An Introduction to the Classification of Finite Groups

Bryce Goodwin

MATH 336

Jim Morrow

June 9, 2019

Introduction

Finite groups are algebraic objects fundamental to the study of symmetry, and therefore widely applicable to most branches of mathematics concerned with finite objects. Their structures have been studied extensively for the last 200 years, and yet mathematicians are still unable to describe them all; at least not in the way that any natural number may be described as a string of digits, or any finite set a collection of elements. However, in 2004, mathematicians completed the classification of finite simple groups, a major step towards the classification of all finite groups. The Classification Project was a combined effort by nearly a hundred mathematicians over the course of 60 years. Its proof consists of hundreds of articles and thousands of pages, and is considered one of the greatest mathematical achievements of the twentieth century.

This paper will not attempt to detail the classification project or its proof. Instead, it will introduce the theory of finite groups and help form an understanding of their structure for those unfamiliar with the subject. We shall then consider how some smaller groups may be built, understand the limitations of such constructions, and suggest how these limitations might be overcome. The exploration will build towards an appreciation of the classification project, and culminate in a brief description of its statement. For the early sections we shall follow text *Theory of Finite Groups* by Jansen and Boon [4], and the description of the classification theorem will follow the Yale Mathematical Monograph: *The Finite Simple Groups and Their Classification* summarizing Michael Aschbacher's 1978 lectures of the same name on the then-current state of the classification project.

1. Groups

As young students become familiar with the calculations of arithmetic they take their first steps into algebra when they realize they can solve for unknowns in equations such as $x + 5 = 7$. These skills are not restricted to integers under addition, and the undergraduate reader has no doubt solved countless equations involving various types of numbers under both addition and multiplication. However, the full generalization of this process extends much further than arithmetic.

Consider this example equation of quarter turns: "two lefts and what is a right", formalized as $2L + x = R$. In this case the elements of the equation to be solved are not numbers and the operation, despite being written as $+$, is not addition. Nonetheless we may intuit that x must be L, as three lefts make a right. We shall call a set with a binary operation that one can "perform basic algebra on" a *group*, and the study of these is group theory.

1.1 Defining Properties of Groups

To motivate a precise definition of a group it will be beneficial to investigate the process of solving equations such as $x + 5 = 7$. Here the group in question is the set of integers under the operation of addition, and while determining x may be trivial, solving the equation explicitly requires making use of a number of properties of arithmetic. The following is one solution process expanded in extensive detail.

Solve: $x + 5 = 7$.

1) $(x + 5) + (-5) = 7 + (-5) = 2$
2) $x + \big(5 + (-5)\big) = 2$
3) $x + 0 = 2$
4) $x = 2$

Note that addition is the only operation being considered, so subtraction must be interpreted as the addition of negatives. Parenthesis have been used extensively for clarity, but this practice will be dropped later. Underlying each step is a property necessary for solving the equation, and these are the properties that shall define a group. We consider them in reverse order for clarity.

Step four isolates x on the left side of the equation. This is only possible because there exists an integer, 0, with the property that $x + 0 = x$ for all integers x. Without an integer with this property, x could not be isolated and the equation could not be solved. In general, an element, e, of a set, G, under an operation, $*$, is called an *identity* if $x * e = x$ for all $x \in G$. Identities are usually denoted as $0, 1$, or e, depending on the context.

Step three combines the integers 5 and -5 under addition to produce 0. Since 0 is necessary for isolating x, producing 0 in the equation is also necessary. In general, an element, a, in a set, G, under an operation $*$ with an identity, 1, is called *invertible* if there exists a $b \in G$ such that $a * b = 1$, and b is called the *inverse* of a. Inverses are usually denoted as $-a$ or a^{-1} depending on context. If 5 did not have an additive inverse the equation could not be solved.

Step two changes the order in which the addition operations are applied. Such a change is necessary to sum 5 and -5, and therefore to solve the equation. An operation, $*$, is *associative* over a set G, if for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

Step one introduces addition of the integer -5 to the equation. Doing so is necessary for isolating x, and is guaranteed to be well defined on the left side of the equation because it is the inverse of 5, but it is also necessary $7 + (-5)$ be defined for the introduction to be valid. Of course, addition is defined for every pair of integers. In general, we call an operation, $*$, *closed* on a set G if $a * b$ is defined for every $a, b \in G$ and $a * b \in G$.

With these concepts understood, we are prepared to define a group. In the preceding explanation we have used the symbols $+$ and $*$ to represent our operations, but this is not necessary. In fact, most of the remainder of this paper will use concatenation to signify the operation.

Definition: A group $(G,*)$ is a set G under a binary operation $*$ that satisfies the following properties:

i. G is closed under $*$.
ii. $*$ is associative over G.
iii. G possesses an identity under $*$.
iv. Every $g \in G$ has an inverse under $*$ in G.

We may abuse notation and refer to a group $(G,*)$ simply as G when the operation is clear from context. Note that the integers have many other properties that are not used in the solving process and not included in the definition of a group. In particular, a group does not need to be commutative. That is, there is no requirement that $ab = ba$ for $a, b \in G$, despite this being true for many classes of numbers. A group that is commutative is called *abelian*.

