UNIT 15 : GALOIS GROUPS AND GALOIS EXTENSIONS

UNIT STRUCTURE

15.1 Learning Objectives

15.2 Introduction

15.3 Galois Groups : Definitions and Examples

15.4 Properties of Galois Groups

15.5 Galois Extensions : Definitions and Examples

15.6 Properties of Galois Extensions

15.7 Let Us Sum Up

15.8 Answer to Check Your Progress

15.9 Further Reading

15.10 Model Questions

15.1 LEARNING OBJECTIVES

After going through this unit, you will able to-

- state and apply the fundamental theorem of Galois Theory;
- define and give examples of the Galois group of an irreducible polynomials;
- explain how Galois theory can be applied to determine those values of primes p for which a regular p-gon can be constructed by ruler and compass.

15.2 INTRODUCTION

We studied that polynomial equations upto degree 4 have algebraic formulae that give their roots in terms of radicals of the coefficients of the polynomial. However, the work of many mathematicians, notably Abel and Ruffini (early19th century), has shown that in general, there cannot exist such formulae for polynomials of degree $n \geq 5$. But it was the pioneering work of Evariste Galois, who gave a criterion for deciding whether the zeros of a given polynomial can be expressed in terms of radicals of the coefficients of the polynomial. This, in turn, would also prove the Abel-Ruffini theorem,

which had been left incomplete by Paoo Ruffini.

Galois died very young, but became immortal with his profound theory, known as Galois Theory today. His fundamental Theorem finally established a necessary and sufficient condition for a polynomial to be solvable by radicals.

15.3 GALOIS GROUPS : DEFINITIONS AND EXAMPLES

Definition: (Galois group) The Galois group G (E; F) of a field extension E|F is the group of all F-automorphisms of E under the operation of composition of maps.

Example. Consider the extension C|R. Suppose the α is IR-automorphism of C. Let α (i) = j, where $i = \sqrt{-1}$. We have

$j^2 = \alpha(i)^2 = \alpha(i^2) = \alpha(-1) = -1$

Since $-1 \in R$ and α fixes IR. Hence, either j = i or j = –i.

Now for any x, y $\in$ IR, we have

$\alpha(x + iy) = \alpha(x) + \alpha(i)\,\alpha(y)$

$= x + jy$

Thus we have two candidates for IR-automorphism :

$\alpha_1 : x+ iy \mapsto x + iy$

and $\alpha_2 : x + iy \mapsto x – iy$

α_1 is the identity and hence an IR-automorphism of C, while α_2 is complex conjugation, also an IR- automorphism of C. Aslo $\alpha_2^2 = \alpha_1$, so the Galois group G (C, IR) is a cyelic group of order 2.

Definition: (Intermediate field). Let E|F be a field extension. If M is a field such that $F \subset M \subset E$, then M is an intermediate field.

If G = G (E, F), then to each intermediate field we associate the group G_M = G (E, M). Thus G_F is the whole Galois group and G_E = {1}. This mapping reverses inclusions because if $M \subset N$, then $G_M \supset G_N$ because any automorphism of E that fixes the elements of N fixes the elements of M.

Conversely, to each subgroup H of G(E, F). We associate the set E^H of all elements $x \in E$ such that $\alpha(x) = x$ for all $\alpha \in H$. In fact, this set as an intermediate field.

15.4 PROPERTIES OF GALOIS GROUPS

Theorem 15.4.1. If E|F is a field extension, then the set of all F-automorphisms of E forms a group under composition of maps.

Proof : Suppose that α and β be two F-automorphisms of E. Then $\alpha\beta$ is clearly an automorphism; further, if $k \in F$ then

$$(\alpha\beta)(k) = \alpha(\beta(k))$$
$$= \alpha(k)$$
$$= k$$

So $\alpha\beta$ is a F-automorphism.

The identity map on E is obviously a F-automorphism. Finally, α^{-1} is an automorphism of E and for any $k \in F$, we have

$$k = \left(\alpha^{-1}\alpha\right)(k) = \alpha^{-1}(\alpha(k)) = \alpha^{-1}(k)$$

so α^{-1} is a F-automorphism. Since composition of maps is associative, so the set of all F-automorphisms of E is a group.

Theorem 15.4.2. If H is a subgroup of G(E, F), then E^H is a subfield of E containing F.

Proof : Let $x,y \in E^H$ and $\alpha \in H$. Then

$$\alpha(x+y) = \alpha(x) + \alpha(y)$$
$$= x + y$$

So $x + y \in E^H$.

Similarly, E^H is closed under subtraction, multiplication and division (by non zero elements), so E^H is a subfield of E. Since for $\alpha \in G(E, F)$, we have

$\alpha(k) = k$ for all $k \in F$

$\therefore F \subset E^H$.

Theorem 15.4.3. IF G (E, F) is a Galois group of the finite extension E|F and H is a finite subgroup of G(E,F), then $\left[E^H : F\right] = \left[E : F\right] \big/ 0(H)$

Proof : We have $F \subseteq E^H \subseteq E$. So

$$\left[E : F\right] = \left[E : E^H\right]\left[E^H : F\right]$$

$$\Rightarrow \left[E^H : F\right] = \left[E : F\right] \Big/ \left[E : E^H\right]$$

$$= \frac{[E:F]}{E(H)}, \text{ by theorem 14.14.4.}$$

Lemma 15.4.4. Suppose E|F is a field extentsion and $\alpha \in 0$ is a zero of the polynomial f(x) over F. If σ is F-automorphism of E, then $\sigma(\alpha)$ is also a zero of f.

Proof : See the proof of Lemma 14.14.1. We will refer to the following special case as "APR" (Automorphism Permute Roots).

Theorem 15.4.5. (APR) Let E|F be a field extension and let $\alpha \in F$ be algebraic over F with minimal polynomial $f \in F[x]$. If $\sigma \in G(E,F)$, then $\sigma(\alpha)$ is also a zero of f(x).

Theorem 15.4.6. Let α be algebraic over F with minimal polynomial $f \in F[x]$ and consider the extension $E = F(\alpha)$ of F. Let K|E is an extension. Then there is a bijeetion between the set of homomorphisms $\sigma : F(\alpha) \to K$ that fix elements of F and the set of distinct zeros of f(x) in K.

