An Introduction to the Classification of Finite Simple Groups

Investigating the DNA of Finite Group Theory

By

Maia Traforti

School of Mathematics and Statistics

University of Canterbury

Submitted on: February 12th, 2024
Under the supervision of Brendan Creutz

A research report submitted in partial fulfillment
of the requirements for the degree of

Bachelor of Science (Mathematics)

Contents

1 Introduction

In this report, we examine the Classification of Finite Simple Groups (CFSG), which was (and still is) an absolute game-changer for group theory — as well as many other areas that are touched by the mathematical sciences. The CFSG provides a structural framework for the basic building blocks of all finite group structures, analogous to how prime numbers scaffold the composite numbers, and can be juxtaposed onto a 'periodic table', of sorts. This exposition covers the foundational concepts, principal theorems, and major contributions that have influenced research in this area — as well as a historical narrative to motivate the mammoth amount of work that has gone into this classification theorem.

We begin with the *Fundamental Theorem of Finite Abelian Groups*, which asserts that every finite Abelian group is isomorphic to a direct product of cyclic groups of prime-power order. This theorem delivers a system for understanding finite Abelian groups by decomposing their orders into prime factors and applying number theory to determine their structure. By reducing finite Abelian groups to well-understood cyclic components, the theorem simplifies the study of their properties and behaviours. Following this, we present a formal proof of the Fundamental Theorem of Finite Abelian Groups, developed through a sequence of lemmas that establish the unique decomposition of finite Abelian groups into cyclic groups of prime-power order. We then explore finite non-Abelian groups, which are characterised by their non-commutative nature. We discuss the concepts of subnormal and composition series as tools for systematically breaking down groups into simpler components. The *Schreier Refinement Theorem* and the *Jordan-Hölder Theorem* are discussed, in their ability to allow for the comparison of different group decompositions and ensure that the simple groups forming the building blocks are uniquely determined by the group's structure.

The CFSG is the result of collaborative efforts by mathematicians from all over the world, spanning upwards of 15,000 pages. This paper aims to provide an introductory understanding of the CFSG, its basic concepts, and elude to just some of the beautiful contributions it makes to the far-reaching limbs of mathematics and beyond. It assumes that the reader has a basic knowledge of group theory roughly equivalent to that covered in a second-year undergraduate mathematics course.

2 Preliminaries

2.1 Cosets, Normal Subgroups, and Quotient Groups

Theorem 2.1 (Lagrange's Theorem). *Let G be a finite group and H a subgroup of G. Then the order of H always divides the order of G.*

Proof. Consider the set of distinct left cosets of H in G, which can be denoted as $a_1H, a_2H, \ldots, a_rH$, where a_i are elements of G. By the definition of cosets, for each element a in G, there exists some a_i such that $aH = a_iH$. From the properties of subgroups, we have that a is an element of some coset a_iH, and thus every element of G is contained in some coset of H. Hence, G can be expressed as a union of these cosets:

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH$$

According to the properties of cosets, this union is disjoint, and thus the order of G is the sum of the orders of the distinct cosets:

$$|G| = |a_1H| + |a_2H| + \ldots + |a_rH|$$

Since the order of each coset $|a_iH|$ is equal to $|H|$ for all i, it follows that:

$$|G| = r|H|$$

where r is the number of distinct cosets of H in G, which is also the index $|G : H|$. This demonstrates that $|H|$ divides $|G|$. □

Lagrange's Theorem establishes a fundamental relationship between finite groups and their subgroups, restricting order in a way that provides lucid structural information about the general form subgroups may take in a finite context. Note that the converse of Lagrange's Theorem need not be true.

Definition 2.1 (Normal Subgroup). *A subgroup H of a group G is termed a normal subgroup if it satisfies the condition that all of its left cosets are also its right cosets. That is to say, for every element $a \in G$, the left coset aH is identical to the right coset Ha. We define H to be normal in G, denoted by $H \trianglelefteq G$, if and only if $aH = Ha$, for all $a \in G$.*

This definition encapsulates a symmetry within the group structure, allowing any element of G to commute with the subgroup H in terms of coset formation. Consequently, normal subgroups are invariant under conjugation by elements of G; for any $h \in H$ and any $a \in G$, there exists some $h' \in H$ such that $ah = h'a$. Normal subgroups are the structural underpinnings that permit the construction of quotient groups. The quotient group G/H is well-defined if and only if H is a normal subgroup of G. The normalcy of H ensures that the operation within the quotient group is well-defined and that the group axioms are preserved. In practice, while this definition offers a straightforward criterion for normalcy, verifying that a subgroup is normal can be more efficiently accomplished using other characterizations, such as checking that $aHa^{-1} \subseteq H$ for all a in G. This alternative approach, involving conjugate elements, can simplifies the verification process in practice.

Definition 2.2 (Simple Group). *A group G is termed simple if it satisfies two conditions:*

(i) The group G is nontrivial, meaning G is not the group consisting only of the identity element.

(ii) The only normal subgroups of G are the trivial subgroup $\{e\}$, and G itself.

Intuition 2.1. Simple groups are often likened to the fundamental units in various domains of science and mathematics due to their indivisible nature in the structure of finite group theory. Just as prime numbers serve as the indivisible elements from which all integers are constructed through multiplication, simple groups are those groups that cannot be further decomposed into smaller, nontrivial normal subgroups. This characteristic makes them the irreducible "quarks" or "primes" of finite group theory, serving as the essential building blocks from which more complex group structures can be assembled.

Theorem 2.2 (Quotient Groups). *Let G be a group and let N be a normal subgroup of G. The set of cosets of N in G, denoted by G/N, together with the operation defined by $(aN)(bN) = (ab)N$ for all $a, b \in G$, constitutes a group called the quotient group or factor group of G by N.*

In this group, the coset N containing the identity element of G serves as the identity element of the quotient group, and the inverse of the coset aN is given by $a^{-1}N$. The group operation is associative and satisfies the group axioms due to the normality of N in G.

Proof. Suppose $aN = a'N$ and $bN = b'N$ for $a, a', b, b' \in G$. There exist $n, m \in N$ such that $a' = an$ and $b' = bm$. Because N is normal in G, for $n \in N$ and $b \in G$, there exists some $n' \in N$ such that $nb = bn'$. Consequently, $a'b' = anbm = abn'm$. We see that $nn'm \in N$, thus $a'b'N = abN$, which confirms the operation is well-defined. For any cosets $aN, bN \in G/N$, the product $(aN)(bN) = abN$ is a coset in G/N, satisfying the closure property. Given cosets $aN, bN, cN \in G/N$, we have $(aN)((bN)(cN)) = (aN)(bcN) = a(bc)N$ and $((aN)(bN))(cN) = (abN)(cN) = (ab)cN$, which are equal by the associativity in G. The coset eN acts as the identity in G/N since e is the identity in G, and for any coset aN, $(aN)(eN) = aeN = aN$. Each coset aN in G/N has an inverse given by $a^{-1}N$, because $(aN)(a^{-1}N) = aa^{-1}N = eN$, where eN is the identity coset. Therefore, with the operation defined and all group axioms satisfied, G/N is a group. □

Intuition 2.2. The concept of a quotient group can be intuitively understood as a means of simplifying the structure of G by 'collapsing' the elements of a normal subgroup N to a single identity element. In this construction, the elements of G that 'differ by an element of N' are considered equivalent, and this equivalence relation partitions G into disjoint subsets - the cosets of N. Specifically, elements a and b in G are considered equivalent if they belong to the same coset of N, that is, if $aN = bN$. Each coset aN is represented by an element $a \in G$, and these cosets form the elements of the quotient group G/N. These cosets become the elements of a new group under a well-defined operation inherited from G. This process essentially 'blurs out' the internal structure of N within G, *focusing instead on the way G behaves relative to the subset N*. To think about quotient groups more concretely, one might consider the analogy of time zones on Earth. If we think of each point in time on Earth as an element of a group, the act of standardising time within a time zone is akin to forming a quotient group. The exact minute differences between two cities within the same zone are 'collapsed', and they share a common representation of time. This unification abstracts away the finer details and simplifies communication and coordination. Quotient groups play a central role because they provide a structured way to understand and analyze the properties of G relative to N, facilitating the study of more complex group structures and enabling the formulation of deeper group-theoretic results, such as the isomorphism theorems. They are crucial in classifying groups, understanding homomorphisms, and more broadly, in discerning the underlying symmetries in various mathematical and real-world systems.

2.2 Classifying Finite Abelian Groups

In this section, we delve into the classification of finite Abelian groups, a cornerstone of group theory that is elegantly encapsulated by the Fundamental Theorem of Finite Abelian Groups. This theorem asserts that every finite Abelian group can be expressed as a direct product of cyclic groups of prime-power order, revealing a clear and systematic structure inherent to these groups. The classification process involves breaking down the group's order into prime factors and leveraging number theory to deduce the group's structure as a unique combination of cyclic groups.

The significance of this theorem lies in its ability to simplify the analysis of finite Abelian groups by reducing them to well-understood cyclic components. This simplification allows for a more straightforward understanding of the group's properties and behaviors, enabling comparisons between different groups and facilitating the solving of abstract algebra problems. It also confirms that identically classified groups are isomorphic, sharing the same structural properties despite potentially differing elements or operations. As we explore the classification of finite Abelian groups, we will see how the theorem categorizes these groups in a standardized manner, emphasizing the uniqueness of the decomposition. This introduction prepares us for a high-level overview of the theorem's proof, which will be presented through a sequence of lemmas, each building upon the last, and culminating in the affirmation of the decomposition's uniqueness.

Theorem 2.3 (Fundamental Theorem of Finite Abelian Groups). *Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.*

This theorem not only categorises finite Abelian groups in a standardised manner but also underscores the uniqueness of this decomposition. Specifically, it tells us that any finite Abelian group G can be represented as:

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}},$$

where $\mathbb{Z}_{p_i^{n_i}}$ denotes a cyclic group of order $p_i^{n_i}$, with each p_i a prime number, and n_i a positive integer. The primes p_i are not necessarily distinct, and the prime powers $p_i^{n_i}$ are determined uniquely by the group G. This means that if G is isomorphic to two such direct products, then both products must have the same number of terms and the same orders of cyclic groups. Moreover, this decomposition is unique up to the order of the factors. This formulation simplifies the study of finite Abelian groups by reducing complex group structures to the study of their cyclic components, which are fundamentally simpler to analyse. Before jumping straight into the proof of this theorem, we'll first take an instructive, informal approach to witness the result that it provides through an example.

