

The Brauer-Fowler Theorem and the CFSG

Henrique Assumpção

Federal University of Minas Gerais

henriquesoares@dcc.ufmg.br

Algebraic Graph Theory 2026

June 16, 2026

Summary

- 1 Group theory basics
- 2 Who cares about simple groups?
- 3 Some History on Finite Simple Groups
- 4 Brauer-Fowler theorem
- 5 Classification of Finite Simple Groups

Group theory Basics

Definition 1 (Group)

Given a set G equipped with a binary operation $\cdot : G \times G \mapsto G$, we say that (G, \cdot) is a *group* if for all $a, b, c \in G$ the following conditions hold:

- 1 $a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- 2 There exists an identity element e in G such that $a \cdot e = e \cdot a = a$;
- 3 There exists an element a^{-1} in G such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Both the identity element and the inverse are unique, and if the operation is commutative, we say the group is *abelian*.

Subgroups, etc

- If $H \subseteq G$ is also a group w.r.t. the same operation as G , we say that H is a subgroup ($H \leq G$). $H \leq G$ iff $xy^{-1} \in H$ for any $x, y \in H$.
- If $H \leq G$ and $g \in G$, we let

$$gH = \{gh : h \in H\}, Hg = \{hg : h \in H\}$$

be the *right and left cosets*.

- If $g, h \in G$, we let $g^h := h^{-1}gh$. If $g \in G$, then its *order* is the smallest n such that $g^n = e$, and we let $\langle g \rangle := \{g^i : i \in \mathbb{Z}\}$.

Subgroups, etc

- $N \leq G$ is *normal* if $N^g = g^{-1}xg : x \in N = N$ for any $g \in G$ ($N \trianglelefteq G$).
- G is said to be *simple* if the only normal subgroups of G are $\{e\}$ and G .
- If $H \leq G$, then $G/H := \{gH : g \in G\}$ is the coset set, whose size is the *index* of H in G . If H is normal, G/H is again a group with operation given by $(gH)(g'H) = (gg')H$.

Homomorphisms

- If $\varphi : G \mapsto H$ is a function such that $\varphi(e_G) = \varphi(e_H)$ and $\varphi(gg') = \varphi(g)\varphi(g')$, then we say that φ is a *group homomorphism* ($\varphi \in \text{Hom}(G, H)$).
- If φ is bijective, then it's called an *isomorphism*, and if $G = H$, an *automorphism*.
- If X is a set, we let $\text{Sym}(X) := \{\sigma : X \mapsto X \mid \sigma \text{ is bijective}\}$ be its *symmetric group*.
- If $\varphi \in \text{Hom}(G, H)$, then

$$G / \ker(\varphi) \cong \text{Im}(\varphi).$$

Actions

- If G is a group and X is a set, then we say that G acts on X if there exists some $\varphi \in \text{Hom}(G, \text{Sym}(X))$, that is, if we can represent the elements of G as permutation of X .
- If the action is clear, we can simply write $gx := \varphi(g)(x)$, for $g \in G, x \in X$.
- If we set $\varphi_L \in \text{Hom}(G, \text{Sym}(G))$ as

$$\varphi_L(g)(h) = gh,$$

then we can easily see that φ_L is injective, hence G is isomorphic to some subgroup of $S_{|G|}$.

Actions

- If G acts on X , we define

$$G_x := \{g \in G : gx = x\} \leq G \text{ and } Gx := \{gx : g \in G\} \subseteq X,$$

and the *stabilizer* and *orbit* of $x \in X$.

- G acts on itself via conjugation, i.e., $\varphi(g)(x) = x^g$, the stabilizer w.r.t. x is the *centralizer* $C(x)$. The orbits are the *conjugacy classes*.
- G also acts on its subgroups via conjugation, and the stabilizer w.r.t. a subset S is the *normalizer* $N(S)$.
- If $H \leq G$, then H acts on G via right-multiplication, and the orbits are the cosets gH .

Basic results

Theorem 2 (Lagrange)

If $H \leq G$, then

$$|G| = |H| \cdot |G/H|.$$

Theorem 3 (Orbit-Stabilizer)

If G acts on X , then for any $x \in X$: $|G| = |G_x| \cdot |Gx|$.

Theorem 4 (Cauchy)

If p is a prime that divides $|G|$, then G has at least one element of order p .

Who cares about simple
groups?

