٩٥٥٦ / ٢

GROUPS OF ORDER
MORE THAN 120

A THESIS

Submitted in Partial fulfilment of the
Requirements for the Award of the M. sc.Degree

BY.

RAGAB ABD EL.KADER OMAR

Submitted to

Ain Shams University
Faculty of Science
Department of Mathematics

1986.

Under Supervision

Prof. Dr. MUNIR SAYED MORSY
Faculty of Science
Ain Shams University

Prof.Dr EL.SAYED MOHAMED EL.GHAZZY
Faculty of Education
Ain Shams University

Dr. ALI AHMED ALI ASSAR
Faculty of Education
Ain Shams University

M. Sc. COURSES

STUDIED BY THE AUTHOR (1982-1983)

AT

AIN SHAMS UNIVERSITY

FACULTY OF SCIENCE

1. Abstract Algebra.
2. Algebriac Topology.
3. Differential Geometry.
4. Functional Analysis.
5. Linear Algebra.

بسم الله الرحمن الرحيم

CONTENTS

PREFACE

One of the most important subjects in abstract algebra is the concept of groups. Every finite group is well defined by a set of generators and some relations connecting them. A group may have several sets of generators, but it is completely defined by any set of generators. This means that, different representations may give isomorphic groups. It is very difficult to show that two representations are isomorphic.

Many authors tried to find all possible groups of a certain order. In [4], the author gave all possible groups of order 1 to 15, together with some studies of their structure. In [2], the auther gave all possible groups of order 1 to 32, with their relations, generators, their lattice diagrams, and another studies to each type alone. In the end of his book he listed the groups of order up to 100 in a table, giving only the number of types of each order, classfying them to abelian or non-abelian without giving any information about their structure or their description. Finally in [5], the groups of all possible order between 100 and 119 were given with their relations, generators, some lattice diagrams, and another some properties.

On the same way, the main purpose of this thesis is finding all possible groups of orders 120 up to 127, with their description and their subgroups. Sometimes we give the lattice diagrams.

This thesis consists of three chapters:

In chapter one we give some definitions, and some important theorems without proof which help us in our subject.

In chapter two we list groups of order up to 119 in a table, together with the generators to some of these groups.

Chapter three forms the principal part of this work. In it we start to compute groups of order 120 up to 127. The cheif idea in this case is finding a normal subgroup using Sylow third theorem. Checking possibility, we get the generators of our group and give the description of it.

Finally, after each group of a certain order, we give a table showing the number of types of this group.

In order to refer to specific groups we have introduced symbolic number for each group, which we call the type of he group. This has the form m/n, where m is the order of the roup and n denotes a particular group of that order.

CHAPTER I

CHAPTER I

GENERAL BASICS

This chapter is devoted for some definitions, theorems, and related results which are needed in our thesis.

§(1.1) Generators of Groups:-

If a set of elements contained in a finite group G has the property that all the elements of G may be obtained by forming products whose factors all occur in the given set, then this set of elements is said to constitute a set of generating elements of G or a set of generators of G.

§(1.2) The order of a group and of an element:-

The order of the group G is the number of elements in G.

The smallest positive integer n for which $a^n=e$, where e is the identity, is called the order of the element a. If no such n exists a is said to have infinite order.

esults:

Let G be a group. Denote the greatest common divisor of n and m by (n,m). Then we have:

1. If $a \in G$, then a and its inverse have the same order
. If $|a|=n$, then $a^m=e$ iff $n \mid m$
. If $|a|=n$, $|b|=m$, $(n,m)=1$ and $ba=ab$, then $|ab|=nm$.
. If p,q are relatively prime, then the products $a^i b^j$ (where $0 \leqslant i \leqslant p$, $0 \leqslant j \leqslant q$) are all distinct for all $a,b \in G$.

§(1.3) Isomorphism:-

Let G and H be groups, let f be a function from G into H. If f satisfies the condition $f(g_1g_2)=f(g_1)\ f(g_2)$ for all g_1, $g_2 \in G$, then f is called a homomorphism from G into H. If f is one-one it is often called a monomorphism. If f is onto it is often called an epimorphism, an isomorphism is a monomorphism onto.