Consider a finite Abelian group G of order 240, which prime factorises as $|G| = 2^4 \cdot 3 \cdot 5$. By identifying the prime components of $|G|$ and their multiplicities, we take the first step towards unravelling the structure of G. For each prime factor, we have by Sylow's First Theorem (see Gallian 2017, Theorem 24.3) and Lemma (2.1) that subgroups of such orders must exist in G. Our study is now focused on the direct product of prime-power ordered groups, which have inherent qualities that will enable us to take clear steps towards our goal to decompose G into a direct product of prime-powered cyclic groups. At this stage, we cannot guarantee cyclicity of our prime-powered groups — further inquiry is warranted for this information. Given their singular multiplicities, the Sylow p-subgroups

related to the primes 3 and 5 — which we will denote accordingly as P_3 and P_5 respectively — are straightforwardly isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_5$. Our investigation into the Sylow 2-subgroup — which we will denote as P_2 — requires some additional attention to decompose due to its order being a non-singular prime-power. We apply a partitioning method from number theory to deduce the potential structures that any prime-power ordered Abelian group may take, which in this case is applied to $|P_2| = 2^4$.

Theorem 2.4 (Partition Theorem). *Given a prime number p and an integer k, for each partition of k—that is, each way of expressing k as a sum of positive integers: $k = n_1 + n_2 + \cdots + n_r$—there exists a unique (up to isomorphism) finite Abelian group P of order p^k. This group P is isomorphic to a direct product of cyclic groups of orders $p^{n_1}, p^{n_2}, \ldots, p^{n_r}$, respectively.*

We observe that if k can be partitioned into the sum of positive integers $n_1, n_2, \ldots, n_r$, then the group P of order p^k can be represented as:

$$P \cong \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_r}},$$

where each $\mathbb{Z}_{p^{n_i}}$ is a cyclic group of order p^{n_i}. The theorem not only provides a method for constructing all possible finite Abelian groups of a given order p^k, but also ensures that each such group corresponds uniquely to a particular structural isomorphism class obtained from the partition of k. Following the example, we may decompose the group P_2 of order 2^4 into potential direct product structures for $p = 2$ and $k = 4$ as follows:

Table 1: Structural isomorphism classes for $|P_2| = p^k = 2^4$.

Partition for $k = 4$	**Isomorphism Classes for $p = 2$**
4	$\mathbb{Z}_{16}$
$3 + 1$	$\mathbb{Z}_8 \times \mathbb{Z}_2$
$2 + 2$	$\mathbb{Z}_4 \times \mathbb{Z}_4$
$2 + 1 + 1$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$1 + 1 + 1 + 1$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Integrating the potential structures for all Sylow p-subgroups, an exhaustive set of five structural isomorphism classes for G emerges:

$$G \cong \mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5, \tag{1}$$
$$G \cong \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \tag{2}$$
$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \tag{3}$$
$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \tag{4}$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5. \tag{5}$$

To confirm the viability of these structures, we ensure that the product of the orders of the involved cyclic groups equals the original order of G, which in this case is 240. To determine which isomorphism class indeed faithfully represents our particular group G, a case-by-case analysis is undertaken based on the order of known elements in G. Through a careful process of elimination, we may narrow our search down to a single isomorphism class. Through the systematic breakdown of any given

finite Abelian group's order into its prime power components and the construction of direct product decompositions, the Fundamental Theorem of Finite Abelian Groups provides a clear pathway to classifying the core structure of any given finite Abelian group.

Following our constructive example that illustrates the decomposition of a finite Abelian group into cyclic groups of prime-power order, we now transition to a formal proof of the Fundamental Theorem of Finite Abelian Groups. We unfold this proof through a sequence of lemmas, each paving the way for the next. The initial lemma establishes the groundwork by showing the feasibility of decomposing any finite Abelian group into subgroups, hinting at the theorem's broader applicability. We then identify the presence of maximal cyclic subgroups within these decompositions, revealing the essential components of an Abelian group's structure. Building on this, the proof progresses to demonstrate that a finite Abelian group of prime-power order is precisely an internal direct product of such cyclic groups, directly aligning with the theorem's claims. Cumulatively, the lemmas collectively fortify the theorem's assertion: every finite Abelian group uniquely corresponds to a direct product of cyclic groups of prime-power order.

Lemma 2.1. Let G be a finite Abelian group of order $p^r m$, where p is a prime number that does not divide m. Then G can be expressed as a direct product of two subgroups, H and K, such that $G = H \times K$. Here, H is defined as the set $\{x \in G \mid x^{p^r} = e\}$, where e is the identity element of G, and K is the set $\{x \in G \mid x^m = e\}$. Moreover, the order of H is p^r.

Proof. Let G be a finite Abelian group of order $p^r m$, where p is a prime and m is an integer such that p does not divide m. We aim to prove that G can be expressed as the direct product of two subgroups H and K where $H = \{x \in G \mid x^{p^r} = e\}$ and $K = \{x \in G \mid x^m = e\}$, and that the order of H is p^r. It is left as an exercise to establish that H and K are subgroups of G. To demonstrate that every element $x \in G$ can be written as a product of elements from H and K, we use the fact that $\gcd(m, p^r) = 1$. By the Bezout's Lemma, there exist integers s and t such that $sm + tp^r = 1$. For any element $x \in G$, we can express x as x^1, which by substitution gives x^{sm+tp^r}. Exploiting the commutativity of G, we rewrite this as $(x^m)^s \cdot (x^{p^r})^t$, which by the definitions of H and K, are elements of K and H, respectively. Thus, $x \in HK$. Next, we show that $H \cap K = \{e\}$. Let x be any element in $H \cap K$. Then $x^{p^r} = e$ and $x^m = e$. As $x^{p^r} = e$, the order of x, $|x|$, must divide p^r. Similarly, since $x^m = e$, $|x|$ must also divide m. Since p does not divide m and $|x|$ divides both p^r and m, the only possible order for x is 1, implying $x = e$. Therefore, $H \cap K$ contains only the identity element e. For the order of H, we note that the order of a subgroup must divide the order of the group. Since $|G| = p^r m$ and $|K|$ divides m, $|H|$ must be a power of p. Specifically, since p does not divide m, $|H|$ must be p^r to satisfy the equation $|G| = |H||K|$. This concludes the proof that G is indeed the direct product of the subgroups H and K, where H has order p^r, and that this direct product is unique. □

Remark 2.1. This lemma serves as the foundational step in the formal proof of the Fundamental Theorem of Finite Abelian Groups, by demonstrating the initial decomposition of a finite Abelian group into two distinct subgroups based on the group's order's prime factorization. It essentially establishes the feasibility of expressing any finite Abelian group as a product of simpler subgroups, which paves the way for further decomposition into cyclic groups. This lemma introduces the concept of direct product composition for the finite Abelian group under investigation and sets the stage for subsequent lemmas to refine this decomposition into prime-power cyclic groups, aligning directly

with the theorem's assertion.

Lemma 2.2. Let G be an Abelian group of prime-power order and let a be an element of maximum order in G. Then G can be written in the form $\langle a\rangle \times K$, where K is some subgroup of G.

Proof. Consider G to be an Abelian group such that the order of G, denoted by $|G|$, is a power of a prime, say p^n. Let a be an element in G of maximum order. We aim to show that G is isomorphic to the direct product of the cyclic subgroup generated by a and some subgroup K of G. Proceed by induction on n. For the base case where $n = 1$, G is trivially $\langle a\rangle \times \{e\}$ because G itself is a cyclic group generated by a. Now, assume for induction that every Abelian group of order p^k, with $k < n$, can be expressed in the form $\langle a\rangle \times K$. Consider G with $|G| = p^n$ and let a be of order p^m, where $m \leq n$. According to the inductive hypothesis, for every element $x \in G$, $x^{p^m} = e$ where e is the identity element in G. Suppose there exists an element $b \in G$ such that $b \notin \langle a\rangle$ and b has the smallest order among such elements. Let the order of b be p^l. Since G is Abelian, every subgroup is normal, and thus $b^{p^l} = e$ and $b^p \in \langle a\rangle$. Let $b^p = a^i$. Since a has maximum order, a^i is not a generator of $\langle a\rangle$ if i is not coprime to p^m, implying $\gcd(p^m, i) \neq 1$. By Euclid's lemma, p divides i and we can write $i = pj$. Consider the element $c = ab^{-j}$. Since G is Abelian, $c^p = a^p b^{-jp} = a^p b^{-i} = e$, showing that c is of order p, and thus $c \notin \langle a\rangle$. However, b was chosen with the smallest order p, which leads to a contradiction unless $b = c$. Therefore, $b \in \langle a\rangle$, which is also a contradiction since we chose $b \notin \langle a\rangle$. Hence, b must have order p and $\langle b\rangle \cap \langle a\rangle = \{e\}$. For the factor group $\bar{G} = G/\langle b\rangle$, we have $\bar{a}^{p^{m-1}} = \bar{e}$, and by the inductive hypothesis, $\bar{G}$ can be written in the form $\langle \bar{a}\rangle \times \bar{K}$. Let K be the pullback (pre-image) of $\bar{K}$ under the natural homomorphism from G to $\bar{G}$. Then $\langle a\rangle \cap K = \{e\}$, and G is the direct product $\langle a\rangle \times K$. □

Remark 2.2. Following the groundwork laid by the first lemma, we advance the decomposition process by identifying a cyclic subgroup of maximum order within an Abelian group of prime-power order and its complement subgroup. This lemma is pivotal in illustrating the inherent structure of prime-power ordered groups as compositions of cyclic groups, a critical component of the theorem. By demonstrating that such a group can be represented as a direct product of a maximal cyclic subgroup and another subgroup, it underscores the stepwise refinement of the group's structure into simpler, well-understood forms, thereby facilitating the theorem's ultimate goal of classifying finite Abelian groups.

Lemma 2.3. A finite Abelian group of prime-power order is an internal direct product of cyclic groups.

Proof. Let G be a finite Abelian group of prime-power order, say p^n. We will use induction on n to show that G can be expressed as an internal direct product of cyclic groups. For the base case, when $n = 1$, G is a group of prime order and hence is cyclic by definition. A cyclic group is trivially an internal direct product of itself, which is a single cyclic group. Now assume that the lemma holds for groups of order p^k where $k < n$. That is, any group H of order p^k can be expressed as an internal direct product of cyclic subgroups. Let G be of order p^n and let $a \in G$ be an element of maximal order in G. By Lemma (2.2), G can be expressed as $\langle a\rangle \times K$ for some subgroup K of G. The order of $\langle a\rangle$ is some power of p, say p^m, and by the definition of a direct product, the order of K must be p^{n-m}, which is less than p^n. By our inductive hypothesis, K can be expressed as an internal direct product of cyclic subgroups because its order is less than p^n. Let's denote this decomposition as $K = \langle b_1\rangle \times \ldots \times \langle b_k\rangle$, where each b_i is a generator of a cyclic subgroup of K. Thus, G can be

expressed as the internal direct product of cyclic groups $\langle a \rangle \times \langle b_1 \rangle \times \ldots \times \langle b_k \rangle$. Each of these cyclic groups is of prime-power order, and their direct product gives the entire group G. Hence, we have shown that G is an internal direct product of cyclic subgroups. □

Remark 2.3. Building directly on the insights from the previous lemma, we now generalise the concept to assert that any finite Abelian group of prime-power order can be fully decomposed into an internal direct product of cyclic groups. This lemma encapsulates the crux of the theorem's classification strategy, bridging the gap between the initial decomposition and the final structured form of the group. It confirms the theorem's claim by showing that the complex structure of a prime-power ordered group simplifies to a combination of cyclic groups, each a fundamental block of group theory, thus providing a systematic method for understanding and analyzing finite Abelian groups.

