On the Classification of Finite Simple Groups

Gracie Sheng

May 22, 2022

Abstract

This paper examines the properties of finite simple groups, which arise from the decomposition of groups into normal subgroups and a quotient group. Finite simple groups are identified by isomorphism to cyclic groups of prime order, alternating groups, groups of Lie type, and sporadic groups.

1 Introduction

The comprehensive classification of finite simple groups is attributed to Daniel Gorenstein in 1983. However, it was not declared complete until revisions were made by Aschbacher and Smith correcting the proof, which initially totaled over 10,000 pages. In this paper, we explore the properties and applications of finite simple groups. We begin by discussing basic definitions and theorems in group theory. We proceed to examine normal subgroups and quotient groups, as well as the isomorphism theorems. We discuss theorems relevant to the structure of simple groups, including the Feit-Thompson Theorem, Jordan-Hölder Theorem, and the classification theorem. Finally, we investigate the groups isomorphic to finite simple groups, specifically the 26 outlying sporadic groups.

2 Groups and Subgroups

Definition 2.1. A *group* is a finite or infinite set G together with a binary group operation $\circ : G \times G \to G$ that fulfill the group axioms:

(i) *Closure:* For all $g, h \in G$, the element $g \circ h \in G$.

(ii) *Associativity:* For $f, g, h \in G$, we have

$$(f \circ g) \circ h = f \circ (g \circ h).$$

(iii) *Identity:* There exists an *identity* element $e \in G$, such that

$$e \circ g = g = g \circ e$$

for all $g \in G$.

(iv) *Inverse:* For each $g \in G$, there exists an *inverse* element $g^{-1} \in G$ such that

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

In the remainder of this paper, we omit the symbol $\circ$ for the group operation for convenience. For example, $g \circ h$ may simply be written as gh.

Definition 2.2. The *order* of a group G is its cardinality. The order of G is denoted by $|G|$.

Definition 2.3. Let G be a group. The subset H of G is a *subgroup* of G if it satisfies the group axioms under the binary operation of G. This relation is denoted as $H \leq G$.

Definition 2.4. A *homomorphism* is a map $\phi : G \to H$ such that

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in G$.

Definition 2.5. Given a homomorphism $\phi : G \to H$, the *kernel* of ϕ is defined by $\ker \phi = \{g \in G \mid \phi(g) = e_H\}$. In other words, the kernel consists of all of elements of G that map to the identity element in H.

Subgroups and homomorphisms are important in group theory because they preserve group structure and operation, respectively, while simplifying the given group into a more manageable structure.

Definition 2.6. A homomorphism $\phi : G \to H$ is an *isomorphism* if ϕ is a bijection. This relation is denoted as $G \cong H$. Isomorphic groups share the same group structure.

Definition 2.7. A group G is *cyclic* if G can be generated by a single element, that is, if there is some element $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$. We say that G is *generated* by g.

Intuitively, we understand that cyclic groups vary based on the order of the generator. Accordingly, the below result demonstrates that the structure of a cyclic group is distinguished by its order.

Theorem 2.8. *Any two cyclic groups of the same order are isomorphic.*

Proof. Let G_1, G_2 be cyclic groups of finite order n. Let

$$G_1 = \langle a \rangle = \{a^0, a^1, a^2, ..., a^{n-1}\},$$
$$G_2 = \langle b \rangle = \{b^0, b^1, b^2, ..., b^{n-1}\}.$$

Define the bijection $\phi : G_1 \to G_2 : \phi(a^i) \to \phi(b^i)$. We prove that ϕ is a homomorphism. Consider $a^r, a^s \in G_1$. Thus

$$\phi(a^r a^s) = \phi(a^{r+s}) = b^{r+s} = b^r b^s = \phi(a^r)\phi(a^s).$$

Hence ϕ is a homomorphism. Since ϕ is also bijective, we have the result $G_1 \cong G_2$. □

We often express the cyclic group of order n as Z_n. Every infinite cyclic group is isomorphic to the additive group of $\mathbb{Z}$, the integers. Likewise, every finite cyclic group of order n is isomorphic to the additive group of $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n.

Definition 2.9. For any $H \leq G$ and any $g \in G$, a *left coset* is obtained by multiplying H on the left by a fixed element g. A left coset is denoted as $gH = \{gh \mid h \in H\}$. Similarly, a *right coset* is denoted as $Hg = \{hg \mid h \in H\}$. The *index of a subgroup* H in G, denoted by $[G : H]$ is the cardinality of the left (or right) coset space G/H.

