M2R: Simple Groups

Supervisor: Prof. Martin Liebeck
Thomas Stobart (CID: 02204762),
Hongyu Wang (CID: 02201132),
Tianyu Wang (CID: 02241944),
Zicheng Yang (CID: 02236925).

May-June 2024

1 Introduction

1.1 Preliminaries

Definition 1.1. A **simple group** is a group with exactly two normal subgroups.

Since every group G has $\{e\}$ and G itself as normal subgroups, we can also say that a nontrivial simple group has no nontrivial proper normal subgroups or that a nontrivial simple group has only $\{e\}$ and itself as quotients.

Example 1.2

The following are simple groups:

1. C_3, the cyclic group on 3 elements.
2. A_5, the alternating group on 5 elements.
3. $\mathrm{GL}_3(2)$, the group of invertible 3×3 matrices over $\mathbb{F}_2$.

The following are not simple groups:

1. $\{e\}$, which has only one normal subgroup, itself.
2. C_6, which has C_2 and C_3 as proper nontrivial normal subgroups
3. $\mathbb{Z}$, which has the even integers $2\mathbb{Z}$ as a proper nontrivial normal subgroup.

To study the properties of simple groups, we will need some basic results from group theory:

Theorem 1.3 (First Isomorphism Theorem)

Let G, H be groups and let $\phi : G \to H$ be a group homomorphism. Then:

1. $\ker(\phi)$ is a normal subgroup of G,
2. $\mathrm{Im}(\phi)$ is a subgroup of H,
3. $\mathrm{Im}(\phi) \cong G/\ker(\phi)$.

The proof of the Isomorphism Theorem can be found in many Algebra textbooks, such as Isaacs (1994).

In a group G that is not simple, there is a nontrivial proper normal subgroup N, and correspondingly by the first isomorphism theorem, there is a short exact sequence

$$1 \to N \to G \to G/N \to 1$$

and we say that G is an extension of G/N by N, and furthermore, this is the only way in which group extensions can occur; if we have the short exact sequence

$$1 \to N \xrightarrow{\phi} G \xrightarrow{\psi} Q \to 1$$

by exactness we see that $\phi(N)$ is normal in G since it is the kernel of ψ and as ψ is surjective that $G/\phi(N) \cong Q$ by the first isomorphism theorem. In this sense, simple groups are indeed the simplest nontrivial groups – they cannot be written as an extension of smaller nontrivial groups in any way. Simple groups are analogous to the prime numbers of group theory in this way.

As occurs with the prime numbers, or the classification of finitely generated abelian groups, we might hope that all finite groups could be written uniquely as a product of simple groups. This is not the case as not all group extensions are products (C_4 can be written as an extension of C_2 by C_2, but is not isomorphic to $C_2 \times C_2$ or even a semidirect product). However, a relatively strong result is still possible, which we will discuss in a later section.

Let G be a finite group and H be a subgroup of G. Turning the problem to classify finite simple groups G, the most straightforward way is to produce normal subgroups H of G.

Recall Lagrange's Theorem, which relates the order of a group and the order of its subgroups.

Theorem 1.4 (Lagrange's Theorem)
Let G be a finite group and H be a subgroup of G. Let $[G : H]$ be the index of H in G, which is the number of left cosets of H in G. Then $|H|$ divides $|G|$ and $|G| = [G : H] \cdot |H|$.

Proof. Decompose G into left cosets of H, say if G can be written as $Hg_1 \cup Hg_2 \cup \cdots \cup Hg_n$. Then $\forall i \in \{1, 2, \cdots, n\}$, consider a map $f_i : H \to Hg_i := h \mapsto hg_i$. It is easy to verify that f_i is a bijection. Therefore, $|H| = |Hg_i|$. Since G is the union of all left cosets of H, which are all pairwise disjoint, we have $|G| = n \cdot |H|$, where n is the number of left cosets of H in G. □

The key part of the proof for Lagrange's Theorem is to decompose G into left cosets of H and prove that each left coset has the same size as the other, which is the cardinality of H.

On the other hand, as an application, the problem of classifying subgroups of a group G turns into considering the prime factorization of the order of G.

1.1.1 Sylow's theorem

Since finding all the normal subgroups of a group G is much harder than finding all the subgroups of G, the idea is to find a prime number p that divides the order of G and then find normal subgroups with the order as a power of p. Hence, we introduce a fundamental theorem of finite groups, Sylow's theorem, which was proposed by Norwegian mathematician Ludwig Sylow in 1872. The main point of Sylow's theorem is the partial converse of Lagrange's Theorem, which asserts that if m is a power of a prime number and divides the order of G, then G must have a subgroup of order m.

Definition 1.5 (Sylow p-subgroups)**.** Let G be a finite group and p be a prime number. We define a **Sylow p-subgroup** of G is a subgroup $H \leq G$ such that $\left|H\right| = p^\alpha$ with $\left|G\right| = p^\alpha m$ for some $\alpha \geq 1$ and $p \nmid m$. The set of all Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$.

Remark 1.6 — A Sylow p-subgroup of G is a subgroup of G whose order is the highest power of p that divides the order of G and the existence of Sylow p-subgroups is guaranteed by the Sylow's theorem in the following.

Theorem 1.7 (Sylow's Theorem)

Let G be a finite group and p be a prime number. If $\left|G\right| = p^\alpha m$ for some $\alpha \geq 1$ and $m \geq 1$ with $p \nmid m$, then the following statements hold:

1. There exists at least one Sylow p-subgroup of G with order p^α. In other words, $\mathrm{Syl}_p(G) \neq \varnothing$.
2. $\forall H, K \in \mathrm{Syl}_p(G)$, then there exists $g \in G$ such that $H = gKg^{-1}$. In other words, any two Sylow p-subgroups of G are conjugate.
3. If we denote the number of Sylow p-subgroups of G by $n_p(G)$, then the following holds:
   (a) $n_p(G) \equiv 1 \mod p$.
   (b) $n_p(G) \mid m$.

As Sylow's theorem is just a tool that we already know to be true to help us classify finite simple groups, we will not prove it here. A proof of Sylow's theorem can be found in Isaacs (1994).

Remark 1.8 — Intuitively, Sylow's theorem says the following:

- The first statement of Sylow's theorem is a strengthening of Cauchy's theorem on the existence of an element of order p.
- The second statement shows that $\mathrm{Syl}_p(G)$ is a single conjugacy class in G.
- The third statement gives us a way to count the number of Sylow $p-$subgroups of G by using number theoretic information. Hence, it is also called Sylow's counting theorem.

1.1.2 Group actions

Besides, we will also need to use the concept of group actions to classify the finite simple groups. The idea behind the theory of group actions is to regain the advantages of studying with the symmetric group other than the abstract group G itself.

Definition 1.9 (Group action)**.** Let G be a group and Ω be any non-empty set. We define a **group action of G on Ω** is a map $\cdot : G \times \Omega \to \Omega$ such that the following two properties hold:

1. $\forall \alpha \in \Omega, \alpha \cdot e = \alpha$.
2. $\forall g, h \in G, \forall \alpha \in \Omega, (\alpha \cdot g) \cdot h = \alpha \cdot (gh)$.

Example 1.10

The following are examples of group actions.

- the most useful actions of the finite group are the actions on itself, let G be any finite group and act on itself by $\cdot : G \times G \to G := (g, h) \mapsto gh$. This is a group action since the identity element e acts as the identity map on G and the group multiplication is associative.
- Consider the general linear group $\mathrm{GL}_n(\mathbb{R})$ acts on n-dimensional Euclidean space $\mathbb{R}^n$ by matrix-vector multiplication. That is, $\cdot : \mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n := (A, v) \mapsto Av$. This is a group action since the identity matrix I_n acts as the identity map on $\mathbb{R}^n$ and the matrix multiplication is associative.
- Consider the general linear group $\mathrm{GL}_n(\mathbb{R})$ acts on the set of all $n \times n$ matrices $\mathrm{M}_n(\mathbb{R})$ by conjugation. That is, $\cdot : \mathrm{GL}_n(\mathbb{R}) \times \mathrm{M}_n(\mathbb{R}) \to \mathrm{M}_n(\mathbb{R}) := (A, B) \mapsto ABA^{-1}$. This is a group action since the identity matrix I_n acts as the identity map on $\mathrm{M}_n(\mathbb{R})$ and the matrix multiplication is associative.
- Let S be the set of all triangles in $\mathbb{R}^2$ and let $G_1 := \{v \mapsto Av + b : A \in \mathrm{GL}_2(\mathbb{R}), b \in \mathbb{R}^2\}$ and $G_2 := \{v \mapsto Av : A \in \mathrm{O}_2(\mathbb{R})\}$. Then G_1 and G_2 act on S by affine transformations and isometries respectively.

1.2 Composition series and the Jordan-Hölder theorem

Definition 1.11. A **composition series** for a group G is a sequence of groups

$$\{e\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_{k-1} \triangleleft H_k \triangleleft G$$

such that each quotient group H_{i+1}/H_i is simple (or equivalently, H_i is a maximal normal subgroup in H_{i+1}). The groups H_{i+1}/H_i are called **composition factors**.

Example 1.12

Consider the group S_4. We have the composition series

$$\{e\} \triangleleft C_2 \triangleleft V \triangleleft A_4 \triangleleft S_4$$

where V is the Klein four-group. The composition factors are $C_2/\{e\} \cong C_2$, $V/C_2 \cong C_2$, $A_4/V \cong C_3$ and $S_4/A_4 \cong C_2$.

For finite groups, composition series always exist but are not unique, as for many groups there are multiple choices of maximal normal subgroup that could be taken. For example

$$\{e\} \triangleleft C_2 \triangleleft C_4 \triangleleft C_{12}$$

and

$$\{e\} \triangleleft C_3 \triangleleft C_6 \triangleleft C_{12}$$

are both composition series for C_{12}. However, we have the following result which shows that any two composition series are in a certain sense equivalent.

Theorem 1.13 (Jordan-Hölder)

Let G be a finite group. Any two composition series for G have the same length, and the same list of composition factors, up to permutation and isomorphism.

Example 1.14

For

$$\{e\} \triangleleft C_2 \triangleleft C_4 \triangleleft C_{12}$$

and

$$\{e\} \triangleleft C_3 \triangleleft C_6 \triangleleft C_{12}$$

the composition series has length 4, and the list of composition factors is C_2, C_2, C_3.

Proof. We proceed by induction on $|G|$. The base case $|G| = 1$ is trivial, so let $|G| = n > 1$. Fix two composition series

$$\{e\} = P_0 \triangleleft P_1 \triangleleft \cdots \triangleleft P_{k-1} \triangleleft P_k = G$$

$$\{e\} = Q_0 \triangleleft Q_1 \triangleleft \cdots \triangleleft Q_{\ell-1} \triangleleft Q_\ell = G$$

If $P_{k-1} \cong Q_{\ell-1}$, then we're done by the inductive hypothesis since $|P_{k-1}| = |Q_{\ell-1}| < n$. Otherwise P_{k-1} and $Q_{\ell-1}$ are distinct.

Now consider the group $R = P_{k-1} \cap Q_{\ell-1}$. We can find a composition series

$$\{e\} = R_0 \triangleleft \cdots \triangleleft R_{m-1} \triangleleft R_m = R$$

and then by induction:

$$P_0 \triangleleft \cdots \triangleleft P_{k-2} \triangleleft P_{k-1}$$

and

$$R_0 \triangleleft \cdots \triangleleft R_{m-1} \triangleleft R \triangleleft P_{k-1}$$

have the same length and the same composition factors. The same reasoning applies to composition series for $Q_{\ell-1}$, and so $k-1 = m+1 = \ell-1$ and $k = \ell$.

Furthermore, the following lists of composition factors are the same, up to isomorphism and permutation:

$$P_1/P_0, \cdots, P_{k-1}/P_{k-2}$$

$$R_1/R_0, \cdots, R/R_{m-1}, P_{k-1}/R$$

and the same is true for the corresponding composition series for $Q_{\ell-1}$. Finally the four lists of composition factors

$$P_1/P_0, \cdots, P_{k-1}/P_{k-2}, G/P_{k-1}$$

$$R_1/R_0, \cdots, R/R_{m-1}, P_{k-1}/R, G/P_{k-1}$$

$$R_1/R_0, \cdots, R/R_{m-1}, Q_{\ell-1}/R, G/Q_{\ell-1}$$

$$Q_1/P_0, \cdots, Q_{\ell-1}/Q_{\ell-2}, G/Q_{\ell-1}$$

are the same since all but the last two entries are the same from above, and $P_{k-1}/R \cong G/Q_{\ell-1}$ and $Q_{\ell-1}/R \cong G/P_{k-1}$ both by the second isomorphism theorem. This completes the proof. □

Remark 1.15 — The Jordan-Hölder theorem only applies to finite groups (for example, $\mathbb{Z}$ does not have a composition series). As such most work on simple groups focuses on the finite simple groups. However, there are infinite simple groups, such as A_∞, the group of even finitely supported permutations of $\mathbb{N}$. In particular, if A_∞ had a proper nontrivial normal subgroup N, then $N \cap A_n$ is nontrivial for sufficiently large n, and is normal in A_n, which contradicts simplicity of A_n.

