The Classification of Finite Simple Groups

Seungjai Lee

National Institute for Mathematical Sciences

May 26, 2016

Overview

Introduction

Theorem (The Classification of Finite Simple Groups)

Every finite simple group is isomorphic to one of the following groups:

1. *A cyclic group* C_p *of prime order*
2. *An alternating group* A_n *of degree at least 5*
3. *A simple group of Lie type*
4. *The 26 sporadic simple groups*

In other words, every finite simple group either belongs to one of the 18 families, or is one of the 26 sporadic groups.

Preliminaries

Definition (Simple Group)

A simple group G is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

For example, C_3 is a finite simple group, whereas C_6 is not, since

$$C_3 \lhd C_6.$$

Finite simple groups are important because they are the "building blocks" of all finite groups.

If a group G has a nontrivial normal subgroup N, then the quotient group G/N can be formed. We can study G by studying the "smaller groups" G/N and N.

Definition (Composition Series)

A composition series of a group G is a subnormal series of finite length

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = G,$$

with strict inclusions, such that each H_i is a maximal normal subgroup of H_{i+1}. The factor groups H_{i+1}/H_i are called composition factors.

The composition series for a given group G may not be unique. However, the following theorem shows why the classification of finite simple groups is important.

Theorem (The Jordan-Hölder Theorem)

Any two composition series of a given group G have the same composition length and the same composition factors, up to permutation and isomorphisms.

Example

- $1 \lhd C_2 \lhd C_6 \lhd C_{12}$,
- $1 \lhd C_2 \lhd C_4 \lhd C_{12}$,
- $1 \lhd C_3 \lhd C_6 \lhd C_{12}$.

The composition factors are C_2, C_2, C_3.

The above example shows C_{12} is made of C_2, C_2, and C_3.

History: Two sides of the same coin

In 1832, Galois, the founder of Group Theory, first introduced normal subgroups and proved that A_n for $n \geq 5$ and $\mathrm{PSL}(2, p)$ for $p \geq 5$.

However, it was Jordan who first tried to list all the known simple groups during his time in 1870 and emphasizes the importance of the simple groups. Later, in 1892, Hölder asked for a classification of finite simple groups ("It would be of the greatest interest if it were possible to give an overview of the entire collection of finite simple groups.").

Since then, two very different approaches have been applied by mathematicians to tackle this huge project. One was to find all the possible simple groups manually, like a treasure hunting. It was very rewarding but also very risky.

The other approach was to rigorously restrict the conditions for G to be simple. It was more systematic and reliable, but not as exciting as the former.

John Conway and the ATLAS of Finite Groups

John Horton Conway FRS(1937-present), Emeritus Professor of Mathematics at Princeton University, can be regarded as one of the most notable figures in the first approach.

In 1970s, John Conway, Robert Curtis, Simon Norton, Richard Parker and Robert Wilson decided to record all the known simple groups in a book called the ATLAS of Finite Groups. This book was first published in December 1985 and reprinted with correction in 2003.

It lists basic information about 93 finite simple groups, from A_5 to the Monster.

Table

Year	Name	Object
1832	Galois	A_n, $\mathrm{PSL}_2(\mathbb{F}_p)$
1861	Mathieu	Mathieu groups M_{11}, M_{12}
1873	Mathieu	Mathieu groups M_{22}, M_{23}, M_{24}
1901	Dickson	Classical Lie groups and Exceptional E_6
1905	Dickson	Exceptional G_2
1955	Chevalley	Exceptional E_7, E_8, F_4
1959	Steinberg	Steinberg groups ${}^3D_4$ and ${}^2E_6$
1960	Suzuki	Suzuki groups ${}^2B_2$
1961	Ree	Ree groups ${}^2F_4$ and ${}^2G_2$
1964	Tits	Tits group ${}^2F_4(2)$
1966	Janko	Janko group J_1
1968	Higman, Sims	Higman-Sims group HS
1968	Conway	Conway groups Co_0, Co_1 and Co_2

1969	Various	Suzuki Sz, Janko J_2, J_3, McLaughlin McL, Held H
1971	Fischer	Fischer groups Fi_{22}, Fi_{23} and Fi_{24}
1972	Lyons	Lyons group Ly
1973	Rudvalis	Rudvalis group Ru
1973	Fischer	Baby Monster group B
1976	Harada, Norton	Harada-Norton group HN
1976	Thompson	Thompson group Th
1976	O'Nan	O'Nan group $O'N$
1976	Janko	Janko J_4
1982	Griess	Monster M

In 1860s and 70s, Mathieu discovered 5 finite simple groups that did not seem to have common properties to describe them as an infinite family. After spending years and years to understand these exotic objects, Burnside(1911) decided to call them "sporadic simple groups". Ironically, Mathieu was not trying to find finite simple groups. He was interested in finding multiply transitive permutation groups.

