MAL-511: M. Sc. Mathematics (Algebra)

Lesson No. 1 **Written by Dr. Pankaj Kumar**

Lesson: Subnormal and Normal series-I **Vetted by Dr. Nawneet Hooda**

STRUCTURE.

1.0 OBJECTIVE. Objective of this Chapter is to study some properties of groups by studying the properties of the series of its subgroups and factor groups.

1.1 INTRODUCTION. Since groups and their subgroups have some relation, therefore, in this Chapter we use subgroups of given group to study subnormal and normal series, refinements, Zassenhaus lemma, Schreier's refinement theorem, Jordan Holder theorem, composition series, derived series, commutator subgroups and their properties and three subgroup lemma of P. Hall. In **Section 1.2**, we study subnormal and normal series. It is also shown that every normal series is a subnormal but converse may not be true. **In Section 1.3,** we study Zassenhaus Lemma and Schreier's refinement theorem. **In Section 1.4,** we study composition series and see that an abelian group has composition series if and only if it is finite. We also study Jordan Holder theorem which say that any two composition series of a finite group are

equivalent. At the end of this chapter we study some more series namely Chief series, derived series and their related theorems.

1.2 SUBNORMAL AND NORMAL SERIES

1.2.1 Definition (Sub-normal series of a group). A finite sequence

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_n=(e)$$

of subgroups of G is called subnormal series of G if G_i is a normal subgroup of G_{i-1} for each i, $1\leq i \leq n$.

1.2.2 Definition (Normal series of a group). A finite sequence

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_n=(e)$$

of subgroups of G is called normal series of G if each G_i is a normal subgroup of G for $1 \leq i \leq n$.

Example. Let $G =\{1, -1, i, -i\}$ where $i^2=-1$, is a group under ordinary multiplication. Consider the sequence;

$$\{1, -1, i, -i\}=G_0\supseteq\{1, -1\}= G_1\supseteq\{1\}=G_2$$

This is normal as well as subnormal series for G.

1.2.3 Theorem. Prove that every normal series of a group G is subnormal but converse may note be true.

Proof. Let G be a non empty set and

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_n=(e) \qquad (*)$$

be its normal series. But then each G_i is normal in G for $1 \leq i \leq n$. i.e. for every $g_i\in G_i$ and for every $g\in G$, we have $(g_i)^{-1}\, g\, g_i\in G_i$. Since $G_i \subseteq G_{i-1} \subseteq G$. Hence for every $g_i\in G_i$ and for every $g_{i-1}\in G_{i-1}$, we have $(g_{i-1})^{-1}\, g_i\, g_{i-1}\in G_i$ i.e. G_i is normal in G_{i-1}. Hence (*) is subnormal series for G also.

For converse part take $G = S_4$, symmetric group of degree 4. Then the sequence

$$S_4= G_0 \supseteq A_4 = G_1\supseteq V_4=G_2\supseteq \{(1\ 2)(3\ 4), e\}= G_3\supseteq (e)= G_4.$$

where A_4 is the group of all even permutations, $V_4 =\{ I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. For showing that it is subnormal series we use following two results:

(i) As we know that if index of a subgroup H of G is 2 then it is always normal in G.

(ii) Take $\alpha^{-1}\beta\alpha$, α and β are permutations from S_n, then cyclic decomposition of permutations $\alpha^{-1}\beta\alpha$ and β remains same. For example, cyclic decomposition of α^{-1} (1 2)(3 4) α is always 2×2 form. Similarly cyclic decomposition of α^{-1} (1 2 3)(4 6) α is always 3×2. In other words we can not find α in S_n such that α^{-1} (1 2)(3 4) α=(1 2 3)(4 6).

Now we prove our result as: Since index of $G_1(= A_4)$ is 2 in $G_0(= S_4)$, by (i) G_1 is normal in G_0. Since $G_2(=V_4)$ contains all permutations of the form (a b)(c d) of S_4, therefore, by (ii) G_2 is normal in G_1. By (i) $G_3(=\{(1\ 2)(3\ 4), e\}$ is normal in G_2. Trivially $G_4(=e)$ is normal in G_3. Hence above series is a subnormal series.

Consider $(1\ 2\ 3\ 4)^{-1}$ (1 2)(3 4)(1 2 3 4)= (1 4 3 2)(1 2)(3 4)(1 2 3 4) =(1 4)(2 3)$\notin G_3$. Hence G_3 is not normal in S_4. Therefore, the required series is subnormal series but not normal.

1.2.4 Definition.(Refinement). Let $G=G_0\supseteq G_1\supseteq G_2\supseteq\ldots\supseteq G_n=(e)$ be a subnormal series of G. Then a subnormal series $G=H_0\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq H_m=(e)$ is called refinement of G if every G_i is one of the H_j's.

Example. Consider two subnormal series of S_4 as:

$$S_4\supseteq A_4\supseteq V_4\supseteq(e)$$

and $$S_4\supseteq A_4\supseteq V_4\supseteq\{(1\ 2)(3\ 4), e\}\supseteq(e).$$

Then second series is refinement of first series.

1.2.5 Definition. Two subnormal series

$$G=G_0\supseteq G_1\supseteq G_2\supseteq\ldots\supseteq G_r=(e)$$

and $$G=H_0\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq H_s=(e) \text{ of } G$$

are isomorphic if there exist a one to one correspondence between the set of non-trivial factor groups $\frac{G_{i-1}}{G_i}$ and the set of non-trivial factor groups $\frac{H_{j-1}}{H_j}$ such that the corresponding factor groups of series are isomorphic.

Example. Take a cyclic group G =<a>of order 6. Then G={e, a, a^2, a^3, a^4, a^5}. Take G_1={e, a^2, a^4} and H_1={e, a^3}. Then G=$G_0 \supseteq G_1$={e, a^2, a^4}$\supseteq G_2$=(e) and G=$H_0 \supseteq H_1$={e, a^3}$\supseteq H_2$=(e) are two subnormal series of G. The set of factor groups is $\{\frac{G_0}{G_1}, \frac{G_1}{G_2}\}$ and $\{\frac{G_0}{H_1}, \frac{H_1}{\{e\}}\}$. Then $\frac{G_0}{G_1} \cong \frac{H_1}{\{e\}}$ and $\frac{G_1}{\{e\}} \cong \frac{H_0}{H_1}$ i.e. above two subnormal series of G are isomorphic.

1.3 ZASSENHAUS LEMMA AND SCHREIER'S REFINEMENT THEOREM.

1.3.1 Lemma. If H and K are two subgroup of G such that kH=Hk for every k in K. Then HK is a subgroup of G, H is normal in HK, H∩K is normal in K and $\frac{HK}{H} \cong \frac{K}{H \cap K}$.

Proof. Since kH=Hk for every k in K, therefore, HK is a subgroup of G. Now let hk∈HK, h∈H and k∈K. Then $(hk)^{-1}h_1(hk) = k^{-1}h^{-1}h_1 hk = k^{-1}h_2 k$. Since kH=Hk, therefore, $h_2 k = k h^*$ for some h*∈H. Hence $(hk)^{-1}h_1(hk)=k^{-1}kh^*=h^*$ ∈H . i.e. H is normal subgroup of HK. Further H is normal in K also since $k^{-1}hk=k^{-1}kh^* \in H$ for all k∈K and h∈H. But then H∩K is normal subgroup in K. Therefore, by fundamental theorem of isomorphism

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

1.3.2 Zassenhaus Lemma. If B and C are two subgroup of group G and B_0 and C_0 are normal subgroup of B and C respectively. Then

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

Proof. Let $K = B \cap C$ and $H = B_0(B \cap C_0)$. Since B_0 is normal in B, therefore, every element of B commutes with B_0. Further $K \subseteq B$, therefore, every element of K also commutes with B_0. Also C_0 is normal in C, therefore, B∩C_0 is normal in B∩C=K. Hence every element of K also commutes with B∩C_0. By above discussion

$$Hk = B_0(B \cap C_0)k = B_0k(B \cap C_0) = kB_0(B \cap C_0) = kH.$$

i.e. we have shown that Hk=kH for every k in K. Then by Lemma 1.3.1,

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

Now we will compute HK and H∩K.

Since $(B \cap C_0) \subset (B \cap C)$, therefore, HK= $B_0(B \cap C_0)(B \cap C) = B_0(B \cap C)$.

Further, let $y \in H \cap K$ then $y \in H$ and $y \in K$. Now $y \in H = B_0(B \cap C_0) \Rightarrow$ $y=b_0 b$ where $b_0 \in B_0$, $b \in (B \cap C_0)$. Let $b_0 b = d$ for $d \in K = B \cap C$. Then $d \in C$. Since $(B \cap C_0) \subseteq C$, therefore, b also belongs to C.

Now $b_0 b = d \Rightarrow b_0 = d\ b^{-1}$. Since $b, d \in C$, therefore, $d\ b^{-1} = b_0$ also belongs to C. Hence $b_0 \in (B_0 \cap C)$. Then $b_0 b \in (B_0 \cap C)(B \cap C_0)$. Hence $H \cap K \subseteq (B_0 \cap C)(B \cap C_0)$.

On the other side,

$$(B_0 \cap C) \subset K\ ,\ (B \cap C_0) \subset K \Rightarrow (B_0 \cap C)(B \cap C_0) \subset K\ .$$

Since $(B_0 \cap C) \subseteq B_0$, therefore, $(B_0 \cap C)(B \cap C_0) \subset B_0(B_0 \cap C) = H$. Hence $(B_0 \cap C)(B \cap C_0) = H \cap K$.

On putting the values of H, K, HK and H∩K in (1) we get,

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

On interchanging role of B and C, we get

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

Since $(B_0 \cap C)$ and $(B \cap C_0)$ are normal subgroup of $B \cap C$, therefore, $(B_0 \cap C)(B \cap C_0) = (B \cap C_0)(B_0 \cap C)$. Hence right hand side of (2) and (3) are equal and hence $\frac{B_0(B \cap C)}{B_0(B \cap C_0)} \cong \frac{C_0(C \cap B)}{C_0(C \cap B_0)}$.

Note. This theorem is also known as butterfly theorem.

1.3.3 **Theorem**. Any two subnormal series of a group have equivalent refinements. This result is known as **Scheier's theorem.**

Proof. Consider the subnormal series

$$G=G_0\supseteq G_1\supseteq\ldots\supseteq G_s=\{e\}, \qquad (1)$$

$$G=H_0\supseteq H_1\supseteq\ldots\supseteq H_t=\{e\} \qquad (2)$$

of a group G. Since G_{i+1} is normal in G_i and $(G_i\cap H_j)$ is a subgroup of G_i, therefore, $G_{i+1}(G_i\cap H_j)= (G_i\cap H_j)\ G_{i+1}$ i.e. $G_{i+1}(G_i\cap H_j)$ is a subgroup of G. Define,

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

Similarly define,

$$H_{k,r}=H_{k+1}(H_k\cap G_r);\ 0\leq k\leq t-1,\ 0\leq r\leq s.$$

As G_i is normal in G_i and H_{j+1} is normal in H_j, therefore, $(G_i\cap H_{j+1})$ is normal in $(G_i\cap H_j)$. Since G_{i+1} is normal in G_{i+1} , therefore, $G_{i+1}(G_i\cap H_{j+1})$ is normal in $G_{i+1}(G_i\cap H_j)$.

Now by use of (1) and (2) we get, $G_{i,\,0} = G_{i+1}(G_i\cap H_0) = G_{i+1}G_i = G_i$ and $G_{i,\,t} = G_{i+1}(G_i\cap H_t) = G_{i+1}G_s = G_{i+1}$.

Hence we have a series

$$G=\mathbf{G_0}=G_{0,0}\supseteq G_{0,1}=G_{0,2}\supseteq\ldots\supseteq G_{0,t}=\mathbf{G_1}=G_{1,0}\supseteq G_{1,1}=G_{1,2}\supseteq\ldots\supseteq G_{1,t}=\mathbf{G_2}=G_{2,0}\supseteq G_{2,1}=G_{2,2}\supseteq\ldots\supseteq G_{2,t}=\mathbf{G_3}=G_{3,0}\supseteq G_{3,1}=G_{3,2}\supseteq\ldots\supseteq G_{3,t}=\mathbf{G_4}=G_{4,0}\supseteq\ldots\supseteq\mathbf{G_{s-1}}=G_{s-1,0}\supseteq G_{s-1,2}\supseteq\ldots\supseteq G_{s-1,t}=\mathbf{G_s}. \qquad (3)$$

Since each G_i for $0\leq i\leq s$ occurs in subnormal series (3), Hence (3) is a refinement of subnormal series (1).

Similarly, series

$$H=\mathbf{H_0}=H_{0,0}\supseteq H_{0,1}=H_{0,2}\supseteq\ldots\supseteq H_{0,s}=\mathbf{H_1}=H_{1,0}\supseteq H_{1,1}=H_{1,2}\supseteq\ldots\supseteq H_{1,s}=\mathbf{H_2}=H_{2,0}\supseteq H_{2,1}=H_{2,2}\supseteq\ldots\supseteq H_{2,s}=\mathbf{H_3}=H_{3,0}\supseteq H_{3,1}=H_{3,2}\supseteq\ldots\supseteq H_{3,s}=\mathbf{H_4}=H_{4,0}\supseteq\ldots\supseteq\mathbf{H_{t-1}}=H_{t-1,0}\supseteq H_{t-1,2}\supseteq\ldots\supseteq H_{t-1,s}=\mathbf{H_t}. \qquad (4)$$

is a refinement of subnormal series (2). Clearly both the series in (3) and (4) have st+1 term.

Since each G_{i+1} is normal in G_i and H_{j+1} is normal in H_j, therefore, by Zassenhaus Lemma $\dfrac{G_{i+1}(G_i\cap H_j)}{G_{i+1}(G_i\cap H_{j+1})}\cong\dfrac{H_{j+1}(G_i\cap H_j)}{H_{j+1}(G_{i+1}\cap H_j)}$ i.e. $\dfrac{G_{i,j}}{G_{i,j+1}}\cong\dfrac{H_{j,i}}{H_{j,i+1}}$

Thus there is a one–one correspondence between factor groups of series (3) and (4) such that corresponding factor groups are isomorphic. Hence the two refinements are isomorphic.

1.4 COMPOSITION SERIES.

1.4.1 Definition (Composition series). A subnormal series

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_r=(e)$$

of group G is called composition series if for $1\leq i \leq r$, all the non trivial factor group $\frac{G_{i-1}}{G_i}$ are simple. The factor groups of this series are called composition factors.

Example. Let $G=\{1, -1, i, -i\}$; $i^2=-1$ be a group under multiplication, then $\{1,-1,i, -i\}\supseteq\{1, -1\}\supseteq\{1\}$ is the required composition series of G.

1.4.2 Lemma. Every finite group G has a composition series.

Proof. Let $o(G)=n$. We will prove the result by induction on n. If n=1. Then the result is trivial. Suppose that result holds for all groups whose order is less than n. If G is simple, then $G=G_0\supseteq G_1=\{e\}$ is the required composition series.

If G is not simple than G has a maximal normal subgroup H say. Definitely $o(H)<n$. Then, by induction hypothesis H has a composition series $H=H_0\supseteq H_1\supseteq H_2\supseteq \dots \supseteq H_s=(e)$ where $\frac{H_{j-1}}{H_j}$ is simple factor group. Now consider the series $G\supseteq H=H_0\supseteq H_1\supseteq \dots \supseteq H_s=(e)$. Since H is maximal normal subgroup, therefore, $\frac{G}{H}$ is simple factor group. Further each $\frac{H_{j-1}}{H_j}$ is simple factor group; therefore, above series is composition series of G. Hence the result follows.

1.4.3 Lemma. If G is a commutative group having a composition series then G is finite

Proof. First we study the nature of every simple abelian group H. Since H is abelian, therefore, each subgroup of it is normal. Since G is simple, therefore, it has no proper normal subgroup. But then G must be a group of prime order. Further we know that every group of prime order is cyclic also. Hence every simple abelian group H is cyclic group of prime order. We also know that every subgroup and factor group of an abelian group is also abelian. Now let

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_r=(e)$$

be a composition series of G. Then each non-trivial factor group $\frac{G_{i-1}}{G_i}$ is simple. As G is abelian, therefore, $\frac{G_{i-1}}{G_i}$ is abelian simple group. Hence by above discussion order of $\frac{G_{i-1}}{G_i}$ is prime i.e. $o(\frac{G_{i-1}}{G_i})=p_i$. Since $\frac{G_{r-1}}{G_r}\cong G_{r-1}$ and $o(\frac{G_{r-1}}{G_r})=p_r$, therefore, $o(G_{r-1})=p_r$.

Further $p_{r-1}= o(\frac{G_{r-2}}{G_{r-1}}) = \frac{o(G_{r-2})}{o(G_{r-1})} = \frac{o(G_{r-2})}{p_r}$, therefore, $o(G_{r-2})$ $=p_rp_{r-1}$. Continuing in this way, we get $o(G)=p_1\dots p_rp_{r-1}$. Hence G is finite.

1.4.4 **Theorem**. If group G has a composition series then prove that

(i) Every factor group has a composition series

(ii) Every normal subgroup of G has a composition series

Proof. Let

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_m=(e) \qquad (1)$$

be the composition series of group G. Then each factor group $\frac{G_i}{G_{i+1}}$ is simple for all i, $0 \le i \le m-1$.

(i) Let H be normal subgroup of G. Consider the quotient group $\frac{G}{H}$. Since $H\Delta G$ (H is normal in G), therefore, HG_i is a subgroup of G containing H and $H\Delta\ HG_i$. Further $H\Delta G$ and $G_{i+1}\ \Delta\ G_i$, therefore, $HG_{i+1}\ \Delta\ HG_i$ and hence $\frac{HG_{i+1}}{H}\Delta\frac{HG_i}{H}$.

Consider the series $\frac{G}{H}=\frac{HG_0}{H}\supseteq\frac{HG_1}{H}\supseteq\frac{HG_2}{H}\supseteq\dots\supseteq\frac{HG_m}{H}=H \qquad (2)$

By above discussion it is a subnormal series of $\frac{G}{H}$.

Define a mapping $f:\frac{G_i}{G_{i+1}}\to\frac{HG_i}{HG_{i+1}}$ by $f(aG_i)= aHG_{i+1}$ where $a\in G_i$.

This mapping is well defined since $aG_{i+1} = bG_{i+1} \Rightarrow ab^{-1} \in G_{i+1}$. Since $G_{i+1} \subseteq HG_{i+1}$, therefore, $ab^{-1} \in HG_{i+1}$. Hence $aHG_i = bHG_i$.

This mapping is homomorphism also since $f(abG_i) = abHG_i = aHG_i \, .bHG_i = f(aG_i)f(bG_i)$.

Since for $xHG_{i+1} \in \frac{HG_i}{HG_{i+1}}$ where $x \in HG_i = G_iH$, we have $x = gh$ for some $g \in G_i$ and $h \in H$. Then $xHG_{i+1} = ghHG_{i+1} = gHG_{i+1} = f(gG_{i+1})$. This mapping is onto also.

Now by fundamental theorem of homomorphism, $\frac{\frac{G_i}{G_{i+1}}}{\ker f} \cong \frac{HG_i}{HG_{i+1}}$. Further we know that Ker f is always a normal subgroup of $\frac{G_i}{G_{i+1}}$. But $\frac{G_i}{G_{i+1}}$ is simple, therefore, Ker $f = \frac{G_i}{G_{i+1}}$ or $\frac{G_{i+1}}{G_{i+1}} = G_{i+1}$ (identity of $\frac{G_i}{G_{i+1}}$). Then $\frac{\frac{G_i}{G_{i+1}}}{\ker f} = \frac{\frac{G_i}{G_{i+1}}}{\frac{G_i}{G_{i+1}}} = \frac{G_i}{G_{i+1}}$ or $\frac{\frac{G_i}{G_{i+1}}}{\ker f} = \frac{\frac{G_i}{G_{i+1}}}{\frac{G_{i+1}}{G_{i+1}}} = \frac{G_i}{G_{i+1}}$. Hence for every case, $\frac{G_i}{G_{i+1}} \cong \frac{HG_i}{HG_{i+1}}$ i.e. $\frac{HG_i}{HG_{i+1}}$ is simple. But $\frac{HG_i}{HG_{i+1}} \cong \frac{\frac{HG_i}{H}}{\frac{HG_{i+1}}{H}}$.

Therefore, $\frac{\frac{HG_i}{H}}{\frac{HG_{i+1}}{H}}$ is simple. Hence the series in (2) is a composition series for $\frac{G}{H}$.

(ii) H is subgroup of G, therefore, $H \cap G_i$ is subgroup of G. It is also subgroup of H. Since $G_{i+1} \vartriangle G_i$, therefore, $H \cap G_{i+1} \vartriangle H \cap G_i$. Let $H_i = H \cap G_i$. Then the series

$$H = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_m \supseteq \{e\} \qquad (3)$$

is a subnormal series for H.

Since $G_i \supseteq G_{i+1}$, therefore, $H_{i+1} = H \cap G_{i+1} = (H \cap (G_i \cap G_{i+1}) = (H \cap G_i) \cap G_{i+1} = H_i \cap G_{i+1}$. Since we know that if A and B are subgroup of G with B is normal

in G, then $\frac{AB}{B} \cong \frac{A}{A \cap B}$, therefore, for two subgroups H_i and G_{i+1} of G_i where G_{i+1} is normal in G, we have

$$\frac{H_i}{H_{i+1}} = \frac{H_i}{H_i \cap G_{i+1}} \cong \frac{H_i G_{i+1}}{G_{i+1}} \qquad (4)$$

Since $H_i = H \cap G_i$ and $G_{i+1} \Delta G_i$, therefore, $H_i G_{i+1}$ is a subgroup of G_i containing G_{i+1}. Since $H \Delta G$, therefore, $H \Delta G_i$. Hence $H_i = H \cap G_i \Delta G_i$. As $G_{i+1} \Delta G_i$, and $H_i \Delta G_i$, therefore, $H_i G_{i+1}$ is a normal subgroup of G_i. Hence $\frac{H_i G_{i+1}}{G_{i+1}}$ is a normal subgroup of $\frac{G_i}{G_{i+1}}$. But $\frac{G_i}{G_{i+1}}$ is simple, therefore, $\frac{H_i G_{i+1}}{G_{i+1}} = \frac{G_i}{G_{i+1}}$ or $\frac{H_i G_{i+1}}{G_{i+1}} = G_{i+1}$. Now $\frac{H_i G_{i+1}}{G_{i+1}} = G_{i+1} \Rightarrow H_i G_{i+1} = G_{i+1}$ and $\frac{H_i G_{i+1}}{G_{i+1}} = \frac{G_i}{G_{i+1}} \Rightarrow H_i G_{i+1} = G_i$. Hence either $\frac{H_i G_{i+1}}{G_{i+1}}$ is trivial group or non-trivial simple group.

But then by (4), $\frac{H_i}{H_{i+1}}$ is trivial or non-trivial simple group. Hence (3) is the composition series for H. It proves the result.

1.4.5 Theorem. (Jordan Theorem). Any two composition series of a finite group are equivalent.

Proof. Let $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_s = \{e\}$, (1)

$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_t = \{e\}$ (2)

be two composition series of a group G.

By definition of composition series it is clear that a composition series can not refined properly. Equivalently, if from refinement of a composition series if we omit repeated terms then we get the original composition series. By Scheier's Theorem, series in (1) and (2) have isomorphic refinement and hence by omitting the trivial factor group of the refinement we see that the original series are isomorphic and therefore, s=t.

Example. Let G be a cyclic group of order 18. Find composition series for G

Solution. Let G=<a>. Then order of *a* is 18. As G is abelian, therefore, every subgroup of G is cyclic. Consider $G_1=\langle a^2\rangle=\{e, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}\}$ $G_2=\langle a^6\rangle=\{e, a^6, a^{12}\}$, $G_3=\{e\}$. Consider the series:

$$G=G_0\supseteq G_1\supseteq G_2\supseteq G_3=\{e\}.$$

The orders of $\frac{G_0}{G_1}$, $\frac{G_1}{G_2}$, $\frac{G_2}{G_3}$ are 2, 3 and 3 respectively, which are prime numbers. Therefore, factor groups of above series are simple and hence it is a composition series for G.

Similarly, by taking, $G=H_0=\langle a\rangle$, $H_1=\langle a^3\rangle=\{e, a^3, a^6, a^9, a^{12}, a^{15}\}$, $H_2=\langle a^6\rangle=\{e, a^6, a^{12}\}$ and $H_3=\{e\}$, we get the factor groups $\frac{H_0}{H_1}$, $\frac{H_1}{H_2}$, $\frac{H_2}{H_3}$ are 3, 2 and 3 respectively. Hence series

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

is also a composition series for G. Further, it is easy to see that $\frac{H_0}{H_1}\cong\frac{G_1}{G_2}$, $\frac{H_1}{H_2}\cong\frac{G_0}{G_1}$ and $\frac{H_2}{H_3}\cong\frac{G_2}{G_3}$. Similarly we see that by taking $G=H_0=\langle a\rangle$, $H_1=\langle a^3\rangle$, $H_2=\langle a^9\rangle$ and $H_3=\{e\}$ gives us another composition series for G.

Example. Show that if G is a group of order p^n, p is prime number. Then G has a composition series such that all its composition factors are of order p.

Solution. Let $G=G_0\supseteq G_1\supseteq\ldots\supseteq G_s=\{e\}$ be the composition series for G. Since $o(G)=p^n$, therefore, order of every subgroup of G is some power of p. But then order of each composition factor $\frac{G_{i-1}}{G_i}$ is p^i, $i<n$. If $i>1$, then $\frac{G_{i-1}}{G_i}$ has a non trivial centre, contradicting that $\frac{G_{i-1}}{G_i}$ is simple. Hence k=1 i.e. each composition factor is of prime order. It proves the result.

1.5 COMMUTATOR SUBGROUP.

1.5.1 Definition (Commutator). Let G be a group. The commutator of the ordered pair of elements x, y in the group G is the element $x^{-1}y^{-1}x\,y$. It is denoted by

[x, y]. Similarly if H and K are two subgroups of G, then for $h \in H$ and $k \in K$, [h, k] is the commutator of ordered pair (h, k).

1.5.2 Commutator subgroup. Let G be a group. The subgroup G' of G generated by commutators of G is called the commutator subgroup of G i.e. $G' = \{[x, y] | x, y \in G\}$. It is also called the derived subgroup of G. Similarly $[H, K] = \langle [h, k] \rangle$ denotes the commutator subgroup of H and K.

Note. If $x \in [H, K]$, then $x = \prod_{i=1}^{n} [h_i, k_i]^{\in_i}$ where $h_i \in H$, $k_i \in K$ and $\in_i = \pm 1$.

Since $[h, k] = h^{-1}k^{-1}h\ k = (k^{-1}h^{-1}k\ h)^{-1} = [k, h]^{-1} \in [K, H]$ for all $h \in H$ and $k \in K$, therefore, $[H, K] \subseteq [K, H]$. Similarly $[K, H] \subseteq [H, K]$. Hence $[H, K] = [K, H]$.

We also define $[x, y, z] = [[x, y]\ z]$. In general $[x_1, x_2, \ldots, x_{n-1}, x_n] = [[x_1, x_2, \ldots, x_{n-1}]\ x_n] = [[[x_1, x_2, \ldots, x_{n-2}]\ x_{n-1}]\ x_n] = \ldots = [\ldots[x_1, x_2]\ldots\ x_{n-1}]\ x_n]$.

1.5.3 Theorem. Let G be a group and G' be its derived group then the following holds

(i) G' is normal in G.

(ii) G/G' is abelian

(iii) If H is normal in G, then G/H is abelian if and only if $G' \subseteq H$.

Proof. (i) Since $y^{-1}x\ y = xx^{-1}y^{-1}xy = x[x, y]\ \forall\ y \in G$ and $x \in G'$. Since x and $[x, y] \in G'$, therefore, $x[x, y] = y^{-1}x\ y \in G'$. Hence G' is normal in G.

(ii) Since $[x, y] = x^{-1}y^{-1}xy \in G'$ for all x and $y \in G$, therefore, $x^{-1}y^{-1}xyG' = G'$. Equivalently $xyG' = G'yx$. Hence $xG'yG' = yG'xG'$. As xG' and yG' are arbitrary element of G/G', therefore, G/G' is abelian.

(iii) As G/H is abelian

iff $xH\ yH = yH\ xH\ \forall\ xH$ and $yH \in G/H$

iff $x^{-1}y^{-1}xyH = H$

iff $[x, y] \in H$

iff $G' \subseteq H$.

Example. Let G be a group and x, y and z are arbitrary elements of G then

(i) $[xy, z]=[x, z]^y [y, z]$

(ii) $[x, yz]=[x, z][x, y]^z$

(iii) $[x,z^{-1},y]^z [z,y^{-1},x]^y [y,x^{-1},z]^x = e$ where $[x, z]^y = y^{-1}[x, z]y$.

Solution. (i) L.H.S = $[xy, z]= (xy)^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}x\ zz^{-1}yz$
$= y^{-1}x^{-1}\ z^{-1}xzyy^{-1}z^{-1}\ yz = y^{-1}[x, z]y[y, z]= [x,z]^y [y,z]$=R.H.S.

(ii) It is easy to show

(iii) Since $[x, z^{-1}, y]^z = z^{-1}[x, z^{-1}, y]z = z^{-1}[[x, z^{-1}], y]z$

$= z^{-1}[x, z^{-1}]^{-1}\ y^{-1}[x, z]yz$

$= z^{-1}(x^{-1}(\ z^{-1})^{-1}\ x\ z^{-1})^{-1}\ y^{-1}(x^{-1}(\ z^{-1})^{-1}\ x\ z^{-1})yz$

$= z^{-1}zx^{-1}\ z^{-1}x\ y^{-1}x^{-1}\ z\ x\ z^{-1}yz$

$= x^{-1}\ z^{-1}x\ y^{-1}x^{-1}\ z\ x\ z^{-1}yz$ (1)

Similarly $[y, x^{-1},z]^x = y^{-1}\ x^{-1}y\ z^{-1}y^{-1}\ x\ y\ x^{-1}zx$ (2)

and $[z, y^{-1},x]^y = z^{-1}\ y^{-1}z\ x^{-1}z^{-1}\ y\ z\ y^{-1}x\ y$ (3).

Hence by use of (1) , (2) and (3) we get that L.H.S is

$[x,z^{-1},y]^z [z,y^{-1},x]^y [y, x^{-1},z]^x$

$= x^{-1}\ z^{-1}x\ y^{-1}x^{-1}\ z\ x\ z^{-1}yz\ z^{-1}\ y^{-1}z\ x^{-1}z^{-1}\ y\ z\ \ y^{-1}x\ y\quad y^{-1}\ x^{-1}y\ z^{-1}y^{-1}\ x\ y\ x^{-1}zx$

=e =R.H.S.

1.5.4 Theorem. Prove that group G is abelian if and only if $G' =\{e\}$

Proof. Let G be an abelian group, then for x and y in G, $[x, y]= x^{-1}y^{-1}x\ y= x^{-1}x\ y^{-1}y=e$. Therefore, $G' =\{e\}$.

Conversely, suppose that $G' =\{e\}$, then for arbitrary x and y in G, $[x,y] \in G'$ i.e. $[x, y]=\{e\}$. Hence $x^{-1}y^{-1}x\ y =e$. But then xy=yx. Hence G is abelian.

1.5.5 Example. Find commutator subgroup of S_3; symmetric group of degree three.

Solution. Let $G= S_3,=\{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Then for x and y in G, $[x, y]= x^{-1}y^{-1}x\ y$. We know that every cyclic of odd(even) length is even(odd) permutation, inverse of an odd(even) permutation is always an odd(even) permutation and product of odd(even) permutation with odd(even)

permutation is always even permutation while product of odd(even) permutation with even(odd) permutation is always odd permutation. Therefore, what ever x and y may be [x, y] is always an even permutation. As S_3 is not an abelian group, therefore, $S_3' \neq \{e\}$. Hence $S_3' = A_3$, group of all even permutation.

