{i=1}^{n} a_i \sigma_i(a) = 0 \qquad \forall a \in F$

Then, $a_i = 0$ for all $i = 1, 2, ..., n$

(i.e. distinct embeddings of F into E are linearly independent over E)

Proof : Suppose, if possible that there exist $a_1, a_2, ..., a_n \in E$ not all zero, such that,

$a_1\sigma_1(a) + a_2\sigma_2(a) + ... + a_n\sigma_n(a) = 0 \qquad \forall a \in E$

Then we can find such a relation having a few non-zero coefficients as possible. On renumering, we can assume that this relation is

$b_1\sigma_1(a) + b_2\sigma_2(a) + ... + b_m\sigma_m(a) = 0 \qquad \forall a \in E \qquad ..... (1)$

Clearly, $m > 1$

Otherwise if $m = 1$ then $b_1\sigma_1(a) = 0 \quad \forall a \in E$

In particular if $a = 1$ then $b_1\sigma_1(1) = b_1 = 0$ which is contradiction since all b_i's are non-zero.

Therefore, $m > 1$

Now, $\sigma_1 \neq \sigma_m$ and hence there exists an element $c \in E$ such that $\sigma_1(c) \neq \sigma_m(c)$.

The equation (1) holds for all $a \in E$ and, in particular for ca $\forall a \in E$.

$\therefore b_1\sigma_1(ca) + b_2\sigma_2(ca) + ... + b_m\sigma_m(ca) = 0$

and hence,

$$b_1\sigma_1(c)\sigma_1(a) + b_2\sigma_2(c)\sigma_2(a) + ... + b_m\sigma_m(c)\sigma_m(a) = 0 \qquad ..... (2)$$

Multiplying eqn. (1) by $\sigma_1(c)$ and substracting it from eqn. (2) we get,

$$b_2\big(\sigma_2(c) - \sigma_1(c)\big)\sigma_2(a) + ... + b_m\big(\sigma_m(c) - \sigma_1(c)\big)\sigma_m(a) = 0 \quad \forall a \in E$$

This is a contradiction to the choice of equation (1), since

$$b_m\big(\sigma_m(c) - \sigma_1(c)\big) \neq 0$$

Therefore, $a_i = 0$ for all $i = 1, 2, ..., n$

Theorem 1.3 : Let H be a finite subgroup of the group of automorphisms of a field E. Then,

$$\big[E : E_H\big] = |H|$$

Proof : Let $H = \{e = g_1, g_2, ..., g_n\}$ and let

$$\big[E : E_H\big] = m$$

Suppose $m < n$.

Let $\{a_1, a_2, ..., a_m\}$ be a basis of E over E_H.

Consider the system of m homogeneous linear equations

$$g_1\big(a_j\big)x_1 + g_2\big(a_j\big)x_2 + ... + g_n\big(a_j\big)x_n = 0$$

$j = 1, 2, ..., m$, in 'n' unknowns x_1, x_2, ..., x_n.

Because $n > m$, this system has a nontrivial solution.

So there exist $y_1, y_2, ..., y_n \in E$, not all zero, such that

$$g_1(a_j)y_1 + g_2(a_j)y_2 + ... + g_n(a_j)y_n = 0$$

$\forall\ j = 1, 2, ..., m$

Let $a \in E$ be any element. Then,

$a = \alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_m a_m$ where $\alpha_1, ..., \alpha_m \in E_H$.

$$\therefore g_1(a)y_1 + g_2(a)y_2 + ... + g_n(a)y_n$$

$$= g_1\left(\sum_{i=1}^{m}\alpha_i a_i\right)y_1 + g_2\left(\sum_{i=1}^{m}\alpha_i a_i\right)y_2 + ... + g_n\left(\sum_{i=1}^{m}\alpha_i a_i\right)y_n$$

$$= \sum_{i=1}^{m}\alpha_i g_1(a_i)y_1 + ... + \sum_{i=1}^{m}\alpha_i g_n(a_i)y_n$$

$$= \sum_{i=1}^{m}\alpha_i\left(g_1(a_i)y_1 + g_2(a_i)y_2 + ... + g_n(a_i)y_n\right) = 0$$

$$g_2(a_2)\left(y_2 g(y_1) - g(y_2)y_1\right) + ... + g_j(a_r)\left(y_r g(y_1) - g(y_r)y_1\right) = 0 \quad ..... (5)$$

For $j = 1, 2, ..., n$

(5) is a system equations like (3) but with fewer terms, which is contradiction unless all the coefficients $y_i g(y_1) - y_1 g(y_i) = 0\ \forall\ i = 1, 2, ..., r$

If this happens i.e. $y_i g(y_1) - y_1 g(y_i) = 0$

Then $y_i y_1^{-1} = g\left(y_i y_1^{-1}\right) \quad \forall g \in H$.

Thus, $y_i y_1^{-1} \in E_H$

$\Rightarrow \exists\ z_1, z_2, ..., z_r \in E_H$ such that $y_i = y_1 z_i$,

for $i = 1, 2, ..., r$

In relation (3), take $j = 1$, we get

$$g_1(a_1)y_1 z_i + ... + g_1(a_r)y_1 z_r = 0$$

$$\Rightarrow g_1(a_1)z_1 + ... + g_1(a_r)z_r = 0 \qquad (\because y_1 \neq 0)$$

Since $z_i \in E_H$, $g_1(z_i) = z_i \quad \forall\ i = 1, 2, ..., r$

$\therefore g_1(a_1)g(z_1) + ... + g_1(a_r)g_1(z_r) = 0$

$\Rightarrow g_1(a_1z_1 + a_2z_2 + ... + a_rz_r) = 0$

Since $g_1 \in H < \text{Aut}(E)$, g_1 is one-one homomorphism on E.

$\therefore a_1z_1 + a_2z_2 + ... + a_rz_r = 0$

But $a_1, a_2, ..., a_r$ are linearly independent over E_H.

$\therefore$ We get $z_1 = z_2 = ... = 0 = z_r$.

$\Rightarrow y_1 = 0 = y_2 = ... = y_r$ which is contradiction to the fact that

$y_i \neq 0 \quad \forall\ i = 1, 2, ..., r$.

Hence, we have $[E : E_H] = n = |H|$.

Theorem 1.4 : Let E be a finite separable extension of a field F, let $H < G(E/F)$.

Then $G(E/E_H) = H$ and $[E : E_H] = |G(E/E_H)|$

Proof : If $\sigma \in H$ then $\sigma(a) = a \quad \forall\ a \in E_H$

$\therefore \sigma \in G(E/E_H)$

$\therefore H < G(E/E_H)$ ..... (1)

But from the theorem 1.3, we have

$|H| = [E : E_H]$ ..... (2)

Also by the theorem 1.1, we have

$|G(E/E_H)| \leq [E : E_H]$ ..... (3)

From (1), (2) and (3) we get $|H| \leq |G(E/E_H)| \leq [E : E_H] = |H|$

$\therefore H = G(E/E_H)$ and $[E : E_H] = |G(E/E_H)|$

Theorem 1.5 : Let E be a finite separable extension of a field F. Then the following are equivalent

(i) E is a normal extension of F.

(ii) F is the fixed field of $G(E/F)$.

(iii) $[E:F] = |G(E/F)|$.

Proof : Since E is a finite separable extension of F, $E = F(\alpha)$ for some $\alpha \in E$.

Let $p(x)$ be the minimal polynomial of α over F, and let its degree be n.

Then $[E:F] = [F(\alpha):F] = n$.

Let E_0 be the fixed field of $G(E/F)$ i.e.

$E_0 = \{s \in E \mid \sigma(s) = s \ \forall \sigma \in G(E/F)\}$

Then $F \subseteq E_0 \subseteq E$ and by the theorem 1.4,

$$[E:E_0] = |G(E/F)|$$

Claim : (i) $\Rightarrow$ (ii)

As we know the number of extensions of the inclusion mapping $F \longrightarrow \overline{F}$ to the embedding $F(\alpha) \longrightarrow \overline{F}$ is equal to the number of distinct roots of $p(x)$.

Since E is separable extension of F, $\alpha \in E$ is a separable element i.e. its minimal polynomial $p(x)$ over F has distinct roots.

So the number of distinct roots of $p(x)$ is equal to $n(= \deg p(x))$.

Also, $E = F(\alpha)$ is a normal extension of F. So E contains all the roots of $p(x)$.

Hence, any embedding $\sigma : F(\alpha) \longrightarrow \overline{F}$ shall map $F(\alpha)$ onto $F(\alpha)$.

Hence, any member of $G(E/F)$ is an extension of the inclusion mapping $F \longrightarrow \overline{F}$.

$\therefore |G(E/F)|$ = number of distinct roots of $p(x) = n$.

$\therefore [E:F] = n = |G(E/F)| = [E:E_0]$

and $[E:F]=[E:E_0][E_0:F]$

$\Rightarrow n=n[E_0:F]$

$\Rightarrow [E_0:F]=1$

$\Rightarrow E_0=F$ i.e. fixed field of $G(E/F)$ is F.

Claim : (ii) $\Rightarrow$ (i)

Let $G(E/F)=\{\sigma_1=\text{identity},\sigma_2,.....,\sigma_n\}$

Consider the polynomial $f(x)=(x-\sigma_1(\alpha))(x-\sigma_2(\alpha)).....(x-\sigma_n(\alpha))$.

Now, each $\sigma_i\in G(E/F)$ induces a natural homomorphism $\sigma_i^*:E[X]\longrightarrow E[X]$ as,

$\sigma_i^*(a_0+a_1x+.....+a_mx^m)=\sigma_i(a_0)+\sigma_i(a_1)x+.....+\sigma_i(a_m)x^m$

So $\sigma_i^*(f(x))=(x-(\sigma_i\sigma_1)(\alpha))(x-(\sigma_i\sigma_2)(\alpha)).....(x-(\sigma_i\sigma_n)(\alpha))$

But since $\sigma_i\sigma_1$, $\sigma_i\sigma_2$, ..., $\sigma_i\sigma_n$ are distinct members of $G(E/F)$ and are only a permutation of σ_1, σ_2, ... , σ_n.

$\therefore \sigma_i^*(f(x))=f(x) \quad \forall\ i=1,2,.....,n$

Now by expanding $f(x)$ we have,

$f(x)=x^n-c_1x^{n-1}+c_2x^{n-2}+.....+(-1)^nc_n$

where $c_i\in E$

Now, $\sigma_i^*(f(x))=f(x)$ implies

$\sigma_i(c_j)=c_j \qquad \forall\ i,j=1,2,.....,n$

$\Rightarrow c_j$ is in the fixed field of $G(E/F)$, which is F.

$\Rightarrow c_j\in F \qquad \forall\ j=1,2,.....,n$

$\Rightarrow f(x) \in F[x]$

Also, all the roots of $f(x)$ which are $\sigma_1(\alpha)$, $\sigma_2(\alpha)$, $\sigma_n(\alpha)$ lie in E.

Now, $E = F(\alpha)$ and α is one of the roots of $f(x)$, E is the splitting field of $f(x) \in F[x]$.

$\Rightarrow E$ is a normal extension of F. Hence the proof.

Claim : (ii) $\Rightarrow$ (iii)

F is the fixed field of $G(E/F)$.

Hence, by the theorem 1.4.

$[E:F] = |G(E/F)|$

Claim : (iii) $\Rightarrow$ (ii)

Let E_0 be the fixed of $G(E/F)$ then,

$F \subseteq E_0 \subseteq E$

Also, $[E:E_0] = |G(E/F)| = [E:F]$

$\Rightarrow E_0 = F$ i.e. F is the fixed field of $G(E/F)$.

EXERCISES :

1. Let $f(x) \in F[x]$ has r distinct roots in its splitting field E over F. Then prove that $G(E/F)$ is isomorphic to a subgroup of the symmetric group S_r of degree r.

Solution : Let $a_1, a_2, ..., a_r$ be all the distinct roots of $f(x)$ in its splitting E over F.

For any $\sigma \in G(E/F)$, $\sigma(a_i)$ is again a root of $f(x)$ in E.

Also, $\sigma(a_i) \neq \sigma(a_j)$ for $i \neq j$ since σ is F-automorphism.

Thus, $\sigma(a_1), \sigma(a_2), ..., \sigma(a_r)$ is a permutation of $a_1, a_2, ..., a_r$ and let us denote this permutation by ϕ_σ.

Therefore, $\phi_\sigma \in S_r$ for each $\sigma \in G(E/F)$.

Define $\phi : G(E/F) \longrightarrow S_r$ by

$$\phi(\sigma) = \phi_\sigma$$

Claim : ϕ is well-defined.

Let $\sigma_1, \sigma_2 \in G(E/F)$ such that

$\sigma_1 = \sigma_2$

$\Rightarrow \sigma_1(a_i) = \sigma_2(a_i) \qquad \forall\ i = 1, 2, ..., r$

Thus, $\sigma_1(a_1)$, $\sigma_1(a_2)$, ..., $\sigma_1(a_r)$ is a same permutation of a_1, a_2, ..., a_r as $\sigma_2(a_1)$, ..., $\sigma_2(a_r)$.

$\Rightarrow \phi_{\sigma_1} = \phi_{\sigma_2}$

$\Rightarrow \phi(\sigma_1) = \phi(\sigma_2)$

Hence, ϕ is well-defined.