Definition (Multiply transitive permutation groups)

For a natural number k, a permutation group G acting on n points is k-**transitive** if, given two sets of distinct points $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$, there is a group element g in G which maps a_i to b_i for each i between 1 and k. Such a group is called **Sharply** k-**transitive** if the element g is unique.

Group	Order	Property
M_8	8	Sharply 1-transitive (Regular)
M_9	72	Sharply 2-transitive
M_{10}	720	Sharply 3-transitive
M_{11}	7920	Sharply 4-transitive
M_{12}	95040	Sharply 5-transitive
M_{20}	960	1-transitive
M_{21}	20160	2-transitive
M_{22}	443520	3-transitive
M_{23}	10200960	4-transitive
M_{24}	244823040	5-transitive

Table: Mathieu Groups

Although mathematicians could not understand why these 5 sporadic simple groups exist, they began to think these groups are the only exceptional ones that they need to know. One reason for this was because they "failed" to discover another such group for almost 100 years.

In the early 1960s, people almost believed that the 18 infinite families and the 5 Mathieu groups are enough to classify all finite simple groups. Especially, Feit and Thomson's proof of Burnside's Odd Order Theorem (which is now called Feit-Thompson Theorem) in 1963 strengthened this belief.

However, their optimism (or a pessimism) was collapsed by a letter from a Croatian mathematician.

When Janko first discovered a simple group of order 175560 (which later called J_1), he too thought it should be one of the 18 families. However, after he failed to see this, he wrote a letter to Thompson about this new group.

In 1965, Janko finally proved that his group J_1 is in fact a new sporadic simple group. Furthermore, he conjectured that there will be at least 3 more sporadic simple groups.

90 years of silence did not guarantee the end of sporadic simple groups. Janko's discovery started the modern theory of sporadic group.

When Janko first discovered a new simple group of order 175560, he too thought it should be one of the 18 families. However, after he failed to see this, he wrote a letter to Thompson about this new group.

Definition (J_1)

J_1 has a standard presentation

$$< a^2 = b^3 = (ab)^7 = (ab(abab^{-1})^3)^5 = (ab(abab^{-1})^6 abab(ab^{-1})^2)^2 = 1 > .$$

The standard generators of J_1 are a and b where a has order 2, b has order 3, ab has order 7 and $ababb$ has order 19.

In 1966, Janko finally proved that his group J_1 is in fact a new sporadic simple group. Furthermore, he conjectured that there will be at least 3 more sporadic simple groups.

90 years of silence did not guarantee the end of sporadic simple groups. Janko's discovery started the modern theory of sporadic group.

The Monster

Before Janko, it took 90 years to find a new sporadic group after Mathieu. However, after Janko's discovery, 12 new sporadic groups were discovered in only 5 years. It was around that time when Gorenstein started his 'Program' to stop this madness.

In 1973, Fischer and Griess predicted an enormous simple group (of order 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000) that is now called the Monster M. Fischer, Conway, Norton and Thompson also proved that if this group exists, then this group contains other sporadic groups as subquotients of this group.

It was Griess in 1982 who finally constructed the Monster, and hence proved its existence. However, no one at that time expected this group has anything to do with Modular Forms. The famous 'Monstrous Moonshine' describes the unexpected connection between M and modular functions.

Eliminating the impossible

Since Hölder asked for a classification of finite simple groups, group theorists tried to list the conditions for an arbitrary finite group G to be simple. Unlike the previous subsection, I cannot list all the individual Lemmas and Theorems that helped finishing this classification project.

Therefore, I decided to select some of the main theorems that I think worth mentioning during this talk.

