2013

The Growth in Normal Subgroups Under Direct Products

Whitney Radil
College of Saint Benedict/Saint John's University

The Growth in Normal Subgroups Under Direct Products

An Honors Thesis

College of St. Benedict/ St. John's University

In Partial Fulfillment
of the requirements for Distinction
in the Department of Mathematics

by

Whitney Radil

Advisor: Bret Benesh

April, 2013

1. Approval Page

Approved by:

Advisor, Bret Benesh
Assistant Professor of Mathematics

Sunil Chetty
Assistant Professor of Mathematics

Michael Gass
Associate professor of Mathematics

Robert Hesse
Chair, Department of Mathematics

Anthony Cunningham
Director, Honors Thesis Program

2. Abstract

This paper will consider the growth of the number of normal subgroups in a nonabelian group under the direct product operation. The groups considered in this paper are dihedral groups and semidirect products with a similar structure. Many proofs will rely on the use of a key property of normal subgroups, namely closure under conjugation, to predict this growth. It will show that for a dihedral group G of order $2m$ where m is odd and has prime factorization $m = \prod_{i=1}^{M} p_i^{\alpha_i}$, the group has $1 + \prod_{i=1}^{M}(\alpha_i + 1)$ normal subgroups, and $G \times G$ has $(1 + \prod_{i=1}^{M}(\alpha_i + 1))^2 + 1$ normal subgroups. This paper will also extend the idea of a dihedral group to a semidirect product of prime cyclic groups for a similar result. Let $H = C_p \rtimes C_q$ where p, q are prime and $p \equiv 1 \bmod q$. This paper will show that there are 3 normal subgroups of H and $9 + (q - 1)$ normal subgroups of $H \times H$.

Contents

3. Acknowledgments

I would like to thank my advisor Dr. Bret Benesh for his guidance; it was no small task to take on my research project and I appreciate the time you spent working with me. I would like to thank my readers Dr.'s Michael Gass and Sunil Chetty. I would like to thank the MapCores program for their support, and for the introduction to mathematical research the last four years. I would also like to thank the math department. I would also like to thank the honors thesis department, particularly Director Anthony Cunningham. Further, I would like to thank the directors of my past research experiences, Dr.'s Chistopher Bernhart and Vadim Ponomarenko for helping me learn the ups and downs of research.

CHAPTER 1

Background

1. Statement of Purpose

The goal of this honors thesis is to determine how certain characteristics of groups behave when we 'glue' groups together. More specifically, this honors thesis will relate to groups that act similarly to the group of symmetries of a square. In this case, gluing two groups together will be like having two squares side by side and doing symmetries on each of them separately.

2. Intuitive Description

A "group" is intuitively a set of symmetries of an object. A subset of a group that is a set of symmetries for a different object is called a "subgroup." There are certain subgroups, called "normal subgroups," that are particularly interesting in mathematics. I will be counting how the number of normal subgroups of a group grows when I build a larger group by "gluing" a group to itself.

3. Definitions

More technically, a *group* G is any set with an operation (denoted by juxtaposition) that satisfies the following four axioms:

(1) There is an identity element $e \in G$ such that $eg = g = ge$ for all $g \in G$.
(2) For every $g \in G$, there is an inverse element $g^{-1} \in G$ such that $gg^{-1} = e = g^{-1}g$.
(3) The operation is associative: for every $g, h, k \in G$, $(gh)k = g(hk)$.
(4) The set is closed under the operation, for every $g, h \in G$, $(gh) \in G$.

In determining properties and characteristics of groups, it is often helpful to look at a subset of the group and examine its properties. A *subgroup* H of G is any subset of G that fulfills the four group axioms with the same operation as G. If H is a subgroup of G we say $H \leq G$. The *trivial subgroup* T is the subgroup containing only the identity element; all other subgroups are *non-trivial.* Any subgroup of G other than G itself is called *proper*; G is *improper*.

Since a mathematician never underestimates the power of simply being able to count something, it is helpful to consider the number of elements of the group. The *order* of a group G is the number of elements in the set G, and is denoted $|G|$. This number will always be a positive integer. Further, the order of a subgroup of G will always divide the order of G. This property is particularly helpful in determining how many and what kinds of subgroups G will have. We will also define the *order* of an element a as the minimal power p such that $a^p = e$.

A group G is *abelian* if $gh = hg$ for all $g, h \in G$, and *nonabelian* if there are some $g \in G$ and $h \in G$ such that $gh \neq hg$. So an abelian group is commutative and a nonabelian group is not. The groups that will be focused on in this paper will be nonabelian groups.

When $a, b \in G$, we refer to *conjugation* of b by a as $b^a = a^{-1}ba$. So in an abelian group, $b^a = b$ for any $a, b \in G$. A *normal subgroup* N of G is a subgroup such that for all $g \in G$ and $n \in N$, $g^{-1}ng \in N$. In other terms, N is closed under conjugation. Note that in abelian groups, all subgroups are normal subgroups.

One goal of this paper is to determine the growth of normal subgroups under the direct product. Since we have determined what normal subgroups are, it is necessary to define a direct product. The *direct product* of a group G with itself (denoted $G \times G$) is the set $\{(g, h) : g, h \in G\}$. It will be shown in the section *Common Theorems* that $G \times G$ forms a group under the operation $(g, h)(a, b) = (ga, hb)$.

Particularly in the area of algebra, mathematicians are concerned with when two things have the same structure. This property is referred to as isomorphism. A group G with operation denoted by $\times$ is *isomorphic* to a group H with operation denoted by juxtaposition provided that there is a bijective function $\phi : G \to H$ such that for all $u, v \in G$, it follows that $\phi(u \times v) = \phi(u)\phi(v)$.

If all elements of a group G can be written as $G = \{aa \cdots a = a^n : n \in \mathbb{Z}\}$ for some $a \in G$ then the group is called *cyclic*. In this paper, we will refer to a cyclic group of k elements by its isomorphism class C_k. The *dihedral group* of order $2m$ can be viewed as the set of symmetries on a regular m-gon. It can be generated by two elements: a rotation (r) and a flip (f). There is a nice property of dihedral groups which allows us to change the order of the flip and rotation. Namely, $r^i f = f r^{-i}$. Since we can always change the order, we can always write r first. Therefore, this group can be written as $D_{2m} = \{r^i f^j : i \in \mathbb{Z}_m \text{ and } j \in \mathbb{Z}_2\}$. The paper then considers a generalization of the dihedral group to a semidirect product. We will define a *semidirect product* of two cyclic groups, generated by a and b respectively, to mimic the structure of a dihedral group. If a has order p and b has order q, then G can be written as $G = \{a^i b^j : 0 < i \leq p \text{ and } 0 < j \leq q\}$. Both the semidirect and the direct products "glue" two groups together, but they are done in different ways.

3.1. Example. The set of the symmetries of a square, called the *dihedral group of order 8* and denoted D_8, is a nonabelian group. The symmetries are: R_0, the rotation of 0°; R_{90}, the rotation of 90°; R_{180}, the rotation of 180°; R_{270}, the rotation of 270°; H, the flip about a horizontal axis; V, the flip about a vertical axis; D, the flip about the main diagonal; and D', the flip about the other diagonal.

Below are examples of how this dihedral group satisfies the four properties required for being a group.

(1) The rotation of 0°, R_0, acts as our identity element since for all $g \in D_8$, it follows that $R_0 g = g = g R_0$.
(2) R_{90} and R_{270} are inverses, and all other symmetries are self inverses.
(3) I will not show this associativity for all $8^3 = 512$ choices, but this is an easy consequence of function composition being associative.
(4) Closure can be shown in entirety, but for now, notice that $R_{270} H = D$.

The dihedral group is nonabelian. We see this because: $R_{270}H = D$, but $HR_{270} = D'$. Since $R_{270}H \neq HR_{270}$, we see that D_8 is nonabelian. From the motivation above, we can now search for subsets that have the abelian-like structure in which they are closed under conjugation. Notice that a normal subgroup of D_8 is $N = \{R_0, R_{90}, R_{180}, R_{270}\}$. For example, $R_{90}^H = H^{-1}R_{90}H = HR_{90}H = R_{270}$. Since R_{90} and R_{270} are in N, this is an example of the closure property being satisfied.