1.5.6 Definition. Let G be a group. Define commutator subgroup $(G')'$ of G' as the group generated by [x, y] where x and y are in G'. It is second commutator subgroup of G denoted by $G^{(2)}$. Similarly, $G^{(k)}$, k^{th} commutator subgroup of G is generated by [x, y], x and y belongs to $G^{(k-1)}$.

Example. **(i)** Find all $G^{(k)}$ for $G=S_3$, symmetric group of degree three.

Solution. By Example 1.5.5, $(S_3)' = A_3$. Since A_3 is group of order 3, therefore, A_3 is abelian. Hence by Definition 1.5.6, $(S_3)^{(2)} = (A_3)' = \{e\}$ and hence $(S_3)^{(k)} = \{e\}\ \forall k \geq 2$.

(ii) If G={1, -1, i, -i, j, -j, k, -k}.Then G is group under the condition that $i^2=j^2=k^2=-1$, ij=k=-ji, jk=i=-kj, ki=j=-ik. The set of all commutators of G is {1, -1}.

1.6 MORE RESULTS ON COMMUTATOR SUBGROUPS.

1.6.1 Theorem. If H and K are normal subgroup of G then

(i) If $H \Delta G$ (H is normal in G) then $[H, K] \subseteq H$. Similarly if $K \Delta G$ then $[H, K] \subseteq K$

(ii) If both H and K are normal in G then $[H, K] \subseteq H \cap K$ and $[H, K] \Delta G$.

(iii) If $G = < H \cup K >$, then $[H, K] \Delta G$.

Proof. (i) Let $H \Delta G$ and let $[H, K] = <[h, k]>$, $h \in H$ and $k \in K$. Since H is normal in G, therefore, $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.

As $K \subseteq G$, therefore, $k^{-1}hk \in H$ for all $k \in K$ and $h \in H$. But then $[h, k] = h^{-1}k^{-1}hk \in H$. i.e. every generator of $[H, K]$ belongs to H. Hence $[H, K] \subseteq H$. Similarly we can show that if $K \Delta G$ then $[H, K] \subseteq K$.

(ii) By (i) it is easy to see that $[H, K] \subseteq H \cap K$. We have to show that $[H, K] \Delta G$. Let $g \in G$ and $u \in [H, K]$. Then $u = \prod_{i=1}^{r} [h_i, k_i]^{a_i}$, where, $h_i \in H$, $k_i \in K$ and $a_i = \pm 1$. Since

$$\begin{aligned}
[h, k]^g &= g^{-1}[h, k]g = g^{-1}h^{-1}k^{-1}hkg \\
&= g^{-1}h^{-1}gg^{-1}k^{-1}gg^{-1}hgg^{-1}kg \\
&= (g^{-1}hg)^{-1}(g^{-1}kg)^{-1}(g^{-1}hg)(g^{-1}kg) \\
&= (h^g)^{-1}(k^g)^{-1}g(h^g)(k^g) \\
&= [h^g, k^g].
\end{aligned}$$

As $H \Delta G$ and $K \Delta G$, therefore, $[h^g, k^g] = [h, k]^g \in [H, K]$. Further $[H, K]$ is a group, $[h, k]^{-g} \in [H, K]$ i.e

$$[h, k]^{ag} \in [H, K] \qquad (*)$$

Now $g^{-1}ug = u^g = (\prod_{i=1}^{r} [h_i, k_i]^{a_i})^g = \prod_{i=1}^{r} [h_i, k_i]^{a_i g} \in [H, K]$ (by use of (*)).

Hence $[H, K]$ is normal in G.

(iii) Since $G = \langle H \cup K \rangle$, therefore, $g \in G$ is of the form $u_1^{a_1} \ldots u_m^{a_m}$, $u_i \in H \cup K$ and $a_i = \pm 1$. Further $u_i^{a_i} \in H \cup K$, therefore, we can write $g = u_1 \ldots u_m$, $u_i \in H \cup K$.

Let $h, h_1 \in H$, $k \in K$. Then

$$\begin{aligned}
[h,k]^{h_1} &= h_1^{-1}[h,k]h_1 = h_1^{-1}h^{-1}k^{-1}hkh_1 \\
&= (hh_1)^{-1}k^{-1}h(h_1kk^{-1}h_1^{-1})kh_1 \\
&= (hh_1)^{-1}k^{-1}(hh_1)kk^{-1}h_1^{-1}kh_1 \\
&= [hh_1, k][k, h_1] \in [H, K] \quad (\Theta\ [H,K] = [K,H]).
\end{aligned}$$

Again if $h \in H$, $k, k_1 \in K$. Then

$$\begin{aligned}
[h,k]^{k_1} &= k_1^{-1}[h,k]k_1 = k_1^{-1}h^{-1}k^{-1}hkk_1 \\
&= k_1^{-1}h^{-1}k_1hh^{-1}k_1^{-1}k^{-1}k^{-1}hkk_1 \\
&= [k_1, h][h, kk_1] \in [H, K] \quad (\Theta\ [H,K] = [K,H]).
\end{aligned}$$

Thus for all $h, h_1 \in H$ and $k, k_1 \in K$,

$$[h,k]^{k_1} \text{ and } [h,k]^{h_1} \in [H, K]$$

and hence $[h,k]^{-k_1}$ and $[h,k]^{-h_1}$ also belongs to [H, K]. i.e. $[h,k]^{a_1 k_1}$ and $[h,k]^{a_1 h_1}$ belongs to [H, K].

Now $g \in G \Rightarrow g = u_1 u_2 \ldots u_m$, $u_i \in H \cup K$ and

$y \in [H, K] \Rightarrow y = \prod_{i=1}^{n} [h_i, k_i]^{a_i}$, where $h_i \in H$, $k_i \in K$, $n > 0$.

Now $g^{-1}yg = y^g = (\prod_{i=1}^{n} [h_i, k_i]^{a_i})^g = \prod_{i=1}^{n} [h_i, k_i]^{a_i g}$. Since $[h_i, k_i]^g = [h_i, k_i]^{u_1 \ldots u_m}$, $u_i \in H \cup K$, therefore, by above discussion, $[h_i, k_i]^g \in [H, K]$ which further implies that $[h_i, k_i]^{a_i g} \in [H, K]$. From this we get $y^g = (\prod_{i=1}^{n} [h_i, k_i]^{a_i})^g \in [H, K]$. Hence [H, K] is normal in G.

1.6.2 Theorem (P Hall Lemma). State and prove three subgroup Lemma of P Hall.

Statement. If A, B, C and M are subgroup of G, $M \Delta G$, $[B, C, A] \subseteq M$ and $[C, A, B] \subseteq M$ then $[A, B, C]] \subseteq M$.

Proof. Let $a \in A$, $b \in B$ and $c \in C$. Since $[a, b^{-1}, c]^b [b, c^{-1}, a]^c [c, a^{-1}, b]^a = e$, therefore, $[a, b^{-1}, c]^b = [b, c^{-1}, a]^{-c} [c, a^{-1}, b]^{-a}$. (1)

Now by our choice

$$[c, a^{-1}, b] = [[c, a^{-1}] b] \in [[C, A], B] = [C, A, B] \subseteq M.$$

As M is normal subgroup of G, therefore,

$$[c, a^{-1}, b] \in M \Rightarrow [c, a^{-1}, b]^{-1} \in M \Rightarrow [c, a^{-1}, b]^{-a} \in M^a = a^{-1} M a = M.$$

Similarly $[b, c^{-1}, a]^{-c} \in [B, C, A] \subseteq M$. Now by (1), $[a, b^{-1}, c]^b \in M$. But then $([a, b^{-1}, c]^b)^{b^{-1}} \in M^{b^{-1}} = bMb^{-1} = M$ i.e.

$$[a, b^{-1}, c] \in M \ \forall \ a \in A, b \in B, c \in C \quad (2).$$

Using b in place of b^{-1} we get

$$[a, b, c] = [[a, b], c] \in M \ \forall \ a \in A, b \in B, c \in C \quad (3)$$

Similarly $[b, a^{-1}, c]^a [a, c^{-1}, b]^c [c, b^{-1}, a]^b = e$

$$\Rightarrow [b, a, c] \in M \ \forall \ a \in A, b \in B, c \in C \quad (4)$$

As $[b, a, c] = [[b, a], c] \in M$ and $[a, b]^{-1} = [b, a]$, therefore, $[[a, b]^{-1}, c] \in M$. Now $[[a, b], c] \in M$ (by(3)) and $[[a, b]^{-1}, c] \in M$ implies that

$$[[a, b]^{-\varepsilon}, c] \in M \text{ , where } \varepsilon = \pm 1 \qquad (5)$$

Let $z \in [A, B, C] = [[A, B], C]$. Then

$$z = \left(\prod_{i=1}^{n} [x_i, c_i]^{\varepsilon_i}\right), \; x_i \in [A, B], \; c_i \in C \text{ and } \varepsilon_i = \pm 1 \qquad (6)$$

In particular, put $x_i = x$, $c_i = c$. Since $x \in [A, B]$, therefore, $x = \left(\prod_{j=1}^{n} [a_j, b_j]^{\eta_j}\right)$, $a_j \in A$, $b_j \in B$, $\eta_j = \pm 1$. Since $[x, c] = \left[\left(\prod_{j=1}^{n} [a_j, b_j]^{\eta_j}\right), c\right]$ or $\prod_{j=1}^{n} [[a_j, b_j]^{\eta_j}, c]^{h_j}$, $h_j \in G$ and by (5) $[[a_j, b_j]^{\eta_j}, c] \in M$, therefore, $[x, c] \in M$ i.e. $[x_i, c_i] \in M$. But then $[x_i, c_i]^{-1} \in M$ i.e. $[x_i, c_i]^{\varepsilon_i}$

From (6), $z = \left(\prod_{i=1}^{n} [x_i, c_i]^{\varepsilon_i}\right) \in M$ i.e. if $z \in [A, B, C] \Rightarrow z \in M$.

Hence $[A, B, C] \subseteq M$.

Example. Show that $[x, z, y^x]\,[y, x, z^y]\,[z, y, x^z] = e$

Solution. Since $[x, z, y^x] = [[x, z], y^x] = [x, z]^{-1} (y^x)^{-1} [x, z] (y^x)$

$$= (x^{-1}z^{-1}xz)^{-1} (x^{-1}yx)^{-1} (x^{-1}z^{-1}xz) (x^{-1}yx)$$
$$= z^{-1}x^{-1} z\, x\, x^{-1}y^{-1}x\, x^{-1}z^{-1}xz\, x^{-1}yx$$
$$= z^{-1}x^{-1} z\, y^{-1}z^{-1}xz\, x^{-1}yx \qquad (1),$$

$$[y, x, z^y] = [[y, x], z^y] = [y, x]^{-1} (z^y)^{-1} [y, x] (z^y)$$
$$= (y^{-1}x^{-1}yx)^{-1} (y^{-1}zy)^{-1} (y^{-1}x^{-1}yx)(y^{-1}zy)$$
$$= x^{-1}y^{-1}\, x\, y\, y^{-1}z^{-1}y\, y^{-1}x^{-1}\, y\, x\, y^{-1}z\, y$$
$$= x^{-1}y^{-1}\, x\, z^{-1}x^{-1}\, y\, x\, y^{-1}z\, y \qquad (2)$$

$$[z, y, x^z] = [[z, y], x^z] = [z, y]^{-1} (x^z)^{-1} [z, y] (x^z)$$
$$= (z^{-1}y^{-1}z\, y)^{-1} (z^{-1}x\, z)^{-1} (z^{-1}y^{-1}z\, y)(z^{-1}x\, z)$$
$$= y^{-1}z^{-1}y\, z\, z^{-1}x^{-1}z\, z^{-1}\, y^{-1}z\, y\, z^{-1}x\, z$$
$$= y^{-1}z^{-1}y\, x^{-1}\, y^{-1}z\, y\, z^{-1}x\, z \qquad (3)$$

Now by (1), (2) and (3), we get L.H.S

$$[x, z, y^x]\,[y, x, z^y]\,[z, y, x^z]$$
$$= z^{-1}x^{-1}\, z\, y^{-1}z^{-1}xz\, x^{-1}yx\, x^{-1}y^{-1}\, x\, z^{-1}x^{-1}\, y\, x\, y^{-1}z\, y\, y^{-1}z^{-1}y\, x^{-1}\, y^{-1}z\, y\, z^{-1}x\, z$$
$$= e = \text{R.H.S.}$$

1.7 INVARIANT SERIES AND CHIEF SERIES.

1.7.1 Definition (Invariant series) A series

$$G=G_0\supseteq G_1\supseteq \dots \supseteq G_r\supseteq \{e\}.$$

of subgroups of G where each $G_i \Delta G$, $1\leq i \leq r$, is called invariant series.

Example. Show that every central series is invariant but converse may not be true.

Solution. By definition of central series, every $G_i \Delta G$, therefore, every central series is invariant. For converse part take $G=S_3$, symmetric group of degree 3. Consider the series

$$S_3=G_0\supseteq G_1=\{e\}.$$

Clearly it is invariant series because $G_1 \Delta G$. But $\frac{G_0}{G_1}=S_3$. As for (1 2) and (1 2 3) $\in S_3$, (1 2)(1 2 3)=(1 3)$\neq$ (2 3)= (1 2 3)(12) i.e. (1 2) does not commute with all the element of S_3. Therefore, $Z(\frac{G}{G_1})=Z(S_3)\neq S_3$. Hence $\frac{G_0}{G_1}\not\subset Z(\frac{G}{G_1})$.

1.7.2 Definition.(Chief series). A chief series of a group G is an invariant series

$$G=G_0\supseteq G_1\supseteq \dots \supseteq G_r\supseteq \{e\}$$

of G such that $G_{i-1}\supset G_i$ and if $G_{i-1}\supseteq N\supseteq G_i$ with $N \Delta G$, then either $G_{i-1}=N$ or $N=G_i$. The factor groups $\frac{G_{i-1}}{G_i}$ are called the chief factors.

1.7.3 Note. Chief series is an invariant series that can not be defined in a non trivial manner. The chief factors need not be a simple group. For example take A_4 and consider the series

$$A_4=G_0\supseteq G_1=V_4=\{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}=G_1\supseteq\{e\}.$$

Then it is easy to see that each $G_i \Delta G$ and there is no normal subgroup of G between G_{i-1} and G_i. But the chief factor $\frac{G_1}{G_2}=\frac{V_4}{\{e\}}=V_4$ which is not simple because {I, (1 2)(3 4)} is normal in V_4.

1.7.4 **Theorem**. Any two invariant series for a given group have isomorphic refinements.

Proof. Let the group G has two invariant series

$$G=G_0\supseteq G_1\supseteq\ldots\supseteq G_s=\{e\}, \qquad (1)$$

$$G=H_0\supseteq H_1\supseteq\ldots\supseteq H_t=\{e\} \qquad (2)$$

of a group G. Since G_{i+1} is normal in G and $(G_i\cap H_j)$ is a subgroup of G, therefore, $G_{i+1}(G_i\cap H_j)=(G_i\cap H_j)\ G_{i+1}$ i.e. $G_{i+1}(G_i\cap H_j)$ is a subgroup of G. Define,

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

Similarly define,

$$H_{k,r}=H_{k+1}(H_k\cap G_r);\ 0\le k\le t-1,\ 0\le r\le s.$$

Since $H_{j+1}\subseteq H_j$, therefore, $(G_i\cap H_{j+1})\subseteq(G_i\cap H_j)$. But then $G_{i+1}(G_i\cap H_{j+1})\subseteq G_{i+1}(G_i\cap H_j)$ i.e. $G_{i,j+1}\subseteq G_{i,j}$. G_i is normal in G and H_j is normal in G, therefore, $(G_i\cap H_j)$ is normal in G and Hence $G_{i,j}\ \Delta\ G$. Now by use of (1) and (2) we get,

$$G_{i,0}=G_{i+1}(G_i\cap H_0)=G_{i+1}G_i=G_i \text{ and } G_{i,t}=G_{i+1}(G_i\cap H_t)=G_{i+1}G_s=G_{i+1}$$

Consider the series

$$G=\mathbf{G_0}=G_{0,0}\supseteq G_{0,1}=G_{0,2}\supseteq\ldots\supseteq G_{0,t}=\mathbf{G_1}=G_{1,0}\supseteq G_{1,1}=G_{1,2}\supseteq\ldots\supseteq G_{1,t}=\mathbf{G_2}=G_{2,0}\supseteq G_{2,1}=G_{2,2}\supseteq\ldots\supseteq G_{2,t}=\mathbf{G_3}=G_{3,0}\supseteq G_{3,1}=G_{3,2}\supseteq\ldots\supseteq G_{3,t}=\mathbf{G_4}=G_{4,0}\supseteq\ldots\supseteq\mathbf{G_{s-1}}=G_{s-1,0}\supseteq G_{s-1,2}\supseteq\ldots\supseteq G_{s-1,t}=\mathbf{G_s}. \qquad (3)$$

and

$$H=\mathbf{H_0}=H_{0,0}\supseteq H_{0,1}=H_{0,2}\supseteq\ldots\supseteq H_{0,s}=\mathbf{H_1}=H_{1,0}\supseteq H_{1,1}=H_{1,2}\supseteq\ldots\supseteq H_{1,s}=\mathbf{H_2}=H_{2,0}\supseteq H_{2,1}=H_{2,2}\supseteq\ldots\supseteq H_{2,s}=\mathbf{H_3}=H_{3,0}\supseteq H_{3,1}=H_{3,2}\supseteq\ldots\supseteq H_{3,s}=\mathbf{H_4}=H_{4,0}\supseteq\ldots\supseteq\mathbf{H_{t-1}}=H_{t-1,0}\supseteq H_{t-1,2}\supseteq\ldots\supseteq H_{t-1,s}=\mathbf{H_t}. \qquad (4)$$

for G. By above discussion the series (3) and (4) are invariant series and are refinements of series (1) and (2). Clearly both the series in (3) and (4) have st+1 terms.

As $G_{i+1}\Delta G$, therefore, $G_{i+1}\ \Delta\ G_i$. Similarly $H_{j+1}\ \Delta\ H_j$. Hence by Zassenhaus Lemma $\dfrac{G_{i+1}(G_i\cap H_j)}{G_{i+1}(G_i\cap H_{j+1})}\cong\dfrac{H_{j+1}(G_i\cap H_j)}{H_{j+1}(G_{i+1}\cap H_j)}$ i.e. $\dfrac{G_{i,j}}{G_{i,j+1}}\cong\dfrac{H_{j,i}}{H_{j,i+1}}$.

Thus there is a one–one correspondence between factor groups of series (3)

and (4) such that corresponding factor groups are isomorphic. Hence the two refinements are isomorphic.

1.7.5 Theorem. In a group with a chief series every chief series is isomorphic to given series.

Proof. As by the definition of chief series every chief series is isomorphic to its refinement. Let $G=G_0\supseteq G_1\supseteq\ldots\supseteq G_s=\{e\}$, (1)

and $G=H_0\supseteq H_1\supseteq\ldots\supseteq H_t=\{e\}$ (2)

are two chief series of group G.

Since G_{i+1} is normal in G_i and $(G_i\cap H_j)$ is a subgroup of G_i, therefore, $G_{i+1}(G_i\cap H_j)= (G_i\cap H_j)\, G_{i+1}$ i.e. $G_{i+1}(G_i\cap H_j)$ is a subgroup of G. Define,

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

Similarly define,

$$H_{k,r}=H_{k+1}(H_k\cap G_r);\ 0\le k\le t-1,\ 0 \le r \le s.$$

As G_i is normal in G_i and H_{j+1} is normal in H_j, therefore, $(G_i\cap H_{j+1})$ is normal in $(G_i\cap H_j)$. Since G_{i+1} is normal in G_{i+1} , therefore, $G_{i+1}(G_i\cap H_{j+1})$ is normal in $G_{i+1}(G_i\cap H_j)$. Now by use of (1) and (2) we get,

$G_{i,0} = G_{i+1}(G_i\cap H_0) = G_{i+1}G_i = G_i$ and $G_{i,t} = G_{i+1}(G_i\cap H_t) = G_{i+1}G_s = G_{i+1}$

Hence we have a series

$$G= \mathbf{G_0} = G_{0,0} \supseteq G_{0,1} = G_{0,2} \supseteq \ldots \supseteq G_{0,t} =\mathbf{G_1}= G_{1,0} \supseteq G_{1,1} = G_{1,2} \supseteq \ldots \supseteq G_{1,t} =\mathbf{G_2}= G_{2,0} \supseteq G_{2,1} = G_{2,2} \supseteq \ldots \supseteq G_{2,t} =\mathbf{G_3}= G_{3,0} \supseteq G_{3,1} = G_{3,2} \supseteq \ldots \supseteq G_{3,t} =\mathbf{G_4}= G_{4,0} \supseteq \ldots \supseteq \mathbf{G_{s-1}} = G_{s-1,0} \supseteq G_{s-1,2} \supseteq \ldots \supseteq G_{s-1,t} =\mathbf{G_s}. \quad (3)$$

Since each G_i for $0\le i \le s$ occurs in subnormal series (3), Hence (3) is a refinement of subnormal series (1).

Similarly, series

$$H= \mathbf{H_0} = H_{0,0} \supseteq H_{0,1} = H_{0,2} \supseteq \ldots \supseteq H_{0,s} =\mathbf{H_1}= H_{1,0} \supseteq H_{1,1} = H_{1,2} \supseteq \ldots \supseteq H_{1,s} =\mathbf{H_2}= H_{2,0} \supseteq H_{2,1} = H_{2,2} \supseteq \ldots \supseteq H_{2,s} =\mathbf{H_3}= H_{3,0} \supseteq H_{3,1} = H_{3,2} \supseteq \ldots \supseteq H_{3,s} =\mathbf{H_4}= H_{4,0} \supseteq \ldots \supseteq \mathbf{H_{t-1}} = H_{t-1,0} \supseteq H_{t-1,2} \supseteq \ldots \supseteq H_{t-1,s} =\mathbf{H_t}. \quad (4)$$

is a refinement of subnormal series(2). Clearly both the series in (3) and (4) have (st+1) terms. But then by Zassenhaus Lemma series (3) and (4) are isomorphic. Since by definition of chief series, series (1) is isomorphic to

series (3) and series (2) is isomorphic to series (4). Hence series (1) and (2) isomorphic. It proves the result.

1.7.6 Definition. (Derived series). Let G be a group. Define $\delta_0(G)=G$ and $\delta_i(G)=\delta(\delta_{i-1}(G)$ for each $i\geq 1$. Then $\delta_1(G)=\delta(G)$. Then the series

$$G=\delta_0(G)\supseteq \delta_1(G)\supseteq \ldots \supseteq \delta_r(G)=\{e\}$$

is called derived series for G.

1.8 KEY WORDS

Normal series, subnormal series, Zassenhaus lemma, Jordan Holder theorm, Commutators etc.

1.9 SUMMARY. This chapter contains subnormal and normal series, refinements, Zassenhaus lemma, Schreier's refinement theorem, Jordan Holder theorem, composition series, derived series, commutator subgroups and their properties, Three subgroup lemma of P. Hall, Chief series, derived series and related theorems.

1.10 SELF ASSESMENT QUESTIONS.

(1) Write all the composition series for octic group.

(2) Find composition series for Klein four group.

(3) Find all the composition series Z/<30>. Verify that they are equivalent.

(4) If a, b are elements of a group for which $a^3=(ab)^3=(ab^{-1})^3=e$ then $[a, b, b]=e$.

(5) If x, y are arbitrary elements in a group of exponent 3 then $[x, y, y] =1$.

1.11 SUGGESTED READING.

(1) **The theory of groups**; IAN D. MACDONALD, Oxford university press 1968.

(2) **Basic Abstract Algebra**; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.

MAL-511: M. Sc. Mathematics (Algebra)

Lesson No. 2 **Written by Dr. Pankaj Kumar**

Lesson: Central series and Field extensions-I **Vetted by Dr. Nawneet Hooda**

STRUCTURE.

2.0 OBJECTIVE. Objective of this chapter is to study some more properties of groups by studying their factor group. Prime fields and finite field extensions are also studied.

2.1 INTRODUCTION. In first Chapter, we have study some series. In this chapter, we study central series, Nilpotent groups, Solvable groups. Solvable groups have their application in the problem that 'whether general polynomial of degree n is solvable by radicals or not'. Prime fields and finite field extensions are also studied.

In Section 2.2, we study central, upper and lower central series of a group G. It is shown that upper and lower central series has same length and is equal to the least length of any central series.

In Section 2.3, we study Nilpotent groups and show that every factor group and subgroup of Nilpotent group is again Nilpotent. We also see every Sylow subgroup of a nilpotent group is normal and direct product of Nilpotent groups is again Nilpotent.

In Section 2.4, we study solvable groups and their properties. Next section contains some definitions and finite field extensions are studied in Section 2.6. In the last Section, we study about prime fields and see that prime fields are unique in the sense that every prime field of characteristic zero is isomorphic to field of rational numbers and the fields with characteristic p are isomorphic to $Z_p=Z/<p>$, p is prime number.

2.2 CENTRAL SERIES

2.2.1 Definition (Central series). Let G be a group. Then normal series

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_n=(e)$$

is central series for G if $\frac{G_i}{G_{i+1}} \subseteq Z(\frac{G}{G_{i+1}})$ $\forall$ i $\geq$ 0.(i.e. all the factor groups $\frac{G_i}{G_{i+1}}$ are central subgroup of $\frac{G}{G_{i+1}}$).

Example. If $G(\neq\{e\})$ is abelian group. Then $G=G_0 \supseteq G_1=\{e\}$. Then G_1 is normal in G. Further $\frac{G_0}{G_1}=G$. Since G is abelian, therefore, $Z(\frac{G}{G_1})=Z(G)=G$. Hence $\frac{G_0}{G_1}\subseteq Z(\frac{G}{G_1})$. It shows that G has a central series.

2.2.2 Theorem. Prove that the series $G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_n=(e)$ is a central series iff $[G, G_i]\subseteq G_{i+1}$.

Proof. Let

$$G=G_0\supseteq G_1\supseteq G_2\supseteq \dots \supseteq G_n=(e) \qquad (1)$$

be given series of group G.

First we assume that it is a central series of G i.e. $G_i \Delta G$ and $\frac{G_i}{G_{i+1}}\subseteq Z(\frac{G}{G_{i+1}})$. Let x and y are arbitrary elements of G and G_i respectively. Then xG_{i+1} and yG_{i+1} are arbitrary elements of $\frac{G}{G_{i+1}}$ and $\frac{G_i}{G_{i+1}}$ respectively. Since $\frac{G_i}{G_{i+1}}\subseteq Z(\frac{G}{G_{i+1}})$, therefore, $xG_{i+1}\, yG_{i+1}= yG_{i+1}\, xG_{i+1}$ i.e. $xyG_{i+1}= yxG_{i+1}$

But then $x^{-1}y^{-1}xyG_{i+1}= G_{i+1}$ i.e. $[x, y]\in G_{i+1}$. Hence the subgroup $<[x, y]> =[G, G_i]\subseteq G_{i+1}$.

Conversely, suppose that $[G, G_i]\subseteq G_{i+1}$. By (1), $G_{i+1} \subseteq G_i$, therefore, $[G, G_i] \subseteq G_i$. Let x and y are arbitrary elements of G and G_i, then $x^{-1}yx=yy^{-1}x^{-1}yx = y[x, y]^{-1}\in G_i$ (because y and $[x, y]^{-1}$ both are in G_i). Hence series (1) is normal series. Since $[G, G_i]\subseteq G_{i+1}$, therefore, for $x\in G$ and $y\in G_{i+1}$ we have $[x, y]\in G_{i+1}$. Hence $x^{-1}y^{-1}xyG_{i+1}= G_{i+1}$ i.e. $xG_{i+1}\ yG_{i+1}= yG_{i+1}\ xG_{i+1}$. Since $xG_{i+1}\ yG_{i+1}= yG_{i+1}\ xG_{i+1}$ holds for all $x\in G$ and $y\in G_{i+1}$, therefore, $yG_{i+1} \in Z(\frac{G}{G_{i+1}})$.

Hence $\frac{G_i}{G_{i+1}} \subseteq Z(\frac{G}{G_{i+1}})$ and the result follows.

2.2.3 Definition (Upper central series). Let $Z_0(G)=\{e\}$ and let $Z_i(G)$ be a subgroup of G for which $\frac{Z_i(G)}{Z_{i-1}(G)} = Z(\frac{G}{Z_{i-1}(G)})$ for each $i\geq 1$. If $Z_s(G)=G$ for some positive integer s then the series

$$\{e\}= Z_0(G)\subseteq Z_1(G)\subseteq\ldots\subseteq Z_s(G)=G$$

is called upper central series.

2.2.4 Example. Show that every upper central series is also a central series.

Solution. Consider the upper central series $\{e\}= Z_0(G)\subseteq Z_1(G)\subseteq\ldots\subseteq Z_s(G)=G$, $\frac{Z_i(G)}{Z_{i-1}(G)} = Z(\frac{(G)}{Z_{i-1}(G)})$ for each $i\geq 1$. By definition, $\frac{Z_i(G)}{Z_{i-1}(G)}$ is a central subgroup, therefore, it is normal in $\frac{(G)}{Z_{i-1}(G)}$ i.e. $g^{-1}Z_i(G)\ g_i\ Z_i(G)\ gZ_i(G)= g^{-1}g_igZ_i(G)\in \frac{Z_i(G)}{Z_{i-1}(G)}\ \forall\ g_i\in Z_i(G)$ and $g\in G$. Hence $g^{-1}g_ig\in Z_i(G)\ \forall\ g_i\in Z_i(G)$ and $g\in G$ and hence $Z_i(G)$ is normal in G.

Further $gZ_{i-1}(G)g_i\ Z_{i-1}(G)= g_i\ Z_{i-1}\ (G)\ gZ_{i-1}(G)\Rightarrow gg_i\ Z_{i-1}(G)= g_igZ_{i-1}(G) \Rightarrow g^{-1}g_i^{-1}gg_i\ Z_{i-1}(G)= Z_{i-1}(G) \Rightarrow [g, g_i]\in Z_{i-1}(G)$. Hence $<[g, g_i]>=[G, Z_i(G)]\subseteq Z_{i-1}$. It proves the result that every upper central series is a central series for G.

2.2.5 Definition.(Lower central series). If we define $\gamma_1(G)=G$ and $\gamma_i(G)=[\gamma_{i-1}, G]$, then the series

$$G=\gamma_1(G)\supseteq \gamma_2(G)\supseteq\dots \supseteq\gamma_{r+1}(G)=\{e\}$$

is called lower central series.

Since we know that $G =\gamma_1(G) \triangle G$. If we suppose that $\gamma_{i-1}(G)\Delta G$, then for $x=[g_{i-1}, g]\in\gamma_i(G)$; $g \in G$ and $g_{i-1}\in\gamma_{i-1}(G)$. Now for $g^*\in G$

$(g^*)^{-1}[g_{i-1}, g]g^* = [g_{i-1}, g]^{g^*}=[g_{i-1}{}^{g^*}, g^{g^*}]$. But by induction $\gamma_{i-1}(G)\Delta G$, therefore $(g^*)^{-1}[g_{i-1}, g]g^*\in[\gamma_{i-1}(G), G]= \gamma_i(G)$ i.e. $\gamma_i(G)\Delta G$ for each i. Hence above series is a normal series.

Further $[\gamma_{i-1}(G), G]= \gamma_i(G)\Rightarrow [\gamma_{i-1}(G), G]\subseteq \gamma_i(G)$. Hence it is central series for G. Now we can say that every lower central series is also a central series.

2.2.6 Theorem. If G has a central series $G=G_0\supseteq G_1\supseteq G_2\supseteq\dots G_r=(e)$ then $G_{r-i}\subseteq Z_i(G)$ and $G_i\supseteq\gamma_{i+1}(G)$ for $0\leq i\leq r$.

Proof. We will prove the result by induction on i. When i=0, then $G_r=\{e\}$, $G_0=G$, $\gamma_1(G)= G$ and $Z_0(G)=\{e\}$. Hence for this case $G_{r-i}\subseteq Z_i(G)$ and $G_i\supseteq\gamma_{i+1}(G)$ holds.