Claim : ϕ is a group homomorphism

Let $\sigma, \eta \in G(E/F)$,

$$\phi(\sigma \circ \eta)(a_i) = (\sigma \circ \eta)(a_i)$$

$$= \sigma(\eta(a_i)) = (\phi(\sigma) \circ \phi(\eta))(a_i)$$

$$= (\phi_\sigma \phi_\eta)(a_i) \qquad \forall\ i = 1, 2, ..., r$$

$\Rightarrow \phi(\sigma \circ \eta) = \phi_\sigma \circ \phi_\eta$

Hence, ϕ is a group homomorphism.

Now, $\ker\phi = \{\sigma \in G(E/F) \mid \phi(\sigma) = \text{identity in } S_r\}$

If $\sigma \in \ker\phi$ then $\phi(\sigma) = \text{Identity in } S_r (Id)$.

$\Rightarrow \sigma(a_i) = a_i \qquad \forall\ 1 \le i \le r$

$\Rightarrow \sigma = Id$ since E is the splitting field of $f(x)$ over F, $E = F(a_1, a_2, ..., a_r)$

i.e. E is generated by $a_1,\ a_2, ...,\ a_r$ over F.

and σ fixes all the generators of E over F.

Hence, it should fix all the elements of E.

i.e. $\sigma = Id$.

$\Rightarrow \ker\phi = \{Id\}$

$\Rightarrow \phi$ is an injective group-homomorphism.

$\therefore G(E/F) \approx \phi(G(E/F))$ which is a subgroup of S_r .

2) The group $G(\mathbb{Q}(\alpha)/\mathbb{Q})$, where $\alpha^5 = 1$ and $\alpha \neq 1$, is isomorphic to the cyclic group of order 4.

Solution : $\alpha^5 = 1$

$\Rightarrow \alpha^5 - 1 = 0$

$\Rightarrow (\alpha - 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = 0$

Since $\alpha \neq 1 \Rightarrow \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$

Hence, α is a root of a polynomial

$p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$

$p(x)$ is a cyclotomic polynomial over $\mathbb{Q}$.

$\therefore p(x)$ is irreducible over $\mathbb{Q}$.

$\therefore [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg p(x) = 4$.

Also, the roots of $x^5 - 1$ are $1, \alpha, \alpha^2, \alpha^3, \alpha^4$.

So $\mathbb{Q}(\alpha)$ is the splitting field of $x^5 - 1$ over $\mathbb{Q}$.

Hence, $\mathbb{Q}(\alpha)$ is a normal extension of $\mathbb{Q}$.

$\therefore \left|G(\mathbb{Q}(\alpha)/\mathbb{Q})\right| = [\mathbb{Q}(\alpha):\mathbb{Q}] = 4$

A basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $\{1, \alpha, \alpha^2, \alpha^3\}$.

$\therefore$ Any element of $\mathbb{Q}(\alpha)$ looks like

$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3,\ a_i \in \mathbb{Q}$

The four $\mathbb{Q}$-automorphism of $\mathbb{Q}(\alpha)$ are as follows :

$\sigma_1 : a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \to a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$

$\sigma_2 : a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \to a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha^6$

$= a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha$

$\sigma_3 : a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \to a_0 + a_1\alpha^3 + a_2\alpha^6 + a_3\alpha^9$

$= a_0 + a_1\alpha^3 + a_2\alpha + a_3\alpha^4$

$\sigma_4 : a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \to a_0 + a_1\alpha^4 + a_2\alpha^8 + a_3\alpha^{12}$

$= a_0 + a_1\alpha^4 + a_2\alpha^3 + a_3\alpha^2$

and order of σ_2 and σ_3 in $G(\mathbb{Q}(\alpha)/\mathbb{Q})$ is 4.

$\therefore G(\mathbb{Q}(\alpha)/\mathbb{Q})$ is a cyclic group of order 4.

3) Let $E = \mathbb{Q}(w, \sqrt[3]{2})$, where $w^3 = 1$ but $w \neq 1$ and let H be the subgroup of $G(E/\mathbb{Q})$ given by $H = \{Id, \sigma\}$ where $\sigma : E \longrightarrow E$ is defined by $\sigma(a) = a \quad \forall a \in \mathbb{Q}$, $\sigma(w) = w^2$ and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}w^2$. Then find the fixed field E_H.

Solution : Let $c = \sqrt[3]{2}$

Then c is a real no. such that $c^3 = 2$.

We are given that $E = \mathbb{Q}(w, c)$ and $H = \{Id, \sigma\}$

where σ is defined by $\sigma / \mathbb{Q}$ = identity on $\mathbb{Q}$.

and $\sigma(w) = w^2$ and $\sigma(c) = cw^2$.

Note that $\mathbb{Q} \subset \mathbb{Q}(c) \subset \mathbb{Q}(c, w) = E$.

$\{1, c, c^2\}$ is a basis of $\mathbb{Q}(c)$ over $\mathbb{Q}$.

and $\{1, w\}$ is a basis of $\mathbb{Q}(w, c)$ over $\mathbb{Q}(c)$.

$\therefore$ The basis of E over $\mathbb{Q}$ is $\{1, c, c^2, w, cw, c^2w\}$.

Consider $a \in E$. Then,

$$a = r_0 + r_1c + r_2c^2 + r_3w + r_4cw + r_5c^2w$$

where $r_i \in \mathbb{Q}$.

Now, $\sigma(a) = r_0 + r_1cw^2 + r_2c^2w + r_3w^2 + r_4cw + r_5c^2$

$$= r_0 + r_1c(-1-w) + r_2c^2w + r_3(-1-w) + r_4cw + r_5c^2$$

(Since $1 + w + w^2 = 0 \Rightarrow w^2 = -1 - w$)

$$\therefore \sigma(a) = (r_0 - r_3) + (-r_1)c + r_5c^2 + (-r_3)w + (-r_1 + r_4)cw + r_2c^2w$$

$\therefore \sigma(a) = a$

$\Rightarrow r_0 - r_3 = r_0$, $-r_1 = r_1$, $r_2 = r_5$, $r_3 = -r_3$, $r_4 = -r_1 + r_4$ and $r_5 = r_2$.

$\Rightarrow r_3 = 0$, $r_1 = 0$, $r_2 = r_5$.

$$\therefore a = r_0 + r_2c^2 + r_4cw + r_2c^2w$$

$$= r_0 + r_2c^2(1 + w) + r_4cw$$

$$\therefore a = r_0 + r_4cw - r_2(cw)^2 \in \mathbb{Q}(cw)$$

$\therefore E_H \subseteq \mathbb{Q}(cw)$

On the other hand if $a \in \mathbb{Q}(cw)$.

Then $a = r_0 + r_1 cw + r_2 (cw)^2$ for some $r_i \in \mathbb{Q}$ and $\sigma(a) = a$.

Hence, $a \in E_H \Rightarrow \mathbb{Q}(cw) \subseteq E_H$.

Thus, the fixed field E_H of H is equal to $\mathbb{Q}(cw) = \mathbb{Q}(\sqrt[3]{2}w)$.

PROBLEMS :

1. Let $E = \mathbb{Q}(\sqrt[3]{2}, w)$ be an extension of a field $\mathbb{Q}$, where $w^3 = 1$, $w \neq 1$.

For each of the following subgroups S_i of the group $G(E/\mathbb{Q})$ find E_{S_i}.

(a) $S_1 = \{Id, \sigma_2\}$ where $\sigma_2 : \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2}w \\ w \to w^2 \end{cases}$

(b) $S_2 = \{Id, \sigma_3\}$ where $\sigma_3 : \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2}w \\ w \to w^2 \end{cases}$

(c) $S_3 = \{Id, \sigma_4, \sigma_5\}$ where

$\sigma_4 : \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2}w \\ w \to w \end{cases}$ and $\sigma_5 : \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2}w^2 \\ w \to w \end{cases}$

2. Let E be the spliting field of $x^4 - x^2 + 1$ over the field of rationals $\mathbb{Q}$. Then determine the group $G(E/\mathbb{Q})$.

3. Let $a \neq 1$ and $a^5 = 1$. Then prove that $\mathbb{Q}(a)$ is a normal extension of $\mathbb{Q}$ and that $G(\mathbb{Q}(a)/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_4$, the group of integers modulo 4.

UNIT II : FUNDAMENTAL THEOREM OF GALOIS THEORY

Definition 2.1 : 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.

Definition 2.2 : A finite, normal and separable extension E of a field F is called a Galois extension of F.

Example : If $f(x) \in F[x]$ is a polynomial over a field F of characteristic zero, then its splitting field E over F is a Galois extension of F.

Theorem 2.1 (Fundamental Theorem of Galois Theory)

Let E be a Galois extension of F. Let K be any subfield of E containing F (i.e. $E \subseteq K \subseteq F$). Then the mapping $K \longrightarrow G(E/K)$ 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 $G(E/F)$, $H = G\left(E/E_H\right)$.

(iii) $[E:K] = |G(E/K)|$, $[K:F]$ = 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 $G(K/F) \approx G(E/F)/G(E/K)$.

Proof :

(i) E is a normal extension of K.

$\therefore$ The fixed field of $G(E/K)$ is K.

i.e. $K = E_{G(E/K)}$.

(ii) As E is Galois extension of F, this extension is a finite separable extension of F.

Now, $H < G(E/F)$. Then clearly $H = G(E/E_H)$.

(iii) As E is a normal extension of F, and $E \supseteq K \supseteq F$ then E is also a normal extension of K.

$\therefore$ We have $[E:F] = |G(E/F)|$ and $[E:K] = |G(E/K)|$

Thus, $[E:F] = [E:K][K:F]$ gives

$$|G(E/F)| = |G(E/K)| \cdot [K:F]$$

$\Rightarrow [K:F]$ = index of $G(E/K)$ in $G(E/F)$.

(iv) Let $\overline{F}$ be an algebraic closure of F containing E. As we know if K is a normal of F if and only if each embedding $\sigma : K \longrightarrow \overline{F}$, which keeps each element of F fixed, maps K onto K.

Claim : K is a normal extension of F if and only if for each $\sigma \in G(E/F)$, $\sigma(K) = K$. If K is a normal extensionof F and $\sigma \in G(E/F)$ then σ restricted to K is an embedding of K into E and hence into $\overline{F}$. Therefore, $\sigma(K) = K$.

Conversely, let $\sigma : K \longrightarrow \overline{F}$ be an embedding that keeps each element of F fixed.

$\therefore \sigma$ can be extended to $\sigma^* : E \longrightarrow \overline{F}$. But then $\sigma^*(E) = E$, because E is a normal extension of F. Thus, $\sigma^* \in G(E/F)$.

As $\sigma^*(K) = K$, $\sigma(K) = K$. Therefore, K is a normal extension of F. This proves our claim.

Therefore, K is a normal extension of F if and only if for all $\sigma \in G(E/F)$ and $k \in K$, $\sigma(k) \in K$.

Then for all $\tau \in G(E/K)$, $\tau(\sigma(k)) = \sigma(k)$.

$\Rightarrow (\sigma^{-1}\tau\sigma)(k) = k \qquad \forall\, k \in K$.

Hence, $\sigma^{-1}\tau\sigma \in G(E/K)$.

$\Rightarrow G(E/K) \lhd G(E/F)$

Conversely, suppose $G(E/K) \lhd G(E/F)$.

Then $\tau(\sigma(k)) = \sigma(k) \ \ \forall \tau \in G(E/K)$.

$\Rightarrow \sigma(k) \in K$.

Therefore, K is a normal extension of F.

(v) Let K be a normal extension of F.

We know that $\sigma \in G(E/F)$ then $\sigma(k) = k$.

Thus, σ induces an automorphism $\sigma*$ of K defined by $\sigma*(k) = k$, $k \in K$.

$\Rightarrow \sigma^* \in G(K/F)$

Conider the mapping $f : G(E/F) \longrightarrow G(K/F)$ defined by,

$$f(\sigma) = \sigma*$$

Let $\sigma_1, \sigma_2 \in G(E/F)$. Then,

$$(\sigma_1 * \sigma_2 *)(k) = \sigma_1 * (\sigma_2 * (k)) = \sigma_1 * (\sigma_2 (k))$$

$$= (\sigma_1 \sigma_2)(k)$$

Therefore, $(\sigma_1 \sigma_2)* = \sigma_1 * \sigma_2 *$. Thus, f is a homomorphim of $G(E/F)$.

$\ker f = \{\sigma \in G(E/F) \mid \sigma^* = \text{ identity}\}$

But, σ^* = identity if and only if $\sigma*(k) = k \ \ \forall k \in K$.

That is $\sigma(k) = k \ \ \forall k \in K$, so $\sigma \in G(E/K)$.

Hence, $\ker f = G(E/K)$.

