# CLASSIFICATION OF FINITE SIMPLE GROUPS

ABHINAV SHRESTHA

Abstract. Analogous to the way the integers can be decomposed uniquely into prime factors, finite groups can be decomposed into finite simple groups, which cannot be further decomposed nontrivially. We will prove the Jordan-Hölder Theorem and show that finite groups can always be decomposed uniquely into finite simple groups, and discuss the classification of these groups. In particular, we will discuss two infinite families of simple groups, the cyclic groups of prime order, and the alternating groups on $n \geq 5$ elements.

## Contents

## 1. Background Theorems and Definitions

We assume the reader has some basic knowledge of group theory. We begin by defining two main concepts related to the classification of simple groups.

**Definition 1.1.** A subgroup $H$ of $G$ is called a *normal subgroup* if for every $g \in G$, $gHg^{-1} = H$. That is, $H$ is closed under conjugation by elements of $G$. If $H$ is normal in $G$, we write $H \trianglelefteq G$.

**Definition 1.2.** A group $G \neq \{\text{id}\}$ is a *simple group* if its only normal subgroups are the trivial subgroup and $G$.

We will also state the following theorems from group theory, which will be of some use to us in future proofs. First, we have two of the isomorphism theorems.

**Theorem 1.3.** *(First Isomorphism Theorem) Suppose $\alpha : G \to H$ is a surjective group homomorphism. Let $K = \ker \alpha \trianglelefteq G$. Then we have the natural surjective homomorphism $\pi : G \to G/K$. There is a unique isomorphism $\hat{\alpha} : G/K \to H$ such that $\alpha = \hat{\alpha} \circ \pi$.*

**Theorem 1.4.** *(Second Isomorphism Theorem) Suppose that $N$ is normal in a group $G$, and $H$ is a subgroup of $G$. Then $HN$ is a subgroup of $G$, and $H \cap N$ is normal in $HN$. In addition, if $\alpha$ is the composition of the inclusion map $H \mapsto G$*

*Date*: DEADLINE AUGUST 31,2010.

*and $\pi : G \to G/N$, the natural projection, then* $\ker \alpha = H \cap N$*, and the image of* $\alpha$ *is* $HN/N$*. Furthermore,* $(H \cap N)h \to Nh$ *is an isomorphism,* $H/H \cap N \to HN/N$*.*

A consequence of the isomorphism theorems is the following lemma.

**Lemma 1.5.** *(Zassenhaus Butterfly Lemma) Suppose $G$ is a group with subgroups $A$, $B$, $C$ and $D$, such that $A \trianglelefteq B$ and $C \trianglelefteq D$. Then,*

$$\frac{A(D \cap B)}{A(C \cap B)} \cong \frac{C(B \cap D)}{C(A \cap D)}.$$

The remaining theorems are well-known results in group theory.

**Theorem 1.6.** *(Lagrange's Theorem) Suppose $G$ is a finite group and $H$ is a subgroup of $G$. Then $|G|= |G : H|\cdot|H|$.*

**Lemma 1.7.** *(Cauchy's Theorem) Suppose $G$ is a finite group, and $p$ is a prime number that divides $|G|$. Then there is an element of $G$ of order $p$.*

**Theorem 1.8.** *(Poincaré's Theorem) Suppose $G$ is a group and $H$ is a subgroup of $G$ of index $n$ (finite). Let $K = \bigcap_{g\in G} gHg^{-1}$, so $K$ is a subgroup of $H$. It follows $m = |G : K|$ is finite, $K \trianglelefteq G$, and $n|m|n!$.*

**Theorem 1.9.** *If $H$ and $K$ are finite subgroups of $G$, then*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

We will employ the following notation for some common group theory terms here.

**Notation 1.10.** The normalizer of a subgroup $H$ of $G$ is denoted $N_G(H)$.

The center of a group $G$ is denoted $Z(G)$.

## 2. Composition Series

**Definition 2.1.** Suppose $G$ is a group with subgroups

$\{\text{id}\}= G_0 \leq G_1 \leq \ldots \leq G_n = G$.

We say such a list of subgroups is a *subnormal series* if $G_{i-1} \trianglelefteq G_i$, for all $1 \leq i \leq n$.

**Example 2.2.** Consider the group $\mathbb{Z}/250\mathbb{Z}$. The following are subnormal series of the group:

(1) $\{\text{id}\}\leq \mathbb{Z}/5\mathbb{Z} \leq \mathbb{Z}/25\mathbb{Z} \leq \mathbb{Z}/125\mathbb{Z} \leq \mathbb{Z}/250\mathbb{Z}$.

(2) $\{\text{id}\}\leq \mathbb{Z}/2\mathbb{Z} \leq \mathbb{Z}/50\mathbb{Z} \leq \mathbb{Z}/250\mathbb{Z}$.

**Definition 2.3.** Suppose that

$\{\text{id}\}= G_0 \leq G_1 \leq \ldots \leq G_n = G$

is a subnormal series for $G$. A *refinement* of this series is any subnormal series which can be obtained by inserting a finite number of subgroups into the series.