While these four properties define groups, additional properties may be derived from them. Five in particular will be important for our investigation[1].

Theorem 1: Inverses commute.

Proof: Let G be a group with identity e, and $a \in G$. Since G is a group, a has an inverse, a^{-1}, and a^{-1} has an inverse, $(a^{-1})^{-1}$. Thus $aa^{-1} = e$, $a^{-1}(a^{-1})^{-1} = e$, and

$$a^{-1}a = a^{-1}ae = a^{-1}aa^{-1}(a^{-1})^{-1} = a^{-1}(a^{-1})^{-1} = e.$$

Therefore $a^{-1}a = aa^{-1} = e$. Note that this also means that a is an inverse of a^{-1}. ■

Theorem 2: Identities commute.

Proof: Let G be a group with identity e and $a \in G$. The proof follows from Theorem 1 as $ae = aa^{-1}a = ea$. ■

Theorem 3: Inverses are unique.

Proof: Let G be a group with identity e and $a \in G$, and let b and c be inverses of a. Then $ab = ac = e$, and by Theorem 1, $b = bac = c$. Therefore, the inverse of an element of a group is uniquely defined and $(a^{-1})^{-1} = a$. ■

Theorem 4: Identities are unique.

Proof: Let G be a group with identities e_1 and e_2. Then $e_1e_2 = e_1$ because e_2 is an identity, and $e_1e_2 = e_2e_1 = e_2$ because identities commute and $_1$ is an identity. Thus $e_1 = e_2$, so the identity of a group is unique. ■

Theorem 5: Given a group G, for any $a \in G$, $\alpha: G \to G$ such that $\alpha(x) = ax$, or $\alpha(x) = xa$, is a bijection.

Proof: Let G be a group with $a \in G$, and $\alpha: G \to G$ such that $\alpha(x) = ax$ for $x \in G$. For any $b \in G$, $\alpha(a^{-1}b) = aa^{-1}b = b$ so α is surjective. If $\alpha(x) = \alpha(y) = b$, then $ax = ay = b$, and

1. The properties of identities and inverses are closely related. There are a number of ways to prove the following theorems in various orders, and it is important to be careful not to be circular when doing so! The structure of these theorems in this paper follow the form of Jansen and Boon's Theory of Finite Groups [4].

$x = y = a^{-1}b$. Therefore α also injective, so it is bijective. An identical argument applies for right multiplication. ■

1.2 Examples of Groups

Integers under addition form a group, as do the rationals, reals, and complex numbers. However, none of these sets form a group under multiplication since 0 does not have an inverse. The rationals, reals, and complex numbers *are* groups under multiplication when 0 is excluded, but the integers are not[1]. Groups may similarly be formed by the equivalence classes of modular arithmetic under addition. Still more abstract are nonarithmetic examples of groups.

Example 1.1: Quarter turns form a group

The previously mentioned example of lefts and rights form a group. Specifically, the set of counter-clockwise rotations of $90°$ (Left-L), $180°$ (Back-B), $270°$ (Right-R), and $0°$ (Forward-F), with composition of rotations as the operation, which may be thought of as addition of angles modulo 360. The operation is closed because the composition of any of these quarter turns is again a quarter turn. The operation is associative by the associativity of addition. The set has an identity, F, and each element has an inverse, with L and R being each other's inverse, and B and F each being their own inverse.

Example 1.2: The symmetries of a square form a group.

The idea of rotations may be expanded by considering the symmetries of a geometric object. By symmetries we refer to transformations that map a geometric object to itself. For a square the symmetries are the reflections along the four lines of symmetry and rotations of $90°, 180°, 270°$, and $0°$. The group operation on these eight transformations is composition. Again, we can confirm this is a group by confirming each property individually. Since the image of each transformation is a square that may again be transformed, the symmetries are closed under composition. Composition of transformations is associative because the composition of any functions is associative[2]. The $0°$ rotation is the identity, and every element is its own inverse, except for $90°$ and $270°$ which are each other's inverse. Note that this is not an abelian group[3].

Example 1.3: The permutations on three elements form a group.

Given three elements in an arrangement, they may be permuted in six ways. Transposing two elements (three ways), cycling all three elements (two ways), or the identity

1. ☺ Why is this? Consider what the identity would be.
2. 😐 Why is this true?
3. ☺ Confirm that there are at least two symmetries that don't commute.

permutation. These permutations with the operation of composition may be shown to be a group[1].

Example 1.4: Invertible $n \times n$ real matrices form a group under matrix multiplication.

The group properties follow from the definition of matrix multiplication. Note that it is necessary to exclude non-invertible matrices because, of course, they do not have inverses. This group is known as the *general linear group*, and is denoted as $GL_n(\mathbb{R})$.

Some of these examples contain infinite elements, while others are finite. It is possible to make statements about the structure of a group based on the how many elements it contains. The number of elements in a group is called the *order* of the group, and is often denoted $|G|$ for a group G. The remainder of this paper will exclusively be concerned with groups of finite order.

2. Cayley Tables

For small groups it is possible to consider the operation on every pair of elements in the group. When formatted in a table it is known as a Cayley table in honor of the British mathematician Arthur Cayley. The Cayley tables for the group of quarter turns and the groups of integer addition modulo 3 and 4 are given below. For consistency we shall always order the elements with the identity first.