1.3 Character theory

It will be useful to have stated and discussed some results from character theory which will be used later in this report. Proofs of all these results can be found in James & Liebeck (2001).

Definition 1.16. A **representation** of a group G is a homomorphism $G \to \mathrm{GL}(V)$ where V is a vector space over a field k.

Definition 1.17. A **character** of a group G is a function $G \to k$ of the form $\chi_\rho : g \mapsto \mathrm{Tr}(\rho(g))$, where ρ is a representation of G.

Definition 1.18. A character χ_ρ is called **irreducible** if ρ is an irreducible representation of G (that is if ρ does not contain any proper subrepresentations).

Theorem 1.19

Characters are constant on conjugacy classes (that is, they are class functions), and furthermore, the set of characters of G form a basis for all class-functions $G \to k$.

From now on, we fix $k = \mathbb{C}$ and do not consider characters in characteristic $p > 0$.

Theorem 1.20

There is a natural inner product on the space of class functions given by:

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}.$$

Furthermore, with respect to this inner product, the irreducible characters of G form an orthonormal basis for the space of class functions.

We also have another orthogonality relation, this time summing along characters:

Theorem 1.21 (Column orthogonality relations)

$$\sum_{\chi} \chi(g)\overline{\chi(h)} = \begin{cases} |C_G(g)| & g, h \text{ are conjugate} \\ 0 & \text{otherwise} \end{cases}$$

where the sum is over all irreducible characters of G.

Example 1.22

Here is the character table for D_8, in which it can be seen that the rows and columns are orthogonal as described above.

	$\{e\}$	$\{r^2\}$	$\{r, r^3\}$	$\{s, r^2s\}$	$\{rs, r^3s\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Definition 1.23. A **generalised** character is a class function which is a sum or difference of characters. That is, a class function of the form

$$\sum_{i=1}^{k} a_i \chi_{\rho_i}$$

where $a_i \in \mathbb{Z}$.

Of course, the inner product on the space of class functions induces a norm, and since generalised characters will have $\langle \chi, \chi \rangle \in \mathbb{N}$, small values of the norm give quite strong information about a generalised character. In particular

Theorem 1.24 (Generalised characters of small norm)

Let χ be a generalised character. Then:

1. $\langle \chi, \chi \rangle = 1$ if and only if $\chi = \varepsilon\chi_\rho$ with $\varepsilon \in \{-1, 1\}$ and ρ irreducible. If $\chi(e) > 0$, then $\varepsilon = 1$.
2. $\langle \chi, \chi \rangle = 2$ if and only if $\chi = \varepsilon_1\chi_{\rho_1} - \varepsilon_2\chi_{\rho_2}$ with $\varepsilon_i \in \{-1, 1\}$ and ρ_i distinct irreducibles. if $\chi(e) = 0$, then $\varepsilon_1 = \varepsilon_2$.
3. $\langle \chi, \chi \rangle = 3$ if and only if $\chi = \varepsilon_1\chi_{\rho_1} + \varepsilon_2\chi_{\rho_2} + \varepsilon_3\chi_{\rho_3}$ with $\varepsilon_i \in \{-1, 1\}$.

Character theory also gives us a way to control the combinatorics of conjugacy classes of G. The precise statement is:

Theorem 1.25 (Class algebra constants)

Let $\{C_i\}_{i=1}^n$ be a partition of G into conjugacy classes. Then, the number of pairs (a, b) with $a \in C_i$, $b \in C_j$ and $ab = c \in C_k$ is given by:

$$\frac{|G|}{|C_G(a)||C_G(b)|} \sum_{\chi} \frac{\chi(a)\chi(b)\overline{\chi(c)}}{\chi(e)}$$

where the sum is over all irreducible characters of G.

Finally, we want to consider how the characters of a group are related to the characters of subgroups.

Definition 1.26 (Restriction of a character)**.** Let χ be a character of G, and let H be a subgroup of G. Then $\mathrm{Res}^H_G \chi$ given by $h \mapsto \chi(h)$ is a character of H.

On the other hand, it is not immediately clear how to go the other way, from characters on a subgroup H of G to characters on G. However, a result is possible. Notice that Res_G^H gives a linear map from the space of class functions on G to the space of class functions on H, and recall that linear maps between inner product spaces have adjoints.

Theorem 1.27 (Frobenius reciprocity)
Let χ be a character of H which is a subgroup of G. Then there is a class function $\mathrm{Ind}_H^G \chi$ such that

$$\left\langle \mathrm{Ind}_H^G \chi, \psi \right\rangle = \left\langle \chi, \mathrm{Res}_G^H \psi \right\rangle.$$

Furthermore, this class function is a character, and we have that

$$\mathrm{Ind}_H^G \chi(x) = \frac{1}{|H|} \sum_{g \in G} \dot{\chi}(g^{-1} x g)$$

where we extend χ to $\dot{\chi}$ on G by $\dot{\chi}(g) = 0$ for $g \in G \setminus H$.

2 Examples of simple groups

In this section, we will discuss some examples of simple groups.

2.1 Alternating groups

Lemma 2.1
In S_n, the alternating group A_n is a normal subgroup of index 2.

Proof. A_n is the kernel of the sign homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$. It is thus a normal subgroup. □

Lemma 2.2
3-cycles generate A_n.

Proof. A 3-cycle is a permutation that only permutes three elements and leaves the others fixed. For example, in S_5, (1 2 3) is a 3-cycle, which maps 1 to 2, 2 to 3, and 3 to 1, leaving other elements unchanged.

To show that 3-cycles generate A_n, we need to prove that any even permutation can be expressed as a product of 3-cycles. Consider an even permutation $\sigma \in A_n$, which can be written as a product of an even number of 2-cycles.

Suppose σ can be written as a product of an even number of 2-cycles:

$$\sigma = (\alpha_1\ \beta_1)(\alpha_2\ \beta_2) \cdots (\alpha_{2k-1}\ \beta_{2k-1})(\alpha_{2k}\ \beta_{2k})$$

We can decompose any pair of 2-cycles into a product of 3-cycles. Note that for any three distinct elements a, b, c, d, we have:

$$(a\ b)(c\ d) = (d\ a\ c)(a\ b\ d)$$

Therefore, we can write any 2-cycles $(\alpha_i\ \beta_i)$, $(\alpha_{i+1}\ \beta_{i+1})$ as a product of two 3-cycles. Since an even permutation is a product of an even number of 2-cycles, we can express the entire permutation as a product of 3-cycles.

Hence, all even permutations can be written as a product of 3-cycles, which proves that 3-cycles generate A_n.

□

Theorem 2.3

The alternating group A_n is simple for $n \geq 5$.

Proof. To prove A_n is simple for $n \geq 5$, we will show that any non-trivial normal subgroup of A_n must be A_n itself.

Consider any non-trivial normal subgroup N of A_n. Since N is normal in A_n, it must be a union of conjugacy classes within A_n. One important observation is that the 3-cycles in A_n are all conjugate to each other. For $n \geq 5$, these 3-cycles generate A_n.

If N contains any 3-cycle, it must contain all 3-cycles because they are conjugate in A_n. As 3-cycles generate A_n when $n \geq 5$, the subgroup N must contain all elements of A_n, implying $N = A_n$.

Therefore, the only non-trivial normal subgroup of A_n is A_n itself, proving that A_n is simple for $n \geq 5$. □

2.2 The projective special linear group

We will prove that the projective special linear group $\mathrm{PSL}_2(q)$ is simple for $q \neq 2, 3$. A group is simple if it has no non-trivial normal subgroups.

Definition 2.4. The projective special linear group $\mathrm{PSL}_2(q)$ is defined as the quotient of the special linear group $\mathrm{SL}_2(q)$ by its centre. Specifically,

$$\mathrm{PSL}_2(q) = \mathrm{SL}_2(q)/Z(\mathrm{SL}_2(q)),$$

where $\mathrm{SL}_2(q)$ consists of 2×2 matrices with determinant 1 over the finite field $\mathbb{F}_q$, and $Z(\mathrm{SL}_2(q))$ is the centre of $\mathrm{SL}_2(q)$, consisting of scalar matrices with determinant 1.

Proving that this group is simple is a very complex problem, so we need to introduce many definitions and theorems to assist in the proof. Some proofs can be found in the article Conrad (2020).

2.2.1 Doubly transitive actions and Iwasawa's criterion

Definition 2.5. In group theory, a group action is said to be **doubly transitive** (or **2-transitive**) if it satisfies the following condition:

A group G acts on a set X in a doubly transitive manner if for any two pairs of elements (x_1, x_2) and (y_1, y_2) in X where $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists an element $g \in G$ such that:

$$g \cdot x_1 = y_1 \quad \text{and} \quad g \cdot x_2 = y_2.$$

This means that the group G can map any ordered pair of distinct elements to any other ordered pair of distinct elements through its action on the set X.

Example 2.6

A classic example of a doubly transitive group action is the action of the symmetric group S_n on the set $\{1, 2, \ldots, n\}$. For any $n \geq 2$, S_n acts doubly transitively on this set because any pair of distinct elements can be mapped to any other pair of distinct elements by some permutation in S_n.

Definition 2.7. A **maximal subgroup** is a proper subgroup contained in no other proper subgroup.

Lemma 2.8

If G acts doubly transitively on X then the stabilizer subgroup of each point in X is a maximal subgroup of G.

Proof. We define the stabilizer subgroup as H_x. For $g, g' \in G$ such that $g, g' \notin H_x$, we will show $g' \in H_x g H_x$. Both gx and $g'x$ are not x, so by double transitivity with the pairs (x, gx) and $(x, g'x)$ there is some $g'' \in G$ such that

$$g''x = x \quad \text{and} \quad g''(gx) = g'x.$$

So $g'' \in H_x$, and this implies $g' \in hgH_x \subseteq H_xgH_x$. Therefore we have $G = H_x \cup H_xgH_x$ and we want to prove H_x is a maximal subgroup of G.

The group H_x is not all of G because $|X| \geq 2$. Choose H as a subgroup of G strictly containing H_x and pick $g \in H \setminus H_x$. Both H_x and H_xgH_x are in H, so $G \subseteq H$. Thus $H = G$.

This concludes the proof that if G acts doubly transitively on X, then the stabilizer subgroup of each point in X is a maximal subgroup of G. □

Lemma 2.9

Suppose G acts doubly transitively on a set X. Any normal subgroup N acts on X either trivially or transitively.

Proof. Assume N does not act trivially on X. Then, there exists some $x \in X$ and some $n \in N \setminus \{1\}$ such that $n \cdot x \neq x$. We need to show that N acts transitively on X. Pick arbitrary y and y' in X with $y \neq y'$. By double transitivity, there exists $g \in G$ such that

$$g \cdot x = y \quad \text{and} \quad g \cdot (n \cdot x) = y'.$$

Then,

$$y' = (gng^{-1}) \cdot (g \cdot x) = (gng^{-1}) \cdot y,$$

and $gng^{-1} \in N$ since N is normal in G. Thus, N acts transitively on X. □

Theorem 2.10 (Iwasawa)

Let G act doubly transitively on a set X. Assume the following:

1. For some $x \in X$, the group Stab_x has an abelian normal subgroup whose conjugate subgroups generate G.
2. $[G, G] = G$.

Then G/K is a simple group, where K is the kernel of the action of G on X.

Note: The kernel of an action is the kernel of the homomorphism $G \to \mathrm{Sym}(X)$; it consists of those g that act like the identity on X.

Proof. To show G/K is simple, we will show the only normal subgroups of G lying between K and G are K and G. Let $K \subseteq N \subseteq G$ with $N \triangleleft G$. Let $H = \mathrm{Stab}_x$, so H is a maximal subgroup of G (2.8). Since N is normal, $NH = \{nh : n \in N, h \in H\}$ is a subgroup of G, and it contains H, so by maximality either $NH = H$ or $NH = G$. By 2.9, N acts trivially or transitively on X.

If $NH = H$, then $N \subseteq H$, so N fixes x. Therefore, N does not act transitively on X, so N must act trivially on X, which implies $N \subseteq K$. Since $K \subseteq N$ by hypothesis, we have $N = K$.

Now suppose $NH = G$. Let U be the abelian normal subgroup of H in the hypothesis: its conjugate subgroups generate G. Since $U \triangleleft H$, $NU \subseteq NH = G$. Then for $g \in G$,

$$gUg^{-1} \subseteq g(NU)g^{-1} = NU,$$

which shows NU contains all the conjugate subgroups of U. By hypothesis, it follows that $NU = G$.

