

On the Lattice Structure of Cyclic Groups of Order the Product of Distinct Primes

Rosemary Jasson Nzobo^{1,*}, Benard Kivunge², Waweru Kamaku³

¹Pan African University Institute for Basic Sciences, Technology and Innovation, Nairobi, Kenya

²Department of Mathematics, Kenyatta University, Nairobi, Kenya

³Pure and Applied Mathematics Department, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Abstract In this paper, we give general formulas for counting the number of levels, subgroups at each level and number of ascending chains of subgroup lattice of cyclic groups of order the product of distinct primes. We also give an example to illustrate the concepts introduced in this work.

Keywords Lattice, Cyclic Group, Subgroups, Chains

1. Introduction

A subgroup lattice is a diagram that includes all the subgroups of the group and then connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments if and only if H is a proper subgroup of K [1]. The study of subgroup lattice structures is traced back from the first half of 20th century. For instance in 1953, Suzuki presented the extent to which a group is determined by its subgroup lattice in [2].

In [2], Suzuki argued that isomorphic groups have the same lattice structure. Also, in [3], Birkhoff and Mac Lane showed that up to isomorphism, there is only one cyclic group of order n . Hence for each n , there is exactly one subgroup lattice structure representing any cyclic group of order n .

Jez in [1] deduced that the subgroup lattice structure of a cyclic group of prime power order (that is, when $n = p^k$ where p is prime and k is a natural number) is a single chain. In [1], it was also shown that if G is a finite group and the subgroup lattice of G is a single chain, then G is cyclic. That is, a finite group has a single chain subgroup lattice if and only if it is isomorphic to \mathbb{Z}_n .

In [4], P'alfy showed that the subgroup lattice of a cyclic group C_{nm} where n and m are distinct primes has two ascending chains and three levels. Furthermore, P'alfy argued that any group whose subgroup lattice is formed by two chains is isomorphic to \mathbb{Z}_{nm} . That is, a finite group has a subgroup lattice with two ascending chains if and only if

it is isomorphic to \mathbb{Z}_{nm} for primes $n \neq m$.

In this paper, we present general formulas for finding the number of levels, subgroups at each level and number of ascending chains of cyclic groups of order $p_1 p_2 p_3 \dots p_m$ where p_i are distinct primes.

2. Preliminaries

Definition 2.1 ([6]) Let L be a non empty set and $<$ be a binary relation.

1. A partially ordered set, poset $(L, <)$ is called a lattice if for every a, b in L , both $\sup\{a, b\}$ and $\inf\{a, b\}$ belong to L .
2. The lattice whose elements are the subgroups of the group G with the partial order relation being set inclusion is called the subgroup lattice of the group G and is denoted by $L(G)$.

Definition 2.2 ([6]) Let G be a group. A sequence $H_1 \subseteq H_2 \subseteq H_3 \subseteq \dots \subseteq G$ of subgroups of G is called an ascending chain.

Theorem 2.3 ([3]) Up to Isomorphism, there is exactly one cyclic group of order n .

Theorem 2.4 ([2]) Isomorphic groups have the same subgroup lattice diagram.

Theorem 2.5 ([5]) If $G = \langle g \rangle$ is a cyclic group of order n , then each subgroup of G has the form $\langle g^d \rangle$ where d is a unique positive divisor of n .

Theorem 2.6 ([5]) In a finite cyclic group, each subgroup has order dividing the order of the group. Conversely, given a positive divisor of the order of the group, there is a subgroup of that order.

Theorem 2.7 ([5]) If $G = \langle g \rangle$ is a cyclic group of order n and $H = \langle g^{d_1} \rangle$, $H' = \langle g^{d_2} \rangle$ are subgroups of G where d_1 and d_2 are positive divisors of n , then $H \subseteq H'$ iff $\gcd(n, d_2)$ divides $\gcd(n, d_1)$.

* Corresponding author:

nzobor@gmail.com (Rosemary Jasson Nzobo)

Published online at <http://journal.sapub.org/ajms>

Copyright © 2018 The Author(s). Published by Scientific & Academic Publishing

This work is licensed under the Creative Commons Attribution International

License (CC BY). <http://creativecommons.org/licenses/by/4.0/>

3. Main Results

Theorem 3.1 If G is a cyclic group of order $p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ where p_i are distinct primes and k_i are positive integers and let $L(G)$ be a subgroup lattice of G , then $L(G)$ has $1 + \sum_{i=1}^m k_i$.