§(1.4) Definitions of some important groups:-

In our work we need to know the structure of some important groups such as:

(1) The cyclic group: A group G is cyclic if every element in it is a power a^i of some fixed element a. If the order of this group is finite, say n, then G is denoted by C_n and its description is

$$C_n = \langle a:\ a^n=e\rangle$$

(2) The Klein 4-group K_4: This group is defined as:

$$K_4 = \langle a,b:\ a^2=b^2=e,\ ab=ba\rangle$$

(3) The symmetric group S_n: Let S be a finite set, the set S_n of all permutations on n members of S forms a group of order n!, called the Symmetric group of degree n, the law of composition being that for maps of the members onto themselves.

(4) The Alternating group A_n: The set of all even permutations on S with the product of permutations is a group of order n!/2 and is denoted by A_n.

(5) The Dihedral group D_n: This is the group of rotational symmetries of a regular n-sided prism or the group of all symmetries of a plane regular n-sided polygon. Its order is 2n, and its description is:

$$D_n = \langle a,b:\ a^n=b^2=e,\ ba=a^{-1}b\rangle$$

(6) The Dicyclic group Q_n: This group is of order 2n, and its description is:

$$Q_n = \langle a,b:\ a^n=e,\ b^2=a^{n/2},\ ba=a^{-1}b\rangle$$

(7) The quaternion group Q: Let the 2x2 matrices

$$a = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad b = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \text{ where } i = \sqrt{-1}$$

Consider the set of 8 matrices $\{e,a,a^2,a^3,b,ab,a^2b,a^3b\}$. This set under ordinary matrix multiplication forms a group, and its description is

$$Q = \langle a,b:\ a^4=e,\ a^2=b^2,\ ba=a^{-1}b\rangle$$

(1.5) Subgroups and normal subgroups:

A nonempty subset H of a group G is said to be a subgroup f G if, under the product in G, H itself forms a group.

heorem 1: [4]

A nonempty subset H of a group G is a subgroup of G iff ,b $\in$ G implies $ab^{-1} \in H$

efinition:

A subgroup H of a group G having the property gH=Hg g $\in$ G is called a normal subgroup of G.

Theorem 2: [4]

A subgroup H of a group G is normal in G iff any one of the following equivalent statements holds:

(1) $gH = Hg$ for all $g \in G$

(2) $g^{-1}Hg = H$ for all $g \in G$

(3) $g^{-1}Hg \subset H$ for all $g \in G$

(4) $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$.

Theorem 3: [10]

There is a one-one correspondence between the set of all right cosets of H in G and the set of all left coset of H in G. The common cardinality of the two sets is called the index of H in G and is usually denoted by $[G:H]$. In the finite case $[G:H] = |G|/|H|$. The number of elements in each coset is $|H|$.

Theorem 4: [10]

Let H be a subgroup of index 2 in the group G. Then H is normal in G. In particular A_n is normal in S_n.

Definition:

Let H be any normal subgroup of a group G we may be able to construct a group whose elements are the cosets aH of H in G with multiplication:

$$aH.bH = abH \quad , \qquad \text{for all } a,b \in G.$$

This group is called the factor or quotient group of G relative to H and is denoted by G/H.

§(1.6) Lagrange's theorems:

(1) Let H be a subgroup of a finite group G, then $|H|$ devides $|G|$. In particular, if $a \in G$, then $|\langle a\rangle|$ must devide $|G|$, hence $|a| \mid |G|$, then we state this as:

(2) Let a be an element of a finite group G, then $|a|$ devides $|G|$.

Theorem 7: [4]

Let G be a finite group of order a prime p, then G is cyclic.

Definition:

Let S be a non-empty set of elements of G and let $\{H_i : i \in \Delta\}$ be the set of all subgroups H_i of G which contain S: $H_i \supseteq S$, then we have the following definition:

The subgroup $\bigcap_{i\in\Delta} H_i$ is defined to be the subgroup of G generated by S. S is called a generating set of $\bigcap_{i\in\Delta} H_i$. The members of S are called generators of $\bigcap_{i\in\Delta} H_i$. If S is a finite set, then $\bigcap_{i\in\Delta} H_i$ is said to be finitely generated. We usually denote $\bigcap_{i\in\Delta} H_i$ by $\langle S\rangle$.