Let us suppose that result hold for all $i<r$ i.e. $G_{r-i+1}\subseteq Z_{i-1}(G)$ and $G_{i-1}\supseteq\gamma_i(G)$.

Take an element $x\in G_{r-i}$. We will show that x lies in $Z_i(G)$. Let $y \in G$. Then $[x, y] \in[G_{r-i}, G]= G_{r-i+1}$. As by induction hypothesis $G_{r-i+1} \subseteq Z_{i-1}(G)$, therefore, $[x, y] \in Z_{i-1}(G)$. Then $[x, y]Z_{i-1}(G)= Z_{i-1}(G)$. Equivalently, $x^{-1}y^{-1}xyZ_{i-1}(G)=Z_{i-1}(G)$ or $xZ_{i-1}(G)yZ_{i-1}(G)=yZ_{i-1}(G)\ xZ_{i-1}(G)$. It means that the elements $xZ_{i-1}(G)$ and $yZ_{i-1}(G)$ of the group $\frac{(G)}{Z_{i-1}(G)}$ commute. But y was arbitrary element of G, which shows that $yZ_{i-1}(G)$ is arbitrary in $\frac{(G)}{Z_{i-1}(G)}$ and hence $xZ_{i-1}(G)$ is in the centre of $\frac{(G)}{Z_{i-1}(G)}$. Now the centre of $\frac{(G)}{Z_{i-1}(G)}$ is $\frac{Z_i(G)}{Z_{i-1}(G)}$, by definition of upper central series. It then follow that $x\in Z_i(G)$. Hence $G_{r-i}\subseteq Z_i(G)$.

For second case by induction assumption $G_{i-1} \supseteq \gamma_i(G)$. Then $\gamma_{i+1}(G) = [\gamma_i(G), G] \subseteq [G_{i-1}, G]$. But by definition of central series $[G_{i-1}, G] \subseteq G_i$. Hence $\gamma_{i+1}(G) \subseteq G_i$.

2.2.7 Corollary. If G is nilpotent group then its upper and lower central series have the same length, and this is the least length for any central series.

Proof. Let G be a nilpotent group and

$$G=G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_r=(e)$$

be its central series of least length r. Further suppose that

$$\{e\}= Z_0(G) \subseteq Z_1(G) \subseteq \dots \subseteq Z_s(G)=G$$

be its upper central series and

$$G=\gamma_1(G) \supseteq \gamma_2(G) \supseteq \dots \supseteq \gamma_{t+1}(G)=\{e\}$$

be its lower central series.

Since $G_{r-i} \subseteq Z_i(G)$ and $G_i \supseteq \gamma_{i+1}(G)$ for $0 \leq i \leq r$. For $i=r$, $G_r \supseteq \gamma_{r+1}(G)$. But then $\gamma_{r+1}(G)=\{e\}$. This implies that $t+1 \leq r+1$. Since every lower central series is again a central series, therefore, if $t+1 < r+1$, then we get a central series of length lower then r, a contradiction. Hence $t+1= r+1$. Now we can say that length of lower central series is equal to length of central series of least length.

Further for $i = r$, $G_0 \subseteq Z_r(G) \Rightarrow Z_r(G)=G$. But then $s \leq r$. Now if $s < r$, then we get a central series (which is upper central series) of length less then r, the least length of central series. Hence $s = r$. Now above discussion, proves the result.

2.3 NILPOTENT GROUPS

2.3.1 Definition (Nilpotent group). A group G is called nilpotent group of class r if it has a central series of length r. i.e. if $G=G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_r=(e)$ is a central series of G.

Example. Every abelian group is nilpotent group of class 1. In fact a group is abelian if it is nilpotent group of class 1.

2.3.2 Theorem. Prove that finite p-group is nilpotent or every group of order p^n is nilpotent, p is prime number.

Proof. Since G is a finite p-group, therefore $o(G)=p^n$ for some $n\geq 1$. We will prove the result by applying induction on n. If n=1, then o(G)=p. But every group of prime order is abelian and hence is nilpotent of class 1. Therefore, result holds for n=1. Suppose result holds for all group of order p^m , m<n. Let $o(G)=p^n$. As p is prime which divides order of G, therefore, $o(Z(G))= p^t$, $1\leq t \leq n$. As Z(G) is normal in G, the subgroup $\frac{G}{Z(G)}$ has order p^{n-t} which is less than order of G. Then by induction hypothesis $\frac{G}{Z(G)}$ is nilpotent of class at most n-t. Let $\frac{G}{Z(G)}=\frac{G_0}{Z(G)}\supseteq \frac{G_1}{Z(G)}\supseteq \frac{G_2}{Z(G)}\supseteq \ldots\supseteq \frac{G_{n-t}}{Z(G)}=Z(G)$ where $\frac{G_i}{Z(G)}\Delta\frac{G}{Z(G)}$ and $[\frac{G_i}{Z(G)}, \frac{G}{Z(G)}]\subseteq \frac{G_{i+1}}{Z(G)}$ for all $0\leq i \leq n-t-1$, be the central series for $\frac{G}{Z(G)}$. Now consider the series

$$G \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{n-t}=Z(G) \supseteq G_{n-t+1}=\{e\}.$$

Since we know that $\frac{K}{H}\Delta\frac{G}{H}$ iff $K\Delta G$ containing H, therefore, $\frac{G_i}{Z(G)}\Delta\frac{G}{Z(G)}$ implies that each $G_i \Delta G$, $0\leq i \leq n-t-1$. G_{n-t} is also normal in G (because centre of a group is always normal in G). Hence it is a normal series of G. As $[\frac{G_i}{Z(G)}, \frac{G}{Z(G)}]\subseteq \frac{G_{i+1}}{Z(G)}$, therefore, for all $x\in G_i$ and $y\in G$, $[x, y]Z(G)\in \frac{G_i}{Z(G)}$ (show it). Hence $[x, y] \in G_{i+1}$ i.e. $[G_i, G]\in G_{i+1}$, $0 \leq i\leq n-t-1$.

Further for i=n-t, $x\in Z(G)$ and $y\in G$, $[x, y]=\{e\}$. Hence $\{e\}=[G_{n-t}, G] \subseteq G_{n-t+1}$. Therefore, it is required central series for G.

2.3.3 Theorem. Let G be a nilpotent group of r, then

(i) each factor group is nilpotent of class ≤ r,

(ii) each subgroup is also nilpotent of class ≤ r.

Proof. It is given that G is nilpotent of class r, therefore, G has a central series

$$G=G_0\supseteq G_1\supseteq \ldots \supseteq G_r\supseteq \{e\}.$$

where each $G_i \Delta G$ and $[G_{i-1}, G] \subseteq G_i$, $1 \leq i \leq r$. Let H be a subgroup of G, therefore, $H_i = H \cap G_i$ is subgroup of G. It is also subgroup of H. Since $H \Delta G$ and $G_i \Delta G$, therefore, $H \cap G_i \Delta H \cap G$. Then the series

$$H = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_r \supseteq \{e\} \qquad (1)$$

is a normal series for H. Now

$$[H_{i-1}, H] = [H \cap G_{i-1}, H] \subseteq [G_{i-1}, G] \subseteq G_i \text{ and}$$

$$[H_{i-1}, H] = [H \cap G_{i-1}, H] \subseteq [H, H] \subseteq H.$$

Hence $[H_{i-1}, H] \subseteq G_i \cap H = H_i$. Hence (*) is central series for H. It proves the result.

(ii) Let $H \Delta G$. Consider the factor group $\frac{G}{H}$. Since $G_i \Delta G$ and $H \Delta G$, therefore, $G_i H = HG_i \Delta G$ and contains H as its normal subgroup. Hence $\frac{HG_i}{H} \Delta \frac{G}{H}$. Also for i=r, $\frac{HG_r}{H} = \frac{He}{H} = H$ and for i=0, $\frac{HG_0}{H} = \frac{G}{H}$. Since $G_i \subseteq G_{i-1}$, therefore, $HG_i \subseteq HG_{i-1}$. But then $\frac{HG_i}{H} \subseteq \frac{HG_{i-1}}{H}$. Now by above discussion the series

$$\frac{G}{H} = \frac{HG_0}{H} \supseteq \frac{HG_1}{H} \supseteq \ldots \supseteq \frac{HG_r}{H} = H \qquad (2)$$

is normal series of $\frac{G}{H}$. Let $[\frac{HG_i}{H}, \frac{G}{H}] = <[xg_iH, yH]>$. Since for $x \in H$, $xH = Hx = H$, therefore, $[xg_iH, yH] = ((xg_i)^{-1}H)(y^{-1}H)(xg_iH)(yH) = g_i^{-1}x^{-1}Hy^{-1}Hxg_iH\, yH = g_i^{-1}H\, y^{-1}Hg_iHyH = g_i^{-1}y^{-1}g_iyH = [g_i, y]H = [g_i, y]hH$. Now $[g_i, y] \in G_{i-1}$ for all $g_i \in G_i$ and $y \in G$, therefore, $[g_i, g]hH \in \frac{G_{i-1}H}{H}$. But G_{i-1} and H are normal subgroup of G, therefore, $G_{i-1}H = HG_{i-1}$. Hence $[xg_iH, yH] \in \frac{HG_{i-1}}{H}$. But then $[\frac{HG_i}{H}, \frac{G}{H}] \subseteq \frac{HG_{i-1}}{H}$. It shows that series (2) is a central series for $\frac{G}{H}$. Hence $\frac{G}{H}$ is nilpotent of class at most r.

2.3.4 Theorem. If G is a nilpotent group and $H(\neq\{e\})$ is a normal subgroup of G, then $H \cap Z(G) \neq \{e\}$, Z(G) is the centre of G.

Proof. It is given that G is nilpotent of class r, therefore, G has a central series

$$G=G_0\supseteq G_1\supseteq \dots \supseteq G_r\supseteq\{e\}.$$

where each $G_i\Delta G$ and $[G_{i-1}, G]\subseteq G_i$, $1\leq i \leq r$. Let $H\neq\{e\}$ be a normal subgroup of G. Let us suppose that $H\cap Z(G)=\{e\}$. Since G is nilpotent of class r, therefore, $G_{r-1}\neq\{e\}$. As $[G_{r-1}, G]\subseteq G_r=\{e\}$, therefore, every element of G_{r-1} commutes with every element of G. Hence $G_{r-1} \subseteq Z(G)$. Now by our assumption $H\cap G_{r-1}\subseteq H\cap Z(G)=\{e\}$. Further $H\cap G_0(=G)=H \neq\{e\}$, therefore, there exist integer k , $1\leq k \leq r-1$ such that

$$H\cap G_{k-1}\neq\{e\} \text{ and } H\cap G_k =\{e\} \qquad (1)$$

Consider $[H\cap G_{k-1}, G] \subseteq[G_{k-1}, G] \subseteq G_k$ and $[H\cap G_{k-1}, G] \subseteq[H, G] \subseteq H$ (because H is normal in G). Hence $[H\cap G_{k-1}, G]\subseteq H\cap G_k=\{e\}$. But then $H\cap G_{k-1} \subseteq Z(G)$. Therefore, $H\cap G_{k-1}\subseteq H\cap Z(G)=\{e\}$, a contradiction to (1). Hence a contradiction to the assumption that $H\cap Z(G)=\{e\}$. It proves that $H\cap Z(G) \neq\{e\}$.

2.3.5 Theorem. Prove that in a nilpotent group every proper subgroup is properly contained in its normalizer.

Proof. It is given that G is nilpotent(of class r), therefore, G has a central series

$$G=G_0\supseteq G_1\supseteq \dots \supseteq G_r\supseteq\{e\}.$$

where each $G_i \Delta G$ and $[G_{i-1}, G]\subseteq G_i$, $1\leq i \leq r$. Let H be a proper subgroup of G. Then $[G_{r-1}, G]\subseteq G_r=\{e\}\subseteq H$ (because $\{e\}\subseteq H$). Since $H\neq G=G_0$, therefore, there exist a positive integer k such that $G_k \not\subseteq H$ and $G_{k+1} \subseteq H$, $0\leq k \leq r-1$.But then $[G_k, H]\subseteq[G_k, G]\subseteq G_{k+1}\subseteq H$. Thus $h\in H$ and $x\in G_k$, $[x, h]\in H\Rightarrow x^{-1}h^{-1}xh\in H$. Equivalently, $x^{-1}h^{-1}x\in H$ or $x^{-1}hx\in H$ i.e. $x^{-1}Hx\subseteq H\ \forall\ x\in G_k$. Further for $x\in G_k$, $x^{-1}\in G_k$. Hence $(x^{-1})^{-1}Hx^{-1}\subseteq H$ i.e. $xHx^{-1}\subseteq H$. But then $xHx^{-1}\subseteq H\Rightarrow H \subseteq x^{-1}Hx$. By above discussion $H = x^{-1}Hx$ or $xH=Hx\ \forall\ x\in G_k$. Therefore, by definition of normalizer of H. $G_k\subseteq N(H)$. But H is a proper subgroup of G_k. Hence $H \not\subseteq N(H)$. It proves the result.

2.3.6 Definition (i)(Sylow's subgroup) Let G be a finite group of order p^mq, gcd(p, q)=1, then a subgroup H of order p^m is called Sylow's p-group or p-

Sylow group.

(ii) **Maximal subgroup**. Let G be a group. The proper subgroup H of G is called maximal subgroup if $H \subseteq K \subseteq G$, then either K=H or K=G.

2.3.7 **Theorem.** Prove that in a nilpotent group all the maximal subgroups are normal.

Proof. Let G be a nilpotent group and M is a maximal subgroup of G. Then $M \neq G$ i.e. M is a proper subgroup of G. But we know that a proper subgroup of a nilpotent group is always a proper subgroup of its normalizer. Therefore, $M \subset N(M)$. As M is maximal subgroup, therefore, N(M)=G. Hence M is normal in G.

2.3.8 **Theorem.** Prove that in a nilpotent group all the Sylow p-subgroups are normal

Proof. Let P be a Sylow-p subgroup of nilpotent group G. It is sufficient to show that N(P)=G. We know that for a Sylow-p subgroup N(P)=N(N(P)). Now let if possible $N(P) \neq G$. Then N(P) is a proper subgroup of G and hence will be a proper subgroup of its normalizer i.e. $N(P) \subset N(N(P))$. But this is a contradiction to the fact that N(P)=N(N(P)). Since this contradiction arises due to the assumption that $N(P) \neq G$. Hence N(P)=G. Therefore, every Sylow-p subgroup of nilpotent group G is normal.

2.3.9 **Theorem**. Prove that a finite direct product of nilpotent groups is again nilpotent.

Proof. For proving the theorem, first we will show that direct product of two nilpotent groups is again nilpotent. Let H and K are two nilpotent groups. Since the length of a central series can be increased (by repeating term {e} as many time as required), therefore, without loss of generality, we can suppose that central series of H and K have same length r and these series are as:

$$H=H_0 \supseteq H_1 \supseteq \dots \supseteq H_r \supseteq \{e\},$$

where each $H_i \Delta H$ and $[H_{i-1}, H] \subseteq H_i$, $1 \leq i \leq r$.

Similarly,

$$K=K_0 \supseteq K_1 \supseteq \dots \supseteq K_r \supseteq \{e\}.$$

where each $K_i \Delta K$ and $[K_{i-1}, K] \subseteq K_i$, $1 \leq i \leq r$.

Since, $H_i \subseteq H_{i-1}$ and $K_i \subseteq K_{i-1}$, therefore, $H_i \times K_i \subseteq H_{i-1} \times K_{i-1}$. Consider the series

$$H \times K = H_0 \times K_0 \supseteq H_1 \times K_1 \supseteq \dots \supseteq H_r \times K_r \supseteq \{(e,e)\} \qquad (1)$$

As $h^{-1}h_i h \in H_i$, $k^{-1}k_i k \in K_i \ \forall\ h \in H$, $h_i \in H_i$, $k \in K$ and $k_i \in K_i$ (because $H_i \Delta H$ and $K_i \Delta K$), therefore, $(h, k)^{-1}(h_i, k_i)(h, k) = (h^{-1}, k^{-1})(h_i, k_i)(h, k) = (h^{-1}h_i h, k^{-1}k_i k) \in H_i \times K_i$. Hence for each i, $H_i \times K_i \ \Delta\ H \times K$ and Hence (*) is normal series.

Let $[(h_{i-1}, k_{i-1}), (h, k)]$ be an arbitrary element of $[H_{i-1} \times K_{i-1}, H \times K]$ Since

$$\begin{aligned}[(h_{i-1}, k_{i-1}), (h, k)] &= (h_{i-1}, k_{i-1})^{-1}(h, k)^{-1}(h_{i-1}, k_{i-1})(h, k) \\ &= (h_{i-1}^{-1}, k_{i-1}^{-1})(h^{-1}, k^{-1})\,(h_{i-1}, k_{i-1})(h, k) \\ &= (h_{i-1}^{-1}h^{-1}h_{i-1}h,\ k_{i-1}^{-1}k^{-1}k_{i-1}k) \\ &= ([h_{i-1}, h], [k_{i-1}, k]) \in ([H_{i-1}, H], [K_{i-1}, K]).\end{aligned}$$

As $[H_{i-1}, H] \subseteq H_i$ and $[K_{i-1}, K] \subseteq K_i$ for $1 \leq i \leq r$, therefore, $[(h_{i-1}, k_{i-1}), (h, k)] \in H_i \times K_i$. Hence $[H_{i-1} \times K_{i-1}, H \times K] \subseteq H_i \times K_i$. It shows that series (1) is a central series for $H \times K$. Therefore, $H \times K$ is nilpotent. Take another nilpotent group T. Since $H \times K$ is nilpotent, therefore, by above discussion $(H \times K) \times T = H \times K \times T$ is also nilpotent. Continuing in this way we get that if $H_1, H_2, \dots, H_n$ are nilpotent then $H_1 \times H_2 \times \dots \times H_n$ is also nilpotent.

2.3.10 Theorem. Let G be a finite group. Then the following conditions are equivalent.

(i) G is nilpotent.

(ii) All maximal subgroup of G are normal.

(iii) All Sylow p-subgroup of G are normal

(iv) Element of co-prime order commutes

(v) G is direct product of its Sylow p-subgroups

Proof. Let G be a finite group. We will prove the result as:

(i)⇒(ii). It is given that G is nilpotent. Let M be a maximal subgroup of G. If $M \neq G$, then M is proper subgroup of its N(M), normalizer of M. But than N(M)=G. Hence M is normal in G.

(ii)⇒(iii). Let G_p be a Sylow p-subgroup of G. We have to prove $N(G_p)=G$. Suppose that $N(G_p) \neq G$. Since G is finite, therefore, there exist a maximal

subgroup M of G such that $N(G_p) \subseteq M \subset G$ and $M \neq G$. Since G_p is Sylow p-subgroup of G and $N(G_p) \subseteq M$, therefore, N(M)=M. Further by (ii) , N(M)=G. Hence M=G, a contradiction. Hence $N(G_p)=G$ i.e. G_p is normal in G.

(iii)⇒(iv). Let x and $y \in G$ be such that (o(x), o(y))=1. Since the result holds for x=e or y=e, therefore, without loss of generality we suppose that $x \neq e$ and $y \neq e$. Then o(x)=m(>1) and o(y)=n(>1), gcd(m, n)=1. Let $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ and $n = q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$, where p_i and q_j are distinct primes and α_i and β_j are positive integers. Since p_i and q_j are distinct primes, therefore, $gcd(p_i, q_j)=1$.

We know that if $o(x)=p^{\alpha}$, then $x \in G_p$, Sylow p-subgoup. Similarly $y \in G_q$, Sylow q-subgoup if $o(y)=q^{\beta}$. By (iii) $G_p \Delta G$ and $G_q \Delta G$, therefore, for $x \in G_p$ and $y \in G_q$, $x^{-1}y^{-1}xy \in G_p \cap G_q = \{e\}$. Hence $x^{-1}y^{-1}xy=e$ i.e. xy=yx.

If we take $m_i = \frac{m}{p_i^{\alpha_i}}$. Then $gcd(m_1, m_2, \ldots, m_r)=1$. Hence we can integers such that $a_1, a_2, \ldots, a_r$ such that $a_1m_1+\ldots+ a_im_i+ \ldots+a_rm_r=1$. Now $x=x^1 = x^{a_1m_1+...+a_im_i+...+a_rm_r} = x^{a_1m_1} ... x^{a_im_i} ... x^{a_rm_r}$. For $1 \leq i \leq r$, choose $x_i = x^{a_im_i}$. Then $x = x_1 \ldots x_i \ldots x_r$ and $(x_i)^{p_i^{\alpha_i}} = (x)^{a_im_ip_i^{\alpha_i}} = (x)^{a_im} = e$. Hence $o(x_i) | p_i^{\alpha_i}$ i.e. $o(x_i)$ is a power of p_i, therefore, for each i, there exist G_{p_i} (Sylow p_i-subgroup) such that $x_i \in G_{p_i}$. Now by above discussion $x_ix_j=x_jx_i$. Similarly $y=y_1 \ldots y_t \ldots y_s$, $y_t \in G_{q_j}$ and all y_t commute with each other. By the same reason $x_i\ y_j=y_jx_i$. Hence $xy=x_1 \ldots x_i \ldots x_r\ y_1 \ldots y_t \ldots y_s = y_1 \ldots y_t \ldots y_s\ x_1 \ldots x_i \ldots x_r = yx$.

(iv)⇒(v) It is given that elements of co-prime order commute, we have to prove that G is direct product of its Sylow subgroups. Let $o(G)= p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, p_i's are distinct primes. Since, for $1 \leq i \leq r$, $p_i^{\alpha_i} \mid o(G)$, G always have G_{p_i} Sylow p_i-subgoup of order $p_i^{\alpha_i}$.

Let $x \in G_{p_i}$ and $y \in G_{p_j}$. Then order of x is some power of p_i and order of y is some power of p_j, therefore, $gcd(o(x), o(y))=1$. Now by given

condition xy=yx. Let $x \in G$, then $o(x) | o(G)$. Therefore, $o(x) = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r} = u$, $0 \le \beta_i \le \alpha_i$. If we take $u_i = \frac{u}{p_i^{\beta_i}}$. Then gcd($u_1$, u_2, …, u_r)=1. Hence we can integers such that $a_1, a_2, \ldots, a_r$ such that $a_1u_1 + \ldots + a_iu_i + \ldots + a_ru_r = 1$. Now $x = x^1 = x^{a_1u_1 + \ldots + a_iu_i + \ldots + a_ru_r} = x^{a_1u_1} \ldots x^{a_iu_i} \ldots x^{a_ru_r}$. For $1 \le i \le r$, choose $x_i = x^{a_iu_i}$. Then $x = x_1 \ldots x_i \ldots x_r$ and $(x_i)^{p_i^{\beta_i}} = (x)^{a_iu_ip_i^{\beta_i}} = (x)^{a_iu} = e$. Hence $o(x_i) | p_i^{\beta_i}$ i.e. $o(x_i)$ is a power of p_i, therefore, for each i, there exist G_{p_i} (Sylow p_i-subgroup) such that $x_i \in G_{p_i}$. Therefore, by given condition $x_ix_j = x_jx_i$. But then $G_{p_i} \Delta G$. hence G_{p_i} is unique sylow p_i subgroup of G. Now for $x_i \in G_{p_i}$, $1 \le i \le r$, $x \in G_{p_1} G_{p_2} \ldots G_{p_r} \subseteq G$. i.e. $G \subseteq G_{p_1} G_{p_2} \ldots G_{p_r} \subseteq G$. In other words $G = G_{p_1} G_{p_2} \ldots G_{p_r}$.

For given i, let if possible, $e \ne t \in G_{p_i} \cap G_{p_1} \ldots G_{p_{i-1}} G_{p_{i+1}} \ldots G_{p_r}$. Then $t \in G_{p_i} \Rightarrow o(t)$ is some power of p_i and $t \in G_{p_1} \ldots G_{p_{i-1}} G_{p_{i+1}} \ldots G_{p_r}$. Let $k = \prod_{\substack{j=0 \\ j \ne i}}^{r} p_j^{\alpha_j}$. Then $t^k = e$ (because $G_{p_1} \ldots G_{p_{i-1}} G_{p_{i+1}} \ldots G_{p_r}$ is a group of order k and t is its element). But then $p_i | k$, a contradiction. Therefore, t=e i.e. $G_{p_i} \cap G_{p_1} \ldots G_{p_{i-1}} G_{p_{i+1}} \ldots G_{p_r} = \{e\}$. It proves that G is direct product of its Sylow subgroups.

(v)⇒(i) We know that each Sylow subgroup is a p-subgroup and each p group is nilpotent. Now using the fact that direct product of nilpotent group is nilpotent group, G is nilpotent (because by (v) G is direct product of p subgroups).

2.4 SOLVABLE GROUP.

2.4.1 Definition.(Solvable group). A group G is said to be solvable if there exist a finite subnormal series for G such that each of its quotient group is abelian i.e. there exist a finite sequence $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots G_n = (e)$ of subgroup of G in which each G_{i+1} is normal in G_i and $\frac{G_i}{G_{i+1}}$ is abelian for each i, $0 \le i \le n-1$.

2.4.2 **Note**. If G is nilpotent group, then G has a central series, $G=G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots$ $G_n=(e)$, where each $G_i \Delta G$ and $\frac{G_i}{G_{i+1}} \subseteq Z(\frac{G}{G_{i+1}})$. Since $G_{i+1} \Delta G$, therefore, $G_{i+1} \Delta G_i$ also. More over $\frac{G_i}{G_{i+1}} \subseteq Z(\frac{G}{G_{i+1}})$, therefore, being a subgroup of commutative group, $\frac{G_i}{G_{i+1}}$ is abelian also. Hence G is solvable i.e. every nilpotent group is solvable also.

But converse may not be true. Take $G=S_3$ and consider the series

$$S_3=G_0 \supseteq A_3= G_1 \supseteq \{e\}=G_2.$$

Trivially $\{e\} \Delta A_3$. Since index of A_3 in S_3 is two, $A_3 \Delta S_3$. Therefore, it is a normal series for S_3. Clearly order of $\frac{G_0}{G_1}$ and $\frac{G_1}{G_2}$ are prime numbers i.e. 2 and 3 respectively, therefore, the factor groups are abelian. Hence G is solvable group.

It is also clear that each $G_i \Delta G$, therefore, it is a normal series for G. Since $Z(S_3)=\{e\}$, therefore, $\frac{A_3}{\{e\}} = A_3 \not\subseteq Z(S_3) = Z(\frac{S_3}{\{e\}})$. Hence S_3 is not nilpotent.

2.4.3 **Theorem.** Prove that every subgroup of a solvable group is again solvable.

Proof. Let G be solvable group. Then G has a subnormal series

$$G=G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n=(e) \qquad (1)$$

such that $\frac{G_i}{G_{i+1}}$ is abelian for each i, $0 \le i \le n-1$. Let H be a subgroup of G. Define $H_i=H \cap G_i$ for all i. Since intersection of two subgroups is always a subgroup of G, therefore, H_i is a subgroup of G. Further since $G_{i+1} \Delta G_i$, therefore, $H_{i+1}= H \cap G_{i+1} \Delta H \cap G_i=H_i$. Then the series

$$H=H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n=(e)$$

is subnormal series of H.

Define a mapping $\phi: H_i \to \frac{G_i}{G_{i+1}}$ by setting $\phi(x)= xG_{i+1} \; \forall \; x \in H_i$. Now

$x \in H_i = H \cap G_i \Rightarrow x \in G_i$. But then $xG_{i+1} \in \frac{G_i}{G_{i+1}}$, therefore, mapping is well defined. Further for x and $y \in H_i$, we have $\phi(xy) = xyG_{i+1} = xG_{i+1}yG_{i+1} = \phi(x)\phi(y)$. Therefore, ϕ is an homomorphism. Further $\ker \phi = \{x \in H_i | \ \phi(x) = G_{i+1} = (\text{identity of } \frac{G_i}{G_{i+1}})\}$. Therefore,

$x \in \ker \phi$ iff $\phi(x) = G_{i+1}$ iff $xG_{i+1} = G_{i+1}$ iff $x \in G_{i+1}$ iff $x \in H \cap G_i$ iff $x \in H_{i+1}$. Hence $\ker \phi = H_{i+1}$. Then by Fundamental theorem on homomorphism, $\frac{H_i}{H_{i+1}} \cong \phi(H_i)$. Being a subset of an abelian group $\frac{G_i}{G_{i+1}}$, $\phi(H_i)$ is also abelian. Since $\frac{H_i}{H_{i+1}}$ is isomorphic to an abelian group, therefore, $\frac{H_i}{H_{i+1}}$ is also abelian. Hence H is solvable.

2.4.4 Example. If G is a group and H is a normal subgroup of G such that both H and $\frac{G}{H}$ are solvable, then G is solvable.

Solution. Since $\frac{G}{H}$ is solvable, therefore, there exist a subnormal series

$$\frac{G}{H} = \frac{G_0}{H} \supseteq \frac{G_1}{H} \supseteq \ldots \supseteq \frac{G_r}{H} = H \qquad (1)$$

Where each G_i is a subgroup of G containing H and each factor group $\frac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}}$ is abelian. Now each $\frac{G_{i+1}}{H} \Delta \frac{G_i}{H}$, therefore, $(xH)^{-1}yHxH \in \frac{G_{i+1}}{H}$ $\forall$ $x \in G_i$ and $y \in G_{i+1}$. But then $x^{-1}yxH \in \frac{G_{i+1}}{H}$ $\forall$ $x \in G_i$ and $y \in G_{i+1}$ which further implies that $x^{-1}yx \in G_{i+1}$ $\forall$ $x \in G_i$ and $y \in G_{i+1}$ i.e. $G_{i+1} \Delta G_i$. Since $\frac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}} \cong \frac{G_i}{G_{i+1}}$, therefore, $\frac{G_i}{G_{i+1}}$ is abelian also. Further $\frac{G_r}{H} = H \Rightarrow G_r = H$.

Since H is solvable, therefore, there exist subnormal series $H=H_0\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq H_n=(e)$ such that $\frac{H_i}{H_{i+1}}$ is abelian for all $0 \le i \le n-1$.

Now by above discussion series,

$$G=G_0\supseteq G_1\supseteq G_2\supseteq\ldots\supseteq G_n=H=H_0\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq H_n=(e)$$

is a subnormal series for G such that each factor group of it is abelian. Hence G is solvable.

2.4.5 Theorem. A group G is solvable if and only if $G^{(k)}$, k^{th} commutator subgroup is identity i.e. $G^{(k)}=\{e\}$.

Proof. Let $G^{(k)}=\{e\}$ for some integer k. We will show that G is solvable. Let $H_0=G$, $H_1=G^{(1)}$, $H_2=G^{(2)},\ldots$, $H_k=G^{(k)}$. Since $G^{(i)}=(G^{(i-1)})^1$, therefore, $G^{(i)}$ is a normal subgroup of $G^{(i-1)}$ and $\frac{G^{(i-1)}}{G^{(i)}}$ is abelian. But then series

$$G=H_0\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq H_k=(e)$$

is a subnormal series for G such that each factor group of it is abelian. Hence G is solvable.

Conversely, suppose that G is solvable group. We will prove that $G^{(k)}=e$ for some integer k. Let $G=N_0\supseteq N_1\supseteq N_2\supseteq\ldots\supseteq N_k=\{e\}$ be a solvable series for G. Then each N_i is normal in N_{i-1} and $\frac{N_{i-1}}{N_i}$ is abelian for all $1\le i \le k$. Since we know that $\frac{G}{H}$ is abelian iff the commutator subgroup $G^{(1)}\subseteq H$, therefore, $N_{i-1}{}^{(1)} \subseteq N_i$. Thus

$$G^{(1)} = N_0{}^{(1)} \subseteq N_1$$

$G^{(2)} = (G^{(1)})^{(1)} = N_1{}^{(1)} \subseteq N_2$. Continuing in this way we get $G^{(k)} \subseteq N_k = \{e\}$. But then $G^{(k)} = \{e\}$. It proves the result.