As an example of how the direct product works, below is a full list of elements in $D_8 \times D_8$. The direct product, $D_8 \times D_8$ is

$$\{(R_0, R_0), (R_0, R_{90}), (R_0, R_{180}), (R_0, R_{270}), (R_0, H), (R_0, V), (R_0, D),$$

$$(R_0, D'), (R_{90}, R_0), (R_{90}, R_{90}), (R_{90}, R_{180}), (R_{90}, R_{270}), (R_{90}, H), (R_{90}, V),$$

$$(R_{90}, D), (R_{90}, D'), (R_{180}, R_0), (R_{180}, R_{90}), (R_{180}, R_{180}), (R_{180}, R_{270}),$$

$$(R_{180}, H), (R_{180}, V), (R_{180}, D), (R_{180}, D'), (R_{270}, R_0), (R_{270}, R_{90}),$$

$$(R_{270}, R_{180}), (R_{270}, R_{270}), (R_{270}, H), (R_{270}, V), (R_{270}, D), (R_{270}, D')\}.$$

$D_8 \times D_8$ is clearly a normal subgroup of itself. Since it is closed, it is closed under conjugation.

4. An Introduction to Semidirect Products

Let us now consider a generalization of the Dihedral Group. We will define a semidirect product of two cyclic groups to mimic the structure of a dihedral group.

Let's motivate the semidirect product $C_p \rtimes C_q$ by looking at a semidirect product $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$. Consider the following example where we will build the group which we will call $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$. First let us note that $\mathbb{Z}_7 = \langle 1 \rangle$ and $\mathbb{Z}_3 = \langle 1 \rangle$. Suppose we wanted to determine conjugacy classes of $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ in $\mathbb{Z}_7 = \langle 1 \rangle$. We know that 0 is in a class of its own. Since we are attempting to involve $\mathbb{Z}_3$, let us try to find conjugacy classes of size 3. Note that $\mathbb{Z}_7^\times = \langle 5 \rangle$ which implies that 5 generates the multiplicative group and has order 6. So $5^2 \equiv 4 \bmod 7$ has order 3. Now we will define the conjugation so that if $c \in \mathbb{Z}_7^\times$ then $c^b = 4c$. Further, $c^{b^2} = (c^b)^b = (4c)^b = 4(4c) = 16c = 2c$ and $c^{b^3} = (c^{b^2})^b = (2c)^b = 8c = c$. Then the conjugacy classes of $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ that will be contained in $\mathbb{Z}_7$ are $\{0\}, \{1,4,2\}, \{3,5,6\}$ since $1 \cdot 4 \equiv 4$, $4 \cdot 4 \equiv 2$, $2 \cdot 4 \equiv 1$ and $3 \cdot 4 \equiv 5$, $5 \cdot 4 \equiv 6$, $6 \cdot 4 \equiv 3$ modulo 7. Note that it was necessary for $c^{b^3} = c$ since b^3 is the identity. In conclusion, the group $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ would be defined as follows:

- Since $\mathbb{Z}_7, \mathbb{Z}_3$ are cyclic, there exist additive generators a, b such that $\mathbb{Z}_7 = \langle a \rangle$ and $\mathbb{Z}_3 = \langle b \rangle$.
- If $g \in \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ then there are unique $i \in \mathbb{Z}_7$ and $j \in \mathbb{Z}_3$ such that $g = ia + jb$.
- $a + b = b - b + a + b = b + a^b = b + (4a)$

Let us now consider defining one type of semidirect product in general. Let G be the set defined as the semidirect product of two of its subgroups C_p and C_q where the following are satisfied:

- p, q be prime such that $p \equiv 1 \bmod q$
- $C_p = \langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{p-1}\}$
- $C_q = \langle b \rangle = \{b^0, b^1, b^2, \ldots, b^{q-1}\}$
- If $g \in G$ then there are unique $0 \le \alpha < p$ and $0 \le \beta < q$ such that $g = a^\alpha b^\beta$.
- Taking motivation from the additive case, let x be the integer corresponding to a multiplicative generator of $\mathbb{Z}_p^\times$ and $m = x^{\frac{p-1}{q}}$. So the order of m is q.
- Define the action *(proof below)* of the group to be $(a^i)^{(b^j)} = a^{im^j}$.

We will prove G is a group in Theorem 2. This group could be alternatively defined by its generators a, b so that $G = \{a^\alpha b^\beta : 0 \le \alpha < p \text{ and } 0 \le \beta < q\}$. Note that the definition implies $D_{2p} = C_p \rtimes C_2$. So, elements of the form a^i are generalized rotations and elements of the form a^ib^j for nonzero j are generalized flips.

Lemma 1. *$(a^i)^{(b^j)} = a^{im^j}$ defines an action on C_p by C_q.*

Proof. First, we must show that G is closed under the action. Note that since i, m, j are all integers, $a^{im^j} \in G$, so G is closed under the action.

Further, we must show that action by the identity preserves the element. Since $(a^i)^e = (a^i)^{b^0} = a^{im^0} = a^{i(1)} = a^i$, this property holds.

Finally, we must show that $((a^i)^{b^j})^{b^k} = (a^i)^{b^jb^k}$. Since, $((a^i)^{b^j})^{b^k} = (a^{im^j})^{b^k} = a^{(im^j)m^k} = a^{im^{j+k}} = (a^i)^{b^{j+k}} = (a^i)^{b^jb^k}$, we have satisfied all conditions and $(a^i)^{b^j} = a^{im^j}$ defines an action on C_p by C_q. $\square$

It is noteworthy to mention that since G is closed and $a, b \in G$, then $b^ia^j \in G$, but this does not follow how the group is defined. However, using properties $ab = ba^m$ and $ba = a^{m^{-1}}b$, we will be able to reorder or "alphabetize" any element. Recall that the trivial subgroup is denoted T and contains only the identity, in this case $T = \{a^0b^0\}$. For future reference, let us consider how to change the order of representation for a general element $g = a^ib^j \in G$.

$$g = a^ib^j = b^jb^{-j}a^ib^j = b^j(a^i)^{b^j} = b^ja^{im^j}$$

Similarly, any element of the form $g' = b^ja^i \in G$ can be alphabetized. Note that m will have a multiplicative inverse in $\mathbb{Z}_p$ since p is prime. Then,

$$g' = b^ja^i = b^ja^{i(m^{-1})^jm^j} = b^j(a^{i(m^{-1})^j})^{b^j} = b^jb^{-j}a^{i(m^{-1})^j}b^j = a^{i(m^{-1})^j}b^j$$

Thus we are able to reorder any element. We now hold the tools to show that this semidirect product is a group.

Theorem 2. *Let G be defined as the semidirect product of C_p and C_q as above. Then G is a group.*

Proof. Let G be defined as the semidirect product of C_p and C_q as above. To show that G is a group, we must show it has identity, has inverses, its operation is associative, and is closed under the operation.

Clearly, a^0b^0 is the identity.

For inverses, what we want for an element $g = a^ib^j$ is an element $g' = b^{-j}a^{-i}$. Then

$$gg' = a^ib^jb^{-j}a^{-i} = a^iea^{-i} = e = b^{-j}b^j = b^{-j}a^{-i}a^ib^j = g'g.$$

Now, all we need to do is alphabetize g', and we're done. Note from above that $g' = a^{-i(m^{-1})^{-j}}b^{-j}$. Now lets check and show that g' is still an appropriate inverse choice:

$$gg' = a^i(b^j a^{-i(m^{-1})^{-j}})b^{-j} = a^i(a^{-i(m^{-1})^{-j}(m^{-1})^j}b^j)b^{-j} = a^i(a^{-i}b^j)b^{-j} = e$$

$$g'g = a^{-i(m^{-1})^{-j}}(b^{-j}a^i)b^j = a^{-i(m^{-1})^{-j}}(a^{i(m^{-1})^{-j}}b^{-j})b^j = e.$$

Thus G has inverses.

For associativity, consider $g = a^i b^j$, $h = a^k b^l$ and $f = a^s b^t$. Then

$$\begin{aligned}
(gh)f &= (a^i b^j a^k b^l)a^s b^t \\
&= (a^i a^{k(m^{-1})^j} b^j b^l)a^s b^t \\
&= a^{i+k(m^{-1})^j} b^{j+l} a^s b^t \\
&= a^{i+k(m^{-1})^j} a^{s(m^{-1})^{j+l}} b^{j+l} b^t \\
&= a^{i+k(m^{-1})^j + s(m^{-1})^{j+l}} b^{j+l+t}.
\end{aligned}$$

Further,

$$\begin{aligned}
g(hf) &= a^i b^j (a^k b^l a^s b^t) \\
&= a^i b^j (a^k a^{s(m^{-1})^l} b^l b^t) \\
&= a^i b^j a^{k+s(m^{-1})^l} b^{l+t} \\
&= a^i a^{(k+s(m^{-1})^l)(m^{-1})^j} b^j b^{l+t} \\
&= a^i a^{k(m^{-1})^j + s(m^{-1})^{j+l}} b^{j+l+t} \\
&= a^{i+k(m^{-1})^j + s(m^{-1})^{j+l}} b^{j+l+t}.
\end{aligned}$$

Thus $(gh)f = a^{i+k(m^{-1})^j+s(m^{-1})^{j+l}} b^{j+l+t} = g(hf)$. So the operation of G is associative.

