Generalized Dihedral Groups of Small Order

Barbara A. Brown

submitted in partial fulfillment of the requirements for Honors in Mathematics at the University of Mary Washington

Fredericksburg, Virginia

April 2010

This thesis by **Barbara A. Brown** is accepted in its present form as satisfying the thesis requirement for Honors in Mathematics.

DATE APPROVED

__________ ______________________________

Randall D. Helmstutler, Ph.D.
thesis advisor

__________ ______________________________

Janusz Konieczny, Ph.D.
committee member

__________ ______________________________

Keith E. Mellinger, Ph.D.
committee member

Contents

Abstract

Given any abelian group G, the generalized dihedral group of G is the semi-direct product of $C_2 = \{\pm 1\}$ and G, denoted $D(G) = C_2 \ltimes_\varphi G$. The homomorphism φ maps C_2 to the automorphism group of G, providing an action on G by inverting elements. The groups $D(G)$ generalize the classical dihedral groups, as evidenced by the isomorphism between $D(\mathbb{Z}_n)$ and D_n. We will characterize the abelian generalized dihedral groups and supply structural information regarding centers and Sylow subgroups. We attempt to identify the groups $D(G)$ up to isomorphism as we dihedralize each abelian group G of order 1 to 24. The results appear in the table in Appendix C.

1 Introduction

Nearly every grade school student, when working with a construction paper square in art class or playing Four Square at recess, has observed the symmetries of a square. What the young students did not realize was that the exploration of symmetries of polygons leads to the *dihedral groups*, which are essential to studies in group theory, geometry and chemistry. The classical dihedral groups have been thoroughly studied by mathematicians for some time, and because of their structure it is not unusual for these groups to be explored in an undergraduate-level course. Initially, our mission will be to determine the correct generalization of the dihedral groups. Once the correct generalization is established, our goal will be to compile a "dictionary" of generalized dihedral groups of small order. The purpose of compiling the dictionary will be to make conjectures about the structure of $D(G)$ based on that of G. The first step in completing the dictionary will be to create a list of all abelian groups up to order 24. We will then attempt to compute the generalized dihedral group $D(G)$ for each abelian group G in our list. We will see that the computation of some groups will require more work than others; we will provide some sample calculations here. Finally, we will study the Sylow structure of $D(G)$ to see how it relates to the Sylow structure of the associated abelian group G. We begin our exploration with a discussion of the classical dihedral groups.

2 The Classical Dihedral Groups

We define the dihedral groups as the groups of geometric symmetries of regular polygons. These symmetries are found in both the rotations and the reflections of the figure. Generally speaking, a regular polygon with n sides has $2n$ different symmetries which include

n rotational symmetries and n reflective symmetries. With the operation of composition, these symmetries form the dihedral group D_n, where the subscript n indicates the number of sides of the polygon.

2.1 The Dihedral Group D_4

As an example, we will focus on the group of symmetries of the square, which is the dihedral group D_4. It should be mentioned here that some mathematicians denote the group of symmetries of the square by D_8, where the subscript indicates the number of symmetries of the square. We, of course, will use the notation D_4.

Rotating the square gives rise to four symmetries. We will label them as follows:

$$\begin{aligned} 1 &= \text{identity rotation (no motion)} \\ R_{90} &= \text{rotation } 90^\circ \text{ counterclockwise} \\ R_{180} &= \text{rotation } 180^\circ \text{ counterclockwise} \\ R_{270} &= \text{rotation } 270^\circ \text{ counterclockwise.} \end{aligned}$$

Additionally, the reflections across the diagonal, vertical, and horizontal lines of symmetry give rise to four more symmetries. We will denote these as follows:

$$\begin{aligned} S_v &= \text{reflection through the vertical line} \\ S_h &= \text{reflection through the horizontal line} \\ S_{d1} &= \text{reflection through the diagonal running northwest to southeast} \\ S_{d2} &= \text{reflection through the diagonal running northeast to southwest.} \end{aligned}$$

We gain a more complete understanding of the group D_4 when we start to combine one motion with another motion. For example, we may combine a rotation of 90° with a rotation of 180°. The result is a rotation by 270°, which we write as $R_{180} \circ R_{90} = R_{270}$. Likewise, we might follow a rotation by 180° with a reflection through the vertical line of symmetry. This composition would be no different than simply performing a reflection through the horizontal line of symmetry, and we can express this as $S_v \circ R_{180} = S_h$.

Since inverse elements play an important role in algebra, it is interesting to think about which motions behave as inverses of other motions. For example, a reflection through the diagonal line running northwest to southeast followed by a reflection through that same diagonal line brings us to the original position, that is, the identity rotation. In fact, each reflection behaves this way: each reflective motion is its own inverse. In other words, the four reflections in this group are each of order two. Notice that while the same can be said for the rotation by 180°, it is the only rotation of order two.

2.2 Structure of D_4

To better understand the generalization of these classical dihedral groups we will look at the structure of the specific dihedral group D_4. The Cayley table for D_4 is given below.

$\circ$	1	R_{90}	R_{180}	R_{270}	S_v	S_h	S_{d1}	S_{d2}
1	1	R_{90}	R_{180}	R_{270}	S_v	S_h	S_{d1}	S_{d2}
R_{90}	R_{90}	R_{180}	R_{270}	1	S_{d1}	S_{d2}	S_h	S_v
R_{180}	R_{180}	R_{270}	1	R_{90}	S_h	S_v	S_{d2}	S_{d1}
R_{270}	R_{270}	1	R_{90}	R_{180}	S_{d2}	S_{d1}	S_v	S_h
S_v	S_v	S_{d2}	S_h	S_{d1}	1	R_{180}	R_{270}	R_{90}
S_h	S_h	S_{d1}	S_v	S_{d2}	R_{180}	1	R_{90}	R_{270}
S_{d1}	S_{d1}	S_v	S_{d2}	S_h	R_{90}	R_{270}	1	R_{180}
S_{d2}	S_{d2}	S_h	S_{d1}	S_v	R_{270}	R_{90}	R_{180}	1

Note that D_4 is non-abelian; for instance the elements S_h and S_{d1} do not commute. Next we may observe the partitioning of the table. Each of the four "quadrants" is exclusively rotations or reflections. It turns out that the rotations form a cyclic subgroup generated by the smallest rotation, R_{90}. What's more, the subgroup of rotations is normal in D_4 as it is of index two.

Take the reflection S_v in D_4, and let H be the subgroup formed by the identity and this reflection, so $H = \{1, S_v\}$. A check of this reflective subgroup reveals that H is not normal: H is not closed under conjugation since $R_{90} \circ S_v \circ R_{90}^{-1} = S_h$. Notice here that $R_{90}^{-1} = R_{270}$. What is truly remarkable is that we can produce *every* element of D_4 simply by hitting each element of H against each element of R, where R is the subgroup of rotations. That is, composing 1 with each element of R will produce all of the rotations, and composing the single reflection S_v with each element of R will produce all of the reflections. For example, we can obtain the reflection S_{d2} in this way by noting the composition $S_v \circ R_{90} = S_{d2}$. Thus the dihedral group D_4 can be expressed as

$$D_4 = HR$$

where the juxtaposition of these subgroups simply means to take all products of elements between them. Additionally, we observe that H and R intersect trivially, that is

$$H \cap R \ = \{1\}.$$

Lastly, we remark on the relation between conjugates and inverses. One can check that if we conjugate a rotation by a reflection, we are returned the inverse of that rotation. For example, we have $S_v \circ R_{90} \circ S_v^{-1} = S_v \circ R_{90} \circ S_v = R_{270}$. Notice here that R_{270} is in fact the inverse of R_{90}. We say that conjugation *acts by inversion* on the subgroup R of rotations.

