CHARACTERIZING THE NUMBER OF SUBGROUPS
OF PRIME INDEX

A Thesis
Presented to the
Faculty of
California State Polytechnic University, Pomona

In Partial Fulfillment
Of the Requirements for the Degree
Master of Science
In
Mathematics

By
Matthew Levi Pineda
2014
ACKNOWLEDGMENTS

To my family, for your continuous support, my classmates, for your camaraderie during stressful times, my university, for the opportunity, and all of my instructors, for everything you have taught me, I would like to thank you all.

To my thesis advisor, whom I have learned so much from and whose teaching style I will mimic for years to come, I am very lucky to have gone on this endeavor with you by my side. Your insightfulness during our research made it seem no obstacle was insurmountable. Thank you especially, Amber.

Without you all this would not be possible.
ABSTRACT

In group theory, one of the most significant properties of normal subgroups is that they allow the formation of quotient groups. More specifically, if $H \trianglelefteq G$, then $G/H$ is a group. Thus is natural to wonder how often do normal subgroups appear in a group, where say we only know the order of the group. In this paper we characterize the possible number of normal subgroups of a specific index in any group. We follow the work in *How Rare are subgroups of Index 2* by Jean Nganou, in which the number of subgroups of index 2 is characterized, and ultimately generalize the result to subgroups of index $p$. There are obstacles along the way in generalizing to index $p$, but we circumvent the obstacles by using a result from *On The Number of Subgroups of Index Two* by Crawford and Wallace, as well as some of our own. Ultimately, we obtain an expression representing the possible quantities for subgroups of index $p$. 
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Page</td>
<td>ii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>iii</td>
</tr>
<tr>
<td>Abstract</td>
<td>iv</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1 The Original Problem</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Preliminary Lemmas</td>
<td>2</td>
</tr>
<tr>
<td>2 Generalizing for Index p</td>
<td>7</td>
</tr>
<tr>
<td>3 Conclusion</td>
<td>19</td>
</tr>
<tr>
<td>3.1 Summary</td>
<td>19</td>
</tr>
<tr>
<td>3.2 Further Questions</td>
<td>20</td>
</tr>
<tr>
<td>Bibliography</td>
<td>21</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 The Original Problem

In this thesis we will be investigating How Rare are Subgroups of Index Two by Jean B. Nganou [2], which in a corollary to one of its major theorems characterizes the possible numbers of subgroups of index two for any group $G$. Our goal in this paper is to generalize these results to subgroups of index $p$, where $p$ is the smallest prime dividing the order of $G$. This is significant to us since we know from Abstract Algebra that if a subgroup $H$ of $G$ has order $p$ where $p$ is the smallest prime dividing the order of $G$, then $H$ must be normal in $G$.

In searching for the number of subgroups of index $p$ it is not as simple as replacing 2 with $p$ in the original paper. There are various places where propositions no longer hold and we must circumvent the propositions that were formerly relied upon. To help with this we will incorporate results from On the Number of Subgroups of Index Two-An Application of Goursat’s Theorem for Groups [1].

We will begin by following a route similar to that of Nganou’s paper. We will then halt at a point where the work can no longer be generalized, i.e. we come
across a key counterexample for the important proposition. We then will reference Crawford’s text, and use a piece that will allow us to move forward, in our goal of a generalized work of Nganou, which ultimately gives a quantity for the amounts of normal subgroups of index $p$ which can appear in any group.

### 1.2 Preliminary Lemmas

Before we begin investigating Nganou’s results, we need some background lemmas in group theory. We will ultimately be concerned with the set of all $p$th powers of elements in a group. Our first lemma shows that in abelian groups, this is always a subgroup.

**Proposition 1.** If $G$ is an abelian group, then for a fixed $n \in \mathbb{N}$ the set $X^n_G = \{g^n : g \in G\}$ is a subgroup of $G$.

**Proof.** Since $G$ is group, it has an identity element $e$. So $e = e^n \in X^n_G$. Thus $X^n_G$ is nonempty. Let $a, b \in X^n_G$. Then $a = x^n$ and $b = y^n$ for some $x, y \in G$. So $ab = x^n y^n = x^n y^n = x^n y^n = (xy)^n \in X^n_G$. Also $a^{-1} = (x^n)^{-1} = x^{-n} = (x^{-1})^n \in X^n_G$. Thus $X^n_G$ is a subgroup of $G$. 

Note that if $G$ is not abelian $X^n_G = \{g^n : g \in G\}$ need not be a subgroup of $G$. Consider the Alternating Group of degree 4,

$A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243)(12)(34), (13)(24), (14)(23)\}$.

In this case,

$$X^n_{A_4} = \{(1), (132), (123), (134), (143), (234), (243)\},$$

which is not a subgroup of $A_4$ since by Lagrange’s Theorem the order of a subgroup must divide the order of the group. Here $|X^n_{A_4}| = 7$, which does not divide $|A_4| = 12$. 

2
Since $X_G^p$ is not always a subgroup of $G$, we will consider the set $G^p = \langle X_G^p \rangle$, the subgroup of $G$ generated by $X_G^p$. Recall that if $A$ is a subset of $G$, $\langle A \rangle$ is the intersection of all subgroups of $G$ containing $A$. Elements of $\langle A \rangle$ look like $a_1^{k_1}a_2^{k_2} \cdots a_s^{k_s}$ where each $a_i \in A$, $s \in \mathbb{N} \cup \{0\}$, and $k_i = \pm 1$.

Our next lemma shows when the subgroup $\langle A \rangle$ is a normal subgroup.

**Proposition 2.** Let $G$ be a group and $A \subseteq G$. If $A$ is closed under conjugation, then $\langle A \rangle$ is normal in $G$.

