GROUP PROPERTIES
AND
GROUP ISOMORPHISM

Evelyn. M. Manalo

Mathematics Honors Thesis
University of California, San Diego
May 25, 2001

Faculty Mentor: Professor John Wavrik
Department of Mathematics

Introduction

THE IMPORTANCE OF GROUP THEORY *is relevant to every branch of Mathematics where symmetry is studied. Every symmetrical object is associated with a group. It is in this association why groups arise in many different areas like in Quantum Mechanics, in Crystallography, in Biology, and even in Computer Science. There is no such easy definition of symmetry among mathematical objects without leading its way to the theory of groups.*

In this paper we present the first stages of constructing a systematic method for classifying groups of small orders. Classifying groups usually arise when trying to distinguish the number of non-isomorphic groups of order n. This paper arose from an attempt to find a formula or an algorithm for classifying groups given invariants that can be readily determined without any other known assumptions about the group. This formula is very useful if we want to know if two groups are isomorphic. Mathematical objects are considered to be essentially the same, from the point of view of their algebraic properties, when they are isomorphic. When two groups Γ and Γ' have exactly the same group-theoretic structure then we say that Γ is isomorphic to Γ' or vice versa. Formally, the map $\varphi : \Gamma \rightarrow \Gamma$' is called an *isomorphism* and Γ and Γ' are said to be *isomorphic* if

i. φ is a homomorphism (i.e., $\varphi(xy) = \varphi(x)\varphi(y)$), and
ii. φ is a bijection.

For two groups of order *n*, there are *n!* 1-1 onto mappings from Γ to Γ'. To check if φ is an isomorphism we need to check $\varphi(ab) = \varphi(a)\varphi(b)$ for all *a, b*. This implies that there are $n! * n^2$ combinations to check. However, for groups of order 32, 32! = 263130836933693530167218012160000000. This implies that even though the problem of telling whether two groups are isomorphic is solvable, checking all the possible combinations is not an efficient way to solve it. It is therefore necessary to design an algorithm that will minimize computation time in determining if two groups are isomorphic.

Groups posses various properties or features that are preserved in isomorphism. An isomorphism preserves properties like the order of the group, whether the group is abelian or non-abelian, the number of elements of each order, etc. Two groups which differ in any of these properties are not isomorphic. We are primarily interested in invariants that can be easily computed and therefore be tested first when determining whether two groups are isomorphic.

M. Hall Jr. and J. Senior [7] used invariants such as the number of elements of each order *k* (*k* small) to determine whether two groups of order 2^n ($n \leq 6$) are isomorphic. Philip Hall [8], in his article *The classification of prime-power*

groups , developed a systematic classification theory for groups of prime-power order. He agreed that the most important number associated with the group after the *order*, is the *class* of the group. In the book *Abstract Algebra 2nd Edition* (page 167), the authors [9] discussed how to find all the abelian groups of order *n* using the Fundamental Theorem of Finite Abelian Groups. However, mentioned that the amount of information necessary to determine to which isomorphism types of groups of order *n* a particular group belongs to may need considerable amount of information.

The intention of this project is to discover enough properties of groups (atleast of order 1-32) that will tell us whether two groups are isomorphic. In particular we want those properties that can be easily computed and which can be used to distinguish groups. So far we have accomplished this purpose for abelian groups. We will show in this paper that for abelian groups of any order, as large as possible, we can determine to what isomorphism type it belong to. We will show in this paper how the structure of an abelian group can be determined from the number of elements of various orders. This result however does not hold in general: the number of elements of each order is not enough to classify groups. That is, there exists two NON-isomorphic NON-abelian groups with the same number of elements of each order. This implies that the number of elements of each order is not enough to determine the structure of non-abelian groups. Thus, for the non-abelian case we need to look at more invariants. We will therefore treat the non-abelian groups a separate case. The object of my *next* paper will be to look at non-abelian groups and find properties (besides orders of elements) that are preserved under isomorphism and hope to find easily calculated properties that can be used to distinguish these groups (at least for orders less than or equal to 32).

The *Groups32* package will be used to compute various properties of groups, such as the order of each elements of the group, the number of subgroups, etc. The Groups32 package is a complete set of groups, one for each isomorphism class, for order 1-32. Any group of order 1-32 must be isomorphic to one of the groups in Groups32. Groups32 has built in tables for the groups of orders 1-32. When a command is issued, the information generated is computed from the tables. Groups32 is extensible. We can add new commands to the system. This package is a very important tool in investigating invariants of groups that can sometimes be very laborious when computed by hand.

Preliminaries: The reader who is familiar with terms and definitions in group theory may skip this section.

Definitions:

1. **Group.** A *group* is a nonempty set Γ with a defined binary operation ($\bullet$) that satisfy the following conditions:
   - *i. Closure:* For all $a, b, \in \Gamma$ the element $a \bullet b$ is a uniquely defined element of Γ.
   - *ii. Associativity:* For all $a, b, c \in \Gamma$, we have $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.
   - *iii. Identity:* There exists an identity element $1 \in \Gamma$ such that $1 \bullet a = a$ and $a \bullet 1 = a$ for all $a \in \Gamma$.
   - *iv. Inverses:* For each $a \in \Gamma$ there exist an inverse element a^{-1} such that $a \bullet a^{-1} = 1$ and $a^{-1} \bullet a = 1$.
2. **Homomorphism.** Let $(\Gamma, \bullet)$ and $(\Gamma', *)$ be groups. A map $\varphi : \Gamma \to \Gamma'$ such that $\varphi(x \bullet y) = \varphi(x) * \varphi(y)$, for all x,y $\in \Gamma$ is called a *homomorphism.*
3. **Isomorphism.** The map $\varphi : \Gamma \to \Gamma'$ is called an *isomorphism* and Γ and Γ' are said to be *isomorphic* if
   - 3.1 φ is a homomorphism.
   - 3.2 φ is a bijection.
4. **Order.** *(of the group).* The number of distinct elements in a group Γ is called the *order* of the group.
5. **Order.** *(of an element).* If Γ is a group and $a \in \Gamma$, the *order* of a is the least positive integer m such that $a^m = 1$. If no such integer m exists we say that x is of infinite order.
6. **Direct Products.** The *direct product* $\Gamma_1 \times \Gamma_2 \times \ldots \times \Gamma_n$ of the groups $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in \Gamma_I$, with operation defined componentwise:
   $$(g_1, g_2, \ldots, g_n) \bullet (h_1, h_2, \ldots, h_n) = (g_1 \circ h_1, g_2 \circ h_2, \ldots, g_n \circ h_n),$$
   where $\circ$ is the binary operation in Γ_i. In particular, if $\Gamma \cong \Gamma_1 \times \Gamma_2$, then $\Gamma_1 \cap \Gamma_2 = \{1\}$ and $\Gamma_1 \Gamma_2 = \Gamma$.

7. **Cyclic.** A group Γ is cyclic if Γ can be generated by a single element, i.e., there is some element $x \in \Gamma$ such that $\Gamma = \{x^n \mid n \in \wedge\}$ (here the operation is multiplication). In additive notation $\Gamma = \{nx \mid n \in \wedge\}$.
8. **Type.** If a finite group Γ is the direct product of cyclic groups of orders $p_1^{r_1}, p_2^{r_2}, .., p_k^{r_k}$, where $p_1, \ldots, p_k$ are primes, $p_1 \le p_2 \le \ldots \le p_k$, $r_1, \ldots, r_k$ positive integers, then the ordered k-tuple $(p_1^{r_1}, p_2^{r_2}, .., p_k^{r_k})$ is called the *type* of Γ.