For closure, let $g, h \in G$, then $g = a^i b^j$ and $h = a^k b^l$ for some integers i, j, k, l. Then $gh = a^i b^j a^k b^l = a^i a^{k(m^{-1})^j} b^j b^l = a^{i+k(m^{-1})^j} b^{j+l}$. Since i, k, m^{-1}, j are integers, so is $i + k(m^{-1})^j$. Since j, l are integers, so is $j + l$. Thus $gh \in G$. So G is closed.

Therefore, G is a group. $\square$

5. Common Theorems

THEOREM 3. *Let G be a group. Then G and the trivial subgroup $T = \{e\}$ are normal.*

PROOF. Let G be a group with identity e. Then $T = \{e\}$ is the trivial subgroup. Let $g \in G$. Then $g^{-1} \in G$. Since $g^{-1}e = g^{-1}g = e \in T$, the trivial subgroup is normal.

Consider the normality of G. Since G is closed, if $h \in G$ then $g^{-1}hg \in G$. Thus G is normal. Therefore the trivial and improper subgroups of a group are normal, as desired. □

THEOREM 4. *Let G be a group Let p be the smallest prime dividing the order of G. If H is a subgroup of index p then H is normal in G.*

PROOF. The proof can be found in [**1**]. □

THEOREM 5. *If G is a group, then the direct product $G \times G$ is a group under component-wise multiplication.*

PROOF. If $e \in G$ is the identity in G then we will show that $(e, e) \in G \times G$ is the identity. Let $(g, h) \in G \times G$, then $g, h \in G$, so $ge = eg = g$ and $eh = he = h$. Thus $(e, e)(g, h) = (eg, eh) = (g, h) = (ge, he) = (g, h)(e, e)$. Therefore (e, e) is the identity in $G \times G$.

Let $(g, h) \in G \times G$. Then there are $g^{-1}, h^{-1} \in G$ so that $gg^{-1} = g^{-1}g = e = hh^{-1} = h^{-1}h$. Since $(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e, e) = (g^{-1}g, h^{-1}h) = (g^{-1}, h^{-1})(g, h)$, it follows that $(g^{-1}, h^{-1}) = (g, h)^{-1}$, so $G \times G$ has inverses.

Let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times G$. Now for associativity, consider

$$[(g_1, h_1)(g_2, h_2)](g_3, h_3) = (g_1g_2, h_1h_2)(g_3, h_3) = ((g_1g_2)g_3, (h_1h_2)h_3).$$

Since the operation of G is associative,

$$(g_1(g_2g_3), h_1(h_2h_3)) = (g_1, h_1)(g_2g_3, h_2h_3) = (g_1, h_1)[(g_2, h_2)(g_3, h_3)].$$

Thus

$$[(g_1, h_1)(g_2, h_2)](g_3, h_3) = (g_1, h_1)[(g_2, h_2)(g_3, h_3)],$$

so $G \times G$ is associative under component-wise multiplication.

For closure, let $(g_1, h_1), (g_2, h_2) \in G \times G$. Then $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$, since G is closed, $g_1g_2 \in G$ and $h_1h_2 \in G$. Therefore $(g_1g_2, h_1h_2) \in G \times G$. So $G \times G$ is closed.

Thus, $G \times G$ is a group, as desired.

□

THEOREM 6. *If M, N are normal in G, then $M \times N$ is normal in $G \times G$.*

Proof. Let M, N be normal in G. Let $(m, n) \in M \times N$ and $(g_1, g_2) \in G \times G$. Then $m \in M$, $n \in N$, $g_1, g_2, g_1^{-1}, g_2^{-1} \in G$, and $(g_1^{-1}, g_2^{-1}) \in G \times G$. Since $(g_1, g_2)(g_1^{-1}, g_2^{-1}) = (g_1 g_1^{-1}, g_2 g_2^{-1}) = (e, e) = (g_1^{-1} g_1, g_2^{-1} g_2) = (g_1^{-1}, g_2^{-1})(g_1, g_2)$. It follows that $(g_1^{-1}, g_2^{-1}) = (g_1, g_2)^{-1}$.

For the normality of $M \times N$, consider $(g_1^{-1}, g_2^{-1})(m, n)(g_1, g_2) = (g_1^{-1} m g_1, g_2^{-1} n g_2)$. Since M is normal it follows that $g_1^{-1} m g_1 \in M$. Since N is normal it follows that $g_2^{-1} n g_2 \in N$. Thus $(g_1^{-1} m g_1, g_2^{-1} n g_2) \in M \times N$ and $M \times N$ is normal in $G \times G$, as desired. $\square$

Corollary 7. *If G has k normal subgroups, then $G \times G$ has at least k^2 normal subgoups.*

Proof. Let G be a group with k normal subgroups. Consider all subgroups of $G \times G$ that are of the form $M \times N$ where M, N are normal in G. Since the selection of M and N for any $M \times N \subseteq G \times G$ is independent, and there are k options for each it follows that there are at least k^2 normal subgroups in $G \times G$. $\square$

CHAPTER 2

Dihedral Groups

A dihedral group of order $2m$ is the set of symmetries on a regular m-gon. The dihedral group can be generated by two elements, a rotation (r) and a flip (f). The following are well known facts and will be stated without proof: $(r^j)^{-1} = r^{-j}$ and $r^k f = fr^{-k}$. Since there is a defined way of reordering the rotations and flips, we can define D_{2m} in the following way. This group can be defined as $D_{2m} = \{r^i f^j : i \in \mathbb{Z}_m \text{ and } j \in \mathbb{Z}_2\}$. For the remainder of the chapter, we consider the prime factorization of m to be $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$

1. D_{2m} for odd m

It is known by [**2**] that if H is a proper subgroup of a dihedral group of order $2k$, then H is normal in D_{2k} if and only if $H \leq C_k = \{r^i : i \in \mathbb{Z}_k\}$ or $2|k$ and H is a special maximal subgroup. A subgroup is *maximal* if no proper subgroup contains it. Since we are dealing with odd m it follows that $2 \not| \, m$ and the second part of this theorem will not apply.

COROLLARY 8. *If H is a proper subgroup of D_{2m} where m is odd, then H is normal if and only if $H = C_a$ for some $a|m$.*

PROOF. Since $2 \not| \, m$, H is normal in D_{2m} if and only if $H \leq C_m$. Thus the order of H must divide m, and the subgroup will be cyclic. Therefore H is normal in D_{2m} if and only if $H = C_a$ for some $a|m$. $\square$

Let us now consider the prime factorization of m which can be written as $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ for some primes p_μ and positive integers α_μ.

LEMMA 9. *Let $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ be odd. Then there are $\prod_{\mu=1}^{M}(\alpha_\mu + 1)$ proper normal subgroups of D_{2m}.*

PROOF. The maximal cyclic subgroup of D_{2m} is isomorphic to C_m and has order m. Thus if H is a subgroup of C_m the order of H must be some a such that $a|m$ by Lagrange's Theorem. So the prime factorization of a must be $a = \prod_{\mu=1}^{M} p_\mu^{\beta_\mu}$ such that $0 \leq \beta_\mu \leq \alpha_\mu$ for all μ. Thus there are $\alpha_\mu + 1$ options for the power of p_μ. Note that this calculation will include the trivial subgroup when all β_i are zero. Therefore there are $\prod_{\mu=1}^{M}(\alpha_\mu + 1)$ such orders and thus $\prod_{\mu=1}^{M}(\alpha_\mu + 1)$ proper normal subgroups of D_{2m}. $\square$

THEOREM 10. *Let* $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ *be odd. There are exactly* $1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1)$ *normal subgroups of* D_{2m}.