**Proof.** Suppose $A$ is closed under conjugation. Then $gag^{-1} \in A$ for all $g \in G$ and all $a \in A$. Let $a_1^{k_1}a_2^{k_2} \cdots a_s^{k_s} \in \langle A \rangle$ where each $a_i \in A$, $s \in \mathbb{N} \cup \{0\}$, and $k_i = \pm 1$. We aim to show $ga_1^{k_1}a_2^{k_2} \cdots a_s^{k_s}g^{-1} \in \langle A \rangle$. Now $ga_1^{k_1}a_2^{k_2} \cdots a_s^{k_s}g^{-1} = (ga_1^{k_1}g^{-1})(ga_2^{k_2}g^{-1}) \cdots (ga_s^{k_s}g^{-1})$. We now need to show $ga_i^{k_i}g^{-1}$ is in $A$ or is the inverse of something in $A$ for $1 \leq i \leq s$ if $k_i = 1$ or $k_i = -1$.

Case 1: Suppose $k_i = 1$. Then $ga_i^{k_i}g^{-1} = ga_i g^{-1} \in A$, since $A$ is closed under conjugation.

Case 2: Suppose $k_i = -1$. Then $ga_i^{-1}g^{-1} = (ga_i^{-1})^{-1} = \alpha^{-1}$ for some $\alpha \in A$. Thus in each case, $ga_i^{k_i}g^{-1}$ is in $A$ or is the inverse of an element in $A$. Hence $ga_1^{k_1}a_2^{k_2} \cdots a_s^{k_s}g^{-1} = (ga_1^{k_1}g^{-1})(ga_2^{k_2}g^{-1}) \cdots (ga_s^{k_s}g^{-1}) \in \langle A \rangle$ which shows that $\langle A \rangle$ is normal in $G$.

We are now in a position to show that the subgroup $G^p$ is always normal in $G$.

**Corollary 3.** For any group $G$, $G^p$ is a normal subgroup of $G$.

**Proof.** Let $x, g \in G$. Then $xp \in X_G^p$. Now $gx^pg^{-1} = \underbrace{gxg^{-1}gxg^{-1} \cdots gxg^{-1}}_{p\text{-times}} = (gxg^{-1})^p \in X_G^p$. Hence $X_G^p$ is closed under conjugation, and therefore $G^p = \langle X_G^p \rangle$ is normal in $G$ by Proposition 2.
The next proposition shows that if every element of a group has order less than or equal to two, then the group is abelian. We will show later that this result does not hold when we replace 2 by $p$.

**Proposition 4.** Let $G$ be a group and suppose that $x^2 = e$ for all $x \in G$. Then $G$ is abelian.

*Proof.* If $x^2 = e$ for all $x$, then $x = x^{-1}$ for all $x \in G$. Let $a, b \in G$. Then $ab = (a^{-1})(b^{-1}) = (ba)^{-1} = ba$, and hence $G$ is abelian. \hfill $\square$

We now show that whenever we have a group homomorphism, the image is always a subgroup of the codomain. We will eventually use this to compute the order of a particular quotient group.

**Lemma 5.** Let $\varphi : G \to H$ be a homomorphism, then $\varphi(G)$ is a subgroup of $H$.

*Proof.* Since $G$ is a group, $e_G \in G$. Also $e_H = \varphi(e_G) \in \varphi(G)$. Thus $\varphi(G) \neq \emptyset$. Let $h_1, h_2 \in \varphi(G)$. Then there exist $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Now $h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \in \varphi(G)$.

Further, $h_1 = \varphi(g_1)$ implies $h_1^{-1} = \varphi(g_1)^{-1} = \varphi(g_1^{-1}) \in \varphi(G)$.

Therefore $\varphi(G) \leq H$ by the subgroup test. \hfill $\square$

It is well known that subgroups of index 2 are normal. If a group has a subgroup of index 2, then the group has even order, so 2 is the least prime dividing the order of the group. The next result shows that when $p$ plays a similar role to 2, subgroups of index $p$ in a group $G$ are normal. The proof is omitted here but can be found on page 120 in [3].

**Lemma 6.** Let $G$ be a group and $p$ the smallest prime dividing $|G|$. Then any subgroup of order $p$ is normal.
Now, recall that for elements $x$ and $y$ in a group $G$, the commutator of $x$ and $y$ is $[x, y] = xyx^{-1}y^{-1}$. In abelian groups, $[x, y] = e$ for all $x, y \in G$. The following Lemma will become useful later when trying to show that a specific quotient group is abelian.

**Lemma 7.** Let $G$ be a group and $H$ a normal subgroup of $G$, then $G/H$ is abelian if and only if $H$ contains all the commutators of $G$.

**Proof.** Let $aH, bH \in G/H$. Now $G/H$ is abelian if and only if $aHbH = bHaH$ if and only if $abH = baH$ if and only if $ab(\cdot)^{-1}a^{-1} \in H$ if and only if $aba^{-1}b^{-1} \in H$. □

The next theorem presented is well known, and is used in proving a major corollary near the end of this paper. The proof to it is omitted but can be found in [3].

**Theorem 8 (Cauchy).** If $G$ is a finite group and $p$ is a prime number dividing the order of $G$, then $G$ contains an element of order $p$.

The following proposition is used in proving the same corollary that requires Cauchy’s Theorem.

**Proposition 9.** Let $p$ be a prime number and $k \in \mathbb{Z}^+$. If $|G| = p^k$, then there exists a subgroup $H$ of $G$ such that $|H| = p^{k-1}$.