Notations:

1. $\Gamma \cong \Gamma'$ denotes Γ is isomorphic to Γ'
2. $|\Gamma|$ denotes the order of the group Γ.

3. | **a** | denotes the order of the element *a.*
4. **1** denotes the identity element of Γ, **1'** denotes the identity element of Γ'.
5. SOLS(k, Γ) = gives the number of elements $\in$ Γ that satisfy the equation $x^k = 1$.
6. Ords(k, Γ) = number of elements of order $k \in \Gamma$.

Groups may be presented to us in several different ways. A group can be described by its multiplication table, by its generators and relations, by a Cayley graph, as a group of transformations (usually of a geometric object), as a subgroup of a permutation group, or as a subgroup of a matrix group to name a few. This project started when I was asked by my mentor to look at tables for groups of orders 1-16 published on the internet by Kenneth Almquist and find out the duplicates. The group tables seem to be generated by a computer algorithm which fails to check some tables that look different but are isomorphic. Here is an example of three group tables in the Almquist file. Two of these represent the same group (up to isomorphism) and one of them is different.

_A_B_C_D_E_F_G_H_I_J_K_L_
A|A B C D E F G H I J K L
B|B C D E F A L G H I J K
C|C D E F A B K L G H I J
D|D E F A B C J K L G H I
E|E F A B C D I J K L G H
F|F A B C D E H I J K L G
G|G H I J K L A B C D E F
H|H I J K L G F A B C D E
I|I J K L G H E F A B C D
J|J K L G H I D E F A B C
K|K L G H I J C D E F A B
L|L G H I J K B C D E F A

_A_B_C_D_E_F_G_H_I_J_K_L_
A|A B C D E F G H I J K L
B|B C A G H I J K L D E F
C|C A B J K L D E F G H I
D|D E F A B C L J K H I G
E|E F D L J K H I G A B C
F|F D E H I G A B C L J K
G|G H I B C A F D E K L J
H|H I G F D E K L J B C A
I|I G H K L J B C A F D E
J|J K L C A B I G H E F D
K|K L J I G H E F D C A B
L|L J K E F D C A B I G H

_A_B_C_D_E_F_G_H_I_J_K_L_
A|A B C D E F G H I J K L
B|B C A L J E K G D F H I
C|C A B I F J H K L E G D
D|D E G J K I L F H A B C
E|E G D C A K B L J I F H
F|F H I B C G A D E L J K
G|G D E H I A F B C K L J
H|H I F K L C J A B G D E
I|I F H E G L D J K C A B
J|J K L A B H C I F D E G
K|K L J G D B E C A H I F
L|L J K F H D I E G B C A

As mentioned above this is not the only one way of describing groups. The isomorphism problem becomes even more complicated if we need to tell whether two groups presented in other ways are isomorphic: Is the group given by generators *x,y,z* with *xy = z, yz = x, zx = y* isomorphic to the group with generators *x,y* so that *xxxx = yyyy = 1, xx = yy, yxy = x?* Is the group generated by permutations *(1 2), (1 2 3)* isomorphic to the group with generators *x,y* so that *xxx = yy = xyxy = 1?* The task of determining if two groups are the same (up to isomorphism) is not trivial.

Suppose we are asked: Is S_3 isomorphic to C_4? The answer is no. C_4 is of order 4 and S_3 is of order 6. Here we are using the theorem

Theorem 1: *If two groups are isomorphic, they must have the same order.*

Proof: By definition, two groups are isomorphic if there exist a 1-1 onto mapping φ from one group to the other. In order for us to have 1-1 onto mapping we need that the number of elements in one group equal to the number of the elements of the other group. Thus, the two groups must have the same order.

Below is a sample run of Groups32 program which shows the orders of the elements for the group S_3 (group #8) and C_4 (group #4). The Groups32 package can be accessed at *http://www.math.ucsd.edu/~jwavrik*. The `ORDERS` command tells us the number of elements of each orders of the group. We note that the particular group number of S_3 and C_4 in Groups32 was determined ahead of time by using the `PERMGRPS` command.

```
Groups32
copyright 1990-2001 John J Wavrik        Dept of Math - UCSD
Ver 6.3.2a  - January 11, 2001
  CENTER       CENTRALIZER  CHART        CONJ-CLS
  COSETS       EVALUATE     EXAMPLES     GENERATE
  GROUP        HELP         INFO         ISOMORPHISM
  LEFT         NORMALIZER   ORDERS       PERMGRPS
  POWERS       QUIT         RESULT       RIGHT
  SEARCH       STOP         SUBGROUPS    TABLE
  X
G1>> ORDERS   for Group Number 8
Group number 8 of Order 6
    1 elements of order  1:   A
    3 elements of order  2:   D E F
    2 elements of order  3:   B C
    0 elements of order  6:

G8>> ORDERS   for Group Number 4
Group number 4 of Order 4
    1 elements of order  1:   A
    1 elements of order  2:   C
    2 elements of order  4:   B D
```

Note: The underlined part implies input from the user.

Below is a list of common names for groups and their number in Groups32 which I was able to determine for some of the groups using the PERMGRPS command.

Table 1

#in G32	ORDER	Common Name	Notes:
1	1	Identity	
2	2	C_2	
3	3	C_3	
4	4	C_4	
5	4	$C_2 \times C_2$	Klein Four Group
6	5	C_5	
7	6	C_6	$\cong C_3 \times C_2$
8	6	S_3	
9	7	C_7	
10	8	C_8	
11	8	$C_4 \times C_2$	
12	8	$C_2 \times C_2 \times C_2$	
13	8	D_4	
14	8	QUATERNION	Hamiltonian (All subgroups are normal but non-abelian)
15	9	C_9	
16	9	$C_3 \times C_3$	
17	10	C_{10}	
18	10	D_5	$C_2 \times C_5$
19	11	C_{11}	
20	12	C_{12}	
21	12	$C_2 \times C_6$	$C_2 \times C_2 \times C_3$
22	12	D_6	$\cong D_3 \times C_2$
23	12	A_4	
24	12	$C_3 \propto C_4$	$\propto$ - semidirect product
25	13	C_{13}	
26	14	C_{14}	
27	14	D_7	
28	15	C_{15}	$C_3 \times C_5$
29	16	C_{16}	
30	16	$C_2 \times C_8$	
31	16	$C_4 \times C_4$	
32	16	$C_4 \times C_2 \times C_2$	
33	16	$C_2 \times C_2 \times C_2 \times C_2$	
96	32	$C_8 \times C_4$	Elements with O(8) = 16, O(4) = 12, O(2) = 3
129	32	$C_8 \times C_2 \times C_2$	Elements with O(8) = 16, O(4) = 8, O(2) = 7

The common names are not installed in Groups32. Below is a sample session showing how to determine which group in Groups32 is isomorphic to $C_4 \times C_2 \times C_2$:

```
G1>> PERMGRPS

  CREATE       ELEMENTS     HELP         INFO
  INSTALL      MAIN         MULTIPLY     QUIT
  X

PERM>> CREATE
Subgroup of Sn -- what is n?  Number 8
     Put in generators as product of cycles.
     End with a blank line
Generator (1 2 3 4)
Generator (5 6)
Generator (7 8)
Generator
Group is of order 16
A  ()             B  (7 8 )                  C  (5 6 )
D  (5 6 )(7 8 )   E  (1 2 3 4 )              F  (1 2 3 4 )(7 8 )
G  (1 2 3 4 )(5 6 )H  (1 2 3 4 )(5 6 )(7 8 )  I (1 3 )(2 4 )
J  (1 3 )(2 4 )(7 8 )                        K  (1 3 )(2 4 )(5 6 )
L  (1 3 )( 2 4 )(5 6 )(7 8 )
M  (1 4 3 2 )     N  (1 4 3 2 )(7 8 )        O  (1 4 3 2 )(5 6 )
P  (1 4 3 2 )(5 6 )(7 8 )

PERM>> INSTALL
    Install as table k (1..5)  Number 1
PERM>> MAIN
```

In the above session we created a subgroup of S_n, where n = 8, generated by a given set of permutations (given as product of cycles). We can install this say as group #1. Installing a group as group #1 then replaces the table for group 1 with the new group. We then type the `MAIN` command so that we can apply all the operations to the newly generated group. Using Table 1 above, let us check if the group #32 is isomorphic to $C_4 \times C_2 \times C_2$.