Lemma 2.4. Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H_i's and K_i's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

Proof. We will prove this lemma by induction on the order of the group $|G|$. For the base case, let $|G| = p$ for some prime p. Then G is cyclic and is generated by a single element because all groups of prime order are cyclic. Therefore, $m = n = 1$ and $|H_1| = |K_1| = p$, satisfying the lemma. Now, assume the lemma holds for all groups of order less than $|G|$, and consider a group G with $|G| = p^k$ for some k greater than 1. We can write G as the internal direct product of cyclic groups $H_1 \times H_2 \times \cdots \times H_m$ and $K_1 \times K_2 \times \cdots \times K_n$ as given in the lemma. Define $G^p = \{x^p | x \in G\}$, which is a subgroup of G. By the properties of the direct product and the fact that G is Abelian, we have $G^p = H_1^p \times H_2^p \times \cdots \times H_m^p$ and $G^p = K_1^p \times K_2^p \times \cdots \times K_n^p$. Let m' be the largest integer such that $|H_i| > p$, and n' be the largest integer such that $|K_j| > p$. Then we have $|G^p| < |G|$, and by the induction hypothesis, $m' = n'$ and $|H_i^p| = |K_i^p|$ for $i = 1, \ldots, m'$. Since $|H_i| = p|H_i^p|$ and $|K_i| = p|K_i^p|$ for $i = 1, \ldots, m'$, we have $|H_i| = |K_i|$ for each i. It remains to show that $m = n$. This follows from the fact that $|H_1||H_2| \cdots |H_m| = |G| = |K_1||K_2| \cdots |K_n|$ and from the established equality $|H_i| = |K_i|$ for $i = 1, \ldots, m'$, implying that the product of the orders of the remaining cyclic groups must also be equal, which means $m = n$. Thus, we have shown that if G is expressed as an internal direct product of cyclic subgroups in two different ways, the number of factors and the orders of the corresponding factors must be equal. □

Remark 2.4. The final lemma addresses the uniqueness aspect of the decomposition, a crucial component of the theorem. By proving that the decomposition of a finite Abelian group into cyclic subgroups is unique up to isomorphism, it solidifies the theorem's assertion about the standardised classification of finite Abelian groups. This lemma assures that the direct product decomposition not only exists but is also invariant under isomorphism, ensuring that the structure of finite Abelian groups can be uniquely determined, thus completing the proof's objective.

2.3 Classifying Finite Non-Abelian Groups

We will now endeavour to explore the structure of finite non-Abelian groups, which are more complex than their Abelian counterparts due to their non-commutative nature. We delve into the concept of subnormal and composition series, which allow us to systematically break down a group into simpler components. The Schreier Refinement Theorem and the Jordan-Hölder Theorem are key in

this process, providing a method to compare different breakdowns of a group and assuring that the ultimate building blocks, the simple groups, are unique to the group's structure. The Jordan-Hölder Theorem is particularly significant as it lays the groundwork for the CFSG, by establishing that the task of classifying all finite groups can be reduced to classifying all finite simple groups. This section sets the stage for understanding the finite group landscape and the order underlying its diversity.

Definition 2.3 (Subnormal Series). *Let G be a finite group. A subnormal series for G is an ascending series of subgroups $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$, where each subgroup G_i is a normal subgroup of G_{i+1} for all integers i such that $0 \leq i < n$.*

Remark 2.5. This hierarchical structure of subgroups provides a framework for analysing the internal composition of a group in terms of simpler components. Each step in the series, moving from G_i to G_{i+1}, involves a subgroup that is normal in the next group, allowing for a well-defined quotient group G_{i+1}/G_i. These quotient groups offer insights into the structure of G by revealing how each layer or level of the group's hierarchy contributes to the overall architecture of the group. Note that each element in the subnormal series need not be a normal subgroup of G itself, only in the next group along the ascending series.

Intuition 2.3. In essence, a subnormal series peels away layers of a group's structure, revealing a sequence of simpler and simpler groups until reaching the most basic unit, the trivial group. This process is akin to dissecting a complex organism to understand its composition through the various systems and sub-systems that constitute its entirety while retaining some systematic structure (such as dissecting a frog into it's various organs rather than arbitrary cubic centimetres).

Theorem 2.5 (Schreier Refinement Theorem). *Let G be a group, and consider two subnormal series of G:*

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$$

and

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

Then, for each of these series, there exist refinements, denoted by $\{G_i'\}$ for the first series and $\{H_j'\}$ for the second series, such that there is a bijection ϕ between the indices of the factors of these refined series with the property that for each index i, the quotient groups G_{i+1}'/G_i' and $H_{\phi(i)+1}'/H_{\phi(i)}'$ are isomorphic. This bijection establishes a correspondence between the factors of the refined series, demonstrating that despite the initial series potentially having different structures, their refinements can be made to exhibit a matching structure at the level of their composition factors. This theorem underscores the intrinsic property of groups that allows for the comparison of their decompositions into simpler components, irrespective of the initial choice of subnormal series.

Remark 2.6. The Schreier Refinement Theorem is a key result in group theory that highlights the intrinsic structure of groups by examining their subnormal series—sequences of subgroups where each is a normal subgroup of the next. It asserts that for any two subnormal series of a group, refinements can be made such that there exists a one-to-one correspondence between the factors of these refined series with isomorphic corresponding factors. This demonstrates that despite different initial decompositions of a group, there is a fundamental equivalence in how groups can be broken down into simpler components.

Definition 2.4 (Composition Series). *A composition series for a finite group G is defined as a special type of normal series that cannot be refined further. This means that within the sequence*

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G,$$

each subgroup G_i is a proper normal subgroup of G_{i+1}, and there are no additional subgroups that can be inserted between any two consecutive groups in the series to refine it further. In essence, a composition series reaches the most granular level of subgroup decomposition within G, where each factor group G_{i+1}/G_i is a simple group.

We may contrast the composition series with a subnormal series, which does not necessarily end with simple factor groups, nor does it have the requirement of being unrefinable. So we see that one could potentially insert additional subgroups into a subnormal series to obtain a finer decomposition of G, whereas this is not the case (by definition) of a composition series. The difference between the two series, therefore, lies in the specific criteria for the factor groups and the potential for refinement. While both offer a method to decompose a group into simpler structures, a composition series does so in the most elemental way possible, setting the stage for deeper insights into the group's architecture. The decomposition into simple groups without the possibility of further refinement provides a foundational understanding that will be crucial as we build up to more complex concepts, such as the Jordan-Hölder theorem (2.6). This theorem, which we will explore soon, delves into the unique properties and implications of composition series in the study of group theory. Understanding the distinction between subnormal and composition series is a vital stepping stone toward grasping its significance.

Algorithm for Finding the Composition Series of a Finite Group

The process of constructing composition series for a finite group G involves a systematic approach to understanding its structure through a sequence of proper normal subgroups and the simplicity of their quotient groups. Iteratively, we may construct a list of all possible composition series for any finite group by following the following general process:

Step 1: Identify Trivial or Simple Group If G is the trivial group (i.e., it has only one element), its only composition series is the singleton set containing the identity element, $\{e\}$. If G is a simple group, meaning it has no nontrivial normal subgroups, its composition series is $\{e\} \subset G$, which includes only the identity and the group itself.

Step 2: Discover Maximal Normal Subgroups If G is not simple, we need to find all maximal normal subgroups of G. A maximal normal subgroup, H, is a normal subgroup that is not contained in any larger normal subgroup except G itself.

Step 3: Recurse on Subgroups For each maximal normal subgroup H found in Step 2, we recursively apply this algorithm to find all composition series of H. This allows us to understand the internal structure of H, which is a crucial part of the overall structure of G.

Step 4: Recurse on Quotient Groups For each maximal normal subgroup H and each composition series of H found in Step 3, we consider the quotient group G/H. This group represents

the structure of G when we "factor out" the structure of H. We recursively apply this algorithm to find all composition series of G/H.

Step 5: Integrate Subgroup and Quotient Series In this step, we blend the composition series of a maximal normal subgroup, H, with that of the quotient group, G/H. For each series in H and each series in G/H, we create a new series for G. This involves mapping each quotient subgroup back to a corresponding subgroup in G that contains H as a normal subgroup. We then extend the series of H by appending these subgroups in order. The final composition series for G will thus be an ordered list of subgroups starting with the identity element and ending with G itself.

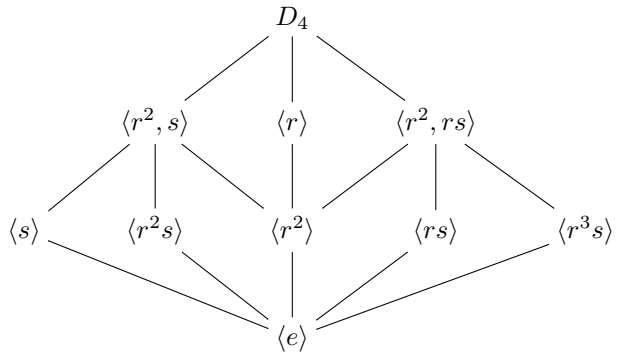
Step 6: Remove Duplicates Since the intersection of subgroups in a composition series may lead to duplicates, we remove any duplicate subgroups to ensure that each subgroup appears only once in the series. This step ensures that our composition series accurately reflects the structure of G.

Step 7: Return All Composition Series Finally, we return the set of all unique composition series constructed for G. Each of these series provides a different perspective on the structure of G, and together they give a complete picture of G's composition.

Remark 2.7. The algorithm for exhaustively listing all possible composition series of a finite group, while systematic, faces practical limitations - particularly as the order of the group increases. For groups with a large number of subgroups or complex subgroup structures, the process can become computationally intensive, as it requires identifying all maximal normal subgroups and their corresponding quotient groups. Additionally, the recursive nature of the algorithm means that the number of steps grows rapidly with the complexity of the group's structure, potentially leading to a combinatorial explosion in the number of composition series to be considered. This makes the algorithm more instructive in nature than practical for large or intricate groups without the aid of sophisticated computational tools. To illustrate the general methodology of this process we observe an application to the dihedral group of order 8, which we will denote D_4.

