Finite and Sporadic Groups

Niva Sethi

June 14, 2023

1 Introduction

In this paper, we explore finite simple groups, in particular sporadic groups. To do this, we begin with a short review of group theory. Then we briefly go over finite simple groups. 26 finite groups exhibit exceptional behaviors, called sporadic groups. There are four classes of sporadic groups. The five Mathieu groups make up the first class. The seven groups related to the Leech lattice, including the three Conway groups, make up the second class. The third and highest class contains the Monster group and seven related groups. Finally, we go over the six pariah groups.

2 Group Theory

Before we define a group, we must define a binary operation.

Definition 2.1. If G is a nonempty set, a *binary operation* μ on G is a function $\mu : G \times G \to G$.

Now we can define a group.

Definition 2.2. A *group* (G, $*$) is a set G with binary operation $*\colon G \times G \to G$ that satisfies:

1. *(closure)* $g * h \in G$. We say that G is closed under $*$.
2. *(associativity)* for any $g, h, i \in G$ we have $(g * h) * i = g * (h * i)$.
3. *(identity)* $e * g = g * e = g$ for all $g \in G$.
4. *(inverse)* Every element $g \in G$ has an inverse g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Definition 2.3. The *order of an element* $g \in G$, written as $o(g)$, is the smallest natural number n, such that $g^n = e$. If no n exists we say the element has an *infinite order*.

There are many different types of groups. Here are some basic ones.

Definition 2.4. A *finite group* is one with only a finite number of elements.

Definition 2.5. The *order* of a finite group, written $|G|$, is the number of elements in G.

Definition 2.6. An *abelian group* is a group that satisfies commutativity, which states that $a * b = b * a$ for all $a, b \in G$.

Definition 2.7. A group is called a *cyclic group* if it is generated by a single element. For example, a cyclic group G with generator g can be written as

$$G = \langle g \rangle = \{..., g^{-3}, g^{-2}, g^{-1}, 0, g^1, g^2, g^3, ...\}$$

Before we define a *infinite group*, we must define the *order* of a group.

Definition 2.8. The *order* of a group G is the number of elements in group G. It is written as $|G|$.

Definition 2.9. An *infinite group* is a group of infinite order.

Definition 2.10. The *order of an element* $g \in G$, written $o(g)$, is the smallest natural number$n$ such that $g^n = e$ if such a number exists. If no such n exists, we say g has an *infinite order*.

Now let's define isomorphisms and homomorphisms.

Definition 2.11. Two groups $(G, *)$ and $(H, \circ)$ are said to be *isomorphic* if there is a one-to-one correspondence $\theta : H \to G$ such that

$$\theta(g_1 * g_2) = \theta(g_1) \circ \theta(g_2)$$

for all $g_1, g_2 \in G$.

The mapping θ is called an *isomorphism* and we say that G is *isomorphic* to H (written as $G \cong H$).

Definition 2.12. If θ satisfies the previously mentioned property but is not a one-to-one correspondence, we say θ is *homomorphism*.

Definition 2.13. An *automorphism* of a group G is an isomorphism of the group with itself. We denote by $Aut(G)$ the set of all automorphisms of G.

Definition 2.14. A homomorphism

$$f : G \to G$$

of a group into itself is called an *endomorphism*.

Definition 2.15. Given a homomorphism $\phi : G \to G'$, we define its *kernel* $\ker \phi$ to be the set of $g \in G$ that get mapped to the identity element in a G' by ϕ. Its image $\phi(G) \subset G'$ is its image as a map on the set G.

Lagrange's Theorem is one of the central theorems of Abstract Algebra and its proof uses several important ideas, including cosets.

First, let's define a left and right coset.

Definition 2.16. Given a subgroup $H \leq G$ and element $g \in G$, the *left coset* is a subset of G of the form $gH := \{gh : h \in H\}$.

Definition 2.17. Similarly, the *right coset* would be $Hg := \{hg : h \in H\}$.

Now let's look at three lemmas.

Lemma 2.18. *If $H \leq G$ there is a one-to-one correspondence between H in any coset of H.*

Lemma 2.19. *If $H \leq G$, then the left coset relation, $g_1 \sim g_2$ if $g_1H = g_2H$ is an equivalence relation.*

Lemma 2.20. *Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.*

With these in mind let's look at Lagrange's Theorem and prove it.