Then by the fundamental theorem of homomorphisms,

$$\frac{G(E/F)}{G(E/K)} \simeq \text{Im } f \subset G(K/F).$$

From (iii), we get

$$\left|\frac{G(E/F)}{G(E/K)}\right| = [K:F]$$

Since, K is a normal extenion over F,

$$|G(K/F)| = [K:F]$$

$$\therefore \left|\frac{G(E/F)}{G(E/K)}\right| \leq |\text{Im } f| < |G(K/F)| = [K:F]$$

$$\therefore \frac{G(E/F)}{G(E/K)} \simeq G(K/F)$$

EXAMPLES :

1. The Galois group of $x^3 - 2 \in \mathbb{Q}[x]$ is the group of symmetries of the triangle i.e. S_3.

Solution : Let E be the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

Hence, $E = \mathbb{Q}\left(\sqrt[3]{2}, w\right)$, where w is the root of the irreducible polynomial $x^2 + x + 1$ in $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

Hence, $E = \mathbb{Q}\left(\sqrt[3]{2}, w\right)$

$\Big\}2$ Basis is $\{1, w\}$

$\mathbb{Q}\left(\sqrt[3]{2}\right)$

$\Big\}3$ Basis is $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$

$\mathbb{Q}$

Hence, $[E:\mathbb{Q}] = 6$

Also, $x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}w\right)\left(x - \sqrt[3]{2}w^2\right)$

Since, E is a normal extension of $\mathbb{Q}$ and $[E:\mathbb{Q}]=6$, $|G(E/\mathbb{Q})|=6$.

These six automorphisms of E are determined by the manner in which they transform the roots of x^3-2.

The root $\sqrt[3]{2}$ can have only three images namely $\sqrt[3]{2}w$ and $\sqrt[3]{2}w^2$.

And the root w can have only two images, namely w and w^2.

The Galois group $G(E/\mathbb{Q})$ of x^3-2 over $\mathbb{Q}$ is given by the table, where

$G(E/\mathbb{Q})=\{Id,\sigma,\sigma^2,\tau,\sigma\tau,\sigma^2\tau\}$

	Id	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
$2^{1/3}$	$2^{1/3}$	$w\sqrt[3]{2}$	$w^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$w\sqrt[3]{2}$	$w^2\sqrt[3]{2}$
w	w	w	w	w^2	w^2	w^2

$S_3=\{(1),(1,2,3),(1,3,2),(1,2),(1,3),(2,3)\}$

Define an iomorphism from $G(E/\mathbb{Q})$ to S_3 as

$\sigma \mapsto (1,2,3)$ and $\tau \mapsto (1,2)$

Thus, $G(E/\mathbb{Q})\cong S_3$.

2. Let F be field of characteristic $\neq 2$.

Let $x^2-a\in[x]$ be an irreducible ploynomial over F. Then its Galois group is of order 2.

Solution : If α is a root of x^2-a then $-\alpha$ is the other root.

Also, $\alpha\neq-\alpha$ since $\mathrm{Ch}\,F\neq 2$.

Thus, x^2-a is separable over F.

Hence, the splitting field $F(\alpha)$ of $x^2 - a$ over F is a finite, separable and normal extension of degree 2 over F.

$\therefore \left|G(F(\alpha)/F)\right| = 2$

3. The Galois group of $x^4 - 2 \in \mathbb{Q}[x]$ is the octic group (i.e. group of symmetries of a square, D_4).

Solution : $x^4 - 2$ is irreducible over $\mathbb{Q}$ and its roots are $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$, $-\sqrt[4]{2}$.

$\therefore$ Spliting field of $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$.

Now, $x^2 + 1$ is irreducible polynomial over $\mathbb{Q}\left(\sqrt[4]{2}\right)$.

$\therefore \left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = 8$

As, $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$

$\Big\}2$ Basis is $\{1, i\}$

$\mathbb{Q}\left(\sqrt[4]{2}\right)$

$\Big\}4$ Basis is $\left\{\sqrt[4]{2}, 1, \sqrt[4]{4}, \sqrt[4]{8}\right\}$

$\mathbb{Q}$

$\therefore$ Basis for $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$ over $\mathbb{Q}$ is $\left\{1, i, \sqrt[4]{2}, \sqrt[4]{2}i, \sqrt[4]{4}, \sqrt[4]{4}i, \sqrt[4]{8}, \sqrt[4]{8}i\right\}$

Let $\beta \in E = \mathbb{Q}\left(\sqrt[4]{2}, i\right)$

Then $\beta = a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8} + a_4 i + a_5\left(i\sqrt[4]{2}\right) + a_6\left(i\sqrt[4]{4}\right) + a_7\left(i\sqrt[4]{8}\right)$

So if $\alpha \in G(E/\mathbb{Q})$ then

$$\sigma(\beta) = a_0 + a_1\sigma\left(\sqrt[4]{2}\right) + a_2\sigma\left(\sqrt[4]{2}\right)^2 + a_3\sigma\left(\sqrt[4]{2}\right)^3 + a_4\sigma(i)$$
$$+ a_5\sigma(i)\sigma\left(\sqrt[4]{2}\right) + a_6\sigma(i)\sigma\left(\sqrt[4]{2}\right)^2 + a_7\sigma(i)\sigma\left(\sqrt[4]{2}\right)^3$$

Therefore, σ is determined by $\sigma(i)$ and $\sigma\left(\sqrt[4]{2}\right)$.

But $\sigma(i)$ must be i or $-i$ and $\sigma\left(\sqrt[4]{2}\right)$ must be $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}i$, $-\sqrt[4]{2}$.

Since E over $\mathbb{Q}$ is Galois extension,

$\left|G(E/\mathbb{Q})\right| = [E:\mathbb{Q}] = 8$

Let $G(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, ..., \sigma_8\}$ where

$\sigma_1 : \sqrt[4]{2} \longrightarrow \sqrt[4]{2}$ $\qquad$ $\sigma_2 : \sqrt[4]{2} \longrightarrow i\sqrt[4]{2}$

$i \longrightarrow i$ $\qquad$ $i \longrightarrow i$

$\sigma_3 : \sqrt[4]{2} \longrightarrow -\sqrt[4]{2}$ $\qquad$ $\sigma_4 : \sqrt[4]{2} \longrightarrow -i\sqrt[4]{2}$

$i \longrightarrow i$ $\qquad$ $i \longrightarrow i$

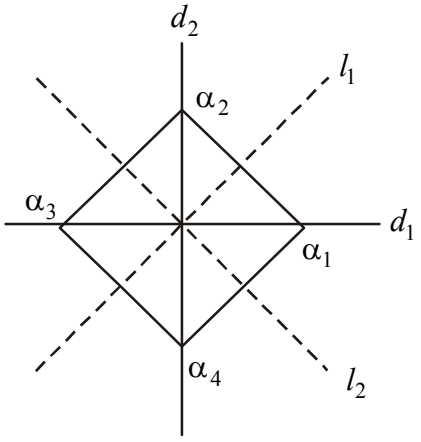
$\sigma_5 : \sqrt[4]{2} \longrightarrow \sqrt[4]{2}$ $\qquad$ $\sigma_6 : \sqrt[4]{2} \longrightarrow i\sqrt[4]{2}$

$i \longrightarrow i$ $\qquad$ $i \longrightarrow i$

$\sigma_7 : \sqrt[4]{2} \longrightarrow -\sqrt[4]{2}$ $\qquad$ $\sigma_8 : \sqrt[4]{2} \longrightarrow -i\sqrt[4]{2}$

$i \longrightarrow i$ $\qquad$ $i \longrightarrow i$

Let $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = i\sqrt[4]{2}$, $\alpha_3 = -\sqrt[4]{2}$, $\alpha_4 = -i\sqrt[4]{2}$.



Then the elements of $G(E/\mathbb{Q})$ permute the roots α_1, α_2, α_3, α_4 of x^4-2 as follows:

σ_1 : 0° rotation; σ_5 : reflection about d_1;

σ_2 : 90° rotation; σ_6 : reflection about l_1;

σ_3 : 180° rotation; σ_7 : reflection about d_2;

σ_4 : 270° rotation; σ_8 : reflection about l_2.

4. Let n be a positive integer, and let F be a field containing all the n^{th} roots of unity. Let K be the splitting field of $x^n-a \in F[x]$. Then $K=F(\alpha)$, where α is any root of x^n-a, and the Galois group $G(K/F)$ is abelian.

Solution : If $w=e^{2\pi i/n}$ and α is an root of x^n-a, then α, αw, ..., αw^{n-1} are all the roots of x^n-a. Thus, the splitting field of x^n-a over F is $K=F(\alpha)$.

Let $\sigma_1, \sigma_2 \in G(K/F)$.

Because α is root of x^n-a, $\sigma_1(\alpha)$ and $\sigma_2(\alpha)$ are also roots of x^n-a.

$\therefore \sigma_1(\alpha)=\alpha w^i$ and $\sigma_2(\alpha)=\alpha w^j$

For $0 \le i, j \le n-1$. Then

$$(\sigma_1\sigma_2)(\alpha)=\sigma_1(\sigma_2(\alpha))=\sigma_1(\alpha w^i)$$

$$=\sigma_1(\alpha)\sigma_1(w^i)$$

$$=\sigma_1(\alpha)w^i \qquad (\because w^i \in F)$$

$$=\alpha w^{j+i}$$

Similarly, $(\sigma_2\sigma_1)(\alpha)=\sigma_2(\sigma_1(\alpha))=\alpha w^{i+j}$.

Hence, $\sigma_1\sigma_2=\sigma_2\sigma_1$.

Thus, $G(K/F)$ is abelian.

Fundamental Theorem of Algebra

Theorem 2.2 : The field $\mathbb{C}$ has no extension of degree 2.

Proof : Let K be a field extension of $\mathbb{C}$ such that $[K:\mathbb{C}]=2$.

Then $\exists a \in K$ s.t. $K=\mathbb{C}(a)$.

Let $p(x)$ be the minimal polynomial of a over $\mathbb{C}$.

Then degree of $p(x)$ must be zero.

Let $p(x)=a+2bx+x^2$ where $a,b\in\mathbb{C}$.

Now, $p(x)=\left(x+b-\sqrt{b^2-a}\right)\left(x+b+\sqrt{b^2-a}\right)$

Where $b\pm\sqrt{b^2-a}\in\mathbb{C}$.

This is contradiction, since $p(x)$ is irreducible over $\mathbb{C}$.

Therefore, the field $\mathbb{C}$ has no extension of degree 2.

Theorem 2.3 : Let $f(x)\in\mathbb{R}[x]$ be of odd degree.

Then $f(x)$ has a real root.

Proof : Without loss of generality, we can assume that $f(x)$ is a monic polynomial.

Suppose $f(x)=a_0+a_1x+.....+a_{n-1}x^{n-1}+x^n$

where n is odd, $a_i\in\mathbb{R}$.

Let $s=1+|a_0|+|a_1|+.....+|a_{n-1}|$

Then, $|a_i|\le s-1 \quad \forall 0\le i\le n-1$.

$$\therefore \left|a_0+a_1s+.....+a_{n-1}s^{n-1}\right| \le (s-1)\left(1+s+....+s^{n-1}\right)$$

$$= s^{n-1} < s^n$$

Therefore, $f(s) > 0$. Also

$$f(-s) = a_0 - a_1 s + a_2 s^2 + \ldots\ldots + (-1)^{n-1} a_{n-1} s^{n-1} + (-s)^n$$

$$= a_0 - a_1 s + a_2 s^2 - \ldots\ldots - s^n \qquad (\because \ n \text{ is odd})$$

$$\leq s^n - 1 - s^n = -1 < 0$$

Therefore, $f(-s) < 0 < f(s)$ and $s \in \mathbb{R}$.

By the intermediate value theorem in analysis, $\exists$ a real number a s.t. $f(a) = 0$.

Thus, a is a root of $f(x)$ in $\mathbb{R}$.

Theorem 2.3 : Every polynomial $f(x) \in \mathbb{C}[x]$ factors into linear factors in $\mathbb{C}[x]$.

Proof : Let $f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$, $n > 0$

and $a_n \neq 0$ be a polynomial in $\mathbb{C}[x]$.

Put $g(x) = (x^2 + 1) f(x) \overline{f}(x)$

$$= (x^2 + 1)\left(a_0 + a_1 x + \ldots\ldots + a_n x^n\right)\left(\overline{a}_0 + \overline{a}_1 x + \ldots\ldots + \overline{a}_n x^n\right)$$

Then, $g(x) \in \mathbb{R}[x]$.

Let E be the splitting field of $g(x)$ over $\mathbb{R}$.

Then $\mathbb{R} \subseteq \mathbb{C} \subseteq E$ since i is a root of $g(x)$.

We prove that $E = \mathbb{C}$.

First observe that $[\mathbb{C} : \mathbb{R}] = 2$ and is a divisor of $[E : \mathbb{R}]$, since

$[E : \mathbb{R}] = [E : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2 \cdot [E : \mathbb{C}]$

$\therefore [E : \mathbb{R}]$ is an even positive integer.

Suppose that $[E : \mathbb{R}] = 2^m q$, where $m, q \in \mathbb{Z}^+$ an q is odd.

Let G be the Galois group $G(E/\mathbb{R})$. Since E is a normal extension of $\mathbb{R}$.

$|G| = |G(E/\mathbb{R})| = [E:\mathbb{R}] = 2^m q$

By the Sylow theorem in group theory,

$\exists$ a subgroup H of G such that $|H| = 2^m$ (i.e. H is a 2-Sylow subgroup of G).

Let E_H be the fixed field of H.

Then $\mathbb{R} \subseteq E_H \subseteq E$ and

$$2^m q = [E:\mathbb{R}] = [E:E_H][E_H:\mathbb{R}] = |H|[E_H:\mathbb{R}]$$

$$= 2^m [E_H:\mathbb{R}]$$

$\Rightarrow [E_H:\mathbb{R}] = q$.