Cosets are significant, as they partition a group into equivalence classes. Observations of cosets help us to prove one of the most applicable theorems in group theory, Lagrange's Theorem.

Theorem 2.10 (Lagrange)**.** *If G is a finite group and $H \leq G$, then the order of H divides the order of G. The number of cosets of H in G is $\frac{|G|}{|H|}$.*

Proof. Let $H \leq G$. Each left coset of H in G has the same cardinality as H, so $\forall g \in G$, we have $|gH| = |H|$. Since left cosets are identical or disjoint, each element of G is in exactly one coset. By definition of index of a subgroup, there are $[G : H]$ left cosets. Hence $|G| = [G : H]|H|$ and the result follows.

Now let G be of infinite order. If $[G : H]$ is finite, then $|H|$ is infinite. If $|H|$ is infinite, then $[G : H]$ is finite. □

Corollary 2.11. *If G is a group of prime order p, then G is cyclic and $G \cong Z_p$.*

Proof. Let $g \in G$, $g \neq e_G$. Thus $|\langle g \rangle| > 1$ and $|\langle g \rangle| \mid |G|$. Since $|G|$ is prime we have $|\langle g \rangle| = |G|$. Hence $G = \langle g \rangle$ is cyclic. Theorem 2.8 completes the proof. □

Definition 2.12. The *symmetric group* S_n is the group of permutations on n elements under the operation of function composition. The elements of S_n are given by bijective functions $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Definition 2.13. A *transposition* is a 2-cycle. The *sign of* σ is denoted by $\epsilon(\sigma)$. A permutation of a finite set is *even* if it can be written as an even number of transpositions, when $\epsilon(\sigma) = 1$. A permutation is *odd* if it can be written as an odd number of transpositions, when $\epsilon(\sigma) = -1$.

Remark 2.14. Transpositions are all odd permutations and ϵ is a surjective homomorphism.

Theorem 2.15. *A permutation of a finite set of two or more elements is a product of transpositions. In other words, every element of S_n may be written as a product of transpositions. In particular, no permutation in S_n may be written as both an even and odd number of transpositions.*

Definition 2.16. The *alternating group of degree* n, denoted by A_n, is the group of even permutations of a finite set. Note that by Theorem 3.4 (First Isomorphism Theorem), $S_n/A_n \cong \epsilon(S_n) = \{\pm 1\}$. It follows that $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}(n!)$.

3 Normal Subgroups and Quotient Groups

The study of cosets motivates discussion of normal subgroups and quotient groups, which are central to the isomorphism theorems, the first of which is presented in this section.

Definition 3.1. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the *conjugate* of N by g. If $gNg^{-1} = N$, the element g is said to *normalize* N. The subgroup N of a group G is *normal* if $gNg^{-1} = N$, or equivalently $gN = Ng$, for all $g \in G$, i.e. if every element of G normalizes N. This relation is denoted as $N \trianglelefteq G$.

Example 3.2. Let G be a group. Then $\{e_G\}$ and G are normal subgroups of G.

Proof. To show that $\{e_G\}$ is normal, let $g \in G$. The only element of $\{e_G\}$ is e_G, and $ge_Gg^{-1} = e_G \in \{e_G\}$. Hence $\{e_G\}$ is normal.

To show that G is normal, let $g, n \in G$. Then $\forall n \in G$ we have $gng^{-1} \in G$. Therefore G is normal by definition. □

Definition 3.3. Given a group G and a normal subgroup N, the *quotient group* G/N is the set of cosets of N in G.

Theorem 3.4 (First Isomorphism Theorem)**.** *Let G, H be groups, and let $\phi : G \to H$ be a homomorphism. Then $\ker\phi \trianglelefteq G$ and $G/\ker\phi \cong \phi(G)$.*

Proof. We first verify $gng^{-1} \in \ker\phi \ \ \forall g \in G$ and $n \in \ker\phi$. To show that the identity element of G is an element of $\ker\phi$, consider $\phi(e_Gg) = \phi(e_G)\phi(g)$. Since $\phi(e_Gg) = \phi(g)$, we have

$$\phi(e_G)\phi(g) = \phi(g)\ \forall g \Rightarrow \phi(e_G) = e_H \Rightarrow e_G \in \ker\phi.$$