Example 2.1 (The Dihedral Group D_4). The dihedral group of order 8, denoted as D_4, is a nontrivial and non-simple group. It has more than one element and possesses nontrivial normal subgroups. Therefore, to construct its composition series, we need to follow a systematic process that involves identifying maximal normal subgroups, recursing on these subgroups and their corresponding quotient groups, integrating the resulting composition series, and removing duplicates. The first step in this process is to identify the maximal normal subgroups of D_4. These are subgroups that are not contained within any larger normal subgroup other than D_4 itself. A subgroup lattice diagram is helpful to organise our understanding of the subgroup structure of D_4, seen below in Figure (1).

Figure 1: Subgroup Lattice Diagram for D_4



We see that the maximal normal subgroups of D_4 include the cyclic subgroup generated by a 90-degree rotation, $\langle r\rangle$, and the Klein four-group $\langle r^2, s\rangle$ denoted V_4. We record the subgroup structure of D_4 in Table (2).

Table 2: Subgroups of the Dihedral Group D_4

Subgroup	**Elements**	**Isomorphic Structure**	**Normal**
D_4	$\{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$	-	Yes
$\langle r\rangle$	$\{e, r, r^2, r^3\}$	$\mathbb{Z}_4$	Yes
$\langle r^2\rangle$	$\{e, r^2\}$	$\mathbb{Z}_2$	Yes
$\langle s\rangle, \langle sr\rangle, \langle sr^2\rangle, \langle sr^3\rangle$	$\{e, s\}, \{e, sr\}, \{e, sr^2\}, \{e, sr^3\}$	$\mathbb{Z}_2$	No
$\langle r^2, s\rangle, \langle r^2, sr\rangle$	$\{e, r^2, s, sr^2\}, \{e, r^2, sr, sr^3\}$	$V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	Yes
$\{e\}$	$\{e\}$	$\mathbb{Z}_1$	Yes

Next, we recursively apply the same process to each of these maximal normal subgroups. Since both $\langle r\rangle$ and $\langle r^2, s\rangle$ are Abelian, their composition series are straightforward, consisting of the identity subgroup, the subgroup itself, and the intermediate subgroups along each path. Simultaneously, we consider the quotient groups formed by dividing D_4 by each of its maximal normal subgroups. These quotient groups are isomorphic to the cyclic group of order 2, $\mathbb{Z}_2$, which is simple. The composition series of these quotient groups are thus composed of the identity subgroup and the group itself. The next step is to integrate the composition series from the maximal normal subgroups with those of the quotient groups. This involves mapping each quotient subgroup back to a corresponding subgroup in D_4 that contains the maximal normal subgroup as a normal subgroup. We then extend the series of the maximal normal subgroups by appending these subgroups in order. Since the intersection of subgroups in a composition series may lead to duplicates, we remove any duplicate subgroups to ensure that each subgroup appears only once in the series. This step ensures that our composition series accurately reflects the structure of D_4. Finally, we return the set of all unique composition series constructed for D_4. Each of these series provides a different perspective on the structure of D_4, and together they give a complete picture of D_4's composition. The two unique composition series for D_4, which reflect its structure through normal subgroups with simple factors, are given by the sequences

$$\{e\} \lhd \langle r^2\rangle \lhd \langle r\rangle \lhd D_4, \tag{6}$$

and

$$\{e\} \lhd \langle r^2 \rangle \lhd \langle r^2, s \rangle \lhd D_4. \tag{7}$$

We turn to Figure (2) and (3) below for a clear visual representation of each unique composition series which can be compared to the subgroup lattice in Figure (1). Here we see each proper normal subgroup chain in isolation, along with the simple groups derived from the quotients of each successive normal subgroup.

Figure 2: Composition Series (6) for D_4.

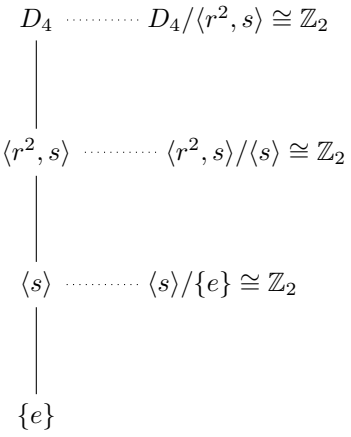
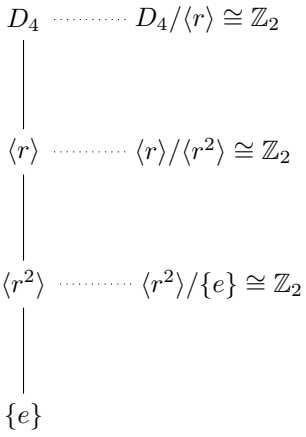


Figure 3: Composition Series (7) for D_4.



Theorem 2.6 (Jordan-Hölder Theorem). *Let G be a finite group and suppose there are two composition series of G:*

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{r-1} \lhd G_r = G,$$

and

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{s-1} \lhd H_s = G.$$

Then $r = s$, and there exists a permutation σ of the indices such that for all i, the quotient groups G_{i+1}/G_i and $H_{\sigma(i)+1}/H_{\sigma(i)}$ are isomorphic. This establishes that, up to isomorphism and the order of the factors, the composition factors of a group are uniquely determined by the group itself.

Remark 2.8. The Jordan-Hölder Theorem provides a fundamental characterization of the structure of finite groups through the lens of their composition series. It asserts that while the composition series of a group—each a chain of normal subgroups descending to the trivial subgroup—may be constructed in various ways, the simple groups that emerge as the factors of these series are invariant up to isomorphism and permutation. This theorem thus encapsulates the idea that the essential building blocks of a group's structure are uniquely determined by the group itself, independent of the particular series chosen to reveal them. The theorem's elegance lies in its assurance that the composition factors of a finite group are as fundamental and characteristic to the group as atoms (or quarks) are to a compound molecule, providing a powerful tool for understanding the deep, intrinsic properties of groups.

Intuition 2.4. Imagine you're part of a team of engineers tasked with understanding the design of a specific model of a car engine. Your goal is to break down the engine into its most fundamental

components — its "simple groups" in group theory terms. You and your team decide to disassemble the engine, piece by piece, until you reach the smallest parts that cannot be broken down further in a meaningful way, such as screws, nuts, and bolts. Now, consider that there's another team with the same model of the car engine. They also disassemble their engine but follow a different sequence, removing components in a different order than your team did. Despite these differences in approach, both teams end up with the exact same set of fundamental components. This outcome illustrates the first part of the Jordan-Hölder Theorem: regardless of how you decompose a group (or disassemble an engine), you will always end up with the same basic components, up to isomorphism and the order in which they appear.

To add another layer to this analogy, imagine that there's a rumor of a mysterious third team that claims to have disassembled the same model of the engine but ended up with a different set of fundamental components. According to the Jordan-Hölder Theorem, this is impossible if indeed they started with the same model of the engine. The theorem asserts that for a given finite group (or a specific model of an engine), the simple groups (or the fundamental components) you end up with are uniquely determined by the group itself. Therefore, if two teams start with the same engine model and fully disassemble it, they must end up with exactly the same fundamental parts. If the parts are different, then they were not working with the same model of the engine to begin with. This aspect of the Jordan-Hölder Theorem emphasises that while many different "disassembly paths" can be taken (reflecting the various subnormal series that can be constructed), no single engine model (or group) can produce a different set of fundamental components (simple groups) while still being the same engine (group). This underscores the deep, intrinsic properties of groups and their structures, revealing that the identity of a group is intimately tied to its composition factors. Note that two different engine models may have the same component parts, but no two identical models will ever differ in those parts.

3 Historical Development and Motivation

The classification of finite simple groups is a huge theorem in modern algebra, the culmination of over a century of work by dozens of mathematicians. It establishes that every finite simple group – the "building blocks" of all finite groups, analogous to prime numbers in integer factorisation – falls into one of four broad families (Gorenstein, 1985). This result was not achieved overnight; its proof, sometimes called the "Enormous Theorem", spans around 15,000 pages across hundreds of journal articles by over 100 authors (Solomon, 2001; Ronan, 2006). The effort began in the 19th century and was essentially completed by 1983, though the final components of the proof were only published in 2004. Below we recount the historical development of the CFSG, from its origins in Galois's ideas to its completion and impact on mathematics and physics.

In the nineteenth century, the groundwork for classifying simple groups was laid. Évariste Galois, in his seminal work of 1832 (published posthumously in 1846), introduced the notion of a simple group in the context of solving polynomial equations — a group with no nontrivial normal subgroups (Galois, 1846). Galois's insight showed that certain groups (now recognised as A_5, the alternating group on five letters, and $\mathbb{Z}_p$, the cyclic group of prime order) are 'simple', and play a critical role in the solvability of equations. The formal concept of an abstract group was defined shortly thereafter by Arthur Cayley (1854), and Camille Jordan's work further solidified the importance of simple groups.

In his 1870 treatise, Jordan catalogued many known finite simple groups — notably the alternating groups A_n (for $n \geq 5$) and some linear groups – and emphasised their role as the fundamental building blocks of all finite groups (Jordan, 1870). The Jordan–Hölder theorem, developed by Jordan and later refined by Otto Hölder, made this precise: any finite group can be decomposed into a series of simple factor groups, analogous to a prime factorisation (Hölder, 1892). This result turned the classification of finite simple groups into a natural goal for mathematicians. As early as 1892, Hölder explicitly posed the problem of determining all finite simple groups, and he proved that any nonabelian simple group's order must be divisible by at least four distinct primes (Hölder, 1892). By the end of the 19th century, the list of known finite simple groups included the cyclic groups of prime order, the infinite family of alternating groups A_n (simple for $n \geq 5$), and a few intriguing exceptions. Chief among these exceptions were the five sporadic simple groups discovered by Émile Mathieu in 1861–1873, the first examples of finite simple groups that do not fall into an obvious infinite family (Mathieu, 1861). These Mathieu groups — $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ — were mysterious outliers at the time, and their discovery hinted that classifying all simple groups could be a challenging task. Nonetheless, by 1900 the problem was clearly formulated: as William Burnside wrote, "the theory of groups is essentially the theory of the simple groups, and one may hope to determine them all" (Burnside, 1911).