The trivial refinement is obtained by inserting groups already in the subnormal series. Nontrivial refinements are obviously much more interesting and are found by inserting proper normal subgroups into the series; that is, one must find a subgroup $N$ such that $G_{i-1} \triangleleft N \triangleleft G_i$, and $G_{i-1} \neq N \neq G$. Specifically, if

$\{\text{id}\}= G_0 \leq G_1 \leq \ldots \leq G_{i-1} \leq G_i \leq \ldots \leq G_n = G$

is a subnormal series of $G$, and $N$ satisfies the conditions discussed above, then

$\{\text{id}\}= G_0 \leq G_1 \leq \ldots \leq G_{i-1} \leq N \leq G_i \leq \ldots \leq G_n = G$

would be a nontrivial refinement.

**Example 2.4.** $\{\text{id}\} \leq \mathbb{Z}/2\mathbb{Z} \leq \mathbb{Z}/10\mathbb{Z} \leq \mathbb{Z}/50\mathbb{Z} \leq \mathbb{Z}/250\mathbb{Z}$ is a refinement of (2).

**Definition 2.5.** Suppose $G$ is a group with two subnormal series
$\{\text{id}\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$,
$\{\text{id}\} = H_0 \leq H_1 \leq \ldots \leq H_m = G$.
We say these series are *equivalent* if $n = m$, and there is a bijection $\sigma : \{1 \ldots n\} \to \{1 \ldots n\}$ such that $G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i-1)}$ for every $i$ in the range $1 \leq i \leq n$.

**Theorem 2.6.** *(Jordan-Hölder Theorem) Suppose that $G$ is a group, with two subnormal series,*
$\{\text{id}\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$,
$\{\text{id}\} = H_0 \leq H_1 \leq \ldots \leq H_m = G$.
*It follows that these series have equivalent refinements.*

*Proof.* We refine the series of $G_i$'s by inserting groups between $G_{i-1}$ and $G_i$ as follows:
$G_{i-1} = G_{i-1}(H_0 \cap G_i) \trianglelefteq G_{i-1}(H_1 \cap G_i) \trianglelefteq \ldots \trianglelefteq G_{i-1}(H_m \cap G_i) = G_i$.
Now we apply the same method, but switch the two series, and insert groups between $H_j$ and $H_{j-1}$:
$H_{j-1} = H_{j-1}(G_0 \cap H_j) \trianglelefteq H_{j-1}(G_1 \cap H_j) \trianglelefteq \ldots \trianglelefteq H_{j-1}(G_n \cap H_j) = H_j$.
We will use the notation $G_{i,j} = G_{i-1}(H_j \cap G_i)$ and analogously for $H_{i,j}$. It follows from the Zassenhaus Butterfly Lemma that $G_{i,j}/G_{i,j-1} \cong H_{j,i}/H_{j,i-1}$, for all $i, j$, $1 \leq i \leq n$, $1 \leq j \leq m$, and we are done. □

A subnormal series allows for only trivial refinements if and only if the quotient group $G_i/G_{i-1}$ is a simple group for all $1 \leq i \leq n$. Any group can be decomposed into a subnormal series that only permits trivial refinements. We call this series the *composition series*. The quotient groups of this series are called the *composition quotients*, or *composition factors*.

The Jordan-Hölder Theorem implies that this decomposition is unique, up to equivalence. If two such composition series exist for a group, then they must have equivalent refinements. However, since composition series have no nontrivial refinements, the series must be equivalent. Let's verify this for a non-abelian group.

**Example 2.7.** Consider the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j2 = k2 = -1$, and $ij = k$, $ji = -k$. The center $Z(Q) = \{\pm 1\}$. Let $R_x = \{\pm 1, \pm x\}$, for $x = i, j, k$. The subnormal series of $Q$ are
$\{1\} \leq Z(Q) \leq R_i \leq Q$,
$\{1\} \leq Z(Q) \leq R_j \leq Q$,
$\{1\} \leq Z(Q) \leq R_k \leq Q$.
These subnormal series do not permit any further nontrivial refinements, so they must be equivalent. This is rather trivial to verify, since $R_i \cong R_j \cong R_k$, and so $R_i/Z(Q) \cong R_j/Z(Q) \cong R_k/Z(Q)$, and $Q/R_i \cong Q/R_j \cong Q/R_k$.

The composition series of a simple group, $G$, consists only of the trivial group and $G$ itself, and the composition quiotients are either trivial or isomorphic to $G$. Thus, simple groups can be thought of as analogous to the prime numbers, in that every group can be decomposed into simple groups, which cannot be further decomposed. In fact, the Fundamental Theorem of Arithmetic can easily be derived by applying the Jordan-Hölder Theorem to $\mathbb{Z}/n\mathbb{Z}$ and identifying subnormal series with factorizations.