Thus,

$$G/N = (NU)/N \cong U/(N \cap U).$$

Since U is abelian, the isomorphism tells us that G/N is abelian, so

$$[G, G] \subseteq N.$$

Since $G = [G, G]$ by hypothesis, we have $N = G$.

This concludes the proof that G/K is simple. □

2.2.2 Simplicity of $\mathrm{PSL}_2(q)$

Lemma 2.11

The action of $\mathrm{SL}_2(\mathbb{F}_q)$ on the linear subspaces of $\mathbb{F}_q^2$ is doubly transitive.

Proof. First, we show that $\mathrm{SL}_2(\mathbb{F}_q)$ acts transitively on the 1-dimensional subspaces of V.

Let U and W be any two 1-dimensional subspaces of V. We can choose bases $\{u\}$ for U and $\{w\}$ for W. Since U and W are 1-dimensional, u and w are nonzero vectors in V.

Consider the matrices in $\mathrm{SL}_2(\mathbb{F}_q)$ that map u to w. Specifically, we can find $A \in \mathrm{SL}_2(\mathbb{F}_q)$ such that $Au = w$. This is possible because $\mathrm{SL}_2(\mathbb{F}_q)$ consists of all 2×2 matrices with determinant 1, and such matrices can map any nonzero vector to any other nonzero vector. Thus, the action is transitive.

Next, we show that the action is doubly transitive. We need to show that given any two pairs of distinct 1-dimensional subspaces (U_1, U_2) and (W_1, W_2) in V, there exists $A \in \mathrm{SL}_2(\mathbb{F}_q)$ such that $AU_1 = W_1$ and $AU_2 = W_2$.

Choose bases $\{u_1\}$ and $\{u_2\}$ for U_1 and U_2 respectively, and $\{w_1\}$ and $\{w_2\}$ for W_1 and W_2 respectively. We can extend $\{u_1, u_2\}$ and $\{w_1, w_2\}$ to bases for V.

Since U_1 and U_2 are distinct 1-dimensional subspaces, $\{u_1, u_2\}$ is a basis for V. Similarly, $\{w_1, w_2\}$ is a basis for V. There exists a unique $A \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $Au_1 = w_1$ and $Au_2 = w_2$. Since $\det(A) \neq 0$, we can scale A by $\frac{1}{\det(A)}$ to ensure that $\det(A) = 1$, thus $A \in \mathrm{SL}_2(\mathbb{F}_q)$.

Therefore, $\mathrm{SL}_2(\mathbb{F}_q)$ can map any pair of distinct 1-dimensional subspaces to any other pair of distinct 1-dimensional subspaces, proving that the action is doubly transitive.

□

Lemma 2.12

The kernel of the action of $\mathrm{SL}_2(\mathbb{F}_q)$ on the linear subspaces of $\mathbb{F}_q^2$ is the center of $\mathrm{SL}_2(\mathbb{F}_q)$.

Proof. Consider the action of $\mathrm{SL}_2(\mathbb{F}_q)$ on the 1-dimensional subspaces of $\mathbb{F}_q^2$. Let $V = \mathbb{F}_q^2$, and let $\mathbb{P}(V)$ denote the projective line, which consists of all 1-dimensional subspaces of V.

Step 1: Define the action

For any $g \in \mathrm{SL}_2(\mathbb{F}_q)$ and a 1-dimensional subspace $\langle v \rangle$ (spanned by a nonzero vector $v \in V$), the action is defined by

$$g \cdot \langle v \rangle = \langle gv \rangle.$$

Step 2: Identify the kernel of the action

The kernel of this action consists of all $g \in \mathrm{SL}_2(\mathbb{F}_q)$ such that $g \cdot \langle v \rangle = \langle v \rangle$ for all $\langle v \rangle \in \mathbb{P}(V)$. This means that gv is a scalar multiple of v for all nonzero $v \in V$:

$$gv = \lambda(v)v \quad \text{for some } \lambda(v) \in \mathbb{F}_q^*.$$

Step 3: Relate to the center of $\mathrm{SL}_2(\mathbb{F}_q)$

We claim that the kernel of this action is the centre $Z(\mathrm{SL}_2(\mathbb{F}_q))$, which consists of scalar matrices that are multiples of the identity matrix:

$$Z(\mathrm{SL}_2(\mathbb{F}_q)) = \left\{ \alpha I : \alpha \in \mathbb{F}_q^*, \alpha^2 = 1 \right\}.$$

Since $g \in \mathrm{SL}_2(\mathbb{F}_q)$ must have determinant 1, the scalar α must satisfy $\alpha^2 = 1$, implying $\alpha = \pm 1$.

Step 4: Prove the kernel is exactly $Z(\mathrm{SL}_2(\mathbb{F}_q))$

Let $g \in \mathrm{SL}_2(\mathbb{F}_q)$ be in the kernel. Then $gv = \lambda v$ for all $v \in V$. This means g must commute with every element of $\mathrm{SL}_2(\mathbb{F}_q)$, hence g is in the center of $\mathrm{SL}_2(\mathbb{F}_q)$. Therefore, $g = \pm I$, where I is the identity matrix.

Conversely, any element $\pm I$ clearly acts as the identity on the projective line since $(\pm I)v = \pm v$ for any $v \in V$, and both $\langle v \rangle = \langle \pm v \rangle$.

Thus, the kernel of the action is $\{I, -I\}$, which is exactly the center of $\mathrm{SL}_2(\mathbb{F}_q)$. □

Lemma 2.13

The subgroup U and its conjugates generate $\mathrm{SL}_2(\mathbb{F}_q)$. More precisely, each matrix of the form

$$\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$$

is conjugate to a matrix of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

and every element of $\mathrm{SL}_2(\mathbb{F}_q)$. is the product of at most 4 elements of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}.$$

Lemma 2.14

If $|\mathbb{F}_q| \geq 4$, then $[\mathrm{SL}_2(\mathbb{F}_q), \mathrm{SL}_2(\mathbb{F}_q)] = \mathrm{SL}_2(\mathbb{F}_q)$.

The above two lemmas exist to satisfy the conditions for the use of Iwasawa's theorem, and their proofs can be completed using similar matrix transformations.

Theorem 2.15

The projective special linear group $\mathrm{SL}_2(\mathbb{F}_q)$ is simple for $q \neq 2, 3$.

Proof. Through the previous four lemmas, $\mathrm{SL}_2(\mathbb{F}_q)$ satisfies the conditions of Iwasawa's theorem, and by 2.12, we know the kernel of $\mathrm{SL}_2(\mathbb{F}_q)$ is similar as the centre of it. So we can complete the proof with the definition of $\mathrm{SL}_2(\mathbb{F}_q)$. □

Now, we will discuss the special cases when $q = 2, 3$. There is a theorem about the order of $\mathrm{PSL}_2(q)$ which the proof can be found in Robinson (1996).

Theorem 2.16

The order of the projective special linear group $\mathrm{PSL}(n, q)$ is given by:

$$|\mathrm{PSL}(n, q)| = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{(q - 1) \cdot d},$$

where $d = \gcd(n, q - 1)$.

Hence, The groups $\mathrm{PSL}_2(2)$ and $\mathrm{PSL}_2(3)$ have orders 6 and 12 respectively, there exist no simple groups of these order obviously. Moreover, $\mathrm{PSL}_2(3) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$. Thus $\mathrm{PSL}_2(2)$ and $\mathrm{PSL}_2(3)$ are not simple.

3 Classification of finite simple groups

One of the major mathematical projects of the 20th century was to classify finite simple groups. We give the statement of the final classification here, following the notation used in Wilson (2009).

Theorem 3.1 (Classification of finite simple groups)

Let G be a finite simple group, then G is isomorphic to one of:

1. A cyclic group C_p, for p prime.
2. An alternating group A_n for $n \geq 5$.
3. A classical group:
   (a) $\mathrm{PSL}_n(q)$, $n \geq 2$ except $\mathrm{PSL}_2(2)$ and $\mathrm{PSL}_2(3)$.
   (b) $\mathrm{PSU}_n(q)$, $n \geq 3$ except $\mathrm{PSU}_3(2)$.
   (c) $\mathrm{PSp}_{2n}(q)$, $n \geq 2$ except $\mathrm{PSp}_4(2)$.
   (d) $\mathrm{P}\Omega_{2n+1}(q)$, $n \geq 3$, q odd.
   (e) $\mathrm{P}\Omega^+_{2n}(q)$, $n \geq 4$.
   (f) $\mathrm{P}\Omega^-_{2n}(q)$, $n \geq 4$.

   where $q = p^k$ for p prime
4. An exceptional group of Lie type

$$G_2(q), F_4(q), E_6(q) {}^2E_6(q), {}^3D_4(q), E_7(q), E_8(q)$$

   for $q = p^k$ except $G_2(2)$, p prime or

$${}^2B_2(2^{2n+1}), {}^2G_2(3^{2n+1}), {}^2F_4(2^{2n+1})$$

   for $n \geq 1$ or the Tits group ${}^2F_4(2)'$.
5. One of 26 sporadic groups:
   (a) A Mathieu group $\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}$.
   (b) A Leech lattice group $\mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{McL}, \mathrm{HS}, \mathrm{Suz}, \mathrm{J}_2$.
   (c) A Fischer group $\mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}'_{24}$.
   (d) A monstrous group $\mathbb{M}, \mathbb{B}, \mathrm{Th}, \mathrm{HN}, \mathrm{He}$.
   (e) A pariah $\mathrm{J}_1, \mathrm{J}_3, \mathrm{J}_4, \mathrm{O'N}, \mathrm{Ly}, \mathrm{Ru}$.

3.1 Classification of finite simple groups with order under 100

Although the classification of finite simple groups is a monumental result and requires tens of thousands of pages to completely prove and verify, we can still classify all finite simple groups of order less than 100 by hand and some fundamental results and techniques in group theory. To begin with, we need some results deduced by group actions and some corollaries of Sylow's theorem.

3.1.1 Applications of group actions

Lemma 3.2

Let G be a group and Ω be any non-empty set and $\mathrm{Sym}(\Omega)$ be the symmetric group on Ω. Consider G acts on Ω by $\cdot : G \times \Omega \to \Omega$. Then the following statements hold:

1. $\forall g \in G$, define a map $\pi_g : \Omega \to \Omega := \alpha \mapsto \alpha \cdot g$. Then $\pi_g \in \mathrm{Sym}(\Omega)$.
2. The map $\theta : G \to \mathrm{Sym}(\Omega) := g \mapsto \pi_g$ is a group homomorphism with $\ker(\theta) = \{g \in G : \forall \alpha \in \Omega, \alpha \cdot g = \alpha\}$.

Proof. 1. Take any $g \in G$ and define $\pi_g : \Omega \to \Omega := \alpha \mapsto \alpha \cdot g$. by the definition of $\mathrm{Sym}(\Omega)$, if we can show

π_g is a bijection, then the proof is done. Take any $x \in \Omega$, calculate

$$(\pi_{g^{-1}} \circ \pi_g)(x) = \pi_{g^{-1}}(\pi_g(x)) = \pi_{g^{-1}}(x \cdot g) = (x \cdot g) \cdot g^{-1} = x \cdot (g \cdot g^{-1}) = x \cdot e = x$$

Hence, π_g is a bijection and $\pi_g \in \mathrm{Sym}(\Omega)$.

2. Take any $g, h \in G$, define $\pi_g, \pi_h \in \mathrm{Sym}(\Omega)$ as above. Calculate

$$\theta(g)\theta(h) = \pi_g \pi_h = \pi_{gh} = \theta(gh)$$

Hence, θ is a group homomorphism. Besides, an element $g \in G$ lies in $\ker(\theta)$ if and only if $\pi_g = \mathrm{id}_\Omega$, which is equivalent to $\forall \alpha \in \Omega, \alpha \cdot g = \alpha$.

□

Corollary 3.3

Let G be a group and Ω be a non-empty set. Consider G acts on Ω by $\cdot : G \times \Omega \to \Omega$. Set $K := \{g \in G : \forall \alpha \in \Omega, \alpha \cdot g = \alpha\}$ and θ is the group homomorphism in 3.2. Then $K \trianglelefteq G$ and $G/K \cong \theta(G) \leq \mathrm{Sym}(\Omega)$.

Proof. $\theta : G \to \mathrm{Sym}(\Omega)$ is defined as $g \mapsto \pi_g$. Since $\ker(\theta) = K$, by 1.3, $G/K \cong \theta(G) \leq \mathrm{Sym}(\Omega)$. □

Theorem 3.4

Let G be a group and $H \lneq G$ be a proper subgroup of G with $[G : H] = n$ for some $n \in \mathbb{N}$. Then there exists a normal subgroup $N \trianglelefteq G$ such that the following statements hold:

1. $[G : N]$ divides $n!$.
2. $N \leq H$.

In particular, if $n > 1$ and $\left|G\right|$ does not divide $n!$, then G is not simple.

