Groups As Unions of Proper Subgroups

BY

R. Usha

A THESIS SUBMITTED TO AVINASHILINGAM INSTITUTE FOR HOMESCIENCE AND HIGHER EDUCATION FOR WOMEN (DEEMED UNIVERSITY) COIMBATORE 641 043.
(ERSTWHILE AVINASHILINGAM HOMESCIENCE COLLEGE AFFILIATED TO BHARATHIAR UNIVERSITY)
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE

MAY 1989

CONTENTS

ACKNOWLEDGEMENT

It is with pleasure the author expresses her sincere gratitude to Dr. K. N. MEENAKSHI, M.Sc., Ph.D., Professor and Head of the Department of Mathematics, Avinashilingam Institute for Homescience and Higher Education for Women (Deemed University) Coimbatore, for the inspiring guidance and valuable advice which enabled the author to bring this dissertation in its present and final form.

The author expresses her heartfelt gratitude to Tmt. M.I. AFTHAB BEGUM, M.Sc(Madras) M.Phil., Assistant professor of Mathematics, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed University), Coimbatore who devoted much of her valuable time in directing her by giving suggestions and timely advice for the preparation of the dissertation work successfully.

The author is also indebted to Dr. (Tmt).RAJAMMAL P.DEVADAS,M.A., M.Sc., Ph.D.(Ohio State), D.Sc(Madras) Vice Chancellor of Avinashilingam Institute for Home Science and Higher Education for Women (Deemed university) Coimbatore for all the facilities given to her in the course of the preparation of this dissertation.

The author records her thanks to Dr. K.KULANDAIVEL, M.A. M.A., (Ohio State) Ph.D. (Madras) Registrar of Avinashilingam Institute for Homescience and Higher Education for Women, Coimbatore and Dr. (Tmt). JANABAI GIRI , M.A. M.Sc., Ph.D. (Madras) Dean, Faculty of Science for providing the necessary facilities.

INTRODUCTION

The object of this dissertation is to discuss groups which are unions of their proper sub groups. Our main interest here is to consider groups which can be written as the union of three sub groups. Groups which are finite union of their proper sub groups and some of their properties are also studied in the last chapter.

In chapter I, we state definitions and some known results of group theory. We also disucss some special groups like klein four group, The Dihedral group D_{2m} of order 4m defined by $a^{2m} = b^2 = (ab)^2 = e$, and the group of order 16 defined by the generating relations $a^2 = b^2 = c^2 = e$, $abc = bca = cab$. These examples are used in the next chapter to discuss the decomposition of a group in to three sub groups.

It is well known that, except the trivial case a group cannot be expressed as the union of two groups. In this chapter we study groups which can be written as a nontrivial union of three of its sub groups. When G is expressed as $G = A \cup B \cup C$ then $K = A \cap B \cap C$ is an invariant subgroup of G and $A \cap B = A \cap C = B \cap C = K$. In such case, we say $\{A, B, C\}$ is a decomposition of G.

A characterization for a group G expressed as the union of three group (such groups are called 3 - groups) is obtained in the following theorem (2.2): "A group G is the nontrivial union of three subgroups if and only if it is homomorphic to the Klein four group". It is deduced from this theorem that a finite 3-group G has order 4 m. On the other hand it is proved by example that there are groups of order 4m which are not the union of three subgrops.

We consider two decomposition $\{X, Y, Z\}$ and $\{X_1, Y_1, Z_1\}$ of a group G as the same if there exists isomorphisms : $X \to X_1$, $Y \to Y_1$, and $Z \to Z_1$. It is shown by examples that 1) A 3 - group can have different decomposition and 2) Two different 3 - groups can have the same decomposition. Next we discuss the different types of decomposition of a 3 - group. If a 3-group is non-abelian then the subgroups of a decomposition can be abelian (@) or non abelian (n). This gives four possible types of decompositions for a 3 - group namely $\{@, @, @\}$ or $\{@, @, n\}$ or $\{@, n, n\}$ or $\{n, n, n\}$.

The type $\{@, @, n\}$ is ruled out from the following theorem "If $G \longrightarrow \{A, B, C\}$ and A and B are abelian then C is also abelian". The existence of the remaining three types of decomposition are illustrated by means of examples (2.7). The following theorem gives a characterization for a non abelian 3-group to have an abelian decomposition.

Theorem : A non abelion 3 - group G has an abelian decomposition if and only if the centre of G is the intersection of the three subgroups. It is also shown that, if G admits a decomposition $\{A, B, C\}$ of type $\{@, n, n\}$ then the centre Z of G is contained in A.

Finally some properties of the group of inner automorphisms of a 3-group are obtained in the following three theorems.

1) The group of inner automorphioms of a 3-group G = $\{A, B, C\}$ is either itself a 3 - group or degenerate, in the sense that it is one of $\tilde{I}(A)$ or $\tilde{I}(B)$ or $\tilde{I}$ (C) where $\tilde{I}(A)$ denotes the set of inner automorphioms of G by elements of A.

2) A non - abelian 3 - group has an abelian decomposition if and only if the group of inner automorphisms is the klein four group.

3. The group of inner automorphisms of a 3 -group is degenerate if and only if the centre contains elements other than elements from K.

It is evident that a group G is non cyclic if and only if it is expressible as a finite (or) infinite union of the proper subgroups. But it is not so easy to characterize groups which are finite union of their proper subgroups. Q^+ - the additive group of rational number is a non cyclic group which is not a finite union of subgroups.

In chapter III we obtain a condition that gives the minimum number of proper subgroups into which a group can be decomposed. The following theorem gives the condition.

" suppose the K^{th} root can be taken in the group G for every positive integer K less than a certain n. Then G is not the irredundant union of n (or fewer) of its subgroups

It is shown by example that the above theorem can not be strengthened (ie) the group G generated by two elements x, y with relation $x^p = y^p = e$ satisfies the criteria of the above theorem for the number p and it can be expressed as the union of p + 1 proper subgroups But a partial converse of the above theorem is obtained in the following way.

Let G be a finite group of order N, p the smallest prime number dividing N and suppose G is the union of p + 1 proper subgroup s_i, then atlast one of s_i has index p. If moreover that s_i is normal then all the s_i's have index p and p^2 divides N

CHAPTER I

Definitions and preliminaries :-

Definition 1:

GROUP:

A non empty set of elements G is said to form a group if in G there is defined a binary operation called the product and denoted by . such that

1) $a, b \in G$ implies $a.b \in G$ (closed)
2) $a, b, c \in G$ implies that $a.(b.c) = (a.b) . c$ (associative)
3) There exists an element $e \in G$ such that

   $e.a = a.e = a$ for all $a \in G$

4) For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a . a^{-1} = a^{-1} . a = e$

Note1

A group is said to be abelian if for every $a, b \in G$ $a . b = b.a.$

Definition 2:

Sub group:- A non empty subset H of a group G is said to be a sub group of G if under the product in G, H itself forms a group.

Definition 3:-

Index of H in G:- If H is a sub group of G, index of H in G is the number of distinct right cosets (left cosets) of H in G.

Note :2

In case G is a finite group $i_G(H) = \frac{\sigma(G)}{\sigma(H)}$ where $\sigma(G)$ denotes the order of the group G(ie number of elements in G).

Definition 4:

NORMAL SUB GROUP (Invariant subgroup):-

A subgroup N of G is said to be a normal subgroup of G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Note 3:

If G is a finite group and N is a normal subgroup of G, then $\frac{\sigma(G)}{\sigma(N)} = \sigma\left(\frac{(G)}{N}\right)$.

where G/N = The collection of right (left) cosets of N in G is a group when ever N is a normal subgroup of G.

Definition 5:

Centre of a group G: The set of all elements of G which commute with every element of G.

$$Z = \text{the centre of } G = \{ z \in Z / gz = zg \quad \forall\, g \in G \}$$

Definition 6:

By an automorphism of a group G, we shall mean an isomorphism of G on to itself.

For $g \in G$, $T_g : G \longrightarrow G$ defined by $T_g(x) = gxg^{-1}$

for all $x \in G$ is called inner automorphism of G denoted by I(G)

Note 4:

I (G) is isomorphic to the factor group G/Z.

Definition 7:

$\tilde{I}$ (A) where A is subgroup of a group G is the set of inner automorphism of G defined by elements of A.

Note 5:-

I (G) is a sub group of group of automorphism of G. $\tilde{I}$ (A) is a subgroup of I(G) When A is a sub group of G.

Definition 8:

MONOGENIC: A group G is said to be monogenic if it is generated by a single element.

Definition 9:

IRREDUNDENT UNION:

A group G is said to be the irredundent union of its sub groups H_i, i = 1 to n if none of the $H^{'}$s is contained in the union of all the others.

Definition 10:

Homomorphic image:

A group G' is said to be the homomorphic image of G if there exists an on to homomorphism $\emptyset : G \longrightarrow G'$.

Note 6:

DECOMPOSITION OF A GROUP:

If G is the union of its proper sub groups, we say it is a decomposition of G.

Detinition 12:

3-group:

A group which allows a decomposition in to three sub groups is called a 3-group.

