UNIT 14 : NORMAL EXTENSIONS AND PERFECT FIELDS

UNIT STRUCTURE

14.1 Learning Objectives
14.2 Introduction
14.3 Normal Extensions : Definitions and Examples
14.4 Properties of Normal Extensions
14.5 Perfect fields : Definitions and Examples
14.6 Properties of Perfect Fields
14.7 Finite fields : Definitions and Examples
14.8 Properties of finite fields.
14.9 Primitive Elements : Definitions and Examples.
14.10 Properties of Primitive Elements
14.11 Algebraically Closed Fields : Definitions and Examples
14.12 Properties of Algebraically Closed Fields.
14.13 Automorphism of Extensions : Definitions and Examples.
14.14 Properties of Automorphism of Extensions.
14.15 Let Us Sum Up
14.16 Answer to Check Your Progress
14.17 Further Reading
14.18 Model Questions

14.1 LEARNING OBJECTIVES

After going through this unit, you will able to-

- define normal extensions
- know perfect fields, finite fields
- define primitive elements
- define algebraically closed fields
- know automorphism of Extensions.

14.2 INTRODUCTION

In the study of field extension, Normal extension plays crucial rule. An algebraic extension E/F is normal if for every irreducible polynomial f (x) $\in$ (F[x], either f(x) splits in E[x] or f(x) has no root in E.

It has long been know that perfect fields are significant because Galois theory over these fields becomes simpler, since the separate condition (the most important condition of Galois extensions) of algebraic extensions over perfect fields are automatically satisfied. A field F is said to be perfect if any one of the following equivalent conditions holds :

i) Every irreducible polynomial over F is separable.

ii) Every finite-degree extension of F is separable

iii) Every algebraic extension of F is separable.

One showed that any field of characteristic 0 is a perfect field

In this unit, we take up one of the most beautiful and important areas of abstract algebra-finite fields. Finite fields were first introduced by Galois in 1830 in his proof of the unsolvability of general quintic equation. For each prime p and each positive integer n, there is, upto isomorphism, a unique finite field of order p^n.

There is an important theorem in field extension which is called Primitive element theorem. The primitive element theorem is state as if E is an extension of Q with [E : Q]< ∞, then E has a primitive element.

A field F is said to be algebraically closed if every non-constant polynomial in F[x] splits completely i.e. has all its zeros in F.

The set of all automorphisms of a field form a group under resultant composition. In this unit we include automorphism of field extensions. Let F be a field and E be any field extension of F. Then an automorphism σ of E is said to be an F-auto-amorphism if σ (x) = x for al x $\in$ F.

14.3 NORMAL EXTENSIONS : DEFINITION AND EXAMPLES

Definition: (Normal Extension) An algebraic extension E/F is normal if for every irreducible polynomial f(x) $\in$ F [x] either f(x) splits in E[x] or f(x)

has no zero in E.

Definition: Two elements α_1, α_2 of $\bar{F}$ are conjugate if the minimal polynomials of α_1, α_2 are same over F.

A useful reformulation of this definition is that E/F is normal if for every $\alpha \in E$, the minimal of x over F splits completely in E[x].

Example1. For any field F, F|F is a normal extension because for any $\alpha \in F$, the minimal polynomial for α is linear, so it splits completely in F(x).

Example 2. For any field F, the algebraic closure of $\bar{F}$ is a normal extension of F because by definition, every polynomial splits completely over $\bar{F}$.

Example 3. For any field F and f(x) $\in$ F[x], the splitting field extension E|F is normal.

Example 4. The extension $Q\left(\sqrt[3]{2}\right)$ of Q is not normal because $\sqrt[3]{2} \in Q\left(\sqrt[3]{2}\right)$, but its minimal polymial $x^3 - 2$ does not split completely in $Q\left(\sqrt[3]{2}\right)$. Since all splitting fields are normal $Q\left(\sqrt[3]{2}\right)$ cannot be the splitting field for any polynomial in Q[x].

Example 5. $Q\left(\sqrt[4]{2}\right) | Q$ is not normal since the minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$ and this does not split completely in $Q\left(\sqrt[4]{2}\right)$.

14.4 PROPERTIES OF NORMAL EXTENSIONS

Theorem 14.4.1. The following are equivalent for any finite extension E|F

i) E|F is the splitting field of a polynomial over F.

ii) For any homomorphism $\psi_1 : E \to \bar{F}$, $\psi_2 : E \to \bar{F}$ over F, $\psi_1(E) = \psi_2(E)$.

iii) E|F is normal.

Proof : We first show that i) $\Rightarrow$ ii)

Suppose E|F is the splitting field of some polynomial f(x) $\in$ F[x]. Then, let $\alpha_1, \alpha_2 ..... \alpha_n$ be the zeros of f(x) in $\bar{F}$. We know by definition of splitting field, E must also have n district zeros of f(x). We can see that for any $\psi : E \to \bar{F}$ since ψ is a homomorphism over F, each of the zeros of

f(x) in E must map to same α_1 in $\bar{F}$. Moreover, since field homomorphism are injective, and there are n distinct zeros in E, all of $\alpha_1, \alpha_2 \ldots, \alpha_n$ must be in the image of ψ and we get ψ (E) is exactly $F(\alpha_1, \alpha_2 \ldots \alpha_n) \subseteq \bar{F}$, for all such ψ.

ii) $\Rightarrow$ iii)

Suppose E|F has a well-defined image E/ in $\bar{F}$. Then, for any $\phi \in$ Aut ($\bar{F}$/F), we see that $\phi(E')$ must equal to E/ (otherwise $\phi \circ \psi$ would give us a distinct image of E, candradicting (ii)). Then, for any $\alpha \in E', E'$ must contain all conjugates of α, so $E' \mid F \cong E \mid F$ is normal.

iii) $\Rightarrow$ i)

Since E|F is finite, it has some basis $\alpha_1, \alpha_2, \ldots \alpha_n$ over F. For each $1 \le i \le n$ let $f_i(x)$ be the minimal polynomial for α_i over F. Then

$$f(x) = \prod_{i=1}^{n} f_i(x)$$

splits completely in E[x] and since E = $F(x_1, x_2 \ldots x_n)$, E is the splitting field of f(x)

Thus, the three properties are equivalent, for finite field extensions.

Remark : If $F \subseteq E \subseteq K$ is a chain of field extensions, then [K : F] is finite if and only if [E : F] and [K : E] are finite.

Similarly, If $F \subseteq E \subseteq K$ is a chain of field extensions, then K|F is algebraic if and only if E|F and K|E are algebraic.

But neither direction of this true for normal extensions. We have the following counter examples :

$$Q \xrightarrow{\text{normal}} Q(\sqrt{2}) \xrightarrow{\text{normal}} Q(4\sqrt{2})$$

not normal

$$Q \xrightarrow{\text{not normal}} Q(3\sqrt{2}) \xrightarrow{\text{normal}} Q(3\sqrt{2}, w)$$

normal

Theorem 14.4.2. If $F \subseteq E \subseteq K$ is a chain of field extension and K|F is normal, then K|E is normal.

Proof : For $\alpha \in K$, define $f_F(x)$ to be the minimal polynomial of α over F and $f_E(x)$ to be the minimal polynomial of α over E. But this means there is some $g(x) \in E[x]$ such that

$f_F(x) = f_E(x)\, g(x) \in E[x]$

So if $f_F(x)$ splits completely in K[x], $f_E(x)$ must also split completely in K[x], so since K is normal over F, it must also be normal over E.

Lemma 14.4.3. If [E : F] = 2, then E is normal extension of F always.