Proof. Consider a set $\Omega := \{Hx : x \in G\}$ and let G acts on Ω by $\cdot : G \times \Omega \to \Omega := (g, Hx) \mapsto Hxg$. Set $N := \{g \in G : \forall x \in \Omega, x \cdot g = x\}$. Applying 3.3 on the action of G on Ω, we have $N \trianglelefteq G$ and $G/N \cong \theta(G) \leq \mathrm{Sym}(\Omega)$, where θ is the group homomorphism defined in 3.2.

1. Since $\left|\Omega\right| = n$, we have $\left|\mathrm{Sym}(\Omega)\right| = n!$. Applying 1.4, we have that $[G : N]$ divides $n!$.
2. Take any $x \in N$. Since $H \in \Omega$, we have $x \in Hx = H \cdot x = H$. Hence, $N \leq H$.

For the last statement, it suffices to show that $\{e\} \lneq N \lneq G$. Since $H \lneq G$ and $N \leq H$, we have $N \lneq G$. If $N = \{e\}$, then $\left|G\right| = \left|G/N\right| = \left|\theta(G)\right|$ which would divide $n!$. This contradicts the assumption that $\left|G\right|$ does not divide $n!$. □

Remark 3.5 — To use the above theorem as a non-simplicity criterion, we need a way to help us find the subgroups with relatively small indexes. Sylow's theorem provides some techniques to find subgroups of finite groups and keep track of their indices.

3.1.2 Applications of Sylow's theorem

With Sylow's theorem, we can introduce some powerful corollaries deduced by it to help us classify finite simple groups with order under 100 more efficiently. To begin with, we introduce an important group theory concept, the normaliser of a subgroup.

Definition 3.6 (Normaliser of a subgroup)**.** Let G be a group and H be a subgroup of G. We define the **normaliser** of H in G as $\{g \in G : gHg^{-1} = H\}$ and denote it by $N_G(H)$.

Remark 3.7 — We have the following facts about normalisers:

1. The normaliser of a subgroup H in a group G is a collection of the elements in the group that commute with all elements in H or conjugate H back to itself.
2. The normaliser of a subgroup H in a group G is a subgroup of G by applying the subgroup criterion.
3. If p is a prime number and G is a finite group with order $p^\alpha m$ for some $\alpha \geq 1$ with $p \nmid m$, then $\forall P \in \mathrm{Syl}_p(G)$, we have $n_p(G) = [G : N_G(P)]$ since $\mathrm{Syl}_p(G)$ is a single conjugacy class in G.

Corollary 3.8

Let p be a prime number and G be a finite group with $\left|G\right| = p^\alpha m$ for some $\alpha \geq 1$ with $p \nmid m$. If $P \in \mathrm{Syl}_p(G)$ and $n_p(G)$ denotes the number of Sylow p-subgroups of G, then $P \triangleleft G$ if and only if $n_p(G) = 1$.

Proof.

- ($\Rightarrow$) Suppose $P \triangleleft G$, we have $N_G(P) = G$ by the definition of normal subgroup and normaliser. Hence, $n_p(G) = [G : N_G(P)] = 1$.
- ($\Leftarrow$) Suppose $n_p(G) = 1$ and take any $g \in G$. Set $Q := gPg^{-1} = \{ghg^{-1} : h \in P\}$. Apply the subgroup criterion on Q, we have $Q \leq G$. By the definition of Q, we have $\left|Q\right| = \left|P\right| = p^\alpha$. Hence, $Q \in \mathrm{Syl}_p(G)$. Since $n_p(G) = 1$, we have $Q = P$. Since g is arbitrary, we have $P \triangleleft G$.

□

Corollary 3.9

Let p be a prime number and G be a finite group with $\left|G\right| = p^\alpha m$ for some $\alpha \geq 1$ and $m \geq 1$ with $p \nmid m$. If G is simple and we write the number of Sylow $p-$subgroups of G as n, then $\left|G\right| \mid n!$.

Proof. Take any simple finite group G with $\left|G\right| = p^\alpha m$ for some $\alpha \geq 1$ and $m \geq 1$ with $p \nmid m$. By the Sylow's theorem, $\mathrm{Syl}_p(G) \neq \varnothing$. Take any $S \in \mathrm{Syl}_p(G)$ and set $H := N_G(S)$, the normaliser of S in G. Then, $[G : H] = n$ by 3.7 Since G is simple, S can not be normal. Hence, $n > 1$. By the simplicity of G and 3.4, we have $\left|G\right| \mid n!$. □

Proposition 3.10

If p is a prime number and G is a finite group with $\left|G\right| = p^\alpha$ for some $\alpha \geq 1$, then G is simple if and only if $\alpha = 1$.

Proof.

- ($\Rightarrow$) Suppose G is simple. Contradiction: Assume $\alpha > 1$. Recall that $Z(G) \triangleleft G$, the centre of a group is normal. We claim that any group with order p^α for some prime number p and $\alpha > 1$ has a non-trivial proper center. The proof of this claim can be found in Beachy & Blair (2006). Hence, $Z(G) \neq \{e\}$ and $Z(G) \neq G$, which contradicts the simplicity of G. We conclude that $\alpha = 1$.
- ($\Leftarrow$) Suppose $\alpha = 1$, take any subgroup $H \leq G$, applying 1.4, we have that $\left|H\right|$ divides $\left|G\right| = p$. Since p is a prime number, we have $\left|H\right| = 1$ or $\left|H\right| = p$. Hence, $H = \{e\}$ or $H = G$. Since the choosing of H is arbitrary, there are only two trivial subgroups of G, and also two normal subgroups of G. Therefore, G is simple.

□

Corollary 3.11

If p, q are two distinct prime numbers with $p < q$ and G is a finite group with $\left|G\right| = pq$, then there is a normal subgroup $N \triangleleft G$ such that $\left|N\right| = q$. Hence, G is not simple.

Proof. Take any two distinct prime numbers p, q and any finite group G with order pq. Then, by Sylow's theorem, we have $n_q(G) \equiv 1 \mod q$. In particular, $n_q(G) \nmid q$. Since $n_q(G) \mid pq$, it must have $n_q(G) \mid p$. Assume $n_q(G) > 1$, then $n_q(G) > q > p$, which contradicts the fact that $n_q(G) \mid p$. Hence, $n_q(G) = 1$. By 3.8, there is a normal subgroup $N \triangleleft G$ with order q. Therefore, G is not simple. □

Corollary 3.12

If p, q are two distinct prime numbers and G is a finite group with $\left|G\right| = p^2q$, then G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup. Hence, G is not simple.

Proof. The proof is adapted from Isaacs (1994). Take any two distinct prime numbers p, q. Applying Sylow's theorem on G and q, we have $n_q(G) \equiv 1 \mod q$ and $n_q(G) \mid p^2$. Hence, $n_q(G) = 1$, p or p^2. By cases:

- $n_q(G) = 1$: By 3.8, there is a normal subgroup $N \triangleleft G$ with order q. Hence, G is not simple.
- $n_q(G) = p$: By Sylow's theorem, we have $p \equiv 1 \mod q$ and $p \neq 1$. Hence, $p > q$, which means that $q \not\equiv 1 \mod p$. Applying Sylow's theorem on G and p, we have $n_p(G) \equiv 1 \mod p$ and $n_p(G) \mid q$. Therefore, we can not have $n_p(G) = q$, which means that $n_p(G) = 1$. By 3.8, there is a normal subgroup $N \triangleleft G$. Hence, G is not simple.
- $n_q(G) = p^2$: Take any two distinct subgroups $Q_1, Q_2 \in \mathrm{Syl}_q(G)$. Since $\left|Q_1\right| = \left|Q_2\right| = q$, which is a prime number, we have $Q_1 \cap Q_2 = \{e\}$. Therefore, there are no two distinct Sylow q-subgroups that have any non-identity elements in common. Since $n_q(G) = p^2$ which the number of Sylow q-subgroups, there are at least $p^2(q-1)$ non-identity elements in G. Denote the set of all such $p^2(q-1)$ elements as X and the left elements in G as Y. Then, $\left|Y\right| = \left|G\right| - \left|X\right| = p^2q - p^2(q-1) = p^2$. Therefore, $\forall g \in G$ with $\mathrm{ord}(g) \neq q$, $g \in Y$. Now, take any $P \in \mathrm{Syl}_p(G)$, there is no element of P with the order of q. Hence, $P \subseteq X$. Besides, since P is a Sylow p-subgroup, we have $\left|S\right| = p^2 = Y$. We can conclude that $P = Y$. Therefore, $n_p(G) = 1$. By 3.8, $P \triangleleft G$. Hence, G is not simple.

□

Corollary 3.13

If p, q are two distinct prime numbers and G is a finite group with $\left|G\right| = p^3q$, then either G has a normal Sylow p-subgroup or a normal Sylow q-subgroup or $p = 2$, $q = 3$ and $\left|G\right| = 24$. Furthermore, G is not simple.

Proof. The first part of the proof is adapted from Isaacs (1994). Take any two distinct prime numbers p, q. Applying Sylow's theorem on G and q, we have $n_q(G) \equiv 1 \mod q$ and $n_q(G) \mid p^3$. Hence, $n_q(G) = 1$, p, p^2 or p^3. By cases:

- $n_q(G) = 1$: By 3.8, there is a normal subgroup $N \triangleleft G$ with order q. Hence, G is not simple.
- $n_q(G) = p$: Applying Sylow's theorem on G and p, we have $n_p(G) \equiv 1 \mod p$ and $n_p(G) \mid q$. Hence, $n_p(G) = 1$ or q. By cases:
  - $n_p(G) = 1$: By 3.8, there is a normal subgroup $N \triangleleft G$ with order p^3. Hence, G is not simple.
  - $n_p(G) = q$: We have $q \equiv 1 \mod p$ and $q \neq 1$. Hence, $q > p$, which contradicts the fact that $n_q(G) = p \equiv 1 \mod q$. Hence, the only possibility is $n_p(G) = 1$. By 3.8, there is a normal subgroup $N \triangleleft G$ with order p^3. Hence, G is not simple.
- $n_q(G) = p^2$: We have $p^2 \equiv 1 \mod q$ and thus $q \mid (p^2 - 1) = (p-1)(p+1)$. Since q is a prime number, either $q \mid (p-1)$ or $q \mid (p+1)$. However, $q > p$, which means that $q \nmid (p-1)$. Hence, $q \mid (p+1)$. So, $p < q \leq p+1$. This implies that $q = p+1$. Since $2, 3$ are the only pair of consecutive prime numbers, we have $p = 2$, $q = 3$ and $\left|G\right| = 24$.
- $n_q(G) = p^3$: Take any two distinct subgroups $Q_1, Q_2 \in \mathrm{Syl}_q(G)$. Since $\left|Q_1\right| = \left|Q_2\right| = q$, which is a prime number, we have $Q_1 \cap Q_2 = \{e\}$. Therefore, there are no two distinct Sylow q-subgroups that have any non-identity elements in common. Since $n_q(G) = p^3$ which the number of Sylow q-subgroups, there are

at least $p^3(q-1)$ non-identity elements in G. Denote the set of all such $p^3(q-1)$ elements as X and the left elements in G as Y. Then, $\left|Y\right| = \left|G\right| - \left|X\right| = p^3q - p^3(q-1) = p^3$. The following argument is similar to the proof of 3.12. We can conclude that G is not simple.

It remains to show that G is not simple when $p = 2$, $q = 3$ and $\left|G\right| = 24$. Applying Sylow's theorem on G and 2, we have $n_2(G) \equiv 1 \mod 2$ and $n_2(G) \mid 3$. Hence, $n_2(G) = 1$ or 3. By cases:

- $n_2(G) = 1$: By 3.8, there is a normal subgroup $N \triangleleft G$ with order 8. Hence, G is not simple.
- $n_2(G) = 3$: Contradiction: Assume G is simple, by 3.9, $\left|G\right|$ divides $3! = 6$. However, $\left|G\right| = 24$ which is a contradiction. Hence, G is not simple.

□

3.1.3 Classification for finite simple groups with order under 100

With the tools prepared enough above, we can now classify all finite simple groups with order less than 100 more efficiently. But there are still some lemmas required to prove the main theorem.

Lemma 3.14

If G is a finite group of order p for some prime number, then G is cyclic and simple.

Proof. Take any finite group G with order p for some prime number p. The simplicity of G is proved by 3.10. The remaining part is to show that G is cyclic. Take any $g \in G$ with $g \neq e$. Consider the subgroup $\langle g \rangle \leq G$ generated by g. Since $\left|\langle g \rangle\right|$ divides $\left|G\right| = p$. Applying the Lagrange theorem, we have $\left|\langle g \rangle\right| = 1$ or $\left|\langle g \rangle\right| = p$. Since $g \neq e$, we have $\left|\langle g \rangle\right| = p$. Hence, G is cyclic. □

Lemma 3.15

The alternating group A_5, whose order is 60, is simple.