## 3. The Cyclic Groups of Prime Order

**Theorem 3.1.** *Suppose $G$ is a group of prime order. Then $G$ is a simple group.*

*Proof.* Suppose $H$ is a subgroup of $G$. Then $|H|$ must divide $|G|$. But $|G|$ is prime. Therefore, $H$ must be the trivial group or $G$. Thus, $G$ cannot have any nontrivial proper normal subgroups. □

This gives us our first family of simple groups, the groups of prime order. All groups of this family are abelian and cyclic. These properties stem from the following fact.

**Proposition 3.2.** *Suppose $G$ is a group of prime order $p$. Then $G$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

*Proof.* Let $g \in G$ such that $g \neq e$. The element $g$ generates a subgroup $H$. However, $|H|$ must divide $|G|$, but since $|G|$ is prime, and $g \neq e$ by assumption, $|H| = |G|$. Therefore, $g$ generates $G$.

We define the isomorphism $\phi : G \to \mathbb{Z}/p\mathbb{Z}$ such that if $e$ is the identity element in $G$, then $\phi(e) = 0 \in \mathbb{Z}/p\mathbb{Z}$, and let $\phi(g^n) = n \mod p$ for all $n \in \mathbb{Z}$. This is obviously well-defined, since $g^n = g^m$ if and only if $n \equiv m \mod p$. Furthermore, $\phi(g^{n+m}) = n + m \mod p$ and $\phi(g^n) + \phi(g^m) = n + m \mod p$. Since this is well-defined, $\phi$ is a homomorphism. In addition, $\phi$ must be injective, since $\phi(g^n) = \phi(g^m)$ if and only if $n = m \mod p$. Since $|G| = |\mathbb{Z}/p\mathbb{Z}|$, $\phi$ must also be surjective, and thus an isomorphism. □

For this reason, this family of simple groups is classified as the cyclic groups of prime order.

## 4. Alternating Groups

**Definition 4.1.** A *permutation* is a bijection from a set to itself. A *transposition* is a permutation that exchanges 2 elements in the set, and fixes all others. A permutation is *even* if it can be written as a product of an even number of transpositions.

**Definition 4.2.** The *symmetric group* on $n$ elements $S_n$ is the set of all permutations on a set of $n$ elements. The *alternating group* on $n$ elements $A_n$ is the set of all even permutations.

*Remark* 4.3. Since the sum of 2 odd or 2 even numbers is even, conjugation does not change the parity of the permutation. Thus, the alternating group $A_n$ is normal in $S_n$.

The alternating group on 3 elements $A_3$ is a member of the family of cyclic groups of prime order, since $|A_3| = |S_3|/2 = 3!/2 = 3$. Thus, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. However, $|A_4| = 12$, so is not a group of prime order. In fact, it is not even simple. Before we prove this, we will prove a simple lemma.

**Lemma 4.4.** *If $H$ is a subgroup of $G$, then its conjugates have the same order.*

*Proof.* Consider $\phi_g : H \to G$, $\phi_g(h) = ghg^{-1}$ for all $h \in H$, and $g \in G$. It is easy to see that $\phi_g$ is a homomorphism, since for any $h_1, h_2 \in H$, $\phi_g(h_1)\phi_g(h_2) = (gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} = \phi_g(h_1h_2)$. Furthermore, $\phi_g^{-1} = \phi_{g^{-1}}$. In particular, $\phi_g^{-1}$ exists for all $g \in G$. Thus, if $\phi_g(h_1) = \phi_g(h_2)$, then $\phi_g^{-1}(\phi_g(h_1)) =$

$\phi_g^{-1}(\phi_g(h_2))$, so $h_1 = h_2$. Therefore, $\phi_g$ is injective and $H$ is isomorphic to its image under $\phi$, which is the set of all conjugates of $h \in H$ by $g$. Thus, $|H| = |gHg^{-1}|$. □

**Corollary 4.5.** *If $H$ is the only subgroup of $G$ of a given order, then $H$ is normal.*

**Proposition 4.6.** *$A_4$ contains a normal subgroup, $V = \{\mathrm{id}$, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)$\}$.*

*Proof.* The group $V$ contains the identity, and it is easy to verify that it is closed under multiplication, since the prodcut of any two non-identity elements is the third. To show that $V$ is a subgroup, we need to show that $V$ contains the inverses of all its elements. However, any transposition is its own inverse, and two disjoint transpositions commute. If we consider the non-identity elements of $V$, we can see that each is a composition of two disjoint transpositions $g$ and $h$. Thus, $ghgh = gghh = \mathrm{id}$, and we can conclude that every element of $V$ is its own inverse.

Now we will show that $V$ is the unique subgroup of order 4. If we prove this, we can apply Corollary 4.5, and $V$ must be normal. Suppose $H$ is a subgroup of order 4, $H \neq V$. There is some $g \in H$ such that $g \notin V$. The element $g$ must be a 3-cycle, because $V$ contains all other even permutations (transpositions and 4-cycles are odd). But any 3-cycle generates a subgroup, $H_g$ of order 3. But 3 does not divide 4, so this would violate Lagrange's theorem. Thus, $V$ is the unique subgroup of order 4, and we are done. □

Next, we should consider $A_5$, the alternating group on 5 elements. The group $A_5$ has order 60, so it is not part of the family of cyclic groups of prime order. It is, however, simple. To prove this, we require some machinery to examine its subgroups.