Note:7

Let $\{X, Y, Z\}$ and $\{x_1, y_1, z_1\}$ be the two decomposition of a group G. The two decomposition are said to be the same if there exists isomorphisms $X \longrightarrow X_1$, $Y \longrightarrow Y_1$, and $Z \longrightarrow Z_1$.

Next we shall see some important examples of groups which are used in this work.

Some special Examples:

1.1: Klein 4 - group :- (V)

A group with four elements $\{a, e, b, c\}$ with the relations $a^2=b^2=c^2=e$, $ab = ba=c$,

$bc = cb = a$, $ca = ac = b$ is said to be Klein 4 - group and through out this thesis it is denoted by the symbol (V)

1.2: C_m-The cyclic group of order m

$$= \{a, a^2, a^3 \ldots a^{m-1}, a^m = e\}$$

1.3: The Dihedral group D_{2m} of order 4m is defined by $a^{2m} = b^2 = (ab)^2 = e$,

The elements of the dihedral group are

$$= a, a^2 \ldots a^{2m-1}, a^{2m} = e,$$

$$b, b^2 = e$$

$$ab, (ab)^2 = e \text{ and}$$

$a^k b$ where $k = 1$ to $2m - 1$

$b a^k$ where $k = 1$ to $2m - 1$

But $(ab)^2 = e \implies (ab)(ab) = e$

$$\implies ba = a^{-1} b^{-1}$$

$$\text{(i.e) } ba = a^{-1} b$$

$$\text{similarly } ab = b^{-1} a^{-1} = ba^{-1}$$

$$ba^k = a^{-k} b = a^{2m-k} b$$

The collection $\{ba^k\}_{1 \le k \le 2m-1}$ is equal to the collection $\{a^{k'} b\}_{1 \le k' \le 2m-1}$

$\therefore$ The elements of D_{2m} are

$$D_{2m} = \{a, a^2 \ldots a^{2m-1}, e, b, a^k b / k = 1 \text{ to } 2m-1\}$$

There are totally 4m elements.

1.4: The group of order 16 defined by the generating relations $a^2 = b^2 = c^2 = e$,

$abc = bca = cab$

using the above operations one can show that

$(ab)^2 = (ba)^2 = (ca)^2 = (ac)^2 = (bc)^2 = (cb)^2$

$abc = bca = cab$: $abc = cba = bac$;

$bab = cac$; $aba = cbc$; $aca = bcb$

$(bc)^3 = cb$; $(ab)^3 = ba$; $(ca)^3 = ac$

$(ab)^4 = e = (bc)^4$ and so on

$\therefore$ The elements of this group are

$\{ e, a, b, c, ab, (ab)^2, (ab)^3, bc, ca, cb,$
$ac, cbc, aca, abc, acb, bab \}$

1.5: S_3-group of permutation on three elements is a group of order 6. The elements of S_3 are of the form $\{\psi, \psi^2, \psi^3 = e, \phi, \phi\psi, \phi\psi^2\}$ and the operation is given by the following table.

•	ψ	ψ^2	e	ϕ	$\phi\psi$	$\phi\psi^2$
ψ	ψ^2	e	ψ	$\phi\psi^2$	ϕ	$\phi\psi$
ψ^2	e	ψ	ψ^2	$\phi\psi$	$\phi\psi^2$	ϕ
e	ψ	ψ^2	e	ϕ	$\phi\psi$	$\phi\psi^2$
ϕ	$\phi\psi$	$\phi\psi^2$	ϕ	e	ψ	ψ^2
$\phi\psi$	$\phi\psi^2$	ϕ	$\phi\psi$	ψ^2	e	ψ
$\phi\psi^2$	ϕ	$\phi\psi$	$\phi\psi^2$	ψ	ψ^2	e

CHAPTER II

GROUPS WHICH ARE THE UNION OF THREE GROUPS:

In this section we consider groups which can be written as the union of three subgroups. We first dispose of the union of two subgroups.

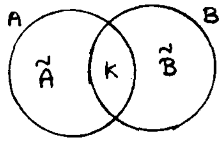
THEOREM 2.1:

Except for trivial cases, a group can not be the union of two subgroups.

PROOF:

Let G be a group, suppose there exists two subgroups A and B such that $A \cup B = G$, then $A = G$ (or) $B = G$ are the two trivial possible cases (In such cases one sub group is a sub set of another sub group).

Suppose we have the situation as in the figure



$\tilde{A} = A - K, \quad \tilde{B} = B - K$

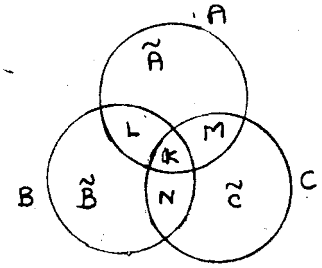
with $\tilde{A} \neq \emptyset$ and $\tilde{B} \neq \emptyset$, then we get a controdiction. Let $\tilde{a} \in \tilde{A}$, $\tilde{b} \in \tilde{B}$ then $\tilde{a}\tilde{b} \in A$ implies $\tilde{b} \in A$ and $\tilde{a}\tilde{b} \in B$ implies $\tilde{a} \in B$. Both of which controdicts the hypothesis. Hence $\tilde{a}\tilde{b} \notin A \cup B = G$ which controdicts the closure property of G.

Now we consider the 3 - group case suppose A, B, C are three subgroups of G such that $A \cup B \cup C = G$ then we have the following results.

RESULT 2.1.

If $A \subsetneq B$ we are effectively dealing with two subgroups of G and this is not possible by theorem 2.1.

$G = A \cup B \cup C$ with $A \subseteq B$ is not possible similarly $B \subsetneq C$, $C \subseteq A$ etc. are not possible. Hence we have the configuration of the following figure, where $\tilde{A} = A-K$, $\tilde{B} = B-K$ and $\tilde{C} = C-K$ are non empty sets.



RESULT 2.2.:

$$L = M = N = \emptyset$$

Proof:

Let $l \in L$, then for any $\tilde{c} \in \tilde{C}$ we've

$\tilde{c}l \in C$ implies $l \in C$ $(\because \tilde{c}^{-1} \in C)$

$\tilde{c}l \in B$ implies $\tilde{c} \in B$ $(\because l^{-1} \in B)$

$\tilde{c}l \in A$ implies $\tilde{c} \in A$ $(\because l^{-1} \in A)$

All of which controdicts the hypothesis.

since $\tilde{C} \neq \emptyset$, we have $L = \emptyset$

similarly we can prove $M=N=\emptyset$

RESULT 2.3:

Each of $\tilde{A}$, $\tilde{B}$ and $\tilde{C}$ contains its inverses

PROOF:

Let $\tilde{a} \in \mathbb{A}$ then $\tilde{a}^{-1} \in \mathbb{A} = \tilde{A} \cup \mathbb{K}$ ($\because \mathbb{A}$ is a group and $L=M=\emptyset$)

If $\tilde{a}^{-1} \in \mathbb{K}$ then

$\tilde{a} = (\tilde{a}^{-1})^{-1} \in \mathbb{K}$ ($\because \mathbb{K} = A \cap B \cap C$ is again a group)

which controdicts the hypothesis.

Hence $\tilde{a}^{-1} \in \tilde{A}$

similarly we can show that each of $\tilde{B}$ and $\tilde{C}$ contains its inverses.

RESULT 2.4:

If $\tilde{a} \in \tilde{A}$ and $\tilde{b} \in \tilde{B}$ then $\tilde{a} \cdot \tilde{b} \in \tilde{C}$

PROOF: If not let $\tilde{a} \cdot \tilde{b} \in A \cup B$ then $\tilde{a}, \tilde{b} \in \tilde{A} \cup \tilde{B}$ (or) $\tilde{a}, \tilde{b} \in \mathbb{K}$.

If $\tilde{a} \cdot \tilde{b} \in \mathbb{K}$ $(\subseteq \mathbb{A})$ then $(\tilde{a}^{-1})$ $(\tilde{a}, \tilde{b}) = \tilde{b} \in \mathbb{A} = \tilde{A} \cup \mathbb{K}$

but $\tilde{b}$ is neither in $\tilde{A}$ nor in $\mathbb{K}$ by hypothesis

$\therefore \tilde{a} \cdot \tilde{b} \notin \mathbb{K}$

If $\tilde{a} \cdot \tilde{b} \in \tilde{A}$ then $\tilde{a}^{-1}$ $(\tilde{a} \cdot \tilde{b}) = \tilde{b} \in A = \tilde{A} \cup \mathbb{K}$ a controdiction

$\therefore \tilde{a} \cdot \tilde{b} \notin \tilde{A}$. for a similar reason $\tilde{a} \cdot \tilde{b} \notin \tilde{B}$

therefore $\tilde{a} \in \tilde{A}$, $\tilde{b} \in \tilde{B}$ implies $\tilde{a}\, \tilde{b} \in \tilde{C}$

similarly we have

$\tilde{a} \in \tilde{A}$, $\tilde{c} \in \tilde{C}$ implies $\tilde{c} . \tilde{a} \in \tilde{B}$

$\tilde{b} \in \tilde{B}$, $\tilde{c} \in \tilde{C}$ implies $\tilde{b} \cdot \tilde{c} \in \tilde{A}$

REMARK:

Since each of $\tilde{A}$, $\tilde{B}$, $\tilde{C}$ contains it's inverses we also have $\tilde{b}, \tilde{a} = (\tilde{a}^{-1}\, \tilde{b}^{-1})^{-1} \in \tilde{C}$ when ever $\tilde{a} \in \tilde{A}$ and $\tilde{b} \in \tilde{B}$ and so on.