For simplicity we let A = the new group #1, and B = group #32. Notice that group #1 is now a group of order 16 (it used to be the trivial group of order 1). Notice also that both A and B are abelian (no asterisk *) as expected. Under isomorphism the abelian property is preserved.

Theorem 2: *Let $\varphi : \Gamma \to \Gamma'$ be an isomorphism. If Γ is abelian, then so is Γ'.*

Proof: Assume that Γ is abelian. Let $a_2, b_2 \in \Gamma'$. Since φ is an onto mapping there exists $a_1, b_1 \in \Gamma$ with $\varphi(a_1) = a_2$ and $\varphi(b_1) = b_2$. Then

$$a_2 b_2 = \varphi(a_1)\, \varphi(b_1) = \varphi(a_1 b_1) = \varphi(b_1 a_1) = \varphi(b_1)\, \varphi(a_1) = b_2 a_2.$$

Thus Γ' is abelian.

The first thing we need to check in determining whether two groups are isomorphic is the order of the groups. We have proven a theorem that stated

this earlier. Both A and B are of order 16. We can use the `ISOMORPHISM` command to check that A ≅ B.

```
G1>> CHART   Order of Groups (1-32 or 0) Number 16
       1   29   30   31   32   33   34*  35*  36*  37*  38*
 39*  40*  41*  42*
        There are 15 Groups of order 16
        6 abelian and 9 non-abelian

G1>> ORDERS   for Group Number 1

Group number 1 of Order 16
    1 elements of order  1:   A
    7 elements of order  2:   B C D I J K L
    8 elements of order  4:   E F G H M N O P
    0 elements of order  8:
    0 elements of order 16:

G1>> ORDERS   for Group Number 32

Group number 32 of Order 16
    1 elements of order  1:   A
    7 elements of order  2:   C E G I K M O
    8 elements of order  4:   B D F H J L N P
    0 elements of order  8:
    0 elements of order 16:

G32>> ISOMORPHISM   from Group Number 1 to Group Number 32
```

When we use the `ISOMORPHISM` command, a separate window pops up.

```
Send: B             To: B

Inconsistent because:
      Your map sends
A --> C
A --> C
A * A is A in Group 1
The mapping sends A --> C
You must redo the last assignment! -- press any key
```

Let's try again:

```
A B C D E F G H I J K L M N O P
A C E G B D F H I K M O

Send: G             To: F
Inconsistent because:
      Your map sends to be mapped
E --> B
E --> B
E * E is I in Group 1
The mapping sends I --> I
You must redo the last assignment! -- press any key
```

It is not easy to match the elements of the groups and find an isomorphism between them. For groups of order 16, we need to check $16^2 * 16!$ possible combinations. What we have shown above is that mapping the element B of Γ to the element B of Γ' will not produce an isomorphism φ because in this mapping the identity element of A will get sent to a non-identity element of B. We will prove later that this is always the case: If $\varphi : \Gamma \to \Gamma'$ is an isomorphism then $\varphi(1) = 1'$, where 1 is the identity element of Γ and 1' is the identity element of Γ'. It is clear that we need to know more about the structure of the group to find an efficient way of finding isomorphism between them.

We can use more of the Groups32 commands to minimize the number of combinations to check. We can use the SUBGROUPS command to look at the generators of the two groups. Here we are going to use the theorem

Theorem 3: *Let $\varphi : \Gamma \to \Gamma'$ be an isomorphism.. The generators of Γ are sent to generators of Γ'.*

Proof: Let $S = \{s_1, s_2, \ldots, s_m\}$ be a generating set for Γ. Let $g' \in \Gamma'$. Since φ is an isomorphism which implies that is φ onto, there exists $g \in \Gamma$ such that $\varphi(g) = g'$. By definition of a generating set, every element in Γ can be written as a product of generators, $g = x_1 x_2 \ldots x_k$, where $x_i \in S$ or $x_i^{-1} \in S$. (for finite groups we only need to consider $x_i \in S$). Thus,

$$\varphi(g) = \varphi(x_1 x_2 \ldots x_k) = \varphi(x_1)\varphi(x_2)\ldots\varphi(x_k) = g'.$$

This implies that any $g' \in \Gamma'$ can be written as a product $g' = y_1 y_2 \ldots y_j$, where y_i or $y_i^{-1} \in T = \{\varphi(s_1), \varphi(s_2), \ldots \varphi(s_m)\}$. (for finite groups we only need to consider $y_i \in T$). By definition, this makes T a generating set for Γ'. Therefore, $\varphi(s_1), \varphi(s_2), \ldots \varphi(s_m)$ are generators in Γ'.

Let us take a look at the subgroups of A and B. Below we start by using the SUBGROUPS command. Here we will see sets of generators for A and B. These sets however are not unique. Groups32 computes the set of generators by first checking if one element generates the whole group. If any one single element does not generate the whole group, Groups 32 then starts to look at a pair of elements and then three elements, etc. The first pair, triplet,…,etc it finds is what is being given as an output.

```
G32>> SUBGROUPS   of Group Number 1
 ... wait

 * = Normal subgroup
 Generators          Subgroup
 0 { }          *{ A }
 1 { B }        *{ A B }
 2 { C }        *{ A C }
 3 { D }        *{ A D }
 4 { I }        *{ A I }
 5 { J }        *{ A J }
 6 { K }        *{ A K }
 7 { L }        *{ A L }
 8 { B C }      *{ A B C D }
 9 { B I }      *{ A B I J }
10 { C I }      *{ A C I K }
11 { D J }      *{ A D J K }
12 { D I }      *{ A D I L }
13 { C J }      *{ A C J L }
14 { B K }      *{ A B K L }
15 { E }        *{ A E I M }
16 { F }        *{ A F I N }
17 { G }        *{ A G I O }
18 { H }        *{ A H I P }
19 { B C I }    *{ A B C D I J K L }
20 { B E }      *{ A B E F I J M N }
21 { C E }      *{ A C E G I K M O }
22 { D F }      *{ A D F G I L N O }
23 { D E }      *{ A D E H I L M P }
24 { C F }      *{ A C F H I K N P }
25 { B G }      *{ A B G H I J O P }
26 { B C E }    *{ A B C D E F G H I J K L M
                   N O P }
```

```
G1>> SUBGROUPS   of Group Number 32
 ... wait

 * = Normal subgroup
 Generators          Subgroup
 0 { }          *{ A }
 1 { C }        *{ A C }
 2 { E }        *{ A E }
 3 { G }        *{ A G }
 4 { I }        *{ A I }
 5 { K }        *{ A K }
 6 { M }        *{ A M }
 7 { O }        *{ A O }
 8 { B }        *{ A B C D }
 9 { C E }      *{ A C E G }
10 { F }        *{ A C F H }
11 { C I }      *{ A C I K }
12 { J }        *{ A C J L }
13 { E I }      *{ A E I M }
14 { G K }      *{ A G K M }
15 { G I }      *{ A G I O }
16 { E K }      *{ A E K O }
17 { C M }      *{ A C M O }
18 { N }        *{ A C N P }
19 { B E }      *{ A B C D E F G H }
20 { B I }      *{ A B C D I J K L }
21 { C E I }    *{ A C E G I K M O }
22 { F M }      *{ A C F H J L M O }
23 { F I }      *{ A C F H I K N P }
24 { E J }      *{ A C E G J L N P }
25 { B M }      *{ A B C D M N O P }
26 { B E I }    *{ A B C D E F G H I J K L M
                   N O P }
```