Proof : Let $\sigma : F \to K$ be a homomorphism such that $\sigma(a) = a$ for all $a \in F$. We have seen that $\sigma(\alpha)$ is a root of f(x) in E. Since every elements of $E = F(\alpha)$ is of the form $\beta = \sum_i a_i \alpha^i$ with $a_i \in F$

$$\sigma(\beta) = \sum_i \sigma(a_i \alpha^i) = \sum_i \sigma(a_i)\, \sigma(\alpha^i)$$

$$= \sum_i a_i \left[\sigma(\alpha^i)\right]$$

Hence σ is determined by its value $\sigma(\alpha)$ on α which says that there is a well-defined, injective function from the set of homomorphism $\sigma : E \to K$ such that $\sigma(a) = a$ for all $a \in F$ to the set of zeros of the polynomial f(x) in K, defined by mapping σ its value $\sigma(\alpha)$ on α. We must show that this function is surjective, in other words, given a zero $\beta \in K$ of f(x), there exists a homomorphism $\sigma : E \to K$ such that $\sigma(a) = a$ for all $\alpha \in F$ and such that $\sigma(\alpha) = \beta$

Let β be a root of f(x) in K.

We know that $F(\alpha) \cong F[x] \Big/ < f(x) >$

and infact $\Phi_\alpha : F[x] \to F(\alpha)$ defines an isomorphism from $F[x] \Big/ < f(x) >$ to $F(\alpha)$, which we denote by $\hat{\Phi}_\alpha$ with the property $\hat{\Phi}_\alpha\left(x + < f(x) >\right) = \alpha$ and $\hat{\Phi}_\alpha(a) = a$ for all $a \in F$ (where we identify $a \in F$ with the coset

$a+<f(x)>\in F[x]/<f(x)>$). On the other hand f (β)=0 by hypothesis, so that irr(β,F,x) divides f(x) are monic irreducible polynomials, irr(β, F, x) = f(x). Thus the subfield F(β) of K is also isomorphism to $F[x]/<f(x)>$ and in fact the evaluation homomorphism $\hat{\Phi}_p : F[x] \to F(\beta)$ defines an isomorphism, with the property $\hat{\Phi}_\beta(x+<f(x)>)=\beta$ and $\hat{\Phi}_\beta(a)=a$ for all $a \in F$. Taking the composition $\sigma = \hat{\Phi}_\beta{}^0\ \hat{\Phi}_{-\alpha}^{-1}$, σ is an isomorphism from F(α) to F(β), with the property that $\sigma(\alpha)=\beta$ and σ(a) = a for all $a \in F$. Viewing the range of σ as K (instead of the supfield F(β) gives a homomorphism as desired.

Corollary 15.4.7 Let α be algebraic over F. Then $\circ(G(F(\alpha),F)$ is equal to the number of distinct zeros of the minimal polynomial m_α of α over F in F(α). If β is such a zero, the corresponding automorphism maps α to β.

Proof : This is just a special case of 15.4.6, when K = k (α), except that theorem 15.4.6. uses homomorphism, while the Galois group consists of automorphisms.

Corollary 15.4.8. If E|F is a field extension, then $\circ(G(E, F))\le[E:F]$

Proof : We may assume E = F(α) for some $\alpha \in F$. Let f$\in$F[x] denote the minimal polynomial of α over F. Then degree of f is [E : F].

But $O(G(E, F))$ is the number of zeros of f in F(α) and this is bounded by the degree of f, which is [E : F], i.e. $O(G(E, F))\le[E:F]$

Example 1. We compute the Galois group of the extension E|F where F = Q and E is the splitting field of x^3-2 namely E = $Q(\sqrt[3]{2}, w)$, where $w = e^{\frac{2\pi i}{3}}$

An automorphism σ of G (E, F) must set $\sqrt[3]{2}$ to another cube root of 2 in E i.e. $\sqrt[3]{2}\ w^i$ for i = 0, 1, 2 and also must send w to another zero of x^2+x+1, so either fixes w or sends it to its conjugate $\overline{w} = w^2$. Therefore, there are 6 F-automorphisms of E, given by

$\sqrt[3]{2} \to \sqrt[3]{2}$ $\quad w \to w$

$\sqrt[3]{2} \to \sqrt[3]{2}$ $\quad w \to w^2$

$\sqrt[3]{2} \to \sqrt[3]{2}w \qquad w \to w$

$\sqrt[3]{2} \to \sqrt[3]{2}w \qquad w \to w^2$

$\sqrt[3]{2} \to \sqrt[3]{2}w^2 \qquad w \to w$

$\sqrt[3]{2} \to \sqrt[3]{2}w^2 \qquad w \to w^2$

Note that if ϕ and ψ denote the second and thrid of this automorphisms, then the automorphisms are I, ϕ, ψ, $\psi\phi$, ψ^2 and $\phi\psi$ respectively. It follows that the Galois group is generated by ϕ and ψ of order 2 and 3 respectively, and one easily verifies that $\phi\psi\phi = \psi^{-1}$, so that the group is isomorphic to D_3, the dihedral group with 6 elements.

The roots of x^3-2 are given by $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}w$ and $\alpha_3 = \sqrt[3]{2}w^2$. Let us work out how these automorphisms act on the zeros of the equation. For example, consider the automorphism which sends $\sqrt[3]{2} \mid\to \sqrt[3]{2}w$ and $w \mid\to w^2$. This sends $\alpha_1 = \sqrt[3]{2}$ to $\sqrt[3]{2}w = \alpha_2$ and $\alpha_2 = \sqrt[3]{2}w$ to $\sqrt[3]{2}w.w^2 = w^3\sqrt[3]{2} = \sqrt[3]{2} = \alpha_1$ and $\alpha_3 = \sqrt[3]{2}w^2$ to $\sqrt[3]{2}w.\left(w^2\right)^2 = 3\sqrt{2}w^2\,\alpha_3$. Thus it exchanges the first two zeros and we regard it as the permutation (1, 2) of S_3. With this notation, we see that the six automorphism correspond to the elements.

I, (2 3), (1 2 3), (1, 2), (1 3 2), (1 3) of S_3 respectively. This proves that the Galois group G(E,F) is equal to S_3.

This example indicate how we can regard the F-automorphisms of E, in the case where E is a splitting field of some polynomial over F, as being permutations of the zeros of the polynomial.

Let's record this formally. Lemma 15.4.9. Suppose E be the splitting field of a polynomial f of degree n over F. List the zeros of f in E as $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$. Then the action of G(E, F) on the zeros gives an injective homomorphism of groups.

$$G(E, F) \to S_n$$

where S_n is the group ofpermutations of n objects.

Here $\phi \in G(E, F)$ gives us a permutation σ in S_n if ϕ acts on s $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ by the permutation σ i.e. if $\Phi(\alpha_i) = \alpha_{\sigma(i)}$.