Proof. This is a special case for 2.3 and $\left|A_5\right| = \frac{1}{2}\left|S_5\right| = \frac{1}{2}5! = 60$. □

Lemma 3.16

If G is a finite simple group with order 60, then $G \cong A_5$.

Proof. Take any finite simple group G with order 60. The part of the proof is adapted from Dummit & Foote (2004) and can be split into two parts:

- **G is isomorphic to A_5 if G has a subgroup with index 5**: Suppose $N \leq G$ with $[G : N] = 5$ and set $X := \{gN : g \in G\}$, the collection of all left cosets of N in G. Consider a group action, that is $\cdot : G \times X \to X := (g, g'N) \mapsto gg'N$. Set $K := \{g \in G : \forall g'N \in X, gg'N = g'N\}$. By 3.3, $K \trianglelefteq G$ and $G/K \cong \theta(G) \leq S_5$, where θ is defined in 3.2. By the simplicity of G, $K = \{e\}$. Hence, G is isomorphic to some subgroup H of S_5. Claim: $H = A_5$. To prove this claim, it suffices to show that $H \leq A_5$ since $\left|H\right| = A_5$. Contradiction: Assume H is not contained in A_5. Then, $A_5 \cap H$ is a subgroup of H with index 2. By the simplicity of H (since $H \cong G$), H has no (normal) subgroup of index 2, which is a contradiction. Hence, $H = A_5$ and $G \cong A_5$.
- **G has a subgroup with index 5**: Factorise $60 = 2^2 \cdot 3 \cdot 5$ into product of primes or powers of primes. Applying Sylow's theorem on G, we have $n_2(G) \equiv 1 \mod 2$ and $n_2(G) \mid 15$. Hence, $n_2(G) = 1$, 3, 5 or 15. By 3.7, we have $n_2(G) = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_2(G)$. If we can show $n_2(G) = 5$ or if $n_2(G) \neq 5$, but there is still a subgroup with index 5, the proof is done. We consider the following cases:
  - $n_2(G) = 1$: By 3.8, there is a normal subgroup $N \triangleleft G$ with order 4, which contradicts the simplicity of G. Hence, $n_2(G) \neq 1$.
  - $n_2(G) = 3$: By 3.9, $\left|G\right| \mid 3! = 6$. However, $\left|G\right| = 60$ which is a contradiction. Hence, $n_2(G) \neq 3$.

– $n_2(G) = 15$: Firstly, we consider the cases any two Sylow 2-subgroups intersect trivially. Take any two distinct Sylow 2-subgroups $P, Q \in \mathrm{Syl}_2(G)$ with $P \cap Q = \{e\}$, then the number of non-identity elements in Sylow 2-subgroups would be $(4-1) \cdot 15 = 45$. Applying Sylow's theorem on G and $p := 5$, we have $n_5(G) \equiv 1 \mod 5$ and $n_5(G) \mid 12$. Hence, $n_5(G) = 1$ or 6. It is impossible for $n_5(G) = 1$ since G is simple. Hence, $n_5(G) = 6$. Therefore, the number of elements with order 5 in G is $(5-1) \cdot 6 = 24$. Since $45 + 24 > 60 = \left|G\right|$, this is a contradiction. Thus, there exist at least 2 Sylow 2-subgroups that intersect non-trivially. Take any two distinct Sylow 2-subgroups $R, S \in \mathrm{Syl}_2(G)$ with $R \cap S \neq \{e\}$. Set $M := N_G(R \cap S)$. Since $\left|R\right| = \left|S\right| = 4$, by properties of groups, they must both be abelian. We can conclude that $R \leq M$ and $S \leq M$ by the definition of normaliser. Since G is simple, $M \neq G$. Thus, $4 \mid \left|M\right|$ and $\left|M\right| > 4$ (otherwise, $R = S$). The only possibility is $\left|M\right| = 12$. Therefore, by Lagrange's theorem, we have $[G : M] = 5$. Hence, M is a subgroup of G with index 5.

Therefore, by the above two parts, we conclude that $G \cong A_5$.

□

Theorem 3.17

If G is a finite simple group with $\left|G\right| < 100$, then G is isomorphic to one of the following groups:

1. A_5, the alternating group of degree 5, whose order is 60.
2. Cyclic groups C_p for some prime number p with $p < 100$.

Proof. By 3.10, 3.11, 3.12, 3.13, 3.14, 3.16, it suffices to show that for any finite group G with order n that is under 100, with the order that is not any forms in the above corollaries and lemmas, G is not simple. The remaining cases that need to be considered are:

$$n = 30, 36, 42, 48, 66, 70, 72, 78, 80, 84, 90, 96.$$

- $n = 30$: Take any finite group G with order 30. Factorise $30 = 2 \cdot 3 \cdot 5$ into a product of primes or powers of primes. Set $p := 5$ and $n_5(G)$ as the number of all Sylow 5-subgroups of G. By Sylow's theorem, we have $n_5(G) \equiv 1 \mod 5$ and $n_5(G) \mid 6$. Hence, $n_5(G) = 1$ or $n_5(G) = 6$. By cases:
  - $n_5(G) = 1$: By 3.8, there is a normal subgroup $N \triangleleft G$ with order 5. Hence, G is not simple.
  - $n_5(G) = 6$: Contradiction: Take any two subgroups $P, Q \in \mathrm{Syl}_5(G)$, then $\left|P\right| = \left|Q\right| = 5$. Since $P \cap Q \leq G$ and by Lagrange's theorem, $\left|P \cap Q\right| = 1$, which means that there are 6 subgroups of G containing 4 elements of order 5 that are not contained in any other subgroup. It follows that there are $6 \cdot 4 = 24$ elements of order 5 in G. Again, set $q := 3$ and apply Sylow's theorem, we have $n_3(G) \equiv 1 \mod 3$ and $n_3(G) \mid 30$. Hence, $n_3(G) = 1$ or $n_3(G) = 10$. If $n_3(G) = 10$, applying the same argument as above, there must be $10 \cdot 2 = 20$ elements of order 3 in G. However, $24 + 20 > \left|30\right|$, which is a contradiction. $n_5(G) \neq 6$.

  Therefore, we can conclude that G is not simple when $n = 30$. In the following cases, by 3.8, if $n_p(G) = 1$, then the argument is the same as above and will be omitted.

- $n = 36$: Take any finite group G with order 36. Factorise $36 = 2^2 \cdot 3^2$ into a product of primes or powers of primes. Set $p := 3$ and $n_3(G)$ as the number of all Sylow 3-subgroups of G. By Sylow's theorem, we have $n_3(G) \equiv 1 \mod 3$ and $n_3(G) \mid 4$. If $n_3(G) = 4$, by 3.9, $\left|G\right|$ divides 4!. However, $\left|G\right| = 36 > 4!$, which is impossible when $\left|G\right|$ divides 4!. Hence, $n_3(G) \neq 4$. Therefore, G is not simple when $n = 36$.

- $n = 32$: Take any finite group G with order 42. Factorise $42 = 2 \cdot 3 \cdot 7$ into a product of primes. Set $p := 7$ and $n_7(G)$ as the number of all Sylow 7-subgroups of G. By Sylow's theorem, we have $n_7(G) \equiv 1 \mod 7$ and $n_7(G) \mid 6$. Hence, $n_7(G) = 1$. Therefore, G is not simple when $n = 42$.

- $n = 48$: Take any finite group G with order 48. Factorise $48 = 2^4 \cdot 3$ into a product of primes. Set $p := 3$ and $n_3(G)$ as the number of all Sylow 3-subgroups of G. By Sylow's theorem, we have $n_3(G) \equiv 1 \mod 3$ and $n_3(G) \mid 16$. Hence, $n_3(G) = 1$ or $n_3(G) = 4$. If $n_3(G) = 4$, by 3.9, $\left|G\right|$ divides 4!. However, $\left|G\right| = 48 > 4!$, which is a contradiction. Hence, $n_3(G) \neq 4$. Therefore, G is not simple when $n = 48$.

- $n = 66$: Take any finite group G with order 66. Factorise $66 = 2 \cdot 3 \cdot 11$ into a product of primes. Set $p := 11$ and $n_{11}(G)$ as the number of all Sylow 11-subgroups of G. By Sylow's theorem, we have $n_{11}(G) \equiv 1 \mod 11$ and $n_{11}(G) \mid 6$. Hence, $n_{11}(G) = 1$. Therefore, G is not simple when $n = 66$.
- $n = 70$: Take any finite group G with order 70. Factorise $70 = 2 \cdot 5 \cdot 7$ into a product of primes. Set $p := 7$ and $n_7(G)$ as the number of all Sylow 7-subgroups of G. By Sylow's theorem, we have $n_7(G) \equiv 1 \mod 7$ and $n_7(G) \mid 10$. Hence, $n_7(G) = 1$. Therefore, G is not simple when $n = 70$.
- $n = 72$: Take any finite group G with order 72. Factorise $72 = 2^3 \cdot 3^2$ into a product of primes. Set $p := 3$ and $n_3(G)$ as the number of all Sylow 3-subgroups of G. By Sylow's theorem, we have $n_3(G) \equiv 1 \mod 3$ and $n_3(G) \mid 8$. Hence, $n_3(G) = 1$ or $n_3(G) = 4$. If $n_3(G) = 4$, by 3.9, $\left|G\right|$ divides 4!. However, $\left|G\right| = 72 > 4!$, which is a condtradiction. Hence, $n_3(G) \neq 4$. Therefore, G is not simple when $n = 72$.
- $n = 78$: Take any finite group G with order 78. Factorise $78 = 2 \cdot 3 \cdot 13$ into a product of primes. Set $p := 13$ and $n_{13}(G)$ as the number of all Sylow 13-subgroups of G. By Sylow's theorem, we have $n_{13}(G) \equiv 1 \mod 13$ and $n_{13}(G) \mid 6$. Hence, $n_{13}(G) = 1$. Therefore, G is not simple when $n = 78$.
- $n = 80$: Take any finite group G with order 80. Factorise $80 = 2^4 \cdot 5$ into a product of primes. Set $p := 2$ and $n_2(G)$ as the number of all Sylow 2-subgroups of G. By Sylow's theorem, we have $n_2(G) \equiv 1 \mod 2$ and $n_2(G) \mid 5$. Hence, $n_2(G) = 1$ or $n_2(G) = 5$. If $n_2(G) = 5$, by 3.9, $\left|G\right|$ divides 5!. However, $\left|G\right|$ is not a factor of $5! = 120$. Hence, $n_2(G) \neq 5$. Therefore, G is not simple when $n = 80$.
- $n = 84$: Take any finite group G with order 84. Factorise $84 = 2^2 \cdot 3 \cdot 7$ into product of primes. Set $p := 7$ and $n_7(G)$ as the number of all Sylow 7-subgroups of G. By Sylow's theorem, we have $n_7(G) \equiv 1 \mod 7$ and $n_7(G) \mid 12$. Hence, $n_7(G) = 1$. Therefore, G is not simple when $n = 84$.
- $n = 90$: Take any finite group G with order 90. Factorise $90 = 2 \cdot 3^2 \cdot 5$ into a product of primes. Set $p := 5$ and $n_5(G)$ as the number of all Sylow 5-subgroups of G. By Sylow's theorem, we have $n_5(G) \equiv 1 \mod 5$ and $n_5(G) \mid 18$. Hence, $n_5(G) = 1$ or $n_5(G) = 6$. If $n_5(G) = 6$, take any two distinct Sylow 5-subgroups $P, Q \in \mathrm{Syl}_5(G)$, then $\left|P\right| = \left|Q\right| = 5$. Since $P \cap Q \leq G$ and by Lagrange's theorem, $\left|P \cap Q\right| = 1$, which means that there are 6 subgroups of G containing 4 elements of order 5 that are not contained in any other subgroup. It follows that there are $6 \cdot 4 = 24$ elements of order 5 in G. Now set $q := 3$ and apply Sylow's theorem, we have $n_3(G) \equiv 1 \mod 3$ and $n_3(G) \mid 10$. Hence, $n_3(G) = 1$ or $n_3(G) = 10$. If $n_3(G) = 10$, take any two distinct Sylow 3-subgroups $R, S \in \mathrm{Syl}_3(G)$, then $\left|R\right| = \left|S\right| = 9$. If $\left|R\right| \cap \left|S\right| = \{e\}$, then the number of non-identity elements in Sylow 3-subgroups would be $(9-1) \cdot 10 = 80$. Since $80+24 > 90 = \left|G\right|$, this is a contradiction. If $\left|R\right| \cap \left|S\right| \neq \{e\}$, the following argument can be found in Wise (2015). Therefore, $n_5(G) \neq 6$. Hence, G is not simple when $n = 90$.
- $n = 96$: Take any finite group G with order 96. Factorise $96 = 2^5 \cdot 3$ into a product of primes. Set $p := 3$ and $n_3(G)$ as the number of all Sylow 3-subgroups of G. By Sylow's theorem, we have $n_3(G) \equiv 1 \mod 3$ and $n_3(G) \mid 32$. Hence, $n_3(G) = 1$ or $n_3(G) = 4$. If $n_3(G) = 4$, by 3.9, $\left|G\right|$ divides 4!. However, this is clearly not the case. Hence, $n_3(G) \neq 4$. Therefore, G is not simple when $n = 96$.