PROOF. By Theorem 3, D_{2m} is normal. By Lemma 9 there are $\prod_{\mu=1}^{M}(\alpha_\mu + 1)$ proper normal subgroups of D_{2m}. Thus there are exactly $1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1)$ normal subgroups of D_{2m}. $\square$

COROLLARY 11. *The number of normal subgroups of* $D_{2m} \times D_{2m}$ *is greater than or equal to* $(1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1))^2$ *where* $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ *is odd.*

PROOF. By Theorem 10 there are exactly $1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1)$ normal subgroups of D_{2m}. By Corollary 7 there are at least k^2 normal subgroups of $G \times G$ when there are k normal subgroups of G. Thus the number of normal subgroups of $D_{2m} \times D_{2m}$ is greater than or equal to $(1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1))^2$. $\square$

2. $D_{2m} \times D_{2m}$ for odd m

The following series of lemmas will be used to exhaustively pinpoint how many normal subgroups are in $D_{2m} \times D_{2m}$ for odd m. In D_{2m}, the only proper normal subgroups are cyclic. If r^i is present in a normal subgroup, then all multiples of that rotation are present in that subgroup. Thus, if r^i is in the normal subgroup denoted by N and $k = \frac{m}{\gcd(i,m)}$, then k is the order of r^i. Further, by Lagrange's Theorem, it follows that k divides the order of N. In other terms, a group isomorphic to C_k is a subgroup of N. Note that since $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$, there are $(\prod_{\mu=1}^{M}(\alpha_\mu + 1)) - 1$ options for k.

I will show the following theorem:

Theorem 12. *If $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ is odd, then there are $(1+\prod_{\mu=1}^{M}(\alpha_\mu + 1))^2 + 1$ normal subgroups of $D_{2m} \times D_{2m}$.*

This value is the lower bound shown above in Corollary 11 plus 1. This extra subgoup will come from a special group that has a index 2 in D_{2m}, this means it contains exactly half of the elements of D_{2m}.

This special group can be described by a semidirect product, namely $(C_m \times C_m) \rtimes C_2$. Note that $(C_m \times C_m) \rtimes C_2 = \{(r^i f^x, r^j f^x) : 0 \leq i, j < m \text{ and } 0 \leq x < 2\}$. In other terms, either both components have a flip, or neither do. This subgroup is the only one that does not follow the form of normal subgroups shown in Theorem 6. Looking at each of the components of the tuple individually for this group we see that each includes all elements from D_{2m}, but they are connected in an unusual way. This group is key in showing why Theorem 6 is not a tight lower bound.

Before we get around to showing the normal subgroups of $D_{2m} \times D_{2m}$, let us consider a few helpful theorems. First we will show that this special group that was just mentioned is, in fact, normal. Then we will show a nice property that allows us to go between generalized flips, and a particular flip.

Lemma 13. *Let m be odd. Then $(C_m \times C_m) \rtimes C_2$ is normal in $D_{2m} \times D_{2m}$.*

Proof. Since this subgroup has index 2 in $D_{2m} \times D_{2m}$ it is normal in $D_{2m} \times D_{2m}$, as desired. □

Lemma 14. *Let m be odd, let N be normal in $D_{2m} \times D_{2m}$ and let i, j be integers. Then $(r^i f, r^j f) \in N$ if and only if $(f, f) \in N$.*

Proof. Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. Suppose $(r^i f, r^j f) \in N$. Note that since m is odd, 2 has a multiplicative inverse modulo m, call it τ. Then since N is normal, we can conjugate $(r^i f, r^j f)$ by $(r^{i\tau}, r^{j\tau})$. So that

$$\begin{aligned}
(r^i f, r^j f)^{(r^{i\tau}, r^{j\tau})} &= (r^{-i\tau}, r^{-j\tau})(r^i f, r^j f)(r^{i\tau}, r^{j\tau}) \\
&= (r^{-i\tau} r^i f r^{i\tau}, r^{-j\tau} r^j f r^{j\tau}) \\
&= (r^{-i\tau} r^i r^{-i\tau} f, r^{-j\tau} r^j r^{-j\tau} f) \\
&= (r^{-i\tau+i-i\tau} f, r^{-j\tau+j-j\tau} f) \\
&= (r^{i-i2\tau} f, r^{j-j2\tau} f) \\
&= (f, f) \in N.
\end{aligned}$$

Thus if $(r^i f, r^j f) \in N$ then $(f, f) \in N$.

Suppose $(f, f) \in N$. Then since N is normal, we can conjugate (f, f) by $(r^{-i\tau}, r^{-j\tau})$. So then

$$\begin{aligned}
(f, f)^{(r^{-i\tau}, r^{-j\tau})} &= (r^{i\tau}, r^{j\tau})(f, f)(r^{-i\tau}, r^{-j\tau}) \\
&= (r^{i\tau} f r^{-i\tau}, r^{j\tau} f r^{-j\tau}) \\
&= (r^{i\tau} r^{-i\tau} f, r^{j\tau} r^{j\tau} f) \\
&= (r^{i2\tau} f, r^{j2\tau} f) \\
&= (r^i f, r^j f) \in N.
\end{aligned}$$

Thus if $(f, f) \in N$ then $(r^i f, r^j f) \in N$.

Therefore $(f, f) \in N$ if and only if $(r^i f, r^j f) \in N$, as desired. □

Corollary 15. *Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. If $(f, f) \in N$, then $(r^s f, r^t f) \in N$ for all s, t.*

Proof. This can be shown by replacing the conjugation of (f, f) by $(r^{-i\tau}, r^{-j\tau})$, with conjugation of (f, f) by $(f^{-s\tau}, r^{-t\tau})$ in the second part of the proof. □

Corollary 16. *Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. Then $(x, r^j f) \in N$ for some integer j and some $x \in D_{2m}$ if and only if $(x, f) \in N$.*

Proof. This can be shown by replacing the conjugation of $(r^i f, r^j f)$ by $(r^{i\tau}, r^{j\tau})$ with conjugation of $(x, r^j f)$ by $(e, r^{j\tau})$ and by replacing the conjugation of (f, f) by $(r^{-i\tau}, r^{-j\tau})$, with conjugation of (x, f) by $(e, r^{-j\tau})$. □

The proofs of the following corollaries are similar.

Corollary 17. *Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. If $(x, f) \in N$ for some $x \in D_{2m}$, then $(x, r^t f) \in N$ for all t.*

COROLLARY 18. *Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. Then $(r^i f, x) \in N$ for some integer i and some $x \in D_{2m}$ if and only if $(f, x) \in N$.*

COROLLARY 19. *Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. If $(f, x) \in N$ for some $x \in D_{2m}$, then $(r^s f, x) \in N$ for all s.*

By Theorem 6, and Lemma 13 we have shown that if $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ is odd, then there are at least $(1+\prod_{\mu=1}^{M}(\alpha_\mu+1))^2+1$ normal subgroups of $D_{2m} \times D_{2m}$. Now we will show exhaustively, through cases, that there are no more than $(1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1))^2 + 1$ normal subgroups of $D_{2m} \times D_{2m}$.

Let N be normal in G. I will determine the number of normal subgroups by exhaustion based on which elements are known to be in N. Recall that $D_{2m} \times D_{2m} = \{(r^i f^x, r^j f^y) : 0 \leq i, j \leq m-1 \text{ and } 0 \leq x, y \leq 1\}$ and that N is a normal subgroup of $D_{2m} \times D_{2m}$. All cases to be used in these lemmas are outlined below:

a) There is a flip in both components. In other terms, $(f, f) \in N$. Note that it was shown above that $(r^i f, r^j f) \in N$ if and only if $(f, f) \in N$.
   - There will be 2 such groups, one isomorphic to $D_{2m} \times D_{2m}$ and the other isomorphic to $(C_m \times C_m) \rtimes C_2$.

b) There is an element with a flip in the second component but there are no elements with a flip in the first component. In other terms, $(r^i, r^j f) \in N$ for some integers i, j and $(f, f) \notin N$
   - There will be $\left(\prod_{\mu i=1}^{M}(\alpha_\mu + 1)\right)$ such groups, each isomorphic to $C_k \times D_{2m}$ for some value of k.

c) There is an element with a flip in the first component but there are no elements with a flip in the second component. In other terms, $(r^i f, r^j) \in N$ for some integers i, j, and $(f, f) \notin N$
   - There will be $\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right)$ such groups, each isomorphic to $D_{2m} \times C_l$ for some value of l.

d) There is not a flip in either component. In other terms, $(r^i, r^j) \in N$ for some integers i, j and $(e, f), (f, e), (f, f) \notin N$.
   - There will be $\left(\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right)\right)^2$ such groups, each isomorphic to $C_k \times C_l$ for some k and l.

Consider case *b)* notice that there does not seem to be a hint as to what k is. Clearly, k must divide m. But how do we decide what k must be just by knowing what i is? We will do this by being more specific about the value of i that is chosen. Note that $C_k = \{r^{\alpha d} : \alpha \in \mathbb{Z}\}$

where $d = \gcd\{j : (r^j, x) \in D_{2m} \times D_{2m}\}$ We will specify cases by the minimum value of $0 < i \le m$ that shows up in the form $(r^i, r^j f)$. Since all integers divide 0, by using the above range for i, we see that $d = i$. Thus in the following cases, the assumption that $(r^i, r^j f) \in N$ for some integer j and some minimal integer i will cover all cases. Note that with the case determined by that minimal integer i (which is d) that $(r^s, x) \in N$ implies that s is a multiple of i.