Composition series

- If G is a finite group, then we can always find a sequence

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G,$$

where each G_i is normal in G_{i+1} and G_{i+1}/G_i is simple for all $0 \leq i < n$. This is the *composition series* of G , and G_{i+1}/G_i are the *composition factors*.

- If $G = \mathbb{Z}_6$, we have

$$1 \trianglelefteq \mathbb{Z}_2 \trianglelefteq \mathbb{Z}_6 \quad \text{and} \quad 1 \trianglelefteq \mathbb{Z}_3 \trianglelefteq \mathbb{Z}_6.$$

Theorem 5 (Jordan-Holder)

Given a finite group G , any two composition series are the same up to permutation/isomorphism of their composition factors.

Thus, in a very precise sense, finite simple groups are the building blocks of all finite groups.

Some History on Finite Simple Groups

History

- The cyclic groups C_p of prime-order are all obviously simple.
- First non-trivial simple groups are due to Galois: $A_n (n \geq 5)$ and $\text{PSL}(n, q) (n \geq 2, q \geq 5)$.
- A_n is the *alternating* group of all even permutations. Proof of simplicity is by induction + analyzing conjugacy classes.
- $\text{PSL}(n, q)$ is defined as the quotient of $\text{SL}(n, q)$ ($n \times n$ matrices over \mathbb{F}_q with determinant 1) by its center (diagonal matrices with determinant 1). Simplicity follows from Iwasawa's Lemma.

- A *Steiner* system $S(t, k, n)$ is a set of k -subsets of a base n element set such that every t -subset is contained in precisely one k -subset.
- The Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ are simple groups, corresponding to automorphisms of the Steiner systems

$$S(4, 5, 11), S(5, 6, 12), S(3, 6, 22), S(4, 7, 23), S(5, 8, 24).$$

- More simple groups constructed as analogues of Lie Groups are found.

- Brauer gave the following idea: choose a group H , and assume G is a finite simple group that has an involution u such that $C_G(u) \cong H$. Can we determine all possible G where this happens?
- For most H , no G had this property. But for some choices one was able to classify all G with this property.

Theorem 6

If G is a finite simple group with involution u such that $C_G(u) \cong GL(2, q)$, then either $G \cong PSL(3, q)$ or $q = 3$ and $G \cong M_{11}$.

Brauer-Fowler theorem

Lemma 7

If G is a finite group of even order and $A \subset G$ is the set of involutions of G , then provided that $|A| \geq 2$, there exists $g \in AA \setminus \{e\}$ such that

$$|N^*(g)| \geq \frac{|A|^2}{2|G|},$$

where $N^(g) = \{x \in G : g^x = g \text{ or } g^x = g^{-1}\}$.*

First, note

$$\begin{aligned}(1_A * 1_A)(g) &:= \sum_{h \in G} 1_A(h) 1_A(h^{-1}g) \\ &= \sum_{h \in A} 1_A(h^{-1}g) \\ &= |\{(x, y) \in A \times A : xy = g\}|.\end{aligned}$$

Thus

$$\sum_{g \in AA} (1_A * 1_A)(g) = |(x, y) \in A \times A| = |A|^2.$$

Also, note that if $h \in A$ and $h^{-1}g \in A$,

$$e = (h^{-1}g)^2 = h^{-1}gh^{-1}g = h^{-1}ghg = g^h g,$$

hence $g^h = g^{-1}$ and $h \in N^*(g)$. This shows that $(1_A * 1_A)(g) \leq |N^*(g)|$. Now we have:

$$|A|^2 = |A| + \sum_{g \in AA \setminus e} (1_A * 1_A)(g) \leq |A| + |G||N^*(g)|,$$

for some $g \in AA \setminus e$, which combined with the fact that $|A| \geq 2$ completes the proof.

Theorem 8 (Brauer-Fowler)

If G is a nonabelian finite simple group with an involution g such that $|N(g)| = n$, then G has at most $(2n^2)!$ elements.

We let A be the set of involutions of G . Since g is an involution, then so are all conjugates to g , i.e., if C is the conjugacy class of g , we get that $|C| = |G|/n$, hence $|A| \geq |G|/n$. We now assume that $|A| \geq 2$ (this turns out to always be the case, but we won't show this here). By applying the Lemma, we can find some $x \in AA \setminus e$ such that

$$|N^*(x)| \geq \frac{|A|^2}{2|G|} \geq \frac{|G|}{2n^2},$$

that is, the index $k = [G : N^*(x)] \leq 2n^2$.