RESULT 2.5

If $\tilde{a}, \tilde{a}_1 \in \tilde{A}$ then $\tilde{a}.\tilde{a}_1 \in K$

PROOF: $\tilde{a}$, $\tilde{a}_1 \in A = \tilde{A} \cup K$ for $\tilde{a}, \tilde{a}_1 \in \tilde{A}$.

If $\tilde{a}, \tilde{a}_1 \in \tilde{A}$ then for $\tilde{b} \in \tilde{B}$, $\tilde{b}(\tilde{a}.\tilde{a}_1) \in \tilde{C}$ (By result 2.4)

but $(\tilde{b}.\tilde{a}) \in \tilde{C}$ and $\tilde{a}_1 \in \tilde{A}$ implies $(\tilde{b}.\tilde{a})\ \tilde{a}_1 \in \tilde{B}$

which controdicts the fact that $\tilde{B} \cap \tilde{C} = \emptyset$.

$\therefore\ \tilde{a}\ \tilde{a}_1 \in K$

REMARK:

Similarly we have

$\tilde{b}, \tilde{b}_1 \in \tilde{B}$ implies $\tilde{b}\ \tilde{b}_1 \in K$ and

$\tilde{c}, \tilde{c}_1 \in \tilde{C}$ implies $\tilde{c}, \tilde{c}_1 \in K$

RESULT 2.6:

$K = A \cap B \cap C$ is an invariant subgroup of G

PROOF: clearly $K = A \cap B \cap C$ is a Subgroup of G

Now to prove that $g\ k\ g^{-1} \in K$. for every $g \in G$ and $k \in K$.

If $\tilde{a} \in \tilde{A}$ and $k \in K$ then $k\ \tilde{a} \in A = \tilde{A} \cup K$

If $k\ \tilde{a} \in K$ then $\tilde{a} \in K$

Theretore $k\ \tilde{a} \in \tilde{A}$, this together with $\tilde{a}^{-1} \in \tilde{A}$

implies $\tilde{a}^{-1}\ k\ \tilde{a} \in K$ (by result 2.5)

Thus we have proved that

$\tilde{a} \in \tilde{A}$, $k \in K$ implies $\tilde{a}^{-1}\ k\ \ \tilde{a} \in K$

similarly we can show that

$\tilde{b} \in \tilde{B}$, $k \in K$ implies $\tilde{b}^{-1}\ k\ \ \tilde{b} \in K$ and

$\tilde{c} \in \tilde{C}$, $k \in K$ implies $\tilde{c}^{-1}\ k\ \tilde{c} \in K$

Since, $G = \tilde{A} \cup \tilde{B} \cup \tilde{C} \cup \tilde{K}$ we have K is an invariant subgroup of G.

RESULT 2.7

$$\tilde{a}K = \tilde{A} \text{ for } \tilde{a} \in \tilde{A} .$$

PROOF:

Let $k \in K$ then

$\tilde{a}, k \in A$ ($\because A$ is a subgroup and $\tilde{A} \cup K = A$).

if $\tilde{a}\, k \in K$ then $(a\, k)k^{-1} = a\, K$ a controdiction

i.e $\tilde{a}\, K \subseteq \tilde{A}$

conversely let $\tilde{a}_1 \in \tilde{A}$ then $\tilde{a}^{-1}\; a_1 \in K$ (by result 2.3 and 2.5)

this implies $\tilde{a}_1 \in \tilde{a}K$.

i.e. $\tilde{A} \subseteq \tilde{a}K$

similarly we can show that $\tilde{b}\, K = \tilde{B}$ and

$$\tilde{c}\, K = \tilde{C}$$

using the above results we can characterize a 3 - group (i.e group which can be expressed as a non trivial union of three group) in the following way.

THEOREM 2.2:

A Group G is the (nontrivial) union of three subgroups if and only if it is homomorphic to the klein four group.

PROOF:

Let $G = A \cup B \cup C$, and $\tilde{A}, \tilde{B}, \tilde{C}$ as given above then $K = A \cap B \cap C$ is an invariant sub group of G by result 2.6 one can prove that

$\frac{G}{\mathbb{K}} = \{\mathbb{K}, \tilde{A}, \tilde{B}, \tilde{C}\}$

For $\frac{G}{\mathbb{K}} = \{gK \mid g \in G\} = \{gK \mid g \in \tilde{A} \cup \tilde{B} \cup \tilde{C} \cup \mathbb{K}\}$

If $g \in \mathbb{K}$ then $gk = \mathbb{K}$

If $g \in \tilde{A}$ then $gk = \tilde{A}$

If $g \in \tilde{B}$ then $gk = \tilde{B}$ (By result 2.7)

If $g \in \tilde{C}$ then $gk = \tilde{C}$

Hence We've $\frac{G}{\mathbb{K}} = \{\tilde{A}, \tilde{B}, \tilde{C}, \mathbb{K}\}$ and it is a factor group

since $\tilde{A}.\tilde{B} = (\tilde{a}\mathbb{K})(\tilde{b}\mathbb{K})$ for $\tilde{a} \in \tilde{A}$, $\tilde{b} \in \tilde{B}$

$= (\tilde{a}.\tilde{b})\,\mathbb{K}$

$= \tilde{C}\,\mathbb{K} = \tilde{C}\ (\tilde{a}.\tilde{b} \in \tilde{C})$

and similarly $\tilde{B}.\tilde{C} = \tilde{A}$, $\tilde{C}.\tilde{A} = \tilde{B}$ and $\tilde{A}.\mathbb{K} = \tilde{A}$ etc.

Also $\tilde{A}^2 = \tilde{a}_1 K . \tilde{a}_2 K = (\tilde{a}_1 \tilde{a}_2)\,\mathbb{K}$ (for $\tilde{a}_1, \tilde{a}_2 \in \tilde{A}$)

$= \mathbb{K}$ ($\because \tilde{a}_1, \tilde{a}_2 \in \mathbb{K}$)

and similarly $\tilde{B}^2 = \tilde{C}^2 = \mathbb{K}$

Hence we have $\frac{G}{\mathbb{K}}$ is a k lein four group

and we denote it by the symbol V

we define a map $\phi : G \longrightarrow G|\mathbb{K}$ $(=V)$ such that

$\phi(g) = g\mathbb{K}$. this gives an on to

homomorphism between G and the klein four group V.

<u>CONVERSE</u>:

Let $\phi : G \longrightarrow V$ be an onto

homomorphism. Then we prove that G can be expressed

as a union of 3 proper subgroups.

Let $\mathbb{K} = \text{Ker}\,\phi$ and $\tilde{A}$, $\tilde{B}$, $\tilde{C}$ be the cosets of $\mathbb{K}$ in G.

Define $\mathbb{A} = \tilde{\mathbb{A}} \cup \mathbb{K}$ $B = \tilde{B} \cup \mathbb{K}$ and $C = \tilde{C} \cup \mathbb{K}$

since $\frac{G}{\operatorname{Ker} \emptyset} = \frac{G}{\mathbb{K}}$ is isomorphic to V-the

klein four group, $\frac{G}{\mathbb{K}}$ has only 4 elements

$\{\mathbb{K}, \tilde{\mathbb{A}}, \tilde{B}, \tilde{C}\}$

such that $\tilde{\mathbb{A}}^2 = \tilde{B}^2 = \tilde{C}^2 = \mathbb{K}$,

$\tilde{\mathbb{A}}\tilde{B} = \tilde{C}$ etc with the identity element $\mathbb{K}$

now we prove that A, B, C defined above

are sub groups of G and $\mathbb{A} \cup B \cup C = G$ gives

the required decomposition of G.

CLOSURE AXIOM:

Let $a, a_1 \in \mathbb{A}$, then

$a \cdot a_1 \in \mathbb{K}$ if both $a, a_1 \in \tilde{\mathbb{A}}$ or $\mathbb{K}$. $(\because \tilde{A}\tilde{A} = K)$

If $a \in \tilde{\mathbb{A}}$ and $a_1 \in \mathbb{K}$ then $a \cdot a_1 \in \tilde{\mathbb{A}}$ $(\because \tilde{\mathbb{A}}\,\mathbb{K} = \tilde{\mathbb{A}})$

Therefore we have $a \cdot a_1 \in \mathbb{A}$ for every $a, a_1 \in \mathbb{A}$.

INVERSE:

If $a \in \mathbb{A}$ then

$a \in \tilde{\mathbb{A}}$ implies $a^{-1} \in \tilde{\mathbb{A}} \subseteq \mathbb{A}$ and

$a \in K$ implies $a^{-1} \in K \subseteq \mathbb{A}$

Therefore A is a subgroup of G

similarly we can prove B, C are subgroups of G.

REMARK:1 If G is a finite group such that it is the union of three non trivial subgroups then order of $(G) = 4m$.