**Proof.** Suppose $|G| = 2$. Then clearly $\{e\} \leq G$, and $|\{e\}| = 1 = 2^{1-1}$. Thus the statement holds true for $k = 1$. Suppose any group of order $p^{k-1}$ has a subgroup of order $p^{k-2}$. Now suppose $|G| = p^k$ and we aim to prove our result by induction. Consider the center of the group $Z(G) = \{x \in G : xy = yx \text{ for all } y \in G\}$. A theorem given in [3] shows that in a $p$-group, the center is nontrivial. Thus $Z(G) \neq \{e\}$. Since $Z(G) \leq G$, $|Z(G)| = p^a$ for some $1 \leq a \leq k$. By Theorem 8, there exists an element $x \in Z(G)$ such that $|x| = p$. Now consider $\langle x \rangle$. Since $x \in Z(G)$, $gxg^{-1} = xgg^{-1} = x^a$.
for all $g \in G$. Thus $\langle x \rangle \cong G$. Now consider $G/\langle x \rangle$. So $|G/\langle x \rangle| = \frac{p^k}{p} = p^{k-1}$, and by the induction hypothesis, $G/\langle x \rangle$ has a subgroup $A/\langle x \rangle$ such that $|A/\langle x \rangle| = p^{k-2}$.

Now $p^{k-2} = |A/\langle x \rangle| = \frac{|A|}{|\langle x \rangle|} = \frac{|A|}{p}$. Thus $|A| = p^{k-1}$. Therefore $A$ is a subgroup of $G$ of order $p^{k-1}$, and we are done.

We are now in a position to begin discussing some of the major results of this thesis. Our goal is to generalize the results of [2] to subgroups of index $p$, where $p$ is prime. We will refer to [2] often and explain the differences between the results there, and our generalized results. Frequently we will find that when considering subgroups of index $p$, much more than a simple substitution of 2 with $p$ is necessary.
Chapter 2

Generalizing for Index p

In Chapter 1 we showed that $G^p$ is a normal subgroup of $G$. Now since $G^p$ is normal in $G$, we can consider the properties of the quotient group $G/G^p$. The next theorem proves an equality relating the number of subgroups of index $p$ in $G$ and the number of subgroups of index $p$ in $G/G^p$. This is how [2] ends up characterizing the possible number of subgroups of index 2. Ultimately we will show that this method does not work when considering subgroups of index $p$. The following theorem generalizes the result in [2] by replacing $G^2$ with $G^p$ and subgroups of index 2 with subgroups of index $p$. Moreover, in [2], only a sketch of the proof is provided, and the bijection is shown by providing an inverse map rather than checking injectivity and surjectivity. We have chosen instead to show that the map is injective and surjective.

**Theorem 10.** The groups $G$ and $G/G^p$ have the same number of subgroups of index $p$.

**Proof.** Let $H$ be a subgroup of index $p$ in $G$. Then $|G/H| = p$. Let $x \in G$, so $xH \in G/H$. By a consequence of Lagrange’s Theorem, $(xH)^p = H$ for all $x \in G$. But $x^pH = (xH)^p = H$, so $x^p \in H$ for all $x$. Thus $X^p_G \subseteq H$, which implies $G^p \subseteq H$. Since $G^p$ is normal in $G$, it is also normal in the subgroup $H$. We can now
consider the quotient group $H/G^p$, which by the Lattice Isomorphism Theorem, is a normal subgroup of $G/G^p$. Then applying the Third Isomorphism Theorem, 
\[ |(G/G^p)/(H/G^p)| = |G/H| = p. \]
Thus whenever $H$ is a subgroup of $G$ of index $p$, $H/G^p$ is a subgroup of $G/G^p$ of index $p$.

We will now show there is a bijection $\varphi$, between the subgroups of index $p$ of $G$ and the subgroups of index $p$ of $G/G^p$. Let $\varphi(H) = H/G^p$. We only need to show that $\varphi$ is one-to-one and onto.

Suppose $J$ and $K$ are subgroups of index $p$ in $G$, and $\varphi(J) = \varphi(K)$. We want to show $J = K$. Now $\varphi(J) = \varphi(K)$ implies $J/G^p = K/G^p$. Thus \( \{G^p, j_1G^p, j_2G^p, \ldots, j_nG^p\} = \{G^p, k_1G^p, k_2G^p, \ldots, k_nG^p\} \) where $G^p, j_1G^p, j_2G^p, \ldots, j_nG^p$ are the distinct elements of $J/G^p$ and $G^p, k_1G^p, k_2G^p, \ldots, k_nG^p$ are the distinct elements of $K/G^p$. Let $j \in J$. Then $jG^p \in J/G^p$. So $jG^p = j_kG^p = k_sG^p$ for some $1 < r, s < n$. So $j = k_sx$ for some $x \in G^p$. But $k_s \in K$ and $x \in G^p \subseteq K$. Thus $j \in K$ and so $J \subseteq K$. Similarly $K \subseteq J$. Thus $K = J$ and $\varphi$ is one-to-one.

So by the Lattice Isomorphism Theorem, subgroups of $G/G^p$ look like $J/G^p$ where $J$ is a subgroup of $G$ that contains $G^p$. Let $J/G^p$ be a subgroup of index $p$ in $G/G^p$. Then \( [(G/G^p) : (J/G^p)] = p. \) But \( [G : J] = [(G/G^p) : (J/G^p)] = p. \) So $J$ is a subgroup of index $p$ in $G$. Thus $\varphi$ is onto. Hence we have a bijection, and we can say $G$ and $G/G^p$ have the same number of subgroups of index $p$. \( \Box \)

The next step in [2] is to show that the group $G/G^2$ is abelian. Unfortunately, as we will show later with a specific counterexample, this result cannot be generalized by replacing 2 with $p$, so we present the original result here.

