6-2015

The Sylow Theorems and Classification of Small Finite Order Groups

William Stearns
Union College - Schenectady, NY

THE SYLOW THEOREMS AND CLASSIFICATION OF SMALL FINITE ORDER GROUPS

WILLIAM W. STEARNS

Abstract. This thesis will provide an overview of various topics in group theory, all in order to accomplish the end goal of classifying all groups of order up to 15. An important precursor to classifying finite order groups, the Sylow Theorems illustrate what subgroups of a given group must exist, and constitute the first half of this thesis. Using these theorems in the latter sections we will classify all the possible groups of various orders up to isomorphism. In concluding this thesis, all possible distinct groups of orders up to 15 will be defined and the groundwork set for further study.

1. Introduction

The results in this thesis require some background knowledge and motivation. To that end, material covered in an introductory course on abstract algebra should be sufficient. In particular, it is assumed that the reader is familiar with the concepts and definitions of: group, subgroup, coset, index, homomorphism, and kernel. If needed, these topics are all covered in Chapter 2 of W. Keith Nicholson's *Introduction to Abstract Algebra: Fourth Edition*[**?**]. However, several of the more specific background topics in these areas which are particularly relevant to this thesis shall be reviewed in this section.

To start, we will remind the reader of the concept of a cyclic subgroup.

Definition 1.1. Let G be a group, with $a \in G$. Then, $\langle a \rangle = \{a^n : n \in \mathbf{Z}\}$ is a subgroup of G, called the *cyclic subgroup generated by* a.

Note that for groups of finite order, this can be adjusted to
$\langle a \rangle = \{a^n : 0 \leq n < \text{ord}(a)\}$.

We will now look at a relation between the different elements of a given group.

Date: May 19, 2015.

Definition 1.2. Let G be a group. If $a \in G$, we say $b \in G$ is *a conjugate of* a, denoted $a \sim b$, if there exists some $x \in G$ such that $xax^{-1} = b$.

Proposition 1.3. *$\sim$ is an equivalence relation on G.*

Proof. To see that $\sim$ is reflexive, note that $\forall a \in G$ we know $eae^{-1} = eae = a$ so clearly $a \sim a$. For symmetry, assume $a \sim b$, that is $\exists x \in G$ such that $xax^{-1} = b$. Then it follows that $a = x^{-1}bx = (x^{-1})b(x^{-1})^{-1}$, which implies $b \sim a$. Last, to see $\sim$ is transitive assume $a \sim b$, $b \sim c$, that is $\exists x, y \in G$ such that $xax^{-1} = b$ and $yby^{-1} = c$. Then $y(xax^{-1})y^{-1} = c$ which implies $yxax^{-1}y^{-1} = c$ or $(yx)a(yx)^{-1} = c$ and thus $a \sim c$. □

It follows then, that $\sim$ partitions G into equivalence classes. We say that a and b are *conjugates* if b is a conjugate of a and the $\sim$ equivalence class of any element a is called the *conjugacy class* of a, denoted $[a]$.

For G a finite group, since we know that the distinct equivalence classes $[a_1], [a_2], [a_3], \ldots, [a_s]$, with sizes $c_1, c_2, c_3, \ldots, c_s$ respectively, partition G, it follows that $|G| = c_1 + c_2 + c_3 + \cdots + c_s$. This is the first version of the *class equation* of G. The next definition will lead to a significant modification of the class equation.

Definition 1.4. The *center of* G is the subgroup of G, denoted $\mathbf{Z}(G)$, such that all elements of $\mathbf{Z}(G)$ commute with all of G, i.e. $\mathbf{Z}(G) = \{a \in G : ag = ga, \ \forall g \in G\}$.

Proposition 1.5. *Using the notation following Prop 1.3, the class equation of a finite group G can be rewritten as:*

$$|G| = |\mathbf{Z}(G)| + c_{r+1} + c_{r+2} + c_{r+3} + \cdots + c_s$$

where $c_{r+1}, \ldots, c_s$ are the sizes of conjugacy classes such that $c_{r+i} > 1$ for $1 \leq i \leq (s - r)$.

Proof. For each $a \in \mathbf{Z}(G)$ the conjugacy class of a contains only a, that is $[a] = \{a\}$, because a commutes with every element. In particular $\forall x \in G$, $xax^{-1} = axx^{-1} = a$.

Combining these one-element conjugacy classes from elements of the center of G we get the size of the center of G, $|\mathbf{Z}(G)|$. □

Definition 1.6. Given a group G and a subgroup N of G. We say that N is a *normal* subgroup of G if it is closed with respect to conjugation. That is, for any $a \in N$, and $x \in G$ we have that $xax^{-1} \in N$.

In particular, this means that left and right cosets of a normal subgroup are equal. This result is important for the next proposition.

Proposition 1.7. *If N is normal in G, then the set of distinct cosets of N, denoted: $G/N = \{aN : a \in G\}$, is itself a group, under the operation defined as follows:*

(1) *$N = eN$ is the identity element*

(2) *Given $aN, bN \in G/N$, $aNbN = (ab)N$.*

Proof. We will leave it to the reader to show that the operation is well-defined and that the inverse of aN is $a^{-1}N$, and focus on closure of the operation. It should then be noted that $NN = N$ as any element of N multiplied by another element of N yields an element of N. Given that N is normal, $Nb = bN$, so $aNbN = a(Nb)N = a(bN)N = (ab)NN = (ab)N$, and so the group G/N is closed under the operation as defined. □

Remark: For more details, see [**?**], pages 147-149.

The previous proposition will feature prominently in the proofs of **Cauchy's Theorem** as well as at least one of the **Sylow Theorems**.

Theorem 1.8. ***[Lagrange's Theorem]*** *Let G be a finite group, and H any subgroup of G. The order of G is a multiple of the order of H.*

We will now sketch a proof of Lagrange's Theorem. An integral part of this proof-sketch, as well as many others going forward, is the notion of the index of a subgroup. As such, from here on we will denote the index of a subgroup H of G by $[H : G]$.

Proof. Let $k = [G : H]$, and let $H_1, \ldots, H_k$ be the distinct cosets of H in G.

Then, $G = H_1 \cup \cdots \cup H_k$, and this union is disjoint because every element of G exists in 1 and only 1 coset of H. Thus we have that $|G| = |H_1| + \cdots + |H_k|$. But, because for all i such that $1 \leq i \leq k$, $|H_i| = |H|$ we can rewrite this as $|G| = |H| + \cdots + |H|$. This then simplifies to $|G| = k\,|H|$ and furthermore $\dfrac{|G|}{|H|} = k = [G : H]$. □

Asking whether or not the converse is true is an important motivating question for the results found in the early part of this thesis. We will see in Section 4 that the Sylow Theorems, in part, answer this question, but more on that later.

Another important piece of background knowledge useful to the reader is the **Fundamental Homomorphism Theorem**. An explanation and proof for this can be found in [**?**] on pages 158-159. An important corollary to this theorem, known as the **Correspondence Theorem**, will be proven here.

Theorem 1.9. ***[Correspondence Theorem]*** *Let f be a homomorphism from G onto H with kernel K. If S is any subgroup of H, let $S^* = \{x \in G : f(x) \in S\}$. Then $S \cong S^*/K$.*

Proof. First we show that S^* is a subgroup of G. Because f is a homomorphism, the identity of G maps to the identity of H, so $e_G \in S^*$. For $a, b \in G$ such that $f(a), f(b) \in S$, then $a, b \in S^*$. It follows that $ab \in S^*$, since $f(b), f(a) \in S$, $f(a)f(b) \in S$ implies $f(ab) \in S$. For $a \in G$ such that $f(a) \in S$, we see that $f(a^{-1})f(a) = e = f(a)f(a^{-1})$, thus $f(a^{-1}) = f(a)^{-1}$, and since S is a subgroup it is closed under inverses, which implies $f(a^{-1}) \in S$, and so $a^{-1} \in S^*$. Thus S^* is closed under the group operation from G, contains arbitrary inverses, and the identity, so is a subgroup. Note also that for $x \in K$, $f(x) = e_H$ where e_H is the identity of H and therefore the identity of S, thus $x \in S^*$, so $K \subseteq S^*$.

Now, take g to be the function f restricted to the domain S^*, i.e. $g(x) = f(x)$ for all $x \in S^*$. Like f, g is a homomorphism, though it is instead from S^* to S. We know

that $S^* = f^{-1}(S)$ and by definition $f : f^{-1}(S) \to S$ is onto as f is onto. Since this is in fact a restriction of f to S^*, it is g, so we see g is onto. Call the kernel of g, K_g. We will show that the kernel of g is K. We have that $e_H = e_S$ and the kernel of f is K, as well as that $K \subseteq S^*$. Then for $x \in K$, $g(x) = e_H = e_S$. We see $x \in K_g$, and so $K \subseteq K_g$. Since there can be no element z of S^* such that $z \notin K$ and $g(z) = e_S$, we see that $K = K_g$.

Thus we now have g, a homomorphism from S^* onto S with kernel K. Thus by the **Fundamental Homomorphism Theorem**, we have that $S \cong S^*/K$. □

2. Introductory Definitions

This section will provide the foundational topics and definitions necessary to understand the Sylow Theorems. Of particular importance is the concept of a group acting on a set, or on itself. This topic is known as the theory of group actions, and provides the basis for many of the proofs we will need going forward.

Since the end goal of this thesis is to classify small order finite groups, from this point on we will always implicitly assume that all groups are finite.

Definition 2.1. We say a group G is a *p-group* if for all $a \in G$ the order of a is a power of p.

Expanding on this idea, we can construct subgroups of a group which are themselves p-groups; these we call p-subgroups of the group. The next definition more thoroughly classifies p-subgroups.

Definition 2.2. We say a subgroup S of a group G is a *p-Sylow subgroup* (of G) if S is a p-subgroup, and S is maximal in G i.e. if there exists some other p-subgroup S' of G such that $S \subseteq S'$, then $S = S'$.

Proposition 2.3. *Let G be a group and K a p-Sylow subgroup of G. Then $\forall g \in G$ the conjugate gKg^{-1} of K is also a p-Sylow subgroup of G.*

Proof. Let K be a p-Sylow subgroup of G, and let gKg^{-1} be a conjugate of K and note that $|K| = |gKg^{-1}|$. We will first show gKg^{-1} is a subgroup of G. Clearly, $e \in gKg^{-1}$, since $geg^{-1} = e$, and for $a, b \in gKg^{-1}$ there exists $k_1, k_2 \in K$ such that $a = gk_1g^{-1}$ and $b = gk_2g^{-1}$. We see that $ab = gk_1g^{-1}gk_2g^{-1} = gk_1k_2g^{-1}$, and since $k_1k_2 \in K$, $ab \in gKg^{-1}$, therefore gKg^{-1} is a subgroup of G. Now, to see gKg^{-1} is a p-subgroup, let $b \in gKg^{-1}$, so $b = gkg^{-1}$ for some $k \in K$. Since $k \in K$ we know $\text{ord}(k)$ is a power of p, say p^r for some $r \in \mathbf{N}$. We see $\text{ord}(b) | \text{ord}(k)$, because $b^{p^r} = g^{p^r}k^{p^r}g^{-p^r} = g^{p^r}eg^{-p^r} = g^{p^r}g^{-p^r} = e$. As such, we have shown that gKg^{-1} is itself a p-subgroup of G. To show it is maximal, take some p-subgroup A of G where $gKg^{-1} \subseteq A$. From the first part of this proof we showed that if A is a subgroup of G then so is gAg^{-1}, and we see that $g^{-1}Ag = (g^{-1})A(g^{-1})^{-1}$, thus $g^{-1}Ag$ is a subgroup of G. Assume there exists an $a \in A$ such that $a \notin gKg^{-1}$. Then $|A| > |gKg^{-1}|$, but that implies $K \subseteq g^{-1}Ag$ and $|g^{-1}Ag| > |K|$, but this violates the maximality of K, therefore $A = gKg^{-1}$, thus gKg^{-1} is also maximal. Because gKg^{-1} is a maximal p-subgroup of G, it is a p-Sylow subgroup of G, and thus every conjugate of K is a p-Sylow subgroup. □

The next few definitions are related to the topic of group actions.