Proof : Let $g(x) \in F[x]$ be any irreducible ploynomial over F. Let α be a zero of f(x) and $\alpha \in E$. Now, we have

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

$\Rightarrow [F(\alpha) : F] \leq 2$

$\Rightarrow \deg f(x) \leq 2$

If deg f(x) = 1, then let f(x) = ax+b, a, b $\in$ F, G $\neq 0$

Then $0 = f(\alpha) = a\alpha + b$

$\Rightarrow \alpha = -\frac{b}{a},\ a \neq 0$

But $-\frac{b}{a} \in F \subseteq E \neq \alpha \in E$

If deg f(x) = 2, then let $f(x) = ax^2+bx+c$ where $a \neq 0$.

If α is a zero of f(x), then

$f(x) = (x-\alpha)\left(x+\alpha+\frac{b}{a}\right),\ a(\neq 0) \in E$

$\Rightarrow -\left(\alpha+\frac{b}{a}\right)$ is other zero of f(x).

Since $\frac{b}{a} \in F \subseteq E$ and $\alpha \in E \Rightarrow -\left(\alpha+\frac{b}{a}\right) \in E$

Hence E is a normal extension of F.



CHECK YOUR PROGRESS :

Q.1. Show that

i) Q(w) is a normal extension of Q, where $w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

ii) Q(w, $\sqrt[3]{2}$) is a normal extension of Q.

iii) Q(w$\sqrt[3]{2}$) is not a normal extension of Q.

iv) Q(w$\sqrt[3]{2}$) is not a normal extension of Q.

v) Q($w^2\sqrt[3]{2}$) is not a normal extension of Q.

14.5 PERFECT FIELDS : DEFINITIONS AND EXAMPLES

Definition : (Simple extension). An extension field E of a field F is simple extension of F if E = f(α) for some $\alpha \in$ E.

Definition : (Algebraic closure) Let E be an extension field of F. Then

$\overline{F}_E = \{\alpha \in E \mid \alpha$ is algebraic over F} is a subfield of E, the algebraic closure of F in E.

Definition : (Algebraically closed) A field F is algebraically closed if every non constant ploynomial in F[x] has a zero in F.

Note that a field F can be the algebraic closure of F in an extension field E without F being algebraically closed. For example, Q is the algebraic closure of Q in Q[x], but Q is not algebraically closed because x^2+1 has no zero in Q.

We shall show that just as these exists an algebraically closed extension C of the set of real numbers R, for any field F there exists similarly an algebraic extension $\overline{F}$ is algebraically closed. To find $\overline{F}$ we proceed as follows. If a polynomial f(x) in F[x] has no zero in F, then adjoin a zero α of such an f(x) to F, thus obtaining the field f(α). If F(α) is still not algebraically closed, then continue the process further. The trouble is that, contrary to the situation for the algebraic closure C of R, we may have to do this a (possibly large) infinite number of times.

Definition : If σ is an isomorphism of a field E onto some field, then an element a of E is left fixed by σ if σ (a) = a. A collection s of isomorphisms of E leaves a subfield F of E fixed if each a $\in$ F is left fixed by every $\sigma \in$ S. If $\{\sigma\}$ leaves F fixed, then σ leaves F fixed.

Definition: Let E be a finite extension of a field F. The number of isomorphisms of E onto a subfield of $\overline{F}$ leaving F fixed is the index {E : F} of E over F.

Unless F is an infinite field of characteristic p $\neq$ o, we always have [E:F] = {E : F} for every finite extension field E of F. For the case E = F(α), the {F(a) : F} extensions of the identity map i : F $\rightarrow$ F to maps of F(α) onto

a subfield of $\bar{F}$ are given by the conjugation isomorphism $\Psi_{\alpha,\beta}$ for each conjugate β in $\bar{F}$ of α over F. Thus if irr(α,F) has distinct zeros in $\bar{F}$, we have {E : F} = n. We shall show later that unless F is infinite and of characteristic p $\neq$ o, the number of distinct zeros of irr(α,F) is deg(α,F) = [F(α): F]

Definition 14.5.6 (Separable Extensions) A finite extension E of F is, a separable extension of F if

{E : F} = [E : F]

An element α in $\bar{F}$ is separable over F if F(α) is a separable extension of F. An irreducible polynomial f(x)$\in$F[x] is separable over F if every zero of f(x) in $\bar{F}$ is separable over F.

Example 1. The field $E = Q\left[\sqrt{2}, \sqrt{3}\right]$ is separable over Q since {E : Q} = 4 = [E : Q].

Lemma 14.5.7. Let $\bar{F}$ be an algebraic closure of F and let $f(x)=x^n + a_{n-1}x^{n-1}+.....+a_1x+a_0$ be any monic polynomial in $\bar{F}$[x]. If $[f(x)]^m \in F[x]$ and m.1 $\neq$ 0 in F, then f(x)$\in$F[x]m that is, all $a_i \in F$.

Proof : We must show that $a_i \in F$, and we proceed, by induction on r, to show that $a_{n-r} \in F$. For r =1,

$$(f(x)^m = x^{mn} + (m.1)a_{n-1}{}^{x^{mn-1}} + ... + a_0^m$$

Since $(f(x)^m \in F[x]$, we have, in particular, $(m.1)a_{n-1} \in F$

Thus $a_{n-1} \in F$, since m.1 $\neq$ 0 in F.

As induction hypothesis, suppose that $a_{n-r} \in F$ for r = 1, 2, ..., k. Then the coefficient of $x^{mn-(k+1)}$ in $[f(x)^m$ is of the form

$$(m.1)a_{n-(k+1)} + g_{k+1}(a_{n-1}, a_{n-2}, a_{n-k})$$

where g_{k+1} (a_{n-1}, a_{n-2}, ... a_{n-k}) is a formal polynomial expression in a_{n-1}, a_{n-2}, ... $a_{n-k.}$ By the induction hypothesis that we just stated,

$g_{k+1}(a_{n-1}, a_{n-2,}.....a_{n-k}) \in F$, so $a_{n-(k+a)} \in F$ since m.1 $\neq$ 0 in F.

Definition: A field is perfect if every finite expension is a separable extension. In other words, a field F is perfect if ch(F) = 0 or ch(F)=p and the map $\phi : F \to F$ defined by $\phi(a) = a^p$ is subjective.

Example 1. Every finite field is perfect.

Example 2. Every algebraic extension of a finite field is perfect.

Example 3. Every field of characteristic zero is perfect.

14.6 PROPERTIES OF PERFECT FIELD

Therorem 14.6.1. In a perfect field F all irreducible polynomial in F[x] are separable.

Proof : Let F be a perfect field. Then we have two possibilities,

(i) ch (F) = 0

or (ii) ch(F) = p

Case (i). Let ch(F) = 0. If $f(x) \in F[x]$ is an irreducible polynomial of degree p, then $f'(x)$ is a non zero polynimal of degree p–1, and f(x) and $f'(x)$ are relatively prime in F[x]. So f(x) is separable.

Case (ii). Let ch(F) = p > 0. Let $f(x) \in F[x]$ be an irreducible polynomial. We have to prove f(x) is separable F[x]. If possible, let f(x) is inseparable. Then f(x) is of the form

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + ... + a_{np} x^{np}$$

for some n. Since F is perfect, a_{ip} can expressed as b_i^p for some $b_i \in F$. Then

$$f(x) = b^p{}_0 + b_0^p x^p + ... + b_n^p x^{np}$$
$$= \left(b_0 + b_1 x + ... + b_n x^n \right)^p$$

So f(x) is not irreducible, which is a contradiction. This contradiction implies that f(x) is separable.