PROOF: By theorem 2.2 $\frac{G}{\mathbb{K}}$ is isomorphic to V with $\mathbb{K} = \mathbb{A} \cap B \cap C$ is an invariant subgroup of G.

order of $(\frac{G}{\mathbb{K}})$ = order of V = 4 i.e. $\frac{\text{order of } G}{\text{order of } K} = 4$

i.e. order of G = 4m where m is an integer

REMARK 2:

But there are many subgroups of order 4m which are not the union of three proper subgroups.

We now give two examples of group of order 4m but 3-groups

EXAMPLE 2.1

Any cyclic group can not be expressed as a union of its proper sub groups. For if G is cyclic with generator a and $G = \bigcup_{i \in I} A_i$ we have $a \in A_i$ for atleast on i and that $A_i = G$ - the whole group Hence in particular a cyclic group (C_{4m}) of order 4m is not a 3-group.

EXAMPLE 2.2

Any locally cyclic group and hence of order 4m is not a 3 - group. (By locally cyclic and it is not necessary cyclic as a whole group).

If G = AUBUC is the decomposition of three group of a locally cyclic group G, then $\tilde{A}$, $\tilde{B}$, $\tilde{C}$ are disjoint subsets of G by result 2.1

for $\tilde{a} \in \tilde{A}$, $\tilde{b} \in \tilde{B}$ we get a non cyclic subgroup generated by and $\tilde{a}$ and $\tilde{b}$ i.e $\langle a, b \rangle$ of G. For if the above subgroup is cyclic subgroup then $\tilde{b} = (\tilde{a})^m$ for some positive integer m

but $\tilde{a}^m \in \mathbb{K}$ by repeated application of 2.5
i.e $\tilde{b} \in \mathbb{K}$ which is a contradiction.

We now list some examples of 3 - groups

EXAMPLE 2.3:

The Klein - four group V itself is a 3 - group

$$V = \left\{ e, a, b, c \;\middle|\; \begin{array}{l} a^2 = b^2 = c^2 = e, \\ ab = c,\ bc = a,\ ca = b \end{array} \right\}$$

consider $C_2 = \{a,\ a^2 = e\}$

$C_2 = \{b,\ b^2 = e\}$

$C_2 = \{c,\ c^2 = e\}$ the cyclic groups of order 2

Then we find $V = \{C_2, C_2, C_2\}$ is the required decomposition.

EXAMPLE 2.4:

There are 5 groups of order 8 they are
C_8, $C_4 x C_2$, $C_2 x C_2 x C_2$, D_4 and
Q = the group of Quaternions except C_8, the other groups are 3-groups.

1) C_8 being a cyclic group it has no decomposition

2) $C_4 \times C_2 = \{ (a,b) \mid$ a is the generator of the cyclic group C_4 and b is the generator of $C_2 \}$

i.e. $C_4 \times C_2 = \{ (a,b), (a^2,b), (a^3,b), (e.b), (a,e'), (a^2, e'), (a^3,e'), (e,e') \}$

where $a^4 = e$ and $b^2 = e'$ are the identity elements of C_4 and C_2 respectively

Then $C_4 = \{(a,b),\ (a^2,e'),\ (a^3,b),\ (e,e')\}$

$C_4 = \{(a,e'),\ (a^2,e'),\ (a^3,e'),\ (e,e')\}$

$V = \{(a^2,b),\ (a^2,e'),\ (e,b),\ (e,e')\}$

give a decomposition for $C_4 \times C_2$

$C_4 \times C_2 = \{C_4,\ C_4,\ V\}$ is a 3-group

where C_4 - is the cyclic group of order 4 and V is the klein gour group

3) $C_2 \times C_2 \times C_2 = \{V,\ V,\ V\}$ is a decomposition

with $C_2 = \{b,\ b^2 = e'\}$

$C_2 \times C_2 \times C_2 = \{(b,\ b,\ b),\ (b,b,e'),\ (b,\ e',b),$
$(e',\ b,\ b),\ (e',\ e',\ b),\ (e',\ b,\ e'),\ (b,\ e',\ e'),$
$(e',\ b,\ b),\ (e',e',b),\ (e',b,e'),\ (b,e',e'),$
$(e',\ e',e')$

$V = \{(b,\ e',\ b),\ (e',b,b),\ (b,b,e')\ (e',\ e',\ e')\}$
$V = \{(b,e',e')\ (e',\ b,e')\ ,\ (b,b,e'),\ (e',e',e')\}$
$V = \{(b,b,b),\ (b,b,e'),\ (e',e',b),\ (e',e',e')\}$

4) D_4 - the dihedral group of order 8.

(Example 3 of section 1) has a decomposition $\{C_4, V, V\}$

The group D_4 is $\{a,\ a^2,\ a^3,\ a^4 = e,\ b,\ ab,\ a^2b,\ a^3b\}$

with $a^4 = b^2 = (ab)^2 = e$

Consider $C_4 = \{a,\ a^2,\ a^3, a^4 = e\}$

$V = \{a^2, b,\ a^2b,\ e\}$

$V = \{ab,\ a^2,\ a^3b,\ e\}$ then $D_4 = \{C_4,\ V,\ V\}$

5) $Q = \{ i, j, k, -i, -j, -k, 1, -1 \}$ with $i^2 = j^2 = k^2 = -1$, $ij = k$; $jk = i$, $ki = j$ and $ij = -ji$.

This group of quaternions Q has decomposition

C_4', C_4, C_4 where $C_4 = i, i^2 = -1, i^3 = i, i^4 = 1$

$C_4 = j, j^2 = -1, j^3 = -j, j^4 = 1$

$C_4 = k, k^2 = -1, k^3 = -r, k^4 = 1$

NOTE: Two decompositions $\{x, y, z\}$ and $\{X_1, Y_1, Z_1\}$ of a group G are said to be the same if there exists isomorphisms $x \to X_1$, $y \to y_1$, and $Z \to Z_1$.

REMARKS:

In the above examples one can prove that they are the only decompositions for the corresponding groups.

EXAMPLE: 2.5:

The Dihedral group D_{2m} of Order 4m for all m admits a decomposition of three groups.

$D_{2m} = \{ a, a^2, a^3 \ldots a^{2m-1}, e, b, a^k b \; k=1 \text{ to } 2m-1 \}$

(As in example 1.3) The subgroup $K = \{ a^2, a^4 \ldots a^{2(m-1)}, e \}$ is an invariant subgroup of D_{2m},

For $a^k k a^{-k} = a^k a^{2k'} a^{-k} = a^{2k'} \in K$

$bkb^{-1} = ba^{2k'} b^{-1} = b^2 a^{-2k} = a^{-2k'} \in K$

$(a^k b) \, k \, (a^k b)^{-1} = a^k (bkb^{-1}) \, a^{-k}$

$= a^k a^{-2k'} a^{-k} = a^{-2k'} \in K$

i.e. $xkx^{-1} \in K$ for every $x \in D_{2m}$, $k \in K$

i.e. K is an invariant subgroup of G.

Therefore $\dfrac{D_{2m}}{K}$ is a group.

$$\frac{D_{2m}}{\mathbb{K}} = \{ x\mathbb{K} \;/\; x \in D_{2m} \}$$

If $x=a^k$, $0 \leq k \leq 2m$ then $a^{2k}\mathbb{K} = \mathbb{K}$ and $a^{2k+1}\mathbb{K} = a\mathbb{K}$

If $x=b$ then $x\mathbb{K} = b\mathbb{K}$

If $x= a^k b$ $1 \leq k \leq 2m-1$ then $x\mathbb{K} = a^k b\mathbb{K} = ba^{-k}\mathbb{K}$

$=ba\mathbb{K}$ if k is odd

$=b\mathbb{K}$ if k is even.

but $ba\mathbb{K} = ab\mathbb{K}$ as $aba^{-1}b^{-1} = a^2 \in \mathbb{K}$

Therefore $\frac{D_{2m}}{\mathbb{K}} = \{ \mathbb{K},\ a\mathbb{K},\ b\mathbb{K},\ ab\mathbb{K} \}$

This is a klein four group, since $\mathbb{K}^2 = \mathbb{K}.\mathbb{K} = \mathbb{K}$, $ab\mathbb{K} = a\mathbb{K}\, b\mathbb{K}$, $b\mathbb{K}.ab\mathbb{K} = bab\mathbb{K} = a^{-1}\mathbb{K} = a\mathbb{K}$, and $a\mathbb{K}.ab\mathbb{K} = a^2b\mathbb{K} = ba^{-2}\mathbb{K} = b\mathbb{K}$. (By the definition of $\mathbb{K}$)

Therefore by theorem 2.2 D_{2m} has a decomposition of three groups AUBUC where $A = \mathbb{K} \cup a\mathbb{K} = \{a, a^2, \ldots a^{2m-1}, a^{2m}=e\} = C_{2m}$

$B = \mathbb{K} \cup b\mathbb{K} = \{a^2, a^4, \ldots a^{2m-2}, e, b, a^k b,\quad k = 2,4,\ldots 2m-2\}$

which is of the form $\{x, x^2, \ldots x^m = e, b, x^{k'}b\}$ where $k'= 1$ to $m-1$ and $x=a^2$ is a dihedral group D_m of order $2m$

$C = \mathbb{K} \cup ab\mathbb{K} = \{a^2, a^4, \ldots a^{2m-2}, a^{2m} = e, aba^k\}$ where $k = 2,4,\ldots 2m.$

$= \{a^2, a^4 \ldots a^{2m-2}, e, a^{k'}b\}$

where $k'= 1,3, \ldots 2m-1$, which is of the form $\{x, x^2 \ldots x^m = e, ab, x^k ab\}$ where $k = 1$ to $m-1$, $x=a^2$ is a dihedral group D_m of order $2m$.