Theorem 2.21 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then $|H|$ will divide $|G|$.*

Proof. Let $\sim$ be the left coset equivalence relation we defined in the second lemma. The last lemma states that any two distinct cosets of $\sim$ are disjoint. This means we can say

$$G = (g_1H) \cup (g_2H) \cup ... \cup (g_nH)$$

The first lemma shows that the order of each coset is the same as the order of H, so

$$|G| = |g_1H| + |g_2H| + ... + |g_nH| = n|H|$$
$$|G| = n|H|$$

showing that $|G|$ is divisible by $|H|$.

Definition 2.22. A subset $H \subseteq G$ is a *subgroup* of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

We write $H \leq G$ if H is a subgroup of G.

Definition 2.23. The *centre* of a group G is the subset

$$Z(G) = g \in G | gx = xg for all x \in G$$

It is a subgroup.

Definition 2.24. If also $H \neq G$, we say that H is a *proper subgroup* and write $H < G$.

The most important subgroups in group theory are the normal subgroup.

Definition 2.25. A subgroup $N \leq G$ is called *normal* (written $N \trianglelefteq G$) if for all $g \in G$, we have the equality of cosets

$$gN = Ng$$

which is often expressed equivalently as

$$gNg^{-1} = N$$

.

Definition 2.26. A group G is said to be *simple* if it has no normal subgroups other than G and e.

Definition 2.27. We call the number of distinct cosets of H in G the index of H in G, written $|G : H|$.

Definition 2.28. If $N \trianglelefteq G$, then we define the *quotient group* G/N (read G mod N) to be the set of cosets gN of N in G with the group law

$$(gN)(hN) = (gh)N$$

If $N \leq G$ is not normal, then G/N still denotes the set of cosets of N in G, but the above operation is no longer well-defined.

Definition 2.29. Let G be a group and let $a, b \in G$. The product $aba^{-1}b^{-1}$ is called the *commutator* of a and b. We write $[a, b] = aba^{-1}b^{-1}$. $[a, b] = e$ if and only if a and b commute.

Definition 2.30. Let G' be the subgroup of G which is generated by the set of all commutators of elements of G, that is

$$G' = gp(\{[x, y] | x, y \in G\}).$$

G' is called the *commutator (or derived) subgroup* of G.

With these things in mind, we can look at an interesting theorem and prove it.

Theorem 2.31. *Let G' be a communicator subgroup of G. G/G' is an abelian group. Moreover, if $N \trianglelefteq G$ such that G/N is abelian, then $G' \subset N$.*

Proof. In order to prove the first part of the theorem, let aG' and bG' be any two elements of G/G'. Then

$$\begin{aligned}[aG', bG'] &= aG' \cdot bG'(aG')^{-1}(bG')^{-1} \\ &= aG' \cdot bG'a^{-1}G' \cdot b^{-1}G' \\ &= aba^{-1}b^{-1}G'\end{aligned}$$

$$= G'$$

because $[a, b] \in G'$. In other words, any two elements of G/G' commute. This means G/G' is abelian. Now let $N \lhd G$. If N does not contain G', then N cannot contain all commutators of elements of G Thus let $a, b \in G$ be such that $[a, b] \notin N$. Then $[aN, bN] = aba^{-1}b^{-1}N = [a, b] \neq N$. Hence G/N is non-abelian. Then taking the contrapositive, we can prove the theorem. □

3 Finite Simple Groups

There are 18 families of finite simple groups. The first is the cyclic Abelian Groups Z_p with order p when p is a prime number. The next family consists of the Alternating Groups A_n when $n > 4$ with order $n!/2$. The other 16 families are Groups of Lie Type, or finite groups that are closely related to the group of rational points of a reductive linear algebraic group with values in a finite field. There are also 26 finite simple groups that four infinite families of finite simple groups. These are called sporadic groups.

Theorem 3.1 (Classification Theorem of Finite Groups)**.** *The finite simple groups can be classified completely into:*

1. *Cyclic groups Z_p of prime group order.*
2. *Alternating Groups A_n where $n > 4$.*
3. *Lie-type Chevalley groups.*
4. *Lie-type.*
5. *Sporadic groups.*

The proof for this theorem is long and extensive and is said to span over 15,000 pages.

4 Sporadic Groups

There are four classes of sporadic groups. The first class is made up of the five Mathieu groups. The seven groups related to the Leech lattice, including the three Conway groups, make up the second class. The third and highest class contains the Monster group and seven related groups. Lastly, there are the Pariah groups. However, before we go over the classes of sporadic groups, we must define transitive group actions.