Theorem 14.6.2. For a field F, the following are equivalent :

(i) F is perfect

(ii) Every irreducible polynimal in F(x) is separable.

(iii) Every algebraic extension of F is separable.

Proof : We already show (i) $\Rightarrow$ (ii) in the above theorem. We will show that (ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (i), to show that the three statements are equivalent.

(ii) $\Rightarrow$ (iii) : We can see that for any algebraic extension E|F and any $\alpha \in F$, the minimal polynomial for α over F is irreducible in F[x]. Thus by (ii), it is separable, so our algebraic extension is separable.

(iii) $\Rightarrow$ (i) : Assume every algebraic extension of F is separable. If ch(F) = 0, then F is perfect by definition. Let ch(F) = p. We need to show the map $\phi : F \to F$ defined as $\phi(a) = a^p$ is surjective, i.e. for every $\alpha \in F$, we need to show that there exixts $b \in F$ such that $b^p = a$. Consider the polynomial

x^p–a. We know that this has some root $b \in \bar{F}$, we want to show that $b \in F$. Consider the minimal polynomial f(x) of b over F. We know that there exists some g(x) such that

$$(x^p - a) = (x-b)^p = f(x)\, g(x) \in \bar{F}\ [x]$$

But this means $f(x) = (x-b)^k \in \bar{F}[x]$, for some $k \leq p$.

We know by (iii), F(b) is separable and therefore f(x) is separable, which means k = 1 and the minimal polynomial for b over F is x–b, so $b \in F$. Thus ϕ is surjective and hence F is perfect.



CHECK YOUR PROGRESS

Q.2. Show that every field of characteristic zero is perfect.

Q.3. Show that every finite field is perfect.

14.7 FINITE FIELD : DEFINITIONS AND EXAMPLES

The purpose of this section is to determine the structure of all finite fields. For every prime p and positive integer n, there is exactly one finite field (upto isomorphism) of order p^n. This field GF(p^n) is usually referred to as the Galois field of order p^n.

The structure of a finite field is discussed in unit 11, section 11.8.

14.8 PROPERTIES OF FINITE FIELD

The properties of finite field is discussed in details in unit–11, section 11.9.

14.9 PRIMITIVE ELEMENT : DEFINITIONS AND EXAMPLES

Definition: An extension field E of a field F is a simple extension of F if $E = F(\alpha)$ for some $\alpha \in F$. Such an element α is called primitive element.

Example, $Q\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in Q\right\}$ is an extension field of the field Q of rational numbers. Therefore $\sqrt{2}$ is a primitive element of $Q\left(\sqrt{2}\right)$.

14.10 PROPERTIES OF PRIMITIVE ELEMENT

Theorem 14.10.1. (Primitive Element Theorem). Let E be a finite separable extension of a field F. Then there exists $\alpha \in F$ such that E = F (α), i.e. a finite separable extension of a field is a simple extension.

Proof : If F is a finite field, then E is also finite. Let α be a generator for the cyclic group E_0 of non zero elements of E under multiplication. Then E = F(α), so α in a primitive element in this case.

We now assume that F is infinite and prove our theorem in the case that $E = F(\beta, \gamma)$. The induction argument from this to the general case is straight forward. Let irr (β,F) have distinct zerons $\beta = \beta_1, \beta_2 ...., \beta_n$ and let irr (γ,F), have distinct zeros $\gamma = \gamma_1, \gamma_2, ... \gamma_m$ in $\bar{F}$, where all zeros are of multiplicity 1, since E is a separable extention of F. Since F is infinite, we can find $a \in F$ such that $a \neq (\beta_i - \beta) / (\gamma - \gamma_j)$ for all i and j with $j \neq 1$. That is, $a(\gamma - \gamma_j) \neq \beta_i - \beta$

Letting $\alpha = \beta + a\gamma$, we have

$\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j$ so

$\alpha - a\gamma_j \neq \beta_i$

for all i and all $j \neq 1$. Let f(x) = irr(β , F) and consider h(x) = f(α –ax) $\in$ F(α) [x]

Now $h(\gamma) = f(\alpha - a\gamma)$

$= f(\beta + a\gamma - a\gamma)$

$= f(\beta)$

= 0

However, for $j \neq 1$ by construction, since β_i were only the zeros of f(x). Hence h(x) and g(x) = irr(ν,F) have a common factor in F(α) [x], namely irr(γ , F(α), which must be linear, since γ is the only common zero of g(x) and h(x). Thus $\gamma \in F(\alpha)$ add therefore $\beta = \alpha - a\gamma \in F(\alpha)$. Hence $F = (\beta, \gamma) = F(\alpha)$.

Corodarly 14.10.2. A finite extension of a field of characteristic zero is a simple extension.

Proof : Let E be a finite extension of a field F of characteristic zero. Since ch(F) = 0, therefore F is perfect, i.e. the finite extension E of F is separable. Thus E is a finite separable extension of the field F. By primitive element therem 14.10.1, E is simple.



CHECK YOUR PROGRESS

Q.4. Find a primitive element of $E = Q\left(i\sqrt{3}, \sqrt[3]{2}\right)$

14.11 ALGEBRAICALLY CLOSED FIELD : DEFINITIONS AND EXAMPLES

Definition: Let F be a field. F is algebraically closed if every non-constant polynomial $f(x) \in F[x]$ has a zero in F or every irreducible polynomial in F[x] has degree 1.

Example1. The set of complex number C is an algebraically closed field.

Example 2. $\overline{Q}$ = the set of all $\alpha \in C$ such that α is algebraic over Q. Take any polynomial f(x) which is irreducible in $\overline{Q}[x]$. If $\alpha \in C$, then $\overline{Q}(\alpha)$ is an algebraic extension of $\overline{Q}$, so $\overline{Q}^{(\alpha)}/_{Q}$ is algebraic and $\alpha \in \overline{Q}$ by definition. So $\overline{Q}$ is algebraically closed.

14.12 PROPERTIES OF ALGEBRAICALLY CLOSED FIELD

Theorem 14.12.1. A field F is algebraically closed if and only if every non constant polynomial in F[x] factors in F[x] into linear factors.

Proof : Let F be algebraically closed and f(x) be nonconstant polynomial in F[x]. Then f(x) has a zero $\alpha \in F$ and x–a is a factor of f(x), so f(x) = (x–a) g(x). If g(x) is nonconstant, it has a zero $b \in F$ and we have f(x) = (x–a) (x–b) h(x). Continue, we get a factorization of f(x) in F(x) into linear factor.

Corollary 14.12.2. An algebraically closed field F has no proper algebraic extension.

Proof : Let E be an algebraic extension of F, so $F \leq E$. Then if $\alpha \in E$, we have $\text{irr}(\alpha, F) = x - \alpha$

Since F is algebraically closed, so $\alpha \in F$ and we must have F = E.

Theorem 14.12.3 (Fundamental theorem of algebra) The field C of complex, numbers is an algebraically closed field.

Proof : Let the polynomial f(z)$\in$ C[z] have no zero in C. Then $\frac{1}{f(z)}$ gives an entire function, i.e., $\frac{1}{f}$ is analytic everywhere. Also if f(z)$\notin$C[z], $\underset{|z|\to\infty}{Lt}|f(z)|=\infty$ then $\underset{|z|\to\infty}{Lt}|\frac{1}{f(z)}|=0$. Thus $\frac{1}{f}$ must be bounded in the plane. Hence by Liouville's theorem of complex function theory, $\frac{1}{f}$ is constant and thus f is constant. Therefore, a nonconstant polynomial in C[z] must have a zero in C, so C is algebraically closed.