3 Semi-direct Products and Generalized Dihedral Groups

3.1 Semi-direct Products

We are nearly ready to generalize the classical dihedral groups, but in order to do so we must discuss the role of automorphisms in semi-direct products.

Definition 3.1. An *automorphism* of a group G is an isomorphism $\varphi : G \to G$. The set of all such automorphisms is denoted $\mathrm{Aut}(G)$.

One can check that $\mathrm{Aut}(G)$ forms a group under composition, known as the *automorphism group* of G.

Let's consider, for example, a group G on which we define a function $i : G \to G$ by $i(g) = g^{-1}$, where i here stands for *inversion*. We will prove in the following proposition that it is the abelian quality of G that makes inversion a homomorphism and ultimately an automorphism.

Proposition 3.2. *Let G be a group and define $i : G \to G$ by $i(g) = g^{-1}$. The function i is an automorphism if and only if G is abelian.*

Proof. First we will show that i is bijective. Take $g \in G$ and apply $i \circ i$:

$$(i \circ i)(g) = i(i(g)) = i(g^{-1}) = (g^{-1})^{-1} = g.$$

Thus we see that $i \circ i = 1_G$, so i is a bijection.

Next we will prove that i is a homomorphism if and only if G is abelian. First assume that G is abelian, and take any $a, b \in G$. Computing the inverse of the product of these two elements we get

$$i(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = i(a)i(b).$$

Hence i is a homomorphism.

Now we will assume that i is a homomorphism. Note that

$$i(ab) = i(a)i(b) = a^{-1}b^{-1} = (ba)^{-1} = i(ba).$$

We now have $i(ab) = i(ba)$, and applying i to both sides of this equation gives $ab = ba$. Hence G is abelian. $\square$

We see now that if G is abelian, then i belongs to $\mathrm{Aut}(G)$, the automorphism group of G. Later we find that this special homomorphism produces the multiplication in the semi-direct product which will generalize the dihedral groups.

Many groups such as $\mathbb{R}^2$ and the Klein four-group are direct products of other groups. We might think of a group like $\mathbb{R}^2$ as being constructed from two copies of $\mathbb{R}$ in a cross product (the external version) or as the decomposition into the x-axis and y-axis (the internal version). In either case, we have a direct product concerning two subgroups, each of which is normal in the parent group. Many groups cannot be distilled into a direct product, however some may be decomposed into a *semi-direct* product. A semi-direct product has both internal and external versions as well, but only one of the factors is normal in the semi-direct product. In essence, the normality of one factor in the direct product is replaced in the semi-direct product with an action on the automorphism group of the other (the normal one). The homomorphism which acts on the normal factor in the semi-direct product gives rise to a group operation.

Definition 3.3. Suppose that G is a group with subgroups H and N. The group G is the *internal semi-direct product* of H with N, written $G = H \ltimes N$, if

1. $G = HN$,
2. $H \cap N = \{e\}$, and
3. N is normal in G.

There is a canonical homomorphism $\varphi : H \to \mathrm{Aut}(N)$ given by conjugation by elements of H. We will write $\varphi_h \in \mathrm{Aut}(N)$ instead of $\varphi(h) \in \mathrm{Aut}(N)$. So, for $h \in H$ and $n \in N$, we have $\varphi_h(n) = hnh^{-1}$. This action determines the operation of G on its elements hn as follows:

$$\begin{aligned}(h_1n_1)(h_2n_2) &= (h_1h_2)(h_2^{-1}n_1h_2n_2)\\ &= (h_1h_2)(\varphi_{h_2^{-1}}(n_1)n_2).\end{aligned}$$

As we have already suggested, there is an external version of the semi-direct product. It is described in the definition that follows.

Definition 3.4. Suppose H and N are groups. Let $\varphi : H \to \mathrm{Aut}(N)$ be a homomorphism. The *external semi-direct product* of H with N under φ, denoted $H \ltimes_\varphi N$, is the group of ordered pairs (h, n) (where $h \in H$ and $n \in N$) under the operation

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, \varphi_{h_2^{-1}}(n_1)n_2).$$

It turns out that the internal and external versions of the semi-direct product are equivalent, but before we prove this we need to address the uniqueness of representation of elements in an internal semi-direct product.

Lemma 3.5. *Assume that $G = H \ltimes N$. Then each $g \in G$ is uniquely expressible as $g = hn$ for $h \in H$ and $n \in N$.*

Proof. We want to show that if $h_1n_1 = h_2n_2$ then $h_1 = h_2$ and $n_1 = n_2$, where $h_1, h_2 \in H$ and $n_1, n_2 \in N$. Supposing $h_1n_1 = h_2n_2$ we have

$$\begin{aligned} h_1n_1 &= h_2n_2 \\ h_1^{-1}h_1n_1 &= h_1^{-1}h_2n_2 \\ n_1n_2^{-1} &= h_1^{-1}h_2n_2n_2^{-1} \\ n_1n_2^{-1} &= h_1^{-1}h_2. \end{aligned}$$

This result indicates that an element in N is equal to an element in H. Since $G = H \ltimes N$, we know that $H \cap N = \{e\}$. Therefore, we can conclude that $n_1n_2^{-1} = h_1^{-1}h_2 = e$. We readily find that $n_1 = n_2$ and $h_1 = h_2$. □

Theorem 3.6. *The internal semi-direct product $G = H \ltimes N$ is isomorphic to the external version $H \ltimes_\varphi N$, where the homomorphism $\varphi : H \to \mathrm{Aut}(N)$ is defined by conjugation.*

Proof. Define $\lambda : H \ltimes N \to H \ltimes_\varphi N$ by $\lambda(hn) = (h, n)$ for $h \in H, n \in N$. Take elements $h_1, h_2 \in H$ and $n_1, n_2 \in N$. Now λ is a homomorphism, as seen in the following:

$$\begin{aligned} \lambda((h_1n_1)(h_2n_2)) &= \lambda((h_1h_2)(\varphi_{h_2^{-1}}(n_1)n_2)) \\ &= (h_1h_2, \varphi_{h_2^{-1}}(n_1)n_2) \\ &= (h_1, n_1)(h_2, n_2) \\ &= \lambda(h_1n_1)\lambda(h_2n_2). \end{aligned}$$

Next we need to show that λ is invertible. Let's define $\kappa : H \ltimes_\varphi N \to H \ltimes N$ by $\kappa(h, n) = hn$ for $h \in H, n \in N$. Apply $\kappa \circ \lambda$ to hn and get

$$(\kappa \circ \lambda)(hn) = \kappa(h, n) = hn.$$

Similarly we compute the following:

$$(\lambda \circ \kappa)(h, n) = \lambda(hn) = (h, n).$$

Hence we have shown that $\kappa \circ \lambda = 1_G$ and $\lambda \circ \kappa = 1_{H \ltimes_\varphi N}$. Therefore λ is an isomorphism between $H \ltimes N$ and $H \ltimes_\varphi N$. □