Definition 2.4. For a non-empty set A and a group G, a mapping from $G \times A \to A$, denoted $(g, a) \to g(a)$ is called an *action* if it satisfies the following conditions:

(1) $e(a) = a \ \forall a \in A$.

(2) $g_1(g_2(a)) = (g_1g_2)(a)$, $\forall g_1, g_2 \in G$, $a \in A$

A is sometimes called a *G-set*.

The following definitions will all have to do with particular results using G, A, and an action as described above. We have already seen one example of a group action, namely conjugation, and in that case the group acts upon itself. I particular, for

$g, a \in G$ $(g, a) \to gag^{-1}$. We leave it to the reader to show this is an action as defined above.

Definition 2.5. For a G-set A, if $a \in A$, the *orbit of* a relative to the group action is the set:

$$O(a) = \{g(a) : g \in G\}$$

Note: $O(a)$ is a subset of A.

We observe that using conjugacy as our action, the orbit of any $a \in G$ by conjugacy is the set of conjugates of a, or the conjugacy class of a. This means, the $c_1, c_2, c_3, \ldots, c_s$ defined after proposition 1.3 to be the sizes of the conjugacy classes of elements of G are the sizes of the different orbits of these elements by the conjugacy action.

Remark 2.6. There is an equivalence relation on A that relates elements of the same orbit. In particular, $b \propto a$ if and only if $b = g(a)$ for some $g \in G$. We see $\propto$ is trivially reflexive by definition, and symmetry and transitivity follow from the definition of group action. Therefore, the distinct orbits of the different a's in A are equivalence classes, and so partition A, i.e. no element $b \in A$ is an element of more than one distinct orbit. This was seen previously in the notion of conjugacy classes.

Definition 2.7. If $a \in A$, the *stabilizer of* a relative to a given group action is the set:

$$G_a = \{g \in G : g(a) = a\}$$

Note: G_a is a subset of G, and it can be easily shown that G_a is a subgroup. This follows from the definition of group action.

Using the conjugacy action from Section 1, we get that the stabilizer of a is all the elements which commute with a, a set which has its own special name defined below:

Definition 2.8. For any $a \in G$, the *centralizer* of a, denoted C_a, is the set of all elements of G that commute with a, that is:

$$C_a = \{x \in G : xax^{-1} = a\}$$

Note: C_a is a subgroup of G. Clearly e is an element of C_a, and it is also easy to see that if $x \in C_a$ so is x^{-1}. Last, if $x, y \in C_a$ then $xax^{-1} = a$ and $yay^{-1} = a$, so $xax^{-1} = xyay^{-1}x^{-1} = xya(xy)^{-1} = a$ which implies $xy \in C_a$.

We will now prove a lemma about the nature of the cosets of the stabilizer.

Lemma 2.9. *The coset g_1G_a of G_a is equal to the set of all elements that map to $g_1(a)$, i.e.:*

$$g_1G_a = \{g \in G : g(a) = g_1(a)\}$$

Proof. To begin with, $g_1G_a = \{g_1g_a : g_a \in G_a\}$ where $g_a(a) = a$. Take $g_1g_a \in g_1G_a$. We see $(g_1g_a)(a) = g_1(g_a(a)) = g_1(a)$ so $g_1g_a \in \{g \in G : g(a) = g_1(a)\}$. Now, take $h \in \{g \in G : g(a) = g_1(a)\}$. Since $h(a) = g_1(a)$ we see that $g_1^{-1}h(a) = a$, so $g_1^{-1}h_a \in G_a$, which implies $\exists h_a \in G_a$ such that $g_1^{-1}h = h_a$, which can be rewritten as $h = g_1h_a$ and so $h \in g_1G_a$ and therefore $g_1G_a = \{g \in G : g(a) = g_1(a)\}$ as desired. □

Using this lemma we will relate the orbit of an element and that elements stabilizer.

Proposition 2.10. *Given a G-set A, for $a \in A$ the order of the orbit of a is equal to the index in G of the stabilizer of a, i.e.*

$$|O(a)| = [G : G_a]$$

Proof. A coset hG_a of G_a is of the form $hG_a = \{hg_a : g_a \in G_a\}$, which can be rewritten as $hG_a = \{g \in G : g(a) = h(a)\}$. Thus, if $f, g \in G$, then f and g are in the same coset of G_a if and only if $f(a) = g(a)$. This implies there is a coset of G_a for each different value of $g(a)$, because if $f(a) \neq g(a)$ then f and g are in different cosets

of G_a. That means the number of cosets of G_a is equal to the number of different values of $g(a)$, which is equivalent to the size of the orbit of a, $|O(a)|$. □

Now, we observe that if $|O(a)| = 1$, that is $O(a) = \{a\}$, then $[G : G_a] = 1$ so $G_a = G$. The next definition looks at elements where this is the case.

Definition 2.11. The subset of all $a \in A$ for which $G_a = G$, or equivalently $O(a) = \{a\}$, is called the *fixed subset*, denoted A_f.

Note: A_f is a subset of A; in particular $A_f = \{a \in A : g(a) = a, \forall g \in G\}$

We saw an example of this in Section 1, where the conjugacy class of an element in the center of a group has only the one element. As we have previously stated, conjugacy is itself a group action where the group acts upon itself. For that, the orbit of an element of the center by conjugacy was shown to be merely the element itself, and so the stabilizer of that element would be the whole of the group.

A special case of the class equation can be seen when partitioning a G-set by its orbits. Note that if $a \in A_f$ then $|O(a)| = 1$.

Corollary 2.12. *Let A be a non-zero G-set, and let $O(a_1), \ldots, O(a_m)$ be the non-singleton orbits, then:*

$$|A| = |A_f| + \sum_{i=1}^{m} |O(a_i)| = |A_f| + \sum_{i=1}^{m} [G : G_{a_i}]$$

Proof. Taking A to be G where G is acting on itself by conjugation this merely becomes Proposition 1.5 and as such the proof is mostly the same. □

We will now look at a group action which acts on the power set of a G-set.

Remark 2.13. If A is a G-set with action g we can define an action on the power set of A. For any $C \subseteq A$ we define $g(C)$ as the mapping from $G \times P(A) \to P(A)$, denoted $(g, C) \to g(C)$, as:

(1) $e(C) = C \ \forall C \subseteq A$.

(2) $g_1(g_2(C)) = (g_1g_2)(C)$, $\forall g_1, g_2 \in G$, $C \subseteq A$

We leave it to the reader to prove this is, in fact, an action.

Note that using the above action we can adjust the centralizer of an element of G. In particular, we will form a subgroup of G with elements $g \in G$, $gCg^{-1} = C$ for $C \subseteq G$. This is the stabilizer under the action above, and has a special name defined below.

Definition 2.14. For any $C \subseteq G$, the *normalizer* of C in G, denoted $N(C)$, is defined by:

$$N(C) = \{a \in G : aC = Ca\}$$

Note: $C \subseteq N(C)$.

Remark 2.15. We reiterate that:

$$N(C) = \{a \in G : aCa^{-1} = C\}$$

Proposition 2.16. *$N(C)$ is a subgroup of G.*

Proof. To show $N(C)$ is a subgroup of G, we need to show three things. First, $e \in N(C)$ as clearly, $eC = C = Ce$. Then, if $a \in N(C)$ we know that $aC = Ca$ thus $aCa^{-1} = C$, so $Ca^{-1} = a^{-1}C$, thus $a^{-1} \in N(C)$. Lastly, for $a, b \in N(C)$ we know that $aC = Ca$ and $bC = Cb$ so for $(ab)C$ we see that $(ab)C = a(bC) = a(Cb) = (aC)b = (Ca)b = C(ab)$. Therefore $(ab) \in N(C)$ as desired. □

Remark 2.17. It will be useful later to know that in particular, for any $C \subseteq G$ with normalizer $N(C)$, the number of conjugates of C in G is equal to the number of distinct cosets of $N(C)$ in G. This comes from extending Proposition 2.9 to use subsets with conjugation instead of elements. More formally, this is explained in the following corollary.

To prove the corollary, we can use proposition 2.10 using the group action on the power set, as seen in the following corollary.

Corollary 2.18. *Using conjugacy for the group action defined in definition 2.13 on a subset C of G, we get:*

$$|[C]| = [G : N(C)]$$

Proof. By proposition 2.10 we have that $|O(a)| = [G : G_a]$, where A is a G-set. Taking the G-set defined by conjugacy on $P(G)$ as in definition 2.13, we get $|O(C)| = [G : G_C]$. We see that in this case, $G_C = \{a \in G : aCa^{-1} = C\} = N(C)$ and $O(C) = \{aCa^{-1} : a \in G\} = [C]$. Therefore $|[C]| = |O(C)| = [G : G_C] = [G : N(C)]$ as desired. □

3. Preliminaries to Sylow's Theorems

The results in this section will form the foundation for the proofs of the Sylow Theorems which appear in the next chapter. Chief among these is what is known as Cauchy's Theorem, which proves an important fact relating the order of certain elements of a group to the order of the group itself.

Theorem 3.1. ***[Cauchy's Theorem]*** *If G is a group and p is any prime such that $p \mid |G|$ then $\exists a \in G$ such that* $\text{ord}(a) = p$.

Before the proof, we recall a result about primes from elementary number theory which says for $k, m \in \mathbf{N}$ and a prime q, if $q|km$ then $q \mid m$ or $q|k$, or equivalently if $q|km$ and $q \nmid m$ then $q|k$.

Proof. This will be done in two parts, first when G is abelian.

We assume G is an abelian group, and will perform induction on the order of G. First, when $|G| = 1$ the result is true by default. For $|G| = 2$, it is also fairly trivial as $G = \{e, g\}$, so then if $\text{ord}(g) = 1$ we'd have $g = e$ and thus $|G| = 1$, so $\text{ord}(g) = 2$.

Now let $|G| = k$, and assume the claim holds for every abelian group of order less than k. Take $a \in G$ where $a \neq e$. If $\text{ord}(a) = p$ we are done. Moreover if there exists $t \in \mathbf{N}$ such that $\text{ord}(a) = tp$ then $\text{ord}\,(a^t) = p$, and we're done.