**Proposition 11.** The group $G/G^2$ is abelian.

**Proof.** Let $xG^2 \in G/G^2$. Then $(xG^2)^2 = (xG^2)(xG^2) = x^2G^2 = G^2$ since $x^2 \in G^2$. Thus by Proposition 4, $G/G^2$ is abelian. \( \Box \)
Since $G/G^2$ is abelian, the Fundamental Theorem of Finite Abelian Groups tells us that $G/G^2$ is isomorphic to a direct product of cyclic groups. Since every non-identity element in $G/G^2$ has order 2, we must have that $G/G^2 \cong \bigoplus_{i=1}^{n} \mathbb{Z}_2$ for some $n$.

Since we want to generalize the results to subgroups of index $p$, it is natural to wonder if $G/G^p \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p$ for all primes $p$. However, proving this in the same fashion we did for the $p = 2$ case, would require us to show (among other things) that $G/G^p$ is abelian for any $p$. It turns out that this need not be true for $p > 2$.

Consider the following. Let $p$ be an odd prime number. The Heisenberg group modulo $p$ is defined to be the set of all matrices \( \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \) such that $a, b, c \in \mathbb{Z}/p\mathbb{Z}$. Under the operation of matrix multiplication, the Heisenberg group modulo $p$, call it $H_p$, forms a group of order $p^3$.

Now $H_p$ is a non-abelian group since \( \begin{pmatrix} 100 \\ 010 \\ 001 \end{pmatrix} \begin{pmatrix} 100 \\ 011 \\ 001 \end{pmatrix} = \begin{pmatrix} 110 \\ 011 \\ 001 \end{pmatrix} \neq \begin{pmatrix} 110 \\ 011 \\ 001 \end{pmatrix} = \begin{pmatrix} 100 \\ 011 \\ 001 \end{pmatrix} \begin{pmatrix} 110 \\ 011 \\ 001 \end{pmatrix} \). 

Further, let $x = \begin{pmatrix} 1a \\ 01 \\ 001 \end{pmatrix} \in H_p$. Then 

\[
x^p = \begin{pmatrix} 1 \ p a \ p(b + \frac{1}{2}ac(p-1)) \\ 0 \ 1 \\ 0 \ 0 \end{pmatrix} \begin{pmatrix} 100 \\ 010 \\ 001 \end{pmatrix} = e_{H_p}.
\]

We can show this by induction on $p$.

We begin with the base case. See that 

\[
\begin{pmatrix} 1 \ 1a \ 1\left(b + \frac{1}{2}ac(1-1)\right) \\ 0 \ 1 \\ 0 \ 0 \end{pmatrix} = \begin{pmatrix} 1 \ a \ b \\ 0 \ 1 \ c \\ 0 \ 0 \ 1 \end{pmatrix}.
\]

Now suppose \( \begin{pmatrix} 1 \ a \ b \\ 0 \ 1 \ c \\ 0 \ 0 \ 1 \end{pmatrix} = \begin{pmatrix} 1 \ (k-1)a \ (k-1)(b + \frac{1}{2}ac(k-2)) \\ 0 \ 1 \\ 0 \ 0 \ 1 \end{pmatrix} \) for $k \geq 1$. \]
Then
\[
\begin{pmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{pmatrix}^k = \begin{pmatrix}
1 & (k-1)a & (k-1)(b + \frac{1}{2}ac(k-2)) \\
0 & 1 & (k-1)c \\
0 & 0 & 1
\end{pmatrix} \begin{pmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{pmatrix}
\]
\[
= \begin{pmatrix}
1 & a + (k-1)a & (b + c)(k-1)a + (k-1)(b + \frac{1}{2}ac(k-2)) \\
0 & 1 & (c + (k-1)c) \\
0 & 0 & 1
\end{pmatrix}
\]
\[
= \begin{pmatrix}
1 & ka & k(b + \frac{1}{2}ac(k-1)) \\
0 & 1 & kc \\
0 & 0 & 1
\end{pmatrix}.
\]

Thus the result holds.

Now since \( p \) is prime, every non-identity element in \( H_p \) must have order \( p \), which implies \( H_p^p = \{e\} \).

Thus for \( G = H_p \), \( G/G^p = G \) which by the counterexample, is not abelian.

Thus it is true that the group \( G/G^p \) need not be abelian. So the statement \( G/G^p \cong \bigoplus_{i=1}^n \mathbb{Z}_p \) may not always be true.

A workaround for this is to no longer consider \( G/G^p \). Instead we will show \( G \) has the same number of subgroups of index \( p \) as \( G/H \) where \( H \) is the intersection of all the normal subgroups of index \( p \) in \( G \). We will ultimately show that \( G/H \cong \bigoplus_{i=1}^n \mathbb{Z}_p \) for some \( n \). Motivation for considering the group \( H \) came from Lemma 1 in [1].

We first need to show that \( H \) is actually a normal subgroup so that we can consider the quotient group.

**Proposition 12.** Let \( H_1, H_2, \ldots, H_k \) be normal subgroups of \( G \), then \( H_1 \cap \ldots \cap H_k \) is a normal subgroup of \( G \).

**Proof.** Let \( H = H_1 \cap \ldots \cap H_k \) and \( h \in H \). Let \( x \in G \). Then \( xhx^{-1} \in H_i \subset H \) for any \( 1 \leq i \leq k \). Thus \( xhx^{-1} \in H_1 \cap H_2 \cap \ldots \cap H_k = H \) and \( H \) is normal in \( G \). \[
\box{}\]

From this point on let \( p \) be the least prime that divides \( |G| \). The reason we do this is that any subgroup of index 2 is automatically normal, but a subgroup of index \( p \) may not be normal for \( p \neq 2 \). However, by Lemma 6, if \( p \) is the least prime
that divides \(|G|\), then any subgroup of index \(p\) will be normal, so we will have the analog of the index 2 case.