Therefore, by verifying all the cases above, we can conclude that if G is a finite simple group with $\left|G\right| < 100$, then G is isomorphic to A_5 or a cyclic group C_p for some prime number p with $p < 100$. □

3.2 The modern classification

Although case-by-case arguments like the above suffice for groups of small order, they only become more and more unwieldy and complicated for larger and larger groups – and such techniques do not provide a complete method for classifying all finite simple groups. An alternative approach is necessary and was provided by Brauer in the 1950s, using two theorems which together give a starting point for a modern classification.

Theorem 3.18 (Feit-Thompson)
Every finite group of odd order is solvable. In particular, every finite simple group of odd order is cyclic.

The proof is also famously long and hard and will not be reproduced or discussed here. Details can be found in Feit & Thompson (1963).

The second theorem, in contrast, has an elegant elementary proof which we include here – the argument is adapted from Brauer & Fowler (1955), slightly simplified and using modern notation (The original result achieves a better bound, but this is unnecessary for the corollary we require).

Definition 3.19. Let $x \in G$. We define the **extended normaliser** $N^*(x) = \{g \in G : g^{-1}xg = x \text{ or } g^{-1}xg = x^{-1}\}$

Definition 3.20. We say that an element of order 2 in a group G is an **involution** of G.

Theorem 3.21 (Brauer-Fowler)
Let G be a finite simple group with an involution ι, then $|G| \leq (2|N(\iota)|^2)!$.

Proof. Let G be a finite simple group of even order, and let A be the set of s in G. We proceed by counting pairs of involutions using the set $A^2 := \{xy : x, y \in A\}$, Let $n(g)$ be the number of ways to write g as a product of involutions. Then for involutions x, y, if $xy = g$ then $x^{-1}gx = yx = g^{-1}$ and so $n(g) \leq |N^*(g)|$. We thus have

$$|A|^2 = \sum_{g \in A^2} n(g) \leq |A| + \sum_{g \in A^2 \setminus \{e\}} |N^*(g)|$$

Since $|A| \geq 2$, this further implies

$$\frac{|A|^2}{2} \leq \sum_{g \in A^2 \setminus \{e\}} |N^*(g)|$$

and then by the pigeonhole principle, we see that there is some $g \in A^2 \setminus \{e\}$ with $|N^*(g)| \geq \frac{|A|^2}{2|G|}$.

With this established, we fix an involution ι and write $n = |N(\iota)|$ and observe that G has at least $|G|/n$ involutions (since conjugates of involutions are involutions). We find that there is a nontrivial $h \in A^2$ such that $|N^*(h)| \leq |G|/2n^2$, and in particular $N^*(h)$ has index at most $2n^2$.

This subgroup is proper. To see this, suppose otherwise. If h is not an involution, then it is straightforward to see that $N(h)$ is a subgroup of $N^*(h) = G$ of index 2, contradicting simplicity of G. Otherwise h is an involution, $N(h) = N^*(h) = G$, and $\langle h \rangle$ is normal in $N(h)$ again contradicting simplicity. Therefore $N^*(h)$ is a proper subgroup of index at most $2n^2$, and so G is isomorphic to a subgroup of S_{2n^2} by simplicity, establishing the required bound. □

These two theorems together give the starting point for the classification theorem. We can consider a minimal unknown finite simple group, we know it has an involution (since it's not cyclic) and we can look at the centraliser of this involution and there will only be finitely many cases to check for each possible centraliser.

3.3 Finite simple groups in which D_8 is the centraliser of an involution

Let's go through a particular case of this programme. We will classify all finite simple groups with an involution ι such that $C_G(\iota) = D \cong D_8$.

We proceed by showing that there is a unique conjugacy class of involutions in G, and using this, the function $n(g)$ from the proof of the Brauer-Fowler theorem will be a class function with which we can control the combinatorics of G with character theory – by this method we get some number-theoretic constraints on $|G|$ which we can apply to complete the proof with some standard divisibility arguments. This argument is adapted from James & Liebeck (2001).

Theorem 3.22
The conjugacy class of ι is the unique conjugacy class of involutions in G.

Proof. Firstly $|D| = 2^3$, so D is contained in a Sylow 2-subgroup P. Then $Z(P) \subseteq D$ and furthermore $Z(P) \subseteq Z(D) = \langle \iota \rangle$. Since $|P| = 2^k$ with $k \geq 3$, $Z(P)$ is nontrivial, and so must be $\langle \iota \rangle$. Therefore $P = C_P(\iota) \subseteq C_G(\iota) = D$ and so $P = D$, and in particular D is a Sylow 2-subgroup. Write

$$D = \langle r, s \mid r^4 = s^2 = e, s^{-1}rs = r^{-1} \rangle$$

Clearly $\iota = r^2$. $C := \langle r \rangle$ is the unique subgroup of index 2 in D.

Consider G acting on Ω, the set of cosets of C, and let κ be an involution in G. If κ does not fix any coset of C, then since $[G : C] = [G : D][D : C] = 2m$ for some odd m (as D is a Sylow 2-subgroup), it must be that κ acts as a product of m disjoint 2-cycles which is an odd permutation. In addition $\iota \neq e$ acts as identity,

implying that $\mathrm{Alt}(\Omega) \cap G$ is a nontrivial proper normal subgroup of G, contradicting simplicity. Therefore there is a coset gC such that $\kappa gC = gC$ and so $g^{-1}\kappa g \in C$. Then $g^{-1}\kappa g = \iota$ since conjugates of involutions are involutions. Therefore κ is conjugate to ι. □

Because of this, $n(g)$ is a class function, counting pairs (x, y) of x, y conjugate to ι with $xy = g$. By the theorem on class algebra constants, we further have:

$$n(g) = \frac{|G|}{|C_G(\iota)|^2} \sum_\chi \frac{\chi(\iota)^2}{\chi(e)} \overline{\chi(g)} = \frac{|G|}{64} \sum_\chi \frac{\chi(\iota)^2}{\chi(e)} \overline{\chi(g)}$$

where we sum over all irreducible characters of G.

Now, we do not know all the irreducible characters of G, but because of orthogonality, we do not need to. Instead, we can build up a nicely behaved character on G from its known subgroups, and to look at its inner product with $n(g)$ – it turns out that this suffices to constrain $|G|$.

Let λ be the unique character on C such that $\lambda(r) = i$ and consider

$$\theta = \mathrm{Ind}_C^D 1 - \mathrm{Ind}_C^D \lambda$$

This takes the value 2 on r and r^{-1}, and 4 on ι and is zero otherwise. From the character table of D_8 we see that this is $\theta = \chi_1 + \chi_2 - \chi_5$. Since irreducible characters have norm 1, we find $\langle \theta, \theta \rangle = 3$. We will then show that $\left\langle \mathrm{Ind}_D^G \theta, \mathrm{Ind}_D^G \theta \right\rangle = 3$. In particular by Frobenius reciprocity

$$\left\langle \mathrm{Res}_G^D \mathrm{Ind}_D^G \theta, \theta \right\rangle = \left\langle \mathrm{Ind}_D^G \theta, \mathrm{Ind}_D^G \theta \right\rangle$$

Applying the Frobenius formula this is:

$$\left\langle \mathrm{Res}_G^D \mathrm{Ind}_D^G \theta, \theta \right\rangle = \frac{1}{8} \sum_{d \in D} \left[\frac{1}{8} \sum_{g \in G} \dot{\theta}(g^{-1} dg) \right] \overline{\theta(d)}$$

$\theta(d) = 0$ except for $d = r, r^2, r^3$, and so we only need to consider when $g^{-1}dg, d \in C \setminus \{e\}$. If this happens, we have $\iota = d$ or d^2, in either case $g^{-1}\iota g = \iota$, and $g \in D$ implying $g^{-1}Cg = C$. In both cases we find $\theta(g^{-1}dg) = \theta(d)$. Therefore

$$\left\langle \mathrm{Res}_G^D \mathrm{Ind}_D^G \theta, \theta \right\rangle = \langle \theta, \theta \rangle = 3$$

Then using the lemma we had for generalised characters of small norm and the fact that

$$\left\langle \mathrm{Ind}_D^G \theta, 1_G \right\rangle = \langle 1_C - \lambda, 1_C \rangle = 1$$

we see that

$$\mathrm{Ind}_D^G \theta = 1_G + \alpha - \beta$$

where α, β are irreducible characters of G. From the known values we also know that $1 + \alpha(e) - \beta(e) = 0$ and $1 + \alpha(\iota) - \beta(\iota) = 4$. Recall that $\alpha(\iota)$ and $\beta(\iota)$ must be integers.

Returning to $n(g)$, we compute using orthogonality that:

$$\left\langle \mathrm{Ind}_D^G \theta, n \right\rangle = \frac{|G|}{64} \left(1 + \frac{\alpha(\iota)^2}{\alpha(e)} - \frac{\beta(\iota)^2}{\beta(e)} \right)$$

on the other hand, by Frobenius reciprocity and straightforward calculations in D_8 we see that

$$\langle 1_C - \lambda, \mathrm{Res}_D^C n \rangle = \frac{1}{4} \left((1 - i) \cdot 4 + 2 \cdot 4 + (1 + i) \cdot 4 \right) = 4$$

and so:

$$|G| \left(1 + \frac{\alpha(\iota)^2}{\alpha(e)} - \frac{\beta(\iota)^2}{\beta(e)} \right) = 256$$

From this, we can begin to deduce number theoretic results about the order of G. Notice also that using the constraints on $\theta(e)$ and $\theta(\iota)$ we know that

$$\beta(e) = \alpha(e) + 1, \quad \beta(\iota) = \alpha(\iota) - 3$$

Using the column orthogonality relations we see that

$$1 + \alpha(\iota)^2 + \beta(\iota)^2 = 1 + \alpha(\iota)^2 + (\alpha(\iota) - 3)^2 = 2\alpha(\iota)^2 - 6\alpha(\iota) + 10 \leq |C_G(\iota)| = 8$$

This implies $\alpha(\iota) = 1$ or 2 which is enough to then finish off the classification.

Theorem 3.23
Let G be a finite simple group with an ι such that $C_G(\iota) \cong D_8$. Then $|G| = 168$ or 360.

Proof. If $\alpha(\iota) = 1$,

$$|G|\left(1 + \frac{1}{\alpha(e)} + \frac{4}{\alpha(e)+1}\right) = 256$$

and so

$$|G| = 256\frac{\alpha(e)(\alpha(e)+1)}{(\alpha(e)-1)^2}$$

By elementary divisibility arguments, $(\alpha(e)-1)^2 \mid 2^{10}$, and so $\alpha(e) = 2^r + 1$ for some $r \leq 5$. Therefore $|G|$ is one of 306, 360, 480, 768, and 1536. Of these, only $|G| = 360$ allows for a a Sylow 2-subgroup of order $2^3 = 8$. On the other hand if $\alpha(\iota) = 2$, we find

$$|G| = 256\frac{d(d+1)}{(d+2)^2}$$

and reasoning as above, we find that $\alpha(e) = 2^3 - 2$, and so $|G| = 168$. □

This narrows down the possible orders of finite simple groups to only two relatively small values (far better than the bound of $|G| \leq 128!$ that we get from Brauer-Fowler). One can also then show both these possibilities are achieved: $|G| = 168$ by $\mathrm{PSL}_2(7)$, and $|G| = 360$ by A_6. In both cases, these are the only finite simple groups of this order,

Theorem 3.24
Let G be a finite simple group with an ι such that $C_G(\iota) \cong D_8$. Then $G \cong \mathrm{PSL}_2(7)$ or $G \cong A_6$.

4 Construction of a graph with large girth

4.1 Introduction to the main problem

The delicate theories introduced in the first three sections have wide-ranging applications. For example, simple groups play a significant role in graph theory, specifically in the area of expander graphs. In this section, we will first take a step back and give a detailed explanation of a beautiful graph construction that kindles consequent research. Then we describe how such a construction contributes to a famous all-encompassing theorem linking simple groups and expander graphs.

The first part of this section aims to give an explicit construction of a graph with a large girth i.e. the length of the shortest circuit in a graph, a remarkable result due to Margulis (1982). The concrete definition of a (large) girth will be given in 4.2, along with some basic theorems that are necessary for the construction.