3.2 Generalized Dihedral Groups

The classical dihedral groups are well-known to mathematicians. The specific case of D_4 considered in Section 2.1 is representative of the classical dihedral groups. As we noted in Section 2.2, the group D_4 with its subgroup of rotations R and subgroup H containing a single reflection can be written as $D_4 = HR$. The cyclic subgroup R is normal in D_4, and the subgroups H and R intersect trivially. The group D_4 meets the definition of semi-direct product and can be expressed as $H \ltimes R$. By Theorem 3.6, we know that $H \ltimes R \cong H \ltimes_{\varphi} R$ where the homomorphism φ is defined by conjugation. Additionally, in D_4, conjugation of a rotation by the single reflection in H results in the inverse of that rotation. Thus H acts on R by inversion. One can check that the two-element group H is isomorphic to the multiplicative group $C_2 = \{\pm 1\}$. Now the homomorphism φ maps C_2 to the automorphism group of R where $\varphi_1(g) = g$ and $\varphi_{-1}(g) = g^{-1}$ for any $g \in R$. This structure leads us directly to the generalization of the dihedral groups. The group of rotations generalizes to any abelian group G and the reflection group H is represented by the group C_2. We can succinctly define the generalized dihedral group $D(G)$ below.

Definition 3.7. Let G be an abelian group. Define an action $\varphi : C_2 \to \mathrm{Aut}(G)$ by

$$\begin{aligned} \varphi_1(g) &= g \\ \varphi_{-1}(g) &= g^{-1} \end{aligned}$$

for each $g \in G$. The *generalized dihedral group* of G is defined as $D(G) = C_2 \ltimes_{\varphi} G$.

Since the subgroup C_2 contains only the elements ± 1, we can simplify the following:

$$\varphi_h(g) = \begin{cases} g, & h = 1 \\ g^{-1}, & h = -1. \end{cases}$$

For any h being ± 1 and any $g \in G$ we can conclude that $\varphi_h(g) = g^h$.

4 Main Results

4.1 The Group Operation and Subgroups

It will be helpful to simplify the multiplication that is part of the structure of the generalized dihedral groups. Since we are working with a semi-direct product we multiply according to the laws described in Section 3.1. For $(c_1, g_1), (c_2, g_2) \in D(G)$ we have by definition

$$\begin{aligned} (c_1, g_1)(c_2, g_2) &= (c_1 c_2, \varphi_{c_2^{-1}}(g_1) g_2) \\ &= (c_1 c_2, \varphi_{c_2}(g_1) g_2) \\ &= (c_1 c_2, g_1^{c_2} g_2). \end{aligned}$$

Note in the above that we used $c_2 = c_2^{-1}$ for $c_2 = \pm 1$. Recognizing this simplified product will be useful in much of the work that follows.

The following proposition states that dihedralization preserves subgroups.

Proposition 4.1. *If H is a subgroup of an abelian group G then $D(H)$ is a subgroup of $D(G)$.*

Proof. We will use the subgroup test. First, $D(H)$ is not empty as $(1, e) \in D(H)$. To show closure under multiplication, take $(c_1, h_1), (c_2, h_2) \in D(H)$. Forming the product, we get

$$(c_1, h_1)(c_2, h_2) = (c_1 c_2, h_1^{c_2} h_2)$$

which lives in $D(H)$. Finally, we claim that inverses exist in $D(H)$. Moreover we assert that $(c, h)^{-1} = (c, h^{-c})$. To see this, note that

$$(c, h)(c, h^{-c}) = (c^2, h^c h^{-c}) = (1, e)$$

and similarly $(c, h^{-c})(c, h)$ produces the identity. Thus $D(H)$ is a subgroup of $D(G)$. $\square$

The next proposition asserts that if H is a subgroup of G then it also appears as a subgroup of $D(G)$.

Proposition 4.2. *If H is a subgroup of the abelian group G, then $H \cong \{1\} \times H$ is a subgroup of $D(G)$.*

Proof. We will use the subgroup test. We first note that $\{1\} \times H$ is not empty for it contains $(1, e)$. Given $(1, h_1), (1, h_2) \in \{1\} \times H$ we get

$$(1, h_1)(1, h_2) = (1, h_1 h_2).$$

Thus $\{1\} \times H$ is closed under multiplication. Given $(1, h) \in \{1\} \times H$ we have $(1, h)^{-1} = (1, h^{-1})$ which shows closure under taking inverses. Thus $\{1\} \times H$ is a subgroup of $D(G)$. $\square$

4.2 Elements of Order Two

Elements of order two are intriguing if for no other reason than they are their own inverses. Their quantity alone is noteworthy in the classical dihedral groups: as we have already seen, every reflection in D_4 is of order two. We will make some observations here about elements that square to the identity. Of particular relevance is the subgroup of these elements.

Definition 4.3. Let G be an abelian group. The set G_2 is comprised of all elements of G which square to the identity, namely $G_2 = \{g \in G \mid g^2 = e\}$.

It is probably not too surprising that the set defined here is a subgroup.

Proposition 4.4. *For any abelian group G, the set G_2 is a subgroup of G.*

Proof. We will use the subgroup test. First, G_2 is non-empty because e lives in G_2 as $e^2 = e$. Secondly, G_2 is closed under multiplication. For $x, y \in G_2$, the square of their product is

$$(xy)^2 = xyxy = xxyy = x^2y^2 = e,$$

so xy belongs to G_2. Finally, we claim that inverses exist in G_2. Take $x \in G_2$ and square its inverse to get

$$(x^{-1})^2 = (x^2)^{-1} = e^{-1} = e.$$

Thus G_2 is closed under taking inverses and is a subgroup of G. □

We can now make some determinations about the elements of order two in generalized dihedral groups.

Proposition 4.5. *Given any generalized dihedral group $D(G)$, every element of the form $(-1, g)$ is of order two.*

Proof. Squaring $(-1, g)$ yields the identity since $(-1, g)^2 = (-1, g)(-1, g) = (1, g^{-1}g) = (1, e)$. □

Half of the elements of $D(G)$ are of the form $(-1, g)$, so it immediately follows that at least half of the elements of $D(G)$ are of order two. Another proposition tells us about elements of the form $(1, g)$.

Proposition 4.6. *Let $D(G)$ be a generalized dihedral group. An element of the form $(1, g)$ squares to the identity if and only if $g^2 = e$.*

Proof. This follows from the identity $(1, g)^2 = (1, g^2)$. □

Theorem 4.7. *Suppose that G is a finite abelian group. Then the number of elements of order two in $D(G)$ is*

$$|G| \ + \ |G_2| \ - \ 1.$$

Proof. We can look at this one piece at a time. First, Proposition 4.5 tells us that every element of the form $(-1, g)$ is of order two, so we have $|G|$ elements of order two thus far. Secondly, we want to include the elements of the form $(1, g)$ that are of order two. By Proposition 4.6 we know that the number of elements of the form $(1, g)$ that square to the identity would be equal to $|G_2|$. Since $|G_2|$ includes $e \in G$ which is of order one, we need to subtract 1 from $|G_2|$. □

Knowing the order of G_2 can actually give us good information about the group $D(G)$. For instance, $D(G)$ is abelian if and only if $G_2 = G$. The following theorem tells us this.