We will now show the relationship between the number of subgroups of index \(p\) in \(G\) and the number of subgroups of index \(p\) in \(G/H\).

**Theorem 13.** Let \(G\) be a group and \(p\) be the least prime dividing \(|G|\). Let \(H_1, H_2, \ldots, H_k\) be all of the distinct subgroups of index \(p\) in \(G\) and \(H = H_1 \cap H_2 \cap \ldots \cap H_k\). Then \(G/H\) has the same number of subgroups of index \(p\) as \(G\) does.

**Proof.** Let \(H^*\) be a subgroup of index \(p\) in \(G\). Now since each \(H_i\) has index \(p\) in \(G\), \(H_i \leq G\) for each \(i\). Now clearly \(H \leq H^*\) and by Prop 12, \(H \leq G\) and therefore \(H \leq H^*\). We can now say that \(H^*/H \leq G/H\). Further \([G/H : H^*/H] = [G/H^*] = p\).

Let \(A\) be the set of subgroups of index \(p\) in \(G\) and \(B\) the set of subgroups of index \(p\) in \(G/H\). Define a map \(\varphi : A \to B\) such that \(\varphi(H^*) = H^*/H\).

Suppose \(J, K\) are subgroups of index \(p\) in \(G\), and \(\varphi(J) = \varphi(K)\). We want to show \(J = K\). Now \(\varphi(J) = \varphi(K)\) implies \(J/H = K/H\). Thus \(\{H, j_1H, j_2H, \ldots, j_nH\} = \{H, k_1H, k_2H, \ldots, k_nH\}\) where \(H, j_1H, j_2H, \ldots, j_nH\) are elements of \(J/H\) and \(H, k_1H, k_2H, \ldots, k_nH\) are elements of \(K/H\). Let \(j \in J\). Then \(jH \in J/H\). So \(jH = j_rH = k_sH\) for some \(1 \leq r, s \leq n\). So \(j = k_sx\) for some \(x \in H\). But \(k_s \in K\) and \(x \in H \leq K\). Thus \(j \in K\) and so \(J \leq K\). Similarly \(K \leq J\). Thus \(\varphi\) is one-to-one.

Let \(J/H\) be a subgroup of index \(p\) in \(G/H\). Then \([G/H : (J/H)] = p\). But \([G : J] = [(G/H) : (J/H)] = p\). So \(J\) is a subgroup of index \(p\) in \(G\). Thus \(\varphi\) is onto.

Hence we have a bijection between \(A\) and \(B\), and we can say \(G\) and \(G/H\) have the same number of subgroups of index \(p\). \(\square\)

The following result is given for the case \(p = 2\) in the proof of Lemma 1 in [1], however the proof is merely sketched. We have generalized \(H\) to any prime \(p\) and filled in the details of the proof.
Proposition 14. Let $H_1, \ldots, H_k$ be the distinct normal subgroups of index $p$ in $G$, then $[G : H_1 \cap \ldots \cap H_k] = p^n$ for some $n$.

Proof. Let $\varphi : G \to G/H_1 \times G/H_2 \times \ldots \times G/H_k$ be defined by $\varphi(g) = (gH_1, gH_2, \ldots, gH_k)$. Let $x, y \in G$. Then $\varphi(x)\varphi(y) = (xH_1, xH_2, \ldots, xH_k)(yH_1, yH_2, \ldots, yH_k)$ $= (xH_1yH_1, xH_2yH_2, \ldots, xH_kyH_k) = (xyH_1, xyH_2, \ldots, xyH_k) = \varphi(xy)$, and hence $\varphi$ is a homomorphism.

Now $x \in \ker \varphi$ if and only if $\varphi(x) = (H_1, H_2, \ldots, H_k)$ if and only if $x \in H_1 \cap H_2 \cap \ldots \cap H_k$. Hence $H_1 \cap H_2 \cap \ldots \cap H_k = \ker \varphi$. Thus by the First Isomorphism Theorem, $G/\ker \varphi \cong \varphi(G)$.

Let $G' = G/H_1 \times G/H_2 \times \ldots \times G/H_k$. We know that $G/\ker \varphi \cong \varphi(G)$ hence $|G/\ker \varphi| = |\varphi(G)|$. Further since $\varphi(G) \leq G'$, $|\varphi(G)|$ divides $|G'|$. Now $G' = G/H_1 \times G/H_2 \times \ldots \times G/H_k$ and each $H_i$ has index $p$ in $G$. Thus $|G'| = p^k$. Finally since $|\varphi(G)|$ divides $|G'|$, we have $|\varphi(G)| = p^n$ for some $n \leq k$, which is to say $|G/\ker \varphi| = p^n$. Hence $|G/(H_1 \cap H_2 \cap \ldots \cap H_k)| = p^n$. \hfill \Box

In addition to what we have just proved, showing that $G/H$ is abelian will be the final result necessarily to prove the generalized version of the main isomorphism found in [2]. Which brings us to the next proposition.

Proposition 15. Let $p$ be the least prime dividing $|G|$. Let $H_1, H_2, \ldots, H_k$ be all of the distinct subgroups of index $p$ in $G$ and $H = H_1 \cap H_2 \cap \ldots \cap H_k$. Then $G/H$ is abelian.

