Classification of Finite Simple Groups

Adam Michael

May 5, 2016

In Abstract Algebra, we give special attention to normal subgroups. Normal subgroups have several interesting properties, including equality of left and right cosets and the ability to construct quotient groups. A natural extension of the study of normal subgroups is the problem of finding the normal subgroups of a given group. For a group G, both the trivial group and G are normal subgroups of G and if G is abelian then every subgroup is normal. But in general, it is not at all obvious if G has any other normal subgroups. This gives rise to the study of simple groups and their classification.

Definition 1. *A nontrivial group G is simple if its only normal subgroups are the trivial group and G.*

I will focus specifically on finite simple groups. The study of finite simple groups is a rich and far-reaching subject. I will give a brief history of the subject, state the most significant major result and provide proofs of a few smaller results.

The study of finite simple groups began with Galois around 1830 when he was studying the solutions by radicals to polynomial equations [2]. Galois proved that the alternating groups on at least five letters are simple. In 1870, Camille Jordan constructed the projective special linear groups $PSL_n(q)$ and proved they are simple for prime-power q. In 1872, Ludwig Sylow proved the Sylow Theorems which were among the first results used to classify finite simple groups [4]. The Sylow Theorems are given below without proof. An example demonstrates how they can be used to study finite simple groups.

Definition 2. *If G is a group, $H_1 \leq G$, $H_2 \leq G$, $g \in G$ and $gH_1g^{-1} = H_2$ then H_1 and H_2 are called conjugate.*

Theorem 1 (Sylow Theorems [4])**.** *If G is a finite group of order $p^k n$, p prime and $p \nmid n$, then*

1. *G has subgroups of order p^k, called Sylow p-subgroups*
2. *The Sylow p-subgroups are all conjugate*
3. *The number s_p of Sylow p-subgroups is such that $s_p \mid m$ and $s_p \equiv 1 \mod p$*

Theorem 2. *If G is a finite group and S is a Sylow p-subgroup, S is normal in G if and only if it is the unique Sylow p-subgroup. [4]*

Proof.

- $\Rightarrow$ Suppose S and S' are normal Sylow p-subgroups. By the second Sylow Theorem, there exists $g \in G$ such that $gSg^{-1} = S'$. S is normal so $gSg^{-1} = S$. So $S = S'$.

- $\Leftarrow$ Suppose S is the unique Sylow p-subgroup. Let $g \in G$. Note that $|gSg^{-1}| = |S|$ because S is a group. Consider $gag^{-1}, gbg^{-1} \in gSg^{-1}$. $gag^{-1}gbg^{-1} = g(ab)g^{-1} \in gSg^{-1}$. So by the finite subgroup test, gSg^{-1} is a subgroup of order $|S|$. So $gSg^{-1} = S$. Therefore S is normal.

□

Example 1. *Let G be a group of order $84 = 2^2 \cdot 3 \cdot 7$. Then by the third Sylow Theorem, $s_7 \mid 12$. So $s_7 \in \{1, 2, 3, 4, 6, 12\}$. Also, $s_7 \equiv 1 \mod 7$, so $s_7 = 1$. Then by Theorem 2, the unique Sylow 7-subgroup is normal in G. Therefore there are no simple groups of order 84.*

As seen in the example above, the Sylow Theorems are useful for proving that all groups of specific orders have a nontrivial proper normal subgroup. In 1892, Otto Hölder proved another remarkable result on the order of finite simple groups. Hölder proved that a non-abelian finite simple group must have order a product of at least four primes. In 1963, Walter Feit and John Thompson narrowed the search for the order of finite simple groups even more. The Feit-Thompson Theorem states that every finite group of odd order is solvable. As corollary, every non-abelian finite simple group has even order. At this point, group theorists began to believe that all finite abelian groups had been found [4]. This sparked a large-scale effort to prove a complete classification theorem for finite simple groups. Over the next two decades, about twenty new finite simple groups were found. In the 1980s, it was generally believed that all finite simple groups had been found and that a proof could be compiled. The resulting Classification Theorem for Finite Simple Group spans tens of thousands of pages across publications by over 100 authors.