Table 1.1

*	**F**	**L**	**B**	**R**
F	F	L	B	R
L	L	B	R	F
B	B	R	F	L
R	R	F	L	B

Table 1.2

$+_3$	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

Table 1.3

$+_4$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2.1 Group Isomorphism Classes

Notice the similarity of the Cayley tables in tables 1.1 and 1.3. The group of quarter turns (F, L, B, R) and the group of integers under addition modulo 4 can be seen to have identical structure by equating L with 1, B with 2, R with 3, and F with 0. We shall call two groups *isomorphic* if their Cayley tables can be shown to be identical by a relabeling of elements. Groups that are isomorphic are said to belong to the same group isomorphism class. Rather than study these groups separately, it is sufficient to study a single representative group of the isomorphism class. To simplify the study of groups shall now focus almost entirely on isomorphism classes, and avoid distinguishing between groups in the same class.

1. ☺ Do this by demonstrating all four properties.

Definition: A *cyclic group* is a group G in which there exists an $a \in G$ such that for every $g \in G$, $g = a^k$ for some $k \in \mathbb{Z}$, where $a^{-k} = (a^{-1})^k$ and $a^0 = 1$. Such a group is said to be *generated* by a.

Theorem 6: If G is a cyclic group of order $n \in \mathbb{N}$ generated by a, then $G = \{a^0, a^1, \dots, a^{n-1}\}$.

Proof: Every element of G may be written as a^k and $a^k \in G$ for all $k \in \mathbb{Z}$ because G is closed. By the pigeon hole principle $\{a^0, a^1, \dots, a^n\}$ contains a pair of expressions that are equal. If $a^{m_1} = a^{m_2}$ with $0 \leq m_1 < m_2 \leq n$, then $a^{m_2 - m_1} = 1$, and $a^k = a^{k \bmod m_2 - m_1}$. Therefore $G \subset \{a^0, a^1, \dots, a^{m_2 - m_1}\}$. Since G has n elements $m_2 - m_1 \geq n$, but $m_2 - m_1 \leq n$ as well, so $G \subset \{a^0, a^1, \dots, a^n\}$. Finally, since $|G| = n$ and $a^n = a^{m_2 - m_1} = a^0 = 1$, $G = \{a^0, a^1, \dots, a^{n-1}\}$. ■

Theorem 7: Cyclic groups of the same order are isomorphic.

Proof: Let G be a cyclic group of order n generated by $a \in G$. Then $G = \{a^0, a^1, \dots, a^{n-1}\}$. Arrange the elements of the Cayley table of G in order of their exponent. Then the table is uniquely determined since $a^{k_1} a^{k_2} = a^{k_1 + k_2 \bmod n}$. If G' is a cyclic group of order n generated by $a' \in G'$, then a uniquely determined Cayley table may be obtained in the same manner, and is isomorphic to G by relabeling a^k as a'^k. ■

Since the group of quarter turns and the group of integer addition modulo 4 both have four elements and can be generated by repeated applications of turning left and adding 1 respectively, they belong the isomorphism class of *cyclic groups of order 4*, denoted C_4.

Table 1.4: Representative group of isomorphism class C_4

*	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

We now turn to the driving question of this paper: what are the finite group isomorphism classes? We have already encountered a number of them. Specifically, we have considered C_4, but this is not the only cyclic group.

Theorem 8: There is a cyclic group isomorphism class of every order.

Proof: The integers $\bmod_n$ form a group under addition of order n and may be generated by repeatedly adding 1. Hence, they are a cyclic group of order n, so the isomorphism class exists.

A *symmetric group* is the group of permutations of an ordered set. Two symmetric groups of the same order may be seen to be isomorphic simply by relabeling the elements of the set being acted upon. The class of symmetric groups on n elements is denoted ${S_n}^{1,2}$.

These two families of group classes are nowhere near exhaustive of the finite group isomorphism classes, and it can be very difficult to identify some of the others. In the following sections we shall outline a process that works for groups of small order.

2.2 Valid Cayley Tables

Identifying the finite group isomorphism classes is equivalent to asking which binary operation tables are Cayley tables, and our initial investigation shall consist of constructing all possible tables for groups of small order. It is very easy to construct a table for an operation that is closed and contains an identity and inverses. Associativity is far more difficult to verify, and is responsible for the lion's share of the complexity of groups. While the number of tables of closed binary operations over even a small set grows very quickly, $O\left(n^{n^2}\right)$, we shall use the properties of a group to restrict the number of valid Cayley tables to a much more manageable number. The following properties of Cayley tables will allow us to narrow the focus our search substantially.

Cayley Table Property 1: The first row and column of a Cayley table are uniquely determined.

Proof: This follows directly from the existence and uniqueness of the identity, and our decision to index it first.

Cayley Table Property 2: Each row and each column must contain each element exactly once.

Proof: Each row (resp. column) corresponds to the image of right (resp. left) multiplication by an element, and such multiplication is a bijection by theorem 5.

Cayley Table Property 3: The identity entries must be symmetric across the diagonal.

Proof: This follows directly from theorem 1 and theorem 3.