Also, since E_H is a finite separable extension of $\mathbb{R}$, E_H is a simple extension of $\mathbb{R}$ and hence $E_H = \mathbb{R}(f)$ for some $f \in E_H$.

Let $q(x) = b_0 + b_1 x + \ldots\ldots + x^q \in \mathbb{R}[x]$ be the minimal polynomial of b over $\mathbb{R}$.

Note that $\deg q(x) = q = [\mathbb{R}(b):\mathbb{R}] = [E_H:\mathbb{R}]$.

Now, $\deg q(x)$ is odd, therefore $q(x)$ has a real root.

i.e. $q(r) = 0$ for some real no. r.

$\Rightarrow (x-r)$ is a factor of $q(x)$ in $\mathbb{R}[x]$.

But $q(x)$ is an irreducible polynomial over $\mathbb{R}$, since $q(x)$ is the minimal polynomial of b over $\mathbb{R}$.

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

i.e. $[E_H:\mathbb{R}] = 1 \Rightarrow E_H = \mathbb{R}$ and $[E:\mathbb{R}] = 2^m$

Claim : $m = 1$

Suppose, if possible $m > 1$.

Then $[E:\mathbb{C}] = 2^{m-1}$ and hence $|G(E/\mathbb{C})| = 2^{m-1}$.

Again, by the Sylow theorem, $G(E/\mathbb{C})$ has a subgroup S of order 2^{m-2}.

If E_S is the fixed field of S then

$$[E : E_S] = |S| = 2^{m-2}$$

Therefore, $[E_S : \mathbb{C}] = 2$, since $[E : \mathbb{C}] = 2^{m-1}$.

This is a contradiction to the fact that $\mathbb{C}$ has no extension of degree 2.

Therefore, $m = 1$ and $[E : \mathbb{R}] = 2$.

$\Rightarrow [E : \mathbb{C}] = 1$ and hence $E = \mathbb{C}$.

Thus, $\mathbb{C}$ is the splitting field of $g(x)$.

Thus, $\mathbb{C}$ contains all the roots of $g(x)$ and hence of $f(x)$.

Thus, $f(x)$ completely factors into linear factors in $\mathbb{C}[x]$.

EXERCISE :

1. Let $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, then find the Galois group $G(E/\mathbb{Q})$.

2. Let a be a real number such that $\mathbb{Q}(a)$ is a normal extension of $\mathbb{Q}$ for which $[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$ where $m \geq 0$.

Prove that there are fields $E_0 = \mathbb{Q} \subset E_1 \subset E_2 \subset \ldots\ldots \subset E_m = \mathbb{Q}(a)$ such that $[E_{i+1} : E_i] = 2$ for each $1 \leq i \leq m$.

UNIT III : CYCLOTOMIC POLYNOMIALS AND CYCLIC EXTENSIONS

Roots of Unity and Cyclotomic Polynomials :

Definition 3.1 : Let E be a field, and let n be a positive integer. An element $w \in E$ is called a primitive n^{th} root of unity in E if $w^n = 1$ but $w^m \neq 1$ for any positive integer $m < n$.

Consider $H = \{x \in \mathbb{C} \mid x^n = 1\}$

Note that,

1. H is a group under multiplication.
2. Also, H is a cyclic group generated by any primitive n^{th} root w of unity.
3. There are exactly $\phi(n)$ primitive n^{th} roots of unity for each positive integer n, where ϕ is Euler's ϕ-function.
4. These primitive n^{th} roots of unity are $\frac{\cos(2k\pi)}{n} + \frac{i\sin(2k\pi)}{n}$, where k is a positive integer less than n and relatively prime to n.

Theorem 3.1 : 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, the roots of $x^n - 1 \in F[x]$ form a cyclic group.

Proof : As U is a finite subgroup of the multiplicative group F^*, which is abelian, hence U is a finite abelian group.

$$\therefore U \approx S(p_1) \times S(p_2) \times ..... \times S(p_k)$$

where $|S(p_i)| = p_i^{r_i}$ and $p_1, p_k, ..., p_k$ are distinct primes.

Claim : $S(p_i)$ is cyclic $\forall\ i = 1, 2, ..., k$.

Let $a \in S(p_i)$ be such that $0(a)$ is maximal say $p_i^{s_i}$.

Because $0(a) \mid p_i^{r_i}$, we have $s_i \leq r_i$.

Also, for each $x \in S(p_i)$, $0(x) = p_i^{t_i} \le p_i^{s_i}$.

Therefore, $x^{p_i^{t_i}} = 1 \Rightarrow x^{p_i^{s_i}} = 1$.

Hence, $\forall x \in S(p_i)$, $x^{p_i^{s_i}} = 1$.

Because, the equation $x^{p_i^{s_i}} = 1$ has atmost $p_i^{s_i}$ roots.

$\therefore p_i^{s_i} \ge p_i^{r_i} \Rightarrow s_i = r_i$, since $p_i^{r_i} \ge p_i^{s_i}$.

$\therefore 0(a) = p_i^{r_i} = |S(p_i)|$ and hence $S(p_i)$ is a cyclic group generated by a.

Now, we know that if A and B are cyclic groups of orders m and n, respectively with $\gcd(m,n) = 1$, then $A \times B$ is again cyclic.

Here, each $S(p_i)$ is cyclic with cardinality $p_i^{r_i}$, and p_1, p_2, ..., p_k are distinct primes.

$\therefore \gcd\left(p_1^{r_1}, p_2^{r_2}, ..., p_k^{r_k}\right) = 1$

Hence, $S(p_1) \times S(p_2) \times ..... \times S(p_k)$ is cyclic but

$U \approx S(p_1) \times S(p_2) \times ..... \times S(p_k)$

Hence, U is cyclic.

Theorem 3.2 : 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 char $F = 0$ or char $F \nmid n$.

Proof : Let $f(x) = x^n - 1 \in F[x]$, and let char $F = 0$ or char $F \nmid n$. Then

$f'(x) = nx^{n-1} \ne 0$. Thus, $f(x)$ has n distinct roots (in its splitting field E over F), and they form a group, say H.

This group H, consisting of the n distinct roots of $x^n - 1$, is a cyclic group.

Now, if $w \in H$ is a generator of H, then $w^n = 1$, but $w^m \ne 1$ for any positive integer $m < n$. Hence, w is a primitive n^{th} root of unity in an extension E of F.

Conversely, let w be a primitive n^{th} root of unity in some extension field E of F.

Then, 1, w, w^2, ..., w^{n-1} are n distinct roots of $f(x) = x^n - 1$.

Otherwise if $w^i = w^j$ with $0 \le j \le i \le n-1$ then $w^{i-j} = 1$ with $0 < i - j < n$ which is contradiction to the fact that w is a primitive n^{th} root of unity.

So $f(x)$ doesn't possess multiple roots.

$\Rightarrow f'(x) = nx^{n-1} \neq 0$

$\Rightarrow \text{char } F = 0 \text{ or char } F \nmid n$.

Definition 3.2 : Let n be a positive integer, and let F be a field of characteristic zero or characteristic $p \nmid n$. Then the polynomial $\Phi_n(x) = \prod_w (x - w)$, where the product runs over all the primitive n^{th} roots w of unity (i.e. the primitive n^{th} root of $x^n - 1$ over F) is called the n^{th} cyclotomic polynomial.

For example, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$,

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

Theorem 3.3 : $\Phi_n(x) = \prod_w (x - w)$, w primitive n^{th} root in $\mathbb{C}$, is an irreducible polynomial of degree $\phi(n)$ in $\mathbb{Z}[x]$ (where ϕ is Euler's ϕ-function).

Proof : Let E be the splitting field of $x^n - 1 \in \mathbb{Q}[x]$.

Hence, the fixed field of $G(E/\mathbb{Q}) = \mathbb{Q}$.

Hence, any $\sigma \in G(E/\mathbb{Q})$, $\sigma(w)$ is again a primitive n^{th} root of unity, for any primitive n^{th} root w of unity.

Also, the induced mapping $\sigma^* : E[x] \longrightarrow E[x]$ keeps $\Phi_n(x)$ unaltered.

Thus, the coefficient of $\Phi_n(x)$ lie in the fixed field of $G(E/\mathbb{Q})$ i.e. $\Phi_n(x) \in \mathbb{Q}[x]$.

But, $\Phi_n(x)$ is a factor of $x^n - 1$ and $\Phi_n(x)$ is monic implies $\Phi_n(x) \in \mathbb{Z}[x]$.

Also, the number of primitive n^{th} roots of unity is $\phi(n)$ implies $\Phi_n(x)$ is of degree $\phi(n)$.

Claim : $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.

Let $f(x) \in \mathbb{Z}[x]$ be an irreducible factor of $\Phi_n(x)$ and let w be a root of $f(x)$, where w is a primitive n^{th} root of unity.

Claim : If p is a prime such that p doesn't divide n then w^p is also a root of $f(x)$.

Note that w^p is also a primitive n^{th} root of unity.

$\Rightarrow w^p$ is also a generator of the cyclic group consisting of the roots of $x^n - 1$.

Because $f(x) \in \mathbb{Z}[x]$ is a factor of $\Phi_n(x)$, there exists $h(x) \in \mathbb{Z}[x]$ such that

$$\Phi_n(x) = f(x)h(x).$$

So if w^p is not a root of $f(x)$, it must be a root of $h(x)$.

Thus, w is a root of $h(x^p)$. So $f(x)$ and $h(x^p)$ have a common factor over some extension of $\mathbb{Q}$. But this implies $f(x)$ and $h(x^p)$ have a common factor over $\mathbb{Q}$.

Also, $f(x)$ is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$. We get $f(x)$ divides $h(x^p)$.

$$\therefore h(x^p) = f(x) \cdot g(x)$$

$g(x)$ is also a monic polynomial over $\mathbb{Z}$, since $f(x)$ and $h(x^p)$ are monic polynomial over $\mathbb{Z}$.

Let $\overline{f}(x) = f(x) \pmod{p}$ and $\overline{h}(x) = h(x) \pmod{p}$.

i.e. polynomials obtained from $f(x)$ and $h(x)$ by replacing their coefficients $a \in \mathbb{Z}$ with $\overline{a} \in \mathbb{Z}_p$.

Now, $a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{Z}$.

$$\therefore \bar{h}(x^p) = (\bar{h}(x))^p$$

So $h(x^p) = f(x) \cdot g(x)$ gives that $\bar{h}(x)$ and $\bar{f}(x)$ have a common factor.

Thus, $\overline{\Phi_n}(x) = f(x)\bar{h}(x)$ and $\Phi_n(x) \mid (x^n - 1)$, we get that $x^n - \bar{1}$ has multiple roots. But this is not possible. For if α is a multiple root, then the derivative of $x^n - \bar{1}$ should vanish at $x = \alpha$; i.e. $\bar{n}\alpha^{n-1} = 0 \Rightarrow \alpha^{n-1} = 0$, since characteristic $p \nmid n$.

$\Rightarrow \alpha = 0$ but α is not a root of $x^n - 1$, we get a contradiction.

Thus, w is a root of $f(x)$, then w^p is also a root of $f(x)$.

Now, any primitive n^{th} root of unity can be obtained by raising w to a succession of prime powers, with primes not dividing n, this implies that all primitive n^{th} roots of unity are roots of $f(x)$.

Hence, $f(x) = \Phi_n(x)$ i.e. $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.

Theorem 3.4 : Let w be a primitive n^{th} root of unity in $\mathbb{C}$. Then $\mathbb{Q}(w)$ is the splitting field of $\Phi_n(x)$ and also of $x^n - 1 \in \mathbb{Q}[x]$.

Further, $[\mathbb{Q}(w) : \mathbb{Q}] = \phi(n) = [G(\mathbb{Q}(w)/\mathbb{Q})]$ and $G(\mathbb{Q}(w)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$, the multiplicative group formed by the units of $\mathbb{Z}_n$.

Proof : The minimal polynomial of w is $\Phi_n(x)$ and $\mathbb{Q}(w)$ contains a primitive n^{th} root of unity, it contains all n^{th} roots of unity.

$\therefore \mathbb{Q}(w)$ is the splitting field of $\Phi_n(x)$ and of $x^n - 1$.

Also, $[\mathbb{Q}(w) : \mathbb{Q}]$ = degree of $\Phi_n(x) = \phi(n)$.

Since, $\mathbb{Q}(w)$ is a finite, separable and normal extension of $\mathbb{Q}$ (i.e. Galois extension of $\Phi_n(x)$ over $\mathbb{Q}$),

$\left|G\left(\mathbb{Q}(w)/\mathbb{Q}\right)\right| = \phi(n) = \left[\mathbb{Q}(w):\mathbb{Q}\right]$

If $\sigma \in G\left(\mathbb{Q}(w)/\mathbb{Q}\right)$, then $\sigma(w)$ is also a primitive n^{th} root of unity.

$\therefore \sigma(w) = w^j$, where $j < n$ and $\left(j,n\right) = 1$.

Denote this σ by σ_j.

We know that there are $\phi(n)$ no. of such j's, and they are precisely the members of the group $\mathbb{Z}_n^*$.