Theorem 8: [14]

Every subgroup of a cyclic group $\langle g\rangle$ is cyclic. Moreover if $\langle g\rangle$ is finite of order n, then there is just one cyclic subgroup of order m. For each divisor m of n this subgroup has the form $\langle g^{n/m}\rangle$, these are all the subgroups of $G = \langle g\rangle$ in the finite case.

§(1.7) The p-subgroup and Sylow theorems:

The subgroups of order p^m, where $|G|=p^m s$, $(p,s)=1$ are called the Sylow p-subgroup of G.

(1) The first Sylow theorem: Let G be a group of order $n=p^m s$ where $(p,s)=1$, and p is a prime. Then G contains subgroups of orders p^i; $i=1,2,\ldots,m$; and each subgroup of order p^i; $i=1,2,3,\ldots,(m-1)$, is a normal subgroup of at least one subgroup of order p^{i+1}.

(2) The second Sylow theorem: In a finite group G the Sylow p-subgroups form a complete conjugate set of subgroups of G.

(3) The third Sylow theorem: Let G be a group, then the number of Sylow p-subgroups is of the form $1+kp$, where k is a non-negative integer, and $1+kp$ divides the order of G.

Results:

1) Let G be a finite group with just one Sylow p-subgroup for each prime p dividing $|G|$. Then G is the direct product of its Sylow p-subgroups.

2) Let $|G| = p^2 q$, where (p^2-1) does not divide q and $(q-1)$ does not divide p. Then G is abelian.

3) A finite abelian group is the direct product of its Sylow subgroups.

Theorem 9:

If the order of a group G is divisible by a prime p, then G contains an element of order p, and hence G has a cyclic subgroup of order p.

Theorem 10: [4]

All groups of order p^2, where p is a prime are abelian.

Theorem 11: [14]

There is one unique Sylow p-subgroup of the finite group G iff it is normal.

Theorem 12: [4]

Let G be a group of order pq, where p,q are distinct primes with $p < q$, then G has just one subgroup of order q. This subgroup of order q is normal subgroup in G. If p does not divide (q-1), then G is a cyclic group.

Theorem 13: [10]

If a group G is of order p^n, where p is a prime number, then G has a normal subgroup.

§(1.8) Conjugacy:

Let H be a subgroup of a group G, then $g^{-1}Hg$ form a ubgroup of G. $g^{-1}Hg$ is called a conjugate set to H in G, 't is isomorphic to H, and $|g^{-1}Hg| = |H|$.

)efinition:

The set $N(H) = \{g : g \in G, gH=Hg\}$ is called the normalizer f H in G.

<u>Definition</u>:

The center $Z(G)$ of a group G is defined as:

$Z(G) = \{x:\ x \in G,\ xg=gx,\ \text{for all } g \in G\}$

<u>Definition</u>:

Two subgroups H and K of a group G are called conjugate if $H=g^{-1}Kg$, for some $g \in G$.

<u>Results</u>:

Let G be a group, then we have:

(1) Conjugate subgroups are isomorphic; in particular they have the same order.

(2) If H is a subgroup of G, then H is normal in $N_G(H)$.

(3) If N is any subgroup of G such that H is normal in N, then $H \subset N \subset N_G(H)$.

(4) All elements in the conjugacy class containing g have the same order as g.

(5) H is normal in G iff H consists of the union of complete conjugacy classes.

(6) $Z(G)$ is a normal abelian subgroup of G.

(7) Let G be a finite group. Then the class equation is in the form $|G| = |Z(G)|+h_1+h_2+\ldots+h_r$, $h_i > 1$

where h_i = the number of elements in the i^{th} conjugacy class

$= [G:N_G(x_i)]$ for any element x_i in the i^{th} conjugacy class.

(8) If $|G|=p^r$ for some prime p, then $|Z(G)|=p^s > 1$. In particular $Z(G) \neq \{e\}$ for a p-group G.