2.4.6 Corollary. Every homomorphic image of a solvable group is solvable.

Proof. Let G be a solvable group and G* be its homomorphic image under the mapping ϕ. Now if $[x, y] = x^{-1}y^{-1}xy \in G^{(1)}$, then $\phi(x^{-1}y^{-1}xy) = \phi(x^{-1})\ \phi(y^{-1})\ \phi(x)$

$\phi(y) = \phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y) = [\phi(x), \phi(y)] \in G^{*(1)}$. Similarly $G^{*(k)} = \phi(G^{(k)}) = \phi(e) = e^*$. Hence G^* is solvable.

2.4.7 Corollary. Prove that every factor group of a solvable group is solvable.

Proof. Let G be solvable group and H be its normal subgroup of G. Consider the factor group $\frac{G}{H}$ and define a mapping $\phi: G \to \frac{G}{H}$ by setting $\phi(g) = gH \ \forall \ g \in G$. Then $\phi(g_1g_2) = g_1Hg_2H = \phi(g_1)\phi(g_2)$. Hence ϕ is an homomorphism. Further for each gH we have $g \in G$ such that $\phi(g) = gH$. Hence $\frac{G}{H}$ is homomorphic image of a solvable group. Therefore $\frac{G}{H}$ is solvable.

2.5 SOME DEFINITIONS.

2.5.1 Ring. A non empty set R is called associative ring if there are two operations defined on R, generally denoted by + and . such that for all a, b, c in R:

(1) a+b is in R,

(2) a+b=b+a,

(3) a+(b+c)=(a+b)+c) (called as associative law under addition)

(4) $0 \in R$ such that 0+a=a+0=a,

(5) For every a in R, there exist (-a) in R such that a+(-a)=(-a)+a=0,

(6) $a \cdot b$ is in R,

(7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (called as associative law under multiplication)

(8) $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c) = a \cdot c + b \cdot c$ (called as distributive laws)

Beside it if there exist 1 in R such that $1 \cdot a = a \cdot 1 = a$ for every a in R, then R is called associative ring with unity.

2.5.2 Integral domain. An associative ring R such that $a \cdot b = 0$ if and only if a=0 or b=0 and $a \cdot b = b \cdot a$ for all a and b in R, then R is called an integral domain.

2.5.3 Field. Every integral domain in which every non-zero element has an inverse is called field.

2.5.4 Vector Space. Let F be a field. Then a non empty set V with two binary operations called addition (+)and scalar multiplications(·) defined on it, is called vector space over F if V is abelian group under + and for $\alpha \in F$, $v \in V$, $\alpha v \in V$ satisfies the following conditions:

(1) $\alpha(v+w) = \alpha v + \alpha w$ for all $\alpha \in F$ and v , w in V,

(2) $(\alpha + \beta)v = \alpha v + \beta v$,

(3) $(\alpha\beta)v = \alpha(\beta v)$

(4) $1v = v$

For all α, $\beta \in F$ and v , w belonging to V. v and w are called vectors and α, β are called scalar.

2.6 FIELD EXTENSION

2.6.1 Definition.(Field extension). Let F be a field; the field K is called the extension of F if K contains F or F is a subfield of K.

Example. The field C (of all complex number) is an extension of field R (of all real numbers).

2.6.2 Note. As it is easy to see that every extension of a field acts as a vector space over that field, therefore, if K is an extension of F, K is a vector space over F and dimension of K is called degree of extension of K over F. It is denoted by [K:F]. If [K:F] is finite, then it is called finite extension otherwise it is called infinite extension. C is a finite extension of R, while R is not finite extension of Q (the field of rational numbers)

2.6.3 Theorem. Let L, K and F are fields such that L is a finite extension of K, K is a finite extension of F, then prove that L is finite extension of F also.

Proof. Since L is a finite extension of K, therefore [L:K] =m(say) and the subset $\{l_1, l_2, ...l_m\}$ of L is a basis of L over K. Similarly take [K:F]=n and $\{k_1, k_2, ...k_n\}$ as a basis of K over F. We will show that the set of mn elements $\{l_i k_j ; 1 \le i \le m, 1 \le j \le n\}$ act as a basis of L over F. First we show that every

element of L is linear combination of elements of $l_i k_j$ over F. Let l be an arbitrary of L. Since $\{l_1, l_2, ... l_m\}$ is a basis of L over K, therefore,

$$l = l_1 k_1 + l_2 k_2 + ... + l_m k_m ; \; k_i \in K \qquad (1)$$

Further using the fact that $\{k_1, k_2, ... k_n\}$ is a basis of K over F, we write

$$k_i = f_{i1} k_1 + f_{i2} k_2 + ... + f_{in} k_n ; \; f_{ij} \in F , \; 1 \le i \le m, 1 \le j \le n$$

On putting the values of k_i in (1) we get

$$\begin{aligned} l = l_1 (f_{11} k_1 + f_{12} k_2 + ... + f_{1n} k_n) + l_2 (f_{21} k_1 + f_{22} k_2 + ... + f_{2n} k_n) \\ + ... + l_m (f_{m1} k_1 + f_{m2} k_2 + ... + f_{mn} k_n) \end{aligned}$$

On simplification we write

$$\begin{aligned} l = f_{11} l_1 k_1 + f_{12} l_1 k_2 + ... + f_{1n} l_1 k_n + f_{21} l_2 k_1 + f_{22} l_2 k_2 + ... + f_{2n} l_2 k_n \\ + ... + f_{m1} l_m k_1 + f_{m2} l_m k_2 + ... + f_{mn} l_m k_n = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} l_i k_j \end{aligned}$$

i.e. l is linear combination of $l_i k_j$ over F.

Now we will show that $l_i k_j ; 1 \le i \le m, 1 \le j \le n$ are linearly independent over F. let

$$\begin{aligned} \alpha_{11} l_1 k_1 + \alpha_{12} l_1 k_2 + ... + \alpha_{1n} l_1 k_n + \alpha_{21} l_2 k_1 + \alpha_{22} l_2 k_2 + ... + \alpha_{2n} l_2 k_n \\ + ... + \alpha_{m1} l_m k_1 + \alpha_{m2} l_m k_2 + ... + \alpha_{mn} l_m k_n = 0 \end{aligned} ; \qquad \alpha_{ij} \in F ,$$

which after re-arrangement can be written as

$$\begin{aligned} l_1 (\alpha_{11} k_1 + \alpha_{12} k_2 + ... + \alpha_{1n} k_n) + l_2 (\alpha_{21} k_1 + \alpha_{22} k_2 + ... + \alpha_{2n} k_n) \\ + ... + l_m (\alpha_{m1} k_1 + \alpha_{m2} k_2 + ... + \alpha_{mn} k_n) = 0. \end{aligned}$$

As $F \subset K$, therefore, $\alpha_{i1} k_1 + \alpha_{i2} k_2 + ... + \alpha_{in} k_n \in K$ for $1 \le i \le m$. Since l_i are linearly independent over K, therefore, $\alpha_{i1} k_1 + \alpha_{i2} k_2 + ... + \alpha_{in} k_n = 0$. Now using the fact that $k_j ; 1 \le j \le n$ are linearly independent over F, we get that $\alpha_{ij} = 0$. Hence $l_i k_j ; 1 \le i \le m, 1 \le j \le n$ are linearly independent over F and hence $\{l_i k_j ; 1 \le i \le m, 1 \le j \le n\}$ is basis of L over F. As this set contains nm element, we have nm=[L:F]= [L:K] [K:F].

2.6.4 **Corollary**. If L is a finite extension of F and K is a subfield of L containing F, then [L:F]= [L:K] [K:F] i.e.[K:F] divides [L:F].

Proof. Since it is given that [L:F] is finite, therefore, for proving above result, it is sufficient to show that [L:K] and [K:F] are also finite. As $F \subset K$, therefore, any subset which is linearly independent over K, is linearly

independent over F also. Hence [L:K] is less then [L:F] i.e. [L:K] is finite. As K is a subfield of L containing F, therefore K is a subspace of L over F. Hence dimension of K as a vector space over F is less then that of L i.e. [K:F] is finite. Now by use of Theorem 2.6.3, we get [L:F]= [L:K] [K:F] . Hence [K:F] divides [L:F].

2.7 PRIME FIELDS

2.7.1 Definition. A Field F is called prime field if it has no proper subfield. (If K is subfield of F containing more than two elements and $K \neq F$, then K is called proper subfield of F).

Example. (i) Set of integers {0, 1, 2, …, p-1} is a field under addition and multiplication modulo p, p is prime number. The order of this field is p. As order of every subfield divides the order of field, the only divisors of p are 1 and p itself. Hence above field has no proper subfield. Therefore, this field is prime field and generally denoted as Z_p.

(ii) Field of rational numbers is also prime field. Let K be a subfield of Q (field of rational numbers) then $1 \in K$. Let m/n be arbitrary element of Q, As m=1+1+…1, (taken m times), $m \in K$, similarly $n \in K$. But then n inverse i.e. $(1/n) \in K$ and then $m/n \in K$. i.e $Q \subset K$. Hence Q=K, Showing that Q has no proper subfield. i.e. Q is a prime field.

2.7.2 Theorem. Prove that any prime field P is either isomorphic to Q (field of rational numbers) or Z_p (field of integers under addition and multiplication modulo p, p is prime).

Proof. Let e be the unity (multiplicative identity) of P. Define a mapping $\phi : Z \to P$ by $\phi(m)=me$, $m \in Z$. It is easy to see that it is a ring homomorphism and $\text{Ker}\phi$ is an ideal of Z. Since Z is a principal ideal domain, therefore, there exist an integer q say such that $\text{Ker}\phi = \langle q \rangle$. Consider the following cases:

Case (i). q=0, then ϕ is one –one mapping. Hence $Z \cong \phi(Z) \subseteq P$. Clearly $\phi(Z)$ is integral domain. We know that if two integral domains are isomorphic then there field of quotient are also isomorphic. Q is the field of quotient of Z and

let Q^* be the field of quotients of $\phi(Z)$, then $Q \cong Q^*$. Since $\phi(Z) \subseteq P$, therefore, $Q^* \subseteq P$. As P is prime field, therefore $Q^* = P$. Hence $P \cong Q$.

Case (ii) If $q \neq 0$, then $q > 0$, q can not be 1 because if q=1, then $\phi(q) = qe = 0$, zero of field P, implies that e=0, a contradiction. Hence $q > 1$. Further if q=ab; $a > 1$, $b > 1$, then $\phi(q) = qe = abe = aebe = 0$ implies that either ae=0 or be=0. A contradiction that q is the smallest integer such that qe =0. Hence $q \neq ab$. Therefore q is some prime number p (say). But then $<p>$ is a maximal ideal and $Z/<p> = Zp$ becomes a field. Now by fundamental theorem of homomorphism. $Z_p \cong \phi(Z)$. As Z_p is a field, therefore, $\phi(Z)$ is also a field. But then $\phi(Z) = P$. Hence $Z_p \cong P$.

2.8 KEY WORDS

Central series, Nilpotent, Solvable, Prime fields, extensions.

2.9 SUMMARY. In first Chapter we study Central series, Nilpotent groups, Solvable groups, upper and lower central series of a group and prime fields .

2.10 SELF ASSESMENT QUESTIONS.

(1) Prove that direct product of solvable group is again solvable.

(2) Prove that S_5 is not solvable. In fact S_n is not solvable for all $n > 4$. S_n is symmetric group of degree n.

(3) Prove that every group of order pq, p^2q and pqr is solvable where p, q and r are distinct primes

(4) Prove that a finite p group is cyclic if and only if it has exactly one composition series.

(5) Prove that every field has a subfield isomorphic to prime field.

2.11 SUGGESTED READINGS.

(1) **Topics in Algebra**; I.N HERSTEIN, John wiley and sons, New York.

(2) **Modern Algebra**; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(3) **The theory of groups**; IAN D. MACDONALD, Oxford university press 1968.

MAL-511: M. Sc. Mathematics (Algebra-I)

Lesson No. 3 **Written by Dr. Pankaj Kumar**

Lesson: Field Extensions-II and constructions. **Vetted by Dr. Nawneet Hooda**

STRUCTURE

3.0 OBJECTIVE. Objective of this lesson is to know more about field extensions and about the geometrical constructions using straight edge and compass.

3.1 INTRODUCTION. Let us take a polynomial x^2-2 over Q (field of rational numbers). This polynomial has no rational root. Then it is general question 'Does there exist a field which contain all the roots of this polynomial'. For answering this question we need the extension of the field Q. Therefore, in this chapter we study algebraic, transcendental and simple extensions. We also study the conjugate element.

In Section 3.2 we study algebraic and transcendental extensions. In Section 3.3 we study about roots of a polynomial over the field F. Next two Sections contain conjugate elements and simple extensions. At the last we study construction by straight edge and compass and see the application of algebra in geometrical constructions.

3.2 ALGEBRAIC AND TRANSCENDENTAL EXTENSIONS.

3.2.1 Definition. An element $a \in K$ is called algebraic over F if it satisfies some non-zero polynomial over F. i.e. if there exist elements $\beta_0, \beta_1, ..., \beta_n$ in F, not all zero such that $\beta_0 a^n + \beta_1 a^{n-1} + ... + \beta_n = 0$.

3.2.2 Minimal polynomial of $a \in K$ over field F. Smallest degree polynomial in F[x] satisfied by a is called minimal polynomial of a over field F. If the coefficient of highest degree of minimal polynomial of a is unity of F, then it is called minimal monic polynomial of a. It is unique always. For it, Let $x^n + \alpha_1 x^{n-1} + ... + \alpha_n$ and $x^n + \beta_1 x^{n-1} + ... + \beta_n$ be two minimal monic polynomials of a. Then $a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$ and $a^n + \beta_1 a^{n-1} + ... + \beta_n = 0$. Equivalently $(\alpha_1 - \beta_1) a^{n-1} + ... + \alpha_n - \beta_n = 0$ i.e. a satisfies a polynomial $(\alpha_1 - \beta_1) x^{n-1} + ... + \alpha_n - \beta_n$ of degree less than n, a contradiction. Hence minimal monic polynomial of a is always unique. Minimal polynomial of a is irreducible also. Note that polynomial p(x) is irreducible over F if it can not be written as product of two non-constant polynomials in F[x]. Let if possible p(x)=h(x)g(x), where p(x) is the minimal polynomial of a in F[x], h(x) and g(x) are non-constant polynomials in F[x]. Then 0= p(a)=h(a) g(a). As h(a) and g(a) are the element of K, therefore, either h(a)=0 or g(a)=0. It means either a satisfies h(x) or g(x), polynomial of lower degree then that of degree of p(x), a contradiction. This contradiction proves that p(x) is irreducible over F.

3.2.3 Definition. Field F(a). Let F be a field, then F(a) is called the smallest field containing F and a. In other word, if K is an extension of F containing a, then intersection of all subfields of K which contains F and a is the smallest field containing F and a. Consider the set $T=\{\frac{\alpha_0 a^m + \alpha_1 a^{m-1} + ... + \alpha_m a + \alpha_m}{\beta_0 a^n + \beta_1 a^{n-1} + ...\beta_{n-1} a + \beta_n}$; $\alpha_i, \beta_j \in F$, n and m are any non-negative integers$\}$. Then it is easy to see that T becomes a subfield of K. Since T contains F and a and F(a) is the smallest field containing F and a, therefore, $F(a) \subseteq T$. As a is in F(a) , therefore, $\alpha_0 a^m + \alpha_1 a^{m-1} + ... + \alpha_{m-1} a + \alpha_m$ and $\beta_0 a^n + \beta_1 a^{n-1} + ...\beta_{n-1} a + \beta_n \in F(a)$. Now

$\beta_0 a^n + \beta_1 a^{n-1} + ... + \beta_{n-1} a + \beta_n \in F(a)$, therefore, inverse of $\beta_0 a^n + \beta_1 a^{n-1} + ... + \beta_{n-1} a + \beta_n$ also belongs to F(a). Hence $\frac{\alpha_0 a^m + \alpha_1 a^{m-1} + ... + \alpha_{m-1} a + \alpha_m}{\beta_0 a^n + \beta_1 a^{n-1} + ... + \beta_{n-1} a + \beta_n} \in F(a)$ and hence $T \subseteq F(a)$. Now by above discussion $F(a)=T$. Here we see that F(a) is the field of quotients of F[a], where F[a] is set of all polynomials in a over F. Now we will study the structure of F(a), when a is algebraic over F.

3.2.4 Theorem. The element $a \in K$ will be algebraic over F if and only if [F(a):F] is finite.

Proof. First suppose that [F(a):F]=n(say). Consider subset {1, a, …, a^n} of F(a) containing n+1 elements. Since the dimension of F(a) is n, these elements will be linearly dependent over F i.e. we can find $\alpha_0, \alpha_1, ..., \alpha_n$ in F, not all zero, such that $\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$. Since a satisfies a non-zero polynomial $\alpha_0 x^n + \alpha_1 x^{n-1} + ... + \alpha_n$ in F, therefore, a is algebraic over F.

Conversely, suppose that a is algebraic over F, then by Definition 3.2.1, a satisfies some non zero polynomial in F. Let p(x)= $x^n + \alpha_1 x^{n-1} + ... + \alpha_n$ be the smallest degree monic polynomial in F such that p(a)=0. i.e $a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$. But then $a^n = -\alpha_1 a^{n-1} - .... - \alpha_n$.

Further

$a^{n+1} = -\alpha_1 a^n - .... - \alpha_n a = -\alpha_1(-\alpha_1 a^{n-1} - .... - \alpha_n) .... - \alpha_n a$ which is again a linear combination of elements 1, a, a^2,…,a^{n-1} over F. Similarly, for non-negative integer k, a^{n+k} is linear combination of elements 1, a, a^2,…,a^{n-1} over F.

Consider the set $T=\{ \alpha_1 a^{n-1} + \alpha_2 a^{n-1} + ... + \alpha_{n-1} a + \alpha_n ; \alpha_i \in F \text{ for } 1 \le i \le n \}$. Let $h(a) = \alpha_1 a^{n-1} + \alpha_2 a^{n-1} + ... + \alpha_{n-1} a + \alpha_n$ and $t(a) = \beta_1 a^{n-1} + \beta_2 a^{n-1} + ... + \beta_{n-1} a + \alpha_n$ are two arbitrary elements of T. Then T is closed under addition. Since every power of a is linear combination of the elements 1, a, a^2,…,a^{n-1} over F, therefore, $h(a)t(a) \in T$ i.e. T is closed under multiplication too. Further $h(a) - t(a) \in T$.

Now we will show that for non-zero element u(a), $h(a)u(a)^{-1} \in T$. Since u(a)= $\gamma_1 a^{n-1} + \gamma_2 a^{n-1} + ... + \gamma_{n-1} a + \alpha_n \neq 0$, therefore, p(x) does not divides u(x).

Since p(x) is irreducible, therefore, gcd(p(x), u(x))=1. Now we can find two polynomials g(x) and h(x) in F[x] such that p(x)h(x)+u(x)g(x)=1 or equivalently p(a)h(a)+u(a)g(a)=1. As p(a)=0, therefore, u(a)g(a)=1. Hence g(a) is inverse of u(a). Now $h(a)u(a)^{-1} = h(a)g(a)$ is also in T. Here we have shown that T is a subfield of K containing F and *a*. Hence F(a)⊆T. Also it can be easily seen that T is contained in F(a). Hence T=F(a).

Now we will show that the subset {1, a, a^2,…,a^{n-1} } of T acts as a basis for F(a) over F. Since every element of T is of the form $\alpha_1 a^{n-1} + \alpha_2 a^{n-1} + ... + \alpha_{n-1} a + \alpha_n$, therefore, every element of T is linear combination of elements of the set {1, a, a^2,…,a^{n-1} }. Now we have to show that these elements are linearly independent over F. Let $\alpha_1 a^{n-1} + ... + \alpha_{n-1} a + \alpha_n = 0; \alpha_i \in F$. Then 'a' satisfies a polynomial $\alpha_1 x^{n-1} + \alpha_2 x^{n-1} + ... + \alpha_{n-1} x + \alpha_n$ of degree n-1 which less then n, the degree of minimal polynomial p(x) over F. Hence it must be a zero polynomial i.e. each $\alpha_i = 0$. Now it is clear that [F(a):F]=n. Hence F(a) is a finite extension of F.

3.2.5 **Definition**. If the minimal polynomial of a∈K is of degree n, then 'a' is algebraic over F of degree n.

As the minimal polynomial of $\sqrt{2}$ is x^2-2. therefore, $\sqrt{2}$ algebraic over Q of degree 2. Similarly $2^{\frac{1}{3}}, 3^{\frac{1}{4}}$ are algebraic over Q and are of degree 3 and 4 respectively.

3.2.6 **Note.** If a∈K is algebraic of degree n, then [F(a):F]=n. See the problem 3.

3.2.7 **Definition.** An extension K of F is called algebraic extension of F if every element of K is algebraic over F.

3.2.8 **Theorem**. Prove that every finite extension K of F is algebraic extension of F.

Proof. Let [K: F]=n and k is arbitrary element of k. Consider n+1 elements 1, k, k^2, …, k^n. As dimension of K is n over F, these elements of K are linearly dependent over F. Hence $\alpha_0 + \alpha_1 k + \alpha_2 k^2 + ... + \alpha_n k^n = 0$ with at least one of

$\alpha_i \in F$ is not zero. In other words, we can say that k satisfies non zero polynomial $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n$ over F, k is algebraic over F. Hence K is algebraic extension of F.

3.2.9 Theorem. Let K be an extension of F. The elements of K which are algebraic over F form a subfield of K.

Proof. Let S be the set of all elements of K which are algebraic over F. Let a and b are two arbitrary elements of S. In order to show that S is a subfield of K, we will show that a+b, a-b, ab and ab^{-1} all are in S. Since field F(a, b) contains all elements of the form a+b, a-b, ab and ab^{-1}, it is sufficient to show that F(a, b) is a finite extension of F. Suppose that a is algebraic of degree n over F and b is algebraic of degree m over F. Then by Note 3.2.6, [F(a): F]=n and [F(b): F]=m. Further a number which is algebraic over F is also algebraic over every extension of F. Hence b is algebraic over F(a) also and therefore, [F(a, b):F(a)] ≤ [F(b):F]=m. By Theorem 2.6.3, [F(a, b): F]= [F(a, b): F(a)] [F(a): F]. Therefore, by above discussion [F(a,b): F] ≤ mn i.e. finite. Now by Theorem 3.2.8, F(a, b) is an algebraic extension of F. Hence a+b, a-b, ab and ab^{-1} all are algebraic over F and hence belongs to S i.e. S is a subfield of K.

3.2.10 Corollary. If a and b in K are algebraic over F of degrees n and m respectively, then a+b, a-b, and a/b (b≠0) are algebraic over F of degree at most mn.

Proof. Given that [F(a):F]=n and [F(b):F]=m. Since a number which is algebraic over F is also algebraic over every extension of F, therefore, b is algebraic over F(a) also and satisfies a polynomial of degree at most m. Hence [F(a, b):F(a)] ≤ [F(b):F]=m. By Theorem 2.6.3, [F(a, b):F]= [F(a, b):F(a)] [F(a):F]. Therefore, by above discussion [F(a, b): F] ≤ mn i.e. finite. Now by Theorem 3.2.8, F(a, b) is an algebraic extension of F. Hence a+b, a-b, ab and ab^{-1} all are algebraic over F. Since [F(a, b): F] ≤ mn, every element of F(a, b) satisfies a polynomial of degree at most mn over F. Since a+b, a-b, ab and ab^{-1} all are in F(a, b), therefore, there minimal polynomial is of degree at most mn and hence are algebraic of degree at most mn over F.

3.2.11 Note. F(a, b) is the field obtained by adjoining b to F(a) or by adjoining a to F(b). Similarly we can obtain $F(a_1, a_2, ..., a_n)$ by adjoining a_1 to F, then a_2 to $F(a_1)$, a_3 to $F(a_1, a_2)$ and so on and at last adjoining a_n to $F(a_1, a_2, \ldots, a_{n-1})$.

3.2.12 Theorem. If L is an algebraic extension of K and K is an algebraic extension of F, then L is an algebraic extension of F.

Proof. Let u be an arbitrary element of field L. We will show that u is algebraic over F. As u is algebraic over K, therefore, u satisfies the polynomial $\alpha_0 + \alpha_1 x + ... + x^n$, $\alpha_i \in K$. Since K is algebraic extension of F, therefore, each α_i is also algebraic over F. As α_0 is algebraic over F, therefore, $[F(\alpha_0) : F]$ is finite. Since α_1 is algebraic over F, therefore, it is algebraic over $F(\alpha_0)$ also. Hence $[F(\alpha_0)(\alpha_1) : F(\alpha_0)] = [F(\alpha_0, \alpha_1) : F(\alpha_0)]$ is finite extension. Similarly we can see that for $0 \le i \le n-1$, $[F(\alpha_0, \alpha_1, .., \alpha_i) : F(\alpha_0, \alpha_1, .., \alpha_{i-1})]$ is finite. Now by Theorem 2.6.3,

$$[F(\alpha_0, \alpha_1, .., \alpha_{n-1}) : F] = [F(\alpha_0, \alpha_1, .., \alpha_{n-1}) : F(\alpha_0, \alpha_1, .., \alpha_{n-2})]$$
$$[F(\alpha_0, \alpha_1, .., \alpha_{n-2}) : F(\alpha_0, \alpha_1, .., \alpha_{n-3})]$$
$$\ldots\ldots [F(\alpha_0, \alpha_1) : F(\alpha_0)] [F(\alpha_0) : F]$$

is finite because for each i, $[F(\alpha_0, \alpha_1, .., \alpha_i) : F(\alpha_0, \alpha_1, .., \alpha_{i-1})]$ is finite. We also see that the polynomial $\alpha_0 + \alpha_1 x + ... + x^n$ has all its coefficients in the field $F(\alpha_0, \alpha_1, .., \alpha_{n-1})$, therefore, u is algebraic over $F(\alpha_0, \alpha_1, .., \alpha_{n-1})$ also. Hence $[F(\alpha_0, \alpha_1, .., \alpha_{n-1})(u) : F(\alpha_0, \alpha_1, .., \alpha_{n-1})]$ is finite. Now

$[F(\alpha_0, \alpha_1, .., \alpha_{n-1})(u) : F]$

$= [F(\alpha_0, \alpha_1, .., \alpha_{n-1})(u) : F(\alpha_0, \alpha_1, .., \alpha_{n-1})] [F(\alpha_0, \alpha_1, .., \alpha_{n-1}) : F]$ is also finite. But then $F(\alpha_0, \alpha_1, .., \alpha_{n-1}, u)$ is algebraic extension of F. As $u \in F(\alpha_0, \alpha_1, .., \alpha_{n-1}, u)$, therefore, u is algebraic over F. Hence L is algebraic extension of F.

3.2.13 Definition. A complex number is said to be algebraic number if it is algebraic over the field of rational numbers. Complex number which is not algebraic is called transcendental.

3.2.14 Example.(i) Show that $\sqrt{2}+\sqrt[3]{5}$ is algebraic over Q of degree 6.

Solution. Let $\alpha=\sqrt{2}+\sqrt[3]{5}$. Then $\alpha-\sqrt{2}=\sqrt[3]{5}$. Cubing on both sides we get

$$\alpha^3-3\alpha^2\sqrt{2}+6\alpha^2\sqrt{2}-2\sqrt{2}=5$$

Then

$\alpha^3-5=\sqrt{2}(3\alpha^2+6\alpha^2-2)$. Squaring on both sides we get

$\alpha^6-10\alpha^3+25=2(3\alpha^2+6\alpha^2-2)^2$ i.e. α satisfies a polynomial $x^6-10x^3+25-2(3x^2+6x^2-2)^2$ of degree six over Q. More over it is the smallest degree polynomial satisfied by α. Hence α is algebraic over Q and is of degree 6.

Example (ii) Show that $\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})=\mathrm{Q}(\sqrt{2},\sqrt[3]{5})$. Then show that $[\mathrm{Q}(\sqrt{2},\sqrt[3]{5}):\mathrm{Q}]=6$.

Solution. First we will show that $\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})\subseteq\mathrm{Q}(\sqrt{2},\sqrt[3]{5})$. Since $\sqrt{2}\in\mathrm{Q}(\sqrt{2},\sqrt[3]{5})$ and $\sqrt[3]{5}\in\mathrm{Q}(\sqrt{2},\sqrt[3]{5})$, therefore, $\sqrt{2}+\sqrt[3]{5}\in\mathrm{Q}(\sqrt{2},\sqrt[3]{5})$. But $\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$ is the smallest field containing $\sqrt{2}+\sqrt[3]{5}$. Hence $\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})\subseteq\mathrm{Q}(\sqrt{2},\sqrt[3]{5})$.

On the other hand $\alpha=\sqrt{2}+\sqrt[3]{5}\in\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$, then $\alpha^2=2+\sqrt[3]{25}+2\sqrt{2}.\sqrt[3]{5}$ also belongs to $\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$. Equivalently,

$$\alpha^2-2=\sqrt[3]{5}(\sqrt[3]{5}+\sqrt{2}+\sqrt{2})=\sqrt[3]{5}(\alpha+\sqrt{2}) \qquad (1)$$

Cubing (1) on both sides, we get

$$(\alpha^2-2)^3=5(\alpha+\sqrt{2})^3=5(\alpha^3+3\alpha^2\sqrt{2}+6\alpha+2\sqrt{2})$$

$$=5\alpha^3+30\alpha+5(3\alpha^2+2)\sqrt{2}.$$

$\Rightarrow(\alpha^2-2)^3-5\alpha^3-30\alpha=5(3\alpha^2+2)\sqrt{2}\in\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$.

Since $\alpha\in\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$, therefore, $5(3\alpha^2+2)\in\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$. But then $(3\alpha^2+2)^{-1}\in\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$. Hence

$$(3\alpha^2+2)^{-1}(3\alpha^2+2)\sqrt{2}=\sqrt{2}\in\mathrm{Q}(\sqrt{2}+\sqrt[3]{5})$$

and hence

$$\alpha - \sqrt{2} = \sqrt{2} + \sqrt[3]{5} - \sqrt{2} = \sqrt[3]{5} \in Q(\sqrt{2} + \sqrt[3]{5})$$

Since $\sqrt{2}$, $\sqrt[3]{5} \in Q(\sqrt{2} + \sqrt[3]{5})$, therefore, $Q(\sqrt{2}, \sqrt[3]{5}) \subseteq Q(\sqrt{2} + \sqrt[3]{5})$. Hence

$$Q(\sqrt{2}, \sqrt[3]{5}) = Q(\sqrt{2} + \sqrt[3]{5}).$$

As $\sqrt{2}$ satisfies the polynomial $x^2 - 2$, therefore, $\sqrt{2}$ is algebraic of degree over Q. Hence $[Q(\sqrt{2}) : Q] = 2$. The general element of the field $Q(\sqrt{2}) = a + b\sqrt{2}\,;\ a, b \in Q$.

Clearly, $\sqrt[3]{5} \neq a + b\sqrt{2}$. Because, if $\sqrt[3]{5} = a + b\sqrt{2}$, then $\sqrt[3]{5} - b\sqrt{2} = a$. As left hand side is an irrational while right hand side is rational number, a contradiction. Since $\sqrt[3]{5}$ satisfies the polynomial $x^3 - 5$ over Q, which is irreducible over Q, therefore, $[Q(\sqrt[3]{5}) : Q] = 3$.

As $\sqrt[3]{5}$ is algebraic over Q, therefore, it is algebraic over $Q(\sqrt{2})$. But then $[Q(\sqrt{2}, \sqrt[3]{5}) : Q(\sqrt{2})] \leq 3$. Because $\sqrt[3]{5} \notin Q(\sqrt{2})$, $[Q(\sqrt{2}, \sqrt[3]{5}) : Q(\sqrt{2})] \neq 1$. Hence $[Q(\sqrt{2}, \sqrt[3]{5}) : Q(\sqrt{2})] = 3$ and hence $[Q(\sqrt{2}, \sqrt[3]{5}) : Q] = [Q(\sqrt{2}, \sqrt[3]{5}) : Q(\sqrt{2}][Q(\sqrt{2}) : Q] = 3.2 = 6$.

Since $Q(\sqrt{2} + \sqrt[3]{5}) = Q(\sqrt{2}, \sqrt[3]{5})$, therefore, $[Q(\sqrt{2} + \sqrt[3]{5}) : Q] = 6$.

