Introduction to finite simple groups

808017424794512875886459904961710757005754368000000000

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

Contents

Literature

◦ R. Wilson: The finite simple groups, Graduate Texts in Mathematics 251, Springer, 2009.

◦ J. Conway, R. Curtis, R. Parker, S. Norton, R. Wilson: Atlas of finite groups, Clarendon Press Oxford, 1985/2004.

◦ P. Cameron: Permutation groups, LMS Student Texts 45, Cambridge, 1999.

◦ D. Taylor: The geometry of the classical groups, Heldermann, 1992.

◦ R. Carter: Simple groups of Lie type, Wiley, 1972/1989.

◦ M. Geck: An introduction to algebraic geometry and algebraic groups, Oxford, 2003.

◦ R. Griess: Twelve sporadic groups, Springer Monographs in Mathematics, 1989.

- **Aim:** Explain the statement of the CFSG:

Classification of finite simple groups (CFSG)

- Cyclic groups of prime order C_p; p a prime.
- Alternating groups $\mathcal{A}_n$; $n \geq 5$.
- Finite groups of Lie type:
  - Classical groups; q a prime power:

    Linear groups $\mathrm{PSL}_n(q)$; $n \geq 2$, $(n, q) \neq (2, 2), (2, 3)$.

    Unitary groups $\mathrm{PSU}_n(q^2)$; $n \geq 3$, $(n, q) \neq (3, 2)$.

    Symplectic groups $\mathrm{PSp}_{2n}(q)$; $n \geq 2$, $(n, q) \neq (2, 2)$.

    Odd-dimensional orthogonal groups $\Omega_{2n+1}(q)$; $n \geq 3$, q odd.

    Even-dimensional orthogonal groups $\mathrm{P}\Omega^+_{2n}(q)$, $\mathrm{P}\Omega^-_{2n}(q)$; $n \geq 4$.
  - Exceptional groups; q a prime power, $f \geq 1$:

    $E_6(q)$. $E_7(q)$. $E_8(q)$. $F_4(q)$. $G_2(q)$; $q \neq 2$.

    Steinberg groups ${}^2E_6(q^2)$. Steinberg triality groups ${}^3D_4(q^3)$.

    Suzuki groups ${}^2B_2(2^{2f+1})$. Small Ree groups ${}^2G_2(3^{2f+1})$.

    Large Ree groups ${}^2F_4(2^{2f+1})$, Tits group ${}^2F_4(2)'$.
- 26 Sporadic groups: ...

Classification of finite simple groups (CFSG), II

- Sporadic groups:
  - Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.
  - Leech lattice groups:

    Conway groups Co_1, Co_2, Co_3.

    McLaughlin group McL. Higman-Sims group HS.

    Suzuki group Suz. Hall-Janko group J_2.
  - Fischer groups Fi_{22}, Fi_{23}, Fi'_{24}.
  - Monstrous groups:

    Fischer-Griess Monster M.

    Baby Monster B. Thompson group Th.

    Harada-Norton group HN. Held group He.
  - Pariahs:

    Janko groups J_1, J_3, J_4. O'Nan group ON.

    Lyons group Ly. Rudvalis group Ru.

- Repetitions:

∘ $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong \mathcal{A}_5$; $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$;

∘ $\mathrm{PSL}_2(9) \cong \mathcal{A}_6$; $\mathrm{PSL}_4(2) \cong \mathcal{A}_8$;

∘ $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$.

Composition series

∘ Let G be a finite group.

• G is called **simple** if G is non-trivial and does not have any proper non-trivial normal subgroup.

• **Composition series:**

∘ G has a **composition series** of **length** $n \in \mathbb{N}_0$

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

∘ where $G_{i-1} \lhd G_i$ such that G_i/G_{i-1} is simple, for all $i \in \{1, \ldots, n\}$.

• **Jordan-Hölder Theorem:**

∘ The set of **composition factors** G_i/G_{i-1}, counting multiplicities, is independent of the choice of a composition series.

• G is called **soluble** if all composition factors G_i/G_{i-1} are abelian, or equivalently cyclic of prime order.

• **Examples:**

∘ $\{1\} \lhd \mathcal{S}_2$ with composition factors C_2.

∘ $\{1\} \lhd \mathcal{A}_3 \lhd \mathcal{S}_3$ with composition factors C_2, C_3.

∘ $\{1\} \lhd C_2 \lhd V_4 \lhd \mathcal{A}_4 \lhd \mathcal{S}_4$ with composition factors C_2, C_2, C_2, C_3.

∘ $\{1\} \lhd \mathcal{A}_5 \lhd \mathcal{S}_5$ with composition factors $\mathcal{A}_5, C_2$.

Some history

• Abel's Theorem:

∘ The **Galois group** of the general polynomial equation of degree $n \in \mathbb{N}$ over any field is isomorphic to the symmmetric group $\mathcal{S}_n$.