By restricting ourselves to tables with properties 1-3 we need to consider far fewer tables, and each table that satisfies these three properties is guaranteed to have both an identity and inverses. However, these are still not sufficient to guarantee associativity and we will consider algorithms that are able to confirm an operation's associativity later.

1. ☺ What is the order of S_n?
2. 😐 Show that there is a symmetric group on a set of any finite set of elements. Consider example 3.

2.3 Constructing Small Finite Groups

We now have the tools to exhaustively identify groups of small order. We shall detail the construction of groups of orders 1 through 5, and outline the process for the groups of

order 6. After this the description of the process becomes tedious to write, but may continue to be effectively implemented by hand for larger groups, and implemented by a computer for groups that are far larger still.

Groups of order 1

Since all groups must have an identity, the smallest group must have at least one element, and the element of the group of order 1 must be the identity. The Cayley table is therefore easily derived, and is known as the trivial group or C_1.

*	**1**
1	1

Table 2.1

Groups of order 2

The case with two elements is not significantly more complicated. All but one entry are determined by property 1, and the final entry is determined by property 2. Hence, there is only one isomorphism class of order 2. This group is cyclic and is known as C_2.

*	**1**	**a**
1	1	a
a	a	1

Table 2.2

Groups of order 3

The table with three elements is also uniquely determined. After applying property 1, the entry for ab must be 1 by property 2, and the rest of the table follows easily. This group is cyclic and is known as C_3.

*	**1**	**a**	**b**
1	1	a	b
a	a	b	1
b	b	1	a

Table 2.3

Groups of Order 4

The table with four elements is not uniquely determined. Following the identity property, we have table 2.4.1, but multiple valid tables may be built from this. At first glance there appear to be three possibilities for the value aa, $aa = 1$, $aa = b$, or $aa = c$. However, at this point b and c are indistinguishable elements. The tables where $aa = c$ could be obtained from the tables with $aa = b$ by a relabeling of elements, so they are isomorphic. It is therefore sufficient to consider only $aa = 1$ and $aa = b$. The choice of $aa = b$ then uniquely determines a Cayley table, the familiar C_4 in table 2.4.2, but $aa = 1$ leads to an additional decision. Either $bb = 1$ or $bb = a$.

*	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a			
b	b			
c	c			

Table 2.4.1

The case of $bb = 1$ yields another group of order 4 (table 2.4.3), named the Klein-4 group in honor of German mathematician Felix Klein, and is usually denoted K_4. Table 2.4.4 shows the case where $bb = a$, which is isomorphic to C_4 as the original C_4 table may be obtained from it by permuting the elements a and b.

Thus, there are two groups of order four with different structure. K_4 is often characterized by its elements having the property that each is its own inverse. This is certainly not the case for C_4.

*	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

Table 2.4.2

*	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Table 2.4.3

*	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	a	1
c	c	b	1	a

Table 2.4.4

Groups of Order 5

There is only one group of order 5 up to isomorphism[1]. We shall prove this easily later, but to be thorough we derive it here as well. After applying Cayley table property 1, there are two possibilities up to isomorphism for aa, $aa = 1$ and $aa = b$.

Case 1: $aa = 1$.

We may determine the second row up to isomorphism since c and d are indistinguishable (table 2.5.1). There are now two possibilities for the entry of ba: $ba = c$ or $ba = d$. Note that c and d are no longer indistinguishable since they have been used differently in the row above! If $ba = c$ then we derive table 2.5.2. However, in this table it is impossible to assign the identity to entries in each row and column without violating Cayley table property 3[2]. Therefore, it is not a valid Cayley table.

*	**1**	**a**	**b**	**c**	**d**
1	1	a	b	c	d
a	a	1	c	d	b
b	b				
c	c				
d	d				

Table 2.5.1

If $ba = d$ then we may determine the rest of the table to be table 2.5.3[3], which satisfies all three Cayley table properties. However, the table describes an operation that is not associative since $(bb)c = c$, while $b(bc) = d$, so this is also not a valid Cayley table. Therefore, we can conclude that $aa \neq 1$.

*	**1**	**a**	**b**	**c**	**d**
1	1	a	b	c	d
a	a	1	c	d	b
b	b	c	d		
c	c	d			
d	d	b			c

Table 2.5.2

*	**1**	**a**	**b**	**c**	**d**
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	1

Table 2.5.3

1. ☺ What isomorphism class must this be?
2. 😐 How else could we confirm this is not a Cayley Table?
3. ☺ Confirm this.

Case 2: $aa = b$.

We immediately come to a second decision as to the value of ab. Up to isomorphism either $ab = 1$ or $ab = c$. In the case that $ab = 1$ we may determine the table to be that of table 2.5.4, but property 2 implies that $bb = c$ and $bb = d$, which is a contradiction. If $ab = c$ the table may be determined to be the familiar C_5, which must exist (table 2.5.5).