Now we issue the isomorphism command, this time we want to make sure that generators of A get sent to generators of B. Here we have found an isomorphism from A to B.

```
G32>> ISOMORPHISM   from Group Number 1 to Group Number 32

G32>> RESULT

        A B C D E F G H I J K L M N O P
        A E I M B F J N C G K O D H L P
```

This means we send $\mathsf{A} \in A$ to $\mathsf{A} \in B$ (A is the identity element in Groups32), $\mathsf{B} \in A$ to $\mathsf{E} \in B$, $\mathsf{C} \to \mathsf{I}$, $\mathsf{E} \to \mathsf{B}$, etc.

But we note that generators and relations of the groups may not always be presented to us. We may be presented only by the number of elements of each order and nothing else. Given only the number of elements of each orders can we identify the structure of the group?

Note: On the first isomorphism popup window, we tried sending $B \rightarrow B$. Notice that $B \in A$ is of order 2 and $B \in B$ is of order 4, and this mapping did not give us an isomorphism. We will discuss below why this is the case. To illustrate why this is not a valid mapping that will produce an isomorphism we will look at the following problem.

Supposed we are asked: Is C_4 isomorphic to C_2 x C_2. In this case, C_4 is of order 4, C_2 x C_2, is of order 4, but here the answer is no: C_4 is NOT isomorphic to C_2 x C_2. We are using the theorem

Theorem 4: *If two groups are isomorphic then the number of elements of each order are the same for both.*

Before we prove this theorem we will first look at some important results:

Lemma 4.1: *If φ is a homomorphism of Γ into Γ', then:*

1) $\varphi(1) = 1'$ *(where $1'$ is the unit element of Γ')*
2) $\varphi(x^{-1}) = \varphi(x)^{-1}$ *for all $x \in \Gamma$.*

Proof (1): $\varphi(x)1' = \varphi(x) = \varphi(x1) = \varphi(x)\varphi(1)$. By cancellation property, $\varphi(1) = 1'$.
Proof(2): $1' = \varphi(1) = \varphi(x\, x^{-1}) = \varphi(x)\varphi(x^{-1})$. This implies that $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Theorem 5: *If $\varphi : \Gamma \rightarrow \Gamma'$ is an isomorphism then an element of order $k \in \Gamma$ must get sent to an element of order $k \in \Gamma'$.*

Proof: Suppose $a \in \Gamma$ has order m (where m is the least positive integer such that $a^m = 1$). Then $\varphi(a)^m = \varphi(a^m)$ since φ an isomorphism implies $\varphi(a \bullet a \bullet \ldots \bullet a) = \varphi(a) * \varphi(a) \ldots * \varphi(a)$, where ($\bullet$) is the binary operation in Γ and ($*$) the binary operation in G'. But $\varphi(a^m) = \varphi(1) = 1$ by lemma 4.1 above. Thus,

$$\varphi(a)^m = \varphi(a^m) = \varphi(1) = 1.$$

If $\varphi(a)^k = 1$ for some $0 < k < m$, then $\varphi(a^k) = \varphi(a)^k = 1$. But this implies that $a^k = 1$ since φ is one-to-one, a contradiction. Hence, if φ is an isomorphism from Γ to Γ' and $a \in \Gamma$, then order of $\varphi(a)$ is equal to order of a.

Now, we are ready to prove the following theorem:

Theorem 4 *(Restated)****:*** *If two groups are isomorphic then the number of elements of each order are the same for both.*

Proof: Use the result above and the fact that isomorphism is a bijective mapping.

Using Groups32 we see that the number of elements of various orders are not the same for both groups. Here are the number of elements of each orders of C_4 and C_2 x C_2 which are groups #4 and # 5 respectively in Groups32.

```
G8>> ORDERS   for Group Number 4

Group number 4 of Order 4
    1 elements of order  1:   A
    1 elements of order  2:   C
    2 elements of order  4:   B D

G4>> ORDERS   for Group Number 5

Group number 5 of Order 4
    1 elements of order  1:   A
    3 elements of order  2:   B C D
    0 elements of order  4:
```

Here, it is clear that C_4 is NOT isomorphic to C_2 x C_2 using the fact that under isomorphism, an element of order *k* must get sent to an element of order *k*. Since isomorphism must be a 1-1 onto mapping, there is no way we can send elements of C_4 to elements of C_2 x C_2 without violating the condition of bijective mapping and the fact that the order of the elements is preserved under isomorphism. By theorem above, if two groups are isomorphic then the number of elements of each order must be the same.

Theorems 1, 2 and 4 deal with properties of groups that can be readily computed. Let us see if these theorems are enough to classify the seven abelian groups of order 32. We will assert here that looking only at the number of elements of each orders is enough to classify these groups. This assertion is deduced from a corollary to the Fundamental Theorem of Finite Abelian Groups which is stated as follows:

Corollary 6: *Any finite abelian group is the direct product (sum) of cyclic groups of prime-power orders.*

Proof: A proof is given in any group theory book. In particular, I find Herstein's [3] interesting.

Now let us look at how we can classify the seven abelian groups of order 32. Here we generated the number of elements of each orders for each of the seven abelian groups of order 32. Our goal is to find to which cyclic decomposition of order 32 each of these groups is isomorphic to.

Here are the seven non-isomorphic abelian groups of order 32:

```
G37>> CHART   Order of Groups (1-32 or 0) Number 32
      94   95*  96   97*  98*  99* 100* 101* 102* 103* 104*
105* 106* 107* 108* 109  110* 111* 112* 113* 114  115* 116*
117* 118* 119* 120* 121* 122* 123* 124* 125* 126* 127* 128*
129  130* 131* 132* 133* 134* 135* 136* 137* 138  139* 140*
141* 142* 143* 144
        There are 51 Groups of order 32
```

```
        7 abelian and 44 non-abelian

G37>> ORDERS   for Group Number 94

Group number 94 of Order 32
    1 elements of order  1:   A
    1 elements of order  2:   L
    2 elements of order  4:   H M
    4 elements of order  8:   D I P S
    8 elements of order 16:   C E K O R [ \ ]
   16 elements of order 32:   B F G J N Q T U V W X Y Z ^ _ `

G94>> ORDERS   for Group Number 96

Group number 96 of Order 32
    1 elements of order  1:   A
    3 elements of order  2:   E I Q
   12 elements of order  4:   C D F J L N P W X Y [ \
   16 elements of order  8:   B G H K M O R S T U V Z ] ^ _ `
    0 elements of order 16:
    0 elements of order 32:

G96>> ORDERS   for Group Number 109

Group number 109 of Order 32
    1 elements of order  1:   A
    3 elements of order  2:   D K Q
    4 elements of order  4:   G L N [
    8 elements of order  8:   C H J O R Y Z ^
   16 elements of order 16:   B E F I M P S T U V W X \ ] _ `
    0 elements of order 32:

G109>> ORDERS   for Group Number 114

Group number 114 of Order 32
    1 elements of order  1:   A
    7 elements of order  2:   C E I M O P Y
   24 elements of order  4:   B D F G H J K L N Q R S T U V W X Z [ \
] ^ _ `
    0 elements of order  8:
    0 elements of order 16:
    0 elements of order 32:

G114>> ORDERS   for Group Number 129

Group number 129 of Order 32
1 elements of order  1:   A
    7 elements of order  2:   D G I J P Q ]
    8 elements of order  4:   C K M N W X Y [
   16 elements of order  8:   B E F H L O R S T U V Z \ ^ _ `
    0 elements of order 16:
    0 elements of order 32:

G129>> ORDERS   for Group Number 138

Group number 138 of Order 32
    1 elements of order  1:   A
   15 elements of order  2:   C D G I J L M N O P W X Y \ _
   16 elements of order  4:   B E F H K Q R S T U V Z [ ] ^ `
    0 elements of order  8:
    0 elements of order 16:
    0 elements of order 32:

    0 elements of order 16:
    0 elements of order 32:
```

```
G138>> ORDERS   for Group Number 144

Group number 144 of Order 32
    1 elements of order  1:   A
   31 elements of order  2:   B C D E F G H I J K L M N O P Q R S T U
V W X Y Z [ \ ] ^ _ `
    0 elements of order  4:
    0 elements of order  8:
    0 elements of order 16:
    0 elements of order 32:
```