∘ The general polynomial equation of degree $n \in \mathbb{N}$ over a field of characteristic 0 is **solvable by radicals** if and only if its Galois group is soluble, that is if and only if $n \leq 4$.

∘ Galois [∼1830]: $\mathcal{A}_n$ simple for $n \geq 5$, $\mathrm{PSL}_2(p)$ for p a prime.

∘ Jordan [1870]: 'Traité des substitutions', $\mathrm{PSL}_n(p)$.

∘ **Sylow Theorems** [1872]: the first classification tool.

∘ Mathieu [1861/1873]: the simple Mathieu groups.

∘ Killing [∼1890]: classification of complex simple Lie algebras.

∘ Dickson [∼1900]: finite field analoga of the classical Lie groups.

∘ Chevalley [1955]: uniform construction of
the classical and exceptional finite groups of Lie type.

∘ Ree, Steinberg, Suzuki, Tits [∼1960]:
twisted classical and exceptional finite groups of Lie type.

∘ ∼1960: common belief is that all finite simple groups are known.

Some history, II

○ Brauer, Fowler [1955]:
Given $n \in \mathbb{N}$, there are at most finitely many simple groups containing an involution with centraliser of order n.

○ **Feit-Thompson Theorem [1963]:**
Any finite group of odd order is soluble.

○ **Brauer program:** Hence any non-abelian finite simple group contains an involution, thus consider centralisers of central involutions and prove completeness of classification by induction.

○ Janko [1964]: (the first since almost a century)
sporadic group J_1 with involution centraliser $C_2 \times \mathcal{A}_5$.

○ Thompson [1968]: classification of minimal simple groups.

○ Janko [1975]: the last sporadic group J_4.

○ ∼1980: common belief is that CFSG is proved.

○ Gorenstein, Lyons, Solomon [≥1994]:
revision project of the proof of CFSG.

○ Aschbacher, Smith [2004]:
the quasithin case, completing the proof of CFSG.

• Do we really believe that the **Four-Colour Theorem**, or **Fermat's Last Theorem**, or the **Poincaré Conjecture**, or the **CFSG** are proved?

Applications of CFSG

• Let T be a non-abelian finite simple group.

◦ Then $Z(T) = \{1\}$ implies $T \cong \mathrm{Inn}(T) \trianglelefteq \mathrm{Aut}(T)$.

• A group G such that $T \leq G \leq \mathrm{Aut}(T)$ is called **almost simple**.

• A perfect group G such that $G/Z(G) \cong T$ is called **quasi-simple**.

• **Schreier's Conjecture:**

◦ The outer automorphism group $\mathrm{Out}(T) := \mathrm{Aut}(T)/\mathrm{Inn}(T)$ of any finite simple group T is soluble.

• **Proof:** by inspection; in all cases $\mathrm{Out}(T)$ is 'very small'. $\sharp$

• **Theorem:** Let $N \trianglelefteq G$ such that $\gcd(|N|, |G/N|) = 1$. Then all complements of N in G are conjugate.

• **Proof:** uses the Feit-Thompson Theorem; or alternatively:

◦ Let $G = N\colon H$ be a minimal counterexample.

◦ Easy: N is non-abelian simple and $C_G(N) = \{1\}$

◦ Hence $G \cong G/C_G(N) \leq \mathrm{Aut}(N)$ such that $N \leq \mathrm{Inn}(N)$.

◦ Thus $G/N \leq \mathrm{Out}(N)$ is soluble.

◦ Hence the assertion follows from **Zassenhaus's Theorem**. $\sharp$

Applications of CFSG, II

• **Multiply-transitive permutation groups:**

◦ The finite 2-transitive groups are explicitly known.

◦ The only finite 6-transitive groups are symmetric and alternating.

◦ The only finite 4-transitive groups are symmetric and alternating, and the Mathieu groups M_{11}, M_{12}, M_{23}, and M_{24}.

• **Proof:**

◦ **Burnside's Theorem:** A minimal non-trivial normal subgroup of a finite 2-transitive group is either elementary-abelian and regular, or simple and primitive.

◦ Hence a 2-transitive group is either **affine** or almost simple:

◦ Huppert and Hering: soluble and insoluble affine cases;

◦ Maillet, Curtis, Kantor, Seitz, Howlett:
almost simple cases.

◦ The higher transitive groups are then found by inspection. ♯

• **Example:**

◦ $\mathrm{ASL}_d(q) \cong [q^d]\colon \mathrm{SL}_d(q)$, where q is a prime power and $n = q^d$.

◦ $\mathrm{PSL}_d(q)$, where q is a prime power, $d \geq 2$, and $n = \frac{q^d-1}{q-1}$.

Symmetric and alternating groups

∘ Let $n \in \mathbb{N}_0$.

• Let $\mathcal{S}_n$ be the **symmetric group** on $\{1, \ldots, n\}$.