So suppose the order of a is not a multiple of p, and construct the cyclic group generated by a, namely $\langle a \rangle$. Then because G is abelian we know $\langle a \rangle$ is normal in G so $G/\langle a \rangle$ is a group of cosets of $\langle a \rangle$, where $|G/\langle a \rangle| < k$. We know by Lagrange's Theorem that $|G| = |G/\langle a \rangle||\langle a \rangle|$, and $p \mid |G|$ but $p \nmid \langle a \rangle$ as we have defined it, thus $p \mid |G/\langle a \rangle|$. Now, because $|G/\langle a \rangle| < k$ and is a multiple of p, by the inductive hypothesis $|G/\langle a \rangle|$ must have an element of order p, say the coset $c\langle a \rangle$, for $c \in G$. For $c \in G$, the order of $c\langle a \rangle$ in $G/\langle a \rangle$ is a divisor of the order of c in G. This follows because $\text{ord}(c) = n$ for some $n \in \mathbf{N}$ implies $(c\langle a \rangle)^n = c^n(\langle a \rangle)^n = e\langle a \rangle$ and so the order of $c\langle a \rangle$ must divide $n = \text{ord}(c)$ as desired. Thus $\text{ord}(c) = tp$ for some $t \in \mathbf{N}$, and therefore there exists an element of G, namely c^t whose order is p.

Now, assume that G is not abelian. Once again we will use induction on the order of G. We note that the beginning of the induction is the same as above, so we let $|G| = k$ and assume that for all $n < k$ the claim is true.

Let $Z = \mathbf{Z}(G)$, and let C_a be the centralizer of a for each $a \in G$. G is non-abelian, so we know that $|Z| < |G|$, and we know that $|C_a| < |G|$ for $a \notin \mathbf{Z}(G)$, and such an a exists since G is non-abelian. Now look at $a \notin Z$. If $p \mid |C_a|$ we are done, as C_a is a group such that $|C_a| < |G|$ and by the inductive hypothesis we can then assume there exists $c \in C_a$ such that $\text{ord}(c) = p$. Otherwise $p \nmid |C_a|$ for all $a \in G$ where $a \notin Z$, we have that $|G| = |C_a|[G : C_a]$ which implies $p \mid [G : C_a]$. We know by the class equation that $|G| = |Z| + k_s + \cdots + k_t$ where $k_s, \ldots, k_t$ are the indices of the distinct C_a. Rearranging this equation we get $|Z| = |G| - (k_s + \cdots + k_t)$. Because each of the k_i as well as $|G|$ is a multiple of p we can factor this p out, to get $|Z| = p(b)$ for some $b \in \mathbf{N}$, so we have constructed an abelian group of order a multiple of p. We proved

this result for abelian groups above, so since $p \mid |Z|$, we know that there exists $g \in Z$ such that $\text{ord}(g) = p$, and $g \in Z \Rightarrow g \in G$, so we are done.

Thus, with these two parts, we have proved the theorem that for all primes p such that $p \mid |G|$, there exists $a \in G$ such that $\text{ord}(a) = p$. □

Corollary 3.2. *If G is a finite p-group, then $|G| = p^n$ for some $n \in \mathbf{N}$.*

Proof. Since G is a p-group we know that every element of G has order p. By Cauchy's Theorem, for every prime q that divides the order of G there is an element of G with order q, thus because every element has order p there can be no other primes that divide the order of G, and so $|G| = p^n$ for some $n \in \mathbf{N}$ as desired. □

Using Cauchy's Theorem and the Correspondence Theorem, we will prove a lemma which shows what size subgroups there are in a p-group, which we shall call the **Subgroups Lemma**.

Lemma 3.3. ***Subgroups Lemma*** *Let p be a prime number. If G is a p-group such that $|G| = p^n$ then G has a normal subgroup of order p^m for all m such that $1 \leq m < n$.*

Proof. Once again we will use induction on $|G|$. For $|G| = p$ we are done, and we assume that the lemma is true for every p-group smaller than G.

We begin by looking at the class equation of G using conjugacy as described in Section 1: $|G| = |\mathbf{Z}(G)| + c_{r+1} + c_{r+2} + c_{r+3} + \cdots + c_s$. Because conjugacy can be viewed as a group action by G on itself, we see the c_i's are the sizes of the orbits of the different elements of G, and thus each of the c_i's must divide $|G|$ by proposition 2.10 and Lagrange's Theorem. Thus, because G is a p-group, the values of the different c_i's have to be powers of p. Furthermore, the class equation can then be changed from $|G| = |\mathbf{Z}(G)| + c_{r+1} + c_{r+2} + c_{r+3} + \cdots + c_s$ to become $p^n = |\mathbf{Z}(G)| + p^{u_{r+1}} + \cdots + p^{u_s}$ for appropriate $u_{r+1}, \ldots, u_s$ and thus it can be rearranged and subsequently factored

to get $|\mathbf{Z}(G)| = mp$ for some $m \in \mathbf{N}$. Now by Cauchy's Theorem we know that there exists an element $a \in \mathbf{Z}(G)$ with order p. We can now construct $\langle a \rangle$, which is a normal subgroup of G because a is in the center of G, and take $G/\langle a \rangle$ which is a group. Because $G/\langle a \rangle$ is a group, we know by Lagrange's Theorem that $|G/\langle a \rangle| = p^{n-1}$, and so it has normal subgroups of orders $p, \ldots, p^{n-2}$ by the inductive hypothesis. Now, let S be the normal subgroup of order p^j, $1 \leq j < n-1$. By the Correspondence Theorem we know there exists a subgroup S^* of G such that $S \cong S^*/\langle a \rangle$. We know S and $\langle a \rangle$ are both normal, thus S^* is a normal subgroup by [**?**] Theorem 7.44 part (2), and it has order $|S|\,|\langle a \rangle| = p^j p = p^{j+1}$ for $1 \leq j < n-1$. This implies that G has a normal subgroup of order p^m for $2 \leq m < n$. We previously defined $\langle a \rangle$ as a normal subgroup of order p, so we have subsets of G with orders p^m for $1 \leq m < n$, so we are done. □

Remark 3.4. If $|G| = p^n$, then since $\mathbf{Z}(G)$ is a subgroup, by Lagrange's Theorem $|\mathbf{Z}(G)| \mid |G|$, so $|\mathbf{Z}(G)| = 1$ or a power of p. In the above proof we showed that $|\mathbf{Z}(G)| \neq 1$, thus $|\mathbf{Z}(G)| = p^r$ for some $r \in \mathbf{N}$, $r > 1$.

The last lemma we will prove in this section will be beneficial in proving the first Sylow Theorem.

Lemma 3.5. *For K a p-Sylow subgroup of G and $a \in G$, if $aKa^{-1} = K$ and $\operatorname{ord}(a) = p^n$ for some n then $a \in K$.*

Proof. Let $a \in G$, and assume $aKa^{-1} = K$. Construct the normalizer of K, and call it N and note that $a \in N$. We know that $K \subseteq N$, and it follows from the definition of normalizer that K is normal in N, so N/K is a group. The order of aK in N/K is a power of p since $(aK)^{p^n} = a^{p^n}K = K$. Thus $\operatorname{ord}(aK)$ divides p^n. Let $S = \langle aK \rangle$ be the cyclic subgroup of N/K generated by aK, where $|S| = |aK| = p^m$ for some $m \in \mathbf{N}$. By the Correspondence Theorem, N has a subgroup S^* such that $S \cong S^*/K$. This implies that $|S^*/K| = |S|$, which means, $|S^*/K| = p^m$, so S^*/K is a p-group.

Also, K is a p-group so we know $\exists n \in \mathbf{N}$ such that $|K| = p^n$. Then, $|S^*| = |S^*/K||K|$ implies $|S^*| = p^m p^n = p^{m+n} = p^r$ for some $r \in \mathbf{N}$ and thus by corollary 3.2, S^* must be a p-group, and because $S^* \subseteq N \subseteq G$ we know $S^* \subseteq G$. Now, since $K \subseteq S^*$ and S^* is a p-subgroup of G, it follows that $S^* = K$, as otherwise it would violate the maximality of K. As such, $S^* = K$ which implies $|S^*/K| = 1$. Then we have $|S| = 1$ and so $\langle aK \rangle = \{K\}$ which leads to $aK = K$ and finally $a \in K$. □

It follows that no element other than the identity of N/K has order a power of p, as any such aK as above, would be equal to K which is the identity of N/K. We can expand this using Cauchy's Theorem to get the following corollary:

Corollary 3.6. *The index of K in N is not a multiple of p.*

Proof. We state in the last line prior to the corollary that no non-identity element of N/K has order a power of p. By Cauchy's Theorem, we know that for any prime $q \in \mathbf{N}$ such that $q \mid |N/K|$ there exists an element of N/K with order q. Since no element of N/K has order a power of p, specifically there is no element $cK \in N/K$ such that $\text{ord}(cK) = p$, it follows that $p \nmid |N/K|$. The group N/K is the set of cosets of K in N, so $[N : K] = |N/K|$, thus if $p \nmid |N/K|$, then $p \nmid [N : K]$. □

4. Sylow's Theorems

Motivation for the Sylow Theorems comes from attempting to determine the validity of the converse of Lagrange's Theorem. To review, Lagrange's Theorem says that the order of any subgroup H of some group G, will divide the order of G. The converse of this would then be that if there exists $n \in \mathbf{N}$ such that $n \mid |G|$ then G has some subgroup H such that $|H| = n$. The first Sylow theorem serves to determine when this converse actually holds, and classifies various subgroups of the group G, based on order. The second and third Sylow theorems classify the relations between some of the subgroups of G that are equal in size.

Theorem 4.1. ***[1st Sylow Theorem]*** *Let G be a group. If p is a prime and p^n divides $|G|$, then G has a subgroup of order p^n.*

Proof. We know by Cauchy's Theorem that for any prime p which divides the order of G there is some element $g \in G$ such that $\text{ord}(g) = p$. Constructing the cyclic subgroup of G generated by g, we get the group $\langle g \rangle$ which is a p-subgroup. Taking this subgroup $\langle g \rangle$ one of two things can be true. Either $\langle g \rangle$ is maximal, in which case it is a p-Sylow subgroup. The other option is that there exists some $H \subseteq G$ with $|H| = p^i$ for some $i \in \mathbf{N}$, $i > 1$ and $\langle g \rangle \subseteq H$. Repeating this process with H, we can see that for any prime p that divides the order of G we can find a p-Sylow subgroup of G since G is finite. We will therefore show that for a group G where $|G| = mp^k$, $m \in \mathbf{N}$, $\gcd(p, m) = 1$, that for K a p-Sylow subgroup of G that $|K| = p^k$.

To that end let G be a group with $|G| = mp^k$, $m \in \mathbf{N}$, $\gcd(p, m) = 1$, and let K be a p-Sylow subgroup of G. Because K is a p-Sylow subgroup we know that $|K| = p^s$ for some $s \in \mathbf{N}$, $s \leq k$.