We now prove that $N^*(x)$ is a proper subgroup. We look at two possible cases. If x is itself an involution, then $N^*(x) = N(x) = G$, which would imply that x commutes with every element in G . This in turn would imply that $\langle x \rangle = \{e, x\}$ is a normal subgroup of G , a contradiction.

If x in turn is not an involution, then $N(x)$ is a proper subgroup of $N^*(x)$. In particular, it would be a subgroup of index two, which is always normal, and as $N^*(x) = G$, this is again a contradiction. Thus, $N^*(x)$ is a proper subgroup of G .

Now consider the action of G on the left-cosets of $N^*(x)$ via left-multiplication. The kernel of this action is contained in H and is a normal subgroup of G . Since H is proper, this implies that this kernel must be trivial, i.e., G is isomorphic to some subgroup of the symmetric group on the cosets of $N^*(x)$, which consists of precisely k elements. This implies that

$$|G| \leq |S_k| = |k!| \leq (2n^2)!,$$

as desired.

Classification of Finite Simple Groups

- The Brauer-Fowler theorem gave the starting point for a program to classify all finite simple groups.
- One problem remained: groups of odd order don't have involutions, so what about finite simple groups of odd order?

Theorem 9 (Feit-Thompson)

All finite groups of odd order are solvable. Consequently, there are no nonabelian finite simple groups of odd order.

- Janko used this technique to find new simple groups.
- Many more finite simple groups are constructed this way.
- Although the CFSG eventually required more sophisticated methods, the Brauer-Fowler theorem was a fundamental starting step.

The Periodic Table Of Finite Simple Groups

B, C, G_2 1 1		Dynkin Diagrams of Simple Lie Algebras														C_2	
$A_1(4), A_1(5)$ A_5 60 168	$A_1(2)$ $A_1(7)$ 168											${}^2A_1(4)$ $B_2(3)$ 25 920	$C_3(3)$ $C_3(5)$ 228 500 690 000 000	$D_4(2)$ $D_4(3)$ 174 182 400	${}^2D_4(2^2)$ ${}^2D_4(3^2)$ 197 496 720	$G_2(2)'$ ${}^2A_2(9)$ 6 040	C_3 3
$A_1(8), B_3(2)$ A_8 360 504	${}^2G_2(3)'$ $A_1(8)$ 504											$B_2(4)$ 979 200	$C_3(5)$ 690 000 000	$D_4(3)$ 4 932 179 816 000	${}^2D_4(3^2)$ 31 151 946 415 520	${}^2A_2(16)$ 62 480	C_5 5
A_7 2 520	$A_1(11)$ 660	$E_6(2)$ 20 848 976 322	$E_7(2)$ 10 424 496	$E_8(2)$ 5 112 228	$F_4(2)$ 4 245 496	$G_2(3)$ 211 341 312	${}^3D_4(2^3)$ 75 302 479 683	${}^2E_6(2^2)$ 71 813 190 300	${}^2B_2(2^3)$ 29 120	${}^2F_4(2)'$ 17 971 200	${}^2C_2(3^3)$ 10 675 448 472	$B_3(2)$ 1 651 520	$C_4(3)$ 467 946 756	$D_5(2)$ 13 699 299 940 800	${}^2D_5(2^2)$ 31 813 379 536 000	${}^2A_2(25)$ 126 000	C_7 7
$A_1(2)$ A_8 20 160	$A_1(13)$ 1 092	$E_6(3)$ 1 774 448 792 314	$E_7(3)$ 871 048 791 608	$E_8(3)$ 427 048 791 608	$F_4(3)$ 5 744 448 792 314	$G_2(4)$ 4 711 048 791 608	${}^3D_4(3^3)$ 20 968 813 366 912	${}^2E_6(3^2)$ 1 774 448 792 314	${}^2B_2(2^5)$ 32 537 000	${}^2F_4(3^2)$ 244 968 002 690	${}^2C_2(3^5)$ 40 823 487	$B_2(5)$ 4 600 000	$C_3(7)$ 646 191 630	$D_4(5)$ 8 911 506 000	${}^2D_4(4^2)$ 47 306 871	${}^2A_3(9)$ 3 265 920	C_{11} 11
A_9 181 440	$A_1(17)$ 2 448	$E_6(4)$ 10 424 496	$E_7(4)$ 5 112 228	$E_8(4)$ 2 556 114	$F_4(4)$ 1 042 512	$G_2(5)$ 4 642 796 160	${}^3D_4(4^3)$ 16 962 560	${}^2E_6(4^2)$ 4 642 796 160	${}^2B_2(2^7)$ 31 083 363 400	${}^2F_4(4^2)$ 238 188 000 264	${}^2C_2(3^7)$ 312 348 132 632	$B_2(7)$ 138 297 600	$C_3(9)$ 499 984 800	$D_5(3)$ 3 289 517 769	${}^2D_4(5^2)$ 943 385 139 200	${}^2A_2(64)$ 800 000 000	C_{13} 13
A_n $\frac{n!}{2}$	$A_n(q)$ $\frac{q^n - 1}{q - 1}$	$E_6(q)$ $\frac{q^6 - 1}{q - 1}$	$E_7(q)$ $\frac{q^7 - 1}{q - 1}$	$E_8(q)$ $\frac{q^8 - 1}{q - 1}$	$F_4(q)$ $\frac{q^4 - 1}{q - 1}$	$G_2(q)$ $\frac{q^2 - 1}{q - 1}$	${}^3D_4(q^3)$ $\frac{q^4 - 1}{q - 1}$	${}^2E_6(q^2)$ $\frac{q^4 - 1}{q - 1}$	${}^2B_2(2^{n+1})$ $\frac{q^{n+1} - 1}{q - 1}$	${}^2F_4(2^{n+1})$ $\frac{q^{n+1} - 1}{q - 1}$	${}^2C_2(3^{n+1})$ $\frac{q^{n+1} - 1}{q - 1}$	$B_n(q)$ $\frac{q^n - 1}{q - 1}$	$C_n(q)$ $\frac{q^n - 1}{q - 1}$	$D_n(q)$ $\frac{q^n - 1}{q - 1}$	${}^2D_n(q^2)$ $\frac{q^n - 1}{q - 1}$	${}^2A_n(q^2)$ $\frac{q^n - 1}{q - 1}$	C_p p