Major Theorems

Year	Name	Object
1872	Sylow	Sylow Theorems
1901	Frobenius	Proved that a Frobenius group is not simple
1901	Dickson	Defined classical Lie groups
1904	Burnside	Burnside's Theorem
1963	Feit, Thompson	Feit-Thompson Theorem

Then, in 1972, Daniel Gorenstein announced a 16-step program for completing the classification of finite simple groups.

Theorem (Sylow Theorem)

Let G be a finite group.

1. *For every prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow p-subgroup $Syl_p(G)$ of G, of order p^n.*
2. *Given a finite group G and a prime number p, all $Syl_p(G)$ are conjugate to each other.*
3. *Let $|G| = p^n m$ where $n > 0$ and p does not divide m. Let n_p be the number of $Syl_p(G)$. Then the following hold:*
    - *n_p divides m.*
    - *$n_p \equiv 1 \mod p$.*
    - *$n_p = |G : N_G(P)|$.*

Consequences: If $n_p = 1$, then $\mathrm{Syl}_p(G) \lhd G$.

Definition (Frobenius Group)

A finite G is said to be a **Frobenius group** if there exist a non-trivial subgroup H of G such that

$$H \cap gHg^{-1} = 1$$

wherever $g \notin H$. We call this H a Frobenius complement of G.

Theorem (Frobenius' theorem)

Let G be a Frobenius group with Frobenius complement H. Let K be the Frobenius Kernel of G, defined as the identity element together with all the non-identity elements that are not conjugate to any element of H. Then $K \triangleleft G$.

Theorem (Burnside Theorem)

If G is a finite group of order $p^a q^b$ where p and q are prime numbers, and a and b are non-negative integers, then G is solvable.

Theorem (Feit-Thompson Theorem)

Every finite group of odd order is solvable.

Consequence:

1. Every non-abelian finite simple group has even order
2. the classification of finite simple groups can be tackled using centralizers of involutions

In 2012, Georges Gonthier announced a computer-checked version of the Feit-Thompson theorem using the Coq proof assistant.

1. Groups of low 2-rank
2. The semisimplicity of 2-layers
3. Standard form in odd characteristic
4. Classification of groups of odd type
5. Quasi-standard form
6. Central involutions
7. Classification of alternating groups
8. Some sporadic groups
9. Thin groups
10. Groups with a strongly p-embedded subgroup for p odd
11. The signalizer functor method for odd primes
12. Groups of characteristic p-type
13. Quasithin groups
14. Groups of low 2-local 3-rank
15. Centralizers of 3-elements in standard form
16. Classification of simple groups of characteristic 2 type

Unfortunately, the details of each step are too difficult and technical. So I decided to just introduce 3 major methods that Gorenstein and his fellow mathematicians applied.

1. Signalizer Method
2. Strong p-embedding
3. Semisimple Elements and Components

Not-so-happy ending?

"In February 1981 the classification of finite simple groups was completed." So wrote Daniel Gorenstein. The whole proof, or rather a collection of proofs of different theorems, consists of more than 10,000 pages. Was this really the end of our fairy tale?

Unfortunately, it was not. In 1989, people realised that No.13 of his program, the Quasithin groups, was incomplete. In other words, the proof of CFSG theorem was relying on 800 pages of incomplete proof.

Gorenstein, who was the leader of the largest collaborative piece of pure mathematics ever attempted, died in 1992. Sadly, he could not see the correction on the Quasithin groups.

The Second-Generation Classification Proof

Even before they knew about the gap in their proof, group theorists felt the necessity of re-write and simplify their result. Again, it was Gorenstein who initiated this "second-generation classification proof" project.

Gorenstein, Lyons and Solomon Launched a so-called GLS program to simplify large parts of the proof and to re-write it down clearly and carefully in one place.

The first volume of the second generation proof was published in 1994. 6 volumes have been published so far, and Solomon in 2012 estimated that the project need another 5 volumes. He estimated that the new volume will eventually fill approximately 5,000 pages.

Of course, the second generation classification proof would make no sense if the first generation proof is incomplete.

It was Michael Aschbacher, one of the main players in Gorenstein's team, that finally completed the unfinished program of Gorenstein. In 2004, more than 20 years since Gorenstein first 'anounced' the end of his program, Aschbacher and Smith published their work on Quasithin group, filling the last gap in the proof. This new proof takes 1221 pages.