3.2.15 Example. Let g(x) be a polynomial with integer coefficients, prove that if p is a prime number then for $i \geq p$, $\frac{d^i}{dx^i}\left(\frac{g(x)}{(p-1)!}\right)$ is a polynomial with integer coefficients each of which is divisible by p.

Solution. As we know that for given integer n and m, ${}^nP_m = m!\,{}^nC_m$ where ${}^nP_m$ is the number of permutations of n distinct things taking m at a time and ${}^nC_m$ is the number of combination of n different things taking m at a time. Further, ${}^nP_m$ and ${}^nC_m$, both are integers, we get that $\frac{{}^nP_m}{m!} = \frac{n(n-1)...(n-m+1)}{m!}$ is an integer. In other words, product of m consective positive integers is always divisible by m!. As $\frac{d^i}{dx^i}\left(\frac{x^k}{(p-1)!}\right)$ =

$k(k-1)...(k-i+1)\frac{x^{k-i}}{(p-1)!}$; if k≥i and zero otherwise. By above discussion $k(k-1)...(k-i+1)$ is the product of i consective integers hecce divisible by i!. But i≥p, hence p! also divides $k(k-1)...(k-i+1)$ and hence p divides $\frac{k(k-1)...(k-i+1)}{(p-1)!}$. Now by above discussion $\frac{d^i}{dx^i}(\frac{g(x)}{(p-1)!})$ is a polynomial with integer coefficients each of which is divisible by p.

3.2.16 Theorem. Prove that number e is transcendental.

Proof. Suppose f(x) is a polynomial of degree r with real coefficient. Let $F(x) = f(x) + f^1(x) + ...f^r(x)$; $f^k(x)$ is the k^{th} derivative of f(x) with respect to x. Consider $e^{-x}F(x)$. Then $\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}f(x)$. As $e^{-x}F(x)$ is continuously differentiable singled valued function in the interval [0, k] for positive integer k, by mean value theorem we get

$$\frac{e^{-k}F(k) - e^{-0}F(0)}{k-0} = \frac{d}{dx}(e^{-x}F(x))_{x=\theta_k k} \; ; 0 < \theta_k < 1$$

On simplification, we get,

$F(k) - e^k F(0) = -ke^{-(1-\theta_k)k}f(\theta_k k)$. We write these out explicitly:

$$F(1) - eF(0) = -e^{-(1-\theta_1)}f(\theta_1 k) = \varepsilon_1$$

$$F(2) - e^2F(0) = -2e^{-2(1-\theta_2)}f(\theta_2 k) = \varepsilon_2$$

.

.

.

$$F(n) - e^nF(0) = -ne^{-(1-\theta_n)}f(\theta_n n) = \varepsilon_n$$

Suppose now that e is an algebraic number ; then it satisfies some relation of the form

$c_n e^n + c_{n-1}e^{n-1} + ... + c_1 e + c_0 = 0$; $c_0, c_1, \ldots, c_n$ are integers and $c_0 > 0$.

Now

$$c_1(F(1) - eF(0)) = -e^{-(1-\theta_1)}f(\theta_1 k) = \varepsilon_1$$

$$+c_2(F(2)-e^2F(0)=-2e^{-2(1-\theta_2)}f(\theta_2 k)=\varepsilon_2$$

$$+\ldots$$

$$+c_n(F(n)-e^nF(0)=-ne^{-(1-\theta_n)}f(\theta_n n)=\varepsilon_n \text{ . Equivalently}$$

$$c_1F(1)+c_2F(2)+\ldots+c_nF(n)-F(0)(c_ne^n+c_{n-1}e^{n-1}+\ldots+c_1e)=c_1\varepsilon_1+\ldots+c_n\varepsilon_n$$

Since

$$c_ne^n+c_{n-1}e^{n-1}+\ldots+c_1e=-c_0\,,$$

therefore, above equation reduces to

$$c_0F(0)+c_1F(1)+c_2F(2)+\ldots+c_nF(n)=c_1\varepsilon_1+\ldots+c_n\varepsilon_n \qquad (*)$$

Since the equation (*) holds for all polynomials f(x), choose

$f(x)=\dfrac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p\ldots(n-x)^p$; p is a prime number so that $p > n$ and $p > c_0$. When expand, f(x) is a polynomial of the form

$$\frac{(n!)^p}{(p-1)!}x^{p-1}+\frac{a_0x^p}{(p-1)!}+\frac{a_1x^{p+1}}{(p-1)!}+\ldots\,, \qquad (**)$$

where $a_0, a_1, \ldots$, are integers.

Consider the following cases:

(i) when $i \geq p$.

By Example 3.2.15, $f^i(x)$ is a polynomial whose coefficients are all multiple of p. Thus for any integer j, $f^i(j)$ is a multiple of p.

(ii) i<p-1. Since f(x) has roots 1, 2, …, n, each with multiplicity p and zero is root of f(x) with multiplicity p-1. therefore, $f^i(x)$ is zero for x=0, 1, 2, …, n.

(iii) i=p-1. Since f(x) has roots 1, 2, …, n, each with multiplicity p and zero is root of f(x) with multiplicity p-1, therefore, $f^{p-1}(x)$ is zero for x= 1, 2, …, n and by (**), $f^{p-1}(0)=(n!)^p$. Since, p > n, therefore, $f^{p-1}(0)$ is not divisible by p .

As $F(x)=f(x)+f^1(x)+\ldots f^r(x)$, therefore, $F(j)=f(j)+f^1(j)+\ldots f^r(j)$.

From the above discussion we conclude that F(j), $1 \leq j \leq n$ is a multiple of p. Further by case (iii) , $f^{p-1}(0)$ is not divisible by p and by case (i) and (ii) $f^i(0)$ is divisible by p, resulting that F(0) is not divisible by p. Since $p > c_0$,

therefore, $c_0F(0)+c_1F(1)+c_2F(2)+...+c_nF(n)$, left hand side of (*) is not divisible by p.

$$\text{Since } \varepsilon_i = \frac{-e^{i(1-\theta_i)}(1-i\theta_i)^p...(n-i\theta_i)^p(i\theta_i)^{p-1}i}{(p-1)!};0<\theta_i<1.$$

Thus $|\varepsilon_i| \le \frac{e^n n^p (n!)^p}{(p-1)!}$, which tends to zero as $p\to\infty$. Therefore, we choose p such a large prime so that $|c_1\varepsilon_1+...+c_n\varepsilon_n|<1$. But $c_0F(0)+...+c_nF(n)$ is an integer, therefore, $c_1\varepsilon_1+...+c_n\varepsilon_n$ is an integer. Hence $c_1\varepsilon_1+...+c_n\varepsilon_n=0$. But then p divides $c_1\varepsilon_1+...+c_n\varepsilon_n$, a contradiction. Hence contradiction to our assumption that e is algebraic. Therefore, e is transcendental.

Example. For m>0 and n are integers, prove that $e^{\frac{m}{n}}$ is transcendental.

Proof. If a number b is algebraic then b^k is also algebraic. Since b is algebraic, therefore, b satisfies polynomial

$$c_nx^n+c_{n-1}x^{n-1}+...+c_1x+c_0.$$

But then $b^{\frac{1}{m}}$ for m>0, satisfies the polynomial $c_nx^{mn}+c_{n-1}x^{m(n-1)}+...+c_1x^m+c_0$. Hence if b is algebraic then $b^{\frac{1}{m}}$ is also algebraic.

Let us suppose that $t=e^{\frac{m}{n}}$ is algebraic, then $t^n=e^m$ is also algebraic. As t^n is algebraic, therefore, by above discussion, $t^{\frac{n}{m}}$ is also algebraic. But $t^{\frac{n}{m}}=e$, therefore, e is also algebraic, a contradiction. Hence a contradiction to our assumption that $e^{\frac{m}{n}}$ is algebraic and hence $e^{\frac{m}{n}}$ is transcendental.

3.3 ROOTS OF A POLYNOMIAL.

3.3.1 Definition. Let K be an extension of field F, then $a\in K$ is called root of $f(x)\in F[x]$ if f(a)=0.

3.3.2 **Definition**. The element a $\in$K is a root of f(x) $\in$F[x] of multiplicity m if $(x\text{-}a)^m \mid f(x)$ and $(x-a)^{m+1} \nmid f(x)$ i.e. $(x\text{-}a)^m$ divides f(x) and $(x-a)^{m+1}$ does not divides f(x).

3.3.3 **Note**. (i) Let K be an extension of field F, If f(x) $\in$F[x], then any element a $\in$K , f(x)=(x-a)g(x)+f(a), where g(x) $\in$K[x] and degree of g(x) = degree of f(x)-1.

(ii) If K is an extension of field F, a $\in$K is a root of f(x) $\in$F[x], then in K[x], (x-a)|f(x).

(iii) A polynomial of degree n over a field can have at most n roots in any extension field

(iv) If p(x) is an irreducible polynomial in F[x] of degree n≥1, then there exist an extension E of F in which p(x) has a root. Further, if f(x) $\in$F[x], then there exist an extension E of F in which f(x) has a root. More over [E:F] ≤ degree of f(x).

(v) If f(x) is a polynomial of degree n (≥1) over a field F, then there exists an extension E of F which contains all the root of f(x). The degree of extension of this field over F is at most n! i.e. [E:F] ≤n!.

(vi) Let $f(x) = c_n x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$ be a polynomial with integer coefficients, then f(x) will be irreducible over the field of rational numbers Q if we can find a prime number p such that $p \mid c_{n-1}, ..., p \mid c_1, p \mid c_0, p \nmid c_n$ and $p^2 \nmid c_0$.

(vii) Let k be a positive integer, then polynomial f(x) is irreducible over the field of rational numbers if and only if f(x+k) or f(x-k) is irreducible. These results are easy to prove.

3.3.4. **Definition.** If f(x) $\in$F[x], a finite extension E of F is said to be splitting field over F for f(x) if over E, but not over any proper subfield of E, f(x) can be factored as a product of linear factors. Since any two splitting fields over F of f(x) are isomorphic, therefore, splitting field of f(x) is unique.

3.3.5. Example (i). Consider the polynomial $f(x)= x^3-2$ over the field of rational numbers. The roots of the polynomials are $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2$; ω is cube root of unity and is a complex number. As the field $Q(2^{\frac{1}{3}})$ is the subset of real numbers, it does not contain ω. As $[Q(2^{\frac{1}{3}}) : Q] = 3$, the degree of spitting field is larger than 3. Also by Note 3.6.3(v), the degree if splitting field is at most 6. Now we can see that if E is the splitting field over F of x^3-2, then [E: F]=6.

(ii) If $f(x)= x^4+ x^2+1$, then $f(x)= x^4+2x^2+1- x^2= (x^2-x+1)(x^2+x+1)$. As ω and ω^2 are the root of the polynomial x^2+x+1, therefore, roots of polynomial (x^2-x+1) are $-\omega$ and $-\omega^2$. Since all the roots are contained in the field $Q(\omega)$. Hence the splitting field is $Q(\omega)$. More over $[Q(\omega): Q]=2$.

(iii) Consider the polynomial x^6+x^3+1. As $x^9-1= (x^3-1)(x^6+x^3+1)$. Choose ω as primitive 9^{th} root of unity. Then $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7, \omega^8$ are the roots of the polynomial x^9-1. Further, $1, \omega^3, \omega^6$ are the roots of the polynomial x^3-1. Hence $\omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^8$ are the roots of the polynomial (x^6+x^3+1). Since all these roots are contained in the field $Q(\omega)$, $Q(\omega)$ is the splitting field of the polynomial x^6+x^3+1. If $f(x)= x^6+x^3+1$, then $f(x+1)= (x+1)^6+(x+1)^3+1= (x^6+6x^5+15x^4+20x^3+15x^2+6x+1)+ (x^3+3x^2+3x +1) +1= x^6+6x^5+15x^4+21x^3+18x^2+9x+3$. By Eisenstein Criterion of irreducible, the polynomial x^6+x^3+1 is irreducible over Q. Hence $[Q(\omega): Q]=6$.

(iv) Show that algebraic extension may or may not be finite extension.

Solution. **Algebraic extension may be finite extension.** Consider an extension $Q(\sqrt{2})$ of Q. Since every element of $Q(\sqrt{2})$ is of the form $x = a + b\sqrt{2}; a, b \in Q$, therefore $(x-a)^2 = 2b^2$ i.e. every element of $Q(\sqrt{2})$ satisfies a polynomial of degree at most 2. Hence every element of $Q(\sqrt{2})$ is

algebraic over Q, therefore, $Q(\sqrt{2})$ is algebraic extension of Q. More over $[Q(\sqrt{2}):Q]$=2.i.e. it is a finite extension also.

Algebraic extension may not be finite extension. Consider the set S of all complex numbers which are algebraic over Q. Clearly it is an algebraic extension of Q. Let if possible, [S: Q]= n (some finite number). Now consider the polynomial $x^{n+1}+2$. It is irreducible over Q. (By Eisenstein criterion of irreducibility) If a complex number 'a' is a root of $x^{n+1}+2$, then [Q(a): Q]= n+1. Further by our choice $a \in S$, therefore, $Q(a) \subset S$. But then we have that dimension of S as a vector space over Q is less then dimension of subspace Q(a) of S over Q, a contradiction and hence a contradiction to the assumption that S is a finite extension of Q. It supports the result that every algebraic extension need not be finite extension.

3.4 SIMPLE EXTENSION.

3.4.1 Definition. An extension K of F is called simple extension if there exist an α in K such that $K=F(\alpha)$.

Example. Let K be an extension of F such that [K:F]=p , p is prime numer then K is a simple extension.

Solution. Let $\alpha \in K$. As K is finite extension of F, α is algebraic over F. Consider $F(\alpha)$. Since, p >1, $\alpha \notin F$. But then $F(\alpha)$ is a subfield of K containing F. Hence $F(\alpha)$ is the subspace of the field K over F and hence dimension of $F(\alpha)$ as a vector space divides the dimension of K as a vector space over F i.e. $[F(\alpha):F]$ divides [K:F]. Because $[F(\alpha): F]>1$, the only possible condition is that $[F(\alpha): F]=p$. But then $K=F(\alpha)$. Hence K is a simple extension of F.

3.5 CONJUGATE ELEMENTS.

3.5.1 Definition. Let K be an extension of the field F. Elements α and β of K are said to be conjugate over F if there exist an isomorphism $\sigma : F(\alpha) \to F(\beta)$ such that $\sigma(\alpha) = \beta$ and $\sigma(\delta) = \delta \ \forall \ \delta \in F$. In other words, σ acts as identity mapping on F and take α to β.

3.5.2 Theorem. Let K be an extension of the field F and the elements α and β of K are algebraic over F. Then α and β are said to be conjugate over F if and only if they have the same minimal polynomial.

Proof. Let us suppose that α and β are conjugate over F. Further let $p(x) = x^n + c_{n-1}x^{(n-1)} + ... + c_1x + c_0$ be the minimal polynomial of α over F. Then $0 = p(\alpha) = \alpha^n + c_{n-1}\alpha^{(n-1)} + ... + c_1\alpha + c_0$. Now

$$0 = \sigma(0) = \sigma(\alpha^n + c_{n-1}\alpha^{(n-1)} + ... + c_1\alpha + c_0)$$

$$\Rightarrow 0 = \sigma(\alpha^n) + \sigma(c_{n-1})\sigma(\alpha^{(n-1)}) + ... + \sigma(c_1)\sigma(\alpha) + \sigma(c_0)$$

Using the fact that $\sigma(\alpha) = \beta$ and $\sigma(\delta) = \delta \ \forall \ \delta \in F$, above equation reduces to $0 = \beta^n + c_{n-1}\beta^{(n-1)} + ... + c_1\beta + c_0$ i.e. β satisfies the polynomial p(x). Let r(x) be the minimal monic polynomial of β. But then r(x)|p(x) where p(x) is irreducible polynomial over F. Since r(x) and p(x) both are monic irreducible polynomials over F, we have r(x)=p(x). Hence α and β have the same minimal polynomial.

Conversely, suppose that they have the same minimal polynomial p(x) of degree n. Then by Theorem 3.5.4, [F(α):F]= [F(β):F]=n. Now 1, α, α^2, … α^{n-1} is a basis of F(α) over F and the general element of F(α) is $a_0+a_1\alpha+a_2\alpha^2+$ …$+a_n\alpha^{n-1}$; a belongs to F. Similarly 1, β, β^2, … β^{n-1} is a basis of F(β) over F and the general element of F(β) is $a_0+a_1\beta+a_2\beta^2+$ …$+a_n\beta^{n-1}$. Define a mapping $\sigma : F(\alpha) \to F(\beta)$ by $\sigma(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}$. Since a_i are unique, therefore, σ is well defined. Now we will show that σ is an isomorphism. It is easy to see that σ is one-one and onto mapping. Only thing is to show that it is a ring homomorphism. Let $a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}$ and $b_0 + b_1\beta + ... + b_{n-1}\beta^{n-1}$ be the two arbitrary element of F(α). Then

$$\sigma((a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) + (b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}))$$
$$= \sigma((a_0 + b_0) + (a_1 + b_1)\alpha + ... + (a_{n-1} + b_{n-1})\alpha^{n-1}))$$

$$= (a_0 + b_0) + (a_1 + b_1)\beta + ... + (a_{n-1} + b_{n-1})\beta^{n-1}$$

$$= a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1} + b_0 + b_1\beta + ... + b_{n-1}\beta^{n-1}$$

$$= \sigma(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) + \sigma(b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}).$$

Since $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = \sum_{i=0}^{n-1} a_i\alpha^i$, $b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} = \sum_{i=0}^{n-1} b_i\alpha^i$

Let $(\sum_{i=0}^{n-1} a_i\alpha^i)(\sum_{i=0}^{n-1} b_i\alpha^i) = \sum_{i=0}^{n-1} c_i\alpha^i$, then $\sigma(\sum_{i=0}^{n-1} a_i\alpha^i)(\sum_{i=0}^{n-1} b_i\alpha^i) = \sum_{i=0}^{n-1} c_i\beta^i$.

Consider the polynomial

$$g(x) = (\sum_{i=0}^{n-1} a_i x^i)(\sum_{i=0}^{n-1} b_i x^i) - \sum_{i=0}^{n-1} c_i x^i \qquad (*)$$

in F[x],

then $g(\alpha) = (\sum_{i=0}^{n-1} a_i\alpha^i)(\sum_{i=0}^{n-1} b_i\alpha^i) - \sum_{i=0}^{n-1} c_i\alpha^i = 0$ and then p(x)|g(x) i.e. g(x)=p(x)h(x). Since $p(\beta) = 0$, therefore, $g(\beta) = p(\beta)h(\beta) = 0$.

Now by (*) $(\sum_{i=0}^{n-1} a_i\beta^i)(\sum_{i=0}^{n-1} b_i\beta^i) = \sum_{i=0}^{n-1} c_i\beta^i$ i.e.

$\sigma(\sum_{i=0}^{n-1} a_i\alpha^i)(\sum_{i=0}^{n-1} b_i\alpha^i) = (\sum_{i=0}^{n-1} a_i\beta^i)(\sum_{i=0}^{n-1} b_i\beta^i)$. Hence σ is an isomorphism. More over if we choose a_l=1 and a_i=0 for all other i, then $\sigma(\alpha) = \beta$ and if we choose all a_i=0 for i>0, then $\sigma(a_0) = a_0$ i.e $\sigma(\delta) = \delta \ \forall\ \delta \in F$ showing that σ is a non-zero isomorphism. It proves the result.

3.5.3 Theorem. Let K be an extension of the field F and the elements α and β of K are transcendental over F. Then α and β are conjugate over F.

Proof. Consider the polynomial ring F[x]. Let $F[\alpha]$ be the sub-ring of K generated by F and α (similarly $F[\beta]$ is sub-ring of K generated by F and β). Then the mapping $\sigma : F[x] \to F[\alpha]$ defined by $\sigma(\sum_{i=1}^{n} c_i x^i) = \sum_{i=1}^{n} c_i\alpha^i;\ c_i \in F$ is an onto ring homomorphism. Further if $\sigma(\sum_{i=1}^{n} c_i x^i) = \sigma(\sum_{i=1}^{n} d_i x^i)$, then $\sum_{i=1}^{n} c_i\alpha^i = \sum_{i=1}^{n} d_i\alpha^i$. This further implies that $\sum_{i=1}^{n} (c_i - d_i)\alpha^i = 0$ i.e. α is algebraic

over F, a contradiction that α is transcendental. Hence $c_i = d_i$ and hence $\sum_{i=1}^{n} c_i x^i = \sum_{i=1}^{n} d_i x^i$ i.e. σ is one-one. Hence σ is an isomorphism. Thus $F[x] \cong F[\alpha]$. Now σ can be extended to a unique isomorphism $\theta : F(x) \to F(\alpha)$, defined by $\theta(\frac{h(x)}{g(x)}) = \frac{h(\alpha)}{g(\alpha)}$, where F(x) is the field of quotient of F[x] and $F(\alpha)$ is the field of quotient of $F[\alpha]$. Now it is clear that $\theta(x) = \alpha$ and $\theta(a) = a \ \forall a \in F$. Similarly, we have an isomorphism $\varphi : F(x) \to F(\beta)$ such that $\varphi(x) = \beta$ and $\varphi(a) = a \ \forall a \in F$. Consider the mapping $\varphi\theta^{-1}$. Then $\varphi\theta^{-1} : F(\alpha) \to F(\beta)$ such that $\varphi\theta^{-1}(\alpha) = \beta$. Since φ and θ^{-1} both are isomorphism, therefore, $\varphi\theta^{-1}$ is also an isomorphism. Hence α and β are conjugate over F.

3.6 CONSTRUCTION WITH STRAIGHT EDGE AND COMPASS.

As in our school class construction, by the use of scale and compass we can draw any line of given length, circle of given radius, and can construct right angle and sixty degree angle.

3.6.1 Definition. A real number α is said to be constructible by straight edge and compass if by the use of straight edge and compass we can construct a line segment of length α. Here by straight edge mean a fundamental unit length.

3.6.2 Note. If a real number α is constructible by straight edge and compass we will use to say that α is constructible.

3.6.3 Theorem. Let F be a field. Then a point α is constructible from F if and only if we can find a finite number of real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $[F(\lambda_1):F] = 1$ or 2; $[F(\lambda_1, \lambda_2, \ldots, \lambda_i): F(\lambda_1, \lambda_2, \ldots, \lambda_{i-1})] = 1$ or 2 for i=1, 2,…,n; and such that α lies in the plane of $F(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

Proof. By a plane of F, we mean set of all points (x, y), where x and y are from F and a real number α is constructible from F if it is point of intersection of lines and circles in the plane of F or it is point of intersection of lines and

circles in the plane of some extension of F. If we take two points (a_1, b_1) and (a_2, b_2) in the plane of F then equation of line passing through these points is $(b_1-b_2)x+(a_2-a_1)y+(a_1b_2)-a_2b_1=0$ which is definitely of the form $ax+by+c = 0$; $a, b, c \in F$. Similarly we can see that equation of circle in the plane of F is $x^2 + y^2 + ax + by + c=0$. Since the point of intersection of two lines in the plane of F always in F, point of intersection of line and circles , circle with circle either lies in F or lies in the plane of $F(\sqrt{\gamma})$ for some positive γ in F. Thus line and circles of F leads to a point in F or in quadratic extension of F.

On similar steps as discussed above, we get that lines and circles in $F(\sqrt{\gamma_1})$ leads to a point in $F(\sqrt{\gamma_1})$ or in quadratic extension of $F(\sqrt{\gamma_1}, \sqrt{\gamma_2})$, for some positive γ_2 in $F(\sqrt{\gamma_1})$. Continuing in this way we get a sequence of extensions such that $[F(\sqrt{\gamma_1},...,\sqrt{\gamma_i}) : F(\sqrt{\gamma_1},...,\sqrt{\gamma_{i-1}})] = 1$ or 2 for each i, positive real number $\gamma_i \in F(\sqrt{\gamma_1},...,\sqrt{\gamma_{i-1}})$ and $\alpha \in F(\sqrt{\gamma_1}, \sqrt{\gamma_2},...,\sqrt{\gamma_n})$.

Now by above discussion, if α is constructible then we can find a finite number of real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $[F(\lambda_1):F]= 1$ or 2; $[F(\lambda_1, \lambda_2, \ldots, \lambda_i): F(\lambda_1, \lambda_2, \ldots, \lambda_{i-1})]= 1$ or 2 for i=1, 2,…,n and $\alpha \in F(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

Conversely if $\gamma \in F$ is such that $\sqrt{\gamma}$ is a real number then γ is a point of intersection of lines and circles in the plane of F. Now $\alpha \in F(\lambda_1, \lambda_2, \ldots, \lambda_n)$, therefore, α is a point of intersection of lines and circles in the plane of $F(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})$. Hence α is constructible. In other words a real number α is constructible from F if and only if we can find real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_1^2 \in F, \lambda_i^2 \in F(\lambda_1, \lambda_2, \lambda_{i-1})$ for i=1, 2, …, n such that $\alpha \in F(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

3.6.4 **Note.** Since it quite easy to see that every rational number is constructible, therefore, by above theorem a real number α is constructible, we start from F_0, the field of rational numbers and get an extension of F_0 in which α lies.

3.6.5 **Therorem.** A real number α is constructible from F_0 if and only if we can find real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_1^2 \in F_0, \lambda_i^2 \in F_0(\lambda_1, \lambda_2, \lambda_{i-1})$ for i=1, 2, …, n such that $\alpha \in F_0(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

Proof. Replace F by F_0 in the proof of Theorem 3.7.3.

3.6.6 Corollary. If α is constructible, then α lies in some extension F of F_0 of degree a power of 2.

Proof. As we know that real number α is constructible if and only if we can find a finite number of real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_1^2 \in F_0$, $\lambda_i^2 \in F(\lambda_1, \lambda_2, \lambda_{i-1})$ for i=1, 2, …, n such that $\alpha \in F(\lambda_1, \lambda_2, \ldots, \lambda_n)$. But then $[F_0(\lambda_1, \lambda_2, \ldots, \lambda_i): F_0(\lambda_1, \lambda_2, \ldots, \lambda_{i-1})] = 1 \text{ or } 2 = 2^{a_i}$, a_i=0 or 1, for i=1, 2,…,n. Since $[F_0(\lambda_1, \lambda_2, \ldots, \lambda_n): F_0] = [F_0(\lambda_1, \lambda_2, \ldots, \lambda_n): F_0(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})]\, [F_0(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}): F_0(\lambda_1, \lambda_2, \ldots, \lambda_{n-2})] \ldots [F_0(\lambda_1): F_0] = 2^{a_n + a_{n-1} + \ldots + a_1}$ is a power of 2.

3.6.7 Corollary. If a real number α satisfies an irreducible polynomial over the field of rational numbers of degree k, and if k is not a power of 2, then α is not constructible.

Proof. Since a real number α is constructible if and only if it lies in an extension K of F_0, a power of 2. If α satisfies an irreducible polynomial of degree k then $[F_0(\alpha):F]=k$. Since k is odd, it can not be a power of 2 and hence it is not constructible.

3.6.8 Theorem. Prove that 60^θ angle is constructible.

Proof. As we know that if an angle θ is constructible if and only if $\cos\theta$ is constructible. Let $\theta=60^\theta$, then $\cos\theta=\cos 60^\theta = \frac{1}{2} \Rightarrow \cos\theta - \frac{1}{2} = 0$ i.e. $\cos\theta$ satisfies an irreducible polynomial of degree $1=2^0$, a power of 2, over the field of rationals. Hence $\cos\theta$ is constructible and hence $\theta=60^\theta$ is constructible.

3.6.9 Theorem. Prove that it is impossible, by straight edge and compass alone, to trisect 60^θ angle.

Proof. By the trisection of 60^θ angle by straight edge and compass alone mean we have to construct 20^θ. As we know that 20^θ is constructible iff $\cos 20^\theta$ is constructible. Let $\theta=20^\theta$. Then $3\theta=60^\theta$ and $\cos 3\theta=\cos 60^\theta$. But then $4\cos^3\theta -$

$3\cos\theta=\frac{1}{2}$ or $8\cos^3\theta-6\cos\theta-1=0$ i.e. $\cos\theta$ satisfies the polynomial $8x^3-6x-1$. Let $f(x)= 8x^3-6x-1$, then $f(x-1)= 8(x-1)^3-(6x-1)-1= 8x^3-24x^2+18x-3$. Since 3 is a prime number which divides every coefficient, except the leading coefficient of the polynomial $f(x-1)$ and 3^2 does not divide constant coefficient of the polynomial $f(x-1)$. Then by Eisenstein criterion of irreducibility, $f(x-1)$ is an irreducible polynomial over field of rational numbers. But then $f(x)$ is also irreducible over field of rational numbers. Therefore, $[Q(\cos\theta):Q]=3$ which is not a power of 2. Hence $\cos\theta$ is not constructible. Equivalently θ is not constructible. Hence we can not trisect 60^θ by straight edge and compass alone.

3.6.10 Theorem. By straight edge and compass it is impossible to duplicate the cube.

Proof. As by duplicate of a cube means construction of cube whose volume is double the volume of given cube. Let us consider the cube of unit length side. Then the volume of cube is 1. For duplicating this cube, we have to construct a cube of volume 2 units i.e. we have to construct a number α such that $\alpha^3=2$. Since 2 is a prime number which divides every coefficient, except the leading coefficient of the polynomial x^3-2 and 2^2 does not divide constant coefficient of the polynomial x^3-2. Then by Eisenstein Criterion of irreducibility, x^3-2 is an irreducible polynomial over field of rational numbers. Hence $[Q(\alpha):Q]=3$ i.e. α is not constructible. It proves the result.

3.6.11 Theorem. Prove that it is impossible to construct a regular septagon.

Proof. Since for construction of regular septagon we need the construction of an angle $\frac{2\pi}{7}$. We will show that $\theta=\frac{2\pi}{7}$ is not constructible. Equivalently we have to show that $\cos\theta$ is not constructible. Since

$$7\theta = 2\pi \Rightarrow 4\theta = 2\pi-3\theta \Rightarrow \cos 4\theta = \cos(2\pi-3\theta) \Rightarrow \cos 4\theta = \cos 3\theta$$

$$\Rightarrow 2\cos^2 2\theta-1 = 4\cos^3\theta-3\cos\theta$$

$$\Rightarrow 2(2\cos^2\theta-1)^2-1 = 4\cos^3\theta-3\cos\theta$$

$$\Rightarrow 8\cos^4\theta+1-8\cos^2\theta = 4\cos^3\theta-3\cos\theta$$

$$\Rightarrow 8\cos^4\theta-4\cos^3\theta-8\cos^2\theta+3\cos\theta+1=0$$

$\Rightarrow(\cos\theta-1)(8\cos^3\theta+4\cos^2\theta-4\cos\theta-1)=0$

Since for given θ, $\cos\theta \neq 1$, therefore, $\cos\theta-1\neq 0$. Hence $\cos\theta$ satisfies the polynomial $f(x)=8x^3+4x^2-4x-1$. Since $f(x+1)=8(x+1)^3+4(x+1)^2-4(x+1)-1 = 8(x^3+3x^2+3x+1)+4(x^2+2x+1)-4(x+1)-1= 8x^3+28x^2+28x+7$.

Since 7 is a prime number which divides every coefficient, except the leading coefficient of the polynomial $f(x+1)$ and 7^2 does not divide constant coefficient of the polynomial $f(x+1)$. Then by Eisenstein Criterion of irreducibility, $f(x+1)$ is an irreducible polynomial over field of rational numbers. But then $f(x)$ is also irreducible over field of rational numbers. By above discussion we get that $\cos\theta$ satisfies an irreducible polynomial of degree three. Hence $\cos\theta$ is not constructible. It proves the result.

3.7 KEY WORDS.

Algebraic, Transcendental, Root, Simple, Conjugate, Construction, Straight edge, Compass.

3.8 SUMMARY. Algebraic, transcendental, simple extensions, conjugate element, roots of a polynomial over the field F and application of algebra in geometrical constructions are studied in this Chapter.

3.9 SELF ASSESMENT QUESTIONS.

(1) Prove that sin m^θ is constructible.