The group # 94 has elements of order 32. This implies that group #94 $\cong C_{32}$. Group #109 has elements of order 16. Therefore, this must be isomorphic to C_{16} x C_2. Now, let's look at group #96 and group #129. Both have elements of order 8. We have two cyclic decompositions to choose from which consist of C_8 as the maximal cyclic subgroup, that is, C_8 x C_4 or C_8 x C_2 x C_2. The question now is how do we know which one is isomorphic to which. To solve this problem, we have the following lemma:

Lemma 7: *Let Γ have type (p^{r_1} , p^{r_2} , ..., p^{r_n}), where n is the number of factors in the direct product of Γ. Then the number of elements of order p in Γ is $p^n - 1$.*

Proof: To prove this we need to first state and prove two important theorems.

Theorem 7.1: *Let Γ be the cyclic group of order n, and let x be an element of Γ. The number of solutions to $x^k = 1$ is gcd(k, n).*

Proof: Case 1 : *k* and *n* are relatively prime. Then by Euclidean algorithm, there exist *s, t* $\in \wedge$, $s \neq 0$, $t \neq 0$ such that

$$ks + nt = 1$$
$$(x^k)^s * (x^n)^t = x^1$$
$$(x^k)^s = x^{1-nt}$$

This implies that if $x^k = 1$, then x^{1-nt} is also equal to the identity 1. In other words,

$$x^{1-nt} = (x^k)^s = 1$$

But $x^{1-nt} = 1$ if and only if $x = 1$ since $y^n = 1$for any element *y* in a group of order *n*. Hence if *k* and *n* are relatively prime, $gcd(k,n) = 1$, then we have one solution to $x^k = 1$.

Case 2: k and n have common divisors. Without loss of generality we will take the highest divisor $d \neq 1$ that divides both k and n. Then, there exist *s* and *t* in $\wedge$, $s \neq 0$, $t \neq 0$ such that

$$d = ks + nt$$
$$x^d = (x^k)^s * (x^n)^t$$
$$x^d = (x^k)^s * 1$$

If $x^k = 1$, then $x^d = 1$ is also satisfied since

$$x^d = (x^k)^s * 1$$
$$x^d = (1)^s * 1 = 1$$

By Thm 8.1 and Thm 8.2, which will be stated and proved in the next few pages we find that for every *d* that divides the order of cyclic group Γ, there is a *unique* cyclic subgroup H of order *d* which contains all the elements $x \in \Gamma$ satisfying the equation $x^d = 1$. Thus, there are exactly *d* solution to $x^d = 1$, where $d = gcd(k,n)$.

We summarize by saying that in a cyclic group of order *n* the number of solutions to $x^k = 1$ is $gcd(k,n)$.

Theorem 7.2: *Let $\Gamma \cong C_1 \times C_2 \times \ldots \times C_m$ and let x in Γ. Let SOLS(k, C_i) be the number of solutions to $x_i^k = 1$, x_i in C_i. Then the number of solutions to $x^k = 1 \in \Gamma$ is equal to $\prod_{i=1}^{m} SOLS(k, C_i)$.*

Proof: $\Gamma \cong C_1 \times C_2 \times \ldots \times C_m$ implies that for any element x in Γ, $x = (x_1, x_2, \ldots, x_m)$ is an *m*-tuple where x_i is an element of C_i. Thus,

$$x^k = (x_1, x_2, \ldots, x_m)^k = (x_1^k, x_2^k \ \ldots, x_m^k) = 1$$

if and only if each $x_i^k = 1$. Therefore, the number of solutions to $x^k = 1$ is equal to the product of the number of solutions of each $x_i^k = 1$ in C_i.

We are now ready to prove our lemma.

Lemma 7 *(Restated):* *Let Γ have type $(p^{r_1}, p^{r_2}, \ldots, p^{r_n})$, where n is the number of factors in the direct product of Γ. Then the number of elements of order p in Γ is $p^n - 1$.*

Proof: Let $\Gamma = C_1 \times C_2 \times \ldots \times C_n$, with C_i cyclic of order $\boldsymbol{p^i}$. Using theorem 7.1 and theorem 7.2 we find that

$$SOLS(p, \Gamma) = \prod_{i=1}^{m} SOLS(p, C_i) \ = \ \prod_{i=1}^{m} \gcd(p, p^{r_i}) \ = \ p^n,$$

but this includes the identity element of Γ since the identity *1* is a solution to $x^p = 1$. Hence, the number of elements of order p in Γ is $p^n - 1$.

Using this lemma, we can now find the cyclic decomposition of group #96 and group #129. As stated in the lemma, we can look at the number of elements of order p, in this case p = 2, since $32 = 2^5$. Notice that group #96 has 3 elements of order 2, in which $3 = 2^2 - 1$. This implies that group #96 is isomorphic to $C_8 \times C_4$. The maximal cyclic subgroup is of order 8 and the cyclic decomposition consists of two invariant factors which satisfy the lemma above. This result implies that group #129 $\cong C_8 \times C_2 \times C_2$. Let us check the number of elements of order 2 in group #129. There are $7 = 2^3 - 1$ elements of order 2, which again satisfy our lemma. Group #138 has highest element of order 4 and the number of elements of order 2 is $15 = 2^4 - 1$. Therefore, group #138 $\cong C_4 \times C_2 \times C_2 \times C_2$. This leads us to group #144 $\cong C_2 \times C_2 \times C_2 \times C_2 \times C_2$.

As mentioned earlier we now state more theorems that lead us to this result.

Theorem 8.1: *Let $\Gamma = C_n$ be the cyclic group of order n. Then for each d that divides n there exists a unique subgroup H(cyclic) of order d.*

Proof: First we recall that the subgroups of a cyclic group are all cyclic. If a is a generator of Γ, then $H = < a^{n/d} >$ is a subgroup of order *d*. Assume $<b>$ is a subgroup of order *d*. Now $b^d = 1$, and $b \in \Gamma$ implies $b = a^m$ for some *m*. Hence $a^{md} = 1$ implies $md = nk$ for some *k*, and $b = a^m = (a^{n/d})^k = 1$. Therefore, $<b> \subset H$. But $|<b>| = |H| = d$ which implies that in fact $<b> = H$ since there is one and only one cyclic group for every order *c*, where *c* is a positive integer.

Theorem 8.2: *Let $\Gamma = C_n$ be the cyclic group of order n. Then Γ contains exactly d elements $x \in G$ satisfying $x^d = 1$ for all positive integer d that divides $n = |\Gamma|$.*

Proof: Combine results in theorems 8.1, 8.3 and 8.4.