Theorem 3 (Classification Theorem for Finite Simple Groups (CTFSG) [4])**.** *The following groups are simple and every finite simple group is isomorphic to one of them:*

1. *A cyclic group Z_p of prime order p*
2. *An alternating group A_n for $n \geq 5$*
3. *A classical group for q a prime-power:*
   - *Linear: $PSL_n(q)$, $n \geq 2$, except $PSL_2(2)$ and $PSL_2(3)$*
   - *Unitary: $PSU_n(q)$, $n \geq 3$, except $PSU_3(2)$*
   - *Symplectic: $PSp_{2n}(q)$, $n \geq 2$, except $PSp_4(2)$*
   - *Orthogonal: $P\Omega_{2n+1}(q)$, $n \geq 3$, q odd*
     $P\Omega^+_{2n}(q)$, $n \geq 4$
     $P\Omega^-_{2n}(q)$, $n \geq 4$
4. *An exceptional group of Lie Type for q a prime-power:*

- $G_2(q)$, $q \geq 3$; $F_4(q)$; $E_6(q)$; ${}^2E_6(q)$; ${}^3D_4(q)$; $E_7(q)$; $E_8(q)$
- ${}^2B_2(2^{2n+1})$, $n \geq 1$; ${}^2G_2(3^{2n+1})$, $n \geq 1$; ${}^2F_4(2^{2n+1})$, $n \geq 1$

or the Tits group ${}^2F_4(2)'$*, which is closely related to a group of Lie Type*

5. *One of 26 sporadic simple groups:*
   - *The Mathieu groups* $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$
   - *The Leech lattice groups* $Co_1, Co_2, Co_3, McL, HS, Suz, J_2$
   - *The Fischer groups* $Fi_{22}, Fi_{23}, Fi'_{24}$
   - *The monstrous groups* $\mathbb{M}, \mathbb{B}, Th, HB, He$
   - *The pariahs* $J_1, J_3, J_4, O'N, Ly, Ru$.

The scope of CTFSG is surprising to say the least. Simple groups are similar to prime numbers in the sense that groups can be factored into quotient groups in much the same way that integers are factored into their prime factorization. (Note that there is not necessarily a unique way to factor a group into quotient groups.) However there is no known analogous classification theorem for prime numbers. Imminent completion of the proof of CTFSG was announced around 1980. Gorenstein, Lyons and Solon have attempted to consolidate the entire proof into one publication. Six of the eleven proposed "volumes" of the proof have been published with the most recent being published in 2005 [3]. Solomon has estimated that the total proof will consist of approximately 5,000 pages. Due to the sheer size of the proof, I will only discuss a small part of it. I will start with the classification of finite abelian simple groups.

Theorem 4. *For prime p, $\mathbb{Z}_p$ is simple.*

Proof. Since $\mathbb{Z}_p$ has p elements, by LaGrange's Theorem all subgroups of $\mathbb{Z}_p$ have order dividing p. Since p is prime, the only subgroups of $\mathbb{Z}_p$ are $\mathbb{Z}_p$ and $\{0\}$. Therefore $\mathbb{Z}_p$ has no nontrivial proper subgroups, so it is simple. □

Theorem 5. *If G is a simple nontrivial abelian group, then $G \cong \mathbb{Z}_p$ from some prime p.*

Proof. Consider $x \in G$, $x \neq e$. Then $\{e\} \neq \langle x \rangle \leq G$. G is abelian so $\langle x \rangle \triangleleft G$. Then since G is simple, $\langle x \rangle = G$. If $|\langle x \rangle| = \infty$, then $\langle x \rangle < \langle x^2 \rangle \leq G$, which contradicts $\langle x \rangle = G$. Thus If $|\langle x \rangle| = p$ for some finite p. Therefore $G \cong \mathbb{Z}_p$. Suppose p is composite, that is $p = mn$, $m > 1, n > 1$. Then $Z_n \leq Z_p \cong G$, so G has a nontrivial proper subgroup. But since G is abelian, this contradicts the supposition that G is simple. Therefore p must be prime. □

Thus we have classified all finite abelian simple groups as exactly the groups $\mathbb{Z}_p$ for prime p. The classification for abelian groups is far simpler than for nonabelian groups. This is not surprising, as the Fundamental Theorem of Finite Abelian Groups states that all finite abelian groups are isomorphic to the direct product of prime-power cyclic groups. The direct product of two prime-power cyclic groups contains a subgroup isomorphic to one of the prime-power cyclic groups, so it is not simple. I will now show that the alternating groups on more than four letters are simple. The proof for A_n is more complicated than that for $\mathbb{Z}_p$, so it is broken into multiple theorems, roughly following the proof in Dummit and Foote [1].