Proof: Every subgroup of G is of the form $\langle n/p_1^{x_1} p_2^{x_2} \dots p_m^{x_m} \rangle$ where $0 \leq x_i \leq k_i$. Subgroups at r^{th} level are such that $x_1 + x_2 + \dots + x_m = r - 1$. The sum of these powers at the first, second to the last level are $0, 1, \dots, \sum_{i=1}^m k_i$ respectively which form arithmetic progression AP with the first term $A_1 = 0$, common difference $d = 1$ and the last term $A_n = \sum_{i=1}^m k_i$. The number of levels, $n(l)$ is the number of terms of this AP . It follows that, $\sum_{i=1}^m k_i = 0 + (n(l) - 1)$ which gives $n(l) = 1 + \sum_{i=1}^m k_i$.

Remarks: Levels are counted from below, that is from the trivially group $\langle 0 \rangle$ to the group G .

Corollary 3.2 If G is a cyclic group of order $p_1 p_2 \dots p_m$ where p_i are distinct primes and $L(G)$ is a subgroup lattice of G , then $L(G)$ has $m + 1$ levels.

Proof: Follows from Theorem 3.1 where $k_i = 1$ for all i .

Theorem 3.3 If G is a cyclic group of order $n = p_1 p_2 \dots p_m$ where p_i are distinct primes and $L(G)$ is a subgroup lattice of G , then the number $n(S_r)$ of subgroups at r^{th} level of $L(G)$ is given by $n(S_r) = \binom{m}{r-1}$.

Proof: For $r = 1$ the result is trivially true since the trivial group is the only subgroup at the first level and we have $n(S_1) = \binom{m}{1-1} = \binom{m}{0} = 1$.

Subgroups at the second level ($r = 2$) are of the form $\langle n/p_i \rangle$ for $i = 1, 2, \dots, m$. Since for each prime p_i there is a unique subgroup $\langle n/p_i \rangle$ of G , the total number of subgroups of this form is the number of ways of choosing (without repetition) one prime p_i from m primes. Hence there are $\binom{m}{1} = \binom{m}{2-1}$ subgroups at the second level.

Again, subgroups at the third level ($r = 3$) are of the form $\langle n/p_i p_j \rangle$ for $i, j = 1, 2, \dots, m$. Since for each product $p_i p_j$ there is a unique subgroup $\langle n/p_i p_j \rangle$ of G , the total number of subgroups of this form is the number of ways of choosing (without repetition) two primes $p_i p_j$ from m primes. Hence there are $\binom{m}{2} = \binom{m}{3-1}$ subgroups.

In a similar way, subgroups at the r^{th} level are generated by divisors of the form $n/\prod_{i=1}^{r-1} p_i$. Since there is a unique subgroup for each divisor of this form, we choose (without repetition) $r - 1$ primes p_i from m primes hence there are $\binom{m}{r-1}$ subgroups at the r^{th} .

Lemma 3.4 If G is a cyclic group of order $n = p_1 p_2 \dots p_m$ where p_i are distinct primes and $L(G)$ is a subgroup lattice of G , then for every subgroup H of G at r^{th} level, there are $m - r + 1$ chains towards $(r + 1)^{th}$ level.

Proof: At the first level ($r = 1$), there is only trivial group which is the subgroup of all m subgroups of the second level. But we also have $m - 1 + 1 = m$ hence the result is true for $r = 1$.

For $r > 1$, subgroups at the r^{th} level are of the form $n/\prod_{i=1}^{r-1} p_i$. Since G is cyclic, given two subgroups of G , $n/\prod_{i=1}^{r-1} p_i$ and $n/\prod_{i=1}^r p_i$, we have $n/\prod_{i=1}^{r-1} p_i \subseteq n/\prod_{i=1}^r p_i$ iff $\prod_{i=1}^r p_i = p_j \prod_{i=1}^{r-1} p_i$ for $j = 1, 2, \dots, m$. Since $\prod_{i=1}^r p_i$, and there are $r - 1$ distinct primes in the product $\prod_{i=1}^{r-1} p_i$, we remain with $m - (r - 1) = m - r + 1$ choices of p_j . Hence there are $m - r + 1$ subgroups of G at $(r + 1)^{th}$ level such that $n/\prod_{i=1}^{r-1} p_i \subseteq n/\prod_{i=1}^r p_i$.