4.2 More preliminaries on groups and graphs

We are going to deal with graphs $X = (V, E)$, where V is the set of vertices and E is the set of edges. Let $|X|$ denote the number of vertices of X. Let $V = \{v_1, v_2, \dots\}$; then the adjacency matrix of X is $A = (A_{ij})$, where

$$A_{ij} = \text{number of edges between } v_i \text{ and } v_j.$$

Definition 4.1. A graph X is **simple** if there is at most one edge between any two vertices. A graphs X is ***k*-regular** if for every $v_i \in V : \sum_{v_j \in V} A_{ij} = k$.

Definition 4.2. The **girth** $g(X)$ of a graph X is the length of the shortest circuit in X.

Definition 4.3. Let $(X_m)_{m \geq 1}$ be a family of simple, finite, connected, k-regular graphs, with $|X| \to \infty$ as $m \to \infty$. Such a family has **large girth** if there exists some constant C such that $g(X_m) \geq (C + o(1)) \log_{k-1} |X_m|$, where $o(1)$ is a function tending to 0 as $m \to \infty$.

We obtain $C \leq 2$ by the following argument.

For a k-regular graph X, we first count the number of walks of length $\leq m$ starting from any vertex of X. There are $k(1+(k-1)^1+(k-1)^2+...+(k-1)^{m-1}) = k\left(\frac{(k-1)^m-1}{k-2}\right)$ of them, obtained by investigating walks of different lengths one by one.

If $g(X) > 2m$, then all the walks starting from a certain vertex will end at different vertices, and setting $m = \frac{g(X)-1}{2}$, we have

$$k\left(\frac{(k-1)^m-1}{k-2}\right) \leq |X|$$

Simplifying for $g(X)$,

$$g(X) \leq 2\log_{k-1}\left(\frac{k-2}{k}|X|+1\right)+1$$

Therefore,

$$\begin{aligned} g(X) &\leq 2\log_{k-1}(|X|) + 2\log_{k-1}\left(\frac{|X|+2}{|X|}\right) + D \\ &\leq 2\log_{k-1}(|X|) + 2\frac{\log_{k-1}\left(\frac{|X|+2}{|X|}\right)+D}{\log_{k-1}(|X|)}\log_{k-1}(|X|) \\ &\leq (2+o(1))\log_{k-1}(|X|) \end{aligned}$$

where $|X|$ is going to ∞ and D is a constant.

Here the definition of a "large girth" starts to make sense: since the girth cannot grow logarithmically too large with respect to the number of vertices, the criterion for having a "large girth" is a logarithmic lower bound, with log base $k-1$ specifically. Much effort is put into tightening the bound i.e. pushing the constant before $\log_{k-1}(|X|)$ as close to 2 as is possible: Erdös proved the existence of large girths with constant $C = 1$ in P. Erdös (1963), and Margulis gave the first explicit construction of such a graph with large girth and the constant $C = \frac{1}{3}\frac{\log 3}{\log(1+\sqrt{2})} \approx 0.415$ in Margulis (1982).

The graphs that Margulis found are examples of Cayley graphs, which are defined as follows:

Definition 4.4. Let G be a group, and let S be a nonempty, finite subset of G with $S = S^{-1}$. The **Cayley graph** $X(G,S)$ is the graph with vertex set $V = G$ and edge set

$$E = \{x, y : x, y \in G, \exists s \in S : y = xs\}.$$

Theorem 4.5 (a) $X(G,S)$ is a k-regular, vertex-transitive graph, where $k = |S|$.

(b) $X(G,S)$ is simple if and only if $1 \notin S$.

(c) $X(G,S)$ is connected if and only if S generates G .

Remark 4.6 — A **vertex-transitive** graph allows us to move a vertex to the position of any other vertex without altering the structure of the graph. Formally, a graph (V,E) is vertex-transitive if for any two vertices $v_1, v_2 \in V$, there exists a permutation of V, $f : (V,E) \to (V,E)$, which preserves its adjacency matrix and satisfies $f(v_1) = v_2$.

Proof.
(a) For any $x \in G, s \in S$, $xs \in G$ since S is a subset of G. Therefore, $X = X(G,S)$ is k-regular. X is vertex-transitive since for any $x_1, x_2 \in G$, there exists a left multiplication ϕ_g by the element $g \in G$ such that $\phi_g(x_1) = x_2$ and ϕ_g is a permutation on the vertices (this actually means that the action of G acting on X by left multiplication is transitive).
(b) The graph clearly has no multiple edges between vertices and has no loops if staying at one vertex is not allowed i.e. $1 \notin S$.
(c) The graph is connected if and only if every vertex is connected to $1 \in G$ by a path, which is equivalent to the fact that every member of G is a product of elements of S i.e. S generates G. □

Also, some results from group theory will be involved in the construction, which we present here.

Theorem 4.7

Let $\mathbb{Z}/q\mathbb{Z}$ be the field of integers modulo q, and let $\mathrm{GL}_2(q)$, $\mathrm{SL}_2(q)$ be the general linear and simple linear groups over $\mathbb{Z}/q\mathbb{Z}$.

(a) $|\mathrm{GL}_2(q)| = q(q-1)(q^2-1)$

(b) $|\mathrm{SL}_2(q)| = q(q^2-1)$

(c) $\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right\}$ generates $\mathrm{SL}_2(q)$.

Proof.

(a) There are (q^2-1) choices for the vector v in the first column, and there are q linearly dependent vectors with respect to v: $0, v, ..., (q-1)v$. Therefore, there are q^2-q choices for the second column, and $|\mathrm{GL}_2(q)| = q(q-1)(q^2-1)$.

(b) By the first isomorphism theorem 1.3 for the homomorphism of taking the determinant $\det : \mathrm{GL}_2(q) \to (\mathbb{Z}/q\mathbb{Z}) \setminus \{0\}$,

$$\mathrm{GL}_2(q)/\mathrm{SL}_2(q) \cong (\mathbb{Z}/q\mathbb{Z}) \setminus \{0\},$$

and therefore $|\mathrm{SL}_2(\mathbb{F}_q)| = |\mathrm{GL}_2(\mathbb{F}_q)|/(q-1) = q(q^2-1)$.

(c) The result is obtained by proving every element of the group is a product of the matrices

$$\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^m, \begin{pmatrix}1 & 0\\ n & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^n$$

for some $m, n \in \mathbb{Z}$. See lemma 3.2.1 of Davidoff et al. (2003) for a detailed proof.

□

There are two more important definitions, stated in the form that facilitates our construction:

Definition 4.8. A **word** over $X \subset G$ is a product $x_1 \dots x_n$ in G, $n \in \mathbb{N}$, where x_i or $x_i^{-1} \in X$. The word is reduced if for any $0 \le i \le n-1$, $x_i \neq x_{i+1}^{-1}$.

Definition 4.9. A group G is **free** if there exists a generating set $X \subset G$ such that every nonempty reduced word over X defines a non-identity element on G.

4.3 Construction

From here we begin our construction. Let $A = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$, $B = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$. For q an odd prime, let ϕ_q be the reduction of a matrix modulo q, i.e. reduction of each entry of the matrix modulo q. Let $A_q = \phi_q(A)$, $B_q = \phi_q(B)$, Let $S = \{A_q, B_q, A_q^{-1}, B_q^{-1}\}$. Then $X_q = X(\mathrm{SL}_2(q), S)$ is a Cayley graph.

We need to check our graph is indeed simple, connected, and regular so that finding its girth large is meaningful.

Theorem 4.10

X_q is a simple, connected, 4-regular Cayley graph with $|X_q| = q(q^2-1)$. Then $|X_q| \to \infty$ as $q \to \infty$.

Proof. By 4.5,x X is simple and 4-regular, and by 4.7(b), $|X| = |\mathrm{SL}_2(q)| = q(q^2-1)$. It remains to prove that X is connected i.e. S generates $\mathrm{SL}_2(q)$. Indeed, $A_q^{\frac{q+1}{2}} = \begin{pmatrix}1 & 2\cdot\frac{q+1}{2}\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, and similarly $B_q^{\frac{q+1}{2}} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$, where $\frac{q+1}{2} \in \mathbb{N}$. Therefore $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \in S$, and by 4.7(c), we have S generates $G = \mathrm{SL}_2(q)$. □

Let H be the group generated by $L = \{A, B, A^{-1}, B^{-1}\}$. The following lemma is important, with its proof using a method first developed by Fricke & Klein (1897) called the "ping pong lemma".

Lemma 4.11

H is a free group.

Proof. For any nonempty reduced word of H over L, it is of one of the 4 forms below:
(a) Starting and ending with a power of A:

$$A^{c_1}B^{c_2}\dots A^{c_{k_1}}$$

(b) Starting and ending with a power of B:

$$B^{d_1}A^{d_2}\dots B^{d_{k_2}}$$

(c) Starting with a power of A and ending with a power of B:

$$A^{e_1}B^{e_2}A^{e_3}\dots B^{e_{k_3}}$$

(d) Starting with a power of B and ending with a power of A:

$$B^{f_1}A^{f_2}B^{f_3}\dots A^{f_{k_4}}$$

where all the powers are integers.

We then define two disjoint sets in the Euclidean plane, as shown in Figure 1 (Davidoff et al. (2003)) where one can easily see that they are indeed disjoint:

$$E = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : |y| > |x| \right\}$$

$$F = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : |x| > |y| \right\}.$$

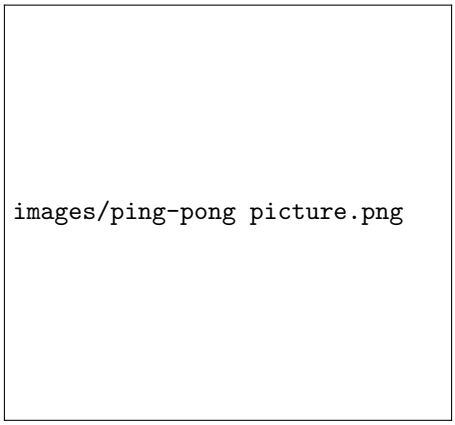

Figure 1: The Sets E and F on the Euclidean plane

Let elements of H act on these sets by their usual matrix multiplication, and we can observe, after simple calculations, that $A^k(E) \subset F$, $B^k(F) \subset E$. Therefore, we have $A^{c_1}B^{c_2}\dots A^{c_{k_1}}(E) \subset F$, $B^{d_1}A^{d_2}\dots B^{d_{k_2}}(F) \subset E$; hence, the reduced words of the first two kinds can never equal the identity given that I and J are disjoint. For reduced words in the form of $A^{e_1}B^{e_2}A^{e_3}\dots B^{e_{k_3}}$, we observe that $A^{-l}A^{e_1}B^{e_2}A^{e_3}\dots B^{e_{k_3}}A^l$ where $l \neq e_1$ is a reduced word of the first kind and $\neq 1$, and thus $A^{e_1}B^{e_2}A^{e_3}\ B^{e_{k_3}} \neq 1$. Similarly, $B^{f_1}A^{f_2}B^{f_3}\dots A^{f_{k_4}} \neq 1$. Therefore, every nonempty reduced word over L defines a non-identity element of H, and H is free. □

We still need some more knowledge about matrix norms. The **operator norm** of a matrix A is the norm

$$\|A\| = \sup\left\{ \frac{\|Ax\|}{\|x\|}, x \in \mathbb{R}^2 \setminus \{0\} \right\}$$

where the norm in the RHS is the usual vector norm. We have the following lemma, which can be proved using the definition of the operator norm, scalar products, and Cauchy-Schwarz inequality. A full proof is provided in the appendix of Davidoff et al. (2003). The lemma provides a way of calculating the operator norms as well as a crucial inequality between the norm of a matrix and its entries.

Lemma 4.12

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B \in M_2(\mathbb{R})$. Then:

(a) $\|A\| = \|A^T\|$

(b) $\|A\| = \|AA^T\|^{1/2}$

(c) $\|AB\| \leq \|A\| \, \|B\|$

(d) $\|A\| \geq \max\{|a|, |b|, |c|, |d|\}$

(e) If A is symmetric with eigenvalues λ_1, λ_2, then $\|A\| = \max\{|\lambda_1|, |\lambda_2|\}$.

With this lemma in mind, we can calculate $||A||$, where $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ as before. We have $A^T A = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$, and $\|A^T A\| = \max\{|\lambda_1|, |\lambda_2|\} = 3 + 2\sqrt{2}$ after calculating the eigenvalues λ_1, λ_2 of $A^T A$. Therefore, $\|A\| = \|AA^T\|^{1/2} = \|A^T A\|^{1/2} = 1 + \sqrt{2}$. Similarly, $\|B\| = \|A^{-1}\| = \|B^{-1}|| = 1 + \sqrt{2}$.