Proof : Consider $E = F(\alpha_1, \alpha_2, \ldots \alpha_n)$ where $\alpha_1, \alpha_2, \ldots \alpha_n$ are the zeros of

f in E. We can look at the action $\phi \in G$ (E, F) on the zeros of f. By APR (Theorem 15.4.5), $\Phi(\alpha_i)$ is also a zero of f, so is one of $\alpha_1, \alpha_2, \ldots \alpha_n$. As Φ is injective, Φ is a permutation of the set $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$. In this way, we obtain a homomorphism $G(E, F) \to S_n$. It is injective –if θ lies in the Kernal, then θ is mapped to the trivial permutation, so that it sends each α_i to itself as well as fixing F, it fixes all of F.



CHECK YOUR PROGRESS

Q 1: Suppose F = Q and E = $Q(\sqrt{2}, \sqrt{3})$. Show that the Galois group G(E, F) is isomorphism to $C_2 \times C_2$.

15.5 GALOIS EXTENSIONS : DEFINITIONS AND EXAMPLES

Definition: A finite extension E|F of fields is Galois if

$$O(G(E, F)) = [E : F]$$

Example 1. The extension $Q(\sqrt[4]{2}) | Q$ is not Galois because 2 = 0 ($G Q(\sqrt[4]{2})$, Q) $\neq$ [$Q(\sqrt[4]{2})$: Q]

Example 2. The extension $Q(\sqrt[3]{2}, w)$|Q is Galois.

Example 3. Every extension E|F of degree 2 is Galois. In deed, we can write E = $F(\sqrt{\beta})$ for some $\beta \in E$ and G(E, F) = {I, conj} where I is the identity map and conj : $\sqrt{\beta} \mid\to \sqrt{\beta}$, so

$$O(G(E, F)) = [E : F] = 2$$

Definition: Let E be a field and let S be a finite set of automorphisms of E. Then the fixed field of S is defined as E^s = {x $\in$ E : θ (x) = x for all $\theta \in S$}

Example 1. If E = $Q(\sqrt[4]{2})$, then $E^{G(E,Q)} = E^{\{I, Conj\}} = Q(\sqrt{2})$

Example 2. If E = $Q(\sqrt{2})$, then $E^{G(E,Q)} = E^{\{I, Conj\}} = Q$

15.6 PROPERTIES OF GALOIS EXTENSIONS

Theorem 15.6.1. Let E|F be a finite extension of fields. Assume that $F \subseteq E \subseteq C$. Then the following are equivalent :

i) E|F is Galois;

ii) E is the splitting field of an irreducible polynomial $f \in F(x)$;

iii) E|F is normal;

iv) $F = E^{G(E,F)}$

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

Suppose E|F be a Galois extension. We have to prove E is the splitting field of an irreducible polynomial $f \in F[x]$.

By TPE (Theorem 15.4.5) there exists an $\alpha \in F$ such that $E = F(\alpha)$. Let f(x) denote the minimal polynomial of α over F. We know

(1) [E : F] is equal to the degree of f.

(2) $O(G(E, F))$ is equal to the number of distinct zeros of f in E.

So we see that $[E : F] = O(G(E, F))$ implies that the number of zeros of f in E is equal to the degree of f, i.e. f factories over E into linear factors. Therefore we have shown that if E|F is Galois, then E is the splitting field of an irreducible polynomial f over F.

(ii) $\Rightarrow$ (iii)

Let E be the splitting field of an irreducible polynomial f over F. We have to prove E|F is normal.

Let $g \in F[x]$ be any other polynomial with a zero $\alpha \in F$. Suppose β is another zero of g. We need to show $\beta \in E$. By theorem 15.4.6, there is an isomorphism $\theta : F(\alpha) \to F(\beta)$ which fixes F and maps $\alpha \mid\to \beta$.

Let $\alpha_1, \alpha_2, ... \alpha_n$ be the zeros of f. Then it is a fact that we can define homomorphism.

$$\Phi : F(\alpha_1, \alpha_2, ...\alpha_n) \to (\beta, \alpha_1, \alpha_2 .....\alpha_n)$$

that maps $\alpha \mid\to \beta$. Note that Φ is a map $E \to E(\beta)$. But by APR (Theorem 15.4.5), Φ must map each of the zeros of f to another zero of f. Since E is generated by the zeros of f, it follows that $\Phi(E) \subseteq E$.

Hence $E(\beta) = E$, So $\beta \in E$ as required.

(iii) $\Rightarrow$ (i)

Suppose E|F be normal. We have to prove E|F is Galois. By TPE (Theorem 15.4.5), there exists an $\alpha \in F$ such that $E = F(\alpha)$. Let f(x) denote the minimal polynomial of α over F. We know

- [E : F] is equal to the degree of f.
- $O(G(E, F))$ is equal to the number of distinct zeros of f.

Since E|F is normal and $\alpha \in E, E$ must contains all the zeros of f.

Hence $O(G(E, F))$ = number of zeros of f

= deg(f)

= [E : F]

Thus E|F is Galois.

(i) $\Rightarrow$ (iv)

Assume that E|F is Galois and Let G = G (E, F). We need to show that E^G = F.

Consider the Galois group G(E, E^G). Then $G \subseteq$ G (E, E^G).

Indeed, G acts on E and fixed E^G.

However we have F $\subseteq E^G \subseteq$ F. so

$$O(G) \leq O\left(G(E, E^G)\right) \leq \left[E : E^G\right] \leq \left[E : F\right]$$

Since E|F is Galois so $O(G)$ = [E : F] and hence [E : E^G] = [E : F] $\Rightarrow E^G$ = F, as required.

(iv) $\Rightarrow$ (i)

Write G = G (E, F) and suppose E^G = F. We need to show that E|F is Galois. By TPE (Theorem 15.4.5), that here exists an $\alpha \in E$ such that E = F(α). Let f(x) denote the minimal polynomial of α over F.

Consider the polynomial

$$g(x) = \prod_{\phi \in G(E,F)} x - \phi(\alpha) \in E[x]$$

i.e. the polynomial in E[x] whose zeros are $\phi(\alpha)$ for all $\phi \in$ G(E, F). We will show that $g(x) \in F[x]$.