CHECK YOUR PROGRESS

Q.5. Show that Q is not algebraically closed.

Q.6. Show that R is not algebraically closed.

14.13 AUTOMORPHISM OF EXTENSIONS

Definition: (Monomorphisms and their Linear Independence) : Let S be any set and E be any field. Let M (S,E) denote the set of all mappings of S into E. Given $\phi_1, \phi_2 \in$ M(S,E) and a $\in$E, we define

$(\phi_1+\phi_2)(s)=\phi_1(s)+\phi_2(s)$

$(a\phi_1)(s)=a\phi_1(s)$ for every s $\in$S.

Then $\phi_1+\phi_2 \in$ M(S,E) and a $\phi_1 \in$ M(S,E) . Under these operations, M(S,E) becomes a vector space over E. The zero vector in M(S,E) is the mapping given by $\bar{o}$(s)=0 for all s $\in$S

Theorem 14.13.2. Let E and K be any two fields. If $\sigma_1, \sigma_2, \ldots \sigma_n$ are any n distinct monomorphisms of E into K, then they are linearly indepedent over K.

Proof : We prove the result by induction on n. Now for any $a_1 \in$K, $a_1\sigma_1=\bar{o}$

$\Rightarrow a_1 = 0$ or $\sigma_1(x) = 0$ for all x $\in$E

$\Rightarrow a_1=0$ as $\sigma_1(x) \neq 0$ for all x$(\neq 0)\in$E

Thus the result holds for n = 1.

Let us suppose that the result holds for any set of monomorphisms of E into K having less than n members.

Suppose for some $a_i \in K$ i = 1, 2, ..., n not all zero, $a_1\sigma_1 + a_2\sigma_2 + ... + a_n\sigma_n = 0$. Let $a_n \neq 0$; dividing by a_n, we get

$$b_1\sigma_1 + b_2\sigma_2 + ... + b_{n-1}\sigma_{n-a} + \sigma_n = \bar{o} \qquad (1)$$

where $b_i = a_i a^{-1}_n$ for all i = 1, 2, 3, ..., n –1.

Since σ_1 and σ_n are distinct, there exists $x_1 \in E$ such that $\sigma_1(x_1) \neq \sigma_n(x_1)$. Clearly $x_1 \neq 0$. For any $x \in E$, we have from (1)

$$b_1\sigma_1(x_1x) + b_2\sigma_2(x_1x) + ... + \sigma_n(x_1x) = 0$$

$$\Rightarrow b_1\sigma_1(x_1)\sigma_1(x) + b\sigma_2(x)\,\sigma_2(x) + ... + \sigma_n(x_1)\,\sigma_n(x) = 0 \qquad (2)$$

$$\Rightarrow b_1\frac{\sigma_1(x_1)}{\sigma_n(x_1)}\sigma_1(x) + b_2\frac{\sigma_2(x_1)}{\sigma_n(x_1)}\sigma_2(x) + ... + \sigma_n(x) = 0 \qquad (3)$$

for all x.

$(2) \Rightarrow b_1\sigma_1(x) + b_2\sigma_2(x_1) + ... + \sigma_n(x) = 0$ for all x (4)

(3) – (4) $\Rightarrow$

$$b_1\left[\frac{\sigma_1(x_1)}{\sigma_n(x_1)} - 1\right]\sigma_1(x) + b_2\left[\frac{\sigma_2(x_1)}{\sigma_n(x_1)} - 1\right]\sigma_2(x) + ... + b_{n-1}\left[\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)} - 1\right]\sigma_{n-1}\backslash(x) = 0$$

for all $x \in E$

Since $b_1\left[\frac{\sigma_1(x_1)}{\sigma_n(x_1)} - 1\right] \neq 0$ therefore $\sigma_1, \sigma_2, ... \sigma_{n-1}$ are linearly dependent over K. This contradict the induction hypothesis.

Hence $\sigma_1, \sigma_2, ... \sigma_n$ are linearly independent over K.

Corollarly 14.13.3. A set of automorphisms of E is linearly independent over E.

Lema 14.13.4. The set of all automorphisms of a field form a group under resulting composition.

Proof : Let Aut(K) be the set of all atuomorphisms of K. Since I, the identity map on K, is an automorphism of K, so $I \in$ Aut(K), i.e. Aut(K) $\neq \phi$

(i) Closure property : Let $\sigma_1, \sigma_2 \in$ Aut(K). Then σ_1 and σ_2 are both 1–1 and onto mappings. So $\sigma_1\sigma_2$ is also 1–1 and onto mapping. Further for any $x, y \in K$

$$\sigma_1\sigma_2(x+y) = \sigma_1[\sigma_2(x+y)]$$
$$= \sigma_1[\sigma_2(x) + \sigma_2(y)]$$
$$= \sigma_1[\sigma_2(x)] + \sigma_1[\sigma_2(y)]$$
$$= \sigma_1\,\sigma_2(x) + \sigma_1\,\sigma_2(y)$$

and $\sigma_1 \sigma_2(xy) = \sigma_1[\sigma_2(xy)]$

$= \sigma_1[\sigma_2(x)] \ \ \sigma_1[\sigma_2(y)]$

$= [\sigma_1 \sigma_2(x)].[\sigma_1 \sigma_2(y)]$

This shows that $\sigma_1 \sigma_2$ is an automorphism of K. Hence $\sigma_1 \sigma_2 \in$ Aut(K).

(ii) Associativity : It follows from the fact that the resultant composition of mappings, in general, is associative.

(iii) Existence of Identity : The identity map I on K is the identity of Aut(K).

(iv) Existence of inverse : Consider any $\sigma \in$ Aut(K). Since σ is one-one and onto, so σ^{-1} exists. For any $x \in K$, $\sigma^{-1}(x) = y \Leftrightarrow \sigma(y) = x$.

Now consider $x_1, x_2 \in K$. Let $\sigma^{-1}(x_1) = y_1$, $\sigma^{-1}(x_2) = y_2$.

Then $\sigma(y_1) = x_1$, $\sigma(y_2) = x_2$ so that

$\sigma(y_2+y_2) = \sigma(y_1) + \sigma(y_2)$

$= x_1 + x_2$

$\Rightarrow \sigma^{-1}(x_1+x_2) = y_1 + y_2 = \sigma^{-1}(x_1) + \sigma^{-1}(x_2)$

and $\sigma(y_1y_2) = \sigma(y_1)\ \sigma(y_2) = x_1x_2$

$\Rightarrow \sigma^{-1}(x_1x_2) = y_1y_2$

$= \sigma^{-1}(x_1)\ \sigma^{-1}(y_2)$

Consequently σ^{-1} is an automorphism of K i.e. $\sigma^{-1} \in$ Aut(K)

Hence Aut(K) is a group.

Definition: Let F be a field and E be any field extension of F. Then an automorphism σ of E is said to be an F–automorphism if $\sigma(x) = x$ for all $x \in F$ (i.e. σ leaves every element of F fixed)

Clearly I, the identity automorphism of E is an F-automorphism. Let $\sigma_1 \sigma_2$ be any two F-automorphisms of E. Then $\sigma_1 \sigma_2^{-1}$ Aut (E) as Aut (E) is a group. At the same time for any $x \in F$, $\sigma_1(x) = x$, $\sigma_2(x) = x$

$\Rightarrow \sigma_1(x) = x$, $\sigma_2^{-1}(x) = x$

$\Rightarrow \sigma_1 \sigma_2^{-1}(x) = x$

Hence $\sigma_1 \sigma_2^{-1}$ is also an F-automorphism of E. Thus the set of all F-automorphism of E is a subgroup of the group of all automorphism of E.