*	**1**	**a**	**b**	**c**	**d**
1	1	a	b	c	d
a	a	b	1	d	c
b	b	1			
c	c	d			
d	d	c			

Table 2.5.4

*	**1**	**a**	**b**	**c**	**d**
1	1	a	b	c	d
a	a	b	c	d	1
b	b	c	d	1	a
c	c	d	1	a	b
d	d	1	a	b	c

Table 2.5.5

Groups of Order 6

The groups of order 6 are more complicated but are still straightforward to derive by hand. A description of such a derivation would be tedious, however, so for brevity we shall only highlight the results. Motivated readers are encouraged to verify the construction themselves[1]. To simplify the process, it is recommended to begin by splitting the tables into three cases based on their possible *skeletons.* The skeleton of a Cayley table is the position of the identities up to isomorphism. In the case of groups of order 6 there are three possibilities, every element is its own inverse, one pair of elements are inverses, or two pairs of elements are inverses[2].

*	1	a	b	c	d	e
1	1					
a		1				
b			1			
c				1		
d					1	
e						1

Table 2.6.1

*	1	a	b	c	d	e
1	1					
a		1				
b			1			
c				1		
d						1
e					1	

Table 2.6.2

*	1	a	b	c	d	e
1	1					
a		1				
b				1		
c			1			
d						1
e					1	

Table 2.6.3

The result of the constructions will be two groups. We are guaranteed that C_6 will be one of them, and the previously mentioned symmetric group S_3 will be the other. Below are their Cayley tables, note that S_3 is not symmetric about the diagonal, so it is not commutative.

1. Be careful with indistinguishable elements in table 2.6.2 and table 2.6.3 since the skeletons immediately distinguish some elements. For instance, in table 2.6.2 elements b and d are clearly distinguishable since one is its own inverse, and the other is not.
2. ☺ Why are these the only possibilities?

*	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	c	d	e	1
b	b	c	d	e	1	a
c	c	d	e	1	a	b
d	d	e	1	a	b	c
e	e	1	a	b	c	1

Table 2.6.4: C_6

*	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	d	e	b	c
b	b	e	1	d	c	a
c	c	d	e	1	a	b
d	d	c	a	b	e	1
e	e	b	c	a	1	d

Table 2.6.5: S_3

2.3 Associativity

It is not surprising that associativity is more difficult to confirm than the other operations. It is a statement about every ordered triple of elements in the table, so naively confirming associativity will have complexity $O(n^3)$. Even after reducing the number of tables to be checked, this is still prohibitive for moderately large n. There are a couple of algorithms that help organize the process and optimize the average time. See Light's Algorithm and Jansen and Boon's Property IV of Cayley Tables [4, pg. 11]. Neither of these reduce the worst case $O(n^3)$ scenario though. If we hope to be able to identify large finite groups we will need a method other than building them directly.

3. Subgroups and Homomorphisms

Just as integers may be characterized by their factors, groups have a similar, though not quite analogous property. How to use this "factorization" to define groups remains an unanswered question in mathematics, known as the Group Extension Problem, but the potential of this characterization has driven the classification effort for the last for the last 100 years.

3.1 Subgroups

Definition: A *subgroup* of a group $(G,*)$ is a subset $H \subset G$ that is also a group under $*$. We denote this as $H \leq G$.

Theorem 9: A subset H of a group G is a subgroup of G if and only if it is closed and contains inverses.

Proof: If H is a subgroup of G then it is a group, so it is closed and contains inverses. In the converse direction, H is closed and contains inverses by hypothesis. Therefore, for $h \in H$, $h^{-1} \in H$ and $hh^{-1} = 1_G \in H$, so H contains an identity. Finally, since every ordered triple in H is in G and G is associative, H is associative. ■

Example 3.1: The group of quarter turns is a subgroup of the group of symmetries of a square.

Example 3.2: The even integers are a subgroup of the integers under addition[1].

Example 3.3: For every group G, the identity element 1_G and G itself are subgroups. These are known as the *trivial subgroups* of G.

Example 3.4: Given an element $a \in G$ for a group G, $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is a subgroup of G. It is closed since $a^x a^y = a^{x+y} \in \langle a \rangle$, and contains inverses because $(a^x)^{-1} = (a^{-1})^x = a^{-x} \in \langle a \rangle$. $\langle a \rangle$ is called *the subgroup of G generated by* a.

3.2 Cosets

Given a subset $H \leq G$ we may consider the set of elements $aH = \{ah \mid h \in H\}$. Such a set is called a *left coset* of H. Similarly $Ha = \{ha \mid h \in H\}$ is a right coset. For simplicity we shall make and prove statements about left cosets, but there are equivalent statements for right cosets. If $a \in H$ then $aH = H$ by the closure of H and Theorem 5. However, if $a \notin H$ then $aH \neq H$. We shall occasionally write AB to signify $\{ab \mid a \in A \text{ and } b \in B\}$[2].

Theorem 10: Cosets of a subgroup $H \leq G$ partition G.

Proof: For every $g \in G$, $g \in gH$ and $gH \subset G$, so $G = \bigcup\{gH \mid g \in G\}$. Suppose $g \in aH$ and $g \in bH$. Then $g = ah_1$ for some $h_1 \in H$, and $g = bh_2$ for some $h_2 \in H$. Let $bh \in bH$. Then $bh = gh_2^{-1}h = ah_1h_2^{-1}h$, so $bh \in aH$. Similarly, for any $ah' \in aH$, $ah' = gh_1^{-1}h' = bh_2h_1^{-1}h'$, so $ah \in bH$. Therefore $bH = aH$, and each $g \in G$ is a member of exactly one coset. Since G is equal to the union of the cosets, they form a partition. ■

This leads us to one of the most useful theorems of finite groups.