The early twentieth century saw steady progress toward this goal, both in cataloguing examples and developing tools to constrain possible simple groups. Burnside himself made a major breakthrough in 1904 by proving what is now called Burnside's $p^a q^b$ theorem: any group whose order has only two prime factors is necessarily solvable (Burnside, 1911). In particular, this result implies there are no simple groups of order $p^a q^b$, eliminating many potential small simple groups and reinforcing the observation that simple groups tend to have 'large' orders with diverse prime factors. Around the same time, Leonard E. Dickson undertook a systematic study of linear groups over finite fields. In 1901, Dickson classified the projective linear groups $PSL(2, q)$ and other classical groups, thereby introducing an infinite family of simple groups arising from matrices over finite fields (Dickson, 1901). These were early members of what we now call the groups of Lie type, finite analogues of Lie groups classified by their algebraic structure. Dickson even identified certain exceptional examples (for instance, groups later understood as of type G_2 and E_6) in his early classifications. By 1911, Burnside conjectured that every nonabelian finite simple group must have even order (Burnside, 1911) — equivalently, that no simple group of odd order exists. This conjecture encapsulated the growing belief that the landscape of simple groups was limited and structured, perhaps even within reach of full classification.

Throughout the mid-20th century, group theorists developed powerful new methods — especially character theory and local subgroup analysis — that dramatically advanced the classification program. A pivotal idea was proposed by Richard Brauer in the 1950s: to study finite simple groups by examining the centralisers of their involutions (elements of order 2). Brauer and Fowler proved in 1955 that for any finite simple group G, if one fixes an involution $t \in G$ and considers its centraliser $C_G(t)$, there are only finitely many finite simple groups that could have that particular structure as an involution centraliser (Brauer & Fowler, 1955). This result, known as the Brauer–Fowler theorem, suggested a strategy of 'local' classification: one could potentially enumerate all simple groups by analysing the possible centraliser subgroups. Meanwhile, Claude Chevalley in 1955 had constructed new infinite families of simple groups by taking analogues of simple Lie algebras over finite fields (Chevalley, 1955). Chevalley's work, soon extended by Robert Steinberg and Ree, led

to the discovery of all the remaining families of groups of Lie type, including the so-called 'twisted' groups that had no classical analogues (Steinberg, 1959; Ree, 1961). By the early 1960s, it was known that in addition to the cyclic and alternating families, there were 16 infinite families of finite simple groups of Lie type (such as $PSL_n(q)$, $PSp_{2n}(q)$, $E_8(q)$, the Suzuki and Ree series, etc.), covering all simple groups arising from algebraic groups over finite fields (Solomon, 2001). Aside from these, the only sporadic examples known were still the five Mathieu groups. Many conjectured that no other sporadic (exceptional) simple groups existed, a belief reinforced by the absence of new sporadic discoveries for nearly a century up to 1960.

A turning point came in 1963 with the proof of the Feit–Thompson theorem. Walter Feit and John G. Thompson proved definitively that every finite group of odd order is solvable, confirming Burnside's conjecture (Feit & Thompson, 1963). This monumental result meant that any nonabelian finite simple group *must* have even order — in other words, every simple group has an involution. The Feit–Thompson theorem dramatically narrowed the classification problem to the case of groups with even order, and it ushered in a new era of intense activity focused on the local analysis of 2-subgroups (i.e. studying the structure of Sylow 2-subgroups and their centralisers). Thompson, who was awarded the Fields Medal in 1970 for his contributions, continued to be a leading figure: in a series of papers on so-called N-groups (finite simple groups whose local subgroups are all solvable), Thompson classified a broad class of simple groups and developed techniques that would be crucial for the general case (Thompson, 1971). Parallel to these theoretical advances, the late 1960s saw a startling renaissance in the discovery of sporadic simple groups. In 1965 Zvonimir Janko unexpectedly announced the existence of a new simple group J_1, the first sporadic group discovered since Mathieu's time (Janko, 1966). This breakthrough was soon followed by a flurry of additional discoveries: between 1965 and 1975, mathematicians found 20 new sporadic simple groups. Notable examples include the Janko groups J_1, J_2, J_3, J_4 (each discovered by Janko and collaborators in the late 1960s and early 1970s), the Higman–Sims group (Higman & Sims, 1968), the Suzuki sporadic group (M. Suzuki, 1969), the Hall–Janko group (isomorphic to J_2, discovered independently by Hall and Wales in 1969), the Conway groups (three groups found by John Conway in 1968 as symmetries of the Leech lattice), the Fischer groups (three groups discovered by Bernd Fischer around 1970 in his study of 3-transposition groups), the Held group (Held, 1969), the Rudvalis group (Rudvalis, 1972), and the Thompson group and Harada–Norton group (predicted by Thompson and Harada around 1973). This proliferation of sporadic examples culminated in the prediction of the largest sporadic group, the Monster ($\mathbb{M}$), in the early 1970s. The Monster was conjectured by Fischer and others to exist as a group of order approximately 8×10^{53}, a behemoth incorporating many of the smaller sporadic groups as subquotients. In 1982 Robert Griess finally constructed the Monster explicitly (Griess, 1982), an achievement often described by the whimsical title of his paper "The Friendly Giant". Soon after, the uniqueness of the Monster was confirmed, and with it, the list of sporadic simple groups closed at 26 in total. Thus, by the early 1980s, the landscape of finite simple groups seemed to consist of four types: cyclic of prime order, alternating groups, the 16 families of Lie type, and 26 sporadic groups. What remained was to show that no other simple groups exist outside these known classes — the central task of the classification theorem's proof.

Under the leadership of Daniel Gorenstein, the 1970s and early 1980s were a period of concerted collaboration devoted to completing the classification. Gorenstein was a key organiser and strategist of the effort (Solomon, 2001). In a 1972 lecture series, he outlined a detailed 16-step program for

attacking the problem, which closely guided the subsequent work (Gorenstein, 1979). The overall strategy divided the problem according to the structure of the Sylow 2-subgroup of the hypothetical simple group. Roughly, researchers split the analysis into the 'odd characteristic' or N-group case (when the group's 2-local subgroups behave in a controlled fashion, analogous to groups of Lie type in odd characteristic) and the 'even characteristic' case (when the group has a large 2-subgroup, analogous to Lie type in characteristic 2). A host of deep local analysis theorems were proved and applied: Bender's strongly embedded subgroup theorem (1970), the Alperin–Brauer–Gorenstein theorem on groups with dihedral Sylow 2-subgroups (1970), the Gorenstein–Walter theorem on groups with a dihedral Sylow 2-subgroup (1965), Glauberman's Z^*-theorem (1966) and ZJ-theorem (1968), and Thompson's classification of quadratic pairs (1971) are just a few eye-opening moments among many. Each eliminated or characterised broad classes of possible simple groups. By 1980, the portion of the classification dealing with groups of 'odd type' (noncharacteristic 2 type) was essentially complete — these are groups in which the 2-subgroup structure resembled that of groups of Lie type in odd characteristic, and this part largely reduced to the known families of Lie type and alternating groups (Gorenstein, 1983). The more difficult 'even characteristic' case, involving groups whose Sylow 2-subgroup was large or had a complicated structure, was tackled with the so-called 'signaliser functor' methods introduced by Gorenstein and others in the 1970s (Gorenstein, 1979). Michael Aschbacher arose as a leading figure in pushing the final steps of the proof in this era; for example, Aschbacher's "classical involution theorem" and "component theorem" provided an incredibly important classification of groups with certain 2-local subgroup configurations (Aschbacher, 1982). By the summer of 1983, the classification effort had reached a milestone: Gorenstein announced that the finite simple groups had been completely classified (Gorenstein, 1983). At that time, the proof was considered essentially finished, aside from writing and refining some remaining technical arguments. The announcement — while essentially correct — was slightly premature on one point: one subcase, the so-called "quasithin groups" (roughly, groups of even characteristic and small 2-rank), had been outlined by Mason but not fully written up or vetted (Solomon, 2001). This gap, however, did not affect any known groups and was expected to be fillable with effort.

After 1983, attention turned to verifying, consolidating, and publishing the enormous body of work constituting the classification proof. Gorenstein, Richard Lyons, and Ronald Solomon undertook a project to simplify and organise the proof into a coherent series of volumes (Gorenstein et al., 1994). Meanwhile, the outstanding quasithin case was resolved by Aschbacher and Stephen Smith: they carried out a thorough analysis of quasithin simple groups, publishing their results in 2004 in a two-volume monograph of over 1200 pages (Aschbacher & Smith, 2004). With the appearance of Aschbacher–Smith (2004), the last gap in the original proof was closed, and the classification theorem was fully published and verified. Thus, 2004 is often cited as the year the classification of finite simple groups was formally completed in print (Solomon, 2005). So by the early 1980s the theorem was proven in principle (enabling widespread use of the result), and by 2004 every portion of the proof had passed through peer-reviewed publication. The final statement of the classification is a testament to how far group theory had progressed since the 19th century. Every finite simple group is isomorphic to one of four types: (1) a cyclic group of prime order, (2) an alternating group A_n for $n \geq 5$, (3) a group of Lie type (including the sixteen infinite families of matrix groups over finite fields first systematically described by Chevalley, Steinberg, and others), or (4) one of the 26 sporadic simple groups (Solomon, 2001). No other finite simple groups exist beyond these. This result answers completely the question posed by Hölder in 1892 and is arguably one of the most

significant achievements in algebra.

The impact of the CFSG on mathematics and related fields has been substantial. Knowing the complete list of finite simple groups has allowed mathematicians to resolve many problems that required a case-by-case analysis of simple subgroups. For example, certain deep results in algebraic number theory and combinatorics now assume the classification as a known input. One especially celebrated outgrowth of the CFSG is the phenomenon of 'Monstrous Moonshine'. In the late 1970s, John Conway and Simon Norton observed a mysterious connection between the Monster sporadic group and the theory of modular functions in number theory (Conway & Norton, 1979). They conjectured that the Fourier coefficients of the classical j-invariant (a function in complex analysis important to number theory) are unexpectedly related to dimensions of Monster group representations. This Monstrous Moonshine conjecture, linking a finite simple group to elliptic modular forms, was proven in 1992 by Richard Borcherds, who constructed a vertex operator algebra (a concept from theoretical physics, specifically conformal field theory) on which the Monster acts (Borcherds, 1992). Borcherds's work not only solved a purely mathematical problem — earning him the Fields Medal in 1998 — but also bridged finite group theory with string theory and other aspects of physics. The Monster group's role in Monstrous Moonshine has led to new insights at the intersection of group theory, number theory, and theoretical physics, illustrating the unforeseen consequences of the CFSG. In combinatorics and coding theory, the classification has illuminated many exceptional structures. Several sporadic groups are symmetry groups of remarkable combinatorial objects: for example, the Mathieu group M_{24} is the automorphism group of a Steiner system (a type of block design) and is deeply connected with the binary Golay error-correcting code — an important object in coding theory. The Leech lattice in 24 dimensions, important in sphere packing problems, has a symmetry group that gives rise to Conway's sporadic groups. The CFSG guarantees that such sporadic examples are limited to the 26 known ones, so researchers can thoroughly study each without fear of missing hidden symmetries of a new simple group. Moreover, the classification theorem is now an indispensable tool in many areas of finite mathematics; for example, results in group theory that classify certain graphical or combinatorial configurations often cite the CFSG to rule out exotic configurations that would require an unknown simple group. In ongoing research, simplified and shorter proofs of the CFSG are being pursued to make this deep result more accessible. While the original proof's length and complexity are daunting, the clarity brought by the classification itself is increedible.