Theorem 6. *For $n \geq 3$, A_n is exactly the set of products of 3-cycles on n letters.*

Proof.

- $\Leftarrow$ Let $\sigma = \sigma_1\sigma_2...\sigma_k$ be a product of 3-cycles. Since each σ_i is even, σ is even. So $\sigma \in A_n$.
- $\Rightarrow$ Let $\sigma \in A_n$. Write σ as a product of transpositions. Since σ is even, $\sigma = (a_1\ b_1)(c_1\ d_1)...(a_k\ b_k)(c_k\ d_k)$. Consider $(a_i\ b_i)(c_i\ d_i)$. Since $(a_i\ b_i)$ and $(c_i\ d_i)$ are transpositions, it must be the case that $a_i \neq b_i$ and $c_i \neq d_i$. If a_i, b_i, c_i, d_i are all distinct, then $(a_i\ b_i)(c_i\ d_i) = (a_i\ b_i\ c_i)(b_i\ c_i\ d_i)$. If a_i, b_i, c_i, d_i contain one duplicate letter, without loss of generality (or by relabeling) suppose $a_i = c_i$. Then $(a_i\ b_i)(a_i\ d_i) = (a_i\ d_i\ b_i)$. If a_i, b_i, c_i, d_i contain two duplicate letters, then $(a_i\ b_i)(a_i\ b_i) = ()$. Thus each pair of transpositions in σ can be replaced by a product of 3-cycles. Therefore σ is a product of 3-cycles.

□

Definition 3. *For a group G, if $a, b \in G$ then b is conjugate to a if there exists $g \in G$ such that $gag^{-1} = b$.*

Theorem 7. *For every pair of 3-cycles $c_1, c_2 \in A_n$, c_2 is conjugate to c_1.*

Proof. Let $c_1 = (a\ b\ c)$. Proceed by cases on the number of letters shared by c_1 and c_2.

Case 1: c_2 shares no letters with c_1. Then $c_2 = (d\ e\ f)$ and a, b, c, d, e, f are all distinct. Let $s = (d\ e)(e\ f)(b\ d)(a\ e) \in A_n$. Then $sc_1s^{-1} = (d\ e)(e\ f)(b\ d)(a\ e)(a\ b\ c)(a\ e)(b\ d)(e\ f)(d\ e) = (d\ e\ f) = c_2$.

Case 2: c_2 shares one letter with c_1. Relabel so that $c_2 = (a\ d\ e)$. Let $s = (b\ d)(c\ e) \in A_n$. Then $sc_1s^{-1} = (b\ d)(c\ e)(a\ b\ c)(c\ e)(b\ d) = (a\ d\ e) = c_2$.

Case 3: c_2 shares two letters with c_1. Relabel so that $c_2 = (a\ b\ d)$. Let $s = (c\ d)(d\ e) \in A_n$. Then $sc_1s^{-1} = (c\ d)(d\ e)(a\ b\ c)(d\ e)(c\ d) = (a\ b\ d) = c_2$.

Case 4: c_2 shares three letters with c_1. Then $c_2 = c_1$. Let $s = () \in A_n$. Then $()c_1()^{-1} = c_1 = c_2$.

□

The remaining proofs will rely on Theorems 6 and 7 to show that if A_n has a nontrivial normal subgroup N, then $N = A_n$ so A_n is normal. Theorem 8 will show that A_5 is simple and will be used as a base case for Theorem 9.

Lemma 1. *If $N \triangleleft A_5$ and $N \neq \{()\}$ then N contains a 3-cycle.*

Proof. Since $N \neq \{()\}$, there exists $\sigma \in N$, $\sigma \neq ()$. Since $\sigma \neq ()$, σ is even and σ acts on 5 letters, there are three possibilities for σ written as a product of disjoint cycles.