(2) Prove that regular pentagon is constructible.

(3) If $a\in K$ is algebraic of degree n, then $[F(a):F]=n$.

(4) Prove that regular 9-gon is not constructible.

(5) Prove that it is possible to trisect 72^θ by straight edge and compass.

3.10 SUGGESTED READINGS.

(1) **Topics in Algebra**; I.N HERSTEIN, John Wiley and sons, New York.

(2) **Modern Algebra**; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

MAL-511: M. Sc. Mathematics (Algebra-I)

Lesson No. 4 **Written by Dr. Pankaj Kumar**

Lesson: Field Extensions-III **Vetted by Dr. Nawneet Hooda**

STRUCTURE

4.0 Objective. Objective of this lesson is to study about normal and separable extension.

4.1 Introduction. In previous Chapter we came to know about some extension and splitting fields of polynomial f(x) in F[x] over F. There are many fields which have no proper algebraic extension; we call such field as algebraically closed fields which are studied in Section 4.2. Separable extensions are studied in Section 4.4. In Section 4.6, we study about rational symmetric functions. Now there is an interesting point "Does there exist an extension K of F such that if it has a root of an irreducible polynomial $p(x) \in F[x]$, then it contains all the root of that polynomial, We call such an extension as normal extension of F which are studied in Section 4.7.

4.2 Algebraically closed field.

4.2.1 Definition (Algebraically closed Field). Field F is called algebraically closed if it has no proper algebraic extension. i.e. if K is an algebraic extension of F then K=F.

4.2.2 Theorem. Let F be a field. Then the following conditions are equivalents:

(i) F is algebraically closed.

(ii) Every non constant reducible polynomial in F[x] is of degree 1.

(iii) Every polynomial of positive degree in F[x] can be written as the product of linear factors in F[x].

(iv) Every polynomial of positive degree in F[x] has at least one root in F.

Proof. **(i)⇒(ii)**

Let F be algebraically closed and let f(x) is an irreducible polynomial of degree n in F[x]. Since f(x) is irreducible, there exist an extension K of F such that [K:F]=n, containing at least one root of f(x). Since K is a finite extension of F, therefore, K is algebraic extension of F. But F is algebraically closed, therefore, K=F. Hence n=1 and hence every irreducible polynomial in F[x] is of degree 1.

(ii)⇒(iii)

Let f(x) be a non constant polynomial in F[x]. Then by unique factorization theorem on polynomials, polynomial f(x) can be written as the product of irreducible polynomials over F. By (ii), every irreducible polynomial is of degree 1, therefore, every polynomial over F can be written as the product of linear factor in F[x].

(iii)⇒(iv)

Let f(x) be a polynomial of degree n(≥1) over F. Then by (iii), $f(x)=\alpha(x-a_1)(x-a_2)\dots(x-a_n)$; $a_i \in F$. Since a_i's are roots of f(x) which all lies in F, proves (iv).

(iv)⇒(i)

Let K be an algebraic extension of F and k be an arbitrary element of K. let f(x) be the minimal polynomial of k over F. By (iv), f(x) has at least one root in F. let α be that root. Then $f(x)=(x-\alpha)g(x)$, where g(x) is in F[x]. On applying the same process on g(x) and continuing in this

way we get every root of f(x) lies in F. Hence k lies in F, therefore, K⊆F, but then K=F. Hence F is algebraically closed.

4.2.3 Theorem. Algebraically closed fields can not be finite.

Proof. Let F be an algebraically closed field. If possible it has finite number of element say $a_1, a_2, \ldots, a_n$. Consider the polynomial $(x-a_1)(x-a_2)\ldots(x-a_n)+1$. This is a polynomial in F[x] which has no root in F, a contradiction that F is algebraically closed. This contradiction proves that F can not be finite.

Example. The field C (field of complex numbers) is algebraically closed.

4.3 More about roots.

4.3.1 Definition. Let $f(x) = \alpha_0 x^n + ... + \alpha_{n-1}x + \alpha_n$ be a polynomial in F[x], then the derivative of f(x), written as $f'(x)$ is the polynomial $n\alpha_0 x^{n-1} + ... + \alpha_{n-1}$ in F[x].

Example. Consider the polynomial $\alpha_0 x^3 + \alpha_1$ over the field F with characteristic 3, then the derivative of this polynomial is zero over F.

4.3.2 Theorem. For f(x) and g(x) in F[x] and any α in F,

(i) $(f(x)+g(x))' = f'(x)+g'(x)$

(ii) $(\alpha f(x))' = \alpha f'(x)$

(iii) $(f(x)g(x))' = f'(x)g(x)+f(x)g'(x)$

Proof. These results can easily be proved by use of Definition 4.3.1.

4.3.3 Theorem. The polynomial f(x) in F[x] has a multiple root if and only if f(x) and $f'(x)$ have non trivial common factor.

Proof. Since we know that if f(x) and g(x) in F[x] have a non trivial common factor in some extension K of F, then they have a non trivial common factor in F[x]. So, without loss of generality suppose that all the roots of f(x) lies in F. Let α be a root of f(x) multiplicity m>1, then $f(x) = (x-\alpha)^m g(x)$. But then

$f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x) = (x-\alpha)t(x)$ i.e. (x-α) is a common factor of f(x) and $f'(x)$.

Conversely suppose that f(x) has no multiple root, then $f(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_m)$; degree of f(x)=m. Then $f'(x) = \sum_{i=1}^{m}(x-\alpha_1)...\overline{(x-\alpha_i)}...(x-\alpha_m)$, where $\overline{\ }$ denote that term is omitted. From here we see that no α_i is a root of the polynomial $f'(x) = \sum_{i=1}^{m}(x-\alpha_1)...\overline{(x-\alpha_i)}...(x-\alpha_m)$, therefore, they have no non trivial factor in common. In other words, f(x) and $f'(x)$ have a non trivial common factor if and only if f(x) has multiple root.

4.3.4 **Corollary**. If f(x) be an irreducible polynomial in F[x], then

(i) If the characteristic of F is zero, then f(x) has no multiple roots

(ii) If the characteristic of F is p≠0, f(x) has a multiple root if it of the form $f(x)= g(x^p)$.

Proof. (i)Since f(x) is irreducible, its only factors are 1 and f(x) in F[x]. Let f(x) has multiple roots, then f(x) and $f'(x)$ has a non trivial common factor. It mean $f(x) \mid f'(x)$. As $f'(x)$ is a polynomial of degree lower then f(x), the only possibility choice is that that $f'(x)=0$. But in case when characteristic of F is zero, $f'(x)$ can be 0 only when f(x) is constant polynomial. Hence f(x) has no multiple root in F.

(ii) Let $f(x) = \alpha_n x^n + ...\alpha_i x^i + \alpha x + \alpha_n$, then $f'(x) = 0$ only when $i\alpha_i = 0$; $2 \le i \le n$. Since characteristic of F is p≠0, $i\alpha_i = 0$ only when $p \mid i\alpha_i$. But p does not divide α_i, therefore p|i. Hence $i=pk_i$ for some k_i. Now $f(x) = \alpha_n x^n + ...\alpha_i x^i + \alpha_n = \alpha_n x^{pk_n} + ...\alpha_i x^{pk_i} + \alpha_n = g(x^p)$.

4.3.5 **Corollary**. If the characteristic of F is p≠0, then for all n≥ 1, the polynomial $x^p - x \in F[x]$ has distinct roots.

Proof. As the derivative of the polynomial $x^p - x = px^{p-1} - 1 = -1$ in F, the polynomial and its derivative has no non trivial factor in common. Hence polynomial $x^p - x$ has no multiple roots i.e. all the roots of the polynomial $x^p - x$ are distinct.

4.4 Separable extensions.

4.4.1 Definition. Separable polynomial. Let p(x) be an irreducible polynomial in F[x], then p(x) is called separable over F if it has no multiple root in its splitting field. In other words we say that all the roots of p(x) are distinct. Otherwise p(x) is called inseparable polynomial over F.

4.4.2 Definition. An arbitrary polynomial f(x) is separable over F, if all its irreducible factors are separable over F.

4.4.3 Definition. An element *a* in extension K of F is called separable over F, if it satisfies some separable polynomial over F. In particular, if it's minimal polynomial is separable over F.

4.4.4 Separable extension. An algebraic extension K of F is called separable extension of F if every element of K is separable over F.

Example (i). Let F be field with characteristic zero. Then every algebraic extension K of F is separable.

Solution. Let *a* be an arbitrary element of field K. Since K is algebraic extension, therefore, *a* satisfies some irreducible polynomial over F. By Corollary 4.2.4(i), this polynomial has no multiple root. Therefore, minimal polynomial of *a* over F is separable. Hence K is separable extension of F.

4.4.5 Theorem. Let characteristic of F is p(≠0). Then every algebraic extension K of F is separable if and only if the mapping $\sigma : F \to F$ given by $\sigma(a)=a^p$ is an automorphism of F.

Solution. Suppose $\sigma(a)= a^p \ \forall\ a \in F$. Then

$\sigma(a+b) = (a+b)^p = a^p + {}^pC_1 a^{p-1}b + {}^pC_2 a^{p-2}b^2 + \ldots + b^p$. But for $1 \leq i \leq p-1$, each ${}^pC_i$ is a multiple of p and hence is zero in F, therefore, $\sigma(a+b) = a^p + b^p = \sigma(a) + \sigma(b)$ and $\sigma(ab) = a^p b^p = \sigma(a)\sigma(b)$. Hence σ is a ring homomorhism on F. Further, suppose that $a^p = b^p$ which further implies that $(a-b)^p = 0$. But then a-b =0 i.e. a=b. showing that σ is one-one also. If σ is onto also, then we have b in F such that $\sigma(b)$=a i.e. b^p=a. Equivalently we say that p^{th} root of every element is also contained in F.

Now we prove theorem as: Let K be an algebraic extension of F and σ be an automorphism on F given by $\sigma(a) = a^p$. Let *a* be arbitrary element of K and g(x) be the minimal of polynomial of *a* over F. Then g(x) is irreducible polynomial over F. Let if possible g(x) has multiple roots. Since characteristic of F is p≠0, by Corollary 4.2.4(ii), $g(x)=h(x^p)= \alpha_0 x^{rp} + \ldots + \alpha_{r-1}x^p + \alpha_r$; rp=n =degree of g(x). Since with the help of σ we can identify $\alpha_i = \beta_i^p$ in F, therefore, $h(x^p)= \beta_0^p x^{rp} + \ldots + \beta_{r-1}^p x^p + \beta_r^p$. Again with the help of σ we have

$$h(x^p)= (\beta_0 x^r + \ldots + \beta_{r-1}x + \beta_r)^p .$$

Then $g(x)= (\beta_0 x^r + \ldots + \beta_{r-1}x + \beta_r)^p$ is a reducible polynomial over F, a contradiction and hence a contradiction to the assumption that g(x) is not separable. Now it follow that every algebraic extension K of F is separable.

Conversely suppose that every algebraic extension K of F is separable. We will show that $\sigma(a)=a^p$ is an automorphism on F. Since this mapping is one–one homomorphism. In order to show that σ is an automorphism, it is sufficient to show that σ is onto also. Let if possible σ is not onto i.e. there exist $a \in F$ such that $\sigma(b) \neq a$ for all b in F. In other words, there does not exist b in F such that b^p=a. Simply we say that polynomial $f(x)= x^p-a$ has no root in F. Let $\alpha_1, \alpha_2, \ldots, \alpha_p$ be the roots of x^p-a. Then $K=F(\alpha_1, \alpha_2, \ldots, \alpha_p)$ is the splitting field of f(x). Further if α and β are two roots of f(x), then $\alpha^p-a=0$ and $\beta^p-a=0$. But then $\alpha^p-\beta^p=0$. Equivalently, $\alpha=\beta$. Thus all the roots of f(x) are equal. Let $\alpha_1= \alpha_2=\ldots=\alpha_p=\alpha$. Then $K=F(\alpha)$.

Now $x^p-a = x^p- \alpha^p = (x-\alpha)^p$. Since α is algebraic over F and does not belong to F, therefore, degree of α is more than one. Let g(x) be the minimal polynomial of α over F. Since α satisfies the polynomial f(x) also, therefore, g(x) divides f(x). Let h(x) be a monic irreducible factor of f(x), then α is a root of h(x). Hence g(x)|h(x) and hence g(x)=h(x). But then $f(x)=g(x)^r$. Now $p=\deg(f(x)) = \deg(g(x)^r)=r \deg(g(x))$. Since $\deg(g(x))>1$, therefore, $\deg(g(x))=p$. Hence r=1. But then f(x) becomes the minimal polynomial for α. As f(x) has multiple roots (namely α), therefore, f(x) is inseparable polynomial. Hence α is not separable and hence K=F(α) is inseparable. Since K is algebraic extension of F which is not separable extension of F, a contradiction. This contradiction proves that σ is an automorphism on F.

4.4.6 Corollary. If F is a finite field then every algebraic extension of F is separable.

Proof. Since F is finite field, its characteristic is finite prime number p (say). Since characteristic of F is p, therefore, mapping $\sigma : F \to F$, defined by $\sigma(a)=a^p$ for all $a \in F$, is an one-one homomorphism. Since F is finite, this mapping is onto also. Hence is an automorphism on F. Now by Theorem 4.3.4, every algebraic extension of F is separable also. It proves the result.

4.4.7 Problem. Let F be a field with characteristic $p(\neq 0)$. Then element a lying in some extension of F is separable over F if and only if $F(a^p)=F(a)$.

Solution. Let K be an extension of F and $a \in K$ be separable over F. The minimal polynomial $f(x) = \beta_0 + \beta_1 x + ... + \beta_{n-1}x^{n-1} + x^n$ of *a* over F is separable. Let $g(x) = \beta_0^p + \beta_1^p x + ... + \beta_{n-1}^p x^{n-1} + x^n$. Then $g(a^p) = \beta_0^p + \beta_1^p a^p + ... + \beta_{n-1}^p a^{p(n-1)} + a^{pn}$. Since the characteristic of F is $p(\neq 0)$, therefore, $g(a^p) = (\beta_0 + \beta_1 x + ... + \beta_{n-1}x^{n-1} + x^n)^p = f(a)^p = 0$ i.e. a^p is a root of g(x). Also g(x) is irreducible over F. In fact if h(x) is a factor of g(x), then $h(x^p)$ is a factor of $g(x^p)$ in F[x]. But $g(x^p)=f(x)^p$ and f(x) is irreducible over F implies that $h(x^p) =f(x)^k$; $0 \leq k \leq p$. Since the derivative of $h(x^p)$ with

respect to x is zero over F, therefore taking derivative of $h(x^p)=f(x)^k$ on both sides, we get $kf'(x)^{k-1}=0$. But then k = 0 or p.

For k=0, h(x)=1. For k=p, $h(x^p)=f(x)^p$ i.e. $h(x^p)= g(x^p)$ and hence h(x)=g(x). Here we see that the only divisors of g(x) are 1 and g(x) itself. Hence g(x) is irreducible over F. Then $[F(a^p): F]$=n=degree of g(x). As [F(a): F]=n, we get $[F(a^p): F]=[F(a): F]$. Since $a^p \in F(a)$, therefore $F(a^p) \subseteq F(a)$. Now by above discussion $F(a^p)=F(a)$.

Conversely, let $F(a^p)=F(a)$ and suppose that a is not separable over over F. The minimal polynomial of a over F is not separable. This gives that $f(x)=g(x^p)$ and so a^p is a root of g(x). Clearly degree of g(x) is $\frac{n}{p}=m$ (say). Hence $[F(a^p): F] \le m < n$. Since $F(a^p)=F(a)$, therefore, $[F(a): F]= [F(a):F(a^p)]$ $[F(a^p): F] \le m$ i.e. n<m, which is not true. Hence a contradiction to the assumption that *a* is not separable. Hence *a* is separable over F.

4.5. Some definition.

4.5.1 Definition. Let K be field. An isomorphism from K to itself is called an automorphism on K. Two automorphisms σ and τ of K are said to be distinct if $\sigma(a) \neq \tau(a)$ for some a in K.

4.5.2 Theorem. If K is a field and if $\sigma_1, \sigma_2,...,\sigma_n$ are distinct automorphisms of K, such that $a_1\sigma_1(u)+a_2\sigma_2(u)+...+a_n\sigma_n(u)=0 \ \forall \ u \in K$ then all $a_1, a_2,...,a_n$ are 0 in K.

Proof. Let if possible we can $a_1, a_2,...,a_n$ in K, not all 0, such that $a_1\sigma_1(u)+a_2\sigma_2(u)+...+a_n\sigma_n(u)=0 \ \forall \ u \in K$. Remove all a_i=0, then after renumbering we obtain the minimal relation such that

$$a_1\sigma_1(u)+a_2\sigma_2(u)+...+a_m\sigma_m(u)=0 \qquad (1)$$

for all $u \in K$ and each $a_i \neq 0, 1 \le i \le m$.

Since $\sigma_1(u) \neq 0 \ \forall \ u \in K$, therefore, if $a_1\sigma_1(u)=0 \ \forall \ u \in K$, then a_1 must be zero in K, a contradiction that all a_i in (1) are non zero, therefore, m>1. As the

automorphisms are distinct, therefore, there exist an element c in K such that $\sigma_1(c) \neq \sigma_m(c)$. Since cu∈K, therefore, by (1)

$$a_1\sigma_1(cu) + a_2\sigma_2(cu) + ... + a_m\sigma_m(cu) = 0$$

$$\Rightarrow a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_1(u) + ... + a_m\sigma_m(c)\sigma_m(u) = 0 \qquad (2)$$

On multiplying (1) by $\sigma_1(c)$ and subtracting it from (2) we get

$$a_2(\sigma_2(c) - \sigma_1(c))\sigma_2(u) + ... + a_m(\sigma_m(c) - \sigma_1(c))\sigma_m(u) = 0 \qquad (3)$$

Since $a_m \neq 0$ and by our choice $\sigma_m(c) - \sigma_1(c) \neq 0$, therefore, we get a relation in which at least one of $a_i \neq 0$ and containing at most m-1 terms, a contradiction that (1) is the minimal relation. Hence contradiction to the assumption that $a_1\sigma_1(u) + a_2\sigma_2(u) + ... + a_n\sigma_n(u) = 0 \ \forall \ u \in K$ and at least one of $a_i \neq 0$. Therefore, if $a_1\sigma_1(u) + a_2\sigma_2(u) + ... + a_n\sigma_n(u) = 0 \ \forall \ u \in K$ then each $a_i = 0$.

4.5.3 Definition. Fix Field of G. Let G be a group of all automorphism of K, then the fixed field of G is the set of all elements 'a' of K such that $\sigma(a) = a \ \forall \sigma \in G$. In other words, the fixed field of G is the set of all elements of K which are left fixed by every element of G.

4.5.4 Lemma. Prove that fixed field of G is a subfield of K.

Proof. Let a, b be two elements of the fixed field. Then $\sigma(a) = a \ \forall \sigma \in G$ and $\sigma(b) = b \ \forall \sigma \in G$. But then $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b \ \forall \ \sigma \in G$. Hence a-b belongs to fixed field of G. As $e = \sigma(bb^{-1}) = \sigma(b)\sigma(b^{-1}) \forall \sigma \in G$ implies that $(\sigma(b))^{-1} = \sigma(b^{-1}) \forall \sigma \in G$ and $b^{-1} = (\sigma(b))^{-1} = \sigma(b^{-1}) \forall \sigma \in G$. Hence b^{-1} also belongs to the fixed field of G. Now $\sigma(ab^{-1})$ $= \sigma(a)\sigma(b^{-1}) = \sigma(a)(\sigma(b))^{-1} = ab^{-1} \ \forall \sigma \in G$ i.e. ab^{-1} belongs to fixed field of G. Hence fixed field of G is a subfield of K.

4.5.5 Definition. **Group of automorphism of K relative to F**. Let K be an extension of the field F. Then the group of automorphism of K relative to F is the set of all automorphisms of K which leaves every element of F fixed. It is

generally denoted by G(K, F) . Hence $\sigma \in G(K, F)$ if and only if $\sigma(\alpha) = \alpha$ for every α in F.

4.5.6 Lemma. Prove that G(K, F) is a subgroup of the group of all automorphisms of K.

Proof. Let $\sigma_1 \ \sigma_2 \in G(K, F)$. Then $\sigma_1(\alpha) = \alpha$ and $\sigma_2(\alpha) = \alpha$ for all $\alpha \in F$.

Since $\sigma_2(\alpha) = \alpha \Rightarrow \sigma_2^{-1}(\alpha) = \alpha \ \forall \alpha \in F$, therefore, σ_2^{-1} belongs to G(K, F).

Now $(\sigma_1\sigma_2^{-1})(\alpha) = \sigma_1(\sigma_2^{-1}(\alpha) = \sigma_1(\alpha) = \alpha \ \forall \alpha \in F$. Hence $\sigma_1\sigma_2^{-1} \in G(K, F)$ and hence G(K, F) is a subgroup of the group of all automorphism of K.

Example (i) Let K be the field with characteristic zero, then show fixed field of any group of automorphisms of K contains Q (the field of rational number).

Solution. Let H be a subgroup of group of automorphisms on K and F be fixed field of H. Then F is a subfield of K. Let $\frac{a}{b}$ be an arbitrary element of Q and σ be an arbitrary element of H. Since $1 \in F$, therefore, $\sigma(1) = 1$. Now $a = \underbrace{1+1+\cdots+1}_{\text{a times}}$, therefore, $\sigma(a) = \sigma(\underbrace{1+1+\cdots+1}_{\text{a times}}) = \underbrace{\sigma(1)+\sigma(1)+\cdots+\sigma(1)}_{\text{a times}} = a$

for all $\sigma \in H$. Hence $a \in F$. Similarly $b \in F$. As F is a field, therefore, b^{-1} and hence $ab^{-1} \in F$. $Q \subset F$.

Example (ii). Show that every automorphism σ of K, field with characteristic zero, leaves every rational number fixed.

Solution. Since Q is a prime field, Q is contained in every field with characteristic zero. Let e be the unit element of K, then e is unit element of Q also. Let σ be an arbitrary automorphism of K. Since e.e = e, therefore, $\sigma(e.e) = \sigma(e) \Rightarrow \sigma(e)\sigma(e) = \sigma(e)$, but then $\sigma(e)\sigma(e) = e.\sigma(e)$. Hence $\sigma(e) = e$.

Further $a = \underbrace{e+e+\cdots+e}_{\text{a times}}$, therefore, $\sigma(a) = \underbrace{\sigma(e)+\cdots+\sigma(e)}_{\text{a times}} = a$. Similarly,

$\sigma(b) = b$. Therefore, a and b belongs to the fixed field of group of

automorphism of K which contains σ. Hence ab^{-1} also belongs to the same fixed field. But then $\sigma(\frac{a}{b}) = \frac{a}{b} \quad \forall \frac{a}{b} \in Q$. It proves the result.

Example (iii). Let K be the field of complex numbers and F be the field of real number. Find G(K, F) and the fixed field under G(K, F).

Solution. General element of K is a+ib, a and b are real numbers. Let $\sigma \in G(K, F)$, then $\sigma(a)=a$ and $\sigma(b)=b$. Since $i^2=-1$, therefore, $\sigma(i^2)= \sigma(-1)= -1$. As $\sigma(i^2)= \sigma(i)^2= -1$, therefore, $\sigma(i)=i$ or $-i$. Then we have two elements in G(K, F), σ_1 and σ_2 where $\sigma_1(a+ib)=a+ib$ and $\sigma_2(a+ib)=a-ib$. Hence G(K, F) $=\{\sigma_1 , \sigma_2\}$. Let c+id is in the fixed field of G(K, F), then $\sigma_1(c+id)= \sigma_2(c+id)$. But then c+id=c-id, which holds only when d=0. Hence fixed field contains only real number. Here in this case the fixed field is F itself.

Example (iv). Let F=Q (the field of rational numbers) and $K=Q(2^{\frac{1}{3}})$. Find G(K, F) and the fixed field of G(K, F).

Solution. The general element of the field K is $a + b.2^{\frac{1}{3}} + c.2^{\frac{2}{3}}$, a, b, $c \in F$. Put $2^{\frac{1}{3}} = \alpha$. Then general element of K is $a + b.\alpha + c.\alpha^2$. Let $\sigma \in G(K, F)$, then $\sigma(a)=a$, $\sigma(b)=b$ and $\sigma(c)=c$. Since $\alpha^3 = 2$, therefore, $\sigma(\alpha^3) = \sigma(2) = 2$. Hence $\sigma(\alpha)^3 = 2$. As the only root of $\sigma(\alpha)^3 = 2$, $2^{\frac{1}{3}} = \alpha$, lies in K. Hence $\sigma(\alpha) = \alpha$. But then $\sigma(a + b.\alpha + c.\alpha^2) = a + b.\alpha + c.\alpha^2$ i.e. σ is identity transformation. Hence G(K, F)={I}. Trivially the fixed field of G(K, F) is K itself.

Example (v). Let F=Q and K= Q(ω), ω is primitive fifth root of unity i.e. ω satisfies the polynomial $1 + x + x^2 + x^3 + x^4$ which is irreducible over F. Therefore, General element of K is $\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3$; $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in F$. Let $\sigma \in G(K, F)$. Then ω and σ(ω) are conjugate over F i.e. σ(ω) is also a root of polynomial $1 + x + x^2 + x^3 + x^4$. Since the roots of above polynomial are ω, ω^2, ω^3, ω^4, therefore,

$\sigma(\omega)=\omega$ or ω^2 or ω^3 or ω^4. If $\sigma(\omega)=\omega^i$, $1\le i\le 4$, denote σ by σ_i. Then $G(K, F)=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. If we denote the fixed field of $G(K, F)$ by $K_{G(K,F)}$, then $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3 \in K_{G(K,F)}$ if

$$\sigma_1(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3) = \sigma_2(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)$$

$$= \sigma_3(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3) = \sigma_4(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3).$$

Using the fact that $\omega^5=1$, above equalities reduces to ,

$$\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3 = \alpha_0+\alpha_1\omega^2+\alpha_2\omega^4+\alpha_3\omega$$

$$= \alpha_0+\alpha_1\omega^3+\alpha_2\omega+\alpha_3\omega^4 = \alpha_0+\alpha_1\omega^4+\alpha_2\omega^3+\alpha_3\omega^2.$$

Since $1+\omega+\omega^2+\omega^3+\omega^4=0$, therefore, $\omega^4=-1-\omega-\omega^2-\omega^3$. But then the above equality reduces to

$$\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$$

$$= \alpha_0-\alpha_2+(\alpha_3-\alpha_2)\omega+(\alpha_1-\alpha_2)\omega^2-\alpha_2\omega^3$$

$$= \alpha_0-\alpha_3+(\alpha_2-\alpha_3)\omega-\alpha_3\omega^2+(\alpha_1-\alpha_3)\omega^3$$

$$= \alpha_0-\alpha_1-\alpha_1\omega+(\alpha_3-\alpha_1)\omega^2+(\alpha_2-\alpha_1)\omega^3.$$

These equality will hold simultaneously if $\alpha_1=\alpha_2=\alpha_3=0$. Hence the general element of $K_{G(K,F)}$ is α_0 i.e. $K_{G(K,F)}=F$.

Further, $\sigma_2(\omega)=\omega^2$, $\sigma_2^2(\omega)=\omega^4=\sigma_4(\omega)$, $\sigma_2^3(\omega)=\omega^3=\sigma_3(\omega)$ and $\sigma_2^4(\omega)=\omega=\sigma(\omega)$ i.e. $\sigma_2^4=I$ of $G(K, F)$. Hence $G(K, F)=\{\sigma_2^1, \sigma_2^2, \sigma_2^3, \sigma_2^4\}$ is a cyclic group generated by σ_2. Consider the subgroup $H = \{\sigma_1, \sigma_4\}$ of $G(K, F)$. Let $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3 \in K_H$. Then

$$\sigma_1(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3) = \sigma_4(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)$$

Equivalently,

$$\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3 = \alpha_0+\alpha_1\omega^4+\alpha_2\omega^3+\alpha_3\omega^2$$

On further simplification, we can write

$$\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$$

$$= \alpha_0-\alpha_1-\alpha_1\omega+(\alpha_3-\alpha_1)\omega^2+(\alpha_2-\alpha_1)\omega^3.$$

These two will be equal if $\alpha_1 = 0$ and $\alpha_2 = \alpha_3$. Hence general element of K_H is $\alpha_0 + \alpha_2(\omega^2 + \omega^3)$. Here we observe that index of H in G(K, F) i.e. no of distinct coset of H in G(K, F)= $[K_H:F]$.

4.5.7 **Theorem**. If K is a finite extension of F, then G(K, F) is a finite group and its order , $o(G(K, F)) \leq [K:F]$.

Proof. Let [K:F]= n with $u_1, u_2, \ldots, u_n$ is a basis of K over F. Further suppose that $f_1, f_2, ..., f_{n+1}$ are distinct automorphisms of K. Consider the system of n homogeneous equation in (n+1) variable $x_1, x_2, \ldots, x_{n+1}$ as:

$$f_1(u_1)x_1 + f_2(u_1)x_2 + ... + f_{n+1}(u_1)x_{n+1} = 0,$$
$$f_1(u_2)x_1 + f_2(u_2)x_2 + ... + f_{n+1}(u_2)x_{n+1} = 0,$$
$$.$$
$$.$$
$$.$$
$$f_1(u_n)x_1 + f_2(u_n)x_2 + ... + f_{n+1}(u_n)x_{n+1} = 0.$$

It always has a non trivial solution say $x_1=a_1, x_2=a_2, \quad x_{n+1}=a_{n+1}$, in K. Therefore,

$$f_1(u_1)a_1 + f_2(u_1)a_2 + ... + f_{n+1}(u_1)a_{n+1} = 0$$
$$f_1(u_2)a_1 + f_2(u_2)a_2 + ... + f_{n+1}(u_2)a_{n+1} = 0,$$
$$.$$
$$.$$
$$.$$
$$f_1(u_n)a_1 + f_2(u_n)a_2 + ... + f_{n+1}(u_n)a_{n+1} = 0.$$

Let u be the arbitrary element of K, then $u=\alpha_1u_1 + ... + \alpha_nu_n$; $\alpha_i \in F$. Since

$$a_1f_1(u) + a_2f_2(u) + ... + a_{n+1}f_{n+1}(u)$$
$$= \alpha_1(f_1(u_1)a_1 + f_2(u_1)a_2 + ... + f_{n+1}(u_1)a_{n+1})$$
$$+ \alpha_2(f_1(u_2)a_1 + f_2(u_2)a_2 + ... + f_{n+1}(u_2)a_{n+1})$$
$$.$$
$$.$$
$$.$$
$$+ \alpha_n(f_1(u_n)a_1 + f_2(u_n)a_2 + ... + f_{n+1}(u_n)a_{n+1}).$$

Now by above discussion,

$a_1f_1(u)+a_2f_2(u)+...+a_{n+1}f_{n+1}(u)=0 \ \forall\ u\in K$. But then by Theorem 4.5.2, each a_i=0, A contradiction and hence contradiction to the assumption that $o(G(K, F)) > [K:F]$. Hence $o(G(K, F)) \le [K:F]$.

4.6 Symmetric rational functions.

4.6.1 Definition. Ring of polynomials in n variables. Let F be a Field. An expression of the form $\Sigma\alpha_{i_1}...\alpha_{i_n}x_1^{i_1}...x_n^{i_n}$; $\alpha_{i_1},\alpha_{i_2},...\alpha_{i_n}\in F$ is called polynomial in n variables $x_1, x_2,\ldots, x_n$. The set of all such polynomials is denoted by $F[x_1, x_2,\ldots, x_n]$. If we define component wise addition as one operation and multiplication of the polynomial using distributive laws as the second operation. Then $F[x_1, x_2,\ldots, x_n]$ becomes ring.