Theorem 4.8. *Let G be an abelian group. The following statements are equivalent:*

1. $D(G)$ *is abelian.*

2. $g^2 = e$ *for all* $g \in G$.

3. $D(G) = C_2 \times G$.

Proof. We will complete the proof in three parts.

Claim. $D(G) = C_2 \times G$ if and only if $g^2 = e$ for all $g \in G$.

First assume $D(G) = C_2 \times G$. Considering the product $(1, g)(-1, e)$ in $D(G)$, we get $(1, g)(-1, e) = (-1, g^{-1})$. The same product in $C_2 \times G$ yields $(1, g)(-1, e) = (-1, g)$. Since these two products are the same we have $g^{-1} = g$, or equivalently, $g^2 = e$.

Next we assume that $g^2 = e$ for all $g \in G$. We take the product $(c_1, g_1)(c_2, g_2)$ in $D(G)$, obtaining

$$(c_1, g_1)(c_2, g_2) = (c_1c_2, g_1^{c_2}g_2) = (c_1c_2, g_1g_2).$$

Note the result in the last equality is true regardless of the value of c_2 since $g_1^{-1} = g_1$. We recognize this product as precisely the product $(c_1, g_1)(c_2, g_2)$ in $C_2 \times G$.

Claim. If $D(G)$ is abelian then $g^2 = e$ for all $g \in G$.

Given $(1, g), (-1, e) \in D(G)$, we compute their products in parallel:

$$\begin{aligned}(1, g)(-1, e) &= (-1, e)(1, g)\\ (-1, g^{-1}) &= (-1, g).\end{aligned}$$

Thus we find $g^{-1} = g$, which implies $g^2 = e$.

Lastly, notice that statement 3 implies statement 1 since the direct product of two abelian groups is itself abelian. □

4.3 Centers

In order to better evaluate generalized dihedral groups we should also explore the notion of centers. We can use centers to classify groups, so they will become a useful tool in calculating $D(G)$.

Definition 4.9. The *center* of a group G, denoted $Z(G)$, is the set of elements that commute with all elements of G. That is, $Z(G) = \{a \in G \mid ag = ga\ \forall g \in G\}$.

The next two propositions will allow us to speak of the center of a group as being a normal subgroup of the parent group.

Proposition 4.10. *The center of a group* G *is a subgroup of* G.

Proof. We will use the subgroup test. We know that $Z(G)$ is non-empty since $e \in Z(G)$. To show closure under multiplication, let's take $x, y \in Z(G)$ and any $g \in G$ and calculate the following product:

$$xyg = xgy = gxy.$$

Thus we conclude that the product xy is in $Z(G)$. We next show that inverses exist in $Z(G)$. Take $x \in Z(G), g \in G$ and note that

$$x^{-1}g = (g^{-1}x)^{-1} = (xg^{-1})^{-1} = gx^{-1}.$$

Thus the inverse of x belongs to $Z(G)$ as well, and we can finally conclude that $Z(G)$ is a subgroup of G. $\square$

Proposition 4.11. *The center $Z(G)$ is a normal subgroup in G.*

Proof. To show that $Z(G)$ is normal in G, we need to show for all g in G and x in $Z(G)$ that gxg^{-1} is in the center of G. That is, we must show $gxg^{-1}h = hgxg^{-1}$ for all $h \in G$. Since $x \in Z(G)$, we have

$$\begin{aligned} gxg^{-1}h &= gg^{-1}xh \\ &= xh \\ &= hx \\ &= hxgg^{-1} \\ &= hgxg^{-1}. \end{aligned}$$

Hence $Z(G)$ is a normal subgroup in G. $\square$

Now let's direct our attention to the centers of generalized dihedral groups.

Proposition 4.12. *Given any abelian group G, the element $(1, g)$ is in $Z(D(G))$ if and only if $g^2 = e$.*

Proof. First we'll assume that $(1, g) \in Z(D(G))$. Take $(-1, e) \in D(G)$. Since $(1, g) \in Z(D(G))$ we have

$$\begin{aligned} (1, g)(-1, e) &= (-1, e)(1, g) \\ (-1, g^{-1}) &= (-1, g). \end{aligned}$$

Hence we have $g^{-1} = g$ which means $g^2 = e$.

Next let's assume that $g^2 = e$. To prove that $(1, g) \in Z(D(G))$ we will show that $(1, g)(c, h) = (c, h)(1, g)$ for all $(c, h) \in D(G)$. On the left we get

$$(1, g)(c, h) = (c, g^c h) = (c, gh).$$

Here this reduces as such regardless of the value of c since $g^{-1} = g$. On the right we get

$$(c, h)(1, g) = (c, hg) = (c, gh).$$

Therefore $(1, g)$ is in $Z(D(G))$. $\square$

Oddly enough, we see in the following proposition that having an element of the form $(-1, g)$ in the center of $D(G)$ is rare.

Proposition 4.13. *Given any abelian group G, the element $(-1, g)$ is in the center of $D(G)$ if and only if $D(G)$ is abelian.*

Proof. The implication $(\Rightarrow)$ is the only direction requiring proof. Suppose that $(-1, g) \in Z(D(G))$. Now take $(1, h) \in D(G)$, where h is any element of G. We know that $(-1, g)$ will commute with $(1, h)$ and so

$$\begin{aligned}
(-1, g)(1, h) &= (1, h)(-1, g) \\
(-1, gh) &= (-1, h^{-1}g) \\
(-1, gh) &= (-1, gh^{-1}).
\end{aligned}$$

The equation above implies that $gh = gh^{-1}$ or that $h = h^{-1}$. Thus we know that $h^2 = e$ for any $h \in G$. We can conclude that $D(G)$ is abelian by Theorem 4.8. $\square$

Next we will focus on the centers of non-abelian generalized dihedral groups. An immediate result of the preceding two propositions resides in the next corollary.

Corollary 4.14. *Given any abelian group G, if the generalized dihedral group $D(G)$ is non-abelian then $Z(D(G)) = \{(1, g) \mid g^2 = e\}$.*

Proof. Elements in $D(G)$ look like either $(1, g)$ or $(-1, g)$. Since $D(G)$ is non-abelian it follows from Proposition 4.13 that $Z(D(G))$ will not contain elements of the form $(-1, g)$. It follows immediately from Proposition 4.12 that the elements of the center of $D(G)$ are of the form $(1, g)$ where $g^2 = e$. $\square$

4.4 The Isomorphism Problem

The next theorem shows that for a large class of abelian groups G, the generalized dihedral group $D(G)$ determines G up to isomorphism.