**Definition 4.7.** A group $G$ is called a *$p$-group* if the order of each element $G$ is a power of $p$.

**Definition 4.8.** Suppose $G$ is a finite group of order $p^a n$ where $p$ does not divide $n$. Any subgroup of $G$ of order $p^a$ is called a *Sylow $p$-subgroup*. The set of all such subgroups is denoted $Syl_p(G)$.

Cauchy's Theorem (Theorem 1.7) gives us a sense of what is to come. Cauchy's Theorem proves the existence of $p$-groups, but not necessarily Sylow $p$-groups. If we knew Sylow $p$-subgroups always existed, we would know a lot about what subgroups a group contains, solely by its order. Luckily, this is the case.

We will now state and prove the Sylow theorems. Let $G$ be a finite group of order $p^a n$ where the prime $p$ does not divide n.

**Theorem 4.9.** *(Existence) There is a Sylow $p$-subgroup $P$ of $G$.*

*Proof.* We proceed by inducting on $|G|$. The trivial group obviously has a $p$-subgroup. Now we only need to consider the case where $|G| = n > 1$. By the class equation,

$$|G| = |Z(G)| + \sum_{j=1}^{s} |G : \mathrm{Stab}_G(x_j)|,$$

where $x_j$ are representatives for non-singleton conjugacy classes of G, and $s$ is the number of representatives.

First, we will consider the case where $p \mid |G : \mathrm{Stab}_G(x_j)|$ for every $j$. If this holds, then $p \mid |Z(G)| \neq 1$. By Cauchy's Theorem, there is an element $z \in Z(G)$ of order $p$. Thus $H = \langle z \rangle$ is a subgroup of $G$. Because $z$ is in the center, it commutes with all elements of $G$, so $H$ is normal. We apply the inductive hypothesis to $G/H$, which has order $p^{a-1}n$. Thus, there is a Sylow $p$-subgroup $P'$ of $G/H$ of order $p^{a-1}$. Now consider the preimage $P$ of $P'$ under the natural projection from $G$ to $G/H$. Then, $P$ is a subgroup of $G$, and $P/H$ has order $p^{a-1}$. Thus, $|P| = p^a$, and $P$ is a Sylow $p$-subgroup of $G$.

If there is an $x_j$ such that $p$ does not divide $|G : \mathrm{Stab}_G(x_j)|$, then $|\mathrm{Stab}_G(x_j)| = p^a m$, for some $m < n$, such that $m$ and $p$ are coprime. By the inductive hypothesis, $\mathrm{Stab}_G(x_j)$ has a subgroup $P$ of order $p^a$, and $P$ is a Sylow $p$-subgroup of $G$. □

Before we prove the next Sylow theorem, we require a small lemma, which is a natural result of the theory of $p$-groups.

**Lemma 4.10.** *If $P$ is a Sylow $p$-subgroup of a group $G$, and $Q$ is a $p$-subgroup of $G$ which normalizes $P$, then $Q$ is a subgroup of $P$.*

*Proof.* Obviously, $P$ is normal in its normalizer $N_G(P)$. Since $Q$ normalizes $P$, $Q$ is also a subgroup of $N_G(P)$. Now, $|PQ| = |P| \cdot |Q|/|P \cap Q|$ is a power of $p$ by Theorem 1.9. However, since $P$ is a Sylow $p$-subgroup, it is a $p$-subgroup of $G$ of greatest order. Since $|PQ| \geq |P|$, $PQ = P$, and $Q$ is a subgroup of $P$. □

**Theorem 4.11.** *(Dominance) If $Q$ is $p$-subgroup of $G$, then there is some $T \in Syl_p(G)$ such that $Q$ is a subgroup of $T$.*

*Proof.* Suppose $Q$ is a $p$-subgroup of $G$. Using the Sylow Existence Theorem, we know $G$ has a Sylow $p$-subgroup, $P$. Let $\Omega = \{gPg^{-1} : g \in G\}$, the set of conjugates of $P$ in $G$. The groups $G$ and $Q$ act on $\Omega$ by conjugation. Because $N_G(P)$ is the stabilizer of P in G with respect to conjugation, by the orbit-stabilizer theorem, we know that $|\Omega| = |G : N_G(P)|$. Now, denote the $Q$-orbits of $\Omega$ as $\Omega_i$. Then $|\Omega| = \sum_i |\Omega_i|$. If we choose $P_i \in \Omega_i$, then $|\Omega_i| = |Q : N_Q(P_i)|$. Here, we define $N_Q(P_i) = N_G(P_i) \cap Q$. Since $|Q|$ is a power of $p$, $p$ necessarily divides $|\Omega_i|$ for all $i$, if and only if $|\Omega_i| \neq 1$. If $|\Omega| = 1$, then $|Q : N_Q(P_i)| = 1$, and $Q$ normalizes $P_i$. However, the order of $\Omega$ does not depend on our choice of $Q$, so we can choose the case where $Q = P$, and find restrictions on the value of $|\Omega|$. We know that $P$ is in some $\Omega_i$. If $P \in \Omega_i$, then $|\Omega_i| = 1$, because $P$ obviously normalizes itself, and $|\Omega_i| = |P : N_P(P)| = 1$. This is the only $\Omega_i$ with order 1. Suppose, for contradiction, that there were some other $\Omega_i$ such that $|\Omega_i| = 1$. Then for any $P_i \in \Omega_i$, $|P : N_P(P_i)| = 1$. However, this implies $P = N_P(P_i)$, and by Lemma 4.10, $P$ is a subgroup of $P_i$. Since they are conjugate, they must be of equal order, so $P = P_i$. Thus, if $P \notin \Omega_i$, then $|\Omega_i|$ is divisible by $p$, since $|\Omega_i| \neq 1$ and must divide $|P|$. Therefore, $|\Omega| \equiv 1 \mod p$.