Suppose $\theta \in G(E, F)$. Then

$$\theta\left(g(x)\right) = \theta\left(\prod_{\phi \in G(E,F} (x - \phi(\alpha)\right)$$

$$= \prod_{\phi \in G(E,F)} \left(x - \theta(\phi(\alpha))\right)$$

$$\prod_{\psi \in G(E,F)} (x - \psi(\alpha)) \quad \text{where } \psi = \theta\phi$$

= g(x)

Hence θ fixes all the coefficients of g(x), so $g(x) \in E^G[x]$. Since $E^G = F$, so $g(x) \in F[x]$.

But α is a zero of g(x), so we must have f(x)|g(x). Hence [E : F] = deg(f) $\leq$ deg(g) = $O(G(E,F)) \leq [E:F]$ from which it follows that $O(G(E,F)) = [E:F]$

Hence E|F is Galois.

Corollary 15.6.2. Suppose E|F be a Galois extension, and M ($F \subseteq M \subseteq E$) be an intermediate field. Then E|M is Galois.

Proof : Suppose E be the splitting field of some polymial $f \in F[x]$. Then certainly $f \in M[x]$ as $F \subseteq M$; but E splits f and is generated over F by the zeros, so it is also generated over M by the zeros. Thus E is the splitting field for f over M and is therefore E|M is Galois.

Note : Any automorphism of E which fixes every element of M will certainly fix every element of F. It follows that G(E, M) is a subgroup of G(E, F).

However, in general, M|F need not be Galois. We have already see a simple example.

$Q \subseteq Q(\sqrt[3]{2}) \subseteq Q(\sqrt[3]{2}, w)$. Here $Q(\sqrt[3]{2}, w) | Q$ and $Q(\sqrt[3]{2}, w) | Q(\sqrt[3]{2})$ are Galois extensions.

Lemma 15.6.3. Let $F \subseteq M \subseteq E$ be finite extensions of fields. If M|F is Galois then $\phi(M) = M$ for all $\phi \in G(E, F)$.

Proof : We may suppose $M = F(\alpha)$ is the splitting field for the irreducible polynomial m_α by TPE (Theorem 15.4.5). The element ϕ must map α to another zero of m_α. But this zero, say β, is also in M, because M splits m_α.Then it follows that $\phi(M) \subseteq M$ and similarly $\phi^{-1}(M) \subseteq M$, so $\phi(M) = M$.

Theorem 15.6.3. Let E|F be a Galois extension and let M be a intermediate field. Then M|F is Galois if and only if G (E,M) $\underline{\Delta}$ G (E, F). In this case, there is an isomorphism

$$\frac{G(E,F)}{G(E,M)} \cong G(M \mid F)$$

Proof : Suppose M|F is Galois. Then by preceding Lemma, $\phi(M) = M$ for all $\phi \in G(E, F)$.

That is, given $m \in M$, $\phi(m) \in M$. Since any $\theta \in G(E, M)$ will fix all elements of M, so

$\theta\ \phi(m) = \phi(m)$ for all $m \in M$, $\theta \in G(E, M)$ and $\phi \in G(E, F)$

$\Rightarrow \left(\phi^{-1}\theta\ \phi\right)(m) = m$

i.e. $\phi^{-1}\theta\ \phi$ fixes every element of M

$\Rightarrow \phi^{-1}\theta\ \phi \in G(E, M)$

Hence $G(E, M) \underline{\Delta}\ G(E, F)$

For the second part, define a map

$$\phi : G(E,F) \to G(M,F)$$
$$\phi \mid\to \phi/_M$$

Where $\phi/_M$ is the restriction of ϕ from $M \to M$. The map that sends ϕ to $\phi/_M$ is easily seen to be a group homomorphism and its kernal consists of all ϕ such that

$\phi/_M(m) = m$ for all $m \in M$, i.e. $\phi \in G(E|M)$.

Then first isomorphism theorem for groups gives

$$\frac{G(E,F)}{G(E,M)} \cong \mathrm{Im}\,\phi \subseteq G(M,F)$$

However, if we compare the sizes of the two sides, bearing in mind that E|F and E|M are both Galois.

$$O(\mathrm{Im}\,\phi) = \frac{O(G(E,F))}{O(G(E,M))} = \frac{[E:F]}{[E:M]} = [M:F] = O(G(M,E))$$

and so $(\mathrm{Im}\,\phi) = G(M,F)$

Conversely, suppose E|F be Galois and M be an intermediate field such that $G(E, M) \underline{\Delta}\, G(E, F)$. We have to prove M|F is Galois.

Note that $G(E, M) \underline{\Delta}\, G(E, F)$

$\Leftrightarrow \phi^{-1}\phi\theta \in G(E,M)$ for all $\theta \in G(E,M)$, $\phi \in G(E,F)$

$\Leftrightarrow \left(\phi^{-1}\theta\phi\right)(m) = m$ for all $m \in M$, $\theta \in G(E,M)$, $\phi \in G(E,F)$

$\Leftrightarrow \theta\phi(m) = \phi(m)$ for all $m \in M$, $\theta \in G(E,M)$, $\phi \in G(E,E)$

$\Leftrightarrow \phi(M) \subseteq E^{G(E,M)}$ for all $\phi \in G(E,F)$

$\Leftrightarrow \phi(M) \subseteq M$ for all $\phi \in G(E,F)$ by Theorem 15.6.1.

$\Leftrightarrow \phi(M) = M$ for all $\phi \in G(E,F)$

$\Leftrightarrow M \mid F$ is Galois.

Theorem 15.6.4. (Fundamental Theorem of Galois Theory) Let E

be a Galois extension of F and let G = G (E, F). Then

(i) There is a bijection from S = {subgroups of G} to

T = { intermediate fields $F \subseteq M \subseteq F$} given by

$H \mid\rightarrow E^H$ with inverse $M \mid\rightarrow G(E, M)$

(ii) Moreover, the correspondence is inclusion reversing, i.e.

$$H_1 \supseteq H_2 \Leftrightarrow E^{H_1} \subseteq E^{H_2}$$

and indexes equal degrees, i.e.

$$\frac{O(H_1)}{O(H_2)} = \left[E^{H_2} : E^{H_1}\right]$$

(iii) Finally, normal subgroups of G corresponds to intermediate fields $F \subseteq M \subseteq E$ such that M|F is Galois.

Terminology : For any inclusion of subgroups of any group, $\frac{O(H_1)}{O(H_2)}$ is called the index of H_2 in H_1. It is the number of cosets h_1H_2 for $h_1 \in H_1$.

Proof : (i) Let H be the subgroup of G = G (E, E) and let M be an intermediate subfield such that $F \subseteq M \subseteq E$. To prove S and T are in bijection, we need to show that the maps we have constructed are mutually invertible, i.e.