If F is field, $F[x_1, x_2, \ldots, x_n]$ becomes an integral domain. Now we can talk about field of quotient of $F[x_1, x_2, \ldots, x_n]$. It is denoted by $F(x_1, x_2,\ldots, x_n)$. It elements are quotient of polynomials from the ring $F[x_1, x_2, \ldots, x_n]$. Let S_n be the symmetric group of degree n considered to be acting on the set {1, 2, …, n}. Let $r(x_1, ..., x_n)\in F(x_1, ..., x_n)$. Define the action of $\sigma\in S_n$ on $r(x_1, ..., x_n)$ by $\sigma(r(x_1, ..., x_n)) = r(x_{\sigma(1)}, ..., x_{\sigma(n)})$. Now we define:

4.6.2 Symmetric rational function. Let $r(x_1, ..., x_n)\in F(x_1, ..., x_n)$. Then $r(x_1, ..., x_n)$ is called symmetric rational function in $F(x_1, ..., x_n)$ if $\sigma(r(x_1, ..., x_n)) = r(x_1, ..., x_n)$ for all $\sigma\in S_n$. In other words, these are the rational functions which are left fixed by S_n. Since symmetric rational functions lies in the fixed field of S_n. They form subfield of $F(x_1, ..., x_n)$. Let S denote the field of symmetric rational functions.

Example. Function given below are elementary rational function..

(i) If $a_1 = x_1 + x_2$, $a_2 = x_1x_2$, then a_1, a_2, are elementary symmetric functions in x_1 and x_2.

(ii) If $a_1 = x_1 + x_2 + x_3$, $a_2 = x_1x_2 + x_2x_3 + x_3x_1$, $a_3 = x_1x_2x_3$, then a_1, a_2,

a_3, are elementary symmetric functions in x_1, x_2 and x_3.

(iii) If $a_1 = x_1 + x_2 + x_3 + x_4$, $a_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$, $a_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$, $a_4 = x_1x_2x_3x_4$, then a_1, a_2, a_3, a_4 are elementary symmetric functions in x_1, x_2, x_3 and x_4.

(iv) If $a_1 = \sum_{i=1}^{n} x_i$, $a_2 = \sum_{i<j} x_ix_j$, $a_3 = \sum_{i<j<k} x_ix_jx_k, \ldots, a_n = \prod_{i=1}^{n} x_i$, then a_1, a_2, $a_3, \ldots, a_n$, are elementary symmetric functions in x_1, $x_2, \ldots, x_n$.

4.6.3 Theorem. Let F be field and $F(x_1, \ldots, x_n)$ be the field of rational functions in $x_1, \ldots, x_n$ over F. Suppose that S is the field of symmetric rational functions; then

(i) $[F(x_1, \ldots, x_n) : S] = n!$

(ii) $G(F(x_1, \ldots, x_n), S) = S_n$, the symmetric group of degree n.

(iii) If $a_1, a_2, \ldots, a_n$ are the elementary symmetric functions in $x_1, x_2, \ldots, x_n$, then $S = F(a_1, \ldots, a_n)$.

(iv) $F(x_1, \ldots, x_n)$ is the splitting field of over $F(a_1, \ldots, a_n) = S$ of the polynomial $t^n - a_1t^{n-1} + a_2t^{n-2} \ldots + a_n(-1)^n$.

Proof. (i) As S_n is the symmetric group of degree n on set {1, 2,…, n} and $G(F(x_1, \ldots, x_n), S)$ is a group of automorphisms of $F(x_1, \ldots, x_n)$ which leaves every element of S fixed. Let $r(x_1, \ldots, x_n) \in S$. Then by definition of symmetric rational function, for $\sigma \in S_n$, $\sigma(r(x_1, \ldots, x_n)) = r(x_1, \ldots, x_n)$ $\forall\, r(x_1, \ldots, x_n) \in S$. But then by definition 4.5.5, $\sigma \in G((F(x_1, \ldots, x_n), S)$. Hence $o(G(F(x_1, \ldots, x_n), S) \geq n!$. By Theorem 4.5.7,

$$[F(x_1, \ldots, x_n) : S] \geq o(G(F(x_1, \ldots, x_n), S) \geq n! \qquad (*)$$

As $a_1, a_2, \ldots, a_n$ are elementary symmetric functions in $x_1, x_2, \ldots, x_n$, therefore, $a_1, a_2, \ldots, a_n$ are contained in S. But then $F(a_1, a_2, \ldots, a_n) \subseteq S$. Hence

$$[F(x_1, \ldots, x_n) : F(a_1, \ldots, a_n)] = [F(x_1, \ldots, x_n) : S][S : F(a_1, \ldots, a_n)] \qquad (**)$$

Consider the polynomial

$$t^n - a_1 t^{n-1} + a_2 t^{n-2} ... + (-1)^n a_n .$$

It is polynomial over $F(a_1, ..., a_n)$. Since $a_1, a_2, \ldots, a_n$ are elementary symmetric functions in $x_1, x_2, \ldots, x_n$, therefore, we have

$$t^n - a_1 t^{n-1} + a_2 t^{n-2} ... + (-1)^n a_n = (t - x_1)(t - x_2)...(t - x_n) .$$

Here we see that $x_1, x_2, \ldots, x_n$ are the roots of above polynomial, therefore, $F(x_1, ..., x_n)$ is splitting field of $t^n - a_1 t^{n-1} + a_2 t^{n-2} ... + (-1)^n a_n$, proving (iv). Further we know that if K is the splitting field of some polynomial f(x) of degree n over the field F, then [K:F]≤n! . Hence

$$[F(x_1, ..., x_n) : F(a_1, ..., a_n)] \leq n!$$

(***)

By (*) and (**) we get that

$$[F(x_1, ..., x_n) : F(a_1, ..., a_n)] \geq n!$$

Using (***), we get $[F(x_1, ..., x_n) : F(a_1, ..., a_n)] = n!$.

But then

$$[F(x_1, ..., x_n) : S][S : F(a_1, ..., a_n)] = n! .$$

Since by (*), $[F(x_1, ..., x_n) : S] \geq n!$, therefore, we get $[F(x_1, ..., x_n) : S] = n!$ and $[S : F(a_1, ..., a_n)] = 1$ i.e. $S = F(a_1, ..., a_n)$, proving (i) and (iii).

Further, n!=$[F(x_1, ..., x_n) : S] \geq o(G(F(x_1, ..., x_n), S) \geq n!$ implies that $o(G(F(x_1, ..., x_n), S) = n!$, proving (i).

4.6.4 **Note**.(i) By above theorem we come to know that symmetric rational functions in n variables is a rational function in the elementary symmetric functions of these variables. More sharply we can say that: A symmetric polynomial in n variables is a polynomial in their elementary symmetric functions.

4.7 Normal extension.

4.7.1 **Defnition. Normal extension.** A finite extension K of field F is called normal extension of F if the fixed field under G(K, F) is F itself.

Example. In 4.5.6, as discussed in example (iii) and (v), K is a normal extension of F while in example (iv), K is not a normal extension of F.

4.7.2 Theorem. Let K be a normal extension of F and let H be a subgroup of G(K, F); let $K_H = \{x \in K \mid \sigma(x)=x \ \forall \ \sigma \in H\}$ be the fixed field under H. Then (i) $[K: K_H]=o(H)$. (ii) $H=G(K, K_H)$.

Proof. Since H leaves every element of K_H fixed, therefore, $H \subseteq G(K, K_H)$. Hence $o(G(K, K_H)) \geq o(H)$. Moreover $[K: K_H] \geq o(G(K, K_H))$. Hence $[K:K_H] \geq o(H)$. As K_H is a subfield of K, we can find $a \in K$ such that $K=K_H(a)$; this a must therefore satisfy an irreducible polynomial over K_H of degree $m=[K: K_H]$ and no nontrivial polynomial of lower degree. Let $\sigma_1, \sigma_2, \ldots, \sigma_h$ be the distinct elements of H, where σ_1 is the identity of G(K, F). Then $o(H)=h$. Consider the following functions:

$$\alpha_1 = \sum_{i=1}^{n} \sigma_i(a), \ \alpha_2 = \sum_{i<j} \sigma_i(a)\sigma_j(a), \ \ldots, \ \alpha_n = \prod_{i=1}^{n} \sigma_i(a).$$

Let $\sigma \in H$, then $\sigma\sigma_1, \sigma\sigma_2, ..., \sigma\sigma_h$ are all distinct elements of H. Hence $\{\sigma\sigma_1, \sigma\sigma_2, ..., \sigma\sigma_h\} = \{\sigma_1, \sigma_2, ..., \sigma_h\}$. Now

$$\sigma(\alpha_1) = \sigma(\sum_{i=1}^{n} \sigma_i(a)) = \sum_{i=1}^{n} \sigma\sigma_i(a) = \sum_{i=1}^{n} \sigma_i(a) \ \forall \sigma \in H,$$

α_1 remains invariant under every $\sigma \in H$ and hence belongs to K_H. Similarly each α_i belongs to K_H.

Consider the polynomial

$$(x - \sigma_1(a))(x - \sigma_2(a))...(x - \sigma_h(a)) = x^h - \alpha_1 x^{h-1} + ... + (-1)^h \alpha_h .$$

The roots of this polynomial are $a = \sigma_1(a), \ \sigma_2(a), \ ..., \sigma_h(a)$. As $\alpha_i \in K_H$, $x^h - \alpha_1 x^{h-1} + ... + (-1)^h \alpha_h$ is a polynomial over K_H with a as its root. Since the degree of minimal polynomial of a is m, therefore, $h \geq m$. Hence $[K:K_H] \leq o(H)$. Now by above discussion, $[K:K_H] = o(H)$. Further $o(H)= [K:K_H] \geq o(G(K, K_H)) \geq o(H)$ implies that $o(H)=o(G(K, K_H))$. Hence $H=G(K, K_H)$.

4.7.3 Note. Let K be a normal extension of F, then $K_{G(K, F)}=F$ and $[K: K_{G(K, F)}] = o(G(K, F))$.

4.7.4 **Theorem**. Let K be finite extension of field F, characteristic F is zero. Then K is a normal extension of F if and only if K is splitting field of some polynomial over F.

Proof. Since characteristic of K is zero; K is simple extension of F. Hence K=F(a) for some $a \in$K. Let σ_1, σ_2, …, σ_n are distinct elements of G(K, F) where σ_1 is the identity of G(K, F). Consider the following functions:

$$\alpha_1 = \sum_{i=1}^{n} \sigma_i(a),\ \alpha_2 = \sum_{i<j} \sigma_i(a)\sigma_j(a),\ \ldots,\ \alpha_n = \prod_{i=1}^{n} \sigma_i(a).$$

Then it is easy to see that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are elementary symmetric functions in $\sigma_1(a)$, $\sigma_2(a)$ …,$\sigma_n(a)$(show that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are elementary symmetric functions in $\sigma_1(a)$, $\sigma_2(a)$ …,$\sigma_n(a)$)

Let us suppose that K is normal extension of field F. Then by definition of normal extension, F is fixed field of G(K, F). Consider the polynomial

$$(x-\sigma_1(a))(x-\sigma_2(a))\ldots(x-\sigma_n(a)) = x^n - \alpha_1 x^{n-1} + \ldots + (-1)^n \alpha_n .$$

The roots of this polynomial are $a = \sigma_1(a),\ \sigma_2(a),\ \ldots, \sigma_n(a)$. Since each α_i is left fixed by each $\sigma \in$G(K, F) and hence belongs to fixed field F of G(K, F). Therefore, $x^n - \alpha_1 x^{n-1} + \ldots + (-1)^n \alpha_n \in F[x]$. Since $a \in$K and σ_i is an automorphism on K, $\sigma_i(a)$ also belongs to K. As K is smallest field containing all the roots of the polynomial $x^n - \alpha_1 x^{n-1} + \ldots + (-1)^n \alpha_n \in F[x]$, K is splitting field of $x^n - \alpha_1 x^{n-1} + \ldots + (-1)^n \alpha_n$ over F. Hence K is splitting field of some polynomial over F.

Conversely, suppose that K is splitting field of polynomial f(x) over F. We want to show that K is normal extension of F. We proceed by applying induction on [K: F]=n. If n=1, then K=F. Since fixed field of G(K, F) is contained in K=F and contains F, therefore, fixed field of G(K, F) is F itself and the result is true in this case. Assume that result is true for any pair of fields K_1 and F_1 of degree less then n that when ever K_1 is

splitting field of some polynomial over F_1, then K_1 is normal extension of F_1 also.

If f(x) $\in$F[x] split into linear factors over F, then K=F, which is certainly a normal extension of F. So, assume that f(x) has an irreducible factor p(x) $\in$F[x] of degree r >1. Since every irreducible polynomial over the field of characteristic zero has no multiple roots, let $\alpha_1, \alpha_2, ..., \alpha_r$ are distinct roots of p(x) all lies in K. Consider the field $F(\alpha_1)$. Since $F \subset F(\alpha_1)$, therefore, $f(x) \in F(\alpha_1)[x]$. But then K is splitting field of f(x) over $F(\alpha_1)$ also. Since $[K:F]=[K:F(\alpha_1)][F(\alpha_1):F]$ and $[F(\alpha_1):F]=r>1$, we have $[K:F(\alpha_1)]<[K:F]$. Hence by induction hypothesis K is normal extension of $F(\alpha_1)$ and Hence fixed field of $G(K, F(\alpha_1))=F(\alpha_1)$.

Let $\omega \in K$ be arbitrary element which is left fixed by every $\sigma \in G(K, F)$. We will show that $\omega \in F$. Let $\sigma_1 \in G(K, F(\alpha_1))$, then σ_1 leaves every element of , $F(\alpha_1)$ fixed and hence also leaves every element of F fixed, therefore, $\sigma_1 \in G(K, F)$. Then by assumption $\sigma_1(\omega) = \omega$ for every $\sigma_1 \in G(K, F(\alpha_1)$ and hence belong to the fixed field $F(\alpha_1)$ of $G(K, F(\alpha_1))$. Since every element of $F(\alpha_1)$ is of the form $\beta_{r-1}\alpha_1^{r-1} + \beta_{r-2}\alpha_1^{r-2} + ... + \beta_0;\ \beta_{r-1}, ..., \beta_0 \in F$, we have

$\omega = \beta_{r-1}\alpha_1^{r-1} + \beta_{r-2}\alpha_1^{r-2} + ... + \beta_0$. Since we always have an automorphism $\sigma_i \in K$ such that $\sigma_i \in G(K, F)$ and $\sigma_i(\alpha_1) = \alpha_i$. Further by our choice $\sigma_i(\omega) = \omega$, and $\sigma_i(\beta) = \beta\ \forall\ \beta \in F$ we have

$$\omega = \sigma_i(\omega) = \beta_{r-1}\sigma_i(\alpha_1^{r-1}) + \beta_{r-2}\sigma_i(\alpha_1^{r-2}) + ... + \beta_0 .$$

Equivalently, $\beta_{r-1}\alpha_i^{r-1} + \beta_{r-2}\alpha_i^{r-2} + ... + \beta_0 - \omega = 0;\ i = 1, 2, ..., r$.

Thus the polynomial $\beta_{r-1}x^{r-1} + \beta_{r-2}x^{r-2} + ... + \beta_0 - \omega$ of degree at most r -1 has α_1, α_2, …, α_r as r distinct root. This is possible only when all the coefficients of the polynomial are zero; in particular $\beta_0 - \omega$ =0. Hence $\omega = \beta_0 \in F$ and hence F is the fixed field of G(K, F) i.e. K is normal extension of F.

4.7.5 Corollary. If K is an extension of field F(characteristic F=0) such that [K: F]=2, then K is normal extension of F.

Proof. Since characteristic of F is zero, therefore, K=F(a) for some $a \in$K. It is given that [K:F]=2, therefore, a satisfies an irreducible polynomial of degree two. Let f(x)=x^2+bx+c be its minimal polynomial of a over F. One of the root of f(x) is a and v be another root of f(x). But then $v + a = -b \Rightarrow v = -b - a$ which lies in K. Hence all the root of f(x) lies in K. Since K is smallest extension which contains all the root of f(x), K becomes splitting field of the polynomial f(x). Hence by Theorem 4.7.4, K is a normal extension of F

Example. Show by an example that normal extension of normal extension of a field need not be a normal extension of that field. In other words if L is normal extension of K and K is normal extension of F, then L may not be a normal extension of F.

Solution. Let F=Q(field of rational numbers), K=$Q(\sqrt{2})$ and L=$Q(2^{\frac{1}{4}})$. Since $\sqrt{2}$ satisfies an irreducible polynomial x^2-2 over F, [K: F]=2. Then by Corollary 4.7.5, K is normal extension of F.

As $2^{\frac{1}{4}} \notin Q(\sqrt{2})$ and satisfies the polynomial $x^2 - \sqrt{2}$ over $Q(\sqrt{2})$, therefore, $[Q(2^{\frac{1}{4}}) : Q(\sqrt{2})]$=2. Again by Corollary 4.7.5, L is normal extension of K.

Since $2^{\frac{1}{4}}$ satisfies the polynomial x^4-2 over F which is irreducible over Q. Its roots are $2^{\frac{1}{4}}$, $-2^{\frac{1}{4}}$, $i2^{\frac{1}{4}}$ and $-i2^{\frac{1}{4}}$. Since the imaginary root of polynomial x^4-2 does not lies in L=$Q(2^{\frac{1}{4}})$, L is not splitting field of x^4-2 over Q. Hence L is not a normal extension of F.

4.8 KEY WORDS.

Normal, Separable, splitting field, rational, Algebraically closed, Symmetric.

4.9 SUMMARY. In this chapter, we study algebraically closed fields, rational symmetric functions, normal extensions and fixed fields.

4.10 SELF ASSESMENT QUESTIONS.

(1) Prove that every automorphism on K must leave rational number fixed.

(2) If K is an extension of field F, char $F=p\neq 0$ and $a\in K$ is separable over F, then F(a) is separable extension of F.

(3) Prove that for given fields $F\subseteq L\subseteq K$, if K is separable over F, then it is separable over L also.

4.11 SUGGESTED READINGS.

(1) **Topics in Algebra**; I.N HERSTEIN, John wiley and sons, New York.

(2) **Modern Algebra**; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(3) **Basic Abstract Algebra**; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.

MAL-511: M. Sc. Mathematics (Algebra-I)

Lesson No. 5 **Written by Dr. Pankaj Kumar**

Lesson: Galois Theory and Finite Fields **Vetted by Dr. Nawneet Hooda**

STRUCTURE

5.0 Objective. Objective of this chapter is to study the Fundamental Theory of Galois. With the help of splitting field K of polynomial f(x) over the field F, Galois Group G(K,F) of the polynomial f(x) is obtained in order to see that the general polynomial of degree n>4 is not solvable by radicals.

5.1 Introduction. In this chapter, we study about perfect fields in the Section 5.2. In next section, we study about Galois group of a polynomial and Galois Theory. In Section 5.4, by the use of Galois Theory, we see that general polynomial of degree $n > 4$ is not solvable by radicals. As there are polynomials (for example x^2+1, x^2+x+1 having primitive second root of unity and primitive third root of unity) whose all roots are primitive n^{th} roots of unity called as n^{th} cyclotomic polynomials, are studied in Section 5.5. In last section we study about finite fields and show that for given prime p and positive integer n, there always exist a finite field of order p^n.

5.2 Perfect field.

5.2.1 Definition. A field F is called perfect if all finite extensions of F are separable.

5.2.2 Theorem. Prove that any field of characteristic 0 is perfect.

Proof. Let F be a field with 0 characteristic. Let K be finite extension of F. Then K is algebraic extension of F also. Therefore, every element k of K satisfies some irreducible polynomial over F. Since characteristic of F is 0, therefore, every irreducible polynomial is separable over F. Hence every element k of K is separable over F. i.e. K is separable extension of F. Therefore, every finite extension K of F is separable over F. i.e. F is perfect field.

5.2.3 Theorem. Prove that a field F of characteristic p ($\neq 0$) is perfect if and only for every $a \in$ F , we can find b in F such that $b^p = a$.

Proof. Proof follows from Theorem 4.4.5.

5.3 Galois Theory.

5.3.1 Definition. **Galois Group.** Let K be the splitting field of some polynomial f(x) over F. The Galois Group of f(x) is the group of all automorphisms of K leaving every element of F fixed.

5.3.2 Lemma. If K is a normal extension of field F(characteristic of F =0) and T is a subfield of K containing F, then T is normal extension of F if and only if $\sigma(T) \subseteq T$ for all $\sigma \in$ G(K, F).

Proof. Since K is normal extension of F, therefore, K is a finite extension of F. Hence T is also a finite extension of F. Since the characteristic of T is zero, therefore, T=F(a) for some a in T. Suppose that T is normal extension of F. Then to prove that $\sigma(T) \subseteq T$ for all $\sigma \in$ G(K, F).

Since T is normal extension of F, therefore, G(T, F) is a finite subgroup of G(K, F). Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be the m distinct elements of G(T, F) where σ_1 is identity element. Since $\sigma_1(a), \ldots, \sigma_m(a)$ are the elements of T, consider the polynomial $p(x) = (x-\sigma_1(a))\ldots(x-\sigma_m(a)) = x^m - \alpha_1 x^{m-1} + \ldots + (-1)^m \alpha_m$ where $\alpha_1, \alpha_2, \ldots, \alpha_m$ are elementary symmetric function in $\sigma_1(a), \ldots, \sigma_m(a)$. Further each α_i is invariant under elements of G(T, F). Since T is normal extension of F, therefore, each α_i belongs to F. Hence p(x) is a polynomial

over F with *a* as its root lying in K. Now for $\sigma \in G(K, F)$, $\sigma(a)$ is also a root of p(x). But all the roots of p(x) lies in T, therefore, $\sigma(a) \in T$. Since T=F(a) and [T: F]=*o*(G(T, F))=m, the arbitrary element t of T is of the form

$$t = \beta_1 a^{m-1} + \beta_2 a^{m-2} + ... + \beta_m ; \beta_1, \beta_2, ... \beta_m \in F .$$

Then for $\sigma \in G(K, F)$,

$$\sigma(t) = \sigma(\beta_1 a^{m-1} + \beta_2 a^{m-2} + ... + \beta_m)$$

$$= \sigma(\beta_1)\sigma(a)^{m-1} + \sigma(\beta_2)\sigma(a)^{m-2} + ... + \sigma(\beta_m)$$

$$= \beta_1 \sigma(a)^{m-1} + \beta_2 \sigma(a)^{m-2} + ... + \beta_m .$$

By above discussion, $\sigma(t) \in T \ \forall \ \sigma \in G(K, F)$. Hence $\sigma(T) \subseteq T \ \forall \sigma \in G(K, F)$.

Now suppose that $\sigma(T) \subseteq T \ \forall \sigma \in G(K, F)$, we will show that T is normal extension of F. Since K is normal extension of F, therefore, G(K, F) is finite. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n distinct elements of G(K, F) where σ_1 is identity element. Since T=F(a) for some a in T and $\sigma(T) \subseteq T \ \forall \sigma \in G(K, F)$, we get that $\sigma_1(a), \ldots, \sigma_n(a)$ are the elements of T. Consider the polynomial $f(x) = (x-\sigma_1(a))\ldots(x-\sigma_n(a)) = x^n - \alpha_1 x^{n-1} + ... + (-1)^m \alpha_n$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are elementary symmetric function in $\sigma_1(a), \ldots, \sigma_n(a)$. Further each α_i is invariant under elements of G(K, F). Since K is normal extension of F, therefore, each α_i belongs to F. Hence f(x) is a polynomial over F with *a* as its root lying in T. Since *a* is a root of f(x) and T=F(a) is the smallest field containing all the roots of f(x), T becomes splitting field of polynomial $f(x) \in F[x]$. Hence T is normal extension of F.

5.3.3 Theorem. Show that Galois group of a polynomial over a field is isomorphic to a subgroup of group of permutation of its root.

Proof. Let f(x) be a polynomial over the field F. Let K be the splitting field of f(x) over F. Then K is normal extension of F. Therefore, the Galois group G(K, F) of f(x) is of finite order [K:F]= n, say. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n distinct elements of G(K, F). Let $S=\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be the set of m distinct roots of f(x) in K and P be the set of all those permutations on S which changes only those elements of S which are not in F i.e. P is the set of all those permutations on S which leaves every element of F fixed. If ψ_1 and ψ_2

are two elements of P then the composite mapping $\psi_1\psi_2$ also fixes every element of F. But then $\psi_1\psi_2 \in P$. Equivalently, we have shown that P is a subgroup of group of all permutations on S.

Let $\sigma \in G(K, F)$. Take σ^* as the restriction of σ to S. If α is a root of f(x) in K, then $\sigma(\alpha) = \sigma^*(\alpha)$ is also a root of f(x) in K. Since S is the set of all the root of f(x), therefore, $\sigma^*(\alpha) \in S$. Hence σ^* is a function from S to S. Being a restriction of σ, σ^* is a one-one and onto mapping which leaves every element of F fixed. Hence $\sigma^* \in P$.

Define a mapping θ from G(K, F) to P by

$$\theta(\sigma) = \sigma^* \quad \forall\ \sigma \in G(K, F)$$

θ is one-one. Let σ_1 and σ_2 belongs to G(K, F). If $\theta(\sigma_1) = \theta(\sigma_2)$, then $\sigma_1^* = \sigma_2^*$. But then $\sigma_1^*(\alpha) = \sigma_2^*(\alpha)$ for all $\alpha \in S$. Equivalently, $\sigma_1(\alpha) = \sigma_2(\alpha)$ for all $\alpha \in S$. Since $K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$, therefore, every element of K can be obtained from F and $\alpha_1, \alpha_2, \ldots, \alpha_m$. Hence if $\beta \in K$, then $\sigma_1(\beta) = \sigma_2(\beta)$ for all $\beta \in K$. Hence $\sigma_1 = \sigma_2$. Therefore, mapping θ is one-one.

θ is onto. Let g be any element of P. Then g is a permutation on S leaving those elements of elements of S fixed which are in F. Obtain an extension mapping g^* of g. i.e. a mapping such that $g^*(\alpha) = g(\alpha)$ for all α belonging to S and which leaves every element of F fixed. Clearly such a mapping g^* is obtainable in G(K, F) because $K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$. Hence mapping θ is onto also.

θ is homomorphism. Let σ_1 and σ_2 belongs to G(K, F). Then $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)^*$, the restriction of $\sigma_1\sigma_2$ on S. But then

$$(\sigma_1\sigma_2)^*(\alpha) = \sigma_1\sigma_2(\alpha) = \sigma_1(\sigma_2(\alpha)) = \sigma_1(\sigma_2^*(\alpha)) = \sigma_1^*\sigma_2^*(\alpha) \quad \forall\ \alpha \in S.$$

Hence $(\sigma_1\sigma_2)^* = \sigma_1^*\sigma_2^*$ and hence $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)^* = \sigma_1^*\sigma_2^* = \theta(\sigma_1)\theta(\sigma_2)$, proving that θ is an isomorphism from G(K, F) to P.

5.3.4 Theorem. Let f(x) be a polynomial in F[x], K its splitting field over F and G(K,F) its Galois group. For any subfield T of K which contain F, let G(K,T) $=\{\sigma\in G(K, F)|\ \sigma(t)=t$ for every $t\in T\}$ and for any subgroup H of G(K, F) let $K_H=\{x\in K|\ \sigma(x)=x$ for every $\sigma\in T\}$. Then association of T with G(K, T) sets up a one-one correspondence of the set of subfield of K containing F onto the set of subgroup of G(K, F) such that

(i) $T=K_{G(K, T)}$

(ii) $H=G(K, K_H)$

(iii) [K:T]=o(G(K, T)), [T:F]= index of G(K, T) in G(K, F)

(iv) T is normal extension of F if and only if G(K, T) is a normal subgroup of G(K, F).

(v) When T is normal extension of F, then G(T, F) is isomorphic to G(K, F)/ G(K, T).

Proof. (i) By Theorem 4.7.2, if K is a normal extension of F, H is a subgroup of G(K, F) and K_H is the fixed field under H. Then $[K: K_H] = o(H)$ and $H=G(K, K_H)$. It is given that K is the splitting field of polynomial f(x) over F. Since $F\subseteq T$, therefore, $f(x)\in T[x]$. But then K is splitting field of f(x) over T. Hence K is normal extension of T also. Therefore $K_{G(K,T)}=T$.

(ii) Again by Theorem 4.7.2, $H=G(K, K_H)$. (write prove the theorem 4.7.2). By this theorem we get that any subgroup of G(K, F) is of the form G(K,T) corresponding to the subfield T of K containing F. Define a mapping from the set of all subfields of K containing F and the set of all subgroup of G(K,F) by setting $\phi(T)=G(K,T)$. This is an onto mapping as for given subgroup G(K,T) we have T as its fixed field. This is one-one mapping as if $\phi(T_1)=\phi(T_2)$, then $G(K,T_1)= G(K,T_2)$. But then $K_{G(K,T_1)} = K_{G(K,T_2)}$. Since T_1 and T_2 are subfield of K containing F, by (i) $T_1 = T_2$. Hence there is one to one correspondence between the set of all subfields of K containing F and the set of all subgroup of G(K,F).

(iii) Since K is normal extension of T, therefore, by Theorem 4.8.2, $[K:T] = o(G(K,T))$. Further K is normal extension of F, therefore, $[K: F]= oG(K,F)$. As K is finite extension of T and T is finite extension of F, therefore, [K:F]=[K:T][T:F]. Equivalently $o(G(K,F))=[K:T]\ o(G(K,T))$ i.e. $[K:T]= o(G(K,F))/\ o(G(K,T))$= index of G(K,T) in G(K, F).

(iv) By Theorem 5.3.2, T is normal extension of F if and only if

$\sigma(T)\subseteq T$ for all $\sigma\in G(K, F)$.

As K is normal extension of T, therefore, fixed field of G(K,T) is T itself. Therefore, T is normal extension of F

if and only if $\tau(\sigma(t))= \sigma(t)$ for all $t\in T$, $\sigma\in G(K, F)$ and $\tau\in G(K,T)$

if and only if $\sigma^{-1}\tau\sigma(t)=(t)$ for all $t\in T$, $\sigma\in G(K, F)$ and $\tau\in G(K,T)$.

But then by definition of G(K,T), $\sigma^{-1}\tau\sigma\in G(K,T)$ for all $\sigma\in G(K, F)$ and $\tau\in G(K,T)$. Hence T is normal extension of F

if and only if $\sigma^{-1}\tau\sigma\in G(K,T)$ for all $\sigma\in G(K, F)$ and $\tau\in G(K,T)$

if and only if G(K,T) is normal subgroup of G(K, F).

Hence T is normal extension of F if and only if G(K,T) is normal subgroup of G(K, F).

(v) It is given that T is normal extension of F. But By 5.3.2, T is normal extension of F if and only if $\sigma(T))\subseteq T$ for all $\sigma\in G(K, F)$. Let σ^* be the restriction of σ on T i.e. $\sigma^*(t) = \sigma(t)$ for every $t\in T$. Since σ leaves every element of F fixed, therefore, σ^* also leaves every element of F fixed and hence $\sigma^*\in G(T, F)$. Define a mapping $\psi : G(K, F)\rightarrow G(T, F)$ by $\psi(\sigma)=\sigma^*$. The mapping is well defined as if $\sigma_1=\sigma_2$, $\sigma_1(k)=\sigma_2(k)$ for every $k\in K$. But then $\sigma_1(t)=\sigma_2(t)$ for every $t \in T$. Equivalently, $\sigma_1^*(t) = \sigma_2^*(t)$. Hence $\sigma_1^* = \sigma_2^*$ and hence $\psi(\sigma_1)= \psi(\sigma_2)$ i.e. mapping is well defined.