Theorem 3.5: If G is a cyclic group of order $p_1 p_2 \dots p_m$ where p_i are distinct primes and $L(G)$ is a subgroup lattice of G , then the total number of chains $n(C_r)$ from r^{th} level to $(r + 1)^{th}$ level of $L(G)$ is given by $\binom{m}{r-1}(m - r + 1)$.

Proof: The number of chains from r^{th} level to $(r + 1)^{th}$ level is the product of the number of subgroups at r^{th} with the number of chains per subgroup from r^{th} level to $(r + 1)^{th}$ level. From Theorem 3.3 and Lemma 3.4, the number of chains from r^{th} level to $(r + 1)^{th}$ level of $L(G)$ is then given by $n(C_r) = \binom{m}{r-1}(m - r + 1)$.

Theorem 3.6: If G is a cyclic group of order $p_1 p_2 \dots p_m$ where p_i are distinct primes and $L(G)$ is a subgroup lattice of G , then the number of ascending chains $n(C)$ from $\langle 0 \rangle$ to G is $m!$.

Proof: From Lemma 3.4, the number of chains per subgroup from r^{th} level to $(r + 1)^{th}$ level is given by $m - r + 1$. To get the total number of ascending chains from the trivial subgroup to G is simply taking products of these numbers over all levels. It follows that, $n(C) = \prod_{r=1}^m m - r + 1 = m(m - 1)(m - 2) \dots 1 = m!$.

Example 3.7: Let G be a cyclic group of order $n = 5 \times 7 \times 13 \times 19$, here $m = 4$. The lattice of G is as shown below;

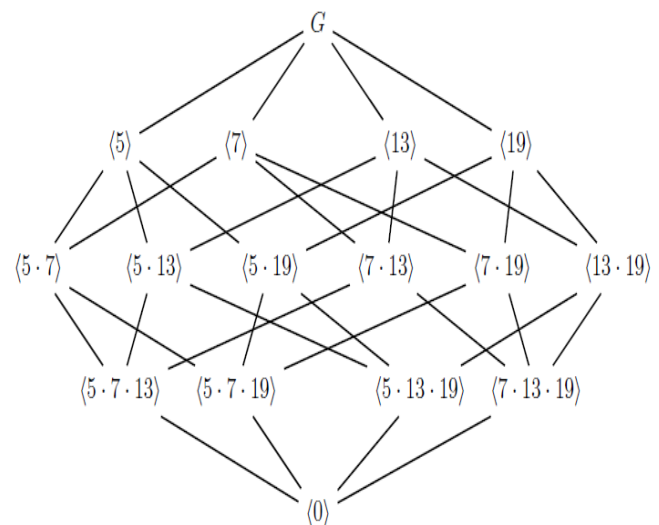


Figure 1. The lattice of a cyclic group G

From Figure 1, we see that the lattice of G has five levels which is equivalent to $m + 1 = 4 + 1$. This justifies Corollary 3.2.

To justify Theorem 3.3 for the number of subgroups at each level, we use the following table.

Table 1. Number of Subgroups at Each Level

Level (r)	Subgroups at G	$(m!r - 1)$
1	1	$(4!0)=1$
2	4	$(4!1)=4$
3	6	$(4!2)=6$
4	4	$(4!3)=4$
5	1	$(4!4)=1$

We can also see that there are 24 ascending chains which is equivalent to $m! = 4!$ as stated in Theorem 3.6. These chains are:

1. $\langle 0 \rangle \subset \langle 5.7.13 \rangle \subset \langle 5.7 \rangle \subset \langle 5 \rangle \subset G$
2. $\langle 0 \rangle \subset \langle 5.7.13 \rangle \subset \langle 5.7 \rangle \subset \langle 7 \rangle \subset G$
3. $\langle 0 \rangle \subset \langle 5.7.13 \rangle \subset \langle 5.13 \rangle \subset \langle 5 \rangle \subset G$
4. $\langle 0 \rangle \subset \langle 5.7.13 \rangle \subset \langle 5.13 \rangle \subset \langle 13 \rangle \subset G$
5. $\langle 0 \rangle \subset \langle 5.7.13 \rangle \subset \langle 7.13 \rangle \subset \langle 7 \rangle \subset G$
6. $\langle 0 \rangle \subset \langle 5.7.13 \rangle \subset \langle 7.13 \rangle \subset \langle 13 \rangle \subset G$
7. $\langle 0 \rangle \subset \langle 5.7.19 \rangle \subset \langle 5.7 \rangle \subset \langle 5 \rangle \subset G$
8. $\langle 0 \rangle \subset \langle 5.7.19 \rangle \subset \langle 5.7 \rangle \subset \langle 7 \rangle \subset G$
9. $\langle 0 \rangle \subset \langle 5.7.19 \rangle \subset \langle 5.19 \rangle \subset \langle 5 \rangle \subset G$
10. $\langle 0 \rangle \subset \langle 5.7.19 \rangle \subset \langle 5.19 \rangle \subset \langle 19 \rangle \subset G$
11. $\langle 0 \rangle \subset \langle 5.7.19 \rangle \subset \langle 7.19 \rangle \subset \langle 7 \rangle \subset G$
12. $\langle 0 \rangle \subset \langle 5.7.19 \rangle \subset \langle 7.19 \rangle \subset \langle 19 \rangle \subset G$
13. $\langle 0 \rangle \subset \langle 5.13.19 \rangle \subset \langle 5.13 \rangle \subset \langle 5 \rangle \subset G$
14. $\langle 0 \rangle \subset \langle 5.13.19 \rangle \subset \langle 5.13 \rangle \subset \langle 13 \rangle \subset G$
15. $\langle 0 \rangle \subset \langle 5.13.19 \rangle \subset \langle 5.19 \rangle \subset \langle 5 \rangle \subset G$
16. $\langle 0 \rangle \subset \langle 5.13.19 \rangle \subset \langle 5.19 \rangle \subset \langle 19 \rangle \subset G$
17. $\langle 0 \rangle \subset \langle 5.13.19 \rangle \subset \langle 13.19 \rangle \subset \langle 13 \rangle \subset G$
18. $\langle 0 \rangle \subset \langle 5.13.19 \rangle \subset \langle 13.19 \rangle \subset \langle 19 \rangle \subset G$
19. $\langle 0 \rangle \subset \langle 7.13.19 \rangle \subset \langle 7.13 \rangle \subset \langle 7 \rangle \subset G$
20. $\langle 0 \rangle \subset \langle 7.13.19 \rangle \subset \langle 7.13 \rangle \subset \langle 13 \rangle \subset G$
21. $\langle 0 \rangle \subset \langle 7.13.19 \rangle \subset \langle 7.19 \rangle \subset \langle 7 \rangle \subset G$
22. $\langle 0 \rangle \subset \langle 7.13.19 \rangle \subset \langle 7.19 \rangle \subset \langle 19 \rangle \subset G$
23. $\langle 0 \rangle \subset \langle 7.13.19 \rangle \subset \langle 13.19 \rangle \subset \langle 13 \rangle \subset G$
24. $\langle 0 \rangle \subset \langle 7.13.19 \rangle \subset \langle 13.19 \rangle \subset \langle 19 \rangle \subset G$

4. Conclusions

General formulas for number of levels, the number of subgroups at each level and the number of ascending chains are presented. It was proved that the number of subgroups at the r^{th} level of a lattice structure $L(G)$ of a cyclic group of order the product of m distinct primes is given by m combination $r - 1$. Furthermore, it was proved that the number of ascending chains of $L(G)$ is given by $m!$

In future work, we will study the lattice structure of cyclic groups of order the product of m prime powers. We will deduce general formulas for finding the number of subgroups at each level and number of ascending chain.

REFERENCES

- [1] A. Jez, Subgroup Lattices That Are Chains, Rose-Hulman Undergraduate Mathematics Journal, vol. 70.2 p. 4, 2006.
- [2] M. Suzuki, On the lattice of subgroups of finite groups, Transactions of the American Mathematical Society, vol. 70.2, pp 345 – 371, 1951.
- [3] G. Birkhoff and S.M. Lane, A survey of modern algebra, Universities Press, 1958.
- [4] P.P. P'alfy, Groups and lattices, Groups St Andrews 2001 in Oxford, vol. 305 pp. 429 – 454.
- [5] K. Conrad, Subgroups of cyclic groups. www.math.uconn.edu/~kconrad/blurbs/grouptheory/cyclicgp.pdf.
- [6] R. Singh, Cyclic groups, Researchgate, 2016.