4.1 Transitive Group Actions

Definition 4.1. The *orbit* of an element $s \in S$ is $orb(s) = \{gs | g \in G\}$.

Definition 4.2. An action of a group on a nonempty set is *transitive* if there is exactly one orbit. For any $x_1, y_1 \in Sthereexistsg$ such that $y_1 = gx_1$. If, for every two pairs of points x_1, x_2 and y_1, y_2, there is a group element g such that $y_i = gx_i$, then the group action is *2-transitive*. In general, a group action is *k-transitive* if every set $\{x1, ..., yk\}$ of 2k distinct elements has a group element g such that $y_i = gx_i$.

Definition 4.3. Let $\alpha : G \bullet E \to E$ be a group action of G on the set E. Also, let $x \in E$. Then

$$Stab(x) = g \in Gs.t.g \cdot x = x$$

is the stabilizer of x.

Definition 4.4. An action is *free* if for all $s \in S$, $gs = s$ implies $g = e_G$. Hence, only the identity element fixes any s.

Definition 4.5. An action is *sharply transitive* if it is transitive and free.

4.2 Mathieu Groups

The discovery of the earliest sporadic groups is attributed to Émile Léonard Mathieu between 1861-1873. The Mathieu groups were introduced because of interest in multiply transitive permutation groups other than symmetric groups and alternating groups.

Group	Order	Transitivity
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	sharp 4-fold
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	sharp 5-fold
M_{21}	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	2-transitive
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	3-transitive
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	4-transitive
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	5-transitive

4.3 The Leech Lattice and Conway Groups

The Leech lattice $\Lambda 24$ was discovered by John Leech in 1967 while trying to optimize sphere packing in higher dimensions. In 1968, John Conway discovered that the automorphism group of the Leech lattice is a group of order

$$|Aut(\Lambda 24)| \equiv |Co_0| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$$

Co_0 itself is not simple but has simple subquotients that form sporadic groups. Below are the orders of the Conway Groups.

Group	Order
$Conway_1, Co_1$	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
$Conway_2, Co_2$	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
$Conway_3, Co_3$	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Higman-Sims, HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
McLaughlin, McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Hall-Janko, H or J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
Suzuki, Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7$

4.4 Monster Group

The monster M, was completed in 1982 and is the largest of the sporadic groups. It is also known as the Fischer-Griess monster because Fischer and Robert Griess were both instrumental to the construction of it. Fischer was also responsible for the baby monster B and another triplet of sporadic made up of Fi_{22}, Fi_{23} and Fi_{24}, which are analogous to the second Mathieu series made up of M_{22}, M_{23}, and M_{24}. The monster is of the order:

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8.08 \times 10^{53}$$

The baby monster is of the order:

$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \approx 4.15 \times 10^{33}$$

Group	Order
Monster, M	$\approx 8 \cdot 10^{54}$
Baby Monster, B	$\approx 4 \cdot 10^{33}$
$Fischer_{24}, Fi_{24}$	$\approx 1 \cdot 10^{24}$
$Fischer_{23}, Fi_{23}$	$\approx 4 \cdot 10^{18}$
$Fischer_{22}, Fi_{22}$	$\approx 6 \cdot 10^{13}$
Harada–Norton, HN	$\approx 2 \cdot 10^{14}$
Thompson, Th	$\approx 9 \cdot 10^{17}$
Held, He	$\approx 4 \cdot 10^9$

4.5 Pariahs

There are six Pariah groups that share no significant relationship with the aforementioned sporadic groups. The Pariah groups are shown below.

Group	Order
Rudvalis, Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
O'Nan, ON	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
$Lyons_{24}, Ly$	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
$Janko_4, J_4$	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
$Janko_3, J_3$	$2^7 \cdot 3^5 5 \cdot 17 \cdot 19$
$Janko_1, J_1$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$

5 Acknowledgements

I would like to thank the MIT PRIMES Circle program, as well as my mentor Gabrielle Kaili-May Liu. I would also like to thank the organizers Mary and Marisa for providing me with this wonderful opportunity to expand my knowledge and love for math through the MIT PRIMES Program. Finally, I would like to thank my parents for supporting me throughout this program.

6 References

Keith Conrad. "Transitive Group Actions". 2009.

David S. Dummit and Richard M. Foote. Abstract Algebra. 3rd ed. Wiley, 2004.

G. Michler. Theory of finite simple groups. New mathematical monographs. Cambridge; New York: Cambridge University Press, 2006.