Therefore $D_{2m} = \{ C_{2m}, D_m, D_m \}$

From the following examples we shall see that a 3-group can have different decompositions and two different 3-groups can have the same decompositions.

EXAMPLES:2.6:

Let $C_2 = \{d, d^2 = e\}$ and $D_4 = \{a, a^2, a^3, a^4 = e, b, ab, a^2b, a^3b\}$. Then
$C_2 X D_4 = \{(d,a), (d,a^2), (d,a^3), (d,e), (d,b), (d,ab), (d,a^2b), (d,a^3b), (e',a), (e',a^2), (e',a^3), (e',e), (e',b), (e',ab), (e',a^2b), (e',a^3b)\}$

$C_2 \times C_4 = \{(d,a), (e',a^2), (d,a^3), (e',a^4) = (e',e), (d,a^2), (d,a^3), (d,e), (e',a)\}$ is isomorphic to $C_4 \times C_2$

$D_4 = \{(d,a), (d,a)^2 (= (e',a^2)), (d,a)^3 = (d,a^3), (d,a)^4 (= (e',e)), (d,b), (e',ab), (d,a^2b), (e',a^3b)\}$

and $D_4 = \{(d,a), (d,a)^2, (d,a)^3, (d,a)^4, = (e',e), (d,ab), (e',a^2b), (d,a^3b), (e',b)\}$

Therefore we find that

$C_2 \times D_4 = \{C_4 \times C_2, D_4, D_4\}$ is a decomposition.

Now Consider $B' = \{(d,a^2), (d,e), (e',a^2), (e',e), (d,b), (e',a^2b), (d,a^2b), (e',b)\}$

and $C' = \{(d,a^2), (d,e), (e',a^2), (e',e), (d,ab), (e',a^3b), (d,a^3b), (e',ab)\}$

Then we see that $C_2 \times D_4$ is also equal to $\{C_4 \times C_2, B', C'\}$

where B' is isomorphic to $C_2 \times C_2 \times C_2$ by means of the isomorphism $\emptyset : B' \longrightarrow C_2 \times C_2 \times C_2$ taking

$(e',e) \longrightarrow (e,e,e)$, $(d,b) \longrightarrow (e',d,d)$, $(d,a^2b) \longrightarrow (d,d,e')$, $(e',a^2) \longrightarrow (d,e',d)$,
$(d,a^2) \longrightarrow (d,d,d)$, $(e',a^2b) \longrightarrow (d,e,e)$,
$(e',b) \longrightarrow (e,e,d)$ and $(d,e) \longrightarrow (e,d,e)$

Similarly C' is also isomorphic to $C_2 \times C_2 \times C_2$

Therefore $C_2 \times D_4$ has two different decompositions,

$\{C_4 \times C_2, D_4, D_4\}$ and $\{C_4 \times C_2, C_2 \times C_2 \times C_2, C_2 \times C_2 \times C_2\}$

In the next example we see that a group of order 16 defined by the generating relations $a^2=b^2=c^2=e$, $abc=bca=cab$ also has the decomposition $\{C_4 \times C_2, D_4, D_4\}$

By example:1.5 the above group of order 16 is given by $\{e, a, b, c, ab, (ab)^2, (ab)^3, bc, ca, cb, ac,$
$cbc, aca, abc, acb, bab\}$

$D_4 = \{(ab), (ab)^2, (ab)^3, (ab)^4=e, a, cbc, bab, b\}$.
$D_4 = \{bc, (ab)^2(=(bc)^2), cb(=(bc)^3), e, c, b, aca, cbc\}$ [∵ from Example 1.5]
$C_4 \times C_2 \simeq D = \{(ca), (ab)^2, (ac), e, cbc, acb, b, abc\}$

under the isomorphism $\emptyset : D \longrightarrow C_4 \times C_2$

given by $(ca) \longrightarrow (g,e)$, $(ab)^2 \longrightarrow (g^2,e)$,
$(ac) \longrightarrow (g^3,e)$, $e \longrightarrow (e',e)$,
$(abc) \longrightarrow (g,h)$, $(cbc) \longrightarrow (g^2,h)$
$(acb) \longrightarrow (g^3,h)$, $b \longrightarrow (e',h)$

∴ The above group of order 16 has decomposition $= \{C_4 \times C_2, D_4, D_4\}$

Next we shall see different types of decomposition of a given 3-group G. If a 3-group is non abelion then the subgroups of a decomposition can be abelian (@) or non abelion (n). This gives 4 possible types of decomposition namely $\{@,@,@\}$, $\{@,@,n\}$, $\{@,n,n\}$, $\{n,n,n\}$. However one can see that the decomposition of type $\{@,@,n\}$ is not possible from the following theorem.

THEOREM:2.3:

If G has decomposition $\{A,B,C\}$ where A and B are abelion then C is also abelion.

PROOF:

$$\mathbb{K} = A \cap B \cap C \subseteq A$$

Therefore $\mathbb{K}$ is abelion.

Now to prove $C = \tilde{C} \cup \mathbb{K}$ is abelion it is enough if we prove that $\tilde{C}$ is commutative and elements of $\tilde{C}$ commute with elements of $\mathbb{K}$.

Let $\tilde{c}_1, \tilde{c}_2$ be two elements of $\tilde{C}$

By theorem 2.2, since G is a 3-group $\tilde{A}\tilde{B} = \tilde{C}$

Therefore $\tilde{c}_1 = \tilde{a}\tilde{b}$ with $\tilde{a} \in A$, $\tilde{b} \in B$

But $\tilde{A} = \tilde{a}\mathbb{k}$; $\tilde{B} = \tilde{b}\mathbb{k}$ implies $\tilde{c}_2 \in \tilde{a}\mathbb{k}.\tilde{b}\mathbb{k}$

i.e. $\tilde{c}_2 \in \tilde{a}\tilde{b}k$ i.e. $\tilde{c}_2 = \tilde{a}\tilde{b}k$ with $k \in K$

Therefore $\tilde{c}_1\tilde{c}_2 = (\tilde{a}\tilde{b})\ (\tilde{a}\tilde{b})k$ (Since A and Bare abelion and $k \in \mathbb{K}$)

$$= (\tilde{a}\tilde{b}k)\ (\tilde{a}\tilde{b})$$

$$= \tilde{c}_2\tilde{c}_1$$

i.e. $\tilde{C}$ is commutative.

Next to prove the elements of $\tilde{C}$ commutes with elements of $\mathbb{k}$.

Let $\tilde{c} \in \tilde{C}$, $k \in \mathbb{K}$

$$\tilde{c}k = (\tilde{a}\tilde{b})k \qquad \text{where } \tilde{a} \in \tilde{A}, \tilde{b} \in \tilde{B}$$

$$= k\ (\tilde{a}\tilde{b}) = k\tilde{c} \qquad (K \subseteq A, \text{Bare abelion})$$

Therefore C is commutative.

NOTE: The remaining three types of decomposition all exist. It is shown in the following examples.

EXAMPLE: 2.7

I. By example(2.4) 5, $Q = \{C_4, C_4, C_4\}$ is of the form $G \longrightarrow \{@, @, @\}$

II. Next we shall give a decomposition of type $\{@, \eta, \eta\}$

i.e. $D_6 = \{C_6, S_3, S_3\}$.

$D_6 = \{ a, a^2, a^3, a^4, a^5, a^6 = e, b, a^k b \quad k = 1 \text{ to } 5\}$

$C_6 = \{ a, a^2, a^3, a^4, a^5, a^6 = e \}$

$S_3 = \{a^2, a^4, a^6 = e, b, a^2 b, a^4 b\}$ of the form

$\{ \psi, \psi^2, \psi^3 = e, \phi = \phi\psi = ba^2 = a^{-2}b = a^4 b,$

$\phi\psi^2 = ba^4 = a^2 b \}$

$S_3 = \{a^2, a^4, a^6 = e\ ab, a^3 b, a^5 b\}$ of the form

$\{\psi, \psi^2, \psi^3 = e, \phi, \phi\psi = aba^2 = a^5 b, \phi\psi^2 = aba^4 = a^3 b\}$

$\therefore D_6 = \{C_6, S_3, S_3\} \longrightarrow \{@, n, n\}$

(3) The following decomposition of $S_3 \times V$ is of type $\{n, n, n\}$

$S_3 = \{ \psi, \psi^2, \psi^3 = e', \phi, \phi\psi, \phi\psi^2\}$

- permutation group of order 6.

$V = \{e, a, b, c\}$ - the klein four group.