Case 1: $\sigma = (a\ b\ c)$. Then σ is a 3-cycle in N.

Case 2: $\sigma = (a\ b\ c\ d\ e)$. Let $\alpha = (a\ b)(c\ d) \in A_n$. Since $N \triangleleft A_n$, $\sigma\alpha\sigma\alpha^{-1} \in N$. $\sigma\alpha\sigma\alpha^{-1} = (a\ b\ c\ d\ e)(a\ b)(c\ d)(a\ b\ c\ d\ e)(a\ b)(c\ d) = (a\ e\ c)$. So $(a\ e\ c)$ is a 3-cycle in N.

Case 3: $\sigma = (a\ b)(c\ d)$. Let $\alpha = (a\ b\ e) \in A_n$. Since $N \triangleleft A_n$, $\sigma\alpha\sigma\alpha^{-1} \in N$. $\sigma\alpha\sigma\alpha^{-1} = (a\ b)(c\ d)(a\ b\ e)(a\ b)(c\ d)(a\ e\ b) = (a\ b\ e)$. So $(a\ b\ e)$ is a 3-cycle in N.

□

Theorem 8. *A_5 is simple.*

Proof. Suppose A_5 has a nontrivial normal subgroup $N \triangleleft A_5$. By Lemma 1, N contains a 3-cycle c_1. Let c_2 be a 3-cycle in A_n. Then by Theorem 7, there exists $s \in A_n$ such that $sc_1s^{-1} = c_2$. Then since N is normal $c_2 \in N$. Therefore N contains all 3-cycles in A_n. Then since N is closed, by Theorem 6 we have $N = A_n$. Therefore A_n is simple. □

Lemma 2. *For $n \geq 5$, if $\sigma \in A_n$, $\sigma \neq ()$, then there exists $\sigma' \in A_n$, $\sigma' \neq \sigma$ conjugate to σ such that for some $i \in \{1, ..., n\}$, $\sigma(i) = \sigma'(i)$.*

Proof. Let $\sigma \in A_n$, $\sigma \neq ()$. Write σ as the product of disjoint cycles and let r be the length of the longest disjoint cycle in σ. Since $\sigma \neq ()$, $r \geq 2$. If $r = 2$, then σ is the product of a non-zero even number of disjoint transpositions. Proceed by cases.

Case 1: $r = 2$ and σ is the product of two disjoint transpositions. Then $\sigma = (a\ b)(c\ d)$. Let $\alpha = (a\ c\ b)$ and $\sigma' = \alpha\sigma\alpha^{-1} = (a\ c\ b)(a\ b)(c\ d)(a\ b\ c) = (a\ c)(b\ d)$. Since $n \geq 5$, there exists $e \notin \{a, b, c, d\}$. So $\sigma \neq \sigma'$ and $\sigma(e) = \sigma'(e) = e$.

Case 2: $r = 2$ and σ is the product of more than two disjoint transpositions. Then write $\sigma = (a\ b)(c\ d)(e\ f)\pi$ where π is a permutation that fixes a, b, c, d, e, f. Let $\alpha = (a\ b)(c\ e)$ and $\sigma' = \alpha\sigma\alpha^{-1}$. Then $\sigma' = (a\ b)(c\ e)(a\ b)(c\ d)(e\ f)\pi(a\ b)(c\ e) = (a\ b)(c\ f)(d\ e)\pi$. So $\sigma \neq \sigma'$ and $\sigma(a) = \sigma'(a) = b$.

Case 3: $r > 2$. Then with relabeling, $\sigma = (1\ 2\ 3\ ...\ r)\pi$ where π is a permutation that fixes 1 through r. Let $\alpha = (3\ 4\ 5)$ and $\sigma' = \alpha\sigma\alpha^{-1} = (3\ 4\ 5)(1\ 2\ 3\ ...\ r)\pi(3\ 5\ 4)$. $\sigma(2) = 3$ and $\sigma'(2) = 4$ so $\sigma \neq \sigma'$ and $\sigma(1) = \sigma'(1) = 2$.