Theorem 4.15. *Let H and K be abelian groups. Then:*

1. *If $H \cong K$ then $D(H) \cong D(K)$.*

2. *If $D(H) \cong D(K)$ and $D(H)$ is not abelian, then $H \cong K$.*

3. *If $D(H) \cong D(K)$ and H is finite, then $H \cong K$.*

Proof. To prove the first statement, suppose $H \cong K$. Then there exists an isomorphism $\theta : H \to K$. Define $\varphi : D(H) \to D(K)$ by $\varphi(c, h) = (c, \theta(h))$. One can easily check that φ is bijective and that φ is a homomorphism; these follow because θ has the same properties. Thus φ provides an isomorphism from $D(H)$ to $D(K)$.

For the second statement, suppose $D(H) \cong D(K)$ and $D(H)$ is not abelian. Then $D(K)$ is also non-abelian and there is an isomorphism $\alpha : D(H) \to D(K)$. Given $(1, h) \in D(H)$, we would like to show that $\alpha(1, h) = (1, k)$ for some $k \in K$. Suppose not, so that $\alpha(1, h) = (-1, k)$. By Proposition 4.5, the element $(-1, k)$ is of order two, and so the same must be true of $(1, h)$. From this we deduce that $h^2 = e$ in H, and Proposition 4.12 shows that $(1, h)$ must belong to $Z(D(H))$. But as α is an isomorphism it preserves central elements, and so $(-1, k)$ must belong to $Z(D(K))$. Proposition 4.13 now shows that $D(K)$ must be abelian, a contradiction.

Given any $h \in H$, we now have that $\alpha(1, h)$ has the form $(1, k)$ for a uniquely determined element $k \in K$. Setting $\tau(h) = k$ defines a function $\tau : H \to K$. In short, $\tau(h)$ is the unique element of K satisfying the equation $\alpha(1, h) = (1, \tau(h))$. We claim that $\tau : H \to K$ is an isomorphism.

First we show that τ is a homomorphism. Apply α to the product $(1, h_1)(1, h_2) \in D(H)$ to get

$$\alpha((1, h_1)(1, h_2)) = \alpha(1, h_1 h_2) = (1, \tau(h_1 h_2)).$$

Now since α is a homomorphism this is equal to

$$\alpha(1, h_1)\alpha(1, h_2) = (1, \tau(h_1))(1, \tau(h_2)) = (1, \tau(h_1)\tau(h_2)).$$

We conclude that $(1, \tau(h_1 h_2)) = (1, \tau(h_1)\tau(h_2))$. Equating corresponding components we get $\tau(h_1 h_2) = \tau(h_1)\tau(h_2)$, and thus τ is a homomorphism.

Next we show that τ is injective. Given $h \in H$, suppose that $\tau(h) = e$. Now we know

$$\alpha(1, h) = (1, \tau(h)) = (1, e).$$

Since α is an isomorphism, $(1, h) = (1, e)$. Therefore we conclude $h = e$ and $\operatorname{Ker}(\tau) = \{e\}$. Thus τ is injective.

Lastly we show that τ is surjective. Fix $k \in K$. Since α is surjective we know there exists $(c, h) \in D(H)$ with $\alpha(c, h) = (1, k)$. We argue on α^{-1} as we did on α above and find that (c, h) must be $(1, h)$. Thus we have

$$\alpha(1, h) = (1, \tau(h)) = (1, k).$$

This implies that $\tau(h) = k$, and thus τ is surjective. Therefore we conclude that τ is an isomorphism and $H \cong K$.

Finally, suppose that $D(H) \cong D(K)$ and that H is finite. If $D(H)$ is non-abelian then $H \cong K$ by the previous result. Suppose that $D(H)$ is abelian. By Theorem 4.8 we know that $D(H)$ abelian implies $h^2 = e$ for all $h \in H$. By the Fundamental Theorem of Finite Abelian Groups, we must have

$$H \cong (\mathbb{Z}_2)^k$$

for some positive integer k. Likewise, we have that $D(K)$ is abelian and so

$$K \cong (\mathbb{Z}_2)^m$$

for some positive integer m. Now by assumption, $D(H) \cong D(K)$, and by Theorem 4.8 we conclude that $\mathbb{Z}_2 \times H \cong \mathbb{Z}_2 \times K$. This forces

$$2^{k+1} = 2^{m+1}$$

since isomorphic groups have the same number of elements. This implies that $k = m$, and hence $H \cong K$. $\square$

When $D(G)$ is infinite and abelian, Theorem 4.15 does not imply that $D(G)$ determines G up to isomorphism. This question remains unresolved.

5 Calculations of Generalized Dihedral Groups

5.1 Dihedralizing $\mathbb{Z}_2 \times \mathbb{Z}_4$

Compiling a list of dihedralized groups will allow us to make some conjectures about the dihedralization of the abelian groups in general. We will begin with a list of known abelian groups and calculate the dihedralized groups for each one in turn. Our exploration of generalized dihedral groups will start then with the smallest of the abelian groups, the trivial group $\{e\}$. It is immediate that when we dihedralize the trivial group we are returned one copy of $\mathbb{Z}_2$. (Note that $C_2 \cong \mathbb{Z}_2$.)

In our calculations we will have many dihedralized groups that reduce to the classical dihedral groups. Recall from Section 3.2 that the group D_4 is representable as $H \ltimes R$, where R is the group of rotations. Since R is a cyclic group of order four, we can rewrite this as $D(\mathbb{Z}_4) \cong D_4$. Likewise, for $n \geq 3$ we have $D(\mathbb{Z}_n) \cong D_n$, the group of symmetries of a regular polygon with n sides.

Additionally, a direct application of Theorem 4.8 reveals that $D((\mathbb{Z}_2)^n) = (\mathbb{Z}_2)^{n+1}$ as each non-identity element of $(\mathbb{Z}_2)^n$ has order two. So for example, we have $D(\mathbb{Z}_2) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus the dihedralization of many of the abelian groups will be rather straightforward. However, those that are not will require some careful consideration.

If we turn to Appendix C we find that the first nine generalized dihedral groups of Table C result in either multiple copies of $\mathbb{Z}_2$ or classical dihedral groups. The first abelian group of interest then is $\mathbb{Z}_2 \times \mathbb{Z}_4$. This group will involve significantly more thought since it is neither of the form $(\mathbb{Z}_2)^n$ nor $\mathbb{Z}_n$. The more challenging groups to decipher will require knowledge of centers and elements of order two.

We assert by Theorem 4.8 that the dihedralization of $\mathbb{Z}_2 \times \mathbb{Z}_4$ results in a non-abelian group, and we also observe that it is of order 16 since $|D(\mathbb{Z}_2 \times \mathbb{Z}_4)| = |C_2||\mathbb{Z}_2||\mathbb{Z}_4|$. To further describe this non-abelian group, we would like to know something about its center. Information about $Z(D(\mathbb{Z}_2 \times \mathbb{Z}_4))$ will come from a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_4$, precisely the subgroup of elements that square to the identity. The following table shows us which elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ square to the identity:

g	$2g$
(0, 0)	**(0, 0)**
$(0, 1)$	$(0, 2)$
(0, 2)	**(0, 0)**
$(0, 3)$	$(0, 2)$
(1, 0)	**(0, 0)**
$(1, 1)$	$(0, 2)$
(1, 2)	**(0, 0)**
$(1, 3)$	$(0, 2)$

Thus if $G = \mathbb{Z}_2 \times \mathbb{Z}_4$, the above table shows that

$$G_2 = \{(0, 0), (0, 2), (1, 0), (1, 2)\}.$$

By applying Corollary 4.14 we find that the elements of $Z(D(\mathbb{Z}_2 \times \mathbb{Z}_4))$ correspond to the elements of G_2. Of note here, too, is that this center must be isomorphic to the Klein four-group since no element of G_2 has order four.