Then $S_3 \times V = \{ (\psi, e), (\psi, a), (\psi, b), (\psi, c),$
$(\psi^2, e), (\psi^2, a), (\psi^2, b), (\psi^2, c),$
$(e', e), (e', a), (e', b), (e', c),$
$(\phi, e), (\phi, a), (\phi, b), (\phi, c),$
$(\phi\psi, e), (\phi\psi, a), (\phi\psi, b), (\phi\psi, c),$
$(\phi\psi^2, e), (\phi\psi^2, a), (\phi\psi^2, b), (\phi\psi^2, c)\}$

$$D_6 = \{ (\psi, a)^k \ , \ k = 1 \text{ to } 6, \ (\phi, a), \ (\psi, a)^k (\phi, a) \ , \ k = 1 \text{ to } 5 \}$$

$$= \{ (\psi, a), \ (\psi^2, e), \ (e', a), \ (\psi, e), \ (\psi^2, a), \ (e', e), \ (\phi, a), \ (\phi\psi^2, e), \ (\phi\psi, a), \ (\phi, e), \ (\phi\psi^2, a), \ (\phi\psi, e) \}$$

$$D_6 = \{ (\psi, b)^k \ , \ k = 1 \text{ to } 6, \ (\phi, b), \ (\psi, b)^k (\phi, b) \ \ k = 1 \text{ to } 5 \}$$

$$= \{ (\psi, b), \ (\psi^2, e), \ (e', b), \ (\psi, e), \ (\psi^2, b), \ (e', e), \ (\phi, b), \ (\phi\psi^2, e), \ (\phi\psi, b), \ (\phi, e), \ (\phi\psi^2, b), \ (\phi\psi, e). \}$$

$$D_6 = \{ (\psi, e)^k, \ (\phi, e), \ (\psi, e)^k \cdot (\phi, c) \ k = 1 \text{ to } 5 \}$$

$$= \{ (\psi, e), \ (\psi^2, e), \ (e', c), (\psi, e), (\psi^2, c), (e', e), (\phi, e), (\phi^2, e), \ (\phi\psi, c), \ (\phi, e), \ (\phi\psi^2, c), \ (\phi\psi, e) \}$$

$$S_3 \times V \rightarrow \{ D_6, D_6, D_6 \} \longrightarrow \{ \eta, \eta, \eta \}$$

Note here $\mathbb{K} = \{(\psi, e), (\psi^2, e), (\phi, e), (\phi\psi, e),$
$(\phi\psi^2, e), (e', e)\}$ of the decomposition

We summarize these results in the following theorem

THEOREM: 2.4

Each decomposition of a 3-group is one of the forms $\{@, @, @\}, \{@, m, n\}$ (or) $\{n, n, n\}$.

We know that the centre of an abelian group G is the whole group G itself. In the next theorem we see that if a non abelian group G has abelian decomposition then the centre of **G=K.**

THEOREM: 2.5:

A non abelian 3-group G has an abelian decomposition (ie) $G \longrightarrow \{@, @, @\}$ if and only if the centre of G is K.

PROOF: Let $G = \{A, B, C\}$ and let Z be the centre of G and $K = A \cap B \cap C$

Firstly we assume that A, B and C are abelian and prove that K=Z.

Let $k \in K$, k commutes with elements of A, B and C as $K \subseteq A, B, C$ are abelian $\therefore k \in z$

(ie) $K \subseteq Z$

Next to prove $Z \subseteq K$

It there exists $x \in z$ such that $x \notin k$ then $x \in \tilde{A}$ or $\tilde{B}$ or $\tilde{C}$

Let $x = a_z \in z \cap \tilde{A}$ then

for each $\tilde{c} \in \tilde{C} = \tilde{A}\tilde{B} = (\tilde{a}_z K)\tilde{B} = \tilde{a}_z \tilde{B}$

There exists $\tilde{b} \in B$ such that $\tilde{C} = \tilde{a}_z \tilde{b}$

For each $b \in B$, $\tilde{C}b = \tilde{a}_z \tilde{b} b = b(\tilde{a}_z \tilde{b})$

$= b\tilde{c}$ ($\because B$ is abelian and $\tilde{a}_z \in Z$)

This implies elements of B commute with elements of C.

Also for each $\tilde{a} \in \tilde{A} = \tilde{a}_z K$ there exists some element $k \in K$ such that $\tilde{a} = \tilde{a}_z k$

For every $b \in B$, $\tilde{a}b = \tilde{a}_z k b = b(\tilde{a}_z k) = b\tilde{a}$

$\Longrightarrow$ Elements of A commute with elements of B.

Similarly we can show that element of A and C commute. Hence it follows that G is abelian which is a controdiction.

Hence $Z=K$.

conversely if $Z=K$ then to prove that G has abelian decomposition let $\tilde{a} \in \tilde{A} = \tilde{a}_1 K$ for some fixed $\tilde{a}_1 \in \tilde{A}$, then

$\tilde{a} = \tilde{a}_1 k$ for some $k \in K$

$\therefore$ for $\tilde{a}, \tilde{a}' \in \tilde{A}$ we have $\tilde{a} = \tilde{a}_1 k$
$\tilde{a}' = \tilde{a}_1 k'$

$$\tilde{a} \cdot \tilde{a}' = (\tilde{a}_1 k) \cdot (\tilde{a}_1 k') = (\tilde{a}_1 k')(\tilde{a}_1 k)$$
$$= \tilde{a}' \tilde{a}$$

$\therefore \tilde{A}$ is commutative, this together with $K=Z$ implies A is abelian

similarly we can prove that B and C are abelian

In the next theorem we see that, when the decomposition of G is of type $\{@, n, n\}$ then the centre of G is contained in A.

THEOREM: 2.6:-

If G admits a decomposition $\{A, B, C\}$ of type $\{@, n, n\}$ then the centre z of G is contained in A.

PROOF:

We prove $Z \subseteq A$ by showing that $\tilde{B}$ and $\tilde{C}$ are disjoint from Z.

Let $\tilde{b}_z \in \tilde{B} \cap Z$. For each $\tilde{b} \in \tilde{B}$ there exists $k \in K$ such that $b = b_z k$

$\therefore \Rightarrow bk' = (\tilde{b}_z . k) k' = k'(\tilde{b}_z k)$ (K is abelian and $\tilde{b}_z \in Z$)

$= k' \tilde{b}$

$\therefore \tilde{B}$ commutes with elements of K

Let $\tilde{b}_1, \tilde{b}_2 \in \tilde{B}$ then $\tilde{b}_1 = \tilde{b}_z k$, $\tilde{b}_2 = \tilde{b}_z k'$

$\tilde{b}_1 \tilde{b}_2 = (\tilde{b}_z k)(\tilde{b}_z k') = (\tilde{b}_z k')(\tilde{b}_z k)$
$= \tilde{b}_2 \tilde{b}_1$

$\Rightarrow \tilde{B}$ is commutative this together with $\tilde{B}$ is commutative with k we have B is abelian which is a controdiction.

Similarly $\tilde{C} \cap Z \neq \emptyset$ implies C is abelian

Remark :1

From the example 2.7, We've seen that

$D_6 \rightarrow \{C_6, S_3, S_3\} \rightarrow \{@, \eta, \eta\}$

In this example $K = \{a^2, a^4, e\}$

$\tilde{A} = C_6 - K = \{a, a^3, a^5\}$ and

$Z = \{a^3, e\}$

$Z \cap A \neq \phi$

REMARK:2

From theorems 2.5 and 2.6 we have If G has a decomposition $\{A, B, C\}$ of type $\{@, \eta, \eta\}$ then the centre Z is either properly contained in K or atmost it also contains elements of $\tilde{A}$

REMARK:3

It is clear that Z cannot contain elements of $\tilde{A}$ and $\tilde{B}$ and not $\tilde{C}$, since in that case $Z\cap A$ and $Z\cap B$ give a nontrivial decomposition for the group Z and this controdicts theorem 2.1

REMARK:4

There is a possibility that Z contains elements of $\tilde{A}$, $\tilde{B}$ and $\tilde{C}$; in this case Z is itself necessarily a 3-group with decomposition

$$Z \longrightarrow \{Z\cap A,\ Z\cap B,\ Z\cap C\}$$

In the following three theorems, we study the properties of the group of inner automorphisms of a 3-group G.

Let $\tilde{I}$ (A) be the set of inner automorphisms of G defined by elements of A. Then $\tilde{I}$ (A) is a subgroup of I (G)-the group of inner automorphisms of G.