Notation : The group of all F-automorphisms of E is denoted by G(E,F). G (E, F) is called the Galois group of E over F.

Example 1. Let F = $Q(\sqrt{2})$. Then the function $\phi : F \to F$ defined as $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism.

Example 2. Let E = $Q(\sqrt{2})$. The minimal polynomial of $\sqrt{2}$ over Q is x^2-2 and $\{1, \sqrt{2}\}$ form a basis of E over Q. Thus any $x \in F$ is of the form $x = a+b\sqrt{2}$; $a, b \in Q$. Let σ be any automorphism of E, $\sigma(a)=a \ \forall\ a \in Q$. Further $\sigma < \sqrt{2} >$ is a conjugate of $\sqrt{2}$ over Q. As $\pm\sqrt{2}$ are the only roots of x^2-2, we get $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$.

Case I. If $\sigma(\sqrt{2}) = \sqrt{2}$, then

$$\begin{aligned}\sigma(x) &= \sigma(a+b\sqrt{2}) \\ &= \sigma(a) + \sigma(b\sqrt{2}) \\ &= a + \sigma(b)\ \sigma(\sqrt{2}) \quad [\because a \in Q] \\ &= a + b\sqrt{2} \quad [\because b \in Q] \\ &= x\end{aligned}$$

In this case σ = I, the identity map on E.

Case II. If $\sigma(\sqrt{2}) = -\sqrt{2}$, then

$$\begin{aligned}\sigma(x) &= \sigma(a+b\sqrt{2}) \\ &= \sigma(a) + \sigma(b)\sigma(\sqrt{2}) \\ &= a + b(-\sqrt{2}) \\ &= a - b\sqrt{2}\end{aligned}$$

Hence Aut(E) consists of only two elements namely I and the automorphism n such that

$n(x) = a - b\sqrt{2}$ for all $x = a + b\sqrt{2} \in E$

Example 3. Let $E = Q(\sqrt[3]{2})$. The minimal polynomial of $(\sqrt[3]{2})$ over Q is $x^3 - 2$. It has only one real zero namely $\sqrt[3]{2}$. Let σ be any Q-automorphism of E. Then $\sigma(\sqrt[3]{2}) \in E$ is a zero of x^3-2. So $\sqrt[3]{2} = \sigma(\sqrt[3]{2})$. Let x be any element of E, x can be expressed as $\alpha + \sqrt[3]{2}\ \beta + (\sqrt[3]{2})^2\gamma$; $\alpha, \beta, \gamma \in Q$.

Now

$$\begin{aligned}\sigma(x) &= \sigma\left[\alpha(\sqrt[3]{2})\ \beta + (\sqrt[3]{2})^2\gamma\right] \\ &= \sigma(\alpha) + \sigma(\sqrt[3]{2})\ \sigma(\beta) + [\alpha(\sqrt[3]{2})]^2\sigma(\gamma) \\ &= \alpha + \sqrt[3]{2}\ \beta + (\sqrt[3]{2})]^2\gamma \quad [\because \alpha, \beta, \gamma \in Q] \\ &= x\end{aligned}$$

That means σ = I. Thus Aut(E) = {I}.

14.14 PROPERTIES OF AUTOMORPHISM OF EXTENSIONS

Lemma 14.14.1. Let E be any field extension of F and $\alpha \in F$ be algebraic over F. Then for every F-automorphism σ of E, $\sigma(a)$ is a conjugate of a over F.

Proof : Let $f(x) = x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + ...+ \alpha_0$ be the minimal polynomial of a over F. Then

$$a^n + \alpha_{n-1}a^{n-1} + \alpha_{n-2}a^{n-2} + ...\alpha_0 = 0$$

So $0 = \sigma(0) = \sigma(a^n + \alpha_{n-1}a^{n-1} + \alpha_{n-2}a^{n-2} + ... + \alpha_0)$

$$= \sigma(a^n) + \sigma\left(\alpha_{n-1}a^{n-1}\right) + \sigma\left(\alpha_{n-1}a^{n-1}\right) + ... + \sigma(\alpha_0)$$

$$= \left[\sigma(a)\right]^n + \sigma(\alpha_{n-1})\left[\sigma(a)\right]^{n-1} + \sigma(\alpha_{n-2})\left[\sigma(a)\right]^{n-2} + + ... \sigma(\alpha_0)$$

$$= \left[\sigma(a)\right]^n + \alpha_{n-1}\left[\sigma(a)\right]^{n-1} + \alpha_{n-2}\left[\sigma(a)\right]^{n-2} + ... + \alpha_0$$

Since $\sigma(\alpha_i) = \alpha_i \in F \quad \forall i = 0, 1, 2, ..., n-1$.

This show that $\sigma(a)$ is also a zero of f(x). Hence $\sigma(a)$ is a conjugate of a over F.

Remark. Let $E = F(a_1, a_2, a_3 ..... a_n)$ be a finite algebraic extension with $\{a_1, a_2, ... a_n\}$ as a basis of E. Then each $x \in F$ is expressible as

$$x = \alpha_1 a_1 + \alpha_2 a_2 + ...+ \alpha_n a_n$$

Suppose σ is any F-automorphism of E. Then

$$\sigma(x) = \sigma(a_1)\ \sigma(\alpha_1) + \sigma(\alpha_2) + (a_2) + ... + \sigma(\alpha_n)\sigma(a_n)$$

$$= \alpha_1\sigma(a_1) + \alpha_2\sigma(a_2) + ...+ \alpha_n\sigma(a_n)$$

So that $\sigma(x)$ is known if we know $\sigma(a_1)$, $\sigma(a_2)$..... $\sigma(a_n)$ i.e. σ is completely determined by the images of the basis element of E. Int fact, more generally, if E is finitely generated over E and $\{a_1, a_2, ... a_n\}$ is a set of generators of E over F then σ is determined by $\sigma(a_1)$, $\sigma(a_2)$ .... , $\sigma(a_n)$.

Lemma 14.14.2. Let G be a group of automorphisms of a field F. Then the set $F_0 = \{x \in F \mid \sigma(x) = x \forall \sigma \in G\}$ is a subfield of E.

Proof : Since $\sigma(0) = 0$ and $\sigma(1) = 1\ \forall \sigma \in G$, so $0, 1 \in F_0$

Let $x, y \in F_0$ Then for every $\sigma \in F$; $\sigma(x) = x$, $\sigma(y) = y$.

Consequently $\sigma(x-y) = \sigma(x) - \sigma(y)$

$$= x - y$$

and when $y \neq 0$, $\sigma(xy^{-1}) = \sigma(x)\ \sigma(y^{-1})$

$= \sigma(x)\,[\sigma(y)]^{-1}$

$= xy^{-1}$

Thus $x-y \in F_0$ and when $y \neq 0$, $xy^{-1} \in F_0$. Hence F_0 is a subfield of E.

Definition: Let G be a group of automorphisms of F. Then subfield F_0 of F consisting of all these elements $x \in F$ such that $\sigma(x) = x$ for every $\sigma \in G$, is called the fixed field under G. The fixed field under G is denoted by $\Gamma(G)$ or F_G.

Remarks :

1. Let P be the prime subfield of F. We know that P is contained in every subfield of G. In particular if F_0 is the fixed field under G, then $P \subseteq F_0$. So that $\sigma(x) = x$ $\forall \alpha \in P$ and $\forall \sigma \in G$. Thus every automorphism of F is a P-automorphism.