Let X be the set of all the conjugates of K, that is $X = \{gKg^{-1} : g \in G\}$. If $C_1, C_2 \in X$, let $C_1 \sim C_2$ if and only if $aC_1a^{-1} = C_2$ for some $a \in K$. It is easy to see that $\sim$ is an equivalence relation on X. That $\sim$ is reflexive follows because $\forall C \in X$ we know $eCe^{-1} = eCe = C$. That $\sim$ is symmetric follows because $C_1 \sim C_2$ implies $\exists a \in K$ such that $aC_1a^{-1} = C_2$. This can be rewritten as $C_1 = a^{-1}C_2a = (a^{-1})C_2(a^{-1})^{-1}$, which implies $C_2 \sim C_1$. Finally, we see $\sim$ is transitive because for $C_1 \sim C_2$, $C_2 \sim C_3$ we have that $\exists a, b \in G$ such that $aC_1a^{-1} = C_2$ and $bC_2b^{-1} = C_3$. Then $b(aC_1a^{-1})b^{-1} = C_3$ which implies $baC_1a^{-1}b^{-1} = C_3$, or $(ba)C_1(ba)^{-1} = C_3$, and thus $C_1 \sim C_3$. Now, we know that because $\sim$ is an equivalence relation that it partitions X into equivalence classes. Denote the equivalence class of $C \in X$ by $[C]$. Now, construct the normalizer of C in G, denoted $N(C)$, to be $N(C) = \{a \in G : aCa^{-1} = C\}$. We know that the set of conjugates of C

in G is in 1-1 correspondence with the set of cosets of $N(C)$, as seen by Corollary 2.19, that is $|\{aN(C) : a \in G\}| = |\{aCa^{-1} : a \in G\}|$. Arguing similarly, we get $|\{aN(C) : a \in K\}| = |\{aCa^{-1} : a \in K\}|$, so $|[C]| = [N : K]$ and thus $|[C]| \mid |K|$, and so $|[C]| = p^r$ for some $0 \leq r < s$.

Going back now to the equivalence classes of conjugates of K, we showed in Proposition 2.3 that the elements of X are in fact themselves p-Sylow subgroups as they are conjugates of a p-Sylow subgroup. Using Lemma 3.4 we see that for $|[C]| = 1$ we have that $\forall a \in K, aCa^{-1} = C$, but then $a \in N(C)$ and $\text{ord}(a) = p^i$ for some $i \in \mathbf{N}$ thus $aCa^{-1} = C \Rightarrow a \in C$ which then means $C = K$ by Lemma 3.5. Therefore, the only equivalence class of size 1 is $[K]$. Now, because all other equivalence classes have size a power of p, then $|X| = 1 + tp$ where $t \in \mathbf{Z}$. Thus, for N the normalizer of K, $[G : N] = |X| = 1+tp \neq lp$ for any $l \in \mathbf{Z}$. By Corollary 3.6, we know that $p \nmid [N : K]$, and so $[G : K]$ is not a multiple of p, as $[G : K] = [G : N][N : K]$ and since neither is a multiple of p their product can't be. Therefore since $p^k m = |G| = |K|[G : K]$, $p^k \mid |K|$, and $|K| \mid p^k$, so we conclude that for a group G with $|G| = mp^k$, $m \in \mathbf{N}$, $\gcd(p, m) = 1$, that every p-Sylow subgroup K of G has order p^k. Combining this with the Lemma 3.3 we have that K has a subgroup of order p^n for all $n < k$, and because $K \subseteq G$ these are subsets of G. □

Remark 4.2. We showed in this proof that $|X| = 1 + tp$ where $t \in \mathbf{Z}$, and we recall from Corollary 2.18 that $|X| \mid |G|$, two results to keep in mind for later theorems.

The Proofs for the Second and Third Sylow Theorems are based on proofs from [?].

Theorem 4.3. ***[2nd Sylow Theorem]*** *If P and K are both p-Sylow subgroups of the group G, then there exists $x \in G$ such that $K = xPx^{-1}$.*

Proof. Let $|G| = mp^n$ with $\gcd(p, m) = 1$, and let $A = \{aP : a \in G\}$ be the set of all left cosets of P in G and have K act on A by left multiplication, $(k, aP) \to (kaP)$.

Since $|A| = [G : P]$, or $|A| = \dfrac{|G|}{|P|}$, and because P is a P-Sylow subgroup of G, we know by the 1st Sylow Theorem that $|P| = p^n$, so $p \nmid |A|$. Let A_f be the fixed subset of A as defined in Definition 2.10, using K acting on A. Denote the distinct stabilizers of elements of A by $K_{a_1}, \ldots, K_{a_m}$. Using Corollary 2.12, we know that $|A| = |A_f| + \sum_{i=1}^{m}[K : K_{a_i}]$ which we can rearrange as $\sum_{i=1}^{m}[K : K_{a_i}] = |A| - |A_f|$. Since K is a p-group, and each of the K_a are subgroups of K, we know that each of the $[K : K_{a_i}]$ is a multiple of p, thus $p \mid \sum_{i=1}^{m}[K : K_{a_i}]$ so $p \mid (|A| - |A_f|)$. Because $p \mid (|A| - |A_f|)$ and $p \nmid |A|$, we then know $p \nmid |A_f|$, and specifically $|A_f|$ is non-empty. Since A_f is non-empty, there is an element $aP \in A_f$ for some $a \in G$. As such, since $aP \in A_f$ we have that $(ka)P = k(aP) = aP$, $\forall k \in K$, and it follows that $a^{-1}ka \in P$, $\forall k \in K$ and thus $K \subseteq aPa^{-1}$. Since $|K| = |aPa^{-1}|$ it follows that $K = aPa^{-1}$ for some $a \in A$. □

Theorem 4.4. ***[3rd Sylow Theorem]*** *The number of p-Sylow subgroups of a finite group G divides $|G|$ and is of the form $1 + kp$ for some $k \in \mathbf{N}$*

Proof. Let K be a p-Sylow subgroup of G. In the proof of the 1st Sylow Theorem, we showed that the set of all conjugates of K, named X, had size $|X| = 1 + kp$ for some non-negative k, and from corollary 2.18 we have $|X| \mid |G|$.(Remark 4.2) The 2nd Sylow Theorem says that all p-Sylow subgroups of G are conjugates of each other, so X is in fact a collection of all the p-Sylow subgroups of G, so we are done. □

5. Classification of Finite Abelian Groups

We now turn to the issue of classification. Our goal is to give the reader a sketch of the picture of the classification of abelian groups and to go into more detail for non-abelian groups. Therefore, in this section many of the proofs are largely based on work from Chapter 8 of Thomas W. Hungerford's *Abstract Algebra, and Introduction: Second Edition*[**?**] which the reader may consult for more details.

We will take $\mathbf{Z}_n = \{0, 1, \ldots, (n-1)\} \cong \mathbf{Z}/n\mathbf{Z}$ for the remainder of this thesis.

Theorem 5.1. *Let G be a cyclic group of order n, then $G \cong \mathbf{Z}_n$.*

Proof. Take $a \in G$ such that $a \neq e$. Now, because G is cyclic, G can be written as $G = \{a^n : 0 \leq n < \text{ord}(a)\}$ where the operation on G is defined by $a^i a^j = a^{i+j \mod (n)}$. Here then, we can define a function $f : \mathbf{Z}_n \to G$ to be $f(i) = a^i$. We see that f is well defined, as $f(t) = f(r)$ implies $a^r = a^t$ which implies that $r \equiv t \mod (n)$ and since we are dealing with $\mathbf{Z}_n$ we know that $r \equiv t \mod (n)$ implies $r = t$ so f is well defined. It is not difficult to see that f as we've defined it is a bijection, since for $g \in G$ we know that $g = a^k$ for some $k < n$ and we see $f(k) = g$ so f is onto, and since $f^{-1}\{(e)\} = \{0\}$ we see $\ker(f) = \{0\}$ which will imply that f is 1-1 once we show it is a homomorphism. To that end, we know that if $z \in \mathbf{Z}_n$ such that $x + y \cong z \mod (n)$, then we have $f(x + y) = f(z) = a^z = a^{x+y} = a^x a^y = f(x)f(y)$ as desired. Therefore f is an homomorphism and a bijection and thus is an isomorphism. Thus $G \cong \mathbf{Z}_n$, as desired. □

Corollary 5.2. *Let p be a prime and let G be a group of order p. Then $G \cong \mathbf{Z}_p$.*

Proof. Take $a \in G$ such that $a \neq e$. We can then construct the cyclic subgroup generated by a, $\langle a \rangle$, where $|\langle a \rangle| \neq 1$. Since by Lagrange's Theorem, $|\langle a \rangle| \mid |G|$, that is $|\langle a \rangle| \mid p$, but since p is prime, we know that $|\langle a \rangle| = p$, so $\langle a \rangle = G$, and so G is cyclic. Using Theorem 5.1 we are done. □

Definition 5.3. For groups $G_1, G_2, \ldots, G_n$, we define a coordinate-wise operation on the Cartesian Product $G_1 \times G_2 \times \cdots \times G_n$ called the *direct product* by:

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

Proposition 5.4. *Let $G_1, G_2, \ldots, G_n$ be groups. Then their Cartesian Product, $G_1 \times G_2 \times \cdots \times G_n$ is a group with the operation defined above.*

Proof. For e_i the identity element of G_i, $1 \leq i \leq n$, we see that $(e_1, e_2, \ldots, e_n)$ is the identity of $G_1 \times G_2 \times \cdots \times G_n$. Also, it is easy to see that $({a_1}^{-1}, {a_2}^{-1}, \ldots, {a_n}^{-1})$

is the inverse of $(a_1, a_2, \ldots, a_n)$. Lastly, by definition of the direct product, we see that if $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in G_1 \times G_2 \times \cdots \times G_n$ then we see that $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$ and since each $a_ib_i \in G_i$ we have that $(a_1b_1, a_2b_2, \ldots, a_nb_n) \in G_1 \times G_2 \times \cdots \times G_n$. Thus $G_1 \times G_2 \times \cdots \times G_n$ is a group. □

Definition 5.5. Let G_i, $1 \leq i \leq n$, be groups with operation $+$. Then the G_i are said to be additive and we call the direct product of $G_1, G_2, \ldots, G_n$ the *direct sum*, denoted:

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n$$

In the rest of Section 5, all groups will be written using additive notation.

Definition 5.6. For a group G and prime p, the set denoted *G(p)* is the set of elements in G which have order a power of p, i.e.:

$$G(p) = \{a \in G : \text{ord}(a) = p^n, \text{ for some } n \geq 0\}$$

Note: It is easy to see that $G(p)$ is a subgroup of G.

Lemma 5.7. *Let G be a group, $a \in G$. If $p_1, p_2, \ldots, p_k$ are the distinct primes that divide the order of a, then, $a = a_1 + a_2 + \cdots + a_k$ with $a_i \in G(p_i)$.*

Proof. Here we will use induction on the number of primes dividing $\text{ord}(a)$. If $\text{ord}(a)$ is only divisible by one prime p_1, then $a \in G(p_1)$, and the lemma holds. Now we assume that the result is true for all elements with order having $k-1$ or fewer distinct prime factors, and then assume $\text{ord}(a)$ is divisible by $p_1, p_2, \ldots, p_k$. This means, $\text{ord}(a) = {p_1}^{r_1}{p_2}^{r_2} \cdots {p_k}^{r_k}$ for some $r_1, r_2, \ldots, r_k \in \mathbf{N}$. Let $m = {p_2}^{r_2} \cdots {p_k}^{r_k}$, and $n = {p_1}^{r_1}$, so that we have $|a| = nm$ where $\gcd(n, m) = 1$. Because $\gcd(n, m) = 1$, it follows that there exist some $u, v \in \mathbf{Z}$ such that $1 = nu + mv$, and thus $a = 1a = (nu + mv)a = nua + mva$. Furthermore, $mva \in G(p_1)$ as $p_1(mva) = n(mva) = (nm)va = v(nma) = v0 = 0$. Similarly, $m(nua) = 0$, so it follows that $\text{ord}(nua)$ |

m. As m is an integer with only $k-1$ distinct prime divisors, we know by the inductive hypothesis that $nua = a_2 + \cdots + a_k$ for $a_i \in G(p_i)$. Let $a_1 = mva$, then $a = mva + nua = a_1 + a_2 + \cdots + a_k$ for $a_i \in G(p_i)$ as desired. □

We will use the previous lemma to prove that much more can be said about the primes dividing the order of a group.