Similarly, we show that inverses are in the kernel. For any $n \in \ker\phi$, we have

$$\phi(n^{-1}) = \phi(n)\phi(n^{-1}) = \phi(nn^{-1}) = \phi(e_G) = e_H$$

$$\Rightarrow \phi(n^{-1}) = e_H\ \forall n \in \ker\phi \Rightarrow n^{-1} \in \ker\phi.$$

The kernel is closed since $\forall n, m \in \ker\phi$, we have

$$\phi(nm) = \phi(n)\phi(m) = e_H \Rightarrow nm \in \ker\phi.$$

We complete the first part of the proof by demonstrating that every element of G normalizes the kernel:

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H$$

$$\Rightarrow gng^{-1} \in ker\phi\ \forall g \in G, n \in \ker\phi \Rightarrow \ker\phi \trianglelefteq G$$

For simplicity, in the second part of this proof, we express $\ker\phi$ as K. Now we consider the quotient group $G/K = \{gK \mid g \in K\}$ under coset multiplication. Consider the homomorphism $\tilde{\phi} : G/K \to \phi(G)$ defined by $gK \mapsto \phi(g)$. In order

for G/K to be isomorphic to the image of G, the function must be bijective. Since any function is surjective into its image, it remains to show that the function is injective. Let $aK, bK \in G/K$ be such that $\phi(aK) = \phi(bK)$. Then

$$\tilde{\phi}(a) = \tilde{\phi}(b) \Rightarrow \tilde{\phi}(b^{-1}a) = e_H \Rightarrow b^{-1}a \in K.$$

We write $b^{-1}a = k \in K$ so that $a = bk \in bK$. Hence $a \in aK \cap bK$. It follows that $aK = bK$. This completes the second part of the proof. □

4 Finite Simple Groups

The classification of finite simple groups is one of the most fundamentally important achievements in algebra. For every group that is not simple, its normal subgroups and quotient group can eventually be decomposed into simple composition factors analogous to the prime factorization of integers. Thus a statement regarding a group is reduced to a problem of its simple constituents.

Definition 4.1. A nontrivial group G is *simple* if its only normal subgroups are the identity and itself.

Definition 4.2. A *composition series* in group G is a sequence of subgroups

$$\{e\} = H_0 \leq H_1 \leq H_2 \cdots \leq H_{k-1} \leq H_k = G$$

for which $H_i \trianglelefteq H_{i+1}$ and each *composition factor* H_{i+1}/H is a simple group for $0 \leq i \leq k-1$.

Example 4.3. The cyclic group Z_{12} satisfies the following composition series:

$$\{e\} \trianglelefteq Z_3 \trianglelefteq Z_6 \trianglelefteq Z_{12}$$

Composition factors: $Z_{12}/Z_6 \cong Z_2, Z_6/Z_3 \cong Z_2, Z_3/Z_1 \cong Z_3$

$$\{e\} \trianglelefteq Z_2 \trianglelefteq Z_6 \trianglelefteq Z_{12}$$

Composition factors: $Z_{12}/Z_6 \cong Z_2, Z_6/Z_2 \cong Z_3, Z_2/Z_1 \cong Z_2$

$$\{e\} \trianglelefteq Z_2 \trianglelefteq Z_4 \trianglelefteq Z_{12}$$

Composition factors: $Z_{12}/Z_4 \cong Z_3, Z_4/Z_2 \cong Z_2, Z_2/Z_1 \cong Z_2$.

Theorem 4.4 (Jordan-Hölder)**.** *Let G be a nontrivial finite group. Then G has a composition series and the composition factors in a composition series are unique.*

Theorem 4.5 (Feit-Thompson)**.** *If G is a simple group of odd order, then $G \cong Z_p$ for some prime p.*

Theorem 4.6 (Classification Theorem, Gorenstein)**.** *Every finite simple group is isomorphic to one of the following:*

(i) A cyclic group of prime order;

(ii) An alternating group;

(iii) A member of one of sixteen infinite families of groups of Lie type; or

(iv) One of 26 sporadic groups not isomorphic to any of the above groups.