Let $f : \mathbb{Z}_n^* \longrightarrow G\left(\mathbb{Q}(w):\mathbb{Q}\right)$ be a map defined by $f\left(j\right) = \sigma_j$.

Claim : f is well-defined and one-one.

$\sigma_j = \sigma_k$ with $j,k < n$ and $\left(j,n\right) = \left(k,n\right) = 1$.

$\Rightarrow \sigma_j(w) = \sigma_k(w)$

$\Rightarrow w^j = w^k$

$\Rightarrow w^{j-k} = 1$

If $j \neq k$ then $j - k < n$ and $w^{j-k} = 1$ which is contradiction to the fact that w is a primitive n^{th} root of unity.

$\therefore j = k \Rightarrow f$ is one-one.

And if $j = k$ for $j,k \in \mathbb{Z}_n^*$.

Then $w^j = w^k$.

$\Rightarrow \sigma_j(w) = \sigma_k(w)$

$\Rightarrow \sigma_j = \sigma_k$ ($\because \sigma_j, \sigma_k$ agree on w, hence agree on every element of $\mathbb{Q}(w)$)

$\Rightarrow f\left(j\right) = f\left(k\right)$

$\therefore$ f is well-defined.

Claim : f is a homomorphism.

Let $j,k \in \mathbb{Z}_n^*$.

Write $jk = qn + r$ with $r < n$.

Now, $jk \pmod n = r$ i.e. in $\mathbb{Z}_n^*$, $jk = r$.

$w^{jk} = w^{qn+r} = w^r$

$f(jk) = f(r) = \sigma_r = \sigma_{jk} = \sigma_j \sigma_k = f(j) f(k)$

$\therefore \mathbb{Z}_n^* \simeq G(\mathbb{Q}(w)/\mathbb{Q})$.

Remark : If p is an odd prime, then $(\mathbb{Z}p^e)^*$ is a cyclic group.

Hence, $G(\mathbb{Q}(w)/\mathbb{Q})$, where w is a primitive p^e th root of unity ($e > 0$), is a cyclic group of order $\phi(p^e) = p^{e-1}(p-1)$.

EXAMPLES :

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

Solution : $x^4 + x^2 + 1 = y^2 + y + 1$ where $y = x^2$.

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

So the splitting field of $x^4 + x^2 + 1$ will contain the square roots of $e^{2\pi i/3}$ and $e^{4\pi i/3}$.

Now, $(e^{2\pi i/3})^{1/2} = \pm e^{\pi i/3}$ and $(e^{4\pi i/3})^{1/2} = \pm e^{2\pi i/3}$.

So $E = \mathbb{Q}(\alpha)$, where $\alpha = e^{\pi i/3}$, is the splitting field of $x^4 + x^2 + 1 \in \mathbb{Q}[x]$.

But $e^{\pi i/3} = e^{2\pi i/6} = \alpha$ is a primitive 6th root of unity, E is the splitting field of $x^6 - 1$.

Then $G(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \mathbb{Z}_6^*$ and $|\mathbb{Z}_6^*| = \phi(6) = 2$

Hence, $G(\mathbb{Q}(\alpha)/\mathbb{Q})$ is of order 2.

CYCLIC EXTENSIONS :

Definition 3.3 : 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.

EXAMPLES :

1. If w is a primitive p^{th} root of unity and the splitting field of $x^p - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(w) = E$ (say). Then E is a Galois extension of $\mathbb{Q}$.

$\therefore G(\mathbb{Q}(w)/\mathbb{Q}) \approx \mathbb{Z}_p^*$ and $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

$\therefore \mathbb{Q}(w)$ is a cyclic extension of $\mathbb{Q}$.

Lemma 3.1 : 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 of F, is an embedding of F into itself. (The mapping $\Pi_1(x) = x^p$ is called the Frobenius endomorphism).

Proof : Consider a map $\Pi_k : F \longrightarrow F$ defined by $\Pi_k(x) = x^{p^k} \quad \forall x \in F$.

Claim : Π_k is well-defined.

Let $x, y \in F$ such that $x = y \Rightarrow x^{p^k} = y^{p^k}$.

$\Rightarrow \Pi_k(x) = \Pi_k(y)$. Hence, Π_k is well-defined.

Claim : Π_k is injective.

Suppose $\Pi_k(x) = \Pi_k(y)$.

$\Rightarrow x^{p^k} = y^{p^k} \Rightarrow x^{p^k} - y^{p^k} = 0$

$\Rightarrow (x-y)^{p^k} = 0 \qquad (\because$ Characteristic of $F = p \neq 0)$

$\Rightarrow x - y = 0 \qquad (\because F$ is a field hence integral domain)

$\Rightarrow x = y$

Therefore, Π_k is injective.

$\therefore \Pi_k$ is an embedding of F into itself for every positive integer k.

Lemma 3.2 : Let E be a finite extension of F.

Suppose $f : G(E/F) \longrightarrow E^*$, $E^* = E - \{0\}$ has the property that $f(\sigma\eta) = \sigma f(\eta) \cdot f(\sigma)$ for all $\sigma, \eta \in G = G(E/F)$. Then there exists $\alpha \in E^*$ such that $f(\sigma) = \sigma(\alpha^{-1})\alpha \quad \forall \sigma \in G$.

(The mapping f in the hypothesis of the lemma is called a crosed homomorphism.)

Proof : For all $\eta \in G$, $f(\eta) \in E^*$, so $f(\eta) \neq 0$.

Thus, if $\sum_{\eta \in G} f(\eta)\eta(b) = 0 \quad \forall b \in E^*$.

Then by the Dedekind lemma, $f(\eta) = 0$, which is not true. Hence, there exists $b \in E^*$, such that

$$\alpha = \sum_{\eta \in G} f(\eta)\eta(b) \neq 0$$

Then for any $\sigma \in G$, we get

$$\sum_{\eta \in G} \sigma\big(f(\eta)\big)\sigma\big(\eta(b)\big) = \sigma(\alpha)$$

Then, by using $\sigma\big(f(\eta)\big) = f(\sigma)^{-1} f(\sigma\eta)$, we get

$$\sum_{\eta \in G} \big(f(\sigma)\big)^{-1} f(\sigma\eta) \cdot \sigma\eta(b) = \sigma(\alpha)$$

But $\{\sigma\eta \mid \eta \in G\} = \{\eta \mid \eta \in G\}$

Hence, $\big(f(\sigma)\big)^{-1} \sum_{\eta \in G} f(\eta) \cdot \eta(b) = \sigma(\alpha)$

$\Rightarrow \left(f(\sigma)\right)^{-1} \cdot \alpha = \sigma(\alpha)$

$\Rightarrow \alpha\sigma\left(\alpha^{-1}\right) = f(\sigma) \qquad \forall \sigma \in G$

Hence, the proof.

Lemma 3.3 : 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 be $w \in E$ such that

$w \cdot \sigma(w) \cdot \sigma^2(w) \ldots \sigma^{n-1}(w) = 1$, then there exists $\alpha \in E^*$ such that $w = \sigma(\alpha) \cdot \alpha^{-1}$.

Proof : By lemma 3.2, we need to define $f : G \longrightarrow E^*$ such that $f(\sigma) = w$ for some $\sigma \in G$ and f is a crossed homomorphism.

Define $f : G \longrightarrow E^*$ as follows :

$f(id) = 1$, $f(\sigma) = w$ and $f\left(\sigma^i\right) = \sigma^{i-1}(w) \ldots\ldots \sigma(w) \cdot w$ for $2 \le i \le n-1$.

Claim : f is a crossed homomorphism i.e.

$$f(\sigma\eta) = \sigma\left(f(\eta)\right) \cdot f(\sigma)$$

Let $\sigma^i, \sigma^j \in G$. If $i + j \equiv 0 \pmod{n}$ then

$f\left(\sigma^i \cdot \sigma^j\right) = f\left(\sigma^{i+j}\right) = f\left(\sigma^n\right) = f(id) = 1$

Also, $\sigma^i\left(f\left(\sigma^j\right)\right) f\left(\sigma^i\right)$

$= \sigma^i\left(\sigma^{j-1}(w) \ldots\ldots \sigma(w) \cdot w\right)\left(\sigma^{i-1}(w) \ldots\ldots \sigma(w) \cdot w\right)$

$= \sigma^{n-1}(w) \cdot \sigma^{n-2}(w) \ldots\ldots \sigma^i(w) \ldots\ldots \sigma(w) \cdot (w)$

$= f\left(\sigma^n\right)$

$= 1$

If $i + j \not\equiv 0 \pmod{n}$, then

$f(\sigma^i\sigma^j) = f(\sigma^{i+j}) = f(\sigma^r) = \sigma^{r-1}(w)\cdot\sigma^{r-2}(w)....\sigma(w)\cdot w$

$i+j = qn+r$ where and $r < n,\ r \neq 0$.

Now, consider

$$\sigma^i \cdot f(\sigma^j) f(\sigma^i) = \sigma^i\left(\sigma^{j-1}(w)\cdot\sigma^{j-2}(w).....\sigma(w)\cdot w\right)\cdot$$

$$\left(\sigma^{j-1}(w)\cdot\sigma^{j-2}(w).....\sigma(w)\cdot w\right)$$

$$= \sigma^{i+j-1}(w)\cdot\sigma^{i+j-2}(w).....\sigma^{i+1}(w)\cdot\sigma^i(w).....\sigma(w)w$$

$$= \sigma^{r-1}(w)\cdot\sigma^{r-2}(w).....\sigma(w)w$$

$$= f(\sigma^r)$$

Hence, f is a crossed homomorphism.

Therefore, using Lemma 3.3, $\exists\ \alpha \in E^*$.

Such that $f(\sigma) = \sigma(\alpha^{-1})\cdot\alpha$.

i.e. $w = \sigma(\alpha^{-1})\cdot\alpha$.

Hence, the proof.

Theorem 3.5 : Let F be a field and contain a primitive n^{th} root w 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 an irreducible polynomial $x^n - b \in F[x]$.

Furthermore note $E = F(\alpha)$, where α is a root of $x^n - b$.

Proof : (i) $\Rightarrow$ (ii)

Let σ be a generator of the finite cyclic group $G(E/F)$.

By Lemma 3.3, there exists $\alpha \in E^*$ such that $\sigma(\alpha) = w\alpha$.

$\therefore \sigma^i(\alpha) = w^i\alpha \qquad \forall i = 1, 2, ...$

$$\therefore \sigma^i(\alpha^n) = (\sigma^i(\alpha))^n$$

$$= (w^i\alpha)^n$$

$$= w^{in} \cdot \alpha^n = \alpha^n$$

Thus, $\alpha^n \in F$, and if $b = \alpha^n$, then $x^n - b \in F[x]$ and $x^n - b = \prod_{i=1}^{n}(x - w^i\alpha)$.

Claim : $x^n - b \in F[x]$ is irreducible over F.

Suppose $x^n - b = f(x) \cdot g(x)$, where $f(x)$ is nonconstant irreducible monic polynomial over *F*.

If $w^i\alpha$ is one root of $f(x)$, then for each positive integer j we have,

$\sigma^{j-i}(w^i\alpha) = \sigma^{j-i}(w^i)\sigma^{j-i}(\alpha)$

But $w^i \in F$ (Since *F* contains a primitive n^{th} root *w* of unity).

So $\sigma^{j-i}(w^i) = w^i$ and also $\sigma^{j-i}(\alpha) = w^{j-i} \cdot \alpha$.

Thus, we have

$\sigma^{j-i}(w^i\alpha) = w^i \cdot w^{j-i} \cdot = w^j \cdot \alpha$

Because any *F*-automorphism maps a root of a polynomial over *F* onto a root of that polynomial, we get that $w^j\alpha$ is also a root of $f(x)$.

Hence, all the roots of $x^n - b$ are roots of $f(x)$.

Thus, $f(x) = x^n - b$. Therefore, $x^n - b$ is irreducible over *F*.

Also, $E = F(\alpha)$, where α is a root of $x^n - b$ (since *F* contains n^{th} root of unity) and *E* is the splitting field of $x^n - b$ over *F*.

Claim : (ii) $\Rightarrow$ (i)

Let $c \in E$ be a root of . So $b = c^n$. Clearly, then, *c*, *cw*, cw^2, ..., cw^{n-1} are *n* distinct roots of $x^n - b$, where $w \in F$ is a primitive n^{th} root of unity.

Thus, $x^n - b$ is a separable irreducible polynomial.

Hence, $E = F(c)$ is a Galois extension of F.

For each $\sigma \in G(E/F)$, let $\chi(\sigma)$ be defined by

$$\chi(\sigma) = \{k \in \mathbb{Z} \mid \sigma(c) = w^k c\}$$

Then $\chi(\sigma) \neq \phi$ becuase $\sigma(c)$ is also a root of $x^n - b$.

Moreover, for any $k \in \chi(\sigma)$, $\chi(\sigma) = \overline{k} \in \mathbb{Z}/n\mathbb{Z}$, for $w^k c = w^j c$ if and only if $k \equiv j \pmod{n}$.

Further if, $\sigma, \tau \in G(E/F)$ and if $\sigma(c) = w^k c$ and $\tau(c) = w^j c$, then

$$(\sigma\tau)(c) = \sigma\left(w^j c\right) = w^j \sigma(c) = w^{j+k}(c)$$

So $\chi(\sigma\tau) = \chi(\sigma) + \chi(\tau) \pmod{n}$

Finally, if $\chi(\sigma) = \overline{0}$ then $\sigma(c) = c$.