We now know that $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$ is a non-abelian group of order 16 whose center is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. If we turn to Table A (taken from [4]) which lists the non-abelian groups of order 16, we see that both of the groups $C_2 \times D_4$ and $C_2 \times Q_8$ have centers isomorphic to the Klein four-group. Note here that Q_8 is the quaternion group with elements $\{\pm 1, \pm i, \pm j, \pm k\}$ under multiplication. We next utilize information about the number of elements of order two to help us distinguish $C_2 \times D_4$ from $C_2 \times Q_8$. In the following analysis we will count the number of elements of order two in $C_2 \times D_4$ and in $C_2 \times Q_8$ as well as in our group $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$. This will determine whether $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$ is isomorphic to $C_2 \times D_4$ or to $C_2 \times Q_8$.

- $C_2 \times D_4$: The group D_4 consists of five elements of order two, namely each of the reflections and the rotation by 180°. So in $C_2 \times D_4$ there are at least ten elements of order two, as we have paired ± 1 with each of the five elements of order two in D_4. To this set of ten elements we must add the ordered pair with -1 in the first slot and the identity rotation from D_4 in the second slot. Thus there are 11 elements of order two in the group $C_2 \times D_4$.

- $C_2 \times Q_8$: The group Q_8 includes only the element -1 that is of order two. So in $C_2 \times Q_8$ there are at least two elements of order two, as we have paired ± 1 with the element -1. Additionally the element $(-1, 1)$ is of order two. Consequently we have determined there to be three elements of order two in the group $C_2 \times Q_8$.

- $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$: We can determine the number of elements of order two in $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$ when we apply Theorem 4.7. Here of course our group G is $\mathbb{Z}_2 \times \mathbb{Z}_4$. Our calculations produce the following:
$$|G| + |G_2| - 1 = 8 + 4 - 1 = 11.$$
So we find there are 11 elements of order two in $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

We can finally conclude that $D(\mathbb{Z}_2 \times \mathbb{Z}_4)$ must be isomorphic to $C_2 \times D_4$. Considerable work went into calculating this rather small generalized dihedral group. A result that follows later will enable us to calculate groups like $\mathbb{Z}_2 \times \mathbb{Z}_n$ with significantly less effort.

5.2 Dihedralizing $\mathbb{Z}_3 \times \mathbb{Z}_3$

The next abelian group in Table C that will require some interesting analysis is the group $\mathbb{Z}_3 \times \mathbb{Z}_3$. We can conclude by Theorem 4.8 that $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$ is a non-abelian group. It of course has order 18. To further characterize this group we will describe its center. Therefore we need to count the number of elements of $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ that square to the identity. Since G here has order nine it contains no elements of order two, and thus we find $G_2 = \{(0, 0)\}$. By Theorem 4.14 we can assert that $D(G)$ has the trivial group as its center. If we turn to the table of non-abelian groups of order 18 in Appendix B (taken from [4]) we discover that the group D_9 has trivial center as does the group $D_3 \times^{\vartheta} D_3$. The construction of the group $D_3 \times^{\vartheta} D_3$ that appears in [4] is beyond the scope of this paper. A distinguishing feature between these two groups is their subgroups. Since having subgroups of equal order is an invariant under isomorphism, we will use this to determine the group that is not isomorphic to $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$ and consequently to determine the group that is.

The classical dihedral group D_9 has a subgroup of order nine, namely the cyclic subgroup of rotations. Now a calculation of the orders of the elements of $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$ reveals that our group does not have a cyclic subgroup of order nine. Therefore we conclude that $D(\mathbb{Z}_3 \times \mathbb{Z}_3) \ncong$

D_9. We can conclude then that our non-abelian group is isomorphic to $D_3 \times^{\vartheta} D_3$, which is not helpful. However we will give a nice matrix representation of $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$ in the next section.

5.3 Matrix Representation of $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$

With the help of Magma [1], a software package designed to solve computationally difficult problems in algebra, we have identified a matrix representation for the group $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$. Recall that $\mathrm{GL}(n, F)$ denotes the group of all nonsingular $n \times n$ matrices over the field F. A matrix representation of $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$ as a subgroup of $\mathrm{GL}(3, \mathbb{Z}_3)$ may be defined by the group of matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & c \end{pmatrix}$$

where $a, b, c \in \mathbb{Z}_3$ with $c = \pm 1$. We will refer to this matrix representation as T_3. With three choices for each of a and b and two choices for c, the order is correct giving $|T_3| = 3 \cdot 3 \cdot 2 = 18$.

We will use the subgroup test to confirm that T_3 is a subgroup of $\mathrm{GL}(3, \mathbb{Z}_3)$.

- The set T_3 is non-empty since it includes the 3-by-3 identity matrix.
- The set T_3 is closed under multiplication. Take any two matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & \pm 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x & y & \pm 1 \end{pmatrix}$$

  where $a, b, x, y \in \mathbb{Z}_3$. We multiply to get

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & \pm 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x & y & \pm 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a \pm x & b \pm y & \pm 1 \end{pmatrix}.$$

  Thus the resulting matrix belongs to T_3.

- The set T_3 is closed under taking inverses. We note two cases.

  Case 1. If $c = -1$ then the matrix is its own inverse.

  Case 2. If $c = 1$ then the inverse is as follows:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -a & -b & 1 \end{pmatrix}.$$

One can check that these inverses are correct, and that they belong to T_3. Thus T_3 is a subgroup of $\mathrm{GL}(3, \mathbb{Z}_3)$.

Matrices do not generally commute under multiplication. In T_3 we have

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}.$$

Notice that these elements do not commute as

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Thus T_3 is a non-abelian group.

To determine the isomorphism type of this non-abelian matrix group of order 18, we turn again to the table in Appendix B. We find that T_3 is one of three groups. We already know a lot about the order of half of the elements in T_3. Each of the elements with $c = -1$ is its own inverse, so we know that at least half of the elements are of order two. It turns out that each of the non-identity elements with $c = 1$ is of order three. We conclude then that T_3 does not have a cyclic subgroup of order nine. Thus it is isomorphic to either $D_3 \times C_3$ or $D_3 \times^\vartheta D_3$. We now consider the center of T_3 in order to distinguish the two groups in the table. It turns out that none of the matrices (with the exception of the identity matrix) will commute with all of the matrices of the group. One can check this by computing ten pairs of matrix products. Thus we find that the center of T_3 is trivial, and T_3 must be isomorphic to $D_3 \times^\vartheta D_3$. We can conclude that T_3 is a matrix representation of $D(\mathbb{Z}_3 \times \mathbb{Z}_3)$.