(a) $E^{G(E, M)} = M$ and (b) $G(E, E^H) = H$

For the part (a), by Corollary 15.6.2, E|M is Galois. Hence by theorem 15.6.1., $E^{G(E, M)} = M$.

For the part (b), first observe that $H \subseteq G(E, E^H)$ – indeed H acts on E and fixes E^H. We will show that , so that $O(G(E,E^H)) \leq O(H)$ this inclusion is an equality.

Let $M = E^H$. Then by Corollary 15.6.2, E|M is Galois. By TPE (Theorem 15.4.5), there exists an $\alpha \in F$ such that $E = M(\alpha)$. Let f(x) denote the minimal polynomial of α over M.

Consider the polynomial,

$$g(x) = \prod_{\phi \in H} (x - \phi(\alpha)) \in E(x) \phi \in H$$

i.e. the polynomial in E[x] whose zeros are $\phi(\alpha)$ for all $\phi \in H$.

We will show that $g(x) \in M[x]$.

Suppose $\theta \in H$. Then

$$\theta(gx) = \theta\left(\prod_{\phi \in H} (x - \theta(\alpha))\right)$$

$$= \prod_{\phi \in H} (x - \theta(\alpha))$$

$$= \prod_{\psi \in H} (x - \psi(\alpha)) \quad \text{where } \psi = \theta\,\phi$$

$$= g(x)$$

Hence θ fixes all the coefficients of g(x), so $g(x) \in E^H[x] = M[x]$. But α is a zero of f(x), so we must have f(x) |g(x).

Hence $[E : M] = \deg(f) \leq \deg(g) = O(H)$

for which it follows that G(E, M) = H, as required. It follows that the two maps $H \mid\!\to E^H$ and $M \mid\!\to G(E, M)$ are inverse bijections.

(ii) We observe that if $H_1 \supseteq H_2$, we have $E^{H_1} \subseteq E^{H_2}$ (anything in E fixed by H_1 will be fixed by H_2); conversely if $E^{H_1} \subseteq E^{H_2}$, the first part of the theorem shows that then $G(E, E^{H_1}) \supseteq G(E, E^{H_2})$ and also that $G(E, E^{H_i}) = H_i$ so that $H_1 \supseteq H_2$

For the assertion about indexes and degrees, first observe that it is immediate if $H_2 = 1$. In this case, $E^{H_2} = E$ and

$$[H_1 : 1] = O(H_2) = O(G(E, E^{H_1})) = [E : E^{H_1}]$$

Now consider the general case. We use the special case above to see that $|H_i| = [E : E^{H_i}]$. But also we have $\circ(H_1) = \circ(H_2)[H_1 : H_2]$ and $O(H_1) = [E : E^{H_1}]$

$$= [E : E^{H_2}]\ [E : E^{H_1}]$$

$$O(H_2)[E^{H_2} : E^{H_1}]$$

Thus $\dfrac{O(H_1)}{O(H)} = [E^{H_2} : E^{H_1}]$

Proof of (iii) follows the proof of Theorem 15.6.3.

Example. We are now going to look at the Galois theory of the polynomial x^3–2. Its splitting field is $Q(\sqrt[3]{2}, w)$, where w is a complex cubic root of unity, so this is Galois over Q. Let us look at all of the subfields of this field. We claim that the subfield lattice is

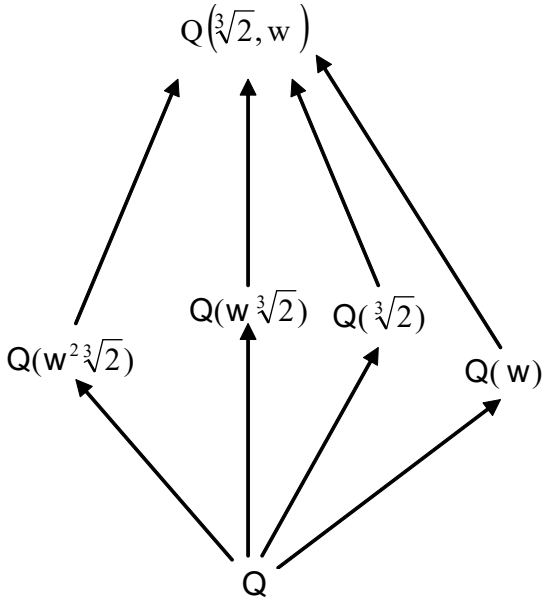


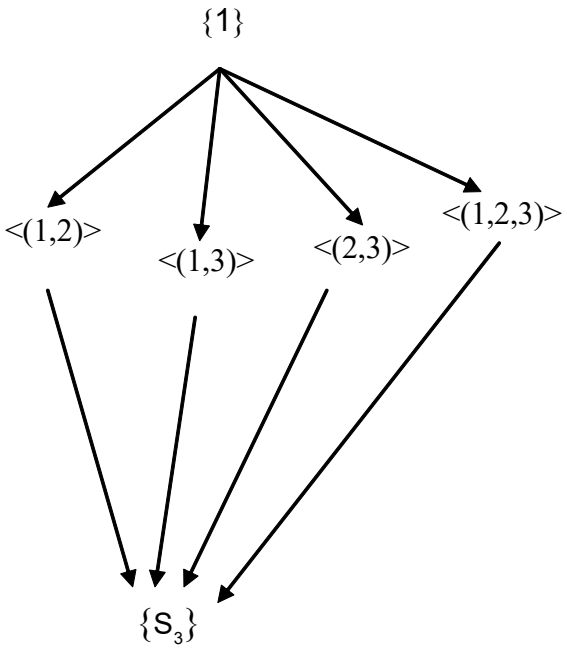
Figure 1 : Lattice of subfields of $Q(\sqrt[3]{2}, w)$

Now we constant the following table

Q-automorphism	effect on $\sqrt[3]{2}$	effect on w	permutation
I	$\sqrt[3]{2}$	w	I
ϕ	$\sqrt[3]{2}$	w^2	(2 3)
ψ	$w\sqrt[3]{2}$	w	(1 2 3)
$\psi\phi$	$w\sqrt[3]{2}$	w^2	(1 2)
ψ^2	$w\sqrt[3]{2}$	w	(1 2 3)
$\phi\ \psi$	$w\sqrt[3]{2}$	w^2	(1 3)

Table 1

The idea of Galois theory is that this is reflected by the group theoretical structure of the subgrous of the Galois group. We have already seen that $G\left(Q(\sqrt[3]{2}, w), Q\right)$ is S_3. Now S_3 has the (upside-down) subgroup lattice show in Figure 2.