So σ is identity on E because $E = F(c)$.

Hence, χ is an isomorphism from $G(E/F)$ onto a subgroup of the additive group $\mathbb{Z}_n$.

Also, $[F(c):F]$ = degree of the minimal polynomial of c over F

= degree of $x^n - b$

$= n.$

Because $E = F(c)$ is a Galois extension,

$|G(E/F)| = [E:F] = n$ and $G(E/F) \approx$ subgroup of $\mathbb{Z}_n$.

$\Rightarrow G(E/F) \approx \mathbb{Z}_n$ (which is a cyclic group)

Hence, E is a cyclic extension of degree n over F.

EXERCISE :

1. If a field F contains a primitive n^{th} root of unity, then the characteristic of F is 0 or a prime p that does not divide n.

2. Let F contain a primitive n^{th} root of unity, and let E be the splitting field of $x^m - b$ over F, where $m \mid n$ and m is prime. Then either $E = F$ or $x^m - b$ is irreducible over F. What can you say of m is not prime ?

UNIT - IV

POLYNOMIALS SOLVABLE BY RADICALS AND SYMMETRIC FUNCTIONS

POLYNOMIALS SOLVABLE BY RADICALS

Definition 4.1 : An extension E of a field F is an extension of radicals (or radical extension) if there are elements $\alpha_1, \alpha_2, ..., \alpha_r \in E$ and positive integers $n_1, n_2, ..., n_r$ such that

$$E = F(\alpha_1, \alpha_2, ..., \alpha_r) \text{ and } \alpha_i^{n_i} \in F(\alpha_1, \alpha_2, ..., \alpha_{i-1}),\ 1 < i \le r .$$

Example : $\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{7})$ is a radical extension of $\mathbb{Q}$.

$$(\sqrt[3]{2})^3 = 2 \in \mathbb{Q} \text{ and } (\sqrt[5]{7})^5 = 7 \in \mathbb{Q}(\sqrt[3]{2})$$

Theorem 4.1 : If E_r is a radical extension of $F = E_0$ with intermediate field $E_1, ..., E_{r-1}$ such that $E_1 \subseteq E_2 \subseteq ..... \subseteq E_{r-1}$, then there exists a radical extension E_s' of $F = E_0$ with intermediate fields $E_1', E_2', ..., E_{s-1}'$ ($E_1' \subseteq E_2' \subseteq ..... \subseteq E_{s-1}'$) such that

(i) $E_s' \supset E_r$

(ii) E_s' is a normal extension of F.

(iii) E_i' is a splitting field of a polynomial of the form $x^{m_i} - b_i \in E_{i-1}'[x],\ i = 1, 2, ..., s.$

Proof : We have an ascending chain of fields $F = E_0 \subset E_1 \subset ..... \subset E_r$ such that $E_i = E_{i-1}(\alpha_i)$ $(1 \le i \le r)$ and α_i is a root of $x^{n_i} - a_i \in E_{i-1}[x]$.

Let w be a primitive n^{th} root of unity, where $n = n_1, n_2, ..., n_r$.

Now, consider

$E_1(w)$

|

$E_0(w) = F(w)$

|

$E_0 = F$

Now, $E_1(w)$ is a radical extension of F.

Since $F = E_0 \subset F(w) = E_0(w) \subset E_1(w)$

$E_1(w) = F(w, \alpha_1)$ such that $w^n \in F$ and $\alpha_1^{n_i} \in F(w)$.

Also, $F(w)$ is a splitting field of $x^n - 1 \in F[x]$, hence is a normal extension of F.

$\Rightarrow$ F is the fixed field of $G(F(w)/F)$.

$$\Rightarrow f_1(x) = \prod_{\sigma \in G(F(w)/F)} \left(x^{n_1} - \sigma(a_1)\right) \in F[x]$$

Here, $f_1(x) = \left(x^{n_1} - a_1\right)^k$, $k = \left|G(F(w)/F)\right|$ since $a_1 \in F$.

Now, consider $g_1(x) = (x^n - 1) f_1(x)$. Then $g_1(x) \in F[x]$.

Let K be the splitting field of $g_1(x)$ over F.

$\Rightarrow$ K is a normal extension of F. Clearly, $\alpha_1 \in K$, $w \in K$ and $E_1 \subset K$.

$\Rightarrow$ There is a finite ascending chain of fields between F and K such that each field is a splitting field of a polynomial of the form $x^m - b$ over the precending field.

Similarly, we construct a field L such that L contains the field K and E_2 and is a normal extension of F.

Construction : Consider a polynomial

$$g_2(x) = g_1(x) f_2(x) \text{ where } f_2(x) = \prod_{\sigma \in G(K/F)} \left(x^{n_2} - \sigma(a_2)\right)$$

Now, K is a normal extension over F, $f_2(x) \in F[x]$.

$\Rightarrow g_2(x) \in F[x]$. Let L be the splitting field of $g_2(x)$ over F.

$\Rightarrow \alpha_2 \in L$ and $K \subseteq L$. Hence, $E_1(\alpha_2) = E_2 \subset L$.

$\Rightarrow$ L is a normal extension of F containing E_2.

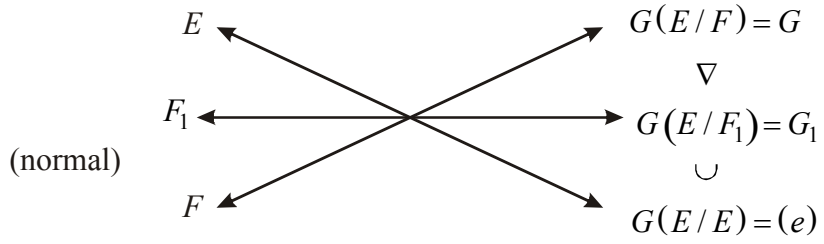
Continuing like this, we can construct a radical extension E_s' of F having the desired properties.

Definition 4.2 : A polynomial $f(x) \in F[x]$ over a field F is said to be solvable by radicals if its splitting field E is contained in some radical extension of F.

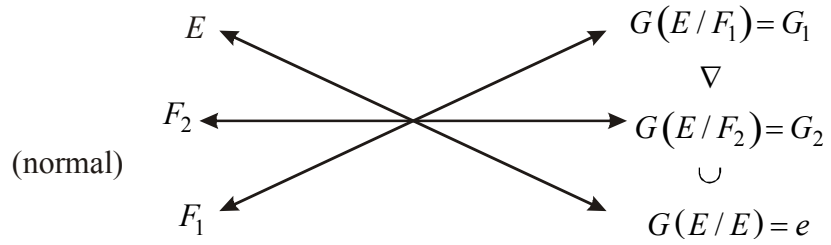
Note : We assume that all fields are of characteristic zero.

Theorem 4.2 : $f(x) \in F[x]$ is solvable by radicals over F if and only if its splitting field E over F has solvable Galois group G (E / F).

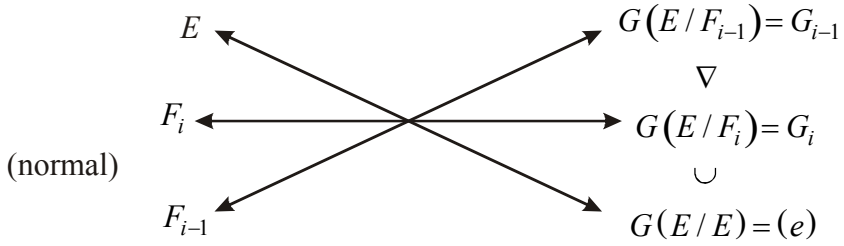
Proof : First suppose that G (E / F) is solvable. Because the characteristic of F is zero, E is a normal separable extension. So $[E : F] = |G(E/F)| = n$, say. Assume first that F contains a primitive n^{th} root of unity. Then F contains primitive n^{th} roots of unity for all positive integers m that divide n. Let $G = G(E/F)$. Because G is solvable and finite, there is a chain $G = G_0 \supset G_1 \supset .... \supset G_r = (e)$ of subgroups of G such that $G_i \lhd G_{i-1}$ and $G_i \lhd G_{i-1}$ is cyclic. Let $F = F_0 \subset F_1 \subset .... \subset F_r = E$ be the corresponding subfields of E given by the fundamental theorem. Then $E_{G_i} = F_i$ and $G(E/F_i) = G_i$. Also, by the fundamental theorem, $G_1 = G(E/F_1) \lhd G(E/F) = G$ implies 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.



Continue in this way to show that F_i is a normal extension of F_{i-1}.



Furthermore, $G(F_i/F_{i-1}) = G(E/F_{i-1})/G(E/F_i) = G_{i-1}/G_i$ by the fundamental theorem. So F_i is a cyclic extension of F_{i-1}. Also, F_i is the splitting field of an irreducible polynomial $x^{n_i} - b_i \in F_{i-1}[x]$ and $F_i = F_{i-1}(\alpha_i)$, where $\alpha_i^{n_i} = b_i \in F_{i-1}$. Then $E = F(\alpha_1, ..., \alpha_r)$, $\alpha_1^{n_1} \in F$ and $\alpha_1^{n_1} \in F_{i-1} = F(\alpha_1, ..., \alpha_{i-1})$ for $1 < i \le r$. Thus, $f(x)$ is solvable by radicals over F.

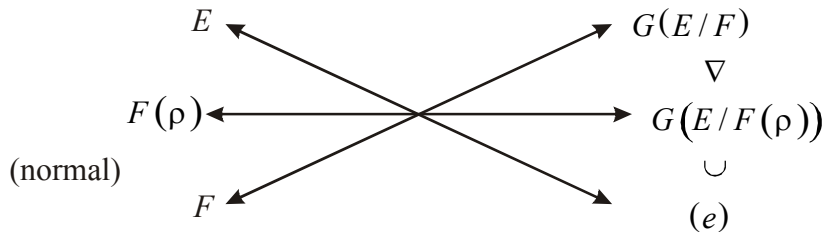
Next we drop the assumption that F contains a primitive n^{th} root of unity. The polynomial $x^n - 1 \in E[x]$ has roots in $\overline{E}$. Let ρ be a primitive n^{th} root of unity lying in $\overline{E}$. Then $E(\rho)$ is the splitting field of $f(x)$ regarded as a polynomial over $F(\rho)$. Any $F(\rho)$-automorphism σ of $E(\rho)$ will leave the coefficients of the polynomial $f(x)$ unaltered. Now, for any automorphism $\sigma \in G(E(\rho)/F(\rho))$, we have $\sigma_0 = \sigma|_E \in G(E/F)$, since E is a normal extension of F. Further, the map $\sigma \mapsto \sigma_0$ is a $1-1$ homomorphism of the group $G(E(\rho)/F(\rho))$ into $G(E/F)$. Then since a subgroup of a solvable group is solvable,

$G\big(E(\rho)/F(\rho)\big)$ is solvable. Now by the first part, $E(\rho)$ is a radical extension of $F(\rho)$; so $E(\rho)$ is a radical extension of F. Then the splitting field E of $f(x)\in F[x]$ is contained in the radical extension $E(\rho)$ of F, so $f(x)$ is solvable by radicals.

Before we prove the converse, we prove a lemma that deals with a particular case.

Lemma 4.1 : Let E be the splitting field of $x^n-a\in F[x]$. Then $G(E/F)$ is a solvable group.

Proof : If F contains a primitive n^{th} root of unity, then we know that $G(E/F)$ is abelian and, hence, solvable. Now suppose that F does not contain a primitive n^{th} root of unity. Let $\rho\in\overline{F}$ be a generator of the cyclic group of the n^{th} roots of unity. Let b be a root of x^n-a. Then $b\rho$ is also a root. So $\rho=b^{-1}(b\rho)$ is in the splitting field E of $x^n-a\in F[x]$. Consider $F\subset F(\rho)\subset E\cdot F(\rho)$ is a normal extension of F, since $F(\rho)$ is the splitting field of x^n-1; so $G\big(E/F(\rho)\big)$ is a normal subgroup of $G(E/F)$ by the fundamental theorem of Galois theory.



But $G\big(E/F(\rho)\big)$ is abelian, because E is the splitting field of $x^n-a\in F[x]$. So $(e)\lhd G\big(E/F(\rho)\big)\lhd G(E/F)$ is a normal series. Again by the fundamental theorem of Galois theory, $G(E/F)/G\big(E/F(\rho)\big)\simeq G\big(F(\rho)/F\big)$, which is abelian (being isomorphic to $(Z/(n))^*$ because $F(\rho)$ is the splitting field of x^n-1. So $G(E/F)$ has a normal series with abelian factors whose last element is the trivial group. Therefore, $G(E/F)$ is solvable.

We are now ready to complete the proof of the theorem.