Since $(\sigma_1\sigma_2)^*(t)=(\sigma_1\sigma_2)(t)=\sigma_1(\sigma_2(t))=\sigma_1(\sigma_2^*(t))=\sigma_1^*(\sigma_2^*(t))=\sigma_1^*\sigma_2^*(t)$

$\forall\ t\in T$, therefore, $(\sigma_1\sigma_2)^*= \sigma_1^*\sigma_2^*$. Then $\psi(\sigma_1\sigma_2)=(\sigma_1\sigma_2)^*=\sigma_1^*\sigma_2^*= \psi(\sigma_1)\psi(\sigma_2)$ i.e. ψ is an homomorphism of G(K,F) into G(T,F). By fundamental theorem on homomorphism, $\frac{G(K,F)}{\text{Ker}\,\psi}\cong\psi(G(K,F))$. Now we evaluate Ker ψ. Let $\sigma\in$ Ker ψ, then $\psi(\sigma)=I$, where I is the identity of G(T,F). Then $\sigma^*=I$ i.e. $\sigma^*(t)=t$ for every t in T. Since $\sigma^*(t)= \sigma(t)=t$, therefore, $\sigma\in G(K, T)$ and vice versa. Hence $\frac{G(K,F)}{G(K,T)}\cong\psi(G(K,F))$. Further $o(\frac{G(K,F)}{G(K,T)})= \frac{o(G(K,F))}{o(G(K,T))}$ = [T:F] (by (iii)). Since [T: F]=o(G(T: F). Therefore, image of G(K, F) in G(T, F) is all of G(T, F). Hence $\frac{G(K,F)}{G(K,T)}\cong G(T,F)$. It completes the proof of theorem.

5.4 Solvability by radicals.

Consider general quadratic polynomial $x^2+a_1x+a_2$ over the field F. This polynomial then can be taken over the field $F(a_1, a_2)$, extension of F obtained by adjoining a_1 and a_2 to F. Let α and β are its roots, then $\alpha = -a_1 + \sqrt{a_1^2 - 4a_2}$ and $\beta = -a_1 - \sqrt{a_1^2 - 4a_2}$. We see that there is a formula, which expresses the roots of p(x) in terms of a_1 and a_2 and square roots of rational functions of these.

Consider general qubic polynomial $t(x)=x^2+a_1x^2+a_2x+a_3$. Then by Cardan's formula if we let

$$p = a_2 - \frac{a_1^2}{3}, \qquad q = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + a_3, \qquad P = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$ and

$Q=\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$ (with cube roots chosen properly) then the roots of equation $x^2+a_1x^2+a_2x+a_3$ are $P + Q - \frac{a_1}{3}$, $\omega P + \omega^2 Q - \frac{a_1}{3}$, $\omega^2 P + \omega Q - \frac{a_1}{3}$; $\omega(\neq 1)$ is cube root of unity. We see that there is a formula, which expresses the roots of p(x) in terms of a_1 and a_2 and square roots of rational functions of these. Similarly we obtain the roots of q(x) in terms of a_1, a_2 , a_3 , by taking relations between square roots and cube root of rational function in a_1, a_2 and a_3. Now the over all observation is that we can obtain an extension of $F(a_1,a_2$, $a_3)$ by adjoining square root and then a cube root to $F(a_1,a_2$, $a_3)$, which contains all the roots of q(x). Similar formula can be obtained for bi-quadratic equations. Can we obtain such an formula for fifth degree equations. ? The answer is no. In mathematical terms we say that every polynomial of degree

less then or equal to four is solvable by radical while general polynomial of degree more than four is not solvable by radicals.

5.4.1 Definition. For given field F, polynomial p(x) in F[x] is solvable by radicals over F if we can find a sequence of fields $F_1=F(\omega_1)$, $F_2=F_1(\omega_2)$, …, $F_k=F_{k-1}(\omega_k)$ $=F(\omega_1, \omega_2,\ldots, \omega_k)$ such that $\omega_1^{n_1} \in F$, $\omega_2^{r_2} \in F_1, \ldots, \omega_k^{n_k} \in F_{k-1}$ such that the roots of p(x) all lies in F_k.

5.4.2 Remark. If K is the splitting field of p(x) over F, then p(x) is solvable by radical over F if we can find a sequence of fields $F \subseteq F_1=F(\omega_1) \subseteq F_2=F_1(\omega_2) \subseteq$ $\ldots \subseteq F_k=F_{k-1}(\omega_k)$ such that $\omega_1^{n_1} \in F$, $\omega_2^{r_2} \in F_1, \ldots, \omega_k^{n_k} \in F_{k-1}$ such that the roots of p(x) all lies in F_k and $F_k \subseteq K$.

5.4.3 Theorem. If the field F contains all the n^{th} roots of unity, a is nonzero element of F, and K is the splitting field of the polynomial x^n-a over F, then

(i) K=F(u); u is the root of x^n-a

(ii) The Galois group of x^n-a over F is abelian.

Proof. Take $\alpha = e^{\frac{2\pi i}{n}}$. Then α is n^{th} root of unity such that $\alpha^m \neq 1$ for $0<m<n$. We call α as primitive n^{th} root of unity. Trivially 1, α, α^2, …, α^{n-1} all are root n^{th} roots of unity. All these are distinct as if $\alpha^i = \alpha^j$, $0 \leq i<j \leq n-1$, then $\alpha^{i-j} =1$, a contradiction that $\alpha^m \neq 1$ for $0<m<n$.

If u is root of x^n-a in K, then $u, u\alpha, u\alpha^2, \ldots, u\alpha^{n-1}$ are distinct roots of x^n-a. By our assumption α lies in F, therefore, all the roots of x^n-a lies in F(u) and F(u) is smallest such field. Hence the splitting field of x^n-a is F(u) and thus K=F(u).

If σ_1, σ_2 are two elements in the Galois group G(K=F(u), F) of x^n-a i.e. σ_1, σ_2 leaves every element of F fixed. But then $\sigma_1(u)$ and $\sigma_2(u)$ are

also roots of x^n-a . Since $u, u\alpha, u\alpha^2, \ldots, u\alpha^{n-1}$ are only distinct roots x^n-a, therefore, $\sigma_1(u) = u\alpha^i$ and $\sigma_2(u) = u\alpha^j$ for some positive integers i and j. Then $\sigma_1\sigma_2(u) = \sigma_1(\sigma_2(u)) = \sigma_1(u\alpha^j) = \sigma_1(u)\,\sigma_1(\alpha^j) = u\alpha^{i+j}$. Similarly $\sigma_2\sigma_1(u) = u\alpha^{j+i} = u\alpha^{i+j}$. Therefore, $\sigma_1\sigma_2$ and $\sigma_2\sigma_1$ agree on u and F, hence on all of K=F(u). But then $\sigma_1\sigma_2 = \sigma_2\sigma_1$, whence the Galois group is abelian.

5.4.4 Corollary. If F has all n^{th} root of unity, then adjoining one root of x^n-a to F, where *a* belong to F, is a normal extension.

Proof. It is clear from Lemma that K=F(u), u is root of x^n-a, is splitting field of x^n -a over F. Hence K is normal extension of F.

5.4.5 Theorem. If F is a field which contains all n^{th} root of unity for every positive integer n and if $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group over F of p(x) is a solvable group.

Proof. Let K be the splitting field of p(x) over F and G(K,F) is Galois group of p(x) over F. Since p(x) is solvable by radicals, there exist a sequence of fields

$$F \subseteq F_1 = F(\omega_1) \subseteq F_2 = F_1(\omega_2) \subseteq \ldots \subseteq F_k = F_{k-1}(\omega_k),$$

such that $\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}$ and where $K \subseteq F_k$. As we pointed out without loss of generality we may assume that F_k. Since $F \subset F_i$ for all $1 \leq i \leq k$, therefore, p(x) also belongs to $F_i[x]$. Hence F_k is the splitting field of p(x) over F_i. Hence F_k is normal extension of F_i also.

By assumption F contains all the n^{th} root of unity for all positive integer n, therefore, each F_{i-1} also contains all the n^{th} root of unity. In particular, F_{i-1} also contains all the r_i^{th} root of unity. If we take a polynomial

$x^{r_i} - \omega_i^{r_i} \in F_{i-1}[x]$, then by Theorem 5.4.3, $F_i = F_{i-1}(\omega_i)$ is normal extension of F_{i-1}. Since F_k is also normal over F_{i-1}, therefore, by Theorem 5.3.4, $G(F_k, F_i)$ is normal subgroup of $G(F_k, F_{i-1})$. Consider the chain

$$G(F_k, F) \supset G(F_k, F_1) \supset G(F_k, F_2) \supset \ldots \supset G(F_k, F_{k-1}) \supset \{e\} \qquad (*)$$

Since for each i, $1 \leq i \leq k$, $G(F_k, F_{i-1})$ is normal in $G(F_k, F_i)$, $G(F_k, F_1)$ is normal in $G(F_k, F)$ and F_i is normal extension of F_{i-1}, by Fundamental Theorem of Galois theory, $G(F_i, F_{i-1}) \cong \frac{G(F_k, F_{i-1})}{G(F_k, F_i)}$. Since by Theorem 5.5.3, $G(F_i, F_{i-1})$ is abelian, therefore, $\frac{G(F_k, F_{i-1})}{G(F_k, F_i)}$ is abelian. Thus each quotient group $\frac{G(F_k, F_{i-1})}{G(F_k, F_i)}$ of the chain (*) is abelian. Thus $G(F_k, F)$ is solvable. Since $K \subset F_k$ and is a normal extension of F. Again by Theorem 5.3.4, $G(F_k, K)$ is a normal subgroup of $G(F_k, F)$ and $G(K, F) \cong \frac{G(F_k, F)}{G(F_k, K)}$. Thus G(K, F) is homomorphic image of $G(F_k, F)$, a solvable group. But we know that homomorphic image of a solvable group is also solvable. Hence G(K, F) is solvable. Since G(K, F) is Galois group of p(x) over F the theorem has been proved.

5.4.6 **Remark**. (i) Converse part of Theorem 5.4.5 is also true; i.e. if Galois group of p(x) over F is solvable then p(x) is solvable by radicals over F.

(ii) Theorem 5.4.5 and its converse part is also true even when F does not contain the roots of unity.

5.4.7 Theorem. The general polynomial of degree $n \geq 5$ is not solvable by radicals.

Proof. Take $F(a_1, a_2, \ldots, a_n)$, the field of symmetric rational functions in the n variables $a_1, a_2, \ldots, a_n$. If $x_1, x_2, \ldots, x_n$ are n variable such that

$$a_1 = \sum_{i=1}^{n} x_i \,,\; a_2 = \sum_{i<j} x_i x_j \,,\; a_3 = \sum_{i<j<k} x_i x_j x_k \,, \ldots, a_n = \prod_{i=1}^{n} x_i \,.$$

Then $x_1, x_2, \ldots, x_n$ are the root of the polynomial

$$t^n + a_1 t^{n-1} + \ldots + a_n.$$

But then $F(x_1, x_2, \ldots, x_n)$ is the splitting field of above polynomial. Since (Theorem 4.6.3) Galois group $G(F(x_1, x_2, \ldots, x_n), F(a_1, a_2, \ldots, a_n)) = S_n$, (symmetric group of degree n on $\{1, 2, \ldots, n\}$). Then, by Theorem 5.5.5, $t^n + a_1 t^{n-1} + \ldots + a_n$ is solvable by radicals over $F(a_1, a_2, \ldots, a_n)$ if and only if S_n is solvable. As we know that S_n is not solvable for $n \geq 5$. Hence the general polynomial of degree $n \geq 5$ is not solvable by radicals.

5.5 Cyclotomic polynomials.

Let C be the field of complex numbers. Consider the complex number $\alpha_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{\frac{i2\pi}{n}}$. Then $\alpha^n = 1$ and $\alpha^m \neq 1$ for $1 \leq m < n$. We call α as a primitive n^{th} root of unity. Clearly α satisfies the polynomial $x^n - 1$ over field of rational numbers. Now the question is that what is minimal polynomial of α ?

5.5.1 Definition. Cyclotomic polynomial. Polynomial $\phi_n(x)$ defined as:

(a) $\phi_1(x) = x - 1$

(b) if $n > 1$, $\phi_n(x) = \dfrac{(x^n - 1)}{\prod \phi_d(x)}$, where d runs over all the divisors of n except for n itself. These polynomials are called cyclotomic polynomials. $\phi_n(x)$ is called n^{th} cyclotomic polynomial.

Example. (i) $\phi_2(x) = \dfrac{(x^2 - 1)}{\prod \phi_1(x)} = \dfrac{(x^2 - 1)}{(x - 1)} = x + 1$

(ii) $\phi_3(x)= \dfrac{(x^3-1)}{\phi_1(x)} = \dfrac{(x^3-1)}{(x-1)} = x^2+x+1$

(iii) $\phi_4(x)= \dfrac{(x^4-1)}{\phi_1(x)\phi_2(x)} = \dfrac{(x^4-1)}{(x+1)(x-1)} = x^2+1$

(v) $\phi_5(x)= \dfrac{(x^5-1)}{\phi_1(x)} = \dfrac{(x^5-1)}{(x-1)} = x^4+x^3+x^2+x+1$

(vi) $\phi_6(x)= \dfrac{(x^6-1)}{\phi_1(x)\phi_2(x)\phi_3(x)} = \dfrac{(x^6-1)}{(x+1)(x-1)(x^2+x+1)} = x^2-x+1$

(vii) $\phi_9(x) = \dfrac{(x^9-1)}{\phi_1(x)\phi_3(x)} = \dfrac{(x^9-1)}{(x-1)(x^2+x+1)} = \dfrac{(x^9-1)}{(x^3-1)}$

$= \dfrac{(x^3)^3-1)}{(x^3-1)} = \dfrac{(x^3-1)(x^6+x^3+1)}{(x^3-1)}$.

$= (x^6+x^3+1)$

5.5.2 Observations made about the Cyclotomic polynomials from above discussion.

(i) These are monic polynomials with integer coefficients.

(ii) Degree of $\phi_n(x)$ is $\varphi(n)$, where φ is Euler's phi-function.

(iii) α_n is a root of $\phi_n(x)$ and $\phi_n(x)$ is minimal polynomial of α_n.

(iv) $\phi_n(x)$ is irreducible polynomial over field of rational numbers.

5.5.3 Notation. When $n=p^m$, denote $\phi_{p^n}(x) = \psi^{(m)}(x)$.

5.5.4 Lemma. For all $m \geq 1$,

$$\psi^{(m)}(x) = \frac{x^{p^m}-1}{x^{p^{m-1}}-1} = 1 + x^{p^{m-1}} + x^{2p^{m-1}} + \ldots + x^{(p-1)p^{m-1}}$$

Proof. We will prove the result by induction on m.

If m=1, then $\psi^{(1)}(x) = \phi_p(x)$. Since 1 is the only divisor of p which is less than p, therefore, $\phi_p(x) = \dfrac{x^p-1}{\phi_1(x)} = \dfrac{x^p-1}{x-1} = 1+x+x^2+\ldots+x^{(p-1)}$. Hence the result is true for m=1.

Let us suppose that result holds for all k < m. i.e.

$$\psi^{(k)}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \ldots + x^{(p-1)p^{k-1}}.$$

Consider $\psi^{(m)}(x)$. Since $\psi^{(m)}(x) = \phi_{p^m}(x)$ and only divisors of p^m are 1, p,…,p^{m-1} which are less than p^m, therefore,

$$\phi_{p^m}(x) = \frac{x^{p^m} - 1}{\phi_1(x)\phi_p(x)\ldots\phi_{p^{m-1}}(x)} = \frac{x^{p^m} - 1}{(x-1)\psi^{(1)}(x)\ldots\psi^{(m-1)}(x)}.$$

Since by induction hypothesis,

$$(x-1)\psi^{(1)}(x)\ldots\psi^{(m-1)}(x) = (x-1)\frac{x^p - 1}{x - 1}\frac{x^{p^2} - 1}{x^p - 1}\ldots\frac{x^{p^{m-1}} - 1}{x^{p^{m-2}} - 1} = x^{p^{m-1}} - 1,$$

therefore,

$$\psi^{(m)}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = 1 + x^{p^{m-1}} + x^{2p^{m-1}} + \ldots + x^{(p-1)p^{m-1}}.$$

It proves the result.

5.5.5 **Theorem**. For any prime p and non negative integer m, the polynomial $\psi^{(m)}(x)$ is irreducible in Q[x].

Proof. Clearly $\psi^{(m)}(x)$ is a monic polynomial of degree $\phi(p^m) = (p-1)p^{m-1}$ with integer coefficients. Further

$$\psi^{(m)}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = \frac{(x^{p^{m-1}})^p - 1}{x^{p^{m-1}} - 1} = \psi^{(1)}(x^{p^{m-1}}) \qquad (1)$$

Let f(x) and g(x) are two polynomials with integer coefficients, define $f(x) \equiv g(x) \bmod p$ if $f(x) = g(x) + pr(x)$, where r(x) is polynomial with integer coefficients.

Now $(f(x)+g(x))^p = f(x)^p + (\sum_{i=1}^{p-1} p_{C_i} f(x)^{p-i} g(x)^i) + g(x)^p$. Since $p_{C_i} \equiv 0 \bmod p$, therefore, $(f(x)+g(x))^p \equiv f(x)^p + g(x)^p \bmod p$. Further, for every positive

integer a, by Fermat Theorem, $a^p \equiv a \bmod p$. Hence if $f(x) = \sum_{i=0}^{n} a_i x^i$, then

$$f(x)^p \equiv \sum_{i=0}^{n} (a_i)^p x^{pi} \equiv \sum_{i=0}^{n} a_i (x^p)^i \equiv f(x^p) \bmod p .$$

Proceeding in the same way we get $f(x)^{p^k} \equiv f(x^{p^k}) \bmod p$ for all non-negative integers k.

By (1), $\psi^{(m)}(x) = \psi^{(1)}(x^{p^{m-1}})$, therefore,

$$\psi^{(1)}(x+1)^{p^{m-1}} = \left(\frac{(x+1)^p - 1)}{(x+1-1)}\right)^{p^{m-1}} = \left(\frac{(x+1)^p - 1)}{x}\right)^{p^{m-1}}$$

$$= \left(\frac{1 + px + \frac{p(p-1)}{2}x^2 + \ldots + x^p - 1}{x}\right)^{p^{m-1}}$$

$$\equiv x^{(p-1)p^{m-1}} \bmod p \equiv \psi^{(m)}(x+1) \bmod p .$$

Hence $\psi^{(m)}(x+1) = x^{(p-1)p^{m-1}} + pr(x)$, r(x) is the polynomial with integer coefficients. As by Lemma 5.5.4,

$$\psi^{(m)}(x+1) = 1 + (x+1)^{p^{m-1}} + (x+1)^{2p^{m-1}} + \ldots + (x+1)^{(p-1)p^{m-1}},$$

Therefore, $\psi^{(m)}(0+1) = p$. i.e. constant term of $\psi^{(m)}(x+1)$ is p.

Now we have a prime p such that p divides every coefficient of $\psi^{(m)}(x+1)$ except the leading coefficient and p^2 does not divides the constant coefficients of $\psi^{(m)}(x+1)$. Hence by Eisenstein Criteria of irreducibility $\psi^{(m)}(x+1)$ is irreducible over Q.

5.5.6 Theorem. For every integer n≥1, $\phi_n(x) = (x - \theta^{(1)})(x - \theta^{(2)})\ldots(x - \theta^{(\varphi(n))})$, where $\theta^{(1)}$, $\theta^{(2)}$,..., $\theta^{(\varphi(n))}$ are the $\varphi(n)$ distinct primitive nth root of unity.

Proof. We will prove the result by induction on n.

If n=1, then $\phi_1(x) = (x-1)$. Since 1 is the only first root of unity, therefore, result is true in this case.

Suppose that the result is true for all m < n. Therefore, if d | n, d < n, we have $\phi_d(x) = (x-\theta_d^{(1)})(x-\theta_d^{(2)})...(x-\theta_d^{(\varphi(d))})$ where $\theta_d^{(i)}$ are primitive d^{th} root of unity. Now,

$x^n - 1 = (x-\zeta_1)(x-\zeta_2)...(x-\zeta_n)$; ζ_1, ζ_2,…, ζ_n are all nth roots of unity. If we separate all primitive n th roots of unity, we get

$$x^n - 1 = (x-\theta^{(1)})(x-\theta^{(2)})...(x-\theta^{(\varphi(n))})v(x)$$

Where v(x) is the product of all other $(x-\zeta_i)$. Thus by our induction hypothesis v(x) is the product of the $\phi_d(x)$ over all the divisors d of n, d≠n. i.e. i.e. $v(x) = \prod_{\substack{d/n \\ d\neq n}} \phi_d(x)$. Then

$$\phi_n(x) = \frac{x^n-1}{\prod_{\substack{d/n \\ d\neq n}} \phi_d(x)} = \frac{(x-\theta_d^{(1)})(x-\theta_d^{(2)})...(x-\theta_d^{(\varphi(d))})v(x)}{v(x)}$$

$= (x-\theta_d^{(1)})(x-\theta_d^{(2)})...(x-\theta_d^{(\varphi(d))})$. It proves the theorem.

5.5.7 Theorem. For every positive integer n, the polynomial $\phi_n(x)$ is a monic polynomial with integer coefficients of degree $\varphi(n)$, φ is the Euler's φ-function.

Proof. Since $\phi_n(x) = (x-\theta^{(1)})(x-\theta^{(2)})...(x-\theta^{(\varphi(n))})$, therefore, its degree is $\varphi(n)$. We now apply induction on n to show that it is a polynomial with integer coefficient.

If n=1, then $\phi_1(x) = (x-1)$ i.e. for n=1, $\phi_1(x)$ is a polynomial with integer coefficient.

Suppose that result is true for all m < n. i.e. $\phi_m(x)$ is the polynomial with integer coefficient.

Since $\phi_n(x) = \frac{x^n-1}{\prod_{\substack{d/n \\ d\neq n}} \phi_d(x)}$. By induction assumption, $\prod_{\substack{d/n \\ d\neq n}} \phi_d(x)$ is a monic polynomial with integer coefficient. If we divide the polynomial x^n-1

by $\prod_{\substack{d/n \\ d\neq n}} \phi_d(x)$, then it is a monic polynomial with integer coefficients. Hence $\phi_n(x)$ is a monic polynomial with integer coefficients.

5.5.8 Theorem. For every positive integer n the polynomial $\phi_n(x)$ is irreducible over the field of rational numbers.

Proof. Let f(x) be an irreducible factor of the polynomial $\phi_n(x)$ in Q[x]. We will show that f(x)=$\phi_n(x)$. Let if possible $\phi_n(x) \neq f(x)$, then $\phi_n(x) = f(x)g(x)$ for polynomial g(x). Since $\phi_n(x)$ has no multiple roots and is monic polynomial, therefore, gcd(f(x), g(x))=1.

Let p be a prime number such that p does not divide n. If θ is a root of f(x) then θ is also root of $\phi_n(x)$, therefore, θ is primitive nth root of unity. By our choice on p, θ^p is also primitive n th root of unity. Now we will show that θ^p is a root of f(x). Let if possible θ^p is not a root of f(x). Then it will be root of g(x). But then θ is root of $g(\theta^p)$. Since f(x) is irreducible polynomial, therefore, it is minimal polynomial of θ. Hence $f(x) \mid g(\theta^p)$. But $g(x^p) \equiv g(x)^p \pmod p$, then $f(x) \mid g(\theta)^p$.

Let $t(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ be a polynomial in Z[x]. Identify t(x) in $Z_p[x]$ by $\bar{t}(x) = \bar{a}_0 + \bar{a}_1x + \bar{a}_3x^2 + \ldots + \bar{a}_nx^n$, where $\bar{a}_i$ is residue of a_i (mod p). Then it is homomorphism from Z[x] onto $Z_p[x]$.

Since all the polynomials $\phi_n(x)$, v(x), f(x) and g(x) lies in Z[x], Let $\bar{\phi}_n(x)$, $\bar{v}(x)$, $\bar{f}(x)$ and $\bar{g}(x)$ are their respective images in $Z_p[x]$. If $t(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ and $r(x)= b_0+b_1x+b_2x^2+\ldots+b_mx^m$ are two polynomials then $t(x)r(x)= \sum_{i=0}^{m+n} c_ix^i$, where $c_i = \sum_{j+k=i} a_jb_k$. Since $a_j = d_jp + \bar{a}_j$ and $b_k = e_kp + \bar{b}_k$, therefore,

$$a_jb_k = d_je_kp^2 + (\bar{a}_je_k + \bar{b}_kd_j)p + \bar{a}_j\bar{b}_k.$$

But then $\overline{a_jb_k} = \bar{a}_j\bar{b}_k$. Hence we can identity t(x)r(x) by $\bar{t}(x)\bar{r}(x)$ in $Z_p[x]$.

Hence $(x^n - 1) = \overline{\phi_n}(x)\bar{v}(x)$, $\overline{\phi_n}(x) = \bar{f}(x)\bar{g}(x)$ and $\bar{f}(x) \mid \bar{g}(x)^p$.

Therefore, $\bar{f}(x)$ and $\bar{g}(x)$ have common root in some extension of Z_p. Now $(x^n - 1) = \overline{\phi_n}(x)\bar{v}(x) = \bar{f}(x)\bar{g}(x)\bar{v}(x)$, hence *a*, as a root of both $\bar{f}(x)$ and $\bar{g}(x)$, is a multiple root of x^n-1. Since derivative $(x^n\text{-}1)'$ of x^n-1 is nx^{n-1}-1 $\neq$0, since p does divides n; therefore, $(x^n\text{-}1)'$ is relatively prime to p. Hence (x^n-1) can not have a multiple root. With this contradiction, we say that whenever θ is a root of f(x) , then so must θ^p be one for any prime p that does not divide n.

Repeating this argument, we arrive at: θ^r is a root of f(x) for every *r* that does not divide n. But θ as a root of f(x), is also a root of $\phi_n(x)$ and hence is a primitive n^{th} root of unity. Thus θ^r is also a primitive nth root of unity for every *r* relatively prime to n. By running *r* over all the number which are less than n and relatively co-prime to n, we get every primitive root of unity is also a root of (x). Hence $\phi_n(x)$=f(x), therefore, $\phi_n(x)$ is irreducible over Q. It proves the theorem.

5.6 Finite fields.

5.6.1 **Definition**. Field F is called finite field if it has finite number of elements. For example, set {0, 1, 2, …, p-1} is a field under addition and multiplication modulo p. It has exactly p elements.

5.6.2 **Lemma**. If F is a finite of order q, then an extension K of F; [K:F]=n, has q^n elements.

Proof. Since extension K of F is a vector space with dimension n over F. Let $v_1, v_2, \ldots, v_n$ be a basis of K over F. Then elements of K are of the form $\alpha_1 v_1 + \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$; $\alpha_i \in$F. Since each α_i has q choice, therefore, number of elements in K are q^n.

5.6.3 **Corollary**. If F is a finite field, then F has p^m elements where p is the characteristic of F.

Proof. If F is prime field with characteristic p then it has exactly p elements. F is not a prime field, then F has a prime subfield P having exactly p elements. Since F is an extension of P, therefore, by Lemma 5.6.2, F has p^m elements.

5.6.4 **Corollary**. If the finite field has p^m elements then every $a \in F$ satisfies $a^{p^m} = a$.

Proof. If a=0, then the above result is trivial. If $a \neq 0$, then the set of all onzero elements form group under multiplication. Hence $a^{p^m - 1} = 1$. Equivalently $a^{p^m} = a$.

5.6.5 **Lemma**. If the field F has p^m elements then the polynomial $x^{p^m} - x$ in F[x] factors in F[x] as $x^{p^m} - x = \prod_{\beta \in F} (x - \beta)$.

Proof. Since the characteristic of field F with p^m elements is p, therefore, derivative $f'(x)$ of $f(x) = x^{p^m} - x$ is $p^m x^{p^m - 1} - 1 = -1 \neq 0$. Hence all the roots of f(x) are distinct. Further, by corollary 5.4.4, each element of F is a root of f(x). Hence $x^{p^m} - x = \prod_{\beta \in F} (x - \beta)$.

5.6.6 **Corollary.** If the field has p^m elements, then F is the splitting field of polynomial $x^{p^m} - x$.

Proof. Result follows by Lemma 5.6.5 and using the fact that no field smaller than F can contain all the roots of f(x).

5.6.7 **Lemma.** Any two finite fields having same number of elements of elements are isomorphic.

Proof. Let the two finite fields F and K have p^m elements. Then By Corollary 5.4.6, these two fields are splitting of the polynomial $x^{p^m} - x$. We know that any two splitting field of the same polynomial are isomorphic (can be easily proved), therefore, F and K are isomorphic.

5.6.8 **Lemma**. For every prime p and every positive integer m there always exist a field of order p^m elements.

Proof. Consider the polynomial $x^{p^m} - x$ in $Z_p[x]$; Z_p is field of integers under addition and multiplication modulo p. Let K be the splitting field of $x^{p^m} - x$. In K let $F=\{a \in K \mid a^{p^m} = a\}$. Clearly elements of F are the roots of the polynomial $x^{p^m} - x$. Since all the roots of $x^{p^m} - x$ are distinct, therefore, F has p^m elements. Further for a and b belonging to F we have $a^{p^m} = a$ and $b^{p^m} = b$. Then $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$, therefore, $ab \in F$. Since the characteristic is p, therefore, $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m} = a \pm b$. Hence F becomes a subfield of K. Therefore, we always have a field of order p^m.

5.6.9 Theorem. For every prime p and every positive integer m there exist a unique field of order p^m elements.

Proof. Proof follows by Corollary 5.6.7 and Lemma 5.6.8.

5.6.10 Lemma. If G is a finite abelian group with the property that the relation $x^n=e$ is satisfied by at most n elements of G, for every integer n. Then G is cyclic group.

Proof. Since G is finite abelian group of order $n=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$; p_i's are distinct primes, we can write $G= S_{p_1} S_{p_2} \ldots S_{p_r}$ as the direct product of Sylow p_i subgroup of G i.e. every element $g \in G$ can be written in a unique way as $g=s_1 s_2 \ldots s_r$, $s_i \in S_{p_i}$. If each S_{p_i} is a cyclic subgroup of G generated by a_i then $a=a_1 a_2 \ldots a_r$. Let $a^m=e$. Then $a_1^m a_2^m \ldots a_r^m = e$. Now using the fact that each element of G has unique representation, in particular e has unique representation. Hence $a_i^m = e$ for $1 \le i \le r$. But then $p_i^{\alpha_i}$ divides m. Since p_i are distinct primes, therefore, $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = o(G)$ divides m. Hence $o(G)= m$.

Therefore, G will be cyclic if each S_{p_i} is cyclic. i.e. in order to show that G is cyclic it is sufficient to show that each p group is cyclic, p is prime. Let H be a group of some prime power. Let *a* is an element of H whose order is as large as possible. Definitely its order is p^r for some positive integer

r. More over if $a^i=a^j$ for $i > j$, $0 \le i, j \le p^r - 1$, then $a^{i-j}=e$. Since the order of *a* is p^r > i-j, $a^{i-j}=e$ only when i=j. Hence all the elements $e, a, a^2, ..., a^{p^r-1}$ are distinct. Further all these elements are the solutions of the equation $x^{p^r} = e$, As by our hypothesis $x^{p^r} = e$ has at most p^r distinct solution, therefore, $e, a, a^2, ..., a^{p^r-1}$ are the only solutions of $x^{p^r} = e$. Now if $b \in H$, its order is p^s where $s \le r$ and $b^{p^r} = (b^{p^s})^{p^{r-s}} = e$. But then by the discussion made above $b = a^i$ for some i. So every element of H is some power of *a*, therefore, H is cyclic. Hence G is cyclic.

5.6.11 Theorem. Let K be a field and G be a finite subgroup of the multiplicative group of non zero elements of K. Then G is cyclic.

Proof. Since K is a field and the multiplicative group of K is abelian. Further for any integer n, equation x^n-1 has at most n root in K and so at the most n roots in G. The hypothesis of Lemma 5.6.10 is satisfied. Hence G is cyclic.

5.7 KEY WORDS.

Galois group, radicals, perfect field, finite fields

5.8 SUMMARY.

In this chapter, perfect fields, Galois Theory, solvability by radicals, Cyclotomic polynomials and finite fields are studied.

5.9 SELF ASSESMENT QUESTIONS.

(1) Prove that $\phi_n(x)$ is the minimal polynomial in Q[x] for the primitive n^{th} root of unity; Q is the field of rational numbers.

(2) Show that the multiplicative group of non-zero elements of a finite field is cyclic.

(3) Find the Galois group of the following polynomials:

x^2+1, x^3-2 and x^4-2.

5.8 SUGGESTED READINGS.

(1) **Topics in Algebra**; I.N HERSTEIN, John wiley and sons, New York.

(2) **Modern Algebra**; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(3) **Basic Abstract Algebra**; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.