Theorem 11 (Lagrange's Theorem): For any finite group G, if H is a subgroup of G then $|H|$ divides $|G|$.

Proof: By Theorem 10, the cosets of H partition G. By Theorem 5, $|aH| = |H|$ for all $a \in G$. Therefore $|G| = |H||G:H|$ where $G:H$ is the set of H cosets in G. ■

Corollary: For any prime p, all groups of order p are isomorphic.

Proof: Let $|G| = p$. Since $|G| \neq 1$, G has a non-identity element a. By Lagrange's Theorem, $|\langle a \rangle|$ divides p, so $|\langle a \rangle| = p$. Therefore $\langle a \rangle = G$, so G is isomorphic to the cyclic group of order p by Theorem 7.

This confirms our investigations into groups of orders 2, 3, and 5, and hints at the utility of Lagrange's Theorem.

1. ☺ What are the other subgroups of $(\mathbb{Z}, +)$?
2. ☺ For a group G, what is GG?

3.3 Homomorphisms

In our discussions of isomorphism classes, we considered informally how some groups may be transformed into others. This section looks to formalize this concept, and investigate how it may be used to develop our understanding of the structure of groups.

Definition: A *homomorphism* is a function $\varphi: G \to H$, where G and H are groups and $\varphi(ab) = \varphi(a)\varphi(b)$ for any $a, b \in G$.

Intuitively, the property $\varphi(ab) = \varphi(a)\varphi(b)$ to some extent preserves the group structure, formalizing our method of relabeling elements in a Cayley table. However, homomorphisms do *not* necessarily describe isomorphisms, i.e. preserve all of the group structure. The constant function $\varphi: G \to G$ such that $\varphi(g) = 1$ for all $g \in G$ is a homomorphism since it is certainly true that $\varphi(ab) = 1 = 1 * 1 = \varphi(a)\varphi(b)$, but G need not be isomorphic to $\{1\}$. If a homomorphism φ does not discard any information of the group, specifically if $\varphi(a) = 1$ iff $a = 1$, then φ will agree with our previous description of isomorphisms. Explicitly, a bijective homomorphism is an isomorphism. An isomorphism from a group to itself is called an automorphism. This question of what φ maps to the identity leads to an important property of homomorphisms.

Definition: The kernel of a homomorphism φ, denoted $\ker(\varphi)$, is the subset X of the domain of φ such that $\varphi(X) = 1$.

As discussed above, the size and structure of the kernel of a homomorphism indicate how much of the original group structure is preserved. Understanding homomorphisms of groups and their kernels will help us understand the structure of the isomorphism classes of groups.

Lemma 1: If $\varphi: G \to H$ is a homomorphism then $1_G \in Ker(\varphi)$.

Proof: For any $a \in G$, $\varphi(a) = \varphi(a1_G) = \varphi(a)\varphi(1_G)$, so $\varphi(1_G) = 1_H$ and $1_G \in Ker(\varphi)$. ■

Theorem 12: The kernel of a homomorphism $\varphi: G \to H$ is a subgroup of G.

Proof: Let $\varphi: G \to H$ be a homomorphism. If $a, b \in Ker(\varphi)$, then $\varphi(ab) = \varphi(a)\varphi(b) = 1_H 1_H = 1_H$, so $ab \in Ker(\varphi)$ and $Ker(\varphi)$ is closed. If $a \in Ker(\varphi)$, then

$$\varphi(a^{-1}) = 1_H\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1_G) = 1_H,$$

so $a^{-1} \in Ker(\varphi)$. Thus, $Ker(\varphi)$ is closed and contains inverses, so by Theorem 9 $Ker(\varphi)$ is a subgroup of G. ■

3.4 Normal Subgroups

The kernel of every homomorphism on G is a subgroup of G, but not every subgroup is the kernel of a homomorphism. If $\varphi: G \to H$ and $a, a' \in \ker(G)$, then

$$\varphi(ab) = \varphi(a)\varphi(b) = \varphi(b) = \varphi(b)\varphi(a') = \varphi(ba'),$$

but if G is not abelian then there is no guarantee that $\varphi(ab) = \varphi(ba')$, or even that $\varphi(ab) = \varphi(ba)$, for all a and a' in an arbitrary $G' \leq G$. If our intention be that $\varphi(G') = 1_H$, then the restriction that $\varphi(ab) = \varphi(ba')$ for all $a, a' \in G'$ is equivalent to requiring $bG' = G'b$, i.e. that it has equal left and right cosets.

Definition: If G' is a subgroup of G such that $aG' = G'a$ for all $a \in G$, then we call G' a *normal subgroup* and denote it $G' \trianglelefteq G$.

Theorem 13: Every normal subgroup $G' \trianglelefteq G$ is the kernel of some homomorphism of G.