Now let us start proving these theorems. In general, we will start by isolating the rotations or flips for a component of an element in the normal subgroup, denoted N. This will allow us to show that a certain subgroup, call it H, of $D_{2m} \times D_{2m}$ is a subset of N. We will then assume there is an element in N that is not in H and arrive at a contradiction. This will show us that $N = H$.

Lemma 20. *Let N be normal in $D_{2m} \times D_{2m}$ where m is odd. If $(f, f) \in N$ then $N = D_{2m} \times D_{2m}$ or $N = (C_m \times C_m) \rtimes C_2$.*

Proof. Let N be normal in $D_{2m} \times D_{2m}$ and let $(f, f) \in N$. Note from above that $(f, f) \in N$ if and only if $(r^i f, r^j f) \in N$ for any integers i, j. Further, by closure $(r^i, r^j) = (r^i f, r^j f)(f, f) \in N$. Thus $\{(r^i f^x, r^j f^x) : 0 \le i, j < m \text{ and } 0 \le x < 2\} = (C_m \times C_m) \rtimes C_2 \subseteq N$.

I will consider two cases: $(e, f) \in N$ and $(e, f) \notin N$. Suppose that $(e, f) \notin N$. Since $(C_m \times C_m) \rtimes C_2 \subseteq N < D_{2m} \times D_{2m}$ and $(C_m \times C_m) \rtimes C_2$ has index 2 in $D_{2m} \times D_{2m}$, it follows that $N = (C_m \times C_m) \rtimes C_2$. Suppose that $(e, f) \in N$. Then $(C_m \times C_m) \rtimes C_2 < N \subseteq D_{2m} \times D_{2m}$. Since $(C_m \times C_m) \rtimes C_2$ has index 2 in $D_{2m} \times D_{2m}$, it follows that $N = D_{2m} \times D_{2m}$. $\square$

Lemma 21. *Let m be odd and let N be normal in $D_{2m} \times D_{2m}$. If the following hold:*

1. *$(r^i, r^j f) \in N$ for some integer j and some minimal integer i*
2. *$(r^s, y) \in N$ for some $0 \le s < m$ and $y \in D_{2m}$ implies s is a multiple of i*
3. *$(f, f) \notin N$*

then $N = C_k \times D_{2m}$ for some k.

Proof. Let m be odd. Let N be normal in $D_{2m} \times D_{2m}$ such that it satisfies the hypothesis. Let $k = m/\gcd(m, i)$. Note that k is the order of r^i.

Consider the elements of N. First notice that by closure $(r^i, r^j f)^2 = (r^{2i}, e) \in N$. Since $\gcd(2, m) = 1$ it follows that all elements of the form (r^{ci}, e) for any integer c are in N. Similarly, $(r^{ci}, r^j f) \in N$ for any integer c. Through conjugation by (e, r^a) on $(r^{ci}, r^j f)$, we see that $(r^{ci}, r^{j-2a} f) = (r^{ci}, r^j f)^{(e, r^a)} \in N$. Since a was arbitrary and m is odd, we see that $(r^{ci}, r^l f) \in N$ for any integers c, l. Taking $c = 0$ and $l = 0$, we see that $(e, f) \in N$. Then by closure $(r^{ci}, r^l) = (r^{ci}, r^l f)(e, f) \in N$ for all integers c, l. Further, $(r^{ci}, r^l f^y) \in N$ for any integers c, l, y. Thus, $C_k \times D_{2m} \subseteq N$.

Suppose for contradiction that there was some element $(r^s f^t, r^u f^v) \notin C_k \times D_{2m}$ such that $(r^s f^t, r^u f^v) \in N$. Since all elements of D_{2m} are possible in the second component, it follows that either s is not a multiple of i or $t = 1$. Suppose $t = 0$; then s is not a multiple of i. This contradicts the hypothesis. Therefore $t = 1$ and $(r^s f, r^u f^v)$ is our element. Note that there is some s_i such that $s + s_i \equiv 0 \bmod m$. Since m is odd, 2 has a multiplicative inverse, call it τ. Next, conjugate $(r^s f^t, r^u f^v)$ by $(r^{-\tau s_i}, e)$. So

$$\begin{aligned}(r^s f, r^u f^v)^{(r^{-\tau s_i}, e)} &= (r^{\tau s_i}, e)(r^s f^t, r^u f^v)(r^{-\tau s_i}, e)\\ &= ((r^{s+2\tau s_i} f, r^u f^v)\\ &= (f, r^u f^v).\end{aligned}$$

Since N is closed under conjugation, $(f, r^u f^v) \in N$. However,

$$(e, (r^u (f^v)^{-1})), (e, f) \in C_k \times D_{2m} \subseteq N.$$

Thus by closure $[(f, r^u f^v)(e, (r^u (f^v)^{-1}))](e, f) = (f, e)(e, f) = (f, f) \in N$ which contradicts the hypothesis.

Therefore $N = C_k \times D_{2m}$. $\square$

Corollary 22. *Let m be odd. Let N be normal in $D_{2m} \times D_{2m}$. If the following hold:*

(1) *$(r^i f, r^j) \in N$ for some integer j and some minimal integer j*
(2) *$(x, r^t) \in N$ for some $0 \leq t < m$ and $x \in D_{2m}$ implies t is a multiple of j*
(3) *$(f, f) \notin N$*

then $N = D_{2m} \times C_k$ for some k.

Proof. This holds by symmetry of Lemma 21. $\square$

Lemma 23. *Let m be odd. Let N be normal in $D_{2m} \times D_{2m}$. If the following hold:*

(1) *$(r^i, r^j) \in N$ for some minimal integers i, j*
(2) *$(r^s, y) \in N$ for some $0 \leq s < m$ and $y \in D_{2m}$ implies s is a multiple of i*
(3) *$(x, r^t) \in N$ for some $0 \leq t < m$ and $x \in D_{2m}$ implies t is a multiple of j*
(4) *$(e, f), (f, e), (f, f) \notin N$*

then $N = C_k \times C_l$ for some integers k, l.

Proof. Let m be odd. Let N be normal in $D_{2m} \times D_{2m}$ such that the hypothesis is satisfied. Let $k = m/\gcd(m,i)$ and $l = m/\gcd(m,j)$. Note that k is the order of r^i and l is the order of r^j.

Conjugating (r^i, r^j) by (e, f) gives $(r^i, fr^jf) = (r^i, f^2r^{-j})$ $= (r^i, r^{-j}) \in N$. Now, since N is closed, it follows that $(r^i, r^j)(r^i, r^{-j}) = (r^{2i}, e) \in N$. Since $\gcd(2, m) = 1$, for any integer c it follows that $(r^{ci}, e) \in N$. Note that there will be k options for c before repetitions since $m/\gcd(m,i) = k$. Similarly, for any integer d it follows that $(e, r^{dj}) \in N$. Also note that there will be l options for d before repetitions since $m/\gcd(m,j) = l$. Thus, by closure, elements of the form (r^{ci}, r^{dj}) are in N for any c, d. So $C_k \times C_l \subseteq N$.

Suppose for contradiction that there was some element of the form $(r^sf^t, r^uf^v) \in N$ where s or u are not multiples of i and j respectfully or where t or v are nonzero. If t is zero, then s must be a multiple of i in order to satisfy condition two of the hypothesis; if v is zero, then u must be a multiple of j to satisfy condition three of the hypothesis. So at least one of t or v is nonzero. Suppose without loss of generality that $t = 1$. Note that there is some s_i such that $s + s_i \equiv 0 \bmod m$. Since m is odd, 2 has a multiplicative inverse in $\mathbb{Z}_m$, call it τ. Now lets conjugate (r^sf, r^uf^v) by $(r^{-\tau s_i}, e)$. So $(r^{\tau s_i}, e)(r^sf, r^uf^v)(r^{-\tau s_i}, e) = ((r^{s+2\tau s_i}f, r^uf^v) = (f, r^uf^v)$. Now, suppose $v = 0$, then u is a multiple of j. Then we can multiply by (e, r^{-u}) which will be in N since $-u$ will also be a multiple of j. So by closure, $(f, r^u)(er^{-u}) = (f, e) \in N$ which contradicts condition five of the hypothesis. So $v = 1$. We can find u_i such that $u + u_i \equiv 0 \bmod m$. Now consider $(r, r^uf)^{(e, r^{-\tau u_i})} = (e, r^{\tau u_i})(f, r^uf)(e, r^{-\tau u_i}) = (f, r^{u+2\tau u_i}f) = (f, f) \in N$. This gives $(f, f) \in N$ which is a contradiction.