2. Every member of G can be regarded as an F_0-automorphism of F where $F_0 = \Gamma(G)$.

3. If E is a field extension of a field F and G is a group of F-automorphisms of E, then $F \subseteq F_0$

Theorem 14.14.4. Let G be a finite group of automorphism of a field F; F_0, the fixed field under G. Then the degree of F_0 over F is equal to the order of the group G.

Proof : Let 0(G) = n. We want to show that

i) if $[F_0:F] = m$, then $m \geq n$ and

ii) If $[F_0 : F] = m$, then $m \leq n$

i) Suppose m<n . Let $\sigma_1 = I$, σ_2, σ_3,.... σ_n be all the members of G. Let $\{x_1, x_2, ...x_m\}$ be a basis of F_0 over F. Consider the system of m linear homogeneous equations.

$\sigma_1(x_j)\, u_1 + \sigma_2(x_j)u_2 + ...+ \sigma_n(x_j)u_n = 0$ ...(1)

$\forall$ j = 1, 2, ..., m.

As the number of equations is less than the number of variables, the equation (1) have a non-trivial solution say, $(y_1, y_2, ...y_n)$. Then

$\sigma_1(x_j)\, y_1 + \sigma_2(x_j)y_2 + ... \sigma_n(x_j)y_n = 0$ ....(2)

$\forall$ j = 1, 2, ..., m.

Consider any $x \in F$. Then

$x = \alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m$ for some $\alpha_i \in F$ as $\{x_1, x_2, ...x_m\}$ is a

basis of F_0 over F. In (2), multiplying j[th] equation by α_j, adding the resulting equations and using the fact $\sigma_i(\alpha_j) = \alpha_j \ \forall$ i, j we get

$y_1\sigma_1(x) + y_2\sigma_2(x) + ... + y_n\sigma_n(x) = 0 \ \forall \ x \in F_0$.

So that $y_1\sigma_1 + y_2\sigma_2 + ... + y_n\sigma_n = \bar{0}$ with at least one of $y_j \neq 0$. This is not possible. Hence $m \not< n$, so $m \geq n$.

(ii) Suppose there exist n+1 linearly independent elements say x_1, x_2, ...x_{n+1} of F_0 over F. Consider the system of n linear homogeneous equations is n+1 unknowns.

$\sigma_j(x_1)\ u_1 + \ \sigma_j(x_i)u_2 + ... \sigma_n(x_{n+1})u_{n+1} = 0$ ...(3)

for j = 1, 2, ..., n.

As the number of variables is greater than the number of equations. This homogeneous equations have a non-trivial solution. Let (z_1, z_2, z_3, ..., z_{n+1}) be a non trivial solution of equations (3) with smallest number, say r of non zero components. We can renumber them and suppose that $z_j = 0 \forall$ j $\geq$ r+1.

Then (3) gives

$\sigma_j(x_1)\ z_1 + \ \sigma_j(x_2)z_2 + ... \sigma_j(x_r)z_p = 0$ ...(4)

$\forall$ j = 1, 2, ..., n.

Dividing the equations of z_r and setting $z'_r = z_i / z_r$, $\forall$ i, we get

$\sigma_j(x_1)\ z'_1 + \ \sigma_j(x_2)z'_2 + ...+ \sigma_j(x_{r-1})z'_{r-1} + \sigma_j(x_r) = 0$ ...(5)

$\forall$ j

Now for j = 1, σ_j=1 so $\sigma_1(x_i) = x_i \ \forall$ i. We get from (4).

$x_1z'_1, x_2\ z'_2 + ...+ x_{r-1}z'_{r-1} + x_r = 0$ .....(6)

If all $z'_1 + \ z'_2$....., z'_{r-1} were in F then (6) gives x_1, x_2, ... x_r are linearly dependent over F. This is not possible. Hence at least one of these, say, z'_1 is not in F. Notice further that r $\neq$ 1., otherwise we would have got z'_1=0. As $z'_1 \notin F$ there exists some $\sigma_1 \in F$ such that $\sigma_1(z'_1) \neq z'_1$. Applying σ_i to (5), we get

$$\sigma_i\,[\sigma_j(x_1) = z'_1] + \sigma_i\,[\sigma_j(x_2) = z'_2] + ...+ \sigma_i\,[\sigma_j(x_{r-1}) = z'_{r-1}] + \sigma_i\,\sigma_j(x_r) = 0, \ \forall j = 1, 2, ...,n$$

$$\Rightarrow \sigma_i\sigma_j(x_1) + \sigma_i(z'_1) + \sigma_i\sigma_j(x_i) + \sigma_i(z'_2) + ...+ \sigma_i\sigma_j(x_{r-1}) + \sigma_i(z'_{r-1}) + \sigma_i\sigma_j(x_r) = 0 \ \forall\ j = 1,2,...,n$$

However σ_i G = G so that $\sigma_k \in$ G in the form $\sigma_i\sigma_j$, we get

$\sigma_j(x_1)\ \ \sigma_i(z'_1) + \ \sigma_j(x_2)\,\sigma_j(z'_2) + ...+ \sigma_j(x_{r-1})\,\sigma_j(z'_{r-1}) + \sigma_j(x_r) = 0$ ...(7)

for all j = 1, 2, ...n.

Subtracting (7) from (5), we get

$\sigma_j(x_1)\ [z'_1 - \sigma_i(z'_1)] + \sigma_j(x_2)[z'_2 - \sigma_i(z'_2)] + \ldots\ldots + \sigma_j(x_{r-1})[z'_{r-1} - \sigma_i(z'_{r-1})] = 0$ ....(8) for all j = 1, 2, ...n.

Now we put $t_k = z'_k - \sigma_i(z'_k) \quad \forall$ k = 1, 2, ... r–1 and $t_k = 0, \quad \forall$ k = r, r+1, ... n+1. Then from (8)

$\sigma_j(x_1)t_1 + \sigma_j(x_2)t_2 + \ldots\ldots\ldots\ldots + \sigma_j(x_{r-1})t_{r-1} + \sigma_j(x_r)t_r + \ldots\ldots + \sigma_j(x_{n+1})t_{n+1} = 0$ ... (9) for all j = 1, 2, ..., n

Further $t_1 \neq 0$ as $z'_1 \neq \sigma_i(z'_1)$ so that $(t_1, t_2, \ldots\ldots t_{r-1}, 0, 0, \ldots 0)$ is a non-trivial solution of the system of equations(3). It has less than r non zero components. But by our choice $(z_1, z_2, \ldots\ldots, z_r)$, 0, 0 ...., 0) is a non trivial solution of (3), having smallest number of non zero components and these are r in number. Hence we get a contradiction. This prove that $m \leq n$ .Hence m = n.

i.e. $[F_0 : F] = 0(G)$

Remark : Let E be a finite extension of F and G be the group of all F-automorphisms of E. Then the fixed F_0 under the group G contains F, so

$[E : F_0] \leq [E : F]$

$\Rightarrow 0(G) \leq [E : F]$

Definition: (Galois Extension) : A finite extension E of a field F is said to be Galois extension of F if F is the fixed subfield of E under the group G(E, F) of all F-automorphisms of E.

Corollary. 14.14.6. Let $E = F(\alpha)$ be a simple finite separable extension of F. Then E is a splitting field of the minimal polynomial of α over F if any only if F is fixed field under the group of all F-automorphisms of E.

Proof : Let f(x) be the minimal polynomial of α over F and let deg f(x) = m. Then [E : F] = m. Let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots\ldots\ldots \alpha_r$ be the distinct conjugates of α in E. Then $E = F(\alpha_i) \ \nabla$ i = 1, 2, ..., r. For each i, there exists an F-automorphism σ_i of E such that $\sigma_i(\alpha_1) = \alpha_i$. Since α_1 generates E over F, each σ_i is uniquely determined. Further for any F-automorphism σ of E, as $\sigma(\alpha_1)$ is a conjugate of α_1, $\sigma(\alpha_1) = \alpha_i$ for some α_i. From this it follows that $\sigma = \sigma_i$. Hence the group G (E, F) consists of σ_1, σ_2, ..., σ_n . Let F_0 be the fixed field under G (E, F). Then y by the above theorem.