In sum, the Classification of Finite Simple Groups stands as a mammoth achievement of 20th-century mathematics. From Galois's 19th-century revelations to the collaborative marathon of the late 20th century, mathematicians gradually uncovered the complete catalogue of finite simple groups. The final theorem, officially published in 2004, tells us that the building blocks of all finite groups come in just four flavours: cyclic, alternating, Lie type, or sporadic. This discovery not only resolved a long-standing puzzle in algebra but also created rich interdisciplinary connections — from the theory of numbers and combinatorial designs to the physics of string theory via Monstrous Moonshine. The journey to classification was long and technically arduous, but the result provides a unifying structure for finite symmetry and a foundation for further exploration in mathematics. The CFSG truly exemplifies how a profound problem can drive the development of vast new theory, ultimately leading to a comprehensive answer that resonates across many fields of inquiry.

4 The Classification Theorem

The CFSG organises all finite simple groups into four main categories: Cyclic Groups of Prime Order, Alternating Groups of degree 5 or greater, Simple Groups of Lie Type, and Sporadic Groups.

We begin our investigation with the most straightforward class of finite simple groups - those cyclic groups of prime order. These groups are defined by their prime number order, making them inherently simple. We will cover the mathematical proofs that confirm their simplicity and their isomorphism to the additive group of integers modulo a prime number. We then move to alternating groups of degree greater than 5, discussing their discovery, proofs of simplicity, and their crucial role in Galois Theory — especially in relation to the unsolvability of certain polynomial equations. Next, we explore simple groups of Lie Type, which are finite analogs of continuous Lie groups defined over finite fields. We will look into their development, the mathematicians who contributed to their discovery, and their importance in connecting discrete and continuous mathematics along with an example from the Projective Special Linear group. Lastly, we briefly introduce Sporadic Groups, setting the stage for a more detailed examination for the interested reader.

Theorem 4.1 (Classification of Finite Simple Groups). *The Classification of Finite Simple Groups states that every finite simple group belongs to one of the following categories:*

(i) Cyclic Groups of Prime Order

(ii) Alternating Groups of degree greater than 5

(iii) Simple Groups of Lie Type

(iv) Sporadic Groups

The Classification Theorem asserts that these families exhaust all possible finite simple groups. Moreover, each group within these families is simple and non-isomorphic to any other group in the list, except for a few duplicates at low orders which are accounted for in the classification. The proof of the Classification of Finite Simple Groups was completed over several decades, with contributions from many mathematicians. It is one of the longest and most complex proofs in the history of mathematics, and it has been divided into a series of separate theorems and papers. The classification is not merely a list but a structural theorem that states that every finite simple group must be isomorphic to one of the groups in these families.

4.1 Cyclic Groups of Prime Order

Proposition 4.1 (Simplicity of Cyclic Groups of Prime Order). Any group G of prime order p is simple.

Proof. Let G be a group such that $|G| = p$, where p is a prime number. Consider any non-trivial subgroup $H \subseteq G$. By Lagrange's Theorem (2.1), the order of any subgroup H must divide the order of G. Since $|G| = p$ and p is prime, the only divisors of p are 1 and p itself. If H is non-trivial (i.e., $H \neq \{e\}$, where e is the identity element), then $|H|$ cannot be 1 and must therefore be p. This means that H must have the same order as G and hence $H = G$. If H were trivial, then $H = \{e\}$, which is a subgroup of every group by definition and is normal since the left and right cosets of $\{e\}$ are identical to G itself. Consequently, the only subgroups of G are G itself and the trivial subgroup

$\{e\}$. Both of these subgroups are normal in G by definition because the group is Abelian (all cyclic groups are Abelian), and therefore all of its subgroups are normal. Thus, G has no non-trivial proper normal subgroups, which by definition means G is simple. □

Corollary 4.1 (Uniqueness of Prime Ordered Groups). All groups of prime order p are isomorphic to the cyclic group $\mathbb{Z}_p$, which consists of the integers modulo p under addition.

The isomorphism $\phi : G \to \mathbb{Z}_p$ can be established by mapping the generator g of G to 1 in $\mathbb{Z}_p$ and extending this map to all elements in G by exploiting the structure of G as a cyclic group generated by g. Formally, if $G = \langle g \rangle$ and $|G| = p$, then for each $k \in \{0, 1, \ldots, p-1\}$, there exists a unique $a_k \in \mathbb{Z}_p$ such that:

$$\phi(g^k) = a_k,$$

where a_k is the equivalence class of k in $\mathbb{Z}_p$. Since p is prime, the integers $\{0, 1, \ldots, p-1\}$ form a complete set of residues modulo p, and the mapping is a bijection. Furthermore, for all $g^k, g^l \in G$, the homomorphism property $\phi(g^k g^l) = \phi(g^k) + \phi(g^l)$ holds in $\mathbb{Z}_p$, which is consistent with the definition of group isomorphism.

In the Classification of Finite Simple Groups, cyclic groups of prime order stand as the prototypical simple groups, their simplicity deriving from the prime nature of their order. These groups, inherently simple due to the indivisibility of their prime order, have no non-trivial, proper normal subgroups. They are characterised by a direct isomorphism to the additive group of integers modulo a prime number, embodying a fundamental link between group theory and number theory. This categorization highlights the elegance of prime order cyclic groups as essential and elementary units within the broader structure of finite group theory.

4.2 Alternating Groups A_n with $n \geq 5$

The alternating groups were the first non-Abelian simple groups to be identified. The alternating group A_n was proven to be simple for $n \geq 5$ by Évariste Galois in the 19th century. Galois' argument is based on the observation that any nontrivial normal subgroup of A_n must contain a 3-cycle. Since 3-cycles generate A_n for $n \geq 3$ and all 3-cycles are conjugate in S_n, it follows that the only normal subgroups of A_n for $n \geq 5$ are the trivial subgroup and A_n itself, thereby establishing its simplicity. This discovery was a significant contribution to the foundation of group theory and influenced subsequent developments in the CFSG. In Galois Theory, the simplicity of A_n for $n \geq 5$ plays a crucial role in explaining why general polynomial equations of degree five or higher cannot be solved by radicals.

Lemma 4.1. For $n \geq 3$, A_n is generated by 3-cycles.

Proof. To prove that 3-cycles generate A_n, it suffices to demonstrate that any pair of transpositions can be expressed as the product of 3-cycles. Given that a transposition (a, b) is equivalent to (b, a), we need to consider that every pair of transpositions must be equivalent to one of the following products:

(i) $(a, b)(a, b)$ which is equal to the identity element in the group,

(ii) $(a, b)(c, d)$ which can be rewritten as $(a, c, b)(a, c, d)$, a product of two 3-cycles,

(iii) $(a, b)(a, c)$ which simplifies to (a, c, b), a single 3-cycle.

It follows that any even permutation group can be decomposed into 3-cycles, hence 3-cycles generate A_n. □

Lemma 4.2. Let N be a normal subgroup of A_n, where $n \geq 3$. If N contains a 3-cycle, then $N = A_n$.

Proof. First, we establish that A_n is generated by 3-cycles of the form (i, j, k), where i and j are fixed in $\{1, 2, \ldots, n\}$ and k varies. This is due to the fact that any 3-cycle can be expressed as a product of 3-cycles of this specified form, as illustrated by the following identities:

$$\begin{aligned}(i, a, j)\& &= (i, j, a)^2,\\ (i, a, b)\& &= (i, j, b)(i, j, a)^2,\\ (j, a, b)\& &= (i, j, b)^2(i, j, a),\\ (a, b, c)\& &= (i, j, a)^2(i, j, c)(i, j, b)^2(i, j, a).\end{aligned}$$

Now, assume N is a nontrivial normal subgroup of A_n for $n \geq 3$ such that N includes a 3-cycle of the form (i, j, a). The normality of N implies that for any (i, j, k) in A_n, the conjugate of (i, j, k) by (i, j, a) must also lie in N, which is shown by the following:

$$[(i, j)(a, k)](i, j, a)^2[(i, j)(a, k)]^{-1} = (i, j, k).$$

Since N contains all 3-cycles of the form (i, j, k) for $1 \leq k \leq n$, and by Lemma (4.1) these 3-cycles generate A_n, it follows that N must be equal to A_n, hence $N = A_n$. □

Proposition 4.2. The alternating group A_n is simple for $n = 5$.

Proof. By Lemma (4.1), we know that for $n \geq 3$, A_n is generated by 3-cycles. Therefore, A_5 is also generated by 3-cycles. Now, let N be a nontrivial normal subgroup of A_5. If N contains a 3-cycle, then by Lemma (4.2), N must be the entire group A_5, since A_5 is generated by 3-cycles and N is normal. On the other hand, if N does not contain a 3-cycle, then N must be contained in the kernel of the homomorphism from A_5 to $\mathbb{Z}_2$ that maps each 3-cycle to 1, as all elements of A_5 are either the identity, a product of two 3-cycles, or a single 3-cycle. Since A_5 is generated by 3-cycles, the kernel of this homomorphism would have to be $\{e\}$, the trivial subgroup. Since A_5 is generated by 3-cycles and every nontrivial normal subgroup must contain a 3-cycle or be the trivial subgroup, and we have shown that containing a 3-cycle implies that the subgroup is the entire group A_5, it follows that A_5 has no nontrivial normal subgroups other than itself. Therefore, A_5 is simple. □

Proposition 4.3. The alternating group A_n is simple for $n \geq 5$.