We know check that the above pictures correspond.

Table 1 shows that the isomorphism $G\left(Q\left(\sqrt[3]{2}, w\right), Q\right) \cong S_3$.

Thus , if we consider the subfield Q(w) of $Q\left(\sqrt[3]{2}, w\right)$, then we can see that

$Q(w) \subseteq Q\left(\sqrt[3]{2}, w\right)^{<1\,2\,3>}$. This is because ψ(w)=w. Note that $[Q(w) : Q] = 2$. Now we use the Galois correspondence to saw that two degree egnols the index and so, we saw that we have an egnolity $Q(w) = Q(s\sqrt{2}, w)^{<1,2,3>}$.

In a similar way, we can identify the fixed field of each subgroup of S_3 and they are correspond as in the figure.



CHECK YOUR PROGRESS

Q.1. Let E = $Q\left(\sqrt[4]{2}, i\right)$. Find all the subgroups of the Galois group, G (E, Q) and give a diagrammatic representation of the correspondence given in fundamental theorem of Galois Theory.

Q.2. Let L = Q($\sqrt{2}$, $\sqrt{3}$). Show the correspondence given in fundamental theorem of Galois Theory.



15.7 LET US SUM UP

- The Galois group G(E, F) of a field extension E|F is the group of all F-automorphisms of E under the operation of composition of maps.
- Let E|F be a field extension. If M is a field such that $F \subset M \subset E$, then M is called an intermediate field.
- To each subgroup H of G(E, F), we associate the set E^H of all elements $x \in E$ such that $\alpha(x) = x$ for all $\alpha \in H$. In face, this set is an intermediate field.
- If G(E, F) is a Galois Group of the finite extension E|F and H is a finite subgroup of G (E, F), then
  $$[E^H : F] = [E : F] / O(H)$$
- Suppose E|F is a field extension and $\alpha \in E$ is a zero of the polynomial f(x) over F. If is σ a F-automorphism of E, then $\sigma(\alpha)$ is also a zero of f.
- Let E|F is a field extension and let $\alpha \in E$ be algebraic over F with minimal polynomial $f \in F[x]$. If $\sigma \in G$ (E, F), then $\sigma(\alpha)$ is also a zero of f(x).
- Let α be algebraic over F with minimal polynomial over $f \in F$ [x] and consider the extension $E = F(\alpha)$. Let K|E is an extension. Then there is a bijection between the set of homomorphism $\sigma : F(\alpha) \to K$ that fix elements of F and the set of distinct zeros of f(x) in K.
- Suppose E be the splitting field of a polynomial f of degree n over F. List the zeros of f in E as $\{\alpha_1, \alpha_2, ... \alpha_n\}$. Then the action of G(E, F) on the zeros gives an injective homomorphism of groups
  G (E, F) $\to S_n$
  where S_n is the group of permutations of n objects.
- A finite extension E|F of field is Galois if $O(G(E,F)) = [E:F]$.
- Let E|F be a finite extenion of fields. Assume that $F \subseteq E \subseteq C$. Then the following are equivalent :

(i) E|F is Galois.

(ii) E is the splitting field of an irreducible polynomial $f \in F[x]$.

(iii) E|F is normal

(iv) $F = E^{G(E,F)}$

- Suppose E|F is a Galois extension and M ($F \subseteq M \subseteq E$) be an intermediate field. Then E|M is Galois.
- Let $F \subseteq M \subseteq E$ be a finite extension of fields. If M|F is Galois then $\phi(M) = M$ for all $\phi \in G(E, F)$.
- Let E|F be a Galois extension and Let M be a intermediate field. Then M|F is Galois if and only if $G(E, M) \triangleq G(E, F)$. In this case, there is a isomorphism

$$\frac{G(E,F)}{G(E,M)} \cong G(M \mid F)$$

- Let E be a Galois extension of F and let G = G (E, F). Then

(i) there is a bijection from S = { subgroup of G} to

T = {intermediate fields $F \subseteq M \subseteq E$ } given by $H \mid\to E^H$ with inverse $M \mid\to G(E, M)$

(ii) Moreover, the correspondence is inclusion reversing i.e

$H_1 \supseteq H_2 \Leftrightarrow E^{H_1} \subseteq E^{H_2}$ and indexes equal degrees, i.e.

$$\frac{O(H_1)}{O(H)} = \left[E^{H_2} : E^{H_1}\right]$$

(iii) Finally, normal subgroup of G corresponds of to the intermediate field $F \subseteq M \subseteq E$ such that M|F is Galois.

- The polynomial $x^2–x$ splits in $Q(\sqrt{2})$ over Q, so $G\left(Q(\sqrt{2}), Q\right) \cong C_2$
- The polynomial x^2+1splits in Q(i) over Q, so $G(Q(i), Q) \cong C_2$
- The polynomial x^2+x+1 splits in Q(w), where $w = e^{\frac{2\pi i}{3}}$, over Q, So $G(Q(w), Q) \cong C_2$
- The polynomial $x^3–1=(x–1)(x^2+x+1)$ also splits in Q(w), so $G(Q(w), Q) \cong C_2$
- The polynomial $x^4–x^2–2 = (x^2–2)(x^2+1)$ splits in Q ($\sqrt{2}$,i), so $G\left(Q(\sqrt{2}), i\right) \cong V_4$

- The polynomial $x^4-5x^2+6 = (x^2-2)(x^2-3)$ splits in $Q(\sqrt{2}, \sqrt{3})$ over Q, so $G\left(Q(\sqrt{2}, \sqrt{3}), Q\right) \cong V_4$



15.8 ANSWER TO CHECK YOUR PROGRESS

Ans to Q.No. 1.

Suppose F = Q and E = $Q(\sqrt{2}, \sqrt{3})$, Let ϕ be a Q-automorphism of $Q(\sqrt{2}, \sqrt{3})$. Since $\left(\sqrt{2}\right)^2 = 2$, so $\phi\left(\sqrt{2}\right)^2 = \phi\left((\sqrt{2})^2\right) = \phi(2) = 2$

$\Rightarrow \phi(\sqrt{2}) = \pm\sqrt{2}$

Similarly, $\phi(\sqrt{3}) = \pm\sqrt{3}$. There are 4 Q-automorphism of $Q\left(\sqrt{2}, \sqrt{3}\right)$, induced by

$I: \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{3} \mapsto \sqrt{3}$

$\phi_1: \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{3} \mapsto -\sqrt{3}$

$\phi_2: \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{3} \mapsto \sqrt{3}$

$\phi_1\phi_2: \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{3} \mapsto -\sqrt{3}$

Since $Q(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3)$ over Q. If the four zeros are $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$, then the four automorphisms permute the α_i as

I (3, 4), (1, 2), (1, 2) (3, 4) respectively.