5.4 Dihedralization of $C_2 \times G$

In mathematics and other sciences, the compilation of data can suggest trends. Notice in our table in Appendix C that a number of the abelian groups are of the form $\mathbb{Z}_2 \times G$ where G is abelian. We have already calculated the dihedralization of one such group when we dihedralized $\mathbb{Z}_2 \times \mathbb{Z}_4$. Recall that the calculation was quite involved. It will ease our work greatly if we can develop a simplification for the dihedralization of groups like this one. The next theorem we discuss does just that.

This theorem indicates that a particular semi-direct product can be rewritten as a direct product that includes as one of its factors a semi-direct product. In essence, we are allowed to "slip out" a factor of $\mathbb{Z}_2$ in certain situations. In proving this result, special attention must be paid to the multiplication of elements in the groups. In some instances we are multiplying elements from a semi-direct product and in other instances we are multiplying elements from a direct product.

Theorem 5.1. *Given any abelian group G, the group $D(C_2 \times G)$ is isomorphic to $C_2 \times D(G)$.*

Proof. Recall that $D(C_2 \times G) = C_2 \ltimes_\varphi (C_2 \times G)$ and $C_2 \times D(G) = C_2 \times (C_2 \ltimes_\varphi G)$. We define $\alpha : D(C_2 \times G) \to C_2 \times D(G)$ by

$$\alpha(a,(b,g)) = (b,(a,g))$$

where $(a,(b,g)) \in D(C_2 \times G)$.

We will first show that α is a homomorphism. Take $(a,(b,g)),(c,(d,h)) \in D(C_2 \times G)$. Now apply α as follows:

$$\begin{aligned}
\alpha((a,(b,g))(c,(d,h))) &= \alpha(ac,(b,g)^c(d,h)) \\
&= \alpha(ac,(b^c,g^c)(d,h)) \\
&= \alpha(ac,(b^c d,g^c h)) \\
&= (b^c d,(ac,g^c h)) \\
&= (bd,(ac,g^c h)).
\end{aligned}$$

In the above, we were able to reduce b^c to b since $b,c = \pm 1$. Next we will apply α to each of $(a,(b,g))$ and $(c,(d,h))$ and compute their product. We get

$$\begin{aligned}
\alpha(a,(b,g))\alpha(c,(d,h)) &= (b,(a,g))(d,(c,h)) \\
&= (bd,(a,g)(c,h)) \\
&= (bd,(ac,g^c h)).
\end{aligned}$$

Thus α is a homomorphism.

Next we define $\beta : C_2 \times D(G) \to D(C_2 \times G)$ by

$$\beta(a,(b,g)) = (b,(a,g))$$

for $(a,(b,g)) \in C_2 \times D(G)$. Given α and β as defined, it follows immediately that

$$\begin{aligned}
\beta \circ \alpha &= 1_{D(C_2 \times G)} \\
\alpha \circ \beta &= 1_{C_2 \times D(G)}.
\end{aligned}$$

Hence α is an isomorphism. □

The ease that this preceding theorem affords is made clear in the next example.

Example 5.2. To dihedralize $\mathbb{Z}_2 \times \mathbb{Z}_6$ we can effectively "slip out" a factor of $\mathbb{Z}_2$. We apply Theorem 5.1 here, and we have

$$D(\mathbb{Z}_2 \times \mathbb{Z}_6) \cong \mathbb{Z}_2 \times D(\mathbb{Z}_6) \cong \mathbb{Z}_2 \times D_6.$$

Now we are equipped with the tools to calculate nearly all of the generalized dihedral groups up to order 48. Theorem 5.1 coupled with our earlier results allows us to dihedralize the abelian groups through order 24, with the single exception of the group $\mathbb{Z}_4 \times \mathbb{Z}_4$. Notice that the order of $D(\mathbb{Z}_4 \times \mathbb{Z}_4)$ is 32, a power of two. There are numerous non-abelian groups of order 32 with centers that are the same as the center of $D(\mathbb{Z}_4 \times \mathbb{Z}_4)$, impacting our ability to identify $D(\mathbb{Z}_4 \times \mathbb{Z}_4)$. Our table of generalized dihedral groups appears in Appendix C.

6 Sylow Structure of Generalized Dihedral Groups

6.1 Sylow Theorems

We know by Lagrange's Theorem that for every subgroup H of a finite group G, the order of H divides the order of G. However, the converse of this theorem does not hold. The First Sylow Theorem offers a quasi-converse to Lagrange's Theorem. The Norwegian mathematician Peter Ludvig Mejdell Sylow did extensive work in the area of group theory. Proofs of the Sylow Theorems are available in [3]. Throughout this section, p will be a prime.

Definition 6.1. A group G is a *p-group* if every element in G has order a power of the prime p. A subgroup of a group G is a *p-subgroup* of G if the subgroup is itself a p-group.

It turns out that finite p-groups are groups of prime-power order. The first of the Sylow Theorems provides for the existence of prime-power subgroups of a finite group G when the prime power divides the order of G.

Theorem 6.2. ***(First Sylow Theorem)*** *Let G be a finite group and let $|G| = p^n m$, where $n \geq 1$ and p does not divide m. Then*

1. *G contains a subgroup of order p^i for each i where $1 \leq i \leq n$, and*
2. *Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.*

Definition 6.3. A *Sylow p-subgroup* of a finite group G is a maximal p-subgroup of G, that is, a p-subgroup contained in no larger p-subgroup.

The second Sylow Theorem describes the relationships between Sylow p-subgroups. It states that any two Sylow p-subgroups of a finite group are conjugate.

Theorem 6.4. ***(Second Sylow Theorem)*** *Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G.*

The last Sylow Theorem gives information about the number of Sylow p-subgroups in a finite group.

Theorem 6.5. ***(Third Sylow Theorem)*** *Suppose G is a finite group and p divides $|G|$. If $|G| = p^n m$ where $p \nmid m$, then the number of Sylow p-subgroups is congruent to 1 modulo p and divides m.*

We apply the Sylow Theorems in the next examples.

Example 6.6. Take a group G of order 180. We completely factor 180 as $2^2 \cdot 3^2 \cdot 5$. The First Sylow Theorem guarantees that G contains subgroups of orders $2, 3, 4, 5$ and 9. The theorem does not assert however that G contains a subgroup of order 6 or of order 10. So we see that the First Sylow Theorem is *nearly* a converse of Lagrange. Now consider the Sylow p-subgroups of G. We can conclude the following for a group of order 180:

- the order of a Sylow 2-subgroup is 4
- the order of a Sylow 3-subgroup is 9
- the order of a Sylow 5-subgroup is 5.

Example 6.7. Next we consider a group G of order 20. We completely factor 20 as $2^2 \cdot 5$. The Third Sylow Theorem provides us with information about the number of Sylow 5-subgroups, which are of order 5. Let n_5 denote the number of Sylow 5-subgroups. We know that n_5 divides 4 and is congruent to 1 modulo 5. The only divisor of 4 that is congruent to 1 (mod 5) is 1. Thus there is a unique Sylow 5-subgroup.

6.2 Sylow Subgroups of Generalized Dihedral Groups

We will now consider the Sylow subgroups of the generalized dihedral groups. Given the nature of the construction of these groups we expect to find that the Sylow subgroup structure of G will affect the Sylow subgroup structure of $D(G)$. We will see that dihedralization gives a correspondence between the Sylow p-subgroups of G and those of $D(G)$ when p is an odd prime. However this is not the case when $p = 2$.