Returning to the general case where $Q$ is arbitrary. Since $|\Omega| \equiv 1 \mod p$, it is clear that there is some $\Omega_i$ whose order does not divide $p$. Thus, $Q$ normalizes $P_i$. We can now apply Lemma 4.10, and $Q$ is a subgroup of $P_i$. Recall that $P_i$ is a conjugate of $P$, a Sylow $p$-subgroup. Since a subgroup and its conjugate have the same order, $P_i$ is also a Sylow $p$-subgroup. □

**Theorem 4.12.** *(Conjugacy) The Sylow $p$-subgroups are conjugate in $G$.*

*Proof.* Let $P$ be a Sylow $p$-subgroup. Define $\Omega = \{gPg^{-1} : g \in G\}$, as above, so that $|\Omega| \equiv 1 \mod p$. Suppose, for contradiction, that $\Omega \neq Syl_p(G)$, so that there is some Sylow $p$-subgroup $T$ that is not conjugate to $P$. $T$ acts on $\Omega$ by conjugation.

Let $P' = gPg^{-1}$ for some $g \in G$. $T$ does not normalize $P'$, because if it did, it would be contained in $P'$, by Lemma 4.10, and therefore be equal, and thus conjugate, to $P'$. Therefore, all $T$-orbits must have size divisible by $p$, by the orbit-stabilizer theorem. However, $\Omega$ is the disjoint union of sets of size divisible by $p$, so $|\Omega| \equiv 0 \mod p$, which we have already shown to be false. Therefore, $\Omega = Syl_p(G)$, and all Sylow $p$-subgroups are conjugate. □

**Theorem 4.13.** *(Congruence) The order of $Syl_p(G)$ divides $n$ and is congruent to 1 modulo $p$.*

*Proof.* The previous proof shows that $|\Omega| = |Syl_p(G)| \equiv 1 \mod p$. As for the first part, we begin by letting $G$ act on $Syl_p(G)$ by conjugation. There is only one orbit. The stabilizer of $P \in Syl_p(G)$ is the normalizer, $N_G(P)$, so $|Syl_p(G)| = |G : N_G(P)|$. Since $P$ is a subgroup of its normalizer, $p^\alpha \mid |N_G(P)|$, and so $|G : N_G(P)|$ must divide $n$. □

Recall that $A_4$ has a normal subgroup $V$. It is easy to see that $V$ is a Sylow 2-subgroup of $A_4$. In accordance with the Sylow Congruence Theorem, we also confirmed that $A_4$ contains exactly one such subgroup. Furthermore, if we had proven that $V$ was normal in $A_4$ without proving it was the only subgroup of its order (such as by brute force), we could have used the Sylow Conjugacy Theorem to show that it was the unique Sylow 2-subgroup. Thus, even in the relatively simple example of $A_4$, the Sylow Theorems provide many ways to determine whether a group has a normal subgroup. Another useful technique involves the following proposition.

**Proposition 4.14.** *If $G$ is a group, and $H$ is a subgroup of index 2 in $G$, then $H$ is normal in $G$.*

*Proof.* Let $g \in G$. If $g \in H$, then $gH = H = Hg$. Otherwise, $gH \neq H$ and $Hg \neq H$. Because $|G : H|= 2$, there is only one other coset. Thus, $gH = G \backslash H = Hg$. □

*Remark* 4.15. By the lemma and the Sylow Theorems, it is clear that a group of order $2p^\alpha$ cannot be simple, for $\alpha > 1$ and $p \neq 2$. (Proposition 4.15 below also proves this for $p = 2$.)

Now that we have the Sylow Theorems at our disposal, we are almost ready to tackle the alternating groups. Our first task will be to prove that $A_5$ is the smallest finite non-abelian simple group. We will start with two more propositions.

