The Classification of the Finite Simple Groups

Damiano Testa

Mathematics Institute, University of Warwick

Tsinghua University, March 16-20, 2026

Introduction and notation

Throughout this lecture, we will be mostly talking about *groups*.

A *group* is a set G with a binary operation $(\_ \cdot \_) \colon G \times G \to G$ (often written by juxtaposition) such that:

- **associativity**: for all $a, b, c \in G$, the identity $(ab)c = a(bc)$ holds;
- **identity**: there exists $e \in G$ with $ae = ea = a$ for all a;
- **inverses**: for each a there exists a^{-1} with $a^{-1}a = aa^{-1} = e$.

An *involution* is an element $i \in G$ with $i \neq e$ and $i^2 = e$.

Involutions play a major role in the classification of finite simple groups.

Examples

- $(\mathbb{Z}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$
  In both cases, the identity is 0 and the inverse of a is $-a$.

  These groups are *abelian*: $a + b = b + a$.

- Let A be any set (e.g., $A = \{1, 2, \ldots, n\}$).

  The group $\mathrm{Sym}(A)$ is the group of bijections of A with itself.

- If R is a ring (associative, not necessarily commutative), then the units of R form a group under multiplication.

  E.g., $\mathrm{GL}_n(k)$ is the group of invertible $n \times n$ matrices over a field k.

Conjugacy and normal subgroups

Let G be a group and $g \in G$. The *conjugate* of $x \in G$ by g is gxg^{-1}.

The conjugate of a *subgroup H* of G is the subgroup

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

A subgroup N of G is *normal* if it is stable under conjugation by all of G:

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} = N \quad \text{for all } g \in G.$$

If N is normal in G, then there is a quotient group G/N and a quotient map $q \colon G \to G/N$ mapping products to products.

The map q is a surjective group homomorphism and the only elements of G mapping to the identity are the elements of N.

Informally, G is "built from" N and G/N.

p-groups and Sylow subgroups

A finite group P is a *p-group* if $|P|$ is a power of a prime p.

Let G be a finite group and let $|G| = p^n m$ with $p \nmid m$.

A subgroup $P \leq G$ of order p^n is called a *Sylow p-subgroup* of G.

- Sylow *p*-subgroups always exist.
- Every *p*-subgroup of G is contained in a Sylow *p*-subgroup.
- Any two Sylow *p*-subgroups are conjugate in G.

For instance, we will see Sylow 2-subgroups in a later slide.

Solvable groups and simple groups

Definition (Solvable group)

A group G is *solvable* if there is a finite chain

$$G_0 = \{e\} \leq G_1 \leq \cdots \leq G_n = G$$

of subgroups, where, for each $i \in \{0, \ldots, n-1\}$, the group G_i is normal in G_{i+1} and the quotient G_{i+1}/G_i is abelian.

Solvable groups are groups whose (recursive) building blocks are abelian.

In some sense, the opposite of solvable is simple.

Definition (Simple group)

A nontrivial group is *simple* if its only normal subgroups are $\{e\}$ and itself.

The statement of the classification

What are all the finite simple groups, then?

The classification of finite simple groups

The finite simple groups are:

- the cyclic groups of prime order;   (related to $\mathbb{Z}/n\mathbb{Z}$)
- the alternating groups;   (related to $\mathrm{Sym}\{1, \ldots, n\}$)
- the groups of Lie type;   (related to $\mathrm{GL}_n(k)$)
- the 26 sporadic groups.

In the proof, these are the *known groups*.

The goal is to show that no other finite simple groups exist.

Minimal counterexample

Let G a finite simple group of minimum order among the ones that have not yet been classified.

By minimality, every proper subgroup of G has all composition factors among the known simple groups.

The task is to deduce that G itself is known.

The Feit–Thompson Theorem

A key starting point is the Feit–Thompson (Odd Order) Theorem.

Theorem (Feit–Thompson, 1963)

Every finite group of odd order is solvable.

We may assume our minimal unknown finite simple group G is not cyclic of prime order.

Hence G is not solvable.

The Feit–Thompson Theorem implies that $|G|$ is even.

In particular, G contains elements of order 2.

Centralisers of involutions

The Feit–Thompson Theorem guarantees that any non-cyclic finite simple group G contains an involution.

This is the starting point of most classification results.

Many steps analyse the structure of *centralisers* of involutions in G.

The *centraliser* of an element $x \in G$ is the subgroup

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Centralisers of elements of prime order also receive a lot of attention.

Information about these centralisers often forces G into a short list of possibilities.

Gorenstein–Walter 1964

Theorem (Gorenstein–Walter, 1964)

A finite simple group whose Sylow 2–subgroups are dihedral is isomorphic to one of:

- $PSL_2(q)$ with q odd, $q > 3$;
- the alternating group A_7.