Theorem 8.3: *Let $\Gamma = C_n$ be the cyclic group of order n. Let $x \in \Gamma$ be a solution to $x^d = 1$, d divides $n=|\Gamma|$, then $x \in H$, where $H \subset \Gamma$ is the unique subgroup of order d.*

Proof: Let $\Gamma = <a>$ and $H = < a^{n/d} >$, then H is the unique subgroup of order d by theorem 0.1. Clearly, $x^d = 1$ implies if $|x| = s$ then $sd = kn$. Thus, $s = (n/d)\,k$. But $H = < a^{n/d} >$ which implies that $x \in H$.

Theorem 8.4: *Let $\Gamma = C_n$ be the cyclic group of order n. Let $H \subset \Gamma$, $|H| = d$. Then for all $y \in H$, $y^d = 1$.*

Proof: Since $|H| = d$ then every element $y \in H$ satisfy $y^d = 1$ by definition of *order* of a group.

Theorem 9: *If Γ is a finite abelian group and p is a prime dividing $|\Gamma|$, then Γ contains an element of order p.*

Proof: [by Dummit[9]] The proof proceeds by induction on |Γ|, namely, we assume the result is valid for every group whose order is strictly smaller than the order of Γ and then prove the result valid for Γ (this is sometimes referred to as *complete* induction). Since $|\Gamma| > 1$, there is an element $x \in \Gamma$ with $x \neq 1$. If $|\Gamma| = p$ then *x* has order *p* by Lagrange's Theorem and we are done. We may therefore assume $|\Gamma| > p$.

Suppose *p* divides |*x*| and write $|x| = pn$. Thus, $|x^n| = p$, and again we have an element of order *p*. We may therefore assume that p does not divide |*x*|.

Let $N = <x>$. Since Γ is abelian, N is normal to Γ. By Lagrange's Theorem, the order of the quotient group $\Gamma/N = |\Gamma| / |N|$ and since $N \neq 1$, $|\Gamma/N| < |\Gamma|$. Since p does not divide |N|, we must have $p \mid |\Gamma/N|$. We can now apply the induction assumption to the smaller group Γ/N to conclude it contains an element, $y' = yN$, of order *p*. Since $y \notin N$ ($y' \neq 1'$)

but $y^p \in N$ ($y'^p = 1'$), we must have $\langle y^p \rangle \neq \langle y \rangle$, that is, $|y^p| < |y|$. This implies $p \mid |y|$. We are now in the situation described in the preceding paragraph, so that argument again produces an element of order p. The induction is complete.

Theorem 10: *Given the number of elements of each order of a group Γ, we can count the number of solutions to $x^k=1$, $x \in \Gamma$, by the following formula:*

$$SOLS(k, \Gamma) = \sum_{d|k} Ords(d, \Gamma)$$

Proof: The formula above is a consequence of the following lemma.

Lemma 10.1: *Let $a \in \Gamma$, $|a| = m$. We have $a^k = 1$ if and only if $m \mid k$.*

Proof: ($\Leftarrow$) If $m \mid k$ then $a^k = 1$.

m divides k implies that there exists an integer c such that $cm = k$. Thus,

$$a^k = a^{cm} = (a^m)^c = (1)^c = 1.$$

($\Rightarrow$) If $a^k = 1$ then $m \mid k$.

Let $d = gcd(k, m)$. Then there exists s, t with

$$sk + tm = d$$
$$a^{sk + tm} = a^d$$
$$(a^k)^s (a^m)^t = a^d$$
$$(1)^s (1)^t = a^d$$
$$1 = a^d$$

But $d = gcd(k, m)$ implies that $d \leq m$. If $d < m$, then $1 = a^d$ is a contradiction to the fact that the order of a is m, since $m = |a|$ implies that m is the smallest number such that $a^m = 1$. Therefore, it must be that $d = m$. Hence $m \mid k$.

Theorem 11. *A finite abelian group can be expressed as a direct product of its Sylow subgroups.*

Proof: [by Beachy[12]] Let Γ be a finite abelian group, with $|\Gamma| = np^\alpha$, where p does not divide n. Let $H_1 = \{a \in \Gamma \mid a^{p^\alpha} = 1\}$ and let $K_1 = \{a \in \Gamma \mid a^n = 1\}$. Since Γ is abelian, both are subgroups, and H_1 is the Sylow p-subgroup of Γ.

We will show that (i) $H_1 \cap K_1 = \{1\}$ and (ii) $H_1K_1 = \Gamma$. This shows that Γ is isomorphic to the direct product of H_1 and K_1. Then we can decompose K_1 in a similar fashion, etc., to get $\Gamma \cong H_1 \times H_2 \times \ldots \times H_k$, where each subgroup H_i is a Sylow p-subgroup for some prime p.

To prove (i), we simply observe that if $a \in H_1 \cap K_1$, then the order of a is a common divisor of p^α and n, which implies that $a = 1$. To prove (ii), let $a \in \Gamma$. Then the order k of a is a divisor of $p^\alpha n$, andso $k = p^\beta m$, where $m \mid n$, $\beta \leq \alpha$, and p does not divide m. Since $\gcd(p^\beta, m) = 1$, there exist $r, s \in \wedge$ with $ms + p^\beta r = 1$. Then $a = (a^m)^s (a^{p^\alpha})^r$, and $a \in H_1K_1$ since $a^m \in H_1$ and $a^{p^\beta} \in K_1$. The last statement follows from the fact that $(a^m)^{p^\beta} = 1$ and $(a^{p^\beta})^n = 1$ since mp^α and np^β are multiples of the order of a.

Below is a recipe on how to get the cyclic decomposition of abelian groups. We will apply this to some abelian groups to see how it works.

Step 1: The first step in determining the cyclic decomposition of an abelian group of order n is the factorization of n into prime powers. We will state without proof that by the Fundamental Theorem of Arithmetic, if $n > 1 \in \wedge$, then n admits a factorization into primes. Further, this factorization is unique up to ordering. So we let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

By theorem 11, a finite abelian group can be expressed as a direct product of its Sylow p-subgroups. Therefore,

$$\Gamma \cong S_1 \, x \, S_2 \, x \, \ldots \, x \, S_k, \qquad (1)$$

where S_i is the Sylow p_i – subgroup of order $p_i^{\alpha_i}$, and where

$$S_i \cong C_{p_i^{\beta_1}} x C_{p_i^{\beta_2}} x \ldots x C_{p_i^{\beta_t}}, \qquad (2)$$

p^{β_j} are called the elementary divisors of Γ, with $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \ldots + \beta_t = \alpha_i$ (where t depend on i).

We note that each Sylow subgroup is normal to Γ since Γ is abelian and thus unique. The decomposition of Γ described in (1) and (2) is therefore unique and is called the elementary decomposition of Γ.

Step 2: We will use lemma 7 to identify the type of S_i. As mentioned earlier, S_i is a p_i – subgroup, hence has an element of order p_i by theorem 9. We count the number of elements of order p_i to determine the number of partition of α_i. Using lemma 7, if the number of elements of order p_i is equal to $p_i^{\,r} - 1$, for some positive integer r, then we partition α_i into r. We also need to identify the maximal cylic subgroup C_m so that m_1 is the highest partition of r and such that $S_i \cong C_{m1} \, x \, C_{m2} \, x \, \ldots \, x \, C_{mr}$, $\alpha = m_1 + m_2 + \ldots + m_r$. We identify m_1 by looking at the highest-order element whose order is a power of p_i. In other words, m_1 is equal to k such that we have an element of order $p_i^{\,k}$ and no elements of order $p_i^{\,t}$, for any $t > k$.