□

Theorem 9. *For $n \geq 5$, A_n is simple.*

Proof. By induction on n.
Base case: $n = 5$. Proved as Theorem 8.
Induction hypothesis: Suppose A_{k-1} is simple for $k \geq 6$.
Now consider A_k. Suppose A_k has a nontrivial normal subgroup $N \triangleleft A_k$ and there exists $\sigma \in N$, $\sigma \neq ()$. By Lemma 2, there exists $\sigma' \in A_k$ conjugate to σ and $i \in \{1, ..., k\}$ such that $\sigma \neq \sigma'$ and $\sigma(i) = \sigma'(i)$. This implies that $\sigma^{-1}\sigma' \neq ()$. Since N is normal, $\sigma' \in N$ and N is closed so $\sigma^{-1}\sigma' \in N$. By multiplication by inverse on the left of $\sigma(i) = \sigma'(i)$, $(\sigma^{-1}\sigma')(i) = i$. Now let

$H_i = \{s \in A_k \mid s(i) = i\} \leq A_k$. Then $H_i \cong A_{k-1}$. By the induction hypothesis, H_i is simple. So $\sigma^{-1}\sigma' \in H_i \cap N$. Since H_i and N are both normal subgroups of A_k, $H_i \cap N \triangleleft G$. $\sigma^{-1}\sigma' \in H_i \cap N$ and H_i is simple so $H_i \cap N = H_i$. Thus $H_i \subseteq N$. Since $H_i \cong A_{k-1}$ and $k \geq 6$, A_{k-1} contains a 3-cycle so H contains a 3-cycle. Therefore N contains a 3-cycle, $c_1 \in N$. Let $c_2 \in A_k$ be another 3-cycle. Then by Theorem 7 there exists $s \in A_k$ such that $sc_1s^{-1} = c_2$. Then since N is normal, $c_2 \in N$. So N contains all 3-cycles in A_k. Then by Theorem 6 we have $N = A_k$. Therefore A_k is simple. □

We have now classified all of the simple finite groups that are discussed in an introductory Abstract Algebra course. Many of the remaining groups require individual study and more background than $\mathbb{Z}_p$ and A_n. The majority of the non-abelian finite simple groups belong to the family of classical groups of Lie type. Each of these can be thought of as a specific group of matrices where the entries belong to a finite field of prime-power characteristic. The primary tool for proving the simplicity of the finite classical groups is Iwasawa's Lemma.

Lemma 3 (Iwasawa's Lemma [4])**.** *If G is a finite perfect group, acting faithfully (that is, there is an injective homomorphism $G \to Sym(\Omega)$) and primitively on a set Ω, such that the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

Definition 4. *The special linear group $SL_n(q)$ is the set of $n \times n$ invertible linear maps with determinant 1. Let $Z \triangleleft SL_n(q)$ be the normal subgroup of scalar multiples of the identity matrix. Then the projective special linear group $PSL_n(q)$ is defined as the quotient group $PSL_n(q) = SL_n(q)/Z$.*

We can apply Iwasawa's Lemma to $PSL_n(q)$ by letting $SL_n(q)$ act on $\Omega = \{\text{one dimensional subspaces of } \mathbb{F}_q^n\}$. Then the kernel of the action of $SL_n(q)$ on Ω is Z so $PSL_n(q) = SL_n(q)/Z$ acts faithfully on Ω. With a few more definitions, checking the stabilizer and checking that $PSL_n(q)$ is perfect, it can be shown by Iwasawa's Lemma that $PSL_n(q)$ is simple for $n > 2$ and $q > 3$.

The Classification Theorem for Finite Simple Groups is a monumental result in Group Theory both in terms of size and impact. There are many more interesting finite simple groups not discussed in this paper, many of which cannot be described succinctly.

References

[1] Dummit, David Steven., and Richard M. Foote. *Abstract Algebra*. New Delhi: Wiley-India, 2004. Print.

[2] Gallian, Joseph A. *Contemporary Abstract Algebra*. Boston, MA: Brooks / Cole Cengage Learning, 2013. Print.

[3] Gorenstein, Daniel, Richard Lyons, and Ronald Solomon. *The Classification of the Finite Simple Groups Number 6*. Providence, RI: American Mathematical Society, 2005. Print.

[4] Wilson, Robert. *The Finite Simple Groups*. London New York: Springer, 2009. Print.