Thus, $N = C_k \times C_l$. $\square$

Theorem 24. *If N is normal in $D_{2m} \times D_2$ where m is odd then N must be one of the following:*

$$\begin{array}{ll} D_{2m} \times D_{2m} & D_{2m} \times C_l \\ C_k \times D_{2m} & C_k \times C_l \\ (C_m \times C_m) \rtimes C_2 & \end{array}$$

Proof. Lemmas 20, 21, 23 and Corollary 22 show exhaustively that these are the normal subgroups of $D_{2m} \times D_{2m}$. $\square$

Theorem 25. *There are $(1 + \prod_{\mu=1}^{M}(\alpha_\mu + 1))^2 + 1$ normal subgroups of $D_{2m} \times D_{2m}$ where $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ is odd.*

PROOF. This follows directly Theorem 24.

Normal Subgroup Category	Number in Category
$D_{2m} \times D_{2m}$	1
$D_{2m} \times C_l$	$\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right)$
$C_k \times D_{2m}$	$\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right)$
$C_k \times C_l$	$\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right)^2$
$(C_m \times C_m) \rtimes C_2$	1

The total of the right column is

$$\left(\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right)^2 + 2\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right) + 1\right) + 1$$

$$= \left(\left(\prod_{\mu=1}^{M}(\alpha_\mu + 1)\right) + 1\right)^2 + 1.$$

Hence there are $(1+\prod_{\mu=1}^{M}(\alpha_\mu+1))^2+1$ normal subgroups of $D_{2m}\times D_{2m}$ when $m = \prod_{\mu=1}^{M} p_\mu^{\alpha_\mu}$ is odd. $\square$

CHAPTER 3

Semidirect Products

Let us now consider a generalization of the Dihedral Group. We defined, in the background section, a semidirect product of two cyclic groups to mimic the structure of a dihedral group. Recall that $G = \{a^\alpha b^\beta : 0 \leq \alpha < p \text{ and } 0 \leq \beta < q\}$ with action $(a^i)^{b^j} = a^{im^j}$. With motivation from the Dihedral Group, a's are generalized rotations and the $b's$ are generalized flips. Finally, recall that we can change the order so that $a^i b^j = b^j a^{im^j}$ and $b^j a^i = a^{i(m^{-1})^j} b^j$.

1. $G = C_p \rtimes C_q$ where prime $p \equiv 1 \bmod q$ with q prime

For the remainder of the chapter, the following notation will be employed:
$G = C_p \rtimes C_q = \{a^\alpha b^\beta : 0 \leq \alpha < p \text{ and } 0 \leq \beta < q\}$ where

- a^α are generalized rotations
- $a^\alpha b^\beta$ for $\beta \neq 0$ are generalized flips
- p, q are prime such that $p \equiv 1 \bmod q$.

Lemma 26. *Let N be a normal subgroup of G. If $b \in N$ then $N = G$.*

Proof. Let N be a normal subgroup of G where $G = C_p \rtimes C_q$. Let x be a multiplicative generator of C_p and $m = x^{\frac{p-1}{q}}$ (the order of m is q). Let $b \in N$. Since N is closed $b^\beta \in N$ for all $0 \leq \beta < q$. Since N is normal, then $b^{a^m} \in N$. So $b^{a^m} = a^{-m} b a^m = a^{-m} ab = a^{1-m} b \in N$. Since N is closed $a^{1-m} b b^{q-1} = a^{1-m} \in N$. Since p is prime and $m \neq 1$, it follows that $a^\alpha \in N$ for all $0 \leq \alpha < p$. Finally, since N is closed $a^\alpha b^\beta \in N$ for all $0 \leq \alpha < p$ and $0 \leq \beta < q$. Thus since N contains all elements of G, it follows that $N = G$. $\square$

Lemma 27. *Let N be a normal subgroup of G. If $b \notin N$ then $N = C_p$ or $N = T$.*

Proof. We will consider two cases: $a \in N$ and $a \notin N$. Let $a \in N$. Then $a^\alpha \in N$ for all $0 \leq \alpha < p$ since N is closed. Suppose for contradiction that $a^i b^j \in N$ for some $0 \leq i < p$ and nonzero $0 \leq j < q$. Since q is prime there exists some $0 \leq k < q$ such that $kj \equiv 1 \bmod q$.

Similarly, there exists some $0 \leq l < p$ such that $i + l \equiv 0 \bmod p$. Then since N is closed and $a^l, a^i b^j \in N$, it follows that $a^l(a^i b^j) = a^{l+i} b^j = b^j \in N$. Thus $b^{kj} = b \in N$ and we have a contradiction. Therefore if $a^i b^j \in N$ then $j = 0$. Since all elements of the form a^α are in N it follows that $N = C_p$.

Consider the second case such that $a \notin N$. Since p is prime, it follows that $a^\alpha \notin N$ for $0 \neq \alpha \in N$. Suppose for contradiction that $a^i b^j \in N$ for some nonzero $0 \leq i < p$ or nonzero $0 \leq j < q$. If $i = 0$, then $j \neq 0$ and $b^j \in N$, which implies $b \in N$ since q is prime. This is a contradiction. If $j = 0$, then $i \neq 0$ and $a^i \in N$ which is a contradiction.

Therefore $i \neq 0$ and $j \neq 0$. Define $0 \leq l < p$ so that $l \equiv (m^{-1})^j - 1 \bmod p$. Note that $l = 0$ implies that $(m^{-1})^j = 1$. However, this implies that $j = 0$ which is a contradiction, so $l \neq 0$. Since p is prime, l^{-1} exists, so we can find a k such that $k \equiv -il^{-1} \bmod p$. So then $kl + i \equiv 0$. Now, since N is normal, we can conjugate by any element in G, so conjugate by a^k. Then

$$\begin{aligned}(a^i b^j)^{a^k} &= a^{-k} a^i b^j a^k = a^{i-k} b^j a^k = a^{i-k+k(m^{-1})^j} b^j \\ &= a^{k((m^{-1})^j - 1) + i} b^j = a^{kl+i} b^j = a^0 b^j = b^j \in N.\end{aligned}$$

Thus $b \in N$, which is a contradiction. Therefore $N = T$.

Thus $N = C_p$ or $N = T$, as desired. □

THEOREM 28. *There are exactly* 3 *normal subgroups of* G *where* $G = C_p \rtimes C_q$.

PROOF. Lemma's 26 and 27 show exhaustively that there are three normal subgroups of G. □

COROLLARY 29. *The number of normal subgroups of* $G \times G$ *is greater than or equal to* 9.

PROOF. By Theorem 28 there are exactly 3 normal subgroups of G. By Corollary 7 there are at least k^2 normal subgroups of $G \times G$ when there are k normal subgroups of G. Thus the number of normal subgroups of $G \times G$ is greater than or equal to 9. □

2. $G \times G$ where $G = C_p \rtimes C_q$ when prime $p \equiv 1 \bmod q$ with q prime

The following series of lemmas will be used to exhaustively pinpoint how many normal subgroups are in $G \times G$ where $G = C_p \rtimes C_q$. I will show that there are $9 + (q - 1)$ normal subgroups of $G \times G$. The 9 are the expected groups from simply taking the direct products of normal subgroups of G. The other $q - 1$ subgroups are related to the special normal subgroup of the dihedral group mentioned in the section regarding D_{2m} for odd m. In that normal subgroup, which was isomorphic to $(C_m \times C_m) \rtimes C_2$, we saw that either both components of the tuple had a flip, or neither did. In the special normal subgroups of $G \times G$, we will see a fixed relationship between the exponent of b in the first component of the tuple and the second component of the tuple. This special normal subgroup will be denoted as $(C_p \times C_p) \rtimes C_q$. It can be defined in the following way: $(C_p \times C_p) \rtimes C_q = \{(a^i b^j, a^k b^{jl}) :$ i, j, k are integers and l is fixed$\}$.