Proof. Since $|G/H_i| = p$ for all $1 \leq i \leq k$, $G/H_i$ is cyclic and thus abelian. Since each $G/H_i$ is abelian, by Lemma 7, each $H_i$ contains all of the commutators of $G$. Thus $H = H_1 \cap H_2 \cap \ldots \cap H_k$ contains all of the commutators of $G$. Thus again by Lemma 7, $G/H$ is abelian. \hfill \Box
Further, note that since each $H_i$ has index $p$ in $G$, $|G/H_i| = p$. Thus for $gH_i \in G/H_i$, $g^pH_i = (gH_i)^p = H_i$. So $g^p \in H_i$ for all $i$. Hence $g^p \in H$, and so for $gH \in G/H$, $(gH)^p = g^pH = H$, which is to say every element in $G/H$ has order $p$.

Since $G/H$ is abelian, the Fundamental Theorem of Finite Abelian Groups tells us that $G/H$ is isomorphic to a direct product of cyclic groups. Because $|G/H| = p^n$ and every element in $G/H$ has order $p$, it must be true that $G/H \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p$.

So it suffices to compute the number of subgroups of index $p$ in $\bigoplus_{i=1}^{n} \mathbb{Z}_p$. The method in [2] for doing this is to consider $\bigoplus_{i=1}^{n} \mathbb{Z}_p$ as a vector space and to compute the number of subspaces of dimension $n - 1$.

We are now in a position to prove a generalized version of Theorem 2 found in [2].

**Proposition 16.** Every $n$-dimensional vector space $V$ over $\mathbb{Z}_p$ is isomorphic to $\bigoplus_{i=1}^{n} \mathbb{Z}_p$.

**Proof.** Let $V$ be a $n$-dimensional vector space over $\mathbb{Z}_p$ and let $\{u_1, u_2, \ldots, u_n\}$ be a basis for $V$. Define $\varphi : V \to \bigoplus_{i=1}^{n} \mathbb{Z}_p$ by $\varphi(x_1u_1 + x_2u_2 + \ldots + x_nu_n) = (x_1, x_2, \ldots, x_n)$. Let $v$ and $w$ be two vectors in $V$. Then $v = a_1u_1 + a_2u_2 + \cdots + a_nu_n$ and $w = b_1u_1 + b_2u_2 + \cdots + b_nu_n$ for some $a_i, b_i \in \mathbb{Z}_p$.

Now, $\varphi(v + w) = \varphi((a_1 + b_1)u_1 + (a_2 + b_2)u_2 + \cdots + (a_n + b_n)u_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = \varphi(a_1u_1 + a_2u_2 + \cdots + a_nu_n) + \varphi(b_1u_1 + b_2u_2 + \cdots + b_nu_n) = \varphi(v) + \varphi(w)$. Thus $\varphi$ is a homomorphism.

Suppose $\varphi(v) = \varphi(w)$. Then $\varphi(a_1u_1 + a_2u_2 + \cdots + a_nu_n) = \varphi(b_1u_1 + b_2u_2 + \cdots + b_nu_n)$. Thus $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ which implies $a_i = b_i$ for all $i$, and so $a_1u_1 + a_2u_2 + \cdots + a_nu_n = b_1u_1 + b_2u_2 + \cdots + b_nu_n$, which is to say $v = w$. Thus $\varphi$ is injective.

Let $(a_1, a_2, \ldots, a_n) \in \bigoplus_{i=1}^{n} \mathbb{Z}_p$. Then $a_1u_1 + a_2u_2 + \ldots + a_nu_n \in V$ and $\varphi(a_1u_1 + a_2u_2 + \ldots + a_nu_n) = (a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ for some $b_i \in \mathbb{Z}_p$. Thus $\varphi$ is surjective.

Therefore $\varphi$ is a bijection, and so $V \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p$. 

This completes the proof.
Thus $\varphi$ is surjective. Consequently, $\varphi$ is a isomorphism.

Note that $V \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p$ implies $|V| = p^n$.

Thus $\bigoplus_{i=1}^{n} \mathbb{Z}_p$ has the structure of a vector space in addition to being a group. There is also an equivalence between the subspaces and subgroups of $\bigoplus_{i=1}^{n} \mathbb{Z}_p$.

Let $W$ be a nonempty subgroup of $\bigoplus_{i=1}^{n} \mathbb{Z}_p$. Then by definition $W$ is closed under addition. Let $k \in \mathbb{Z}_p$ and $w \in W$. Then $kw = (ka_1, ka_2, \ldots, ka_n)$

$= (a_1, a_2, \ldots, a_n) + (a_1, a_2, \ldots, a_n) + \ldots + (a_1, a_2, \ldots, a_n) \in W$ since $W$ is closed under addition. Thus $W$ is closed under scalar multiplication. So $W$ is a subspace by the subspace test.

Conversely, every subspace of $\bigoplus_{i=1}^{n} \mathbb{Z}_p$ by definition is closed under addition and inverses. Thus every space is a subgroup by the subgroup test.

Lastly, subspaces of order $p^{n-1}$ correspond to subgroups of index $p$ of $\bigoplus_{i=1}^{n} \mathbb{Z}_p$, which has order $p^n$. Further, as a consequence of Prop. 16, a subspace of $\bigoplus_{i=1}^{n} \mathbb{Z}_p$ with order $p^{n-1}$ has dimension $n - 1$, and has the following name.

**Definition 1.** An $(n - 1)$-dimensional subspace of an $n$-dimensional vector space $V$ is called a hyperplane of $V$.

Before we present our next theorem, we need to prove the following lemma.

**Lemma 17.** Let $V$ be an $n$-dimensional vector space over $\mathbb{Z}_p$ and $v_1, v_2, \ldots, v_n$ be linearly independent vectors of $V$. Then $|\text{span}\{v_1, v_2, \ldots, v_n\}| = p^n$.