If a polynomial $f(x) \in F[x]$ is solvable by radicals, we may, without any loss of generality, assume that the splitting field E of $f(x)$ is contained in a radical extension E_r of F such that E_r is a normal extension of F and there exist intermediate fields $E_1, \ldots, E_{r-1}$ such that E_i is a splitting field of a polynomial of the form $x^{m_i} - b_i \in E_{i-1}[x]$. Thus, by the fundamental theorem of Galois theory

$$(e) \subset G(E_r / E_{r-1}) \subset G(E_r / E_{r-2}) \subset \ldots \subset G(E_r / F)$$

is a normal series. Also,

$$G(E_r / E_{r-i}) / G(E_r / E_{r-i+1}) \simeq G(E_{r-i+1} / F_{r-i})$$

is solvable. Then,

$$(e) \subset G(E_r / E_{r-1}) \subset G(E_r / E_{r-2}) \subset \ldots \subset G(E_r / F)$$

is a normal series with solvable quotient groups, so $G(E_r / F)$ is solvable. Further, since $G(E / F) \simeq G(E_r / F) / G(E_r / E)$, $G(E / F)$ is a homomorphic image of $G(E_r / F)$. Hence, it is solvable.

Remark : We know that the symmetric group S_n is not solvable if $n \geq 5$. Thus, any polynomial whose Galois group is S_n, $n \geq 5$, is not solvable by radicals.

Recall the important fact that the Galois group of a polynomial $f(x) \in F[x]$ having r distinct roots is embedable in the symmetric group S_r, the group of all permutations of the r distinct roots $(\alpha_1, \ldots, \alpha_r)$.

We call a subgroup H of S_n a transitive permutation group if, for all $i, j \in \{1, 2, \ldots, n\}$, there exists $\sigma \in H$ such that $\sigma(i) = j$.

We also recall the following result from group theory.

If p is a prime number and if a subgroup G of S_p is a transitive group of permutations containing a transportation (a, b), then $G = S_p$.

Theorem 4.3 : Let $f(x)$ be a polynomial over a field F with no multiple roots. Then $f(x)$ is irreducible over F if and only if the Galois group G of $f(x)$ is isomorphic to a transitive permutation group.

Proof : Let $\alpha_1,.....,\alpha_n$ be the roots of $f(x)$ in some splitting field E. Then for each $\sigma \in G$, $\sigma(\alpha_1),....,\sigma(\alpha_n)$ is a permutation of $\alpha_1,.....,\alpha_n$. We may look upon G as a subgroup of S_n.

First assume $f(x)$ is irreducible over F. Then for each $i = 1, ..., n$

$$F(\alpha_i) \simeq F[x]/(f(x))$$

in which $\alpha_i \mapsto x+(f(x))$, $a \mapsto a+(f(x))$, $a \in F$. This isomorphism induces the isomorphism $\eta : F(\alpha_i) \to F(\alpha_j)$, where $\alpha_i \mapsto \alpha_j$ and $a \mapsto a$, $a \in F$. But since E is a normal extension of F, η can be extended to an F-homomorphism $\eta^* : E \to E$. Then $\eta^* \in G(E/F)$ and $\eta^*(\alpha_i) = \alpha_j$. Thus, G is a transitive permutation group.

Conversely, let F be transitive. Let $p(x)$ be the minimal polynomial for α_1 over F. Suppose α_i is any root. Because G is transitive, there exists $\sigma \in G$ such that $\sigma(\alpha_1) = \alpha_i$. Then $p(\alpha_i) = p(\sigma(\alpha_1)) = \sigma p(\alpha_1) = 0$. Hence, each α_i is a root of $p(x)$. Because $p(x) \mid f(x)$, it follows that $f(x) = cp(x)$, $c \in F$. Thus, $f(x)$ is irreducible over F.

Theorem 4.4 : Let $f(x) \in Q[x]$ be a monic irreducible polynomial over Q of degree p, where p is prime. If $f(x)$ has exactly two nonreal roots in C, then the Galois group of $f(x)$ is isomorphic tp S_p.

Proof : Let $E \subset C$ be a splitting field of $f(x)$ over Q. $G(E/Q)$ is isomorphic to a transitive permutation group H, which is a subgroup of S_p. Let $\alpha_1,....,\alpha_p$ be roots of $f(x)$, and let α_i be its complex root. Because $f(x) \in Q[x]$, α_i is also a root of $f(x)$. Hence, $\overline{\alpha_i} = \alpha_j$ for some $1 \le j \le p$, $j \ne i$. Consider the embedding $\sigma : z \mapsto \overline{z}$ from E to Q. Because E is a normal extension of Q, σ maps E onto E. Thus, $\sigma \in G(E/Q)$. Then the permutation of the roots $\alpha_1,....,\alpha_p$ of $f(x)$ corresponding to the element σ of the Galois group $G(E/Q)$

takes α_i to α_j and α_j to α_i, and keeps all α_k $(k \neq i, j)$ fixed. Hence, $H \simeq S_p$. Thus, $G(E/Q) \simeq S_p$, as required.

EXAMPLES :

(a) Show that if an irreducible polynomial $p(x) \in F[x]$ over a field F has a root in a radical extension of F, then $p(x)$ is solvable by radicals over F.

Solution : Let E_r be a radical extension of F. Then there exists a radical extension E_s' of F such that $E_s' \supset E_r$ and E_s' is a normal extension of F. Because $p(x)$ is irreducible over F and has a root in E_r, it has a root in E_s'. But because E_s' is a normal extension of F, it follows that E_s' contains a splitting field of $p(x)$. This shows that $p(x)$ is solvable by radicals.

(b) Show that the polynomial $x^7 - 10x^5 + 15x + 5$ is not solvable by radicals over Q.

Solution : By Eisentein's criterion $f(x) = x^7 - 10x^5 + 15x + 5$ is irreducible over Q. Further, by Descartes's rule of signs it is known that

The number of positive real roots $\leq$ The number of changes in signs in $f(x) = 2$,

and The number of negative real roots $\leq$ The number of changes in signs in $f(-x) = 3$.

Thus, the total number of real roots ≤ 5. Moreover, by the intermediate value theorem there are 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 nonreal roots. By theorem 4.4 the Galois group of $f(x)$ is S_7. Hence, by Theorem 4.2 $f(x)$ is not solvable by radicals.

PROBLEMS :

1. Show that the following polynomials are not solvable by radicals over Q :

(a) $x^5 - 9x + 3$ (b) $2x^5 - 5x^4 + 5$

(c) $x^5 - 8x + 6$ (d) $x^5 - 4x + 2$

2. Let $F[x_1, x_2, x_3]$ be a polynomial ring in x_1, x_2, x_3 over a field F. Let $K = F(x_1, x_2, x_3)$ be the field of rational functions (i.e. the field of fractions of the ring $F[x_1, x_2, x_3]$). Suppose

$$f(t) = t^3 - x_1 t^2 + x_2 t - x_3 \in K[t]$$

Prove that the Galois group of $f(t)$ over K is S_3. Generalize this result to a polynomial of degree n (see Theorem 4.1).

SYMMETRIC FUNCTIONS :

In this section we give an application of Galois theory to the symmetric functions. Let F be a field, and let $y_1, \ldots, y_n$ be n indeterminates. Consider the field of rational functions $F(y_1, \ldots, y_n)$ over F. If σ is a permutation of $\{1, \ldots, n\}$ – that is, $\sigma \in S_n$ – then σ gives rise to a natural map.

$$\bar{\sigma} : F(y_1, \ldots, y_n) \to F(y_1, \ldots, y_n)$$

given by,

$$\bar{\sigma}\left(\frac{f(y_1, \ldots, y_n)}{g(y_1, \ldots, y_n)}\right) = \frac{f(y_{\sigma(1)}, \ldots, y_{\sigma(n)})}{g(y_{\sigma(1)}, \ldots, y_{\sigma(n)})},$$

where $f(y_1, \ldots, y_n)$, $g(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$ and $g(y_1, \ldots, y_n) \neq 0$. It is immediate that $\bar{\sigma}$ is an automosphism of $F(y_1, \ldots, y_n)$ leaving each element of F fixed.

Definition 4.3 : An element $f(y_1, \ldots, y_n)/g(y_1, \ldots, y_n)$ of $F(y_1, \ldots, y_n)$ is called a symmetric function in $y_1, \ldots, y_n$ over F if it is left fixed by all permutations of 1, ..., n that is, for all $\sigma \in S_n$.

$$\bar{\sigma}\left(\frac{f(y_1, \ldots, y_n)}{g(y_1, \ldots, y_n)}\right) = \frac{f(y_1, \ldots, y_n)}{g(y_1, \ldots, y_n)}$$

Let $\overline{S}_n$ be the group of all F-automosphisms $\overline{\sigma}$ of $F(y_1,....,y_n)$ corresponding to $\sigma \in S_n$. Obviously, $\overline{S}_n \simeq S_n$. Let K be the subfield of $F(y_1,....,y_n)$ that is the fixed field of $\overline{S}_n$. Consider the polynomial

$$f(x) = \prod_{i=1}^{n}(x - y_i)$$

Now $f(x) \in F(y_1,....,y_n)[x]$. Clearly, the natural mapping

$$F(y_1,....,y_n)[x] \to F(y_1,....,y_n)[x]$$

induced by each $\overline{\sigma} \in \overline{S}_n$ leaves $f(x)$ unaltered. Thus, the coefficients of $f(x)$ are unaltered by each $\overline{\sigma} \in \overline{S}_n$. Hence, the coefficients lie in the fixed field K.

Let us write the polynomial $\overline{\sigma} \in \overline{S}_n$ as $x^n + a_1x^{n-1} + a_2x^{-2} + ... + a_n$, where $a_i \in K$.

Definition 4.4 : If a_i is the coefficient of x^{n-i} in the polynomial $f(x) = \prod_{i=1}^{n}(x - y_i)$, then $(-1)^i a_i$ is called the i^{th} elementary symmetric function in $y_1,....,y_n$ and is denoted by s_i.

Thus,

$$s_1 = y_1 + y_2 + ... + y_n,$$

$$s_2 = y_1y_2 + y_1y_3 + ... + y_{n-1}y_n,$$

$$\vdots$$

$$s_n = y_1y_2 \cdots y_n.$$

Theorem 4.5 : Let $s_1,....,s_n$ be the elementary symmetric functions in the indeterminates $y_1, \ldots, y_n$. Then every symmetric function in $y_1, \ldots, y_n$ over F is a rational function of the elementary symmetric functions. Also, $F(y_1,....,y_n)$ is a finite normal extension of $F(y_1,....,y_n)$ of degree $n!$, and the Galois group of this extension is isomorphic to S_n.

Proof : Consider the field $E = F(s_1, ..., s_n)$. Becausee K is the field of all symmetric functions in $y_1, ..., y_n$ over F, $E \subset K$. Also, because $F(y_1, ..., y_n)$ is a splitting field of the polynomial $f(x) = \prod_{i=1}^{n}(x - y_i)$, of degree *n* over E, we have,

$$\left[F(y_1, ..., y_n) : E\right] \leq n! \qquad \text{..... (1)}$$

Further,

$$\left[F(y_1, ..., y_n) : K\right] \geq \left|\overline{S}_n\right| = n! \qquad \text{..... (2)}$$

But since $E \subset K$, we obtain from (1) and (2) that E = K.

Now $f(x)$ is a separable polynomial over E, and $F(y_1, ..., y_n)$ is its splitting field. Thus $F(y_1, ..., y_n)$ is a finite, separable, normal extension of E.

$$\left[F(y_1, ..., y_n) : E\right] \geq \left|G\left(F(y_1, ..., y_n)/E\right)\right| \qquad \text{..... (3)}$$

Because $G\left(F(y_1, ..., y_n)/E\right)$ is embeddable in S_n, and $\left[F(y_1, ..., y_n) : E\right] = n!$, we get from (3) that,

$$G\left(F(y_1, ..., y_n)/E\right) \simeq S_n$$

Finally, the fact that K = E shows that every symmetric function can be expressed as a rational function of the elementary symmetric functions $s_1, ..., s_n$.

EXAMPLE :

1) 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) $(x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2$

Solution :

(a) $\left(x_1^2+x_2^2+x_3^2\right)=\left(x_1+x_2+x_3\right)^2-2\left(x_1x_2+x_2x_3+x_3x_1\right)=s_1^2-2s_2$

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

$$y_1=x_1-\frac{s_1}{3},\quad y_2=x_2-\frac{s_1}{3},\quad y_3=x_3-\frac{s_1}{3}$$

are the roots of $x^3+3\alpha x+\beta=0$, where

$$\alpha=\frac{-s_1^2}{3}+s_2,\quad \beta=-s_3-\frac{2s_1^3}{27}+\frac{s_1s_2}{3}.$$

Then the cubic equation whose roots are $\left(y_1-y_2\right)^2$, $\left(y_2-y_3\right)^2$ and $\left(y_3-y_1\right)^2$ is

$$\left(3\alpha+y\right)^3+9\alpha\left(3\alpha+y\right)^2+27\beta^2=0 \qquad \text{..... (1)}$$

Now, $\left(x_1-x_2\right)^2\left(x_2-x_3\right)^2\left(x_3-x_1\right)^2=\left(y_1-y_2\right)^2\left(y_2-y_3\right)^2\left(y_3-y_1\right)^2$

$$=\text{Product of all the roots of (1)}$$

$$=-27\left(\beta^2+4\alpha^3\right)$$

PROBLEM :

1. Express the following symmetric functions as rational functions of elementary symmetric functions.

(a) $x_1^3+x_2^3+x_3^3$

(b) $x_1^2+x_2^2+x_2^2x_3^2+x_3^2x_1^2$

(c) $\left(x_1^2+x_2^2\right)\left(x_2^2+x_3^2\right)\left(x_3^2+x_1^2\right)$

(d) $\left(x_1+x_2\right)^3\left(x_2+x_3\right)^3\left(x_3+x_1\right)^3$

UNIT - V

RULER AND COMPASS CONSTRUCTIONS

The theory of fields provides solutions to many ancient geometric problems. Among such problems are the following :

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.