**Proposition 4.16.** *Suppose $G$ is of order $p^n$ for $n > 1$, or $pq$ for distinct primes $p$ and $q$. Then $G$ cannot be an non-abelian simple group.*

*Proof.* If $G$ is of order $p^n$, for prime $p$, $G$ cannot be a non-abelian simple group, because then $G$ is a nontrivial $p$-group, and, by the conjugacy class equation, $|G| = |Z(G)| + \sum_{j=1}^{s} |G : C_G(x_j)|$, where the $x_j$ are representatives for nonsingleton conjugacy classes. Then $p$ divides the $|G : C_G(x_j)|$ by the orbit-stabilizer theorem, and so $p$ must also divide $|Z(G)|$. The identity is in $Z(G)$, so the order cannot be 0, and $G$ must have a nontrivial center. Since $Z(G) \trianglelefteq G$, if $G$ is simple, then $G = Z(G)$ and it is abelian. If $G$ has order $pq$ for distinct primes $p$ and $q$, then we assume $p > q$ without loss of generality, and by the Sylow Existence and Congruence Theorems, $G$ has a unique subgroup of order $p$, which is normal by its uniqueness. □

**Proposition 4.17.** *Suppose that the finite group $G$ has order $pr$, where $p$ is a prime number and $r < p$. Then $G$ is not a non-abelian finite simple group.*

*Proof.* The Sylow Congruence Theorem implies $|Syl_p(G)|= 1$. Now suppose $G$ is simple. Then, $Syl_p(G) = \{G\}$ and r = 1, because the Sylow subgroup is normal by Corollary 4.5. Thus $G$ is of prime order and is abelian. □

**Proposition 4.18.** *There is no non-abelian finite simple group of order less than 60.*

*Proof.* Suppose $G$ is a group of order less than 60. By the 2 previous propositions, we know that the only candidates for non-abelian finite simple groups are those of orders 12, 18, 24, 30, 36, 40, 45, 48, 50, 54, and 56. We can eliminate groups of order 18, 50, and 54 as well, because they contain a Sylow subgroup of index 2, which are normal by Proposition 4.14.

For the next few groups we will use Corollary 4.5 with Poincaré's Theorem. In groups of order 12, 24, and 48, a Sylow 2-subgroup has index 3. Consider $P$, a Sylow 2-subgroup of $G$. Let $K = \bigcap_{g\in G} gPg^{-1}$. By Poincaré's Theorem, $K$ is normal in $G$. We need to show that it is not the trivial group or all of $G$. However, $K$ is a subgroup of $P$, which is a proper subgroup of $G$, so $K \neq G$. Furthermore, if $K$ were trivial, $|G : K| = |G|$. But Poincaré's Theorem says $|G : K|$ divides $|G : P|! = 3!$. But clearly, 12, 24, and 48 do not divide 3!, so $K$ is not trivial. Thus, groups of order 12, 24, and 48 have nontrivial normal subgroups, and are not simple. Using analogous argument, we can show that groups of order 36 and 45 are not simple. A group of order 36 has a Sylow 3-subgroup of index 4, but 36 does not divide $4! = 24$. A group of order 45 has a Sylow 3-subgroup of index 5, but 45 does not divide $5! = 120$.

The remaining candidates for nonabelian simple groups are those of orders 30, 40, and 56. Suppose for contradiction that a group of order 30 were simple. Then, it would contain 6 Sylow 5-subgroups. Thus, it must have 24 elements of order 5. In addition, it must contain 10 Sylow 3-subgroups, meaning it contains 20 elements of order 3. But $20 + 24 > 30$, so a group of order 30 is not simple. A group of order 40 must have exactly 1 Sylow 5-subgroup, so it cannot be simple. Finally, suppose a group of order 56 were simple. Then it must contain 8 Sylow 7-subgroups, and so 48 elements of order 7. There are 8 elements remaining in the group. Since the group has a Sylow 2-subgroup, the elements of this group must be the 8 elements not of order 7. Thus, there is a unique group of order 8, which must be normal. Therefore, we have a contradiction, and a group of order 56 is not simple. □

To proceed, we require some machinery from theory of group actions. The theorems are well-known, and the proofs are not particular to the study of simple groups, so we will not prove them here.

**Definition 4.19.** Suppose that a group $G$ acts on a set $\Omega$. We say that $G$ acts transitively on $\Omega$ if the action of $G$ has a single orbit. Equivalently, if $\omega_1, \omega_2 \in \Omega$, then there exists $g \in G$ such that $g\omega_1 = \omega_2$.

**Definition 4.20.** We say that a group $G$ acts $m$-transitively on a set $\Omega$ if for any two ordered $m$-tuples $(a_1, a_2, \dots a_m)$ and $(b_1, b_2, \dots b_m)$, where $a_i, b_i \in \Omega$, for $1 \leq i \leq m$, and $a_i \neq a_j$ and $b_i \neq b_j$, for all $1 \leq i, j \leq m$, then there is $g \in G$ such that $ga_i = b_i$ for $1 \leq i \leq m$.