This shows that the Galois group has four element and looks like the subgroup of S_4 ismorphic to $C_2 \times C_2$ generated by to disjoint transpositions.

Ans to Q.No. 2.

Let E = $Q\left(\sqrt[4]{2}, i\right)$, the splitting field x^4-2 over Q. Thus E|Q is Galois. [E : Q] = 8 as [E : $Q\left(\sqrt[4]{2}\right)$] = 2 and [$Q\left(\sqrt[4]{2}\right)$: Q] = 4. Then $\circ\left(G(E, Q)\right)$ = 8.

Now $\sqrt[4]{2}$ has minimal polynomial x^4-2 whose zeros are $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$ and $-i\sqrt[4]{2}$. Further, i has minimal polynomial x^2+1, whose zeros are $\pm$ i.

The eight possible Q-automorphisms of M are given in the following table:

Q-automorphism	effect on $\sqrt[4]{2}$	effect on i	permutation	Remarks
I	$\sqrt[4]{2}$	i	I	
ϕ	$i\sqrt[4]{2}$	i	(1 2 3 4)	$\phi^4 = I$
ϕ^2	$-\sqrt[4]{2}$	i	(1 3) (2 4)	
ϕ^3	$-i\sqrt[4]{2}$	i	(1 4 3 2)	
ψ	$\sqrt[4]{2}$	– i	(2 4)	$\psi^2 = I$
$\phi\,\psi$	$i\sqrt[4]{2}$	– i	(1 2) (3 4)	
$\phi^2\psi$	$-\sqrt[4]{2}$	– i	(1 3)	
$\phi^3\psi$	$-i\sqrt[4]{2}$	– i	(1 4) (2 3)	$\phi^3\psi = \psi\ \phi$

It follows that G (E, Q) = {I, ϕ, ϕ^2, ϕ^3, ψ, $\phi\,\psi$, $\phi^2\psi$, $\phi^3\psi \cong D_4$,
the dihedral group of order 8.

The (upside – down) subgroup lattice of D_4 is shown in Figure 3.

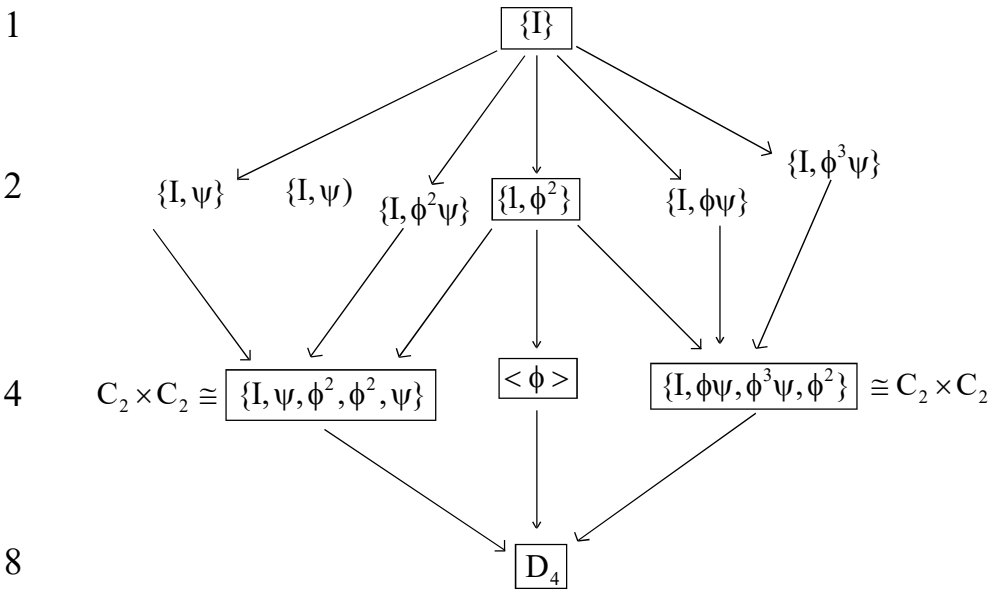


Figure 3 : The subgroup lattice of D_4. The normal subgroups are boxed.

The subfield lattice of E = Q ($\sqrt[4]{2}$, i) is shown Figure 4.

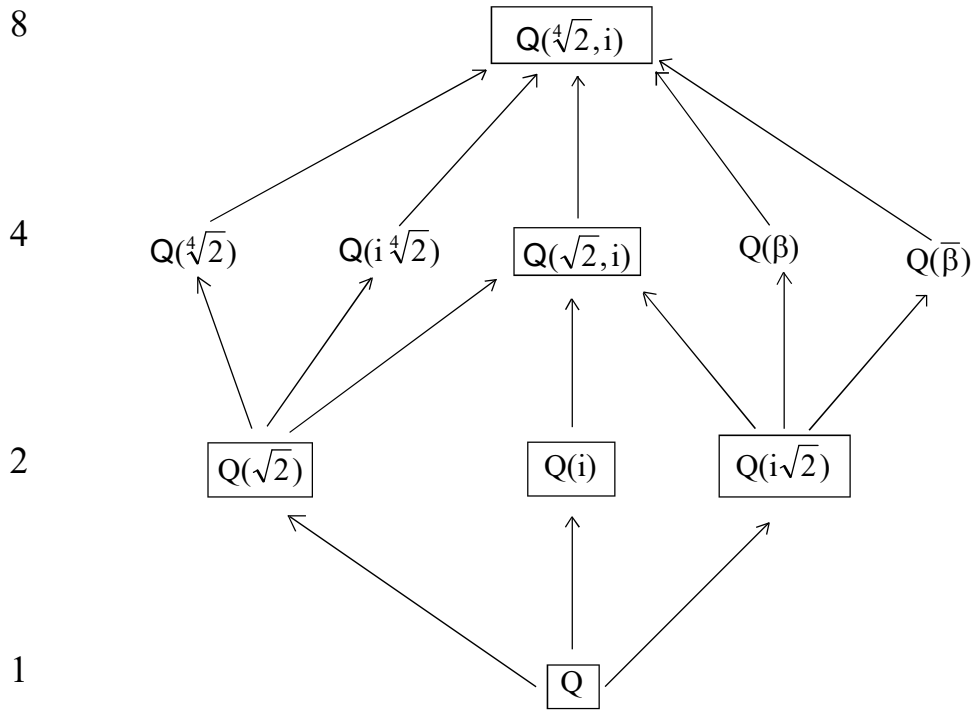


Figure 4 : The subfield lattice of E = Q ($\sqrt[4]{2}$, i). The subfield of E which are Galois extensions of Q are boxed. Note β = (1+i) $\sqrt[4]{2}$

