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

Group theory Basics

Groups

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 $G/H := \{gH : g \in H\}$ 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* ($\varphi \in \mathrm{Hom}(G, H)$).
- If φ is bijective, then its called an *isomorphism*, and if $G = H$, an *automorphism*.
- If X is a set, we let $\mathrm{Sym}(X) := \{\sigma : X \mapsto X | \sigma \text{ is bijective}\}$ be its *symmetric group*.
- If $\varphi \in \mathrm{Hom}(G, H)$, then

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

Actions

- If G is a group and X is a set, then we say that G *acts* of X if there exists some $\varphi \in \mathrm{Hom}(G, \mathrm{Sym}(X))$, 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 $\varphi_L \in \mathrm{Hom}(G, \mathrm{Sym}(G))$ 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 of 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

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

  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

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

Jordan-Holder

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 $\mathrm{PSL}(n, q)(n \geq 2, q \geq 5)$.
- A_n is the *alternating* group of all even permutations. Proof of simplicity is by induction + analyzing conjugacy classes.
- $\mathrm{PSL}(n, q)$ is defined as the quotient of $\mathrm{SL}(n, q)$ ($n \times n$ matrices over $\mathbb{F}_q$ with determinant 1) by its center (diagonal matrices with determinant 1). Simplicity follows from Iwasawa's Lemma.

History

- 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.

History

- 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

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

Proof

First, note

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

Thus

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

Proof

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

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.

Proof

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 $k = [G : N^*(x)] \leq 2n^2$.

Proof

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.

Proof

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

CFSG

- 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)

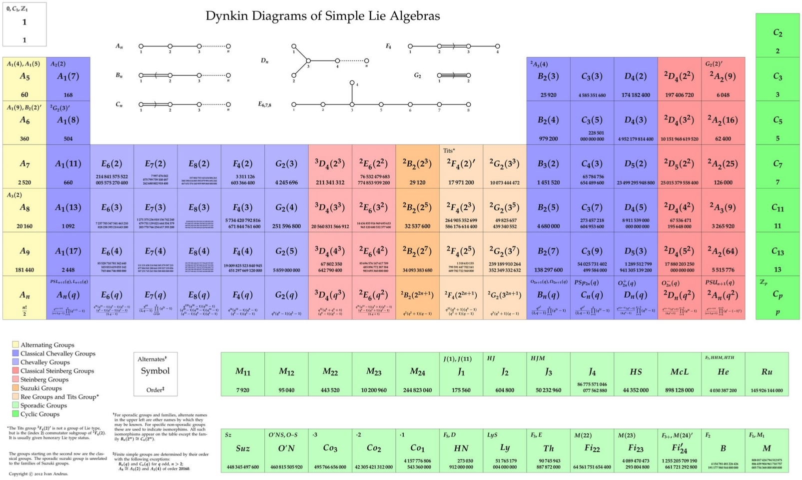
All finite groups of odd order are solvable. Consequently, there are no nonabelian finite simple groups of odd order.

CFSG

- 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.

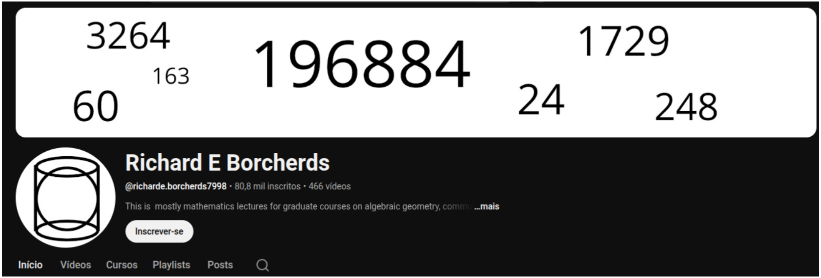
Table

The Periodic Table Of Finite Simple Groups

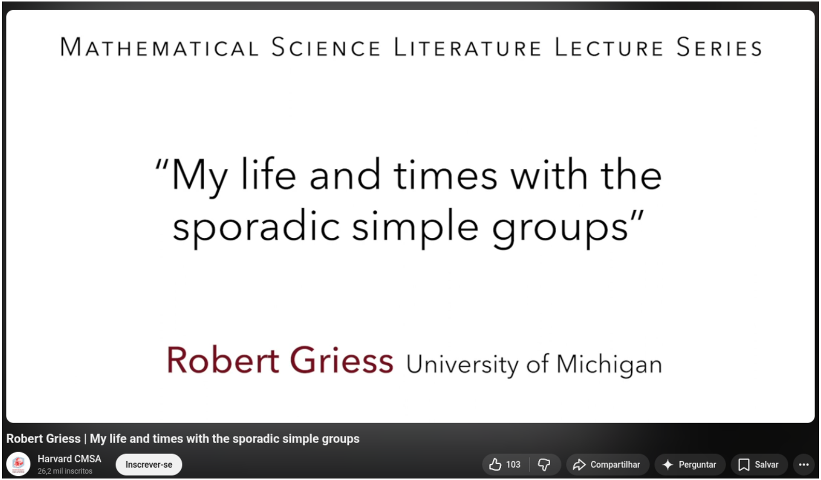


References

Borcherds


3264
163
60
196884
1729
24
248
Richard E Borcherds
@richarde.borcherds7998 • 80,8 mil inscritos • 466 vídeos
This is mostly mathematics lectures for graduate courses on algebraic geometry, commu ...mais
Inscrever-se
Início
Vídeos
Cursos
Playlists
Posts

Griess


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
Inscrever-se
103
Compartilhar
Perguntar
Salvar

Questions?

henriquesoares@dcc.ufmg.br