**Definition 4.21.** Suppose that $G$ acts on a set $\Omega$ and that $B \subsetneq \Omega$. $B$ is a *block* of the action of $G$ on $\Omega$ if whenever $g \in G$, either $gB = B$ or $gB \cap B = \emptyset$. A block is *trivial* if it is empty, a singleton, or $\Omega$, and *non-trivial* otherwise.

**Definition 4.22.** Suppose a group $G$ acts on a set $\Omega$. The action is said to be *primitive* if there are no non-trivial blocks.

**Proposition 4.23.** *If a group $G$ acts 2-transitively on $\Omega$, then the action is primitive.*

*Proof.* The action of $G$ on $\Omega$ cannot have a nontrivial block, since for any potential nontrivial block $B$, we can use the 2-transitivity of the action to fix one element of $B$ and move the other element to an element outside of $B$. □

**Definition 4.24.** A proper subgroup $M$ of $G$ is *maximal* if for every subgroup $H$ of $G$, whenever $M$ is a subgroup of $H$, $M = H$.

**Proposition 4.25.** *Suppose that $G$ acts transitively on $\Omega$, where $|\Omega| \geq 2$. The action is primitive if and only if for every $\omega \in \Omega$, the stabilizer of $\omega$ in $G$ is a maximal subgroup of $G$.*

*Remark* 4.26. If a group acts 2-transitively on a set, the stabilizers of the elements of that set are maximal.

**Lemma 4.27.** *Suppose $\sigma$ and $\tau$ are permutations of $A_n$ of the same cycle shape. Then, there is some permutation $\omega$ such that $\omega\sigma\omega^{-1} = \tau$.*

*Proof.* All permutations can be written as a composition of disjoint cycles, ignoring the fixed elements. Since disjoint cycles commute, we can then order them by ascending length. We do not care about the order of cycles of the same length, but let us order them ascending by their smallest element. We can now list the elements of the set in the order they appear in the cycles, giving us two lists, $s_1, s_2, \dots s_n$ and $t_1, t_2, \dots t_n$, such that the $s_i$ are distinct and the $t_i$ are distinct for all $1 \leq i \leq n$. Since $S_n$ acts $n$-transitively on a set of $n$ elements, there is $\omega' \in S_n$, such that $\omega'(t_i) = s_i$ for all $1 \leq i \leq n$. We claim that $\omega'$ is the $\omega$ we are searching for. This is equivalent to proving that they are equivalent as functions, which can be tested by applying it to an arbitrary element. Since $\sigma$ and $\tau$ have the same cycle structure, if $\sigma$ takes $s_i$ to $s_j$, then $\tau$ takes $t_i$ to $t_j$. Thus, if we apply $\omega'^{-1}\sigma\omega'$ to $t_i$, we see that $t_i \mapsto s_i \mapsto s_j \mapsto t_j$. □

**Proposition 4.28.** *The alternating group $A_5$ is a simple group of order 60.*

*Proof.* The alternating group $A_5$ has order 60. By Lagrange's Theorem, any subgroup of $A_5$ must have order 1, 2, 3, 4, 5, 6, 12, 20, 30, or 60. First, let us consider the subgroups containing 5-cycles. If a normal subgroup contains one 5-cycle, it must contain all 24 5-cycles, because it contains the powers and conjugates of that cycle. Therefore, the only candidate for a proper normal subgroup containing a 5-cycle would be a subgroup of order 30. By Cauchy's Theorem, to contain 30 elements, the subgroup must contain at least one cycle of order 3, which are the 3-cycles. However, by normality, it must contain all 20 3-cycles. Thus, a subgroup containing 30 elements is not normal. Moreover, this rules out all subgroups of orders divisible 3 or 5.

The remaining candidates are subgroups of order 2 and 4. Assume $N$ is normal of order 2 or 4. The subgroup $N$ is contained in a Sylow 2-subgroup by the Sylow

Dominance Theorem. However, the Sylow 2-subgroups of $A_5$ are the conjugates of $V = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$. The reader should recall that this subgroup was normal in $A_4$. In $A_5$, however, $V \subseteq \text{Stab}_{A_5}(5)$, and for any $g \in A_5$, $gVg^{-1} \subseteq \text{Stab}_{A_n}(g5)$, since conjugation is an automorphism. It is easy to see that the intersection of the conjugates of $V$ is contained in $\bigcap_{g \in G} \text{Stab}(g5) = \{\text{id}\}$. Since $N$ is normal, $N \subseteq \bigcap_{g \in A_5} gVg^{-1} \subseteq \{\text{id}\}$. So $N = \{\text{id}\}$, and we have a contradiction. □

**Theorem 4.29.** *The alternating group $A_n$ is a simple group of order $\frac{n!}{2}$, for $n \geq 5$.*

*Proof.* We proceed inductively on $n \geq 6$, since the case for $n = 5$ is provided above.