For, if ϕ, $\phi' \in \tilde{I}$ (A), then $\phi\,(g) = aga^{-1}$ with $a \in A$

and $\phi'\,(g) = a_1 . g a_1^{-1}$ with $a_1 \in A$

Now $\phi . \phi'^{-1}(g) = a(a_1^{-1} . g a_1)a^{-1}$

$$= (aa_1^{-1})g(aa_1^{-1})^{-1} \quad \text{where } aa_1^{-1} \in A$$

$\therefore\ \phi . \phi'^{-1} \in \tilde{I}$ (A)

THEOREM 2.7: The group of inner automorphisms of a 3-group G is either itself a 3-group or degenerate in the sense that it is one of $\tilde{I}(A)$, $\tilde{I}(B)$ (or) $\tilde{I}(c)$

PROOF: G=AUBUC implies

$$I(G) = \tilde{I}(A) \cup \tilde{I}(B) \cup \tilde{I}(C)$$

If $I(G)$ is not a 3-group then we have

$I(G)$ is either $\tilde{I}(A)$ (or) $\tilde{I}(B)$ (or) $\tilde{I}(c)$

REMARK:

we see from the following examples that the degeneracy does not necessarily preclude $I(G)$ from being 3-group

EXAMPLE: 2.8:

1) $Q \rightarrow \{C_4, C_4, C_4\}$ (Examples (2.4)(5))

This is of type $\{@, @, @\}$

$\therefore$ Z of $Q = \mathbb{K}$ by theorem 2.5

i.e. $I(Q) = \frac{Q}{Z} = \frac{Q}{\mathbb{K}} = V$ {By theorem 2.2}

In this example $\tilde{I}(c_4) = \{$identity mapping, the automorphism that takes $j \longrightarrow -j$, $k \longrightarrow -k\}$

But order of $(I(Q))$ = order(V)=4 implies

$I(G)$ is non degenerate and a 3-group

2) $D_6 \rightarrow \{C_6, S_3, S_3\}$ (Example (2.7) (2))

From remark (1) of theorem 2.6 Z of D_6 is $\{a^3, e\}$ and

$$I(D_6) = \frac{D_6}{Z} = S_3$$

$I(D_6)$ is degenerate (proved in remark 1 of theorem 2.8). As $S_3 = I(D_6)$ is not a 3-group (by the remark of theorem 2.2) we have

$I(D_6)$ is Degenerate but not a 3-group

3) $C_2 \times D_4 = \{C_4 \times C_2, D_4, D_4\}$ Example (2.6)

$I(C_2 \times D_4) = V$ and $C_2 \times D_4$ is degenerate by the remark of theorem 2.8

$\therefore I(C_2 x D_4)$ is degenerate and 3-group.

THEOREM:2.8:- A non-abelian 3-group has an abelian decomposition if and only if the group of inner automorphisms is the klein four group.

PROOF:

If $G \longrightarrow \{@,@,@\}$ then by theorem 2.5 Z of $G = K$

$\therefore I(G) = \frac{G}{Z} = \frac{G}{K} \cong V$ (by theorem 2.2)

conversely if $I(G) = V$ then $\frac{G}{Z} = V$. But G being a 3-group $\frac{G}{K} = V \therefore \frac{G}{Z} \cong \frac{G}{K}$ implies $Z \cong K$

$\therefore$ By the converse of theorem 2.5

$G \rightarrow \{@,@,@\}$

Finally we consider the relation between the 3-group structure and degeneracy of $I(G)$. This is given by the following theorem

THEOREM:2.9: The group of inner automorphism of a 3-group is degenerate if and only if the centre contains elements other than elements from K

PROOF:

Assume Z contains elements other than K then they are from $\tilde{A}$ or $\tilde{B}$ or $\tilde{C}$.

If $A \cap Z \neq \emptyset$ let $\tilde{a}_z \in \tilde{A} \cap Z$ then

for every $\tilde{b} \in B = \tilde{C}\tilde{A} = \tilde{C}(\tilde{a}_z k)$, there exists $\tilde{c}_1 \in \tilde{C}$

and $k \in K$ such that

$\tilde{b} = \tilde{c}_1, \tilde{a}_z k = (\tilde{c}_1 k)\tilde{a}_z = \tilde{c}\tilde{a}_z \quad (\because \tilde{c}, k \in \tilde{C}$ and $a_z \in Z)$

Let $i(g)$ be the inner automorphism of G defined by g then we have

$$i(\tilde{b}) = i(\tilde{c}),$$

Since $i(\tilde{b})(g) = \tilde{b} g \tilde{b}^{-1} = \tilde{c}(\tilde{a}_z g \tilde{a}_z^{-1}) \tilde{c}^{-1}$

$= \tilde{c}\, g\, \tilde{c}^{-1} \qquad (\because \tilde{a} \in z)$

$= i(\tilde{c})\ (g)$

$\therefore\ \tilde{I}\ (\tilde{B}) = \tilde{I}(\tilde{c})$ which implies

$\tilde{I}\ (B) = \tilde{I}\ (c)$, and $[\because B = \tilde{B} \cup K,\ C = \tilde{C} \cup K]$

$\therefore\ \tilde{I}\ (G) = \tilde{I}\ (A)\ \cup \tilde{I}(B) \cup \tilde{I}(c)$

implies $I(G) = \tilde{I}\ (A)$ (or) $\tilde{I}(B)$

Conversely:- Assuming I (G) is degenerate we prove that Z contains elements other than k

Let $I\ (G) = \tilde{I}(c)$

then $\tilde{I}\ (B) \subseteq \tilde{I}\ (c)$

This implies either $i(b) \in \tilde{I}(c)$ (or) $\tilde{I}\ (K)$

i.e. $i(\tilde{b}) = i(k)$ (or) $i(\tilde{c})$

If $i(\tilde{b}) = i(k)$ then

$\tilde{b} g \tilde{b}^{-1} = k g k^{-1}$ for every $g \in G$

i.e. $k^{-1}\tilde{b} g = g k^{-1} \tilde{b}$ for every $g \in G$

i.e $k^{-1}\tilde{b}$ commutes with every elements of G

$k^{-1}\tilde{b} \in z$ (or) $\tilde{b} = kz$

$\therefore\ z = k^{-1}\tilde{b} \in k\tilde{B} = \tilde{B}$

$\therefore\ Z \cap \tilde{B} \neq \phi$

Similarly $i\ (\tilde{b}) = i(\tilde{c})$ implies

$\tilde{b} = \tilde{c}z$ with $\tilde{c} \in \tilde{C}$, $z \in Z$.

$z = \tilde{c}^{-1}\tilde{b} \in \tilde{C}\tilde{B} = \tilde{A}$

$\tilde{A} \cap Z \neq \phi$

In a similar manner we prove the results for other cases also .

<u>REMARK:1</u>

Using this theorem one can check the degeneracy of D_6

with respect to the decomposition $\{C_6, S_3, S_3\}$.

K of $D_6 = \{a^2, a^4, e\}$ (Example 2.7-2)

Z of $D_6 = \{a^3, e\}$

i.e. The centre of D_6 contains elements from $\tilde{A}$. Therefore $I(D_6)$ is degenerate by the above theorem.

Remark: 2.

From example 2.6 we have $\tilde{A}$ of $C_2 X D_4$ contain (d, a^2) which is in the centre of $C_2 X D_4 = \{C_4 X C_2, D_4, D_4\}$

$I(C_2 X D_4)$ is degenerate with respect to the decomposition $\{C_4 X C_2, D_4, D_4\}$.

CHAPTER III

GROUPS AS UNIONS OF PROPER SUBGROUPS:

A group G is said to be monogenic if it is generated by a single element. In the following theorem we obtain a characterization for groups which are the unions of their proper subgroups.

RESULT: 3.1

Any group G is expressible as a union of proper subgroups if and only if it is not monogenic.

PROOF:

If G is not monogenic then it can be expressed as the union of its monogenic subgroups which by hypothesis are all proper. conversely if $G = \bigcup_{i \in I} G_i$ and G is monogenic then $G = \langle a \rangle$ implies

$a \in G_i$ for some i and that $G_i \neq G$.

Next we shall see there are non monogenic groups which cannot be expressible as a <u>finite</u> union of their proper subgroups.

EXAMPLE: 3.1:

Let Q^+ be the additive group of rational numbers If $Q^+ = H_1 U H_2 U \; . \; . \; . \; . \; U H_n$ where each H_i is a proper subgroup of Q^+, then we get a controdiction. Since there are only finite number of H's, it can be assumed that this union is irredundant i.e. none of the H's is contained in the union of all the others.

Hence any one of these H's, for example H_1 contains a rational number $r = m/n$ which is in no other H_i. This implies for all integers h,

$\frac{r}{h}$ is in no H_i except in H_1.

(For otherwise $h \cdot \frac{r}{h} = r \in Hi$ for that i)

but $\frac{r}{h} \in Q^+ = \bigcup_{i=1}^{n} Hi \Longrightarrow r/h \in H_1$

Taking h = some multiple of m say = dm

we have $r/h = \frac{m}{n} \cdot \frac{1}{dm} = \frac{1}{nd} \in H_1$

This implies any multiple of $\frac{1}{nd}$ and hence

$cn \times \frac{1}{nd} = c/d \in H_1$ where c, d are arbitrary integers

i.e We have $Q^+ \subseteq H_1$ of $H_1 = Q^+$

Remark: This proof incidentally shows that Q^+ can never be an irredundant union of even infinitely many of its proper subgroups.

Now we shall see the following theorem.

Theorem:3.2

If G is the irredundant union of the subgroups H_i, then for each i, H_i contains the intersection of all the remaining H's.

PROOF:

$$\text{Let } G = \bigcup_{j \in J} H_j = H_i \cup H \text{ where } H = \bigcup_{\substack{j \neq i \\ j \in H}} H_j$$

since the union is irredundant, H_i cannot be contained in the union H of the remaining H's. i.e There exists

$x \in H_i$ such that x is not in the remaining H's. Now to prove that $H_i \supseteq$ the intersection of all the remaining H's.

Let y be an element contained in all the other $H_i'^s$ and so in the intersection.

If $xy \in H$ then $xy \in H_j$ for some j

$\therefore$ $x = xyy^{-1} \in H_j$ (as $y \in H_j$ for every j)

which is a controdiction.