Theorem 5.8. *Let G be a group, and let $p_1, p_2, \ldots, p_n$ be the distinct primes that divide the order of G. Then, G is isomorphic to the direct sum of the $G(p_i)$, i.e.:*

$$G \cong G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_n)$$

Proof. Let a be an element of G. By the previous lemma, we know that we can represent a as $a = a_1 + a_2 + \cdots + a_n$ for $a_i \in G(p_i)$, with $a_j = 0$ for $p_j \nmid \text{ord}(a)$, and $(a_1, a_2, \ldots, a_n) \in G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_n)$. According to Theorem 8.1 in [**?**], to prove $G \cong G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_n)$, we need this representation to be unique.

Assume for contradiction that this representation is not unique. In other words assume there are two elements of $G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_n)$, call them $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$, such that $x_1 + x_2 + \cdots + x_n = a = y_1 + y_2 + \cdots + y_n$. Because G is abelian, we can rearrange this to get $x_1 - y_1 = (y_2 - x_2) + \cdots + (y_n - x_n)$. Now, since each of the $G(p_i)$ is a subgroup of G, we know that for every i, $(x_i - y_i) \in G(p_i)$, so specifically $\text{ord}(x_i - y_i)$ is some power of p_i, call this ${p_i}^{k_i}$. Now, let $m = {p_2}^{k_2} \cdots {p_n}^{k_n}$. Multiplying both sides of the equation by m from the left we get $m(x_1 - y_1) = m(y_2 - x_2) + \cdots + m(y_n - x_n) = 0 + \cdots + 0 = 0$. Thus we have that $m(x_1 - y_1) = 0$ which means that $\text{ord}(x_1 - y_1) \mid m$. Since $\text{ord}(x_1 - y_1)$ is a power of p_1, and the only power of p_1 which divides m is ${p_1}^0 = 1$, we see that $(x_1 - y_1) = 0$, or $x_1 = y_1$. This argument can be repeated for each i to show that $x_i = y_i$ for $1 \leq i \leq n$, therefore $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$. Thus, a is uniquely represented by $x_1 + x_2 + \cdots + x_n$ for $x_i \in G(p_i)$, as desired. □

We now state a final result useful for the proof of **The Fundamental Theorem of Finite Abelian Groups**.

Lemma 5.9. *Let G be a p-group and a an element of maximal order in G. Then there is a subgroup K of G such that $G = \langle a \rangle \oplus K$.*

Proof. For a proof of the lemma, see [**?**] page 255, lemma 8.6. □

Using these definitions and theorems, we will now state and prove **The Fundamental Theorem of Finite Abelian Groups**. The corollaries and other theorems related to this result will form the basis for the classification of all finite abelian groups.

Theorem 5.10. ***[The Fundamental Theorem of Finite Abelian Groups]*** *Every finite abelian group G is a direct sum of cyclic groups, each of prime power order.*

Proof. By Theorem 5.6, $G = G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_n)$ where $p_1, \ldots, p_n$ are the primes dividing $\text{ord}(a)$. We know each $G(p_k)$ is a p-group, so we need only show that each p-group P is a direct sum of cyclic groups of order a power of p. We will prove this by induction on the order of P. This is trivially true for $|P| = p$ by Corollary 5.2. Now assume this is true for all p-groups of order less than $|P|$, and let $a \in P$ be an element of maximal order. Then, $P = \langle a \rangle \oplus K$ for some $K \subseteq P$ by the previous Lemma. Since we know by induction that K is a direct sum of cyclic groups each of order a power of p, then so too is P, and so we have that G is a direct sum of cyclic groups. □

Using Theorem 5.9 we can now construct, up to isomorphism, all of the abelian groups of order less than 15. We shall further refine this list in the rest of this section.

Order	Groups
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_2 \oplus \mathbf{Z}_3$
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \oplus \mathbf{Z}_3$
10	$\mathbf{Z}_2 \oplus \mathbf{Z}_5$
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$, $\mathbf{Z}_3 \oplus \mathbf{Z}_4$
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_2 \oplus \mathbf{Z}_7$
15	$\mathbf{Z}_3 \oplus \mathbf{Z}_5$

While it may not be obvious to the reader that this is in fact a complete list, the next example should rectify that.

Example 5.11. Up to the order of the primes, 12 can be represented exactly 2 ways as a product of powers of primes, namely $2 * 2 * 3$ and $4 * 3$.

To see this note that the prime factorization of 12 is $2 * 2 * 3$. We can write this as a product of powers of primes as $2 * 2 * 3 = 2^1 * 2^1 * 3^1$ or $2 * 2 * 3 = 2^2 * 3^1$. Since there are no other primes which divide 12, by the Fundamental Theorem of Arithmetic, we cannot represent 12 by any other products of powers of primes so we see there are only 2. Now, since $2^2 = 4$ we can simplify the second representation to $4 * 3^1$, and we see that the two representation are then $2 * 2 * 3$ and $4 * 3$ as desired.

Some of the groups on this list appear rather unwieldy and as such will be renamed using the next lemma.

Lemma 5.12. *If* $\gcd(m, k) = 1$, *then* $\mathbf{Z}_m \oplus \mathbf{Z}_k \cong \mathbf{Z}_{mk}$.

Proof. Take the element $(1, 1)$ which we know to be in $\mathbf{Z}_m \oplus \mathbf{Z}_k$. The order of $(1, 1)$ in $\mathbf{Z}_m \oplus \mathbf{Z}_k$ is the smallest $t \in \mathbf{Z}$ such that $t(1, 1) = (0, 0)$. We know $t(1, 1) = (t, t)$ so for this to be equal to $(0, 0)$ we have $t \equiv 0 \mod (m)$ and $t \equiv 0 \mod (k)$. With this we have that $m|t$ and $k|t$, which then becomes $mk|t$ because $\gcd(m, k) = 1$, and so

$mk \leq t$. Since we know $mk(1,1) = (0,0)$ and because t was defined as the smallest such integer, then $t = mk$. Thus, $\mathbf{Z}_m \oplus \mathbf{Z}_k$ is a cyclic group of order mk, and by Theorem 5.1 then we see that $\mathbf{Z}_m \oplus \mathbf{Z}_k \cong \mathbf{Z}_{mk}$ as desired. □

We can rewrite the table now to get:

Order	Groups
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \oplus \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_{12}$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_{14}$
15	$\mathbf{Z}_{15}$

While this list is certainly complete, as it contains all the possible abelian groups of order up to 15, we need to show that no two groups here are isomorphic. To show this we first need to expand on the previous lemma.

Theorem 5.13. *If $n = {p_1}^{n_1}{p_2}^{n_2}\cdots{p_t}^{n_t}$ where $p_1, p_2, \ldots, p_t$ are distinct primes, then $\mathbf{Z}_n \cong \mathbf{Z}_{{p_1}^{n_1}} \oplus \mathbf{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{{p_t}^{n_t}}$.*

Proof. We will use induction on the number of distinct summands. First, by lemma 5.12 the theorem is clearly true for all groups with 2 summands. We then assume for induction that it's true of all groups with fewer than n summands. Take $m = {p_1}^{n_1}$ and $k = {p_2}^{n_2}\cdots{p_t}^{n_t}$ and using Lemma 5.12 we get $\mathbf{Z}_n \cong \mathbf{Z}_m \oplus \mathbf{Z}_k$, and the inductive hypothesis shows that $\mathbf{Z}_k \cong \mathbf{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{{p_t}^{n_t}}$. □

The last thing we need to do in this section is to show that our list in in fact complete for abelian groups of order up to 15. This will be accomplished with the help of the following lemmas and a final theorem.

Lemma 5.14. *Let G be a p-group and define pG as $pG = \{px : x \in G\}$. Then pG is a subgroup of G.*

Proof. We see that $p0 = 0$, since $0+0+\cdots+0 = 0$, $0 \in pG$. If $pa \in pG$ for some $a \in G$ then $p(-a) \in pG$ and we see that $pa+p(-a) = p(a+-a) = 0 = p(-a+a) = p(-a)+pa$ thus $p(-a) = (-pa)$ so pG contains arbitrary inverses. Last, if $pa, pb \in G$ for some $a, b \in G$, we see that $pa + pb = p(a + b)$ and since G is a group $a + b \in G$ so $p(a + b) \in pG$ and thus pG is closed under its operation, so is a group. □

Lemma 5.15. *Let G be a group. If $G \cong C_1 \oplus C_2 \oplus \cdots \oplus C_n$ for some groups $C_1, \ldots, C_n$, then $pG \cong pC_1 \oplus pC_2 \oplus \cdots \oplus pC_n$.*

Proof. Since $G \cong C_1 \oplus C_2 \oplus \cdots \oplus C_n$, $\forall a \in G$ the exists unique $(a_1, \ldots, a_n) \in C_1 \oplus C_2 \oplus \cdots \oplus C_n$ such that $a = (a_1, \ldots, a_n)$, defined by an isomorphism $f : G \to C_1 \oplus C_2 \oplus \cdots \oplus C_n$ such that $f(a) = (a_1, \ldots, a_n)$. Now define $f_p : pG \to pC_1 \oplus pC_2 \oplus \cdots \oplus pC_n$ by $f_p(pa) = (pa_1, \ldots, pa_n)$. First, note that $f_p(pa) = p(f(a))$ since $f_p(pa) = (pa_1, \ldots, pa_n) = p(a_1, \ldots, a_n) = p(f(a))$, and since f is an isomorphism, this implies f_p is a well defined homomorphism. Now, take $pa, pb \in pG$, $pa \neq pb$. If $f_p(pa) = (pa_1, \ldots, pa_n) = f_p(pb)$ for some $pa_i \in pC_i$, then we get that $f_p(pa) = p(a_1, \ldots, a_n) = p(f(a))$ and $f_p(pb) = p(a_1, \ldots, a_n) = p(f(b))$ which implies $p(f(a)) = p(f(b)) \Rightarrow f(a) = f(b)$, which implies $a = b$ which contradicts $pa \neq pb$ so f_p is injective. To see f_p is surjective, take an arbitrary element of $pC_1 \oplus pC_2 \oplus \cdots \oplus pC_n$ call it $(pc_1, \ldots, pc_n)$. Since f is surjective we know there exists $c \in G$ such that $f(c) = (c_1, \ldots, c_n)$. Now, we've previously noted that $f_p(pa) = p(f(a))$, so in particular $p(f(c)) = f_p(pc)$, and since $f_p(pc) = p(f(c)) = p(c_1, \ldots, c_n) = (pc_1, \ldots, pc_n)$ we see that $f_p(pc) = (pc_1, \ldots, pc_n)$, and so f_p is surjective. As f_p is both injective and surjective it is a bijection and thus $pG \cong pC_1 \oplus pC_2 \oplus \cdots \oplus pC_n$ as desired. □

One last definition will be needed to show that our list contains no isomorphic groups.