**Proof.** Let $n = 1$, then $\text{span}\{v_1\} = \{a_1v_1|a_1 \in \mathbb{Z}_p\} = \{0, v_1, 2v_1, \ldots, (p-1)v_1\}$. Thus $|\text{span}\{v_1\}| = p$. 

14
Suppose that the statement is true for \( n = k - 1 \), i.e. \( |\text{span}\{v_1, v_2, \ldots, v_{k-1}\}| = p^{k-1} \).

Note that \( \{a_1v_1 + \ldots + a_kv_k : a_i \in \mathbb{Z}_p\} \) is equal to the union of the disjoint sets
\[ \{a_1v_1 + \ldots + a_{k-1}v_{k-1} : a_i \in \mathbb{Z}_p\}, \{a_1v_1 + \ldots + a_{k-1}v_{k-1} + v_k : a_i \in \mathbb{Z}_p\}, \ldots, \{a_1v_1 + \ldots + a_{k-1}v_{k-1} + (p-1)v_k : a_i \in \mathbb{Z}_p\}. \]
Further each of these sets has \( p^{k-1} \) elements.

So \( |\text{span}\{v_1, v_2, \ldots, v_k\}| = |\{a_1v_1 + \ldots + a_{k-1}v_{k-1}\} \cup \{a_1v_1 + \ldots + a_{k-1}v_{k-1} + v_k\} \cup \ldots \cup \{a_1v_1 + \ldots + a_{k-1}v_{k-1} + (p-1)v_k\}| = p^{k-1} + p^{k-1} + \ldots + p^{k-1} = p \cdot p^{k-1} = p^k. \)

The next theorem is a generalized version of Theorem 2 in [2]. This is the theorem that will allow us to actually characterize the possible number of subgroups of index \( p \) in a group.

**Theorem 18.** Every \( n \)-dimensional vector space over \( \mathbb{Z}_p \) has exactly \( \frac{p^n - 1}{p - 1} \) hyperplanes.

**Proof.** Let \( V \) be an \( n \)-dimensional vector space over \( \mathbb{Z}_p \). Then \( V \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p \). Since dimension is equal to the number of elements in a basis, our goal is to count the potential bases for hyperplanes of \( V \) by counting the number of sets of \( n-1 \) linearly independent vectors.

Let us choose \( n-1 \) linearly independent vectors of \( V \) in the following way. First we choose \( v_1 \). To maintain linear independence we must avoid only the zero vector of \( V \). This means that there are \( p^n - 1 \) choices for \( v_1 \). Once \( v_1 \) is chosen, we must then choose \( v_2 \notin \text{span}\{v_1\} = \{0, v_1, 2v_1, \ldots, (p-1)v_1\} \). Thus there are \( p^n - p \) choices for \( v_2 \).

Suppose we have chosen vectors \( v_1 \) through \( v_{k-2} \) and we are seeking \( v_{k-1} \notin \text{span}\{v_1, \ldots, v_{k-2}\} \). By the previous lemma, we know the \( \text{span}\{v_1, \ldots, v_{k-2}\} \) has \( p^{k-2} \) elements. Thus there are \( p^n - p^{k-2} \) choices for \( v_{k-1} \).
This tells us we have \((p^n - 1)(p^n - p) \cdots (p^n - p^{n-2})\) subsets of \(n - 1\) linearly independent vectors. Further, we know each hyperplane of \(V\) contains \(p^{n-1}\) vectors, so we can also say that each hyperplane has \((p^{n-1} - 1)(p^{n-1} - p) \cdots (p^{n-1} - p^{n-2})\) linearly independent subsets of \(n - 1\) vectors. But each of these linearly independent sets are bases for the hyperplane that contains them. Thus we can say there are \((p^{n-1} - 1)(p^{n-1} - p) \cdots (p^{n-1} - p^{n-2})\) distinct bases for each hyperplane.

Finally, the number of distinct hyperplanes of \(V\) is the number of hyperplane bases divided by the number of bases per hyperplane.

Hence,

\[
\frac{(p^n - 1)(p^n - p) \cdots (p^n - p^{n-2})}{(p^{n-1} - 1)(p^{n-1} - p) \cdots (p^{n-1} - p^{n-2})} = \frac{(p^n - 1)p(p^{n-1} - 1) \cdots p(p^{n-1} - p^{n-3})}{(p^{n-1} - 1)(p^{n-1} - p) \cdots (p^{n-1} - p^{n-2})}
\]

\[
= \frac{(p^n - 1) \cdots p}{p^{n-1} - p^{n-2}}
\]

\[
= \frac{(p^n - 1)p^{n-2}}{p^{n-2}(p - 1)}
\]

\[
= \frac{(p^n - 1)}{(p - 1)}
\]

is the number of distinct hyperplanes in \(V\).

The result given in [2] is that the number of distinct hyperplanes is \(2^n - 1\), and this coincides with our result when \(p = 2\). So we are finally in a position to generalize Corollary 1 from [2], which characterizes the number of subgroups of index 2.

**Corollary 19.** Suppose \(p\) is the smallest prime dividing \(|G|\) and \(G\) has \(k\) subgroups of index \(p\). Then \(k = \frac{(p^n - 1)}{(p - 1)}\) for some \(n \geq 0\).