$\therefore xy \notin H$ i.e. $xy \in H_i$

$y = (x^{-1})\ (xy) \in H_i$

This completes the proof of the result. Next we shall see the condition which restricts the minimum number of proper subgroups into which a group can be decomposed. Before deriving the condition we prove the following result.

RESULT: 3.2

Let G be the irredundant union of subgroups A_i ($i = 1, 2 \ldots n > 2$) and set $M = A_2 \cup A_3 \cup \ldots \cup A_n$. Then if x is not in M, we have x^k is M for some $k = 1, 2 \ldots n-1$

Proof:

$x \notin M$ implies $x \in A_1$

choose $y \in A_2$ such that y is not in A_1.

If $x^j y \in A_2$ for some $j = 1$ to $n-1$, then $x^j = (x^j y)\ y^{-1} \in A_2 \subseteq (M)$ as desired.

If $x^j y \notin A_2$ then we claim that either $A_3 \cup A_4 \cup \ldots \cup A_n$ has $n-1$ distinct elements

$xy, x^2y, \ldots x^{n-1}y$ (or) $x^{j-m} \in M$ for $j > m$

$x^jy \notin A_2$ for $j=1$ to $n-1$, together with $y \notin A_1$ and

$x \in A_1$, implies that $xy, x^2y, \ldots x^{n-1}y \in A_3 \cup A_4 \cup \ldots \cup A_n$

If they are not distinct let $x^jy = x^my$ for some j, $m = 1$ to $n-1$ and $j > m$ then $x^{j-m} = e \in M$ as desired.

If they are distinct we find that $xy, x^2y, \ldots x^{n-1}y$ are $n-1$ in number belonging to $A_3 \cup A_4 \cup A_5 \ldots \cup A_n$.

But this union contains $n-2$ members.

Therefore distinct x^jy, x^my must belong to the same A_q where $q=3$ to n with $j > m = 1, 2, \ldots n-1$.

Therefore $x^{j-m} = (x^jy)(x^my)^{-1} \in A_q \subseteq M$.

THEOREM: 3.1

Suppose that K^{th} roots can be taken in the group G for every positive integer $k < n$, then G is not the irredundant union of n (or fewer) of its proper subgroups.

PROOF:

If G is the irredundant union of exactly n subgroups then $G = \bigcup_{i=1}^{n} A_i$ such that there exist $x \in A_1$ but $x \notin M = A_2 \cup A_3 \ldots \cup A_n$

Clearly no root y of x belong to M.

(For if $y = k^{th}$ root of $x \in M$ then $y^k = x \in M$)

Let y = The $(n-1)!^{th}$ root of x which exists in G by hypothesis. This $y \notin M$, by the result 3.2, $y^{k'} \in M$ for some $K' < n$.

Therefore $x = \left(y^{k'}\right)^{\frac{(n-1)!}{k'}}$ $\left(\frac{(n-1)!}{k'}\right.$ is an integer) i.e. $x = y^{(n-1)!} \in M$

This controdicts the fact that $x \notin M$.

$\therefore$ G cannot be the irredundant union of n of its proper subgroups.

If $m<n$ is any integer, then from the hypothesis of the theorem G contains k^{th} roots for $k<m$ also and hence G cannot be the irredundant union of m of its proper subgroups.

REMARK:

If G is a finite group of order N, the hypothesis of theorem 3 is equivalent to the requirement that $(n-1)!$ is prime to N(4). This gives us the following result immediately.

COROLLARY:

Let G be a finite group of order N, p the smallest prime dividing N. Then G is not the union of p or fewer of its proper subgroups. Since p is the smallest prime number that divides N, no factor of 1, 2 . . . . p-1 can divide N

$\therefore (p-1)!$ is prime to N

$\therefore$ By the above remark, G satisfies the hypothesis of the theorem (3.1) for p.

i.e k^{th} roots of elements belong to G for every $k<p$

$\therefore$ G is not the union of p or fewer of its proper subgroups.

REMARK:

The criterian of theorem (3.1) cannot be strengthened. Let G be the abelian group generated by x and y with relations $x^p = y^p = e$. Then G is the union of (p+1) proper subgroups generated by $x, y, xy, x^2y, \ldots x^{p-1}y$ respectively.

$G = \langle x, y\rangle$ such that $x^p = y^p = e$, implies that p is the smallest prime number that divides $\sigma(G) = N$.

for $x^p = e \implies \sigma(x) = p$ divides N .

If q is a prime number $< p$ and divides N. then there exists an element $g \in G$ such that $\sigma(g) = q$ (by cauchy's theorem for finite abelian groups)

but $g = x^m y^n$ for some integers m and n implies

$g^p = x^{mp} y^{np} = e$ (G is abelian)

This implies q divides p which is a controdiction, i.e. p is the smallest prime number that divides $\sigma(G)$. Thus G satisfies the hypothesis of theorem 3.3

But $G = \langle x\rangle \cup \langle y\rangle \cup \langle xy\rangle \cup \langle x^2y\rangle \cup \ldots$

$\ldots \cup \langle x^{p-1}y\rangle$ shows that it can be expressed as the union of p+1 proper subgroups.

A partial converse of the theorem 3.1 is the following theorem.

<u>THEOREM: 3.2</u>

Let G be a finite group of order N, p is the smallest prime number dividing N. Suppose that G is the union of exactly p+1 proper subgroups S_i, then atleast one of the S's say s_j has index p. If moreover this s_j is normal, then all the Si have index p and p^2 divides N.

<u>PROOF</u>:

Let $G = \bigcup_{i=1}^{p+1} S_i$

Index of $S_i = \frac{\sigma(G)}{\sigma(si)}$ divides $N=\sigma(G)$

Hence $\frac{\sigma(G)}{\sigma(si)}$ cannot be less than p, since p is the smallest integet that divides N

i.e. Index $S_i \geqslant p \quad \forall i$

If none of the S_i's has index equal to p, then they must all have indexes greater than p. (or) Index of $S_i \geqslant (p+1)$ for every i

$\frac{\sigma(G)}{\sigma(S_i)} \geqslant p+1$ implies $\sigma(Si) \leq \frac{N}{p+1}$ for every i

$G = \bigcup_{i=1}^{p+1} S_i$ implies

$N < \sum_{i=1}^{p+1} \sigma(Si) \leq (p+1)\frac{N}{P+1} = N$

(i.e) $N < N$ a controdiction

$\therefore$ S_j has the index p for some j

Now we assume that this S_j is normal in G.

The for $i \neq j$, $s_i sj$ is a subgroup of G.

This subgroup $S_i\ S_j$ cannot be a proper subgroup of G, for in that case

$S_i \cup S_j \subseteq S_i S_j$ implies

$$G = \bigcup_{\substack{k=1 \\ k\neq i,j}}^{p+1} \left(S_k (\cup s_i \cup s_j)\right) \subseteq \bigcup_{\substack{k=1 \\ k\neq i,j}}^{p+1} S_k \cup (S_i s_j)$$

This implies G is the union of S_iS_j and (p-1) of its proper subgroups which controdicts the corollary.

Therefore $S_iS_j = G$ for $i \neq j$

i.e. $\sigma(G) = \sigma(S_iS_j)$

But S_j is normal

Therefore $\sigma(G) = \sigma(S_iS_j) = \dfrac{\sigma(S_i)\,\sigma(S_j)}{\sigma(S_iS_j)}$ for $i \neq j$

(or) $\dfrac{\sigma(G)}{\sigma(S_j)} \times \sigma(S_iS_j) = \sigma(S_i)$ for $i \neq j$

$$p.\,\sigma(S_i \cap S_j) = \sigma(S_i)$$

Let $\sigma(S_i) = \dfrac{N}{q_i}$ for $i \neq j$

then $q_i \geq p$ (since all the indexes are $\geq p$)

Suppose $q_i > p$ for some $i \neq j$ then

$$N = \sigma(G) \leq \sigma(S_j) + \sum_{\substack{i \neq j \\ i=1}}^{p+1} \sigma(S_i) - \sigma(S_i \cap S_j)$$

$$\leq \frac{N}{p} + \sum_{i \neq j} \left(\frac{N}{q_i} - \frac{N}{pq_i}\right)$$

$$< \frac{N}{p} + p\left(\frac{N}{p} - \frac{N}{p_i}\right) = N$$

which is a controdiction. Therefore $q_i = p$ for every $i \neq j$

and $\sigma(S_iS_j) = \dfrac{\sigma(S_i)}{p} = \dfrac{N}{p.p}$

$$= \frac{N}{p^2}$$ shows that p^2 divides N.

BIBLIOGRAPHY

1. HERSTEIN . I.N. : Topics in Algebra, 2nd Edition, Vikas publishing house Pvt. Ltd., Utterpradesh, 1987, (37-44).

2. BRUCKHEIMER.M. (The open university England) BRYAN.A.C. and MUIR.A. (The city university London, England) : 'Groups which are the union of three subgroups' American Mathematical Monthly 1970, (52-57)

3. SEYMOUR HABER, (Polytechnic institute of Brooklyn) AZRIEL ROSENLAND, (Ford Instrument Company and Yeshiva University) ' Groups as unions of proper subgroups' American Mathematical monthly, 1959, (491-494).

4. -.- - -.-. American Mathematical monthly, Vol.60, 1953, (185-186)

5. VASISHTHA.A.R. Modern Algebra.