For these we must translate the geometric problem into an algebraic problem. We shall regard the plane as the coordinate plane R^2 of analytic geometry. Let $P_0 \subset R^2$. Assume P_0 has at least two points. We construct an ascending chain of subsets P_i of R^2, $i = 0, 1, 2, \ldots$, inductively as follows : Let P_{i+1} be the union of P_i and the set of points obtained by intersection of (i) two distinct lines each passing through two distinct points in P_i, or (ii) two distinct circles each with its center in P_i and passing through another point in P_i, or (iii) a line and a circle of the types described in (i) and (ii).

Suppose that the coordinates of points in P_0 belong to a subfield of K of R. The equation of a line passing through two distinct points in P_0 and the equation of a circle whose center is in P_0 and that passes through another point in P_0 are

$$ax + by + c = 0, \qquad a, b, c \in K \qquad \ldots\ldots (1)$$

$$x^2 + y^2 + 2gx + 2fy + d = 0, \qquad g, f, d \in K \qquad \ldots\ldots (2)$$

respectively.

It follows then that the coordinates of the point of intersection of two such lines (1) lie in K. Also, the coordinates of the points of intersection of a line (1) and a circle (2), as well as

the coordinates of the ponts of intersection of two distinct circles (2), lie in $K\left(\sqrt{\alpha_1}\right)$, $\alpha_1 > 0$, $\alpha_1 \in K$. Likewise, we get that the coordinates of points in P_i lie in $K\left(\sqrt{\alpha_1},....,\sqrt{\alpha_i}\right)$, $\alpha_1,.....,\alpha_i > 0$, $\alpha_1 \in K$, $\alpha_2 \in K\left(\sqrt{\alpha_1}\right),.....,\alpha_i \in K\left(\sqrt{\alpha_1},....,\sqrt{\alpha_{i-1}}\right)$.

Definition 5.1 : (a) A point X is constructible from P_0 if $X \in P_i$ for . $i \in \{0,1,2,....\}$.

(b) A line *l* is constructible from P_0 if it passes through two distinct points in some P_i, $i \in \{0,1,2,....\}$.

(c) A circle C is constructible from P_0 if its center is in some P_i, and it passes through another point in P_i, $i \in \{0,1,2,....\}$.

From now on whenever a point X (a line *l*, a circle C) is constructible from $Q \times Q$, we shall also say that the point X (the line *l*, the circle C) is constructible.

DEfinition 5.2 : A real number *u* is constructible from Q if the point (*u*, 0) is constructible from $Q \times Q$, the subset of the plane R^2.

It then follows from all this that if $u \in R$ is constructible from Q, then there exists an ascending chain.

$$Q = K_0 \subset K_1 \subset K_2 \subset .... \subset K_n$$

of subfields K_1, K_2, ..., K_n of R such that.

(i) $u \in K_n$

(ii) $K_i = K_{i-1}(\alpha_i)$, $1 \le i \le n$, where $\alpha_i^2 \in K_{i-1}$.

Thus, $\left[K_i : K_{i-1}\right] \le 2$ and, hence, $\left[K_n : Q\right] = 2^m$, $m \le n$.

So we have shown.

Theorem 5.1 : Let $u \in R$ 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.

Theorem 5.2 : 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.

Before we prove this theorem, we prove a series of lemmas.

Lemma 5.1 : The following are equivalent statements :

(i) $u \in R$ is constructible from Q.

(ii) $(a, 0)$ is a constructible point from $Q \times Q$.

(iii) (a, a) is a constructible point from $Q \times Q$.

(iv) $(0, a)$ is a constructible point from $Q \times Q$.

Proof : (i) $\Rightarrow$ (ii) Definition.

(ii) $\Rightarrow$ (iii) The circle $(x-a)^2 + y^2 = a^2$ is constructible because its center $(a, 0)$ is a constructible point, and it passes through a constructible point (0, 0). Also, the line $x = y$ is constructible because it passes through constructible points (0, 0) and (1, 1). The point (a, a) is clearly a point of intersection of the citcle and the line. Hence, (a, a) is constructible.

(iii) $\Rightarrow$ (iv) The circle $x^2 + y^2 = 2a^2$ is constructible because its center (0, 0) is constructible, and it passes through a constructible point (a, a). Also, the line $y = -x$ is constructible because it passes through two distinct constructible points (0, 0) and (1, –1). One of the points of intersection of this circle and this line is $(-a, a)$. This implies that $(0, a)$ is a constructible point because it is the intersection of the constructible lines $y = a$ [which passes through two distinct constructible points $(-a, a)$ and (a, a)] and $x = 0$.

(iv) $\Rightarrow$ (ii) Follows by symmetry.

Henceforth, whenever we say that a real number a is constructible, we mean that a is constructible from Q.

Lemma 5.2 : If a is a constructible number, then $x = a$ and $y = a$ are constructible lines.

Proof : If $a = 0$, then $x = 0$ is clearly constructible. So let $a \neq 0$. Then $x = a$ passes through two distinct constructible points $(a, 0)$ and (a, a). Hence, $x = a$ is constructible. Similarly, $y = a$ is constructible.

Lemma 5.3 : If a and b are constructible numbers, then (a, b) is a constructible point.

Proof : (a, b) is the intersection of the constructible lines $x = a$ and $y = b$.

Lemma 5.4 : If a and b are constructible numbers, then $a \pm b$ are also constructible.

Proof : $(a \pm b, 0)$ are the points of intersection of the constructible line $y = 0$ and the constructible circle $(x - a)^2 + y^2 = b^2$ (the center $(a, 0)$ is constructible; the point (a, b) through which the circle passes is constructible).

Lemma 5.5 : If a and b are constructible numbers, then

(i) ab is constructible

(ii) a / b, $b \neq 0$, is constructible.

Proof : (i) The line $ay = -x + ab$ is constructible because it passes through constructible points $(0, b)$ and $(a, b - 1)$. The intersection of this line with the constructible line $y = 0$ is $(ab, 0)$. Hence ab is constructible.

(Note that we have used the fact that if b is constructible, then $b - 1$ is also constructible).

(ii) If $a = 0$, then it is clear. So let $a \neq 0$. Then the line $bx = a - y$ is constructible because it passes through two distinct constructible points : $(0, a)$ and $(a, a(1 - b))$. The intersection of this line with the constructible line $y = 0$ is $(a / b, 0)$. Hence, a / b is ocnstructible.

Lemma 5.6 : If $a > 0$ is constructible, then $\sqrt{a}$ is constructible.

Proof : The point $\left(1, \sqrt{a}\right)$ is a point of intersection of the constructible circle

$$\left(x - \frac{1+a}{2}\right)^2 + y^2 = \left(\frac{1+a}{2}\right)^2$$

[which passes through the constructible point (0, 0) and which has constructible center $((1+a)/2, 0)$] and the constructible line $x = 1$. Thus, $(1, \sqrt{a})$ is a constructible point.

Next, $(0, 2\sqrt{a})$ is also a constructible point because it is a point of intersection of the constructible circle $(x-1)^2 + (y-\sqrt{a})^2 = a+1$ and the constructible line $x = 0$. Therefore, $2\sqrt{a}$ is a constructible number. Then by Lemma 5.5, $\sqrt{a}$ is a constructible number.

Proof of the theorem 5.2 follows from Lemmas 5.4 – 5.6.

Theorem 5.3 : If $u \in K_m$, where $K_0 = Q \subset K_1 \subset K_2 \subset .... \subset K_m$ is an ascending tower of fields K_i such that $[K_i : K_{i-1}] = 2$, then u is constructible.

Equivalently, if $[Q(u) : Q] = 2^t$ for some $t > 0$, then u is constructible.

Proof : Since rationals are constructible, the proof follows from Lemmas 5.4 – 5.6.

Definition 5.3 : An angle α is constructible by ruler and compass if the point $(\cos \alpha, \sin \alpha)$ is constructible from $Q \times Q$.

Remark : The point $(\cos\alpha, \sin\alpha)$ is constructible from $Q \times Q$ if and only if $\cos \alpha$ is a constructible number (equivalently, if and only if $\sin \alpha$ is a constructible number).

Proof : Let $(\cos\alpha, \sin\alpha)$ be a constructible point. Then $(2\cos \alpha, 0)$ is a point of intersection of the constructible circle $(x - \cos\alpha)^2 + (y - \sin\alpha)^2 = 1$ and the constructible line $y = 0$, so $(2\cos\alpha, 0)$ is a constructible point. Thus, $2\cos \alpha$ is a constructible number. So by Throem 5.2, $\cos\alpha$ is a constructible number. Conversely, assume that $\cos \alpha$ is a constructible number. Then by Theorem 5.2, $\sin \alpha$ is also a constructible number. This yields, by Lemma 5.1 that the points $(\cos\alpha, 0)$, $(\cos \alpha, \cos \alpha)$, $(0, \sin\alpha)$, and $(\sin \alpha, \sin\alpha)$ are constructible points. This means that the lines $x = \cos \alpha$ and $y = \sin \alpha$ are constructible lines. Hence, their intersection, namely, the point $(\cos \alpha, \sin \alpha)$ is a constructible point. The statement in parenthese can be proved the same way.

EXAMPLE :

(a) Problem of Squaring a Circle

It is impossible to construct a square equal in area to the area of a circle of radius 1.

Solution : Assume we have a circle of unit radius. If a is the side of the square whose area is equal to that of this circle, then $\alpha^2 = \pi$. But since π is not algebraic over Q, a^2 and, hence, a is not algebraic over Q. So $[Q(a) : Q] \neq 2^m$ for any positive integer m. Hence, by Theorem 5.1, a is not constructible by ruler and compass.

(b) Problem of Duplicating a Cube.

It is impossible to construct a cube with a volume equal to wtice the volume of a given cube by using ruler and compass only.

Solution : We can assume that the side of the given cube is 1. Let the side of the cube to be constructed be x. Then $x^3 - 2 = 0$. So we have to construct the number $2^{1/3}$ (the real cube root of 2). Because $x^3 - 2$ is irreducible over Q.

$$\left[Q\left(2^{1/3}\right) : Q\right] = 3 \neq a \text{ a power of 12.}$$

Thus, by Theorem 5.1. $2^{1/3}$ is not constructible from Q by ruler and compass.

(c) Problem of Trisecting and Angle

There exists an angle that cannot be trisected by using ruler and compass only.

Solution : We show that the angle 60° cannot be trisected by ruler and compass. Now if this angle can be trisected by ruler and compass, then the number cos 20° is constructible from Q. This is equivalent to the constructibility of 2 cos 20° from Q. Set $a = 2 \cos 20°$. Then from $\cos 3\theta = 4 \cos^3\theta - 3 \cos \theta$, we deduce $a^3 - 3a - 1 = 0$. Because the polynomial $x^3 - 3x - 1 \in Q[x]$ is irreducible over Q and has a root a, it follows that

$$[Q(a) : Q] = 3 \neq \text{ power of 2.}$$

Thus, by Theorem 5.1, $a = 2 \cos 20°$ (or, equivalently, an angle of 20°) cannot be constructed by ruler and compass from Q. This completes the solution.

(d) Problem of Constructing a Regular n-gon

A regular *n*-gon is constructible (equivalently, the angle $\frac{2\pi}{n}$ is constructible) if and only if $\varphi(n)$ is a power of 2.

Solution : Let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, where ω is a primitive n^{th} root of unity. Then $\omega + \bar{\omega} = 2\cos\frac{2\pi}{n}$. Set $u = \cos\frac{2\pi}{n}$. To show that *u* is constructible, we need to prove that $[Q(u):Q] = 2^k$, $k \geq 0$. Consider the following tower :

$$Q(\omega)$$
$$|$$
$$Q(u)$$
$$|$$
$$Q$$

Now $\left(\omega - \cos\frac{2\pi}{n}\right)^2 = -\sin^2\frac{2\pi}{n}$, and so $\omega^2 - 2\cos\frac{2\pi}{n}\omega + 1 = 0$. Thus ω satisfies.

$$x^2 - \left(2\cos\frac{2\pi}{n}\right)x + 1 \in Q(u)$$

Which is clearly an irreducible polynomial over Q (u), proving that $[Q(\omega):Q(u)] = 2$. Now $[Q(\omega):Q] = \varphi(n)$, $[Q(u):Q] = \frac{1}{2}\varphi(n)$. This shows that *u* is constructible if and only if $\varphi(n)$ is a power of 2.

Problems :

1. Show that the angle $\frac{2\pi}{5}$ can be trisected using ruler and compass.

2. Show that it is impossible to construct a regular 9-gon or 7-gon using ruler and compass.

3. Show that it is possible to trisect 54° using ruler and compass.

4. Prove that the regular 17-gon is constructible with ruler and compass.

5. Find which of the following numbers are constructible.

(i) $\sqrt{3}+1$

(ii) π^2+1

(iii) $\sqrt{\sqrt{3}-1}+1$

(iv) $\sqrt[3]{2}+1$

(v) $\sqrt[4]{\sqrt{2}+\sqrt{5}}$