Definition 5.16. When a group G is written as a direct sum of cyclic groups of prime power orders, as in Theorem 5.10, the prime powers are called the *elementary divisors* of G.

Theorem 5.17. *Let G and H be abelian groups, then $G \cong H$ if and only if they have the same elementary divisors.*

Proof. $\Leftarrow$: If G and H have the same elementary divisors, then they can both be written as a direct sum of cyclic groups of the same prime power orders, and thus are isomorphic to each other.

$\Rightarrow$ If $G \cong H$ then we know there is some isomorphism $f : G \to H$, and that $\text{ord}(f(a)) = \text{ord}(a)$ for all $a \in G$. Look at the subgroup $G(p)$ where $p \mid |G|$ and p is prime. Each element $a \in G(p)$ has order a power of p, so $f(a) = b$ implies that the order of b is a power of p, so then $b \in H(p)$, and it follows that $f(G(p)) \subseteq H(p)$, and similarly the inverse function shows $f^{-1}(H(p)) \subseteq G(p)$, which implies $G(p) \cong H(p)$. Because the elementary divisors of G that are powers of p are merely the elementary divisors of $G(p)$ all we need to show is that the claim is true of p-groups.

Let $|G| = p^n$ for some prime p and $n \in \mathbf{N}$. We will use induction on the order of G to show this is true for all p-groups. All groups of order p have the same elementary divisor p, and nothing else, so the claim is obviously true in this case. Now assume for induction that the claim is true for all groups of order less than $|G|$, and let the elementary divisors of G be $p^{n_1}, p^{n_2}, \ldots, p^{n_k}, p^u$ where p^u represents all the elementary divisors of the form p^1, and $n_1 \geq n_2 \geq \cdots \geq n_k > 1$. We can similarly define the elementary divisors of H as $p^{m_1}, p^{m_2}, \ldots, p^{m_r}, p^v$ where again, p^v represents all the elementary divisors of the form p^1, and $m_1 \geq m_2 \geq \cdots \geq m_r > 1$. We know that $pG = \{px : x \in G\}$ is a subgroup of G by Lemma 5.14. Since G is the direct sum of cyclic groups, choose an arbitrary one, say C_i. We see by Lemma 5.15 that pG is a direct sum of cyclic groups of the form pC_i, and we see that for $|C_i| = p^t$, $|pC_i| = p^{t-1}$. This follows since C_i is cyclic there is an element $a \in C_i$ such that a is a generator for

C_i, thus $\text{ord}(a) = p^t$, then $\text{ord}(pa) = p^{t-1}$ and pa is a generator of pC_i, so $|pC_i| = p^{t-1}$. Since the C_i's correspond to the elementary divisors, we have that the orders of the C_i's are the elementary divisors. For the cases of $|C_j| = p$ (all the p^u and p^v) we have that $|pC_j| = 1$, thus no longer an elementary divisor of pG, so the elementary divisors of pG are: $p^{n_1-1}, p^{n_2-1}, \ldots, p^{n_k-1}$. We can do the same thing with pH to get its elementary divisors: $p^{m_1-1}, p^{m_2-1}, \ldots, p^{m_r-1}$.

Since f is an isomorphism it follows that $pG \cong pH$ by defining $f_p : pG \to pH$ as $f_p(pg) = p(f(g))$. Showing this is an isomorphism is similar to the work in the proof of Lemma 5.15 and will therefore be left as an exercise for the reader. Furthermore, since $|pG| < |G|$ we know by the inductive hypothesis that pG and pH have the same elementary divisors, and that $k = r$. Thus we know that $p^{n_i-1} = p^{m_i-1} \Rightarrow n_i - 1 = m_i - 1$ which implies $n_i = m_i$ for all $1 \leq i \leq k$. Therefore, the only possible difference in the elementary divisors of G and H come in the number of p's with power 1, that is the size of u and v from the p^u, p^v above. Since $G \cong H$ we know $|G| = |H|$ which is $p^{n_1}p^{n_2} \cdots p^{n_k}p^u = p^{m_1}p^{m_2} \cdots p^{m_r}p^v$ and because $n_i = m_i$ for all $1 \leq i \leq k = r$ we can reduce this to $p^u = p^v$ which clearly shows that $u = v$ so G and H had the same number of p's with power 1, so they have the same elementary divisors, as desired. $\square$

Thus, our table from above has been shown to contain unique groups, and so it is in fact a complete list up to isomorphism of abelian groups of order less than or equal to 15.

6. Classification of Finite Non-Abelian Groups

Now that we've compiled a list of abelian groups of order less than or equal to 15, we need to add on any non-abelian groups of these sizes to complete the list. In this section we will prove results that do just that. These results will be of two different varieties, some which introduce new non-abelian groups to the table, and

others which restrict various non-abelian additions. Work in this section will revert back to working with multiplicative groups.

An example of the latter type of result can be seen in the following theorem, which states that no additional groups of order 4 or 9 need be added to our list.

Theorem 6.1. *If G is a group of order p^2 for some prime p, then G is abelian.*

Proof. By Lagrange's Theorem we know that $|\mathbf{Z}(G)| \mid |G|$, and by Remark 3.4 we see that $|\mathbf{Z}(G)|$ is a multiple of p, and so in this case we get $|\mathbf{Z}(G)| = p$ or $|\mathbf{Z}(G)| = p^2$. In the case that $|\mathbf{Z}(G)| = p^2$ then $|\mathbf{Z}(G)| = |G|$ so G is abelian. Otherwise, $|\mathbf{Z}(G)| = p$ and we can construct the quotient group $G/\mathbf{Z}(G)$. We see that this group has order p and by Corollary 5.2 $G/\mathbf{Z}(G) \cong \mathbf{Z}_p$ it is cyclic. Since $G/\mathbf{Z}(G)$ is cyclic, it has some generator $g\mathbf{Z}(G)$, where $g \in G$, and every coset in $G/\mathbf{Z}(G)$ is of the form $(g\mathbf{Z}(G))^k = g^k\mathbf{Z}(G)$ for some $k \in \mathbf{N}$. Let a, b be elements of G. Since $a \in g^i\mathbf{Z}(G)$ for some $i \in \mathbf{N} \cup \{0\}$ thus there exists some $c_1 \in \mathbf{Z}(G)$ such that $a = g^i c_1$. Similarly it follows that for $b \in g^j\mathbf{Z}(G)$ for some $j \in \mathbf{N}$ so there exists $c_2 \in \mathbf{Z}(G)$ such that $b = g^j c_2$. We know that $g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$, and c_1, c_2 commute with all element of G by definition, so $ab = g^i c_1 g^j c_2 = g^i g^j c_1 c_2 = g^j g^i c_2 c_1 = g^j c_2 g^i c_1 = ba$ so G is abelian, as desired. □

Next we will prove that there are no non-abelian groups of order 15. We begin this with the proof of a lemma about subgroups of a given group G from [**?**].

Lemma 6.2. *If H and K are subgroups of G, then HK denotes the subset $\{hk \in G : h \in H,\ k \in K\}$ of G and, $|HK| = \dfrac{|H||K|}{|H \cap K|}$.*

Proof. Note that HK is the union of distinct left cosets of K, $HK = \bigcup hK$. Since $\forall h \in H$, $|hK| = |K|$ so we need to find the number m, of distinct left cosets of the form hK, $h \in H$. Since $h_1K = h_2K$ if and only if $h_2^{-1}h_1 \in K$ it follows that $h_1K = h_2K$ if and only if $h_2^{-1}h_1 \in H \cap K$ if and only if $h_1(H \cap K) = h_2(H \cap K)$. We

see that m is the number of distinct cosets $h(H \cap K),\ \ h \in H$. Since $H \cap K \subseteq H$, we see $m = \dfrac{|H|}{|H \cap K|}$. Then, $|HK| = m|K| = \frac{|H||K|}{|H \cap K|}$ as desired. $\square$

Theorem 6.3. *Let G be a group of order pq where p, q are primes such that $p > q$ and $q \nmid (p-1)$. Then $G \cong \mathbf{Z}_{pq}$.*

Proof. By the **Third Sylow Theorem**, we know that the number of p-Sylow subgroups of G, call it x, must divide the order of G and be of the form $x = 1 + tp$ for some $t \in \mathbf{Z}$. In this case, there are only 4 possibilities for x since $|G| = pq$, which only has 4 divisors: $1, q, p, pq$. Since a p-Sylow subgroup K of G is a p-subgroup, and $|G| = pq$, we know that $K = p$. If $pq = 1 + tp$ for some $t \in \mathbf{Z}$, then $pq - tp = 1 \Rightarrow p(q - t) = 1$ which is a contradiction, so $x \neq pq$. If $p = 1 + tp$ for some $t \in \mathbf{Z}$ then $p - tp = 1 \Rightarrow p(1 - t) = 1$ which is a contradiction, so $x \neq p$. Thus there are either 1 or q p-Sylow subgroups of G, but because $1 < q < p$, $q \neq 1 + kp$ for any $k \in \mathbf{Z}$ clearly there is only 1 p-Sylow subgroups of G, namely K. Similarly we see that there is only 1 q-Sylow subgroup of G as pq and q can be eliminated as in the case of the p-Sylow subgroups, and we cannot have $p = 1 + tq$ since by our assumption $q \nmid (p-1)$. Call the q-Sylow subgroup H. Since $K \cap H$ is a subgroup of both K and H, by Lagrange's Theorem the only element they share is the identity, so $K \cap H = \{e\}$. We claim that K is a normal subgroup of G since K is the only p-Sylow subgroup of G. This follows from the **2nd Sylow Theorem** because $aKa^{-1} = K$ $\forall a \in G$, can be rearranged to be $aK = Ka$ $\forall a \in G$. Similarly H is also normal in G. Using the previous lemma we see that $|HK| = pq = |G|$, and since $HK \subseteq G$ this implies $HK \cong G$. We then observe that if $h_1k_1 = h_2k_2$ it follows that $h_2^{-1}h_1 = k_2k_1^{-1}$ which is $h_3 = k_3$ for some $h_3 \in H$, $k_3 \in K$. We know that $h_3 = k_3$ implies $h_3 = e$, $k_3 = e$ since $H \cap K = \{e\}$. This in turn implies $h_2^{-1}h_1 = e$, $k_2k_1^{-1} = e$ so $h_1 = h_2$ and $k_1 = k_2$, thus every element of G can be uniquely represented by a product of elements of H and K, so $G \cong H \times K$ by Theorem 8.1 from [**?**]. Since H, and K are

groups of prime order, they are cyclic by Corollary 5.2, and so $H \cong \mathbf{Z}_q$, $K \cong \mathbf{Z}_p$ thus $H \times K \cong \mathbf{Z}_q \times \mathbf{Z}_p \cong \mathbf{Z}_{pq}$ by Lemma 5.12 and we have $G \cong \mathbf{Z}_{pq}$ as desired. □

Now we will move on to adding non-abelian groups to our table. In what follows a number of different groups will be defined, all of which are non-abelian. We will also show that these defined groups are in fact not isomorphic to each other. After introducing these new groups, our last task will be to show the new list is complete. Since in many cases we shall be illustrating the distinctness of groups by the differences in their multiplication tables, we will use the following theorem.