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Bee Groups and Tits Group*
- Sporadic Groups
- Cyclic Groups

Alternates*
Symbol
Order!

M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	$J(1), J(11)$	HI	HIM	I_4	HS	McL	He	Ru
7 920	95 040	443 520	10 200 960	244 823 040	175 560	648 800	10 232 960	86 775 971 888 677 922 800	41 352 000	898 128 000	4 000 367 200	140 954 344 000

Sz	$O'N$	Co_3	Co_2	Co_1	F_4, D	HN	Ly	F_4, E	Th	F_{22}	F_{23}	F_{24}^*	B	M
440 345 897 600	446 815 903 423	499 756 436 800	42 965 823 312 000	4 137 766 865 562 960 800	273 000 912 000 000	808 600 000	51 763 176 808 600 000	90 183 960 807 672 000	44 561 716 836 800	4 888 476 473 203 693 800	1 230 265 709 196 943 721 292 800	4 789 864 000 1 000 000 000 000	4 789 864 000 1 000 000 000 000	4 789 864 000 1 000 000 000 000

*The group ${}^2F_4(2)'$ is not a group of Lie type, but is the index 2 commensurable subgroup of ${}^2F_4(2)$. It is usually given hexavalent Lie type notation.


The groups starting on the second row are the classical groups. The sporadic groups given are identified by the number of fixed points.

*Fixed simple groups are determined by their order with the following exception:
 ${}^2F_4(2)'$ and ${}^2F_4(2)$ for $q = 2$, $n = 2$.
 A_6 for $A_6(2)$ and $A_6(3)$ of order 2016.


Copyright © 2004 from Andran.

References

3264		1729
60 ¹⁶³	196884	24 ²⁴⁸

 **Richard E Borcherds**
@richarde.borcherds7998 · 80,8 mil inscritos · 466 videos
This is mostly mathematics lectures for graduate courses on algebraic geometry, commutative algebra, and number theory.

[Inscrever-se](#)

[Inicio](#) [Videos](#) [Cursos](#) [Playlists](#) [Posts](#) 

MATHEMATICAL SCIENCE LITERATURE LECTURE SERIES

“My life and times with the
sporadic simple groups”

Robert Griess University of Michigan

Robert Griess | My life and times with the sporadic simple groups



Harvard CMSA
26,2 mil inscritos

Inscriver-se

103



Compartilhar

Perguntar

Salvar



Questions?

henriquesoares@dcc.ufmg.br