Theorem 6.8. *Let G be a finite abelian group, and let p be an odd prime. There is an isomorphism-preserving correspondence between the Sylow p-subgroups of G and the Sylow p-subgroups of $D(G)$.*

Proof. We have $|G| = p^n m$ where $p \nmid m$ and $n \geq 1$. The order of $D(G)$ is then $p^n(2m)$. Let H be a Sylow p-subgroup of G, so $|H| = p^n$. By Proposition 4.2, $\{1\} \times H$ is a subgroup of

$D(G)$. Since p is odd and does not divide m, we have $p \nmid 2m$. Hence $\{1\} \times H$ is a Sylow p-subgroup of $D(G)$.

Recall that every element of the form $(-1, g) \in D(G)$ has order two. Since p is odd, a Sylow p-subgroup of $D(G)$ contains no elements of this form, as this would violate Lagrange's Theorem. Thus its elements must all be of the form $(1, g)$. So a Sylow p-subgroup of $D(G)$ must be of the form $\{1\} \times H$, where H is a Sylow p-subgroup of G. □

Theorem 6.9. *Let G be an abelian group. If H is a Sylow 2-subgroup of G then $D(H)$ is a Sylow 2-subgroup of $D(G)$.*

Proof. Suppose the order of G is of the form $2^n m$, where $n \geq 1$ and m is odd. Since H is a Sylow 2-subgroup of G we know $|H| = 2^n$. We can determine the order of $D(H)$ as

$$|D(H)| = |C_2| \cdot |H| = 2 \cdot 2^n = 2^{n+1}.$$

Since $|D(G)| = 2^{n+1}m$, $D(H)$ is a Sylow 2-subgroup of $D(G)$. □

For p an odd prime, Theorem 6.8 says that the number of Sylow p-subgroups of G is the same as the number of Sylow p-subgroups of $D(G)$. By contrast, we find in Theorem 6.9 that the number of Sylow 2-subgroups of G is less than or equal to the number of Sylow 2-subgroups of $D(G)$. It should be noted that this need not be an equality. For instance, take any abelian group G of odd order. The trivial group is the only Sylow 2-subgroup of G. However, given $g \in G$, $\{(1, 1), (-1, g)\}$ is a Sylow 2-subgroup of $D(G)$. In fact, $D(G)$ has $|G|$ Sylow 2-subgroups when G is of odd order.

A Table A: Non-abelian Groups of Order 16

Group	$Z(G)$
$C_2 \times D_4$	$C_2 \times C_2$
$C_2 \times Q_8$	$C_2 \times C_2$
D_8	C_2
Q_{16}	C_2
$\langle x, y : x^8 = 1 = y^2, x^y = x^3 \rangle$	$\langle x^4 \rangle$
$\langle x, y : x^8 = 1 = y^2, x^y = x^5 \rangle$	$\langle x^2 \rangle$
$\langle x, y, z : x^4 = 1 = y^2 = z^2, x \text{ central}, z^y = zx^2 \rangle$	$\langle x \rangle$
$\langle x, y : x^4 = 1 = y^4, x^y = x^3 \rangle$	$\langle x^2, y^2 \rangle$
$\langle x, y, z : x^4 = 1 = y^2 = z^2, z \text{ central}, x^y = xz \rangle$	$\langle z, x^2 \rangle$

Taken from [4]

B Table B: Non-abelian Groups of Order 18

Group	$Z(G)$	Sylow 3-subgroup
D_9	$\{1\}$	C_9
$D_3 \times C_3$	C_3	$C_3 \times C_3$
$D_3 \times^{\vartheta} D_3$	$\{1\}$	$C_3 \times C_3$

Taken from [4]

C Table C: Generalized Dihedral Groups of Order ≤ 48

	Order	# of Groups	# of Abelian Groups	Abelian G	$D(G)$
1	order 1	1	1	$\{e\}$	$\mathbb{Z}_2$
2	order 2	1	1	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$
3	order 3	1	1	$\mathbb{Z}_3$	D_3
4	order 4	2	2	$\mathbb{Z}_4$	D_4
5				$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
6	order 5	1	1	$\mathbb{Z}_5$	D_5
7	order 6	2	1	$\mathbb{Z}_6$	D_6
8	order 7	1	1	$\mathbb{Z}_7$	D_7
9	order 8	5	3	$\mathbb{Z}_8$	D_8
10				$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2 \times D_4$
11				$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$(\mathbb{Z}_2)^4$
12	order 9	2	2	$\mathbb{Z}_9$	D_9
13				$\mathbb{Z}_3 \times \mathbb{Z}_3$	T_3
14	order 10	2	1	$\mathbb{Z}_{10}$	D_{10}
15	order 11	1	1	$\mathbb{Z}_{11}$	D_{11}
16	order 12	5	2	$\mathbb{Z}_{12}$	D_{12}
17				$\mathbb{Z}_2 \times \mathbb{Z}_6$	$\mathbb{Z}_2 \times D_6$
18	order 13	1	1	$\mathbb{Z}_{13}$	D_{13}
19	order 14	2	1	$\mathbb{Z}_{14}$	D_{14}
20	order 15	1	1	$\mathbb{Z}_{15}$	D_{15}
21	order 16	14	5	$\mathbb{Z}_{16}$	D_{16}
22				$\mathbb{Z}_2 \times \mathbb{Z}_8$	$\mathbb{Z}_2 \times D_8$
23				$\mathbb{Z}_4 \times \mathbb{Z}_4$	?
24				$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times D_4$
25				$(\mathbb{Z}_2)^4$	$(\mathbb{Z}_2)^5$
26	order 17	1	1	$\mathbb{Z}_{17}$	D_{17}
27	order 18	5	2	$\mathbb{Z}_{18}$	D_{18}
28				$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_2 \times T_3$
29	order 19	1	1	$\mathbb{Z}_{19}$	D_{19}
30	order 20	5	2	$\mathbb{Z}_{20}$	D_{20}
31				$\mathbb{Z}_2 \times \mathbb{Z}_{10}$	$\mathbb{Z}_2 \times D_{10}$
32	order 21	2	1	$\mathbb{Z}_{21}$	D_{21}
33	order 22	2	1	$\mathbb{Z}_{22}$	D_{22}
34	order 23	1	1	$\mathbb{Z}_{23}$	D_{23}
35	order 24	15	3	$\mathbb{Z}_{24}$	D_{24}
36				$\mathbb{Z}_2 \times \mathbb{Z}_{12}$	$\mathbb{Z}_2 \times D_{12}$
37				$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times D_6$

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma Algebra System. I. The User Language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[2] John R. Durbin, *Modern Algebra an Introduction*, fifth ed., John Wiley and Sons, Inc., Hoboken, NJ, 2005.

[3] John B. Fraleigh, *A First Course in Abstract Algebra*, fifth ed., Addison-Wesley Publishing Co., New York, NY, 1994.

[4] John F. Humphreys, *A Course in Group Theory*, Oxford University Press, Inc., New York, NY, 1996.