In 2004, the same year he proved the last piece of Gorenstein's original program, Aschbacher called for a third generation program.

Consequences of the classification

This is a list of some results that have been proved using the classification of finite simple groups.

- The Schreier conjecture
- The Signalizer functor theorem
- The B conjecture
- The Schur-Zassenhaus theorem for all groups
- The classification of 2-transitive permutation groups
- The classification of rank 3 permutation groups
- The Sims conjecture
- Frobenius's conjecture on the number of solutions of $x^n = 1$.

Next step

It is a fair criticism that it is too premature to call this classification a "Theorem". Even Conway admit that his ATLAS, or Gorenstein's Program can contain errors. However, it does not mean that these 18 families and 26 sporadic groups are wrong. Our 'periodic table' might not be complete, but at least all of our known elements are correct.

The real problem is, that people think the finite group theory has reached its end. Of course, this is not true. There are many areas and problems in finite group theory that need to be studied, just like any other parts of mathematics.

The obvious one is, as I wrote earlier, simplifying and re-writing the proof in a more accessible form. There is a real risk that if the techniques get forgotten before the proof is put into an accessible form, then, in the words of Gorenstein, "it will gradually become lost to the living world of mathematics, buried deep within the dusty pages of forgotten journals".

A second major theme in finite group theory is the Extension problem for finite group. The Jordan-Hölder Theorem suggests we can 'factorise' any finite group into a 'product' of finite simple groups. Informally speaking, Extension problem wants to study the opposite. To be precise

The Extension Problem

Given groups X and Y, determine all extensions of X by Y; i.e. determine all groups G with a normal subgroup H such that $H \cong X$ and $G/H \cong Y$.

If the classification problem is analogous to constructing a periodic table of the elements, the extension problem is analogous to studying what can be created by combining these elements. So, in a way the classification problem was a beginning of finite group theory, rather than the end.

This example shows why the extension problem is more difficult than the classification problem.

Example

- $C_3 \times C_2 = C_6$
- $C_3 \rtimes C_2 = D_6$
- $C_2 \triangleleft C_4$
- $C_2 \triangleleft C_2 \times C_2 = V_4$

The point is, unlike the prime factorization, it is not enough to know only the "simple factors" of a finite group G. We also need to know how they are extended.

One of the main conjecture in the extension problem is Higman's PORC conjecture. In 1960, Higman conjectured that for fixed n, the number $f_n(p)$ of finite $p-$groups of order p^n is given by a polynomial in p whose coefficients depend on the residue class of p modulo some fixed integer N.

Theorem (Higman's PORC Conjecture)

For any n, there exists a fixed integer N and finitely many polynomials $g_i(x)$ ($i = 1, \ldots, k \leq N$) such that if $p \equiv i \pmod N$ then

$$f_n(p) = g_i(p).$$

Example

For $p \geq 5$,

$$f(p^5) = 2p + 2\mathrm{gcd}(p-1, 3) + \mathrm{gcd}(p-1, 4) + 61$$

so $f(p^5)$ is one of 4 polynomials in p, with the choice of polynomials depending on the residue class of p modulo 12.

Fact

	$p = 2$	$p = 3$	$p \geq 5$
$f(p)$	1	1	1
$f(p^2)$	2	2	2
$f(p^3)$	5	5	5
$f(p^4)$	14	15	15

Up to this day, Higman's conjecture is proved to be true for $n \leq 7$.

What I do

Fact

A finitely generated group G has only a finite number of subgroups/normal subgroups of each finite index. In other words,

$$a_n^*(G) := \#\{H : H * G \text{ and } |G : H| = n\} < \infty$$

for each $n \in \mathbb{N}$, where $* \in \{\leq, \lhd\}$.

We want to study the asymptotic behaviour of the sequence $((a_n^*(G)))$.

Zeta Functions of Groups and Rings

In 1988, Grunewald, Segal and Smith introduced a new kind of zeta function, **zeta functions of groups and rings**, to count subgroups/normal subgroups of finite index in an infinite group.

Definition

Let G be a group. We define

$$\zeta_G^*(s) = \sum_{H * G} |G : H|^{-s} = \sum_{n=1}^{\infty} a_n^*(G) n^{-s}$$

the zeta function of a group G.

Thank you!