Proof: We show this by considering the cosets of G'. Let $(G{:}\,G',*)$ be the group[1] of G' cosets of G where $aG' * bG' = abG'$. Let $\varphi{:}\, G \to (G{:}\,G',*)$ be defined as $\varphi(a) = aG'$. Then $\varphi(ab) = abG'$. Since G' is normal, $abG'G' = aG'bG' = \varphi(a) * \varphi(b)$, so φ is a homomorphism, and

$$\ker(\varphi) = \{a \in G \mid \varphi(a) = aG' = 1G' = G'\} = G'$$

because G' is closed. ■

3.5 Quotient Groups

The concept of a normal group and its group of cosets allows us to consider the decomposition of groups into smaller groups, similar to factoring integers.

Definition: Given a group G with $N \trianglelefteq G$, the group of cosets of N in G is called the quotient group of G by N, and is denoted G/N.

By Lagrange's Theorem, $|G| = |N||G/N|$, so the comparison with factoring integers is appropriate. Decomposing groups in this way is subtler than the case of integers though. First of all, there are multiple groups of most orders, so given N and G, it may not be immediately clear what G/N would be. Second, while $|N|$ is a subgroup of G, there is no guarantee that $|G/N|$ is. Third, the decomposition of $|G|$ need not be unique to G. The simplest case is K_4 and C_4. In both cases C_2 is a normal subgroup, however, $K_4/C_2 = C_2$ and $C_4/C_2 = C_2$.

3.6 The Extension Problem

Nonetheless, such decompositions reveal a new path towards classifying the finite groups.

Definition: Given two groups A and B, an *extension* of B by A is the group G such that $A \trianglelefteq G$ and $B = G/A$.

1. ☺ Confirm this is indeed a group.

Definition: A simple group is a group with no nontrivial normal subgroups.

As noted above, an extension need not be unique. However, if given two groups A and B, it was possible to identify the extensions of G then we would be able to identify every group with a normal subgroup. This concept is known as the Extension Problem, and is a significant unsolved problem in mathematics. There are some well understood extensions, the direct product and the semidirect product are two examples, but there are many extensions that these do not describe. Nonetheless, if we had a more complete understanding of extensions and knew which groups were simple (the equivalent of primes in the integer factoring analogy) we would be able to **identify any group of finite order**.

The second part of this goal has been accomplished. The Classification of Finite Simple Groups was a major mathematical undertaking of the twentieth century, and declared complete in 2004. The classification identifies each family of simple groups, proves their simplicity, and shows that there are no others. The proof of the classification is made up of thousands of pages from many papers and authors, and is far beyond the scope of this paper. We shall, however, give a brief overview.

4. The Classification of Finite Simple Groups

There are three infinite families of simple groups, and an additional 26 "sporadic" groups. We shall give an overview each family, however all of the sporadic groups are complicated (ranging from very complicated to unimaginably complicated) -to be written-

4.1 Cyclic Groups of Prime Order

The ~~simplest~~ least complicated family of simple groups are the cyclic groups of prime order. We saw previously that by Lagrange's Theorem, a group of prime order has no nontrivial subgroups, so it certainly has no nontrivial normal subgroups. By Theorems 7 and 8, for any prime p, C_p exists and is unique, so these make up a family of finite simple groups.

These are in fact the only abelian simple groups, and it is possible to show that every abelian group may be formed by extensions of these groups. This extension process, called direct products, is well understood, so the abelian groups have been completely classified.

4.2 Alternating Groups

We have considered the symmetric groups S_n, the permutations of n arranged elements. A transposition is a permutation that changes only two elements in the arrangement. It should not be surprising that every permutation in S_n may be generated by a sequence of transpositions. This sequence of transpositions is by no means unique, but perhaps surprising is that the parity of the sequence is. Thus, we are able to classify permutations as being either "even" or "odd" based on the parity of their transposition decompositions. The set of even permutations on n elements form a subgroup of S_n, known as the alternating group on n elements, and is denoted A_n.

Definition: Given a group G, $a, b \in G$ are *conjugates* if $ag = gb$ for some $g \in G$. The set $\{b \mid ag = bg \text{ for some } g \in G\} = a^G$ is the *conjugacy class* of a in G.

Theorem 14: The conjugacy classes of a group partition the group.

Proof: Let $a \sim b$ indicate that a and b are conjugates. Then clearly $a \sim a$ because $a1 = 1a$. If $a \sim b$, then $ag = gb$ for some $g \in G$, and $bg^{-1} = g^{-1}a$, so $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $ag = gb$ and $bh = hc$ for some $g, h \in G$. Therefore $g^{-1}agh = hc$, so $a(gh) = (gh)c$ and $a \sim c$. Thus, conjugacy is an equivalence relation, and partitions the group. ■

Theorem 15: Suppose $N \lhd G$. If $a \in N$, then $a^G \subset N$.

Proof: The proof follows trivially from the definition of a normal subgroup. Let $ag = gb$ for some $g \in G$. If $a \in N$, then $ag \in gN$, so $gb \in gN$, and $b \in N$.

Thus, conjugacy classes give us a powerful tool for identifying normal subgroups. When combined with Lagrange's Theorem, we know that a normal subgroup must be the union of some conjugacy classes, and its order must divide the order of the group. The following is an important example of how these facts may be used.

Theorem 16: A_5 is simple.