Suppose, for contradiction, that $A_n$ has a proper (non-trivial) normal subgroup $M$. The permutation group $A_n$ acts on $\Omega = \{1, 2, \dots n\}$ at least 4-transitively. This is easy to verify because $S_n$ is the set of all permutations and acts $n$-transitively on $\Omega$. Thus, if we want to take $(a_1, a_2, a_3, a_4)$ to $(b_1, b_2, b_3, b_4)$, such a permutation $\sigma$ exists in $S_n$. If it is even, it is in $A_n$. Otherwise, we can precompose $\sigma$ with the transposition $(a_5\ a_6)$ such that $a_5, a_6$ are 2 elements not in our first list (these exist because $n \geq 6$).

For any $\omega \in \Omega$, the stabilizer of $\omega$ in $A_n$, $\text{Stab}_{A_n}(\omega)$, is isomorphic to $A_{n-1}$. Now we can apply Propositions 4.23 and 4.25. Since $A_n$ acts 2-transitively on $\Omega$, $\text{Stab}_{A_n}(\omega)$ is a maximal subgroup. Now it is easy to see that if we conguate $\text{Stab}_{A_n}(\omega)$ by $(\omega\ \omega')$, we have $\text{Stab}_{A_n}(\omega')$. Since $M$ is normal, if it contained any of the stabilizers, it would contain all of them by conjugacy, and $M = A_n$, because they are maximal. This is a contradiction, so $M$ cannot contain any $\text{Stab}_{A_n}(\omega)$. We can apply the inductive hypothesis and see that each $\text{Stab}_{A_n}(\omega)$ is simple. Thus, $M \cap \text{Stab}_{A_n}(\omega) \trianglelefteq \text{Stab}_{A_n}(\omega)$ is $\{\text{id}\}$ or $\text{Stab}_{A_n}(\omega)$. But $M \not\supseteq \text{Stab}_{A_n}(\omega)$, so $M \cap \text{Stab}_{A_n}(\omega) = \{\text{id}\}$. The maximality of $\text{Stab}_{A_n}(\omega)$ now ensures that $M\text{Stab}_{A_n}(\omega) = A_n$. Therefore,

$$n!/2 = |A_n| = |M\text{Stab}_{A_n}(\omega)| = \frac{|M||\text{Stab}_{A_n}(\omega)|}{|M \cap \text{Stab}_{A_n}(\omega)|} = |M|(n-1)!/2,$$

and so $|M| = n$. We will now show that $M$ must contain more than $n$ elements to be normal, when $n \geq 6$.

Let $\tau \in S_n$. Conjugation by $\tau$ induces an automorphism of $A_n$. Define $\phi_\tau(M) = \tau M \tau^{-1}$. We claim $M$ is normal in $S_n$. Suppose, for contradiction, $M \neq \phi_\tau(M)$. Now, $M\phi_\tau(M)$ will be a normal subgroup of $A_n$ that contains $M$, so $|M\phi_\tau(M)| > n$. We have shown that any proper normal subgroup of $A_n$ must have order $n$, so $M\phi_\tau(M) = A_n$. In addition, $|M\phi_\tau(M)| \leq n2$, by Theorem 1.9, so $|A_n| = n!/2 \leq n2$, which is false for $n \geq 5$. This contradiction proves that $M = \phi_\tau(M)$, and $M$ is normal in $S_n$. By Cauchy's theorem, we may choose $m \in M$ of prime order $p$, where $p|n$. Because the intersection of $M$ and any of the $\text{Stab}_{A_n}(\omega)$ is trivial, $m$ has no fixed points when acting on $\Omega$. In particular, the cycle shape of $m$ contains no 1-cycles. In addition, the order of an element is the least common multiple of the lengths of its cycles, so $m$ must be a product of $r$ disjoint cycles of length $p$, where $pr = n$.

Let us consider the case where $p > 2$. In this case, we consider just the cycles that start with $(1\ a\ b \dots)$. There are $(n-1)$ ways to choose $a$, and $(n-2)$ ways to choose $b$, so there must be at least $(n-1)(n-2)+1$ elements in $M$, since all cycles of the same shape are conjugate, as proven previously. But then $(n-1)(n-2)+1 \geq n$

which is incorrect for $n \geq 3$.

If $p = 2$, the statement is weaker. We have already shown that $A_4$ is not simple, so our argument must rely on the fact that we are considering $n \geq 6$. In this case, $m$ is composed of at least 3 2-cycles, so we consider the cycles of the form $(1a)(2b)(3c)\ldots$. Thus, we have at least $(n-3)(n-4)(n-5)+1$ elements in $M$, by a similar argument as in the $p > 2$ case, but that implies $(n-3)(n-4)(n-5)+1 < |M| = n$ for $n \geq 6$. Therefore, this also results in a contradiction, and we are done. □

**Acknowledgments.** It is a pleasure to thank my mentor, Robin Walters, for providing guidance and support, and for illuminating the complexities of the finite groups. Also, I would also like to thank Peter May for giving me this opportunity and for his joint class with Rina Anno which provided many of the exercises that guided me.

## References

[1] Patrick J. Morandi. $A_n$ is simple. http://sierra.nmsu.edu/morandi/notes/an-is-simple.pdf
[2] Geoff Smith and Olga Tabachnikova. Topics in Group Theory Springer. 1999.