Theorem 4.7. *Simple abelian groups are cyclic groups of prime order.*

Proof. ($\Rightarrow$) *If G is a simple abelian group, then the order of G is prime.*
Suppose that G is a simple abelian group. Then G is a nontrivial group by definition. We first show that G is a finite group. Let $g \in G$ be a nonidentity element. Then $\langle g \rangle \leq G$. Since G is abelian, every subgroup of G is normal. Since G is simple, we must have $\langle g \rangle = G$. If the order of g is not finite, then $\langle g^2 \rangle$ is a proper normal subgroup of $\langle g \rangle = G$, but G is simple. Thus the order of g is finite. Hence $G = \langle g \rangle$ is a finite group. Let $|g| = |G| = p$. FSOC assume that $p = mn$ is a composite number with integers $m > 1, n > 1$. Then $\langle g^m \rangle$ is a proper normal subgroup of G, but G is simple, so p must be prime.

($\Leftarrow$) *If the order of G is prime, then G is a simple abelian group.*
Now suppose that the order of G is a prime. Let $g \in G$ be a nonidentity element. Then $|\langle g \rangle| \mid |G|$. Hence $|\langle g \rangle|$ must be p. Therefore we have $G = \langle g \rangle$, and G is a cyclic group and in particular an abelian group. Since any normal subgroup $H \leq G$ has order 1 or p, H must be either trivial or G itself. Hence G is simple. Thus G is a simple abelian group. □

Theorem 4.8. *A_n is a simple group for $n \geq 5$.*

We outline the proof of the above theorem:

1. For $n \geq 3$, A_n contains every 3-cycle.
2. For $n \geq 3$, A_n is generated by the 3-cycles
3. Let r, s be distinct fixed elements of $\{1, 2, ..., n\}$ for $n \geq 3$. Then A_n is generated by the n 3-cycles of the form (r, s, i) for $1 \leq i \leq n, i \neq r, i \neq s$.
4. Let $N \trianglelefteq A_n$ for $n \geq 3$. If N contains a 3-cycle, then $N = A_n$.
5. Let N be a nontrivial normal subgroup of A_n for $n \geq 5$. Then one of the following cases must hold. In each case, $N = A_n$.

   Case I. N contains a 3-cycle.

   Case II. N contains a product of disjoint cycles, at least one of which has length greater than 3.

   Case III. N contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$.

   Case IV. N contains a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$ where μ is a product of an even number of disjoint 2-cycles.

   Case V. N contains a disjoint product σ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$ where μ is a product of an even number of disjoint 2-cycles.

5 Sporadic Groups

Of the 26 sporadic groups, the 20 subquotients of the monster group are referred to as the "Happy Family," whereas the remaining 6 as "Pariah groups." Before describing the first generation of the Happy Family known as Mathieu groups, we will provide background on transitive group actions.

Definition 5.1. A group G *acts* on a set S when there is a map $G \times S \to S$ such that the following conditions hold for all $s \in S$.

(i) *Identity:* The action of the identity element in G on every element $s \in S$ gives S.

$$e_G s = s$$

(ii) *Associativity:* For $g, h \in G$ and $s \in S$,

$$g(hs) = (gh)s$$

Definition 5.2. The *orbit* of an element $s \in S$ is $\text{orb}(s) = \{gs \mid g \in G\}$, equivalently the set of objects that each s is sent to under the action of G.

Definition 5.3. A action of a group on a nonempty set is *transitive* if there is exactly one orbit. For any $x_1, y_1 \in S$, $\exists g$ 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 $\{x_1, ..., y_k\}$ of $2k$ distinct elements has a group element g such that $y_i = gx_i$.

Example 5.4. For $n \geq 1$, the usual action of S_n on $\{1, 2, \ldots, n\}$ is transitive since there is a permutation sending 1 to every other number in the set. Thus the orbit of 1 is $\{1, 2, \ldots, n\}$.

Example 5.5. For $n \geq 3$, the usual action of A_n on $\{1, 2, \ldots, n\}$ is transitive since the 3-cycles $(12n), (13n), \ldots, (1(n-1)n), (1n2)$ send 1 to every other number, so the orbit of 1 is $\{1, 2, \ldots, n\}$.

Example 5.6. If $|S| = 2$, every non-trivial action of G on S is 2-transitive. Let $S = \{s_1, s_2\}$. Then the only ordered pairs of distinct elements are (s_1, s_2) and (s_2, s_1). The identity in G sends each pair to itself, and an element of G that acts non-trivially on S must send each ordered pair to the other.