Note: In the case that α can be partitioned into r parts in more than one way having the same highest partition m_1 we resolve this by Step 2.1.

Otherwise we proceed to step 3.

Step 2.1: To resolve the problem mentioned above, we will use theorems 7.1, 7.2 and 10. Since we are given the number of elements of each order d dividing the order of the group Γ, we can calculate the number of solutions to $x^d = 1$ using theorem 10. We then compare the result to one of the cyclic decomposition we computed in step 2. By theorem 7.2, given the cyclic decomposition we can compute easily the number of elements in Γ satisfying $x^d = 1$. If we get a match then we have the correct cyclic decomposition, otherwise we proceed to the other cyclic decomposition we got from step 2. We keep doing this until we get a match.

We note that this is not very expensive to execute since we have a simple formula for calculating the solutions to $x^d = 1$ either given the cyclic decomposition or given the number of elements of each orders dividing n.

Step 3: Now that we have the elementary decomposition of Γ the next step is to obtain the invariant factors of Γ from its elementary divisors. By the Fundamental Theorem of Finite Abelian groups,

$$\Gamma \cong C_{n_1} x C_{n_2} x ... x C_{n_s},$$

for some integers $n_1, n_2, \ldots, n_s$ satisfying the following conditions:

(a) $n_j \geq 2$ for all j and
(b) $n_{j+1} \mid n_i$ for $1 \leq j \leq s-1$

The integers $n_1, n_2, \ldots, n_s$ are called the invariant factors of Γ.

We obtain the invariant factors by following these steps:

(i) For every S_i arrange its elementary divisors in non-increasing order. In this way we obtain k list of integers one for each p_i.
(ii) To obtain the j^{th} invariant factor of Γ, n_j, we take the product of the j^{th} component of each of our k list of elementary divisors. In the case that there is no j^{th} component in a list we multiply it by 1.

This procedure guarantees that we have divisibility condition satisfied. We also note that because the integers in one list is relatively prime to all the other integers in the other lists, C_{n_i} is cyclic. This is in fact always true since the direct product of cyclic groups whose orders are relatively prime is isomorphic to the cyclic group of order q, where q is the product of orders of each cyclic group in the direct product.

To illustrate how the procedure works we will take a look at some examples.

Input: 1) | A | = 256

Number of elements	Of order
1	1
15	2
112	4
128	8
0	16
0	32
0	64
0	128
0	256

Output: Cyclic decomposition of A.

Step 1: $|A| = 256 = 2^8$

Step 2: $|S_1| = 2^8$. $\alpha = 8$. The number of elements of order 2 is equal to 15 which implies that by lemma 2, $r = 4$ since $2^4 - 1 = 15$. Thus we need to partition $\alpha = 8$ into $r = 4$ parts $m_1, m_2, m_3, m_4,$ such that $m_1 + m_2 + m_3 + m_4 = 8$.

Notice that the element with highest order is of order $8 = 2^3$. This implies that $m_1 = 3$. Now we need to partition $8 - 3 = 5$ into 3 parts. We have two choices $5 = 3 + 1 + 1$ or $5 = 2 + 2 + 1$. To resolve this conflict we proceed to step 2.1.

Step 2.1 Calculate the number of solutions to $x^k = 1$, for every k dividing $|A| = 256$. Using the formula in theorem 10:

$$SOLS(k,\Gamma) = \sum_{d|k} Ord(d,\Gamma),$$

we get the following result:

k	Number of solutions to $x^k = 1$ SOLS(k,Γ)
1	1
2	1 + 15 = 16
4	1 + 15 + 112 = 128
8	1 + 15 + 112 + 128 = 256
16	1 + 15 + 112 + 128 + 0 = 256
32	1 + 15 + 112 + 128 + 0 + 0= 256
64	1 + 15 + 112 + 128 + 0 + 0 + 0 = 256
128	1 + 15 + 112 + 128 + 0 + 0 + 0 + 0 = 256
256	1 + 15 + 112 + 128 + 0 + 0 + 0 + 0 + 0 = 256

Now we calculate the number of solutions to $x^k = 1, x \in C_8 \times C_8 \times C_2 \times C_2$. This corresponds to partition of $\alpha = 8 = 3 + 3 + 1 + 1$. Using the formula in theorem 7.1 and 7.2:

$$SOLS(k, C_n) = gcd(k,n),$$
$$SOLS(k, C_1 \times C_2 \times \ldots \times C_m) = \prod_{i=1}^{m} SOLS(k, C_i)$$

we get the following result:

k	Number of solutions to $x^k = 1$ SOLS(k,Γ)
1	1
2	16
4	64
8	256
16	256
32	256
64	256
128	256
256	256

Notice that the number of solutions to $x^k = 1$ in A does not match with the number of solutions to $x^k = 1$ in $\in C_8 \times C_8 \times C_2 \times C_2$.

Clearly, this implies that we should have the other partition of $\alpha = 8 = 3 + 2 + 2 + 1$ which corresponds to the cyclic decomposition $C_8 \times C_4 \times C_4 \times C_2$. To verify that we have the correct cyclic decomposition for A we calculate the number of solutions to $x^k = 1$ in $C_8 \times C_4 \times C_4 \times C_2$ and see if it matches the number of solutions to $x^k = 1$ in A. Again using the formula in theorem 7.1 and 7.2 we get the following result:

k	Number of solutions to $x^k = 1$ SOLS(k,Γ)
1	1
2	16
4	128
8	256
16	256
32	256
64	256
128	256
256	256

Indeed, we have a match.

Step 3: Check if the decomposition satisfies condition a) and b). Since we only have one Sylow p – subgroup, our elementary divisors is exactly the invariant factors of Γ.

Output: $A \cong C_8 \times C_4 \times C_4 \times C_2$.

To summarize this result :

We started by factoring |A| = 256 into prime powers. Then we note that the number of elements of order 2 is equal to $2^4 - 1 = 15$. This implies that our cyclic decomposition for group A consist of 4 invariant factors.

Now we look at the highest order of element in A. The highest order of element in A is 8 therefore C_8 must be present in our decomposition. So far we have that $A \cong C_8 \times H$ where |H| = 32 since 8 * 32 = 256 = |A|. Now we need to find the cyclic decomposition for H. We know from the previous computation that H must consist of 3 factors. There are two choices for H having 3 factors and in which |H| = 32, that is, $C_8 \times C_2 \times C_2$ or $C_4 \times C_4 \times C_2$.

We then use theorem 7.1 and 7.1 to resolve this conflict. We proceed by matching the number of solutions to $x^k = e$ in A to the number of solutions to $x^k = 1$ in $\cong C_8 \times H$. If we take $H = C_4 \times C_4 \times C_2$, we are then testing if $A \cong C_8 \times C_4 \times C_4 \times C_2$. Now we check the number of elements of order 8. There are 4 elements of order 8 in C_8. This implies that there are 4*4*4*2 = 128 elements of order 8 in A, which is the same number given above. We do this until we find a match.

Let us look at another example.

Input: 1) $|B| = 2592$

Number of elements	Of order
1	1
7	2
26	3
24	4
182	6
0	8
54	9
624	12
0	16
378	18
0	24
0	27
0	32
1296	36
0	48
0	54
0	72
0	81
0	96
0	108
0	144
0	162
0	288
0	864
0	324
0	216
0	648
0	432
0	1296
0	2592

Output: Cyclic decomposition of B.