Let N be a normal subgroup of $G \times G$. I will show the number of normal subgroups by exhaustion based on which elements are known to be in N. All cases to be used in the lemmas that follow are outlined below:

a) There is a generalized flip in both components. In other terms $(b, b^l) \in N$ for some $0 \leq l < q$.
   - There are q such normal subgroups of this form, one is isomorphic to $G \times G$. The others are the special normal subgroups mentioned above. Each is isomorphic to $(C_p \times C_p) \rtimes C_q$.

b) There is only a generalized flip in the second component. In other terms, $(a^i, a^k b^\beta) \in N$ for some integers i, k and $l \neq 0$ and $(b, b^l) \notin N$ for all l. Further, we will note that minimal i implies if $(a^s, x) \in N$ for some integer s and some $x \in G$ then s is a multiple of i.
   - There two such groups of this form and they are isomorphic to $C_m \times G$. Note that if $i \neq 0$ since p is prime, we will have $m = p$. If $i = 0$ we will have $m = 1$.

c) There is only a generalized flip in the first component. In other terms, $(a^i b^j, a^k) \in N$ for some integers i, k and $j \neq 0$ and $(b, b^l) \notin N$ for all l. Further, we note that minimal i implies if $(x, a^t) \in N$ for some integer t and some $x \in G$ then t is a multiple of k.

- There are two such groups of this form and they are isomorphic to $G \times C_n$. This will follow by symmetry of the previous case

d) There are no generalized flips in either component. In other terms, $(a^i, a^k) \in N$ for some integers a, k , $(a^s, x) \in N$ for some integer s and some $x \in G$ implies s is a multiple of i, $(x, a^t) \in N$ for some integer t and some $x \in G$ implies t is a multiple of k, and $(b, b^l) \notin N$ for all l.

- There are four such group of this form and they are isomorphic to $C_m \times C_n$. Similarly to above, $m = 1$ if and only if $i = 0$ and $n = 1$ if and only if $k = 0$. Otherwise $m, n = p$.

Lemma 30. *Let $G = C_p \rtimes C_q$. Let N be normal in $G \times G$ such that $(b, b^l) \in N$ for some $0 \leq l < q$ then $N = G \times G$ or $N = (C_p \times C_p) \rtimes C_q$.*

Proof. Let N be normal in $G \times G$ such that the hypothesis is satisfied. Since N is normal it is closed under conjugation.

To determine what kinds of generalized rotations N has, let us attempt to isolate the a's. So let us consider the conjugation of (b, b^l) by some arbitrary rotations. Then

$$\begin{aligned}(b, b^l)^{(a^i, a^k)} &= (a^{-i}, a^{-k})(b, b^l)(a^i, a^k) \\ &= (a^{-i} b a^i, a^{-k} b^l a^k) \\ &= (a^{-i} a^{i(m^{-1})} b, a^{-k} a^{k(m^{-1})^l} b^l) \\ &= (a^{-i+i(m^{-1})} b, a^{-k+k(m^{-1})^l} b^l).\end{aligned}$$

Therefore $(a^{-i+i(m^{-1})} b, a^{-k+k(m^{-1})^l} b^l) \in N$. Note that since m^{-1} is not 1 and $l \neq 0$, it follows that $-i + i(m^{-1}) \neq 0$ and $-k + k(m^{-1})^l \neq 0$. Since p is prime, and i, k were arbitrary, it follows that $(a^\alpha b, a^\gamma b^l) \in N$ for all integers α, γ. Now, since N is a group, it has inverses. Namely, $(b^{-1}, b^{-l}) \in N$. Thus by closure, $(a^\alpha, a^\gamma) = (a^\alpha b, a^\gamma b^l)(b^{-1}, b^{-l}) \in N$. Since α, γ are arbitrary $C_p \times C_p \subset N$. Note that the inclusion is strict since $(b, b^l) \notin C_p \times C_p$.

Now consider an index argument:

$$q^2 = |G \times G : C_p \times C_p| = |G \times G : N||N : C_p \times C_p|.$$

Since $|N : C_p \times C_p| \neq 1$ and q is prime, then $|G \times G : N| = 1$ or q. If $|G \times G : N| = 1$, then $N = G \times G$ and we're done. If $|G \times G : N| = q$, then since $(b, b^l)^\beta \in N$ and $(C_p \times C_p) \rtimes C_q = \{(a^i b^j, a^k b^{jl}) :$ i, j, k are integers and l is fixed$\}$ we have $N = (C_p \times C_p \rtimes C_q)$.

$\square$

Lemma 31. *Let N be normal in $G \times G$ where $G = C_p \rtimes C_q$. If the following hold:*

(1) *$(a^i, a^k b^l) \in N$ for some integers k, l such that $k, l \neq 0$ and some minimal integer i*
(2) *$(a^s, x) \in N$ for some integer s and some $x \in C_p \rtimes C_q$ implies that s is a multiple of i*
(3) *$(b, b^t) \notin N$ for all t*

then $N = C_m \times G$ for some m.

Proof. Let N be normal in $G \times G$ such that the hypothesis is satisfied. Let $m = p/\gcd(i,p)$. Note that m is the order of a^i. Further, $m = p$ if $i \neq 0$ and $m = 1$ if $i = 0$. When $m = 1$, then C_m is the trivial subgroup.

Define $0 \leq s < p$ so that $s \equiv (m^{-1})^l - 1 \bmod p$. Note that $s = 0$ implies that $(m^{-1})^l = 1$. However, this implies that $l = 0$ which is a contradiction, so $s \neq 0$. Since p is prime, s^{-1} exists, so we can find a w such that $w \equiv -ks^{-1} \bmod p$. So then $ws + k \equiv 0$. Now, since N is normal, we can conjugate by any element in G, so conjugate $(a^i, a^k b^l)$ by (e, a^w). Then

$$(a^i, a^k b^l)^{(e,a^w)} = (a^i, a^{-w} a^k b^l a^w) = (a^i, a^{k-w} b^l a^w) = (a^i, a^{k-w+w(m^{-1})^l} b^l)$$

$$= (a^i, a^{w((m^{-1})^l - 1)+k} b^l) = (a^i, a^{ws+k} b^l) = (a^i, a^0 b^l) = (a^i, b^l) \in N.$$

Since $p \equiv 1 \bmod q$, and $a^p = e$, by closure $(a^i, b^l)^p = (a^{ip}, b^{lp}) = (e, b^{lp}) \in N$. Thus, since q is prime and $\gcd(q,p) = 1$, $(e, b^\beta) \in N$ for all $0 \leq \beta < q$. By closure, $(a^i, b^l)(e, b^{-1}) = (a^i, e) \in N$. Since p is prime $(a^{\alpha i}, e) \in N$ for all integers α. Further, since N has inverses, $(a^{-i}, b^{-l}) \in N$. Recall that $(a^i, a^k b^l) \in N$. By closure, $(a^i, a^k b^l)(a^{-i}, b^{-l}) = (e, a^k) \in N$. Thus $(e, a^\gamma) \in N$ for all integers γ. Therefore, $(a^{\alpha i}, a^\gamma b^\beta) \in N$ for all integers α, γ, β. Thus $C_m \times G \subseteq N$.

Suppose there was some element $(a^s b^t, a^u b^v) \in N$, but not in $C_m \times G$. Then $t \neq 0$ or s is not a multiple of i. If $t = 0$, then s is not a multiple of i, which contradicts the hypothesis. So $t \neq 0$. If s is a multiple of i then by closure $(a^s b^t, a^u b^v)(a^{-s}, b^{-v})(e, a^{-u}) = (b^t, e) \in N$. Since q is prime, then $(b, e) \in N$, and this contradicts that $(b, b^t) \notin N$ for all t. So $t \neq 0$ and s is not a multiple of i. First, since N is closed and $(e, (a^u b^v)^{-1}) \in N$, we have $(a^s b^t, e) = (a^s b^t, a^u b^v)(e, (a^u b^v)^{-1}) \in N$. Define $0 \leq r < p$ so that $r \equiv (m^{-1})^t - 1 \bmod p$. Note that $r = 0$ implies that $(m^{-1})^t = 1$. However, this implies that $t = 0$ which is a contradiction, so $r \neq 0$. Since p is prime, r^{-1} exists, so we can find a w such that $w \equiv -sr^{-1} \bmod p$. So then $wr + s \equiv 0$. Next, conjugate $(a^s b^t, e)$ by (a^w, e). Then $(a^s b^t, e)^{(a^w, e)} = (a^{-w}, e)(a^s b^t, e)(a^w, e) = (a^{w-s} b^t a^w, e) =$

$(a^{s-w}a^{w(m^{-1})^t}b^t, e) = (a^{s+w((m^{-1})^t-1)}b^t, e) = (a^{s+wr}b^t, e) = (b^t, e)$ Since N is closed under conjugation, $(b^t, e) \in N$. This contradicts the hypothesis. Therefore, there is no element in N that is not in $C_m \times G$.

Therefore $N = C_m \times G$. $\square$

COROLLARY 32. *Let N be normal in $G \times G$ where $G = C_p \rtimes C_q$. If the following hold:*

(1) *$(a^i b^j, a^k) \in N$ for some integers i, j such that $i, j \neq 0$ and some minimal integer k*
(2) *$(x, a^t) \in N$ for some integer t and some $x \in C_p \rtimes C_q$ implies that t is a multiple of k*
(3) *$(b, b^t) \notin N$ for all t*

then $N = G \times C_n$ for some n.