Definition 5.7. An action is *free* if $\forall s \in S$, $gs = s$ implies $g = e_G$. Hence, only the identity element fixes any s.

Definition 5.8. An action is *sharply transitive* if it is transitive and free.

5.1 First Generation: Mathieu Groups

The discovery of the earliest sporadic groups is attributed to Émile Léonard Mathieu in the period 1861-1873. The Mathieu groups were introduced due to interest in multiply transitive permutation groups apart from 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

The list of known sporadic groups remained sparse until the latter half of the 20th century.

5.2 Second Generation: Leech Lattice

The *Leech lattice* Λ_{24} was discovered by John Leech in 1967 while working on the kissing number problem – to optimize sphere packing in higher dimensions. In 1968, John Conway found that the automorphism group (isometries fixing the center) of the Leech lattice is a group of order

$$|\mathrm{Aut}(\Lambda_{24})| \equiv |\mathrm{Co}_0| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23.$$

Although Co_0 itself is not simple, it has simple subquotients that form sporadic groups. We do not elaborate but include below the orders of the second generation sporadic 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, HJ or J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
Suzuki, Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7$

5.3 Third Generation: Monster Group

The monster M, constituting the top of the third level of sporadic groups, is the largest and is related to 20 of the 26 sporadic groups. Bernd Fischer and Robert Griess were both instrumental to the construction of the Monster, which was completed in 1982. Hence it is also known as the Fischer-Griess monster. Fischer was also responsible for the baby monster B and another triplet of sporadics consisting of Fi_{22}, Fi_{23} and Fi_{24}, which are analogous to the second Mathieu

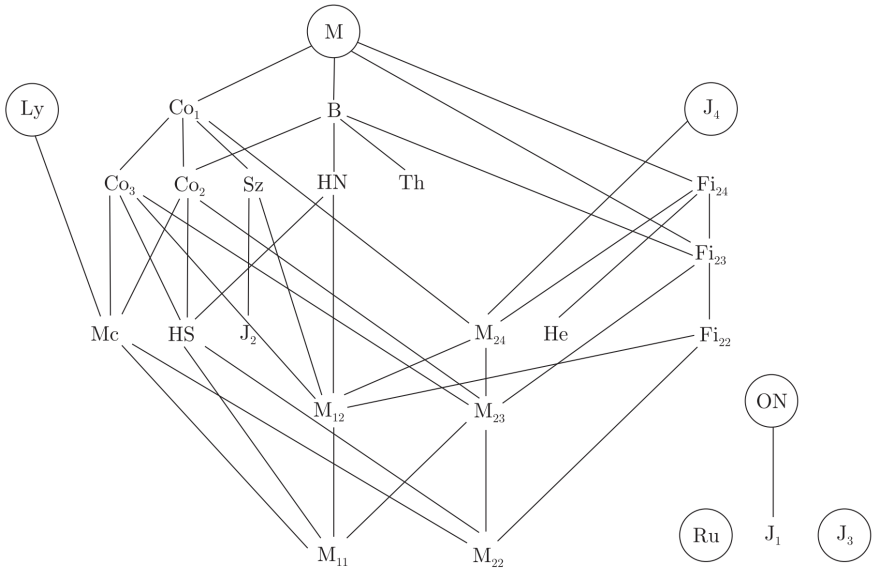

Figure 1: Relationships between the sporadic simple groups.

series consisting of M_{22}, M_{23}, and M_{24}.

Notably, the monster and baby monster are respectively of the orders

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

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

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	$\approx 4 \cdot 10^{9}$

5.4 Pariahs

Each of the 20 members of the Happy Family is considered a subquotient of the Monster group. Still, there exist six Pariah groups that share no significant relationship with the aforementioned sporadic groups. The Pariah groups are exhibited 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	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
Janko$_1$, J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$

6 Acknowledgements

I would like to thank the MIT PRIMES Circle program, coordinators Marisa Gaetz and Mary Stelow, my mentor Gabrielle Kaili-May Liu, as well as my groupmate Evelyn Zhu for their support throughout the past semester.

References

[1] Luis J. Boya. "Introduction to Sporadic Groups". In: *Symmetry, Integrability and Geometry: Methods and Applications* (Jan. 16, 2011). DOI: 10.3842/SIGMA.2011.009.

[2] Keith Conrad. "Transitive Group Actions". 2009.

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

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