Step 1: $|B| = 2592 = 2^5 * 3^4$

Step 2: First we note that a group of order $2592 = 2^5 * 3^4$ has a 2- Sylow subgroup and a 3-Sylow subgroup. Let S_2 = 2-Sylow subgroup, S_3 = 3-Sylow subgroup. By the Fundamental Theorem of Finite Abelian Groups we know that $\Gamma \cong S_2 \times S_3$. $|S_2| = 32$, $|S_3| = 81$, $|\Gamma| = 2592$. We need to find the cyclic decomposition of S_2 and S_3. Here we assert that if S_2 is of type $(2^{r_1},...,2^{r_n})$ and S_3 is of type $(3^{s_1},...,3^{s_m})$ then the type of $\Gamma = S_2 \times S_3$ is $(2^{r_1},...,2^{r_n},3^{s_1},...,3^{s_m})$. This assertion is as a result of the Fundamental

Theorem of Finite Abelian Groups which states that every abelian group is a direct product of its Sylow subgroups. Every p-Sylow subgroup can be decomposed as a direct product of cyclic groups of prime power order. Thus, by the definition of type, this implies that the type of $S_2 \times S_3$ is $(2^{r_1},...,2^{r_n},3^{s_1},...,3^{s_m})$. All we need to do now is to find the cyclic decomposition of S_2 and S_3 and then augmenting the result will give the cyclic decomposition of Γ.

To find the cyclic decomposition of S_2, we only look at the elements of G of order 2^k, for some constant *k*. Notice that there are no elements of order 32, order 16 or order 8. Also note that the number of elements of order 2 is equal to $7 = 2^3 - 1$. This implies that S_2 have 3 factors in its cyclic decomposition and the factor with the highest order is C_4 since there are no elements of order 32,16 or 8. Hence, $S_2 = C_4 \times C_4 \times C_2$.

To find the cyclic decomposition of S_3, we look at the elements of G of order 3^k, for some constant *k*. Notice that there are no elements of order 81 or order 27. Also note that the number of elements of order 3 equals $26 = 3^3 - 1$. This implies that S_3 have 3 factors in its cyclic decomposition and the factor with the highest order is C_9. Hence $S_3 = C_9 \times C_3 \times C_3$. Thus we have $\Gamma \cong C_4 \times C_4 \times C_2 \times C_9 \times C_3 \times C_3$.

Step 3: To satisfy condition a) and b) above we follow steps i) and ii) to find the invariant factors of Γ. Thus, we get $\Gamma \cong C_{36} \times C_{12} \times C_6$. Notice that the element with the highest order in Γ has order 36. We can use Theorem 7.1 and 7.2 stated above to verify that this is correct.

What we have shown here is that the structure of an abelian group can be determined from the number of elements of various orders.

The converse is: Suppose two groups have certain properties the same – for example, suppose they have the same number of elements of each order – are they isomorphic? The answer is YES for ABELIAN groups but NO in general. As mentioned earlier, there exist two NON-isomorphic NON-abelian groups with the same number of elements of each order. Now we will look at the non-abelian case and see that these groups are not classified so simply.

Here is our counter-example to the converse of theorem above:

```
G35>> ORDERS   for Group Number 36

Group number 36 of Order 16
    1 elements of order  1:   A
    7 elements of order  2:   C E G I K N P
    8 elements of order  4:   B D F H J L M O
    0 elements of order  8:
    0 elements of order 16:
```

```
G36>> ORDERS   for Group Number 37

Group number 37 of Order 16
    1 elements of order  1:   A
    7 elements of order  2:   C E G I K M O
    8 elements of order  4:   B D F H J L N P
    0 elements of order  8:
    0 elements of order 16:
```

The two smallest non-isomorphic groups with this property are group #36 and group #37 of order 16 in Groups32 package. First of all, we know that these two groups are non-abelian. We can use the CHART command or the EVALUATE command and see that not all the elements of the group commute with each other. Another way to check if a group is non-abelian is by using the CENTER command. This command outputs the center of the group. If the center of the group Γ is all of Γ then Γ is abelian otherwise it is non-abelian. Here is an example using the EVALUATE and CHART command:

```
G37>> EVALUATE   (use ' for inverse) bc= D
G37>> EVALUATE   (use ' for inverse) cb= D
G37>> EVALUATE   (use ' for inverse) bi= N
G37>> EVALUATE   (use ' for inverse) ib= J

G37>> GROUP   Group Number 36
G36>> EVALUATE   (use ' for inverse) bc= D
G36>> EVALUATE   (use ' for inverse) cb= D
G36>> EVALUATE   (use ' for inverse) bp= M
G36>> EVALUATE   (use ' for inverse) pb= M
G36>> EVALUATE   (use ' for inverse) ei= O
G36>> EVALUATE   (use ' for inverse) ie= M

G36>> CHART   Order of Groups (1-32 or 0) Number 16
      29   30   31   32   33   34*  35*  36*  37*  38*  39*  40*
      41*  42*
        There are 14 Groups of order 16
        5 abelian and 9 non-abelian
```

Note: In Groups32 (*) means NON-ABELIAN

Below is an example using the CENTER command. Notice that in each case, the center of groups #36 and #37 is not the whole group since we know from the earlier result the groups #36 and #37 are of order 16.

```
 CENTER       CENTRALIZER  CHART        CONJ-CLS
  COSETS       EVALUATE     EXAMPLES     GENERATE
  GROUP        HELP         INFO         ISOMORPHISM
  LEFT         NORMALIZER   ORDERS       PERMGRPS
  POWERS       QUIT         RESULT       RIGHT
  SEARCH       STOP         SUBGROUPS    TABLE
  X

G1>> CENTER   of Group Number 36
{ A B C D }
G36>> CENTER   of Group Number 37
{ A C E G }
```

What we have shown here is that the number of elements of each order is not enough to determine the structure of NON-abelian groups. Thus, for non-abelian groups, we need to look at more invariants beside the number of elements of each order. Here, we find that particular invariants of a group which can be readily calculated have different significance in classifying groups. For the abelian our answer is YES we can classify them by looking at the number of elements of each orders, for the non-abelian groups our answer is NO.

To identify invariants that will distinguish non-abelian groups (at least for groups of orders 1–32) from one another will be the goal of my next paper.

BIBLIOGRAPHY

[0] Tzusuku, T. 1982. *Finite Groups and Finite Geometries.* Cambridge University Press.

[1] Thomas, A. and Wood, G. 1980. *Group Tables.* Shiva Publishing Limited.

[2] Rotman, J. 1984. *An Introduction to the Theory of Groups.* Allyn and Bacon, Inc., Newton Massachusetts.

[3] Johnson, D. 1976. *Presentation of Groups.* Cambridge University Press.

[4] Hoffman, C. 1982. *Group-Theoretic Algorithms and Graph Isomorphism.* Springer-Verlag Berlin Heidelberg Press.

[5] Herstein, I. 1964. *Topics in Algebra.* Xerox College Publishing.

[6] Hall, P. 1964. *Theory of Groups.* The Macmillan Company.

[7] Hall, M. and Senior, J. 1964. *The groups of order 2^n*. Macmillan Company.

[8] *(Compiled by)* Gruenberg, K. and Roseblade, J. 1988. *Collected Works of Philip Hall.* Oxford University Press.

[9] Dummit, D. and Foote, R. 1999. *Abstract Algebra 2^{nd} Edition.* John Wiley and Sons, Inc.

[10] Coxeter, H. and Moser, W. 1965. *Generators and Relations for Discrete Groups. 2^{nd} edition.* Springer-Verlag Berlin Heidelberg Press.

[11] Burnside, W. 1897. *The Theory of Groups.* Cambridge University Press.

[12] Beachy, J. and Blair W. 1990. *Abstract Algebra with a Concrete Introduction.* Prentice Hall New Jersey.