PROOF. This holds by symmetry of Lemma 31. $\square$

LEMMA 33. *Let $G = C_p \rtimes C_q$. Let N be normal in $G \times G$. If the following hold:*

- *$(a^i, a^k) \in N$ for some integers i, k*
- *$(a^s, a^u) \in N$ implies s is a multiple of i and u is a multiple of k.*
- *$(b, b^l) \notin N$ for all $0 \leq l < q$*

then $N = C_m \times C_n$ for some m, n.

PROOF. Let N be normal in $G \times G$ such that the hypothesis holds. Let $m = p/\gcd(i, p)$ and $n = p/\gcd(k, p)$. Note that m is the order of a^i and n is the order of a^k.

Since N is normal, we see by conjugation of (a^i, a^k) by (e, b) that

$$\begin{aligned}(a^i, a^k)^{(e,b)} &= (e, b^{-1})(a^i, a^k)(e, b) = (a^i, b^{-1}a^k b)\\ &= (a^i, b^{-1}ba^{km}) = (a^i, a^{km}) \in N.\end{aligned}$$

N is a subgroup, so it has inverse. Thus $(a^{-i}, a^{-k}) \in N$. By closure, $(a^i, a^{km})(a^{-i}, a^{-k}) = (e, a^{k(m-1)}) \in N$. Since $m \neq 1$ and p prime, it follows that $(e, a^{\gamma k}) \in N$ for all integers γ. Then $(a^i, a^k)(e, a^{-k}) = (a^i, e) \in N$ by closure. Thus, $(a^{\alpha i}, e) \in N$ for all integers α. Therefore $(a^{\alpha i}, a^{\gamma k}) \in N$ for any integers α, γ. Since m is the order of a^i and n is the order of a^k, we have $C_m \times C_n \subseteq N$.

Suppose for contradiction that there was some $(a^s b^t, a^u b^v) \in N$ and not in $C_m \times C_n$. Then s is not a multiple of i, u is not a multiple of k, $t \neq 0$ or $v \neq 0$. If $t = 0$ and $v = 0$ then either s is not a multiple of i or u is not a multiple of k. Either would contradict condition two of the hypothesis. Suppose without loss of generality that $t \neq 0$. If $v = 0$, then u is a multiple of k. So $(a^s b^t, a^u) \in N$ and by closure $(a^s b^t, e) =$

$(a^s b^t, a^u)(e, a^{-u}) \in N$. If s is a multiple of i, we can left multiply by (a^{-s}, e) to contradict condition three of the hypothesis. Now we will show that even if s is not a multiple of i, we have a contradiction to condition three. Define $0 \leq l < p$ so that $l \equiv (m^{-1})^t - 1 \bmod p$. Note that $l = 0$ implies that $(m^{-1})^t = 1$. However, this implies that $t = 0$ which is a contradiction, so $l \neq 0$. Since p is prime, l^{-1} exists, so we can find a q such that $q \equiv -sl^{-1} \bmod p$. So then $ql + s \equiv 0$. Now, since N is normal, we can conjugate by any element in G, so conjugate $(a^s b^t, e)$ by (a^q, e). Then

$$\begin{aligned}(a^s b^t, e)^{(a^q, e)} &= (a^{-q} a^s b^t a^q, e) = (a^{s-q} b^t a^q, e) = (a^{s-q+q(m^{-1})^t} b^t, e) \\ &= (a^{q((m^{-1})^t - 1)+s} b^t, e) = (a^{ql+s} b^t, e) = (a^0 b^t, e) = (b^t, e) \in N.\end{aligned}$$

This contradicts condition three of the hypothesis. So $t \neq 0$ and $v \neq 0$. By a similar conjugation to above, we can see that $(b^t, b^v) \in N$. But since t has a multiplicative inverse, it follows that $(b^t, b^v)^{t^{-1}} = (b, b^{vt^{-1}}) \in N$. This contradicts the fourth condition of the hypothesis. So no such element exists. Therefore $N = C_m \times C_n$.

□

COROLLARY 34. *Let N be normal in $G \times G$ where $G = C_p \rtimes C_q$. Then N is one of the following:*

$$\begin{array}{ll} G \times G & G \times C_n \\ C_m \times G & C_m \times C_n \\ (C_p \times C_p) \rtimes C_q & \end{array}$$

PROOF. Lemmas 30, 31, 33 and Corollary 32 show exhaustively that these are the normal subgroups of $G \times G$. □

THEOREM 35. *There are $9 + (q - 1)$ normal subgroups of $G \times G$ where $G = C_p \rtimes C_q$ when prime $p \equiv 1 \bmod q$ with q prime.*

PROOF. This follows directly from Corollary 34.

Normal Subgroup Category	Number in Category
$G \times G$	1
$G \times C_n$	2
$C_m \times G$	2
$C_m \times C_n$	4
$(C_p \times C_p) \rtimes C_q$	$q - 1$

The total of the right column is $9+(q-1)$ and hence there are $9+(q-1)$ normal subgroups of $G \times G$ where $G = C_p \rtimes C_q$.

□

CHAPTER 4

Closing Remarks

1. Open Questions

This honors thesis leads to a wide variety of open questions, approachable and difficult.

- If m is even, how many normal subgroups do D_{2m} and $D_{2m} \times D_{2m}$ have?
- Can the result found in D_{2m} for odd m be extended to $C_m \rtimes C_q$? This honors thesis considered $C_p \rtimes C_q$ for p, q prime and $p \equiv 1 \bmod q$. It was important that p was 1 modulo q so that conjugacy classes could be constructed to the correct size. So we know that if this result were to be extended, we would need $m \equiv 1 \bmod q$. This still fits the dihedral case, since $D_{2m} = C_m \rtimes C_2$ and an odd number is 1 mod 2. What is yet unknown is how restrictive the condition would need to be for m in the general $C_m \rtimes C_q$ case. Would it be enough to say $m \equiv 1 \bmod q$, or would each of its prime factors need to be $1 \bmod q$?
- If we are able to answer the previous bullet point, the next logical question is: what happens to the semidirect product group $C_m \rtimes C_n$ for composite m, n? Does it have similar growth to $C_m \rtimes C_q$ and $C_p \rtimes C_q$?
- On a different line of thinking, what happens if we consider $D_{2m} \times D_{2m} \times D_{2m}$? How many normal subgroups does $D_{2m} \times D_{2m} \times D_{2m}$ have? What about $D_{2m} \times \cdots \times D_{2m}$ for n direct products? If we can have a result with dihedral groups, can we find a similar one with semidirect products? I believe that this problem will generalize by looking at how many components have flips. If we have k flips and n direct products, we can then count isomorphic copies using $\binom{n}{k}$. The trick will be to look at how the flips interact together. Some components may act independently and others may act together. This was shown in $D_{2p} \times D_{2p}$ by the normal subgroups $D_{2p} \times D_{2p}$ and $(C_p \times C_p) \rtimes C_2$. I do not believe that this will be a huge leap, however, time did not allow me to reach results in this area.

- Why does the subgroup count of some groups grow so quickly while others grow slowly and predictably like the dihedral group? This question stems from computer research at the beginning of my thesis. To begin my research, I searched for the normal subgroup count of small groups and their direct product through a program called GAP. I made lists of these numbers for all nonabelian groups of order less than 150. I then started manually looking for patterns. I noticed that all groups of order $2p$ where p was prime followed a $3 - 10$ pattern: three normal subgroups and 10 for the direct product. I was able to use the GAP program to search for what the structure of this group of order $2p$ was. When I found out that it was the dihedral group, I was able to start trying to prove my goal, that this pattern held for all primes, and not just primes under 75. From there I was able to extend my result to dihedral groups of order $2p^n$ and then $2m$. When I had this result, I looked for groups of order pq where p and q were prime. This, along with the dihedral group result led me to semidirect products. Not all groups had such a small growth pattern, though. For example, there were groups of order 2^k that had normal subgroups growing approximately linearly but under the direct product they seemed to be growing exponentially. Further, there is one group of order 20 with 5 normal subgroups and 36 under the direct product. But there is another group of order 20 with 7 normal subgroups and 104 under the direct product. What is so different about their structure that can account for that discrepancy?

Bibliography

[1] I. Martin Isaacs *Algebra: A Graduate Course* 1994: Brooks/Cole Publishing Company.

[2] "Dihedral Group Properties" *Planet Math* 2006. Web.