$[E : F_0] = 0$ [G (E, F)]

= r

So F = F_0 if any only if r = m. Hence F is a fixed field under G if and only if f(x) has all its m zeros in E i.e. iff E is the spilitting field of f(x) over F.



CHECK YOUR PROGRESS

Q. 7. Let p be a prime number, α_1, α_2, α_3, ... α_{p-1} are the zeros of $f(x) = x^{p-1} + x^{p-2} + ...$ x+1 such that $E = Q(\alpha_1, \alpha_2, ..., \alpha_{p-1})$. Show that E is a Galois extension of Q.

Q. 8. Let $E = Q\left(\sqrt{-3}, \sqrt[3]{2}\right)$. Show that E is a Galois extension of Q.

Q. 9. Consider the polynomial $x^4 - x^2 + 1$ over Q. Find the Galois group of the spilitting field of $x^4 - x^2 + 1$ over Q.



14.15 LET US SUM UP

- An algebraic extension E|F is normal if for every irreducible polynomial $f(x) \in F[x]$ either f(x) splits in E[x] or f(x) has no zero in E.
- Two elements α_1, α_2 of $\bar{F}$ are conjugate if minimal polynomial of α_1 and α_2 are same over F.
- If [E : F] = 2, then E is always normal extension of F.
- An extension field E of a field F is simple extension of F if $E = F(\alpha)$ for some $\alpha \in F$.
- A finite extension E of F is a separable extension of F if {E : F} = [E : F].
- A field is perfect if every finite extension is a separable extension. In other words a field F is perfect if Ch(F) = 0 or ch(F) = p and the map ϕ : F $\rightarrow$ F defined by $\phi(a) = a^p$ is surjective.
- In a perfect field F, all irreducible polynomial in F[x] are separable.
- A field F is perfect if and only if every algebraic extension of F is separable.
- For every prime p and positive integer n, there are exactly one finite field (upto isomorphism) of order p^n. This field GF(p^n) is usually referred

to as the Galois field of order p^n.

- An extension field E of a field F is a simple extension of E = F(α) for some $\alpha \in F$. Such an element α is called primitive element.
- Let E be a finite separable extension of a field F. Then there exists $\alpha \in F$ such E = F(α).
- Let F be a field. F is algebraically closed if every nonconstant polynomial f(x)$\in$ F[x] has a zero in F or every irreducible polynomial f(x) in F[x] has degree 1.
- A field F is algebraically closed if and only if every nonconstant polynomial in F[x] factors in F[x] into linear factors.
- The field C of complex numbers is an algebraically closed field.
- Let F be a field and E be any field extension of F. Then an automorphism σ of E is said to be an F-Automorphism of σ(x) = x for all $\alpha \in F$.
- Let G be a group of automorphism of a field F. The subfield F_0 of F consisting of all those elements $x \in F$ such that σ(x) = x for every $\sigma \in G$, is called the fixed field under G.
- Let G be a finite group of automorphism of a field F, F_0 the fixed field under G. Then $[F_0 : F] = 0(G)$.

14.16 ANSWER TO CHECK YOUR PROGRESS

Ans to Q. No.1

(i) Since Q(w), where $w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ is a spilitting field x^2+x+1 over Q, so Q(w 3/2) is a normal extension of Q.

ii) Since Q (w, $\sqrt[3]{2}$) is a spilitting field of x^3-2 over Q, so Q (w, $\sqrt[3]{2}$) is a normal extension of Q.

iii) Since Q ($\sqrt[3]{2}$) contains only one zero of x^3-2, so Q ($\sqrt[3]{2}$) is not normal extension of Q.

iv) Since Q (w$\sqrt[3]{2}$) contain only one zero of x^3-2, so Q (w$\sqrt[3]{2}$) is not a normal extension of Q.

v) Similarly Q ($w^2\sqrt[3]{2}$) is not a normal extension of Q.

Ans to Q. No. 2

Let E be a finite extension of a field F of characteristic zero and let $\alpha \in F$. Then f(x) = irr(α, F) factors in $\bar{F}$[x] into $\prod_i (x-\alpha_i)^\gamma$, where the are the distinct zeros of irr(α,F) and say, $\alpha = \alpha_i$. Thus $f(x) = \left[\prod_i (x-\alpha_i)\right]^\gamma$

and since $\gamma.1 \neq 0$ for a field F of characteristic 0, we must have $\prod_i (x-\alpha_i) \in F[x]$

Since f(x) is irreducible and of minimal degree in F[x] having α as a zero, we then see that γ=1. Therefore, α is separable over F for all $\alpha \in F$ and hence E is a separable extension of F.

Ans to Q. No. 3

Let F be a finite field of characteristic p, and let E be a finite extension of F. Let $\alpha \in F$. We need to show that α is separable over F. Now f(x) = irr (α, F) factors in $\bar{F}$ into $f(x) = \prod_i (x-\alpha_i)^\gamma$, where the α_i are the distinct zeros of f(x), and say $\alpha = \alpha_i$. Let $\gamma = p^t e$, wher p does not divide e. Then

$$fx = \prod_i (x-\alpha_i)^\gamma$$

$$= \left[\prod_i (x-\alpha_i)^{p^t}\right]^e$$

is in F[x] and $\prod_i (x-\alpha_i)^{p^t}$ is in F[x] since e.1 $\neq$ 0 in F. Since f(x) = irr(α,F) is of minimal degree over F having α as a zero, we must have e = 1. Thus

$$f(x) = \prod_i (x-\alpha_i)^{p^t}$$

$$= \prod_i (x^{p^t} - \alpha_i^{p^t})$$

Thus, if we regard f(x) as $g(x^{p^t})$, we must have g(x) $\in$ F[x]. Now g(x) is separable over F with distinct zero $\alpha_i^{p^t}$. Consider F($\alpha_1^{p^t}$) = F(α^{p^t}). Then F($\alpha_1^{p^t}$) is separable over F. Since $x^{p^t} - \alpha^{p^t} = (x-\alpha)^{p^t}$, we see that α is the only zero of $x^{p^t} - \alpha^{p^t}$ in $\bar{F}$. As a finite dimonsional vector space of a finite field F, F(α^{p^t}) must be again a finite field. Hence the map

$$\sigma_p : F(\alpha^{p^t}) \to F(\alpha^{p^t})$$

given by $\sigma_p(a) = a^p$ for $a \in F(\alpha^{p^t})$ is an auto-morphism of $F(\alpha^{p^t})$. Consequently $(\sigma_p)^t$ is also an automorphism of $F(\alpha^{p^t})$ and $(\sigma_p)^t(a) = a^{p^t}$

Since an automorphism of $F(\alpha^{p^t})$ is an onto map, there is $\beta \in F(\alpha^{p^t})$ such that $(\sigma_p)^t(\beta) = a^{p^t}$

Then $\beta^{p^t} = a^{p^t}$ and we saw that α was the one zero of $x^{p^t} - \alpha^{p^t}$, so we must have $\beta = \alpha$. Since $\beta \in F(\alpha^{p^t})$, we have $F(\alpha) = F(\alpha^{p^t})$. Since $F(\alpha^{p^t})$ is separable over F, we now see that $F(\alpha)$ is separable over F. Therefore α is separable over F and t = 0.