Theorem 6.4. *A multiplication table for a group defines the group uniquely, that is any two groups with the same multiplication table are isomorphic to each other.*

Proof. For a proof and more details, the reader can consult [**?**] section 2.3, as well as [**?**] pages 19-20. □

The first family of non-abelian groups we will look at are called the *Dihedral Groups*. For geometric motivation for the *dihedral group of degree n*, denoted D_n please refer to [**?**] page 277. While the geometric definition is useful it does not provide a means of comparison to other groups. To rectify this we will use the next theorem from *Hungerford*, stated here for convenience.

Theorem 6.5. *The dihedral group D_n is a group of order $2n$, generated by elements r and d such that:*

$$|r| = n, \;\; |d| = 2, \;\; \text{and} \;\; rdr = d$$

Proof. For a proof see Theorem 8.32 in [**?**], pages 277-278. □

We can then update our table to include this new family of groups

Order	Groups
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$, D_3
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$, D_4
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \oplus \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$, D_5
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_{12}$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$, D_6
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_{14}$, D_7
15	$\mathbf{Z}_{15}$

We will now show that $D_3 \cong S_3$ by looking at their multiplication tables.

D_3**:**

x	e	r	r^2	d	dr	dr^2
e	e	r	r^2	d	dr	dr^2
r	r	r^2	e	dr^2	d	dr
r^2	r^2	e	r	dr	dr^2	d
d	d	dr	dr^2	e	r	r^2
dr	dr	dr^2	d	r^2	e	r
dr^2	dr^2	d	dr	r	r^2	e

We will now construct a table for S_3. To simplify the symbols, we will use the permutations of the group of order 3 as defined in [**?**] on page 71 and then rearrange the table from page 72 as follows:

S_3**:**

x	e	β	δ	α	γ	κ
e	e	β	δ	α	γ	κ
β	β	δ	e	κ	α	γ
δ	δ	e	β	γ	κ	α
α	α	γ	κ	e	β	δ
γ	γ	κ	α	δ	e	β
κ	κ	α	γ	β	δ	e

If we substitute r for β and d for α, the multiplication table constructed is exactly the same as that of D_3, thus our table of groups can be rewritten as:

Order	Groups
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$, S_3
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$, D_4
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \oplus \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$, D_5
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_{12}$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$, D_6
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_{14}$, D_7
15	$\mathbf{Z}_{15}$

We will now show that for orders 6, 10, and 14 our table is complete using the next theorem.

Theorem 6.6. *If G is a group of order $2p$ where p is an odd prime, then $G \cong \mathbf{Z}_{2p}$ or $G \cong D_p$.*

Proof. By Cauchy's Theorem, G contains elements a, b such that $\text{ord}(a) = p$, $\text{ord}(b) = 2$. Note that for $\text{ord}(b) = 2$, $b^2 = e$ which implies $b = b^{-1}$. Let H be the cyclic group generated by a, $H = \langle a \rangle$, and note that $|H| = p$. Because $|G| = 2p$, we know that $[G : H] = 2$ and H is normal in G. It follows that $bab = bab^{-1} \in H$, as H is closed with respect to conjugation. Now, since H is cyclic, we know that $bab = a^t$ for some $t \in \mathbf{Z}$, and using $b^2 = e$ we see that:

$$a^{t^2} = (a^t)^t = (bab)^t = (bab)(bab)(bab)\cdots(bab) = ba^tb = b(bab)b = a$$

Thus, $t^2 \equiv 1 \mod (p)$, which means $p \mid (t^2 - 1)$ so $p \mid (t-1)(t+1)$. Since p is prime, and $(t-1)$ and $(t+1)$ cannot possibly both be divisible by $p > 2$, we know that either $p \mid (t-1)$ or $p \mid (t+1)$. Therefore, either $t \equiv 1 \mod (p)$ or $t \equiv -1 \mod (p)$.

If $t \equiv 1 \mod (p)$, then we have that $bab = a^t = a$. Multiplying both sides by b^{-1} on the left we have $ab = b^{-1}a$ Since $b^{-1} = b$, this becomes $ab = ba$, and so G is

abelian, and we have previously shown in lemma 5.12 that any abelian group of order $2p$ is isomorphic to $\mathbf{Z}_{2p}$.

If $t \equiv -1 \mod (p)$, then $bab = a^t = a^{-1}$, this means $baba = e$ so $aba = b$. Notice that this group is defined by $\text{ord}(a) = p$, $\text{ord}(b) = 2$, and $aba = b$. We know D_p is defined by $\text{ord}(r) = p$, $\text{ord}(d) = 2$, and $rdr = d$, so using these definitions to construct multiplication tables, we construct the same table, and so by theorem 6.5 we get that $G \cong D_p$ as desired. □

We will now introduce another family of non-abelian groups for our table, the dicyclic groups.

Definition 6.7. If $n = 2m$ for some $m \geq 1$, we define the *dicyclic group* Q_n as the group of order $2n$ generated by two elements a, b as follows:

$$Q_n = \{e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$$

where $\text{ord}(a) = n$, $aba = b$ and $b^2 = a^m$.

For our table, the only relevant dicyclic groups are Q_2, Q_4, and Q_6, as all others have higher order than 15. We know from Theorem 6.1 that since $|Q_2| = 4$, Q_2 is abelian, so is already isomorphic to a group on the list. This just leaves Q_4 and Q_6. The multiplication tables for Q_4 and D_4 will be displayed here to illustrate their differences and prove that they are groups.

Q_4**:**

x	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

D_4**:**

x	e	r	r^2	r^3	d	dr	dr^2	dr^3
e	e	r	r^2	r^3	d	dr	dr^2	dr^3
r	r	r^2	r^3	e	dr^3	d	dr	dr^2
r^2	r^2	r^3	e	r	dr^2	dr^3	d	dr
r^3	r^3	e	r	r^2	dr	dr^2	dr^3	d
d	d	dr	dr^2	dr^3	e	r	r^2	r^3
dr	dr	dr^2	dr^3	d	r^3	e	r	r^2
dr^2	dr^2	dr^3	d	dr	r^2	r^3	e	r
dr^3	dr^3	d	dr	dr^2	r	r^2	r^3	e

Clearly $D_4 \neq Q_4$ as D_4 has many more elements of order 2 (represented by e's on the diagonal), and the same can be seen for D_6 and Q_6. To reflect these additions, our table from before shall be updated as follows:

Order	Groups
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$, S_3
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$, D_4, Q_4
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \oplus \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$, D_5
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_{12}$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$, D_6, Q_6
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_{14}$, D_7
15	$\mathbf{Z}_{15}$

We will now show that our list for order 8 is in fact complete.

Theorem 6.8. *If G is a non-abelian group where $|G| = 8$ then G is isomorphic to either D_4 or Q_4.*

Proof. The non-identity elements of G must have orders 2, 4, or 8. Since G is non-abelian and therefore non-cyclic, no element of G has order 8. If every non-identity element of G had order 2, then G would be abelian, as for $g_1, g_2 \in G$, $\text{ord}(g_1) = \text{ord}(g_2) = \text{ord}(g_1 g_2) = 2$, and so $g_1 g_2 g_1 g_2 = e$ which implies $g_2 g_1 = g_1 g_2$. Thus, there exists some $a \in G$, $a \neq e$ such that $\text{ord}(a) = 4$. Let K be the cyclic-subgroup of G generated by a, i.e. $K = \langle a \rangle$. If $b \notin K$ then $G = K \cup bK$ since $[G : K] = 2$ and we claim that $aba = b$. We know $bab^{-1} \in K$ as $[G : K] = 2$ so K is normal and therefore

closed under conjugacy. Since $\text{ord}(bab^{-1}) = \text{ord}(a) = 4$, and because G isn't abelian $bab^{-1} \neq a$, thus $bab^{-1} = a^{-1}$, which can be rewritten as $aba = b$. Now there are two possibilities for the order of b, either $\text{ord}(b) = 2$ or $\text{ord}(b) = 4$. If $\text{ord}(b) = 2$ for some $b \notin K$, then $G \cong D_4$ by Theorem 6.5. Else, $\text{ord}(b) = 4\ \forall b \notin K$, and so a^2 is the only element of order 2, and since $\text{ord}(b^2) = 2$, we get $b^2 = a^2$ for all $b \notin K$. Thus for a given $b \in \langle a \rangle$ G is generated by a and b with $\text{ord}(a) = 4$, $aba = b$, and $b^2 = a^2$. It follows that $G \cong Q_4$ by Theorem 6.7. □

The last group to be added to our table is A_4, the alternating group of degree 4. Since $A_3 \cong S_3$ it is therefore already included in our table. Recall that $|A_n| = n!/2$, which is in this case $|A_4| = 4!/2 = 12$. We also know that A_4 is the unique subgroup of S_4 whose order is 12, as seen in [**?**], Theorem 7.51. We will construct the multiplication tables for A_4, D_6, and Q_6 to see that no two of these are isomorphic. We will first construct A_4 using the following notation:

$$\alpha = (1,2), \beta = (1,3), \gamma = (1,4), \delta = (2,3), \varphi = (2,4), \kappa = (3,4)$$

Using these we can construct A_4 as:

$$A_4 = \{e, \alpha\beta, \beta\alpha, \alpha\varphi, \varphi\alpha, \alpha\kappa, \beta\varphi, \beta\kappa, \kappa\beta, \gamma\delta, \varphi\delta, \delta\varphi\}$$

After constructing the multiplication table for A_4 we will use it to verify that no two elements are repeated in this listing. We know that if any two elements are the same then the multiplication table will have two identical rows, which we shall see is in fact not the case, thus A_4 is well defined.