Proof. Assume for the sake of contradiction that A_n is not simple for some $n \geq 5$. This would mean there exists a nontrivial normal subgroup N of A_n other than $\{e\}$ and A_n itself. By Lemma (4.1), we have established that A_n is generated by 3-cycles for $n \geq 3$. Thus, any element of A_n can be expressed as a product of 3-cycles. Now, if N is nontrivial and normal in A_n, then N must contain a 3-cycle, since the product of any non-identity element in N with itself enough times will eventually yield a 3-cycle (due to the fact that the order of any element divides the order of the group, and

the order of a 3-cycle is 3, which is prime). In particular, if N contains any element that is not the identity, the product of this element with conjugates of itself will result in 3-cycles being formed within N, by the properties of conjugation in a normal subgroup and the structure of A_n. By Lemma (4.2), if N contains a 3-cycle and N is normal in A_n, then N must be equal to A_n. This contradicts our assumption that N is a nontrivial normal subgroup other than A_n itself. Hence, our initial assumption must be wrong. Therefore, there are no nontrivial normal subgroups of A_n other than A_n itself for $n \geq 5$. Hence A_n is simple for $n \geq 5$. □

4.3 Simple Groups of Lie Type

Simple Groups of Lie Type are finite groups that serve as discrete analogs to the continuous Lie groups, which are structured as manifolds over real or complex numbers. Unlike Lie groups that are inherently continuous, Groups of Lie Type are defined over finite fields $\mathbb{F}_q$, where $q = p^n$ for a prime number p and a positive integer n, thus embodying the properties of linear algebraic groups within a finite setting. This discrete nature renders them invaluable across various mathematical disciplines, including number theory and combinatorics, where their finite structure allows for thorough analysis. The construction of Groups of Lie Type was pioneered by Claude Chevalley in the 1950s, who developed a method to construct finite analogues of the simple complex Lie groups, thereby laying the groundwork for a vast new domain of mathematical exploration. Chevalley's construction was later expanded by Steinberg, Tits, and others through generalizations that included twisted forms, significantly broadening the scope and diversity of these groups. As a result, the family of Groups of Lie Type encompasses Chevalley groups, Steinberg groups, and various twisted groups, each defined by specific algebraic and geometric properties.

Lie Groups and Lie Algebras

Lie Groups epitomize the concept of continuous symmetry, integral to various fields of mathematics and physics. Each Lie group is associated with a Lie algebra, a vector space equipped with a binary operation known as the Lie bracket, which captures the group's infinitesimal symmetries. This intricate relationship between Lie groups and their algebras underscores the profound connection between continuous symmetries and their algebraic structures.

Groups of Lie Type

Groups of Lie Type are realized as subgroups of matrix groups over finite fields, inheriting the structural characteristics of algebraic groups in a discrete setting. This discrete nature allows for comprehensive analysis within combinatorics, number theory, and other areas of discrete mathematics. The construction of these groups facilitated the definition of finite groups exhibiting the properties of continuous algebraic groups, significantly contributing to the understanding and classification of finite groups.

The study of Simple Groups of Lie Type not only enriches our comprehension of the structure and classification of finite groups but also enhances the connection between discrete and continuous mathematical theories. Through the lens of these groups, the CFSG reveals the vast diversity and richness within the universe of finite simple groups, underscoring the intricate tapestry of symmetries that govern the mathematical world.

Families of Lie Type Groups

Chevalley Groups Chevalley groups are finite groups constructed from complex simple Lie algebras. A complex simple Lie algebra is defined as a non-abelian algebra that is maximally non-commutative and contains no non-trivial ideal. These algebras are associated with root systems, collections of vectors in a Euclidean space that satisfy specific symmetry conditions reflecting the algebra's structure. The construction of Chevalley groups involves defining a group structure over a finite field $\mathbb{F}_q$ using a complex simple Lie algebra and its root system. The rank of the Lie algebra, indicative of the dimension of its maximal toral subalgebra, directly correlates with the classification into types A_n, B_n, C_n, and D_n, while types E_6, E_7, E_8, F_4, and G_2 represent exceptional cases with unique root systems.

Example 4.1 (Projective Special Linear Group: PSL$(2, \mathbb{F}_7)$). Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^k$ for some prime number p and a positive integer k. Consider the set of all $n \times n$ matrices over $\mathbb{F}_q$ with determinant equal to 1, which forms the Special Linear Group $\mathrm{SL}(n, \mathbb{F}_q)$. The Projective Special Linear Group $\mathrm{PSL}(n, \mathbb{F}_q)$ is then defined as the quotient of $\mathrm{SL}(n, \mathbb{F}_q)$ by its centre. Formally, the centre of $\mathrm{SL}(n, \mathbb{F}_q)$, denoted $Z(\mathrm{SL}(n, \mathbb{F}_q))$, is the subgroup consisting of all scalar matrices λI_n, where I_n is the $n \times n$ identity matrix and λ is an element of $\mathbb{F}_q$ such that $\lambda^n = 1$. The group $\mathrm{PSL}(n, \mathbb{F}_q)$ is then the quotient group:

$$\mathrm{PSL}(n, \mathbb{F}_q) = \mathrm{SL}(n, \mathbb{F}_q)/Z(\mathrm{SL}(n, \mathbb{F}_q)).$$

The Projective Special Linear group $\mathrm{PSL}(2, \mathbb{F}_7)$, emerges from the quotient of the Special Linear Group $\mathrm{SL}(2, \mathbb{F}_7)$ over its centre $Z(\mathrm{SL}(2, \mathbb{F}_7))$. This construction encapsulates a transition from the general linear transformations preserving volume and orientation in a two-dimensional vector space over the finite field $\mathbb{F}_7$, to a projective representation that abstracts away scalar multiples, focusing solely on the inherent geometry of the transformations. The Special Linear Group $\mathrm{SL}(2, \mathbb{F}_7)$ is the set of all 2×2 matrices with entries from the finite field $\mathbb{F}_7$ that have a determinant of 1. Formally, it is defined as:

$$\mathrm{SL}(2, \mathbb{F}_7) = \{A \in \mathrm{M}_2(\mathbb{F}_7) \mid \det(A) = 1\},$$

where $\mathrm{M}_2(\mathbb{F}_7)$ represents the space of all 2×2 matrices over $\mathbb{F}_7$. The centre of $\mathrm{SL}(2, \mathbb{F}_7)$, denoted by $Z(\mathrm{SL}(2, \mathbb{F}_7))$, includes all scalar matrices in $\mathrm{SL}(2, \mathbb{F}_7)$ that commute with every element within the group. It is precisely described as:

$$Z(\mathrm{SL}(2, \mathbb{F}_7)) = \left\{\lambda I_2 \mid \lambda \in \mathbb{F}_7^{\times}, \lambda^2 = 1\right\}.$$

Given this, $\mathrm{PSL}(2, \mathbb{F}_7)$ is the quotient group:

$$\mathrm{PSL}(2, \mathbb{F}_7) = \mathrm{SL}(2, \mathbb{F}_7)/Z(\mathrm{SL}(2, \mathbb{F}_7)).$$

The order of $\mathrm{PSL}(2, \mathbb{F}_7)$ is deduced from the cardinality of $\mathrm{SL}(2, \mathbb{F}_7)$, which is computed as $(7^2 - 1)(7^2 - 7)/2$ owing to the formula for $\mathrm{GL}(2, \mathbb{F}_q)$ adjusted for the determinant restriction, and subsequently halved to account for the quotient by its centre, resulting in 168 distinct elements. This group's simplicity is a hallmark of its structure; $\mathrm{PSL}(2, \mathbb{F}_7)$ admits no nontrivial normal subgroups, embodying the definition of a simple group. The action of $\mathrm{PSL}(2, \mathbb{F}_7)$ can be interpreted on the projective line over $\mathbb{F}_7$, effectively modeling transformations that preserve projective properties. Each matrix in $\mathrm{SL}(2, \mathbb{F}_7)$, upon projection into $\mathrm{PSL}(2, \mathbb{F}_7)$, corresponds to an equivalence class of linear transformations devoid of scale, emphasizing the intrinsic geometric relations. The group $\mathrm{PSL}(2, \mathbb{F}_7)$

serves as an instructive exploration into the symmetry and structure inherent in two-dimensional projective spaces over finite fields.

Steinberg (Twisted) Groups These groups are derived from Chevalley groups through the application of automorphisms either to the Dynkin diagram (graphical representation) of the Lie algebra or to the finite field over which the group is defined. These automorphisms, which can be viewed as symmetries of the Dynkin diagram, modify the root system and result in a new group structure, termed a twisted group. Notations such as ${}^2A_n$,${}^2D_n$,${}^3D_4$, and ${}^2E_6$ denote the specific automorphism applied, with the superscript indicating the order of the field automorphism involved.

Suzuki Groups The Suzuki groups, denoted by ${}^2B_2$, emerge from a construction distinct from the standard Chevalley framework and are defined exclusively over fields of characteristic 2. These groups are associated with type B_2 Lie algebras but exhibit unique properties and structures necessitating specialized analytical approaches. The characteristic of the field fundamentally impacts the group's algebraic structure, introducing distinctive elements into the group theory landscape.

Ree Groups Named after Rimhak Ree, Ree groups are defined over fields with specific characteristics, similar to Suzuki groups, but arise from constructions unique to types ${}^2F_4$ and ${}^2G_2$. These types are related to exceptional Lie algebras, and the groups are constructed using field automorphisms, emphasizing the influence of the field's characteristic on the group's structure. Ree groups highlight the diversity of symmetries in finite settings, diverging from the classical Chevalley constructions.

Unitary Groups Unitary groups, often denoted as ${}^2A_n$, are defined in relation to symmetries that preserve a Hermitian form over a finite field. This form, analogous to a symmetric bilinear form but for complex vectors, incorporates conjugation to capture complex structures. Unitary groups represent the finite analogs of continuous unitary symmetries, extending the concept of unitary operations to finite fields through specific field automorphisms.

Orthogonal Groups Orthogonal groups are defined as those preserving a quadratic form over a finite field, analogous to preserving distances and angles in Euclidean spaces. Classified into types B_n, C_n, D_n, and ${}^2D_n$, these groups act on spaces of varying dimensions and preserve different forms of quadratic equations, illustrating the range of symmetries related to orthogonal transformations in a finite context.

Symplectic Groups Symplectic groups preserve a non-degenerate, skew-symmetric bilinear form known as a symplectic form. These forms enable the definition of volume and orientation in vector spaces over finite fields, devoid of traditional Euclidean angles. Denoted by C_n, symplectic groups underscore the geometric and algebraic significance of preserving specific forms in the realm of finite fields, playing a crucial role in the study of phase spaces and classical mechanics.

Exceptional Groups of Lie Type Exceptional groups of Lie type correspond to the finite groups arising from the exceptional Lie algebras E_6, E_7, E_8, F_4, and G_2. These groups, defined over finite fields, possess unique and complex structures mirroring their Lie algebra counterparts, demonstrating the breadth of finite simple groups and their pivotal roles in advancing mathematical understanding across various domains.

The families of Lie type groups embody a vast and intricate array of algebraic structures that reflect the symmetries of diverse geometrical and algebraic systems in a finite setting. The exploration of these groups is indispensable for a comprehensive grasp of the algebraic, geometric, and theoretical underpinnings of symmetry and structure.