Proof: The conjugacy classes of A_5 are the identity, cycles of three elements, pairs of nonintersecting transpositions, and cycles of five elements (split into two classes). The size of these conjugacy classes are $1, 15, 20, 12$, and 12 respectively. Note that these do indeed sum to $|A_5| = 60$. A nontrivial normal subgroup must contain the identity and at least one other conjugacy class, however, the order of any such combination of conjugacy classes will not divide 60. Therefore A_5 has no normal subgroup.

Using this, it may be shown by induction that A_n is simple for all $n \geq 5$. The proof of this is just beyond the scope of this paper, but uses similar ideas of combining information about the conjugacy classes with the order of A_n. Thus, we have another infinite family of finite simple groups.

4.3 Groups of Lie Type

The remaining finite simple groups, the groups of Lie type and the sporadic groups are far more complicated, and most of their descriptions, let alone the proofs of their simplicity, are far beyond the scope of this paper. Nonetheless, we shall endeavor to obtain some level of understanding of them, and where additional investigations may lead. Much of the remained of this paper follows from a Yale Mathematical Monograph summarizing Michael Aschbacher's 1978 lectures on the then-current state of the classification project [1].

The groups of Lie type are named for their similarity to a class of Lie groups. The study of Lie groups is a very important branch of algebra in its own right, but it will not be necessary for

this paper. We previously mentioned the group $GL_n(\mathbb{R})$, the group of $n \times n$ invertible matrices with real value entries. $GL_n(\mathbb{R})$ is, of course, infinite because $\mathbb{R}$ is infinite, but if $\mathbb{R}$ were replaced with a finite field $\mathbb{F}_q$, where q is the order of $\mathbb{F}$, then $GL_n(\mathbb{F}_q)$ would also be finite (of order q^{n^2}). $GL_n(\mathbb{R})$ has some interesting subgroups, and some of these subgroups, when considered over finite fields, are simple. These are the groups of Lie type. In total there are sixteen classes of the groups of Lie type. We shall specifically describe how three of them are constructed. Their simplicity will be stated without proof.

The *special linear group* $SL_n(\mathbb{R})$ is the subset of matrices in $GL_n(\mathbb{R})$ with determinant 1. The *scalar transformation group* $Z_n(\mathbb{R})$ is the set of scalar transformations in $GL_n(\mathbb{R})$. $Z_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$ since scalar multiplication is commutative, so $GL_n(\mathbb{R})/Z_n(\mathbb{R})$ is well defined and called the *projective linear group*, $PGL_n(\mathbb{R})$. The projective special linear group, $PSL_n(\mathbb{R})$ is classes the matrices in $PGL_n(\mathbb{R})$ with determinant 1. The orthogonal group $O_n(\mathbb{R})$ is the set of orthogonal matrices in $GL_n(\mathbb{R})$, the special orthogonal group $SO_n(\mathbb{R})$ is the set of orthogonal matrices with determinant 1.

Example 4.1: $PSL_n(\mathbb{F}_q)$ is a simple group for $n \neq 1$, except in the cases that $n = 2$ and $q \leq 3$.

Example 4.2: $SO_{2n+1}(\mathbb{F}_q)$ is a simple group for $n > 1$, except when $n = q = 2$.

The bulk of the classification theorem concerns the proof that that these sixteen classes of groups of Lie type, along with the alternating and prime cyclic groups, are all of the finite simple groups, with a small number of exceptions known as the sporadic groups.

4.4 The Sporadic Groups

In total there are 26 sporadic groups, and while some have been known of since they were described by Mathieu in 1861, their complete discovery and the proof of their simplicity took decades of concentrated study. They range from the Mathieu 11, M_{11} group, of order 7920, to the Monster Group of order $\approx 10^{53}$. The monster group itself is large enough that it contains 19 of the other sporadic groups as subgroups [1].

M_{11} is small enough to be understood without additional machinery. It is isomorphic to any subgroup of S_{11} generated by any 11-cycle, and any double 4-cycle. An elementary proof of its simplicity exists, but requires familiarity with the Sylow theorems [2].

Conclusion

The classification project has cemented the importance of the extension problem and enabled new paths of research into to the finite group isomorphisms. The complexity of the proof and its disjoint nature remain significant barriers for anyone intending to research the subject, and no one person understands the entirety of it. However there has been progress towards collecting and simplifying the proof [3]. With continued effort we may someday be able to recognize the structure of a group as easily as we can the size of a set, or at least the factors of an integer.

References

1. Aschbacher, Michael. “The Finite Simple Groups and Their Classification.” James K. Whittmore Lectures in Mathematics.

2. Chapman, Robin J. “An Elementary Proof of the Simplicity of the Mathieu Groups M 11 and M 23.” *The American Mathematical Monthly*, vol. 102, no. 6, 1995, pp. 544–545., doi:10.2307/2974771.

3. Gorenstein, Daniel, et al. “The Finite Groups of Lie Type.” *Mathematical Surveys and Monographs The Classification of the Finite Simple Groups, Number 3*, 1997, pp. 31–89., doi:10.1090/surv/040.3/02.

4. Jansen, Laurens, and Michael Boon. *Theory of Finite Groups, Applications in Physics: Symmetry Groups of Quantum Mechanical Systems*. North-Holland, 1967.