A_4:

x	e	$\alpha\beta$	$\beta\alpha$	$\alpha\varphi$	$\varphi\alpha$	$\alpha\kappa$	$\beta\varphi$	$\beta\kappa$	$\kappa\beta$	$\gamma\delta$	$\varphi\delta$	$\delta\varphi$
e	e	$\alpha\beta$	$\beta\alpha$	$\alpha\varphi$	$\varphi\alpha$	$\alpha\kappa$	$\beta\varphi$	$\beta\kappa$	$\kappa\beta$	$\gamma\delta$	$\varphi\delta$	$\delta\varphi$
$\alpha\beta$	$\alpha\beta$	$\beta\alpha$	e	$\delta\varphi$	$\gamma\delta$	$\varphi\delta$	$\alpha\varphi$	$\alpha\kappa$	$\varphi\alpha$	$\kappa\beta$	$\beta\kappa$	$\beta\varphi$
$\beta\alpha$	$\beta\alpha$	e	$\alpha\beta$	$\beta\varphi$	$\kappa\beta$	$\beta\kappa$	$\delta\varphi$	$\varphi\delta$	$\gamma\delta$	$\varphi\alpha$	$\alpha\kappa$	$\alpha\varphi$
$\alpha\varphi$	$\alpha\varphi$	$\beta\kappa$	$\gamma\delta$	$\varphi\alpha$	e	$\kappa\beta$	$\alpha\beta$	$\beta\varphi$	$\delta\varphi$	$\varphi\delta$	$\beta\alpha$	$\alpha\kappa$
$\varphi\alpha$	$\varphi\alpha$	$\beta\varphi$	$\varphi\delta$	e	$\alpha\varphi$	$\delta\varphi$	$\beta\kappa$	$\alpha\beta$	$\alpha\kappa$	$\beta\alpha$	$\gamma\delta$	$\kappa\beta$
$\alpha\kappa$	$\alpha\kappa$	$\kappa\beta$	$\delta\varphi$	$\varphi\delta$	$\beta\kappa$	e	$\gamma\delta$	$\varphi\alpha$	$\alpha\beta$	$\beta\varphi$	$\alpha\varphi$	$\beta\alpha$
$\beta\varphi$	$\beta\varphi$	$\varphi\delta$	$\varphi\alpha$	$\kappa\beta$	$\beta\alpha$	$\gamma\delta$	e	$\delta\varphi$	$\alpha\varphi$	$\alpha\kappa$	$\alpha\beta$	$\beta\kappa$
$\beta\kappa$	$\beta\kappa$	$\gamma\delta$	$\alpha\varphi$	$\alpha\kappa$	$\varphi\delta$	$\beta\alpha$	$\varphi\alpha$	$\kappa\beta$	e	$\delta\varphi$	$\beta\varphi$	$\alpha\beta$
$\kappa\beta$	$\kappa\beta$	$\delta\varphi$	$\alpha\kappa$	$\beta\alpha$	$\beta\varphi$	$\alpha\varphi$	$\varphi\delta$	e	$\beta\kappa$	$\alpha\beta$	$\varphi\alpha$	$\gamma\delta$
$\gamma\delta$	$\gamma\delta$	$\alpha\varphi$	$\beta\kappa$	$\alpha\beta$	$\delta\varphi$	$\beta\varphi$	$\alpha\kappa$	$\beta\alpha$	$\varphi\delta$	e	$\kappa\beta$	$\varphi\alpha$
$\varphi\delta$	$\varphi\delta$	$\varphi\alpha$	$\beta\varphi$	$\beta\kappa$	$\alpha\kappa$	$\alpha\beta$	$\kappa\beta$	$\gamma\delta$	$\beta\alpha$	$\alpha\varphi$	$\delta\varphi$	e
$\delta\varphi$	$\delta\varphi$	$\alpha\kappa$	$\kappa\beta$	$\gamma\delta$	$\alpha\beta$	$\varphi\alpha$	$\beta\alpha$	$\alpha\varphi$	$\beta\varphi$	$\beta\kappa$	e	$\varphi\delta$

Q_6:

x	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
e	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
a	a	a^2	a^3	a^4	a^5	e	ba^5	b	ba	ba^2	ba^3	ba^4
a^2	a^2	a^3	a^4	a^5	e	a	ba^4	ba^5	b	ba	ba^2	ba^3
a^3	a^3	a^4	a^5	e	a	a^2	ba^3	ba^4	ba^5	b	ba	ba^2
a^4	a^4	a^5	e	a	a^2	a^3	ba^2	ba^3	ba^4	ba^5	b	ba
a^5	a^5	e	a	a^2	a^3	a^4	ba	ba^2	ba^3	ba^4	ba^5	b
b	b	ba	ba^2	ba^3	ba^4	ba^5	a^3	a^4	a^5	e	a	a^2
ba	ba	ba^2	ba^3	ba^4	ba^5	b	a^2	a^3	a^4	a^5	e	a
ba^2	ba^2	ba^3	ba^4	ba^5	b	ba	a	a^2	a^3	a^4	a^5	e
ba^3	ba^3	ba^4	ba^5	b	ba	ba^2	e	a	a^2	a^3	a^4	a^5
ba^4	ba^4	ba^5	b	ba	ba^2	ba^3	a^5	e	a	a^2	a^3	a^4
ba^5	ba^5	b	ba	ba^2	ba^3	ba^4	a^4	a^5	e	a	a^2	a^3

D_6:

x	e	r	r^2	r^3	r^4	r^5	d	dr	dr^2	dr^3	dr^4	dr^5
e	e	r	r^2	r^3	r^4	r^5	d	dr	dr^2	dr^3	dr^4	dr^5
r	r	r^2	r^3	r^4	r^5	e	dr^5	d	dr	dr^2	dr^3	dr^4
r^2	r^2	r^3	r^4	r^5	e	r	dr^4	dr^5	d	dr	dr^2	dr^3
r^3	r^3	r^4	r^5	e	r	r^2	dr^3	dr^4	dr^5	d	dr	dr^2
r^4	r^4	r^5	e	r	r^2	r^3	dr^2	dr^3	dr^4	dr^5	d	dr
r^5	r^5	e	r	r^2	r^3	r^4	dr	dr^2	dr^3	dr^4	dr^5	d
d	d	dr	dr^2	dr^3	dr^4	dr^5	e	r	r^2	r^3	r^4	r^5
dr	dr	dr^2	dr^3	dr^4	dr^5	d	r^5	e	r	r^2	r^3	r^4
dr^2	dr^2	dr^3	dr^4	dr^5	d	dr	r^4	r^5	e	r	r^2	r^3
dr^3	dr^3	dr^4	dr^5	d	dr	dr^2	r^3	r^4	r^5	e	r	r^2
dr^4	dr^4	dr^5	d	dr	dr^2	dr^3	r^2	r^3	r^4	r^5	e	r
dr^5	dr^5	d	dr	dr^2	dr^3	dr^4	r	r^2	r^3	r^4	r^5	e

We see in particular that no two of these groups have the same number of e's on the main diagonal, which implies they all have a different number of elements of order 2: A_4 has 4, Q_6 has 2, and D_6 has 8.

With this final addition, our table becomes:

Order	Groups
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$, S_3
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$, D_4, Q_4
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \oplus \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$, D_5
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_{12}$, $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$, D_6, Q_6, A_4
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_{14}$, D_7
15	$\mathbf{Z}_{15}$

A final proposition is needed before we prove that our list is complete: [**?**] Proposition 4.8 on page 91. To see that the induced homomorphism τ_g (defined below) is in fact a homomorphism, see Theorem 4.5 in [**?**] on page 90.

Proposition 6.9. *Let H be a subgroup of a group G and let G act on the set of all left cosets of H, call it S, by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H, where $A(S)$ denotes the group of all permutations of elements of S.*

Proof. The induced homomorphism $G \to A(S)$ is given by $g \to \tau_g$ where $\tau_g : S \to S$, and $\tau_g(xH) = gxH$. If g is in the kernel, then $\tau_g = 1$, and $gxH = xH \ \forall x \in G$. In particular for $x = e$, $geH = eH = H \Rightarrow g \in H$, so $\ker(\tau_g) \subseteq H$ as desired. □

To finish up this thesis we will prove the completeness of the list for order 12 by the following theorem.

Theorem 6.10. *If G is an non-abelian group of order 12, then it is isomorphic to one of A_4, D_6, or Q_6.*

Proof. Let P be a 3-Sylow subgroup of G. Then, $|P| = 3$ and $[G : P] = 4$. Let $S = G/P$ and notice $|S| = 4$, then by Proposition 6.9 there is a homomorphism $f : G \to S_4$ whose kernel is contained in P. Thus, either $K = \langle e \rangle$ or $K = P$.

If $K = \langle e \rangle$ then f is injective, and so $f(G)$ is some subgroup of S_4 of order 12, of which only one exists, namely A_4.

If $K = P$, since the kernel of a homomorphism is always normal, P is normal in G, and as such is the unique 3-Sylow subgroup of G since any conjugate of a Sylow subgroup is a Sylow subgroup. Therefore, G contains only two elements of order 3, call one of them g. From Proposition 2.9 we see $[G : C_g]$ is equal to the number of conjugates of g, and since all conjugates of g must have order 3, it follows that $[G : C_g] = 1$ or 2, and therefore $|C_g| = 12$ or 6 respectively.

In both cases, by Cauchy's Theorem there must exist some $c \in C_g$ such that $\text{ord}(c) = 2$. We can then multiply g and c to get an element of order 6, call this a, i.e. $a = cg$, $\text{ord}(a) = 6$. The cyclic group generated by a, $\langle a \rangle$, then has 6 elements, so $[G : \langle a \rangle] = 2$, and so $\langle a \rangle$ is normal in G. Thus, there exists some element $b \in G$ such that $b \notin \langle a \rangle$, $b^2 \in \langle a \rangle$, and $bab^{-1} \in \langle a \rangle$. Since $\text{ord}(bab^{-1}) = \text{ord}(a)$, $\text{ord}(bab^{-1}) = 6$, we get that $bab^{-1} = a$ or $bab^{-1} = a^5$. Since G isn't abelian $bab^{-1} = a$ cannot occur, so $bab^{-1} = a^5 = a^{-1} \Rightarrow aba = b$.

Now, for $b^2 \in \langle a \rangle$ there are 6 different possibilities as follows:

(1) $b^2 = e$: Coupled with $aba = b$ and $\text{ord}(a) = 6$ we have that $G \cong D_6$.
(2) $b^2 = a$: If $b^2 = a$ it follows that $\text{ord}(b^2) = \text{ord}(a)$ which implies $\text{ord}(b) = 12$ which contradicts G being non-abelian, so this case cannot occur.
(3) $b^2 = a^2$: If $b^2 = a^2$ then we see that $b^3 = a^2b = ba^{-2} = ba^4$, which implies when multiplying both sides by b on the left that $b^2 = a^4 \Rightarrow a^2 = a^4$ which is clearly a contradiction as this implies $\text{ord}(a) = 2$, so this case cannot occur.
(4) $b^2 = a^3$: Coupled with $aba = b$ and $\text{ord}(a) = 6$ we have that $G \cong Q_6$.

(5) $b^2 = a^4$: If $b^2 = a^4$ then we see that $b^3 = a^4b = ba^{-4} = ba^2$, which implies when multiplying both sides by b on the left that $b^2 = a^2 \Rightarrow a^2 = a^4$ which is clearly a contradiction as this implies $\text{ord}(a) = 2$, so this case cannot occur.

(6) $b^2 = a^5$: If $b^2 = a^5$ it follows that $\text{ord}(b^2) = \text{ord}(a^5)$ which implies $\text{ord}(b) = 12$ which contradicts G being non-abelian, so this case cannot occur.

Thus there are only two possibilities that can hold, so G is isomorphic to one of A_4, D_6, Q_6 as desired. □

References

[1] W. Keith Nicholson, Introduction to Abstract Algebra: Fourth Edition, John Wiley and Sons INC, Hoboken, NJ (2012).
[2] C. Pinter, A Book of Abstract Algebra: Second Edition, Dover Publications INC, Mineola, NY (1990).
[3] T. Hungerford, Abstract Algebra, and Introduction: Second Edition, Saunders College Publishing, Orlando, FL (1997).
[4] D. Dummit and R. Foote, Abstract Algebra: Second Edition, John Wiley and Sons INC, Hoboken, NJ (1999).
[5] J. Fraleigh, A First Course in Abstract Algebra, Addison-Wesley Publishing Company, Redding, MA (1968).
[6] J. Gallian, Contemporary Abstract Algebra, D.C. Health and Company, Lexington, MA (1986).
[7] T. Hungerford, Algebra, Springer-Verlag, New York City, NT (1974).

E-mail address: william.stearns@earthlink.net

William Stearns, Senior Thesis Student, Department of Mathematics, Union College, Schenectady, NY 12308