4.4 Sporadic Groups

Sporadic groups are a distinctive collection of finite simple groups that do not belong to the infinite families typically classified in group theory (Conway, Curtis, Norton, Parker, & Wilson, 1985). These groups are characterized by their rarity and the unconventional structures they present within the realm of mathematical symmetry. Unlike other finite simple groups that are categorized into well-defined families, sporadic groups are unique in that they do not emerge from the standard constructions used to generate other group families (Gorenstein, Lyons, & Solomon, 1994). The discovery of sporadic groups has been a product of individual mathematical research, often occurring serendipitously rather than through a deliberate theoretical approach. The first of these groups was discovered by Émile Mathieu in the mid-19th century, and the identification of sporadic groups continued until 1980, culminating in a total of twenty-six known sporadic groups (Atlas of Finite Group Representations, n.d.). These groups exhibit a broad spectrum of sizes and complexities, ranging from the smaller Mathieu groups to the vast Monster group, each with its own order and intricate symmetries (Wilson, 2009).

The Mathieu groups, which were the first to be discovered among the sporadic groups, consist of five groups denoted as M11, M12, M22, M23, and M24. The numbers in their names indicate the degree of the permutation representation with which they were originally associated. These groups have been particularly noted for their applications in the theory of error-correcting codes and combinatorial designs (Thompson, 1983). Sporadic groups enrich our understanding of mathematical symmetry by showcasing the diversity and complexity of group structures. Their study has been instrumental in advancing the field of group theory and has provided a deeper insight into the unexpected and multifaceted nature of mathematical structures.

Example 4.2 (The Monster Group). The Monster Group, denoted as M, stands as a monumental figure in the classification of finite simple groups, particularly among the 26 sporadic groups. Its discovery marks a significant milestone in the landscape of group theory, celebrated for its unparalleled size and intricate structure. The journey to the Monster Group's confirmation began in the early 1970s, sparked by Bernd Fischer and Robert Griess's prediction of its existence. This prediction was rooted in the exploration and classification of other sporadic groups, hinting at the presence of a group of extraordinary magnitude and complexity.

Robert Griess played a pivotal role in substantiating the existence of M through his construction of the Griess algebra, a 196,883-dimensional commutative, nonassociative algebra. This algebra serves as a foundation upon which the Monster Group exhibits its symmetries, acting as its automorphism group. Griess's announcement of this groundbreaking discovery in 1980, followed by his detailed exposition in 1982, not only confirmed the existence of M but also showcased its unique position as a central object in group theory. The name "Friendly Giant" was initially proposed by Griess for this behemoth of mathematical symmetry, though it has since been affectionately known as the Monster Group.

The construction of the Griess algebra and the subsequent revelation of the Monster Group's symmetries underscore the group's significance. It embodies the culmination of efforts to understand the sporadic groups, those that do not fit neatly into the established infinite families of group theory. The Monster Group's discovery and the innovative methods developed to study it have enriched mathematical discourse, offering new perspectives on symmetry, algebra, and the very fabric of mathematical structure.

Structure and Subgroups The subgroup composition of M is remarkable for its depth and complexity. Among its numerous subgroups, M contains several other sporadic groups, establishing a hierarchical network within the realm of finite groups. Notably, it includes multiple copies of the Conway groups and the Baby Monster group, the latter being the second-largest sporadic group. This inclusion forms a lineage or 'family tree' of sporadic groups with M at its pinnacle, indicating a profound interconnectedness and underlying symmetry among these exceptional groups. The order of M is exactly

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47,$$

amounting to approximately 8×10^{53} elements.

The representation theory of the Monster Group is particularly rich and complex. The smallest non-trivial irreducible representation of M has a dimension of $196,883$, which interestingly matches the dimension of the Griess algebra. This algebra is significant as it provides a natural action for M, revealing the group's symmetries. The dimensions of the irreducible representations of M are not just large numbers; they have profound implications, especially when linked to the coefficients of the modular j-function, a connection that is at the heart of the Monstrous Moonshine conjecture.

The Monstrous Moonshine conjecture, initially suggested by John McKay and later proven by Richard Borcherds, uncovers a deep and surprising relationship between the Fourier coefficients of the modular j-function and the dimensions of the irreducible representations of M. This unexpected link has far-reaching consequences, providing valuable insights across various mathematical fields, including number theory, algebra, and mathematical physics. It particularly resonates within the contexts of modular functions, string theory, and conformal field theory, where the implications of this connection continue to be explored.

Beyond the realm of pure algebra, the symmetry properties of the Monster Group have significant interdisciplinary connections, particularly in theoretical physics. The group's algebraic structure is related to elliptic curves and modular forms, thereby connecting abstract algebra with geometric and number-theoretic concepts. These relationships are not merely academic; they have practical implications in the mathematics underpinning string theory and conformal field theory, suggesting that the Monster Group may play a role in the fundamental understanding of the universe. The Monstrous Moonshine and its implications thus exemplify the profound interconnectedness of different areas within mathematics and its application to other scientific disciplines. The study of the Monster Group M presents formidable challenges due to its unparalleled size and the complexity of its structure. Yet, these challenges underscore the group's significance in mathematical research. Exploring M's structure, representations, and automorphisms continues to be a source of potential breakthroughs, not only within group theory but also in number theory, geometry, quantum physics, and beyond,

marking it as a cornerstone of mathematical symmetry and an emblem of the interconnectivity within mathematics.

Singularity of Sporadic Groups

Sporadic groups represent a unique and enigmatic subset within the classification of finite simple groups. Unlike their counterparts that fit neatly into the established infinite families of group theory, sporadic groups are characterised by their exceptional nature and the distinct properties they exhibit. These properties are not shared by the more systematic families of finite simple groups. The study of sporadic groups often requires specialized methods and insights due to their individual peculiarities, making them a fascinating subject within the field of group theory. The discovery and subsequent analysis of sporadic groups have been pivotal in advancing our understanding of group structures and symmetry. These groups serve as critical test cases for theorems postulated to be universally applicable to all finite simple groups. Moreover, they provide concrete examples of group structures that defy conventional classification, thereby deepening our comprehension of symmetry in mathematical contexts.

Sporadic groups have significantly contributed to the depth and breadth of group theory. Often described as the exceptions that test the rule, their intricate structures have led to novel discoveries and insights across mathematics. The study of these groups is not only central to the understanding of group theory but also demonstrates the diversity and richness of mathematical structures. Each sporadic group is distinguished by its distinctiveness, which adds to the diversity of the field and presents mathematicians with challenging and intriguing problems. The connections that sporadic groups have with other areas of mathematics and physics are particularly noteworthy. For instance, the Monster Group has been linked to string theory and other areas of theoretical physics. Sporadic groups stand out as outliers in the classification of finite simple groups due to their unique and individual properties. Their study is indispensable for a comprehensive understanding of group theory, providing a window into the variety and complexity of structures that exist out in the mathematical wilds.

References

[1] Aschbacher, M. (2004). The status of the classification of the finite simple groups. *Notices of the AMS*, **51**(7), 736–740.

[2] Aschbacher, M., and Smith, S. D. (2004). *The Classification of Quasithin Groups I, II*. Mathematical Surveys and Monographs, Vols. 111–112. Providence, RI: American Mathematical Society.

[3] Borcherds, R. E. (1992). Monstrous moonshine and monstrous Lie superalgebras. *Inventiones Mathematicae*, **109**(2), 405–444.

[4] Brauer, R. (1955). On the structure of groups of finite order. *Proceedings of the International Congress of Mathematicians, Amsterdam*, 209–217.

[5] Brauer, R., and Fowler, K. A. (1955). On groups of even order. *Annals of Mathematics*, **62**(3), 565–583.

[6] Burnside, W. (1911). *Theory of Groups of Finite Order* (2nd ed.). Cambridge University Press.

[7] Cayley, A. (1854). On the theory of groups, as depending on the symbolic equation $\theta^n = 1$. *Philosophical Magazine*, **7**(42), 40–47.

[8] Chevalley, C. (1955). Sur certains groupes simples. *Tôhoku Mathematical Journal*, **7**(3), 14–66.

[9] Conway, J. H., and Norton, S. P. (1979). Monstrous moonshine. *Bulletin of the London Mathematical Society*, **11**(3), 308–339.

[10] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., and Wilson, R. A. (1985). *Atlas of Finite Groups*. Oxford University Press.

[11] Dickson, L. E. (1901). *Linear groups: With an exposition of the Galois field theory*. Leipzig: B. G. Teubner.

[12] Feit, W., and Thompson, J. G. (1963). Solvability of groups of odd order. *Pacific Journal of Mathematics*, **13**(3), 775–1029.

[13] Galois, É. (1832). Mémoire sur les conditions de résolubilité des équations par radicaux. *Journal de Mathématiques Pures et Appliquées*, **11**, 417–444.

[14] Gallian, J. A. (2017). *Contemporary Abstract Algebra* (9th ed.). Cengage Learning.

[15] Gorenstein, D. (1983). *The Classification of Finite Simple Groups*. Plenum Press.

[16] Gorenstein, D. (1985). The enormous theorem (Classification of finite simple groups). *Scientific American*, **253**(6), 104–115.

[17] Gorenstein, D., Lyons, R., and Solomon, R. (1994). *The Classification of the Finite Simple Groups*. American Mathematical Society.

[18] Griess, R. L. (1982). The friendly giant. *Inventiones Mathematicae*, **69**(1), 1–102.

[19] Hölder, O. (1892). Die einfachen Gruppen im ersten Hundert der Ordnungszahlen. *Mathematische Annalen*, **40**(1), 55–88.

[20] Janko, Z. (1966). A new finite simple group with abelian Sylow 2-subgroups. *Journal of Algebra*, **3**(2), 147–186.

[21] Jordan, C. (1870). *Traité des substitutions et des équations algébriques*. Paris: Gauthier-Villars.

[22] Mathieu, É. (1861). Mémoire sur l'étude des fonctions de plusieurs quantités, et en particulier des substitutions, des combinaisons et des permutations d'un nombre quelconque de lettres. *Journal de Mathématiques Pures et Appliquées*, **6**, 241–323.

[23] Ree, R. (1961). A family of simple groups associated with the Lie algebra of type G_2. *American Journal of Mathematics*, **83**(3), 432–462.

[24] Ronan, M. (2006). *Symmetry and the Monster: One of the Greatest Quests of Mathematics*. Oxford: Oxford University Press.

[25] Solomon, R. (2001). A brief history of the classification of finite simple groups. *Bulletin of the American Mathematical Society*, **38**(3), 315–352.

[26] Steinberg, R. (1959). Variations on a theme of Chevalley. *Pacific Journal of Mathematics*, **9**(3), 875–891.

[27] Thompson, J. G. (1959). Finite groups with fixed-point-free automorphisms of prime order. *Proceedings of the National Academy of Sciences*, **45**(4), 578–581.

[28] Thompson, J. G. (1983). Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$. *Journal of Algebra*, **89**(2), 437–499.

[29] Wilson, R. A. (2009). *The Finite Simple Groups*. Springer-Verlag London.

[30] Atlas of Finite Group Representations. Retrieved January 10, 2024, from `http://brauer.maths.qmul.ac.uk/Atlas/v3/`