**Proof.** Theorem 13 gives that a group \(G\) has the same number of subgroups of index \(p\) as \(G/H\). Also \(G/H\) is isomorphic to \(\bigoplus_{i=1}^{n} \mathbb{Z}_p\), where the latter is an \(n\)-dimensional vector space over \(\mathbb{Z}_p\), call it \(V\). Further we have shown that hyperplanes
of $V$ correspond to subgroups of index $p$ in $G/H$. By Theorem 18, $V$ has $\frac{(p^n - 1)}{(p - 1)}$ hyperplanes. Hence $G$ has $\frac{(p^n - 1)}{(p - 1)}$ subgroups of index $p$ for some $n$. \hfill \Box

The next result is a generalized form of Corollary 2 found in [2]. However, unlike the result in [2], the generalized form does not rely on Theorem 18; thus we shall call it a proposition. It also has a proof that differs greatly from the $p = 2$ case. It uses several results from group theory, specifically those related to $p$-groups and Cauchy’s Theorem.

**Proposition 20.** A group $G$ has no subgroup of index $p$ if and only if $G = G^p$.

**Proof.** Suppose $G \neq G^p$. Thus $G/G^p \neq \{e\}$. As we have shown before, for an element $xG^p \in G/G^p$, $(xG^p)^p = G^p$, which is the identity element of $G/G^p$. Thus every nonidentity element in $G/G^p$ has order $p$. Since $p \mid |G/G^p|$, $|G/G^p| = p^k m$ for some positive integers $k$ and $m$ with $p \nmid m$. If $m \neq 1$, there exists a prime $q \neq p$ such that $q \mid m$. Thus $q \mid |G/G^p|$, and by Theorem 8 (Cauchy’s Theorem) there must exist an element of order $q$ in $G/G^p$. But this is impossible since every element must have order $p$ or $1$. Therefore $|G/G^p| = p^k$.

Since $|G/G^p| = p^k$, Proposition 9 implies that there exists a subgroup $F$ of $G/G^p$ such that $|F| = p^{k-1}$. Since $\frac{p^k}{p^{k-1}} = p$, we have that $F$ has index $p$ in $G/G^p$. Thus $G$ has a subgroup of index $p$. Therefore if $G$ has no subgroup of index $p$ then $G = G^p$.

Conversely, suppose $G = G^p$. Thus $G/G^p = \{e\}$, which has no subgroup of index $p$. Thus by Theorem 10, $G$ has no subgroup of index $p$. \hfill \Box

In Nganou’s paper there is a third corollary which says that a group $G$ has a unique subgroup of index 2 if and only if $G^2$ has index 2 in $G$. We were unable to generalize for $p > 2$, nor find a counterexample, so we include the original corollary (which was not proved in [2]) here.

17
Corollary 21. A group $G$ has a unique subgroup of index 2 if and only if $G^2$ has index 2 in $G$.

Proof. Suppose $G$ has a unique subgroup of index 2 in $G$. Then $\frac{2^n - 1}{2 - 1} = 1$ implies $n = 1$. We know that $G/G^2 \cong \bigoplus_{i=1}^{n} \mathbb{Z}_2$, so substituting $n = 1$ here gives $G/G^2 \cong \mathbb{Z}_2$. Thus $|G/G^2| = 2$, and so $G^2$ has index 2 in $G$.

Conversely suppose $G^2$ has index 2 in $G$. Then $|G/G^2| = 2$. Now we know that $G/G^2$ must be isomorphic to some product of cyclic groups, thus the only possibility is that $G/G^2 \cong \mathbb{Z}_2$. Since $\mathbb{Z}_2$ has a unique subgroup of index 2, namely $\{e\}$, $G/G^2$ must also only have a unique subgroup of index 2. Lastly, we know that $G$ and $G/G^2$ share the same number of subgroups of index 2 by Theorem 13, hence $G$ has a unique subgroup of index 2.

Thus we have have managed to generalize two of the three main corollaries stated in [2], and filled in the proof the one that we only know holds for the index 2 case.
Chapter 3

Conclusion

3.1 Summary

Let us recap some of the major results discussed in this paper that lead us to our final results. We first showed that \( G \) has the same number of subgroups of index \( p \) as \( G/H \) does. Then after proving that \( G/H \) is abelian and has order \( p^n \), it becomes evident that \( G/H \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p \) by applying the Fundamental Theorem for Finite Abelian Groups. Then we find that \( \bigoplus_{i=1}^{n} \mathbb{Z}_p \cong V \), an \( n \)-dimensional vector space over \( \mathbb{Z}_p \). Further we argue that subgroups of index \( p \) in \( \bigoplus_{i=1}^{n} \mathbb{Z}_p \) correspond to hyperplanes of \( V \). Ultimately we get that the number of hyperplanes in \( V \) is \( \frac{p^n - 1}{p - 1} \) by using basic counting principles and known properties of bases. This leads to a few other corollaries, one of which is our most important result, which is a characterization for the number of subgroups of index \( p \) in \( G \).
3.2 Further Questions

Of the three corollaries stated in [2], Corollary 3 was not able to be generalized in this paper due to the fact that $G/G^p$ is not always abelian. Thus we could not apply the Fundamental Theorem of Finite Abelian Groups. Hence we have the following question: is $G/G^p$ isomorphic to some group other than $\bigoplus_{i=1}^{n} \mathbb{Z}_{p^i}$ such that we can use its structure to find its number of subgroups of index $p$?

Another question also remains. Theorem 13 gives that $G$ has the same number of subgroups in index $p$ as $G/H$ does, however this is only true if we assumed $p$ was the smallest prime dividing $|G|$ (or that all of the subgroups of index $p$ are normal). If $p$ is not the smallest prime dividing the order of $|G|$, then because of the way we defined $H$, $H$ may not be normal in $G$. Consequently $G/H$ is not a group. Thus it is important to note that Corollary 19 only gives the number of subgroups of index $p$ if $p$ is the smallest prime dividing $|G|$. So our remaining question would be, is this a way to characterize the number of subgroups of index $p$ if $p$ is not the smallest prime dividing $|G|$?
Bibliography