This is a consequence of a more general characterisation.

Gorenstein–Walter 1964 (general form)

For a finite group G, denote by $\mathbf{O}_{2'}(G)$ the maximal normal subgroup of G of odd order.

Theorem (Gorenstein–Walter, 1964)

Let G be a finite group whose Sylow 2-subgroups are dihedral.

Then $G/\mathbf{O}_{2'}(G)$ is isomorphic to:

- a subgroup of $\mathrm{P\Gamma L}_2(q)$ containing $\mathrm{PSL}_2(q)$, for some odd q;
- the alternating group A_7;
- a 2-group.

In particular, the simple groups with dihedral Sylow 2-subgroups are precisely $\mathrm{PSL}_2(q)$ (odd $q > 3$) and A_7.

Observations

1. The theorem classifies *all* finite groups with dihedral Sylow 2-subgroups, not just simple ones.
   This is crucial for inductive and reductive steps.

2. The simple groups that occur are exactly $PSL_2(q)$ (odd $q > 3$) and A_7
   No other simple groups have dihedral Sylow 2-subgroups.

3. Groups "close to simple" are important.
   Here, subgroups of $P\Gamma L_2(q)$ containing $PSL_2(q)$ play a key role.

4. The subgroup $\mathbf{O}_{2'}(G)$ (the largest normal subgroup of odd order) is not constrained by the conclusion; it is solvable (by Feit–Thompson).

A later result of Alperin–Brauer–Gorenstein treats the cases where the Sylow 2-subgroups are quasi-dihedral or wreathed.

The known groups (refined)

It is often helpful to separate Lie-type groups by the characteristic of the defining field:

- cyclic groups of prime order;
- alternating groups;
- groups of Lie type over fields of *odd characteristic*;
- groups of Lie type over fields of *characteristic* 2;
- the 26 sporadic groups.

Characteristic 2 is separated because involutions behave differently.

Centralisers of involutions in $SL_3(q)$

Odd characteristic (q odd)	**Characteristic 2 ($q = 2^f$)**
Involutions are **semisimple**	Involutions are **unipotent**
$$t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$	$$u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
Centraliser	**Centraliser**
$$C_{\mathrm{SL}_3(q)}(t) \subset \begin{pmatrix} GL_2(q) & 0 \\ 0 & * \end{pmatrix}$$	$$C_{\mathrm{SL}_3(q)}(u) \subset \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$$
Reductive (Lie type)	**Solvable (Borel type)**

Families of groups of Lie type

Of course, the "groups of Lie type" are also not an indivisible block.

They naturally subdivide into subclasses.

- **Classical:** linear, symplectic, even/odd orthogonal
- **Exceptional (untwisted):** G_2, F_4, E_6, E_7, E_8
- **Twisted:** ^2A_n (unitary), ^2D_n (including triality $^3D_4$), $^2E_6$, and the Suzuki $^2B_2(2^{2m+1})$, Ree $^2G_2(3^{2m+1})$, $^2F_4(2^{2m+1})$ families.

In classification arguments, each one must either occur or be ruled out.

The 26 sporadic groups

Each sporadic group comes with distinctive local and global features:

- Sylow subgroups,
- subgroup lattices,
- centralisers of elements,
- geometries,

and so on.

Every sporadic group arises somewhere in the classification and must be handled individually.

Case analysis and discovery

The proof consists of a massive case analysis.

Each case proves a classification theorem under additional hypotheses.

Once all options are covered, the full list of finite simple groups emerges.

Several sporadic groups were discovered through such local analyses.

These relations reveal that the classification is a tightly woven network of interconnected structures, and not a list of isolated objects.

These internal relations are instrumental in the proof.

Computer calculations

Besides pen-and-paper arguments, many parts of the classification require substantial computer calculations verifying properties of finite simple groups.

Many of these computations have not been thoroughly verified.

Formally checking these computations is a challenge of a different nature than formalising proofs intended for humans.

Humans, AI, and computation

Many parts of the classification are driven by broad organizing principles.

These ideas shape the whole proof and provide insight and direction.

Yet the endgame often reduces to case-specific arguments with limited transferability.

This mixture can possibly be leveraged to parallelise automated formalisation.

Even so, the formalisation of the proof of the classification of finite simple groups remains a daunting mathematical, software engineering and technological challenge.

Conclusion

The CFSG is probably the longest proofs in mathematics.

Formalizing it raises multiple challenges:

- the statement alone already involves complex mathematical objects (families of groups of Lie type, sporadic groups);
- assembling extensive background results across group theory, representation and character theory, algebraic groups, Lie theory, finite geometry, homological algebra, etc.;
- managing substantial computational input alongside human-readable arguments,

to name a few.

This does not contemplate the possibility that a gap is found and a fix is needed!

Thank you!

Questions?