Now we verify the Galois correspondence. Consider the subfield M = Q(β) = Q ((1+i) $\sqrt[4]{2}$). We first prove it is fixed by $\phi\psi$

$$\begin{aligned}
\phi\psi((1+i)\sqrt[4]{2}) &= \phi\psi\left(\sqrt[4]{2}\right)+\phi\psi\left(i\sqrt[4]{2}\right)\\
&= \phi\left(\psi\sqrt[4]{2}\right)+\phi\left(\psi(i)\,\psi\sqrt[4]{2}\right)\\
&= \phi\left(\left(\sqrt[4]{2}\right)\right)+\phi\left(-i\sqrt[4]{2}\right)\\
&= i\sqrt[4]{2}+\phi(-i)\,\phi\left(\sqrt[4]{2}\right)\\
&= i\sqrt[4]{2}+(-1).i\sqrt[4]{2}\\
&= \sqrt[4]{2}+i\sqrt[4]{2}\\
&= (1+i)\sqrt[4]{2}
\end{aligned}$$

Next we check that it is not fixed by ϕ^2

$$\begin{aligned}
\phi^2\left((1+i)\sqrt[4]{2}\right) &= \phi^2\left(\sqrt[4]{2}\right)+\phi^2\left(i\sqrt[4]{2}\right)\\
&= -\sqrt[4]{2}-i\sqrt[4]{2}\\
&= -(1+i)\sqrt[4]{2}
\end{aligned}$$

It follows the subgroup of D_4 corresponding to M must be a subgroup containing $\phi\psi$ but not ϕ^2 . A quick examination of the list of subgroups

shows that the only possibility is $\{1, \phi\psi\}$. The other correspondances are similar.

Ans to Q. No. 3

We know that E = Q ($\sqrt{2}, \sqrt{3}$) is a Galois extension of Q and G (E, Q) = {I, ϕ_1, ϕ_2, $\phi_1 \phi_2$}from Ans to Q.No. 1. Which is isomorphic to the Klein-four group $C_2 \times C_2$. Following diagram represent the correspondence given in fundamental theorem of Galois theory. We can see the strong similarity between the lattie for the subfields of E and the lattice for the subgroups of G (E, Q)

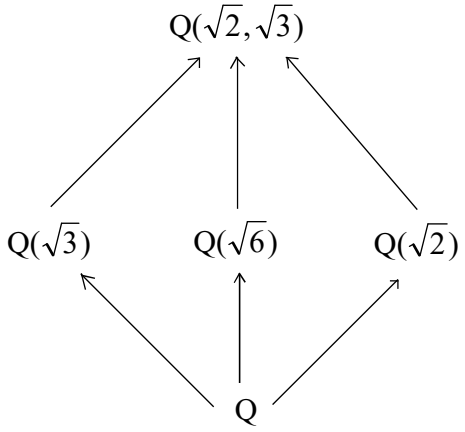
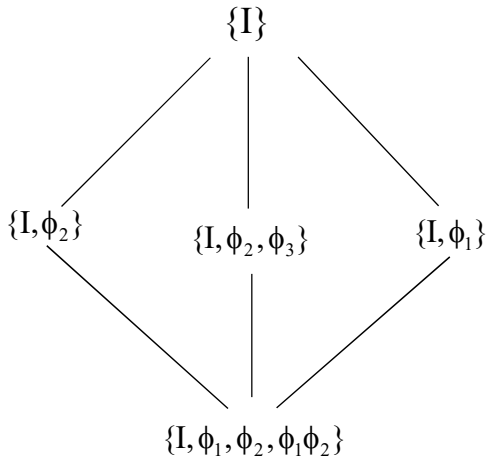


Figure 5 : (a) The lattice of subfields of Q ($\sqrt{2}, \sqrt{3}$)



(b) The lattice of the corresponding subgroups of G (E, Q)



15.9 FURTHER READING

1) Fraleigh, John B : A first course in Abstract Algebra, Pearson Education (Singapure) Pvt. Ltd.
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) Stewart, I : Galois Theory, CRC Press, Taylor and Francis Group, 6000 Broken Sound Parkway NW, Suite Zoo Boca Raton, FL 33487-2742
5) Mackenzie, K and Weiss, A : Galois Theory, Algebra I, Notes by A.F. Jarvis, http:// ariel-weiss.postgrad.shef.ac.uk/teaching/galois-theory.



15.10 MODEL QUESTIONS

Q 1: Find the Galois group of field extension $Q(\sqrt{2}) \mid Q$.

Q 2: Show that the extension $Q(\sqrt[4]{2}) \mid Q$ is not Galois.

Q 3: Let E = Q $\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$. Find the subgroups of the Galois group, G (E, Q) and the corresponding subfields of E.

*** ***** ***



REFERENCES

1. Gallian, J.A. Contemporary Abstract Algebra. 9th edition. Cengage Learning, 2015.
2. Lang, S. Algebra. 3rd edition, Springer 2012.
3. Herstein, I. N. Topics in Algebra. 2nd edition. John Wiley and Sons, 2006.
4. Bhattacharya, P. B. Jain. S. K. and Nagpaul, S. R. Basic Abstract Algebra. 2nd edition, Cambridge University Press, 2003.
5. Khanna, V. K. and Bhammbri, S. K. A Course in Abstract Algebra. Vikash Publishing House, 1999.
6. Cohn, P. M. Algebra, Vols. I & II, John Wiley & Sons, 1991.
7. Luther, S. and Passi, I. B. S. Algebra. Vol. I Groups, Vol. II-Rings, Narosa Publishing House (Vol. I – 1996, Vol. II – 1990).
8. Hungerford, T. W., Algebra. (1947). Springer-Verlag. New York.
9. D. S. Dummit and R. M. Foote, Abstract Algebra (3rd Edition), Wiley, 2011.
10. N. Jacobson, Basic Algebra I (3rd edition), Hindustan Publishing corporation, New Delhi, 2002.
11. J. B. Fraleigh, A First Course in Abstract Algebra (4th edition), Narosa Publishing House, New Delhi, 2002.