Here is the final theorem:

Theorem 4.13

The family of graphs X_q has a large girth. Precisely,

$$g(X_q) \geq \left(\tfrac{1}{3 \log_3(1+\sqrt{2})} + o(1) \right) \log_3 |X_q|.$$

Proof. Considering only a fixed q, let $g = g(X_q)$. By definition of a girth, there exists a circuit of length g in X_q. Since X_q is vertex-transitive, we can assume the circuit starts and ends with $1 \in G = \mathrm{SL}_2(\mathbb{Z}_q)$. The circuit can then be represented by the reduced word $p_1 p_2 \dots p_g$, where $p_i \in S$ and $p_1 p_2 \dots p_g = 1$. Let $\tilde{p}_i$ be an element of $L = \{A, B, A^{-1}, B^{-1}\}$ such that $\phi_q(\tilde{p}_i) = p_i$. Since ϕ_q is a homomorphism, the word $\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g$ over L in H is also reduced. However, since H is free by 4.11, $\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g \neq 1$.

Now we have $\phi_q(\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g) = p_1 p_2 \dots p_g = 1$ and thus $\phi_q(\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g - 1) = 0$ while $\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g \neq 1$. Therefore, the matrix $\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g - 1$ is divided by q i.e. its entries are all divided by q, but it is not a zero matrix. This means at least one entry is larger or equal to q in absolute value, and $\max\{|a|, |b|, |c|, |d|\} \geq q$, where a, b, c, d are entries of $\tilde{p}_1 \tilde{p}_2 \dots \tilde{p}_g - 1$. By 4.12(d), we have:

$$||\tilde{p}_1 \tilde{p}_2 ... \tilde{p}_g - 1|| \geq \max\{|a|, |b|, |c|, |d|\} \geq q$$
$$||\tilde{p}_1 \tilde{p}_2 ... \tilde{p}_g|| \geq \max\{|a|, |b|, |c|, |d|\} \geq q - 1$$

by the triangular inequality. By 4.12(c), we have $||\tilde{p}_1 \tilde{p}_2 ... \tilde{p}_g|| \leq ||\tilde{p}_1|| \, ||\tilde{p}_2|| ... ||\tilde{p}_g|| = (1 + \sqrt{2})^g$, from previous calculations. The inequality combining g and q emerges:

$$(1 + \sqrt{2})^g \geq q - 1$$
$$g \geq \frac{\log_3(q-1)}{\log_3(1+\sqrt{2})}$$

Since $|X_q| = q(q^2 - 1)$ by 4.10,

$$\log_3(q-1) = \frac{1}{3} \log_3(q-1)^3 = \frac{1}{3} \left(\log_3 \left(\frac{(q-1)^3}{|X_q|} \right) + \log_3 |X_q| \right)$$

where $\frac{1}{3} \log_3 \left(\frac{(q-1)^3}{|X_q|} \right) = o(1)$ as $q \to \infty$. Therefore,

$$g(X_q) \geq \tfrac{1}{3 \log_3(1+\sqrt{2})} \log_3 |X_q| + o(1) = \left(\tfrac{1}{3 \log_3(1+\sqrt{2})} + o(1) \right) \log_3 |X_q|$$

and the family of Cayley graphs has a large girth. □

4.4 Cayley graphs of simple groups

It is time to introduce expander graphs, or expanders, a family of highly connected sparse graphs.

Definition 4.14. Let $X = (V, E)$ be a finite, k-regular graph. For $0 < \epsilon \in \mathbb{R}$, X is **ϵ-expander** if for every $V \subset V$ such that $|Y| \leq \frac{1}{2}|V|$, we have

$$|\partial Y| \geq \epsilon |Y|$$

where ∂Y is the boundary of Y i.e. the set of vertices in V which are connected to some vertices of Y but are not in Y. A family of k-regular graphs is a **family of expanders** if all of them are ϵ-expanders for the same $\epsilon > 0$.

Remark 4.15 — A finite group G is an **expander**, or an ϵ-expander, if G has a generating set S for which the Cayley graph $X(G, S)$ is an ϵ-expander.

A family of finite groups $\{A_i\}_{i \in I}$ (where I is an index set) are **uniform expanders**, or expanders in a uniform way, if there exists $k \in \mathbb{N}$ and $\epsilon > 0$ such that any group A_i in $\{A_i\}_{i \in I}$ has a generating set S_i of k elements for which the Cayley graph $X(A_i, S_i)$ is an ϵ-expander (i.e. they are all expanders for the same k and ϵ, or their Cayley graphs form a family of expanders for the same k).

For simplicity, we will sometimes denote $\{A_i\}_{i \in I}$ as A_i, such as denoting $\{\mathrm{SL}(q)\}_{q \text{ prime}}$ as $\mathrm{SL}(q)$, which also applies to families of graphs.

We now present the groundbreaking theorem combining the "large girth" and expanding properties, due to Bourgain & Gamburd (2008).

Theorem 4.16

Suppose that for a fixed $k \geq 2$, $S_p = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ is a symmetric generating set for $\mathrm{SL}_2(\mathbb{F}_p)$ such that

$$g(X(\mathrm{SL}_2(\mathbb{F}_p), S_p)) \geq \tau \log_{2k} p$$

where τ is a fixed constant independent of p. Then $X(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ form a family of expanders for prime p.

The notations above are in line with 4.2 and 4.4. A detailed proof can be found in Bourgain & Gamburd (2008), using the character theory introduced in 1.3.

4.16 clearly holds for $X(\mathrm{SL}_2(p), S_p)$, too, as a result of the isomorphism between $\mathbb{F}_p$ and $\mathbb{Z}/p\mathbb{Z}$. From the proof of 4.13, we know $g \geq C \log_3(q-1)$, where $g = g(X(\mathrm{SL}_2(q), S_q))$ for some constant C and generating set S_q satisfying the conditions in 4.16. Simple manipulations give:

$$g(X(\mathrm{SL}_2(q), S_q)) \geq \frac{C}{\log_4(3)} \log_4(q) + f(q) \geq \tau \log_4(q)$$

where $f(q)$ is a bounded negative term going to 0, and τ is a constant independent of q. Therefore, applying 4.16 for $k = 2$ in the case of $X(\mathrm{SL}_2(q), S_q)$ in Margulis's construction, we obtain:

$$\text{for } |S_q| = 4,\ X(\mathrm{SL}_2(q), S_q) \text{ form a family of expanders.}$$

In other words, $\mathrm{SL}_2(q)$ are uniform expanders. This is by no means a by-product of some convoluted math games; in fact, it is a crucial ingredient for proving a famous conjecture on expanders that will be presented later. With a systematic approach, as presented in the corollary 2.3.2 of Tao (2015), we can only obtain an expander family of $X(\mathrm{SL}_d(q), S_q)$ for $d \geq 3$ because $\mathrm{SL}_2(\mathbb{R})$ does not have the *property* (T), whose definition is well explained in Tao (2015). Interestingly enough, the free group presented in 4.11 that rules out the *property* (T) for $\mathrm{SL}_2(\mathbb{R})$ (see lemma 2.3.3 in Tao (2015)) gives rise to Margulis's constructions, which, ultimately, still leads to the expanding property of $\mathrm{SL}_2(q)$ in its own way.

Not only does $\mathrm{SL}_2(q)$ deviate from the general case, but it also turns out to be more important and fundamental, as proven by Lubotzky (2012) in the following theorem:

Theorem 4.17

There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that if G is a finite simple group of Lie type of rank r, but not of Suzuki type, then it is a product of $f(r)$ copies of SL_2.

One can refer to Lubotzky (2012) for the definition of being a product of $f(r)$ copies of SL_2. A group theoretic proof also involving character theory can be found in Liebeck et al. (2011). Basically, with the above theorem and the fact that the bounded product of expander groups are uniform expanders (see Lubotzky (2012) and also Liebeck et al. (2011) for details), we deduce from $\mathrm{SL}_2(q)$ being uniform expanders (and thus all expanders) that finite simple Lie groups of bounded rank are uniform expanders. Together with the theorem mainly deduced from Nikolov (2007) that all classical groups of high rank are expanders, we have the following important theorem:

Theorem 4.18

There exists $0 < \epsilon \in \mathbb{R}$ such that if G is a finite simple group of Lie type, but not a Suzuki group, then G is a uniform expander.

4.18 leads to a remarkable theorem below, first fully proven in Lubotzky (2012):

Theorem 4.19

All non-abelian finite simple groups that are not Suzuki groups are uniform expanders.

By 3.1 introduced in the last section, 4.18 encompasses all the simple groups except for finitely many sporadic groups, for which the theorem is trivial, and the alternating groups, for which 4.19 holds due to Kassabov (2007).

After Suzuki groups are proven to be expanders by Breuillard et al. (2011), 4.19 turns out to be a key step to the final theorem of this section that had been an open conjecture for many years. A sketch of its proof is provided by Lubotzky (2012).

Theorem 4.20

There exists $k \in \mathbb{N}$ and $\epsilon > 0$ such that every non-abelian finite simple group G has a symmetric set of generators Σ of size $\leq k$ such that $X(G, \Sigma)$ is an ϵ-expander.

Math seems to also appreciate the delicacy of Margulis's construction, making it an indispensable part of the long journey to a beautiful theorem. This is how an explicit construction contributes to a general statement on simple groups as expanders: Cayley graphs consisting of $\mathrm{SL}_2(q)$ are shown to have large girth, magically implying the expanding properties of $\mathrm{SL}_2(q)$ that are then generalised to all non-Suzuki finite simple Lie groups; by the classification of finite simple groups and management of Suzuki groups, the final theorem follows.

References

Beachy, J. A. & Blair, W. D. (2006), *Abstract Algebra*, 3rd ed. edn, Waveland Press, Long Grove, IL.

Bourgain, J. & Gamburd, A. (2008), 'Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$', *Annals of Mathematics* **167**(2), 625–642.
URL: *http://annals.math.princeton.edu/2008/167-2/p07*

Brauer, R. & Fowler, K. A. (1955), 'On groups of even order', *Annals of Mathematics* .

Breuillard, E., Green, B. J. & Tao, T. (2011), 'Suzuki groups as expanders', *Groups, Geometry, and Dynamics* **5**(2), 281–299.
URL: *https://ems.press/doi/10.4171/ggd/128*

Conrad, K. (2020), 'Simplicity of $\mathrm{PSL}_n(F)$', `https://kconrad.math.uconn.edu/blurbs/grouptheory/PSLnsimple.pdf`. Accessed: 2024-06-14.

Davidoff, G. P., Sarnak, P. & Valette, A. (2003), *Elementary number theory, group theory, and Ramanujan graphs*, number 55 *in* 'London Mathematical Society student texts', Cambridge University Press, New York.

Dummit, D. S. & Foote, R. M. (2004), *Abstract Algebra*, 3rd ed. edn, John Wiley & Sons, Hoboken, NJ.

Feit, W. & Thompson, J. G. (1963), 'Solvability of groups of odd order', *Pacific Journal of Mathematics* .

Fricke, R. & Klein, F. (1897), *Vorlesungen über die Theorie der automorphen Functionen*, Leipzig B.G. Teubner.

Isaacs, I. M. (1994), *Algebra: A Graduate Course*, Books/Cole Publishing Company, Pacific Grove, CA.

James, G. & Liebeck, M. (2001), *Representations and Characters of Groups*, 2nd ed. edn, Cambridge University Press, Cambridge.

Kassabov, M. (2007), 'Symmetric groups and expander graphs', *Inventiones mathematicae* **170**(2), 327–354.
URL: *http://link.springer.com/10.1007/s00222-007-0065-y*

Liebeck, M. W., Nikolov, N. & Shalev, A. (2011), 'Groups of Lie type as products of SL2 subgroups', *Journal of Algebra* **326**(1), 201–207.
URL: *https://www.sciencedirect.com/science/article/pii/S0021869309000994*

Lubotzky, A. (2012), 'Expander graphs in pure and applied mathematics', *Bulletin of the American Mathematical Society* **49**(1), 113–162.
URL: *http://www.ams.org/jourcgi/jour-getitem?pii=S0273-0979-2011-01359-3*

Margulis, G. A. (1982), 'Explicit constructions of graphs without short cycles and low density codes', *Combinatorica* **2**(1), 71–78.
URL: *https://doi.org/10.1007/BF02579283*

Nikolov, N. (2007), 'A product decomposition for the classical quasisimple groups', *Journal of Group Theory* **10**(1).
URL: *https://www.degruyter.com/document/doi/10.1515/JGT.2007.005/html*

P. Erdös, H. S. (1963), 'Reguläre graphen gegebener taillenweite mit minimaler knollenzahh', *Wiss. Z. Univ. Halle-Willenberg Math. Nat. R.* **12**, 251–258.

Robinson, D. J. (1996), *A Course in a Theory of Groups*, 2nd ed. edn, Springer-Verlag New York, Inc.

Tao, T. (2015), *Expansion in finite simple groups of Lie type*, Vol. 164 of *Graduate studies in mathematics*, American Mathematical Society, Providence, Rhode Island.

Wilson, R. A. (2009), *The Finite Simple Groups*, Springer London.

Wise, J. (2015), `https://math.colorado.edu/~jonathan.wise/teaching/math6130-fall-2015/size90.pdf`. Accessed: 2024-06-14.