We have shown that for $\alpha \in F$, α is separable over F. Hence E is a separable extension of F.

Ans to Q. No. 4.

We have to find a primitive element of α of $E = Q\left(i\sqrt{3}, \sqrt[3]{2}\right)$. Let $\alpha = i\sqrt{3}\ \sqrt[3]{2} \in E$.

$\Rightarrow \alpha^6 = -108$

$\Rightarrow \alpha^6 + 108 = 0$

Thus α is a zero of $x^6 + 108$. The following are equivalent :

i) α is a primitive element of F;

ii) $[Q(\alpha) : Q] = 6$;

iii) The minimal polynomial m(x) of α has degree 6;

iv) $x^6 + 108$ is irreducible.

In fact, $[Q(\alpha) : Q] = 6$ holds because both 2 and 3 divide $[Q(\alpha) : Q]$

$[Q(\alpha) : Q] = [Q(\alpha) : Q\ i\sqrt{3}]\ [Q\ i\sqrt{3} : Q]$

$= [Q(\alpha) : Q\ i\sqrt{3}].2$

and $[Q(\alpha) : Q] = [Q(\alpha) : Q\left(\sqrt[3]{2}\right)]\ [Q\left(\sqrt[3]{2}\right) : Q]$

$= [Q(\alpha) : Q\left(\sqrt[3]{2}\right).3$

Ans to Q. No. 5

Q is not algebraically closed because

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

has a root $\sqrt{2} \notin Q$.

Ans to Q. No. 6.

R is not algebraically closed because

$f(x) = x^2 + 1 \in R[x]$

has a root $\sqrt{-1} \notin R$

Ans to Q.No. 7

Let p be any prime integer and $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$. Then

$f(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + ... + (x+1) + 1$

$= x^{p-1} + {}^{p}C_1 x^{p-2} + {}^{p}C_2 x^{p-3} + ... + {}^{p}C_{p-2} x + p$

Since p divides the coefficients of x^{p-2}, x^{p-3}, ..., x and constant term p; p^2 does not divide the constant term and p does not divide the coefficient of x^{p-1}. So by Eisenstein's Criterion, f(x+1) is irreducible over Q. Hence f(x) is irreducible.

$x^{p-1} = (x-1)(x^{p-1} + x^{p-2} + ... + x + 1)$

So for any complex zero of α of $x^p - 1$ if $\alpha \neq 1$, then α is a root of $x^{p-1} + x^{p-2} + ... + x + 1$.

Consider $\alpha_i = e^{\frac{2\pi i}{p}}$, i = 1, 2, ..., p–1. None of α_i is equal to 1 and all these α_i's are distince. Hence $\alpha_1, \alpha_2, ... \alpha_{p-1}$ are p–1 distinct zeros of f(x) over Q. So E = Q ($\alpha_1, \alpha_2, ... \alpha_{p-1}$) is the splitting field of the minimal polynomial f(x) over Q. Hence the fixed field of the group G of all Q-automorphism of E is Q. Hence Q is the fixed field under the group of all automorphisms of E. Thus E is a Galois extension of Q.

Ans to Q. No. 8

We know that $E = Q\left(\sqrt{-3}, \sqrt[3]{2}\right)$ is the splitting field of $x^3 - 2$ over Q. Let G be the group of all automorphism of E. Indeed G is the group of all Q-automorphisms of E. Since [E : Q] = 6, so $O(G) \leq 6$. Suppose $x^3 - 2$ is not irreducible over $F = Q\left(\sqrt{-3}\right)$. Then at least one root, say β of $x^3 - 2$ is in $Q\left(\sqrt{-3}\right)$. So $Q(\beta) \subseteq Q\left(\sqrt{-3}\right)$ Then $\left[Q(\beta) : Q\right] \Big| \left[Q\left(\sqrt{-3}\right) : Q\right]$.

However $[Q(\beta) : Q] = 3$ and $\left[Q\left(\sqrt{-3}\right) : Q\right] = 2$; we get 3 divides 2. That is not possible. Hence we get a contradiction. This contradiction implies that $x^3 - 2$ is irreducible over $F = Q\left(\sqrt{-3}\right)$.

Now $E = Q\left(\sqrt{-3}, \sqrt[3]{2}\right) = F\left(\sqrt[3]{2}\right)$ is a simple extension of F. As it contains all zeros of $x^3 - 2$, E is the splitting field of the minimal polynomial $x^3 - 2$ over F. Hence the group G_1 of all F-automorphism of K is such that F is the fixed field under G_1. So

3 = [E : F] = O(G)

However G_1 is a subgroup of G. Consequently $3|\circ(G)$. Again $x^2 + 3$ is a irreducible polynomial over $F_1 = Q\left(\sqrt[3]{2}\right)$ and E is the splitting field of $x^2 + 3$ over F_1 with $[E : F_1] = 2$. So we get 2|O(G). Hence 6|O(G). Thus O(G)=6. So it proves that [E : Q] = O(G). Consequently Q is the fixed field under G and E is a Galois extension of Q.

Ans to Q. No. 9

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

$$\therefore x = \frac{\pm\sqrt{3} \pm i}{2}$$

The splitting field of $x^4 - x^2 + 1$ over Q is

$$E = Q\left(\frac{\pm\sqrt{3} \pm i}{2}\right) = Q\left(\sqrt{3}, i\right)$$

Also [E : Q] = 4. We have to determine the Galois group of E over Q. Since $x^4 - x^2 + 1$ is irreducible over Q, there exist such that $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in G(E,Q)$ such that

$$\sigma_1\left(\frac{\sqrt{3}+i}{2}\right) = \frac{\sqrt{3}+i}{2}$$

$$\sigma_2\left(\frac{\sqrt{3}+i}{2}\right) = \frac{\sqrt{3}-i}{2}$$

$$\sigma_3\left(\frac{\sqrt{3}+i}{2}\right) = \frac{-\sqrt{3}-i}{2}$$

$$\sigma_4\left(\frac{\sqrt{3}+i}{2}\right) = \frac{-\sqrt{3}+i}{2}$$

Further for any $\sigma \in G(E, Q), \sigma\left(\frac{\sqrt{3}+i}{2}\right)$ is a zero of $x^4 - x^2 + 1$. So

G(E, Q) = $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$



14.17 FURTHER READINGS

1) Fraleigh, John B : A first course in abstract Algebra, Pearson Education (Singapure) Pvt. Ltd. India Branch, Delhi - 11092.
2) Singh, S and Qazi, Z : Modern Algebra, Vikas Publicasting House Pvt. Ltd, New Delhi - 110014.
3) Macauley, M. : Section 6 : Fields and Galois Theory, http :// www.math.clemson.edu/~macaule/.
4) Talati, A. : Class Notes of Professor June Huh, 2022.
5) Singh, J. : Theory of Field Extension, Maharshi Dayanand University Press, Rohtal-124001.



14.18 MODEL QUESTIONS

Q.1: Find the Galois group of E = $Q\left(\sqrt{2}, i\right)$ over Q.

Q.2: Let F be a Galois field having q elements and E be a field extension of E of degree n. Prove that E is a normal exterssion of F.

Q.3: Let E be a finite extension of a field F. Prove that there exists a minimal normal extension of F containing E.

Q.4: A field F is algebraically closed iff every polynomial has a zero in F.

Q.5: Show that if E is an algebraic extension of a field F and contains all zeros in $\overline{F}$ of every f(x) $\in$ F[x], then E is an algebraically closed field.

Q.6: Prove that if E is an algebraic extension of a perfect field F, then E is perfect.

*** ***** ***