∘ Let $\mathrm{sgn}\colon \mathcal{S}_n \to \{\pm 1\} \cong C_2$ be the **sign representation**.

∘ Let $\mathcal{A}_n := \ker(\mathrm{sgn}) \trianglelefteq \mathcal{S}_n$ be the **alternating group** on $\{1, \ldots, n\}$;

∘ the elements of $\mathcal{A}_n$ are called **even permutations**,

∘ the elements of $\mathcal{S}_n \setminus \mathcal{A}_n$ are called **odd** permutations.

• The **cycle type** of a permutation is the partition of n indicating the lengths of its distinct **cycles**, counting multiplicities.

∘ **Example:** The identity has cycle type $[1^n]$,
a 2**-cycle** or **transposition** has cycle type $[2, 1^{n-2}]$,
a 3**-cycle** has cycle type $[3, 1^{n-3}]$.

∘ A permutation is even if and only if it has an even number of cycles of even length.

• The **conjugacy classes** of $\mathcal{S}_n$ are parametrised by cycle types.

∘ A permutation is **centralised** by no odd permutation if and only if it is the product of cycles of distinct odd lengths.

∘ Hence the **orbit-stabiliser theorem** implies:

∘ A conjugacy class of $\mathcal{S}_n$ contained in $\mathcal{A}_n$ splits into two conjugacy classes of $\mathcal{A}_n$ if and only if its cycle type has pairwise distinct odd parts, otherwise it is a single conjugacy class of $\mathcal{A}_n$.

Simplicity of $\mathcal{A}_n$

• **Theorem:** Let $n \geq 5$. Then $\mathcal{A}_n$ is simple.

• **Proof:** by induction on n; let $\{1\} \neq N \trianglelefteq \mathcal{A}_n$.

• Let $n = 5$. Then N is a union of conjugacy classes.

∘ The cycle types of even permutations are $[1^5], [3, 1^2], [2^2, 1], [5]$, where only type $[5]$ splits into two conjugacy classes.

∘ The conjugacy class lengths are $1, 20, 15, 12, 12$, respectively.

∘ No sub-sum of these, strictly including 1, divides 60; thus $N = \mathcal{A}_n$.

• Let $n > 5$. Then $\mathcal{A}_{n-1} = \mathrm{Stab}_{\mathcal{A}_n}(n)$ is simple.

∘ $N \cap \mathcal{A}_{n-1} \trianglelefteq \mathcal{A}_{n-1}$, hence **i)** $\mathcal{A}_{n-1} \leq N$ or **ii)** $N \cap \mathcal{A}_{n-1} = \{1\}$:

i) Then N contains all elements of cycle type $[3, 1^{n-3}]$.

∘ Any even permutation is a product of 3-cycles; thus $N = \mathcal{A}_n$.

ii) Then any non-trivial element of N acts **fixed-point-free**.

∘ If $1^\sigma = 1^\tau$ for $\sigma, \tau \in N$, then $\sigma\tau^{-1} \in N \cap \mathcal{A}_{n-1} = \{1\}$.

∘ Thus $|N| \leq n$.

∘ But $\mathcal{A}_n$ does not have a non-trivial conjugacy class with fewer than n elements, a contradiction. ♯

Automorphisms of $\mathcal{A}_n$

○ Let $n \geq 4$. Then $Z(\mathcal{A}_n) = \{1\}$, hence $\mathcal{A}_n \cong \mathrm{Inn}(\mathcal{A}_n) \trianglelefteq \mathrm{Aut}(\mathcal{A}_n)$;

○ and $\mathcal{S}_n$ acts faithfully by conjugation, hence $\mathcal{S}_n \leq \mathrm{Aut}(\mathcal{A}_n)$.

• **Theorem:** Let $n \geq 7$. Then $\mathrm{Aut}(\mathcal{A}_n) = \mathcal{S}_n$.

• **Proof:** [C. Parker]

○ $\mathcal{A}_n$ being simple, it cannot possess a proper subgroup of index $k < n$, since otherwise there would be an injective map $\mathcal{A}_n \to \mathcal{A}_k$.

• We show $(*)$: If $\mathcal{A}_{n-1} \cong H < \mathcal{A}_n$, then $H = \mathrm{Stab}_{\mathcal{A}_n}(i)$ for some i.

○ Let $n = 7$. H cannot have a non-trivial orbit of less than 6 points.

If H is not a point stabiliser, then H acts transitively on $\{1, \ldots, 7\}$.

This is a contradiction since $7 \not| \; |H| = |\mathcal{A}_6|$, proving $(*)$ for $n = 7$.

○ Let $n \geq 9$. A '3-cycle' of H centralises a group $\cong \mathcal{A}_{n-4}$.

Since $n - 4 \geq 5$ the latter has an orbit of at least $n - 4$ points.

Thus a '3-cycle' of H moves at most 4 points, thus is a 3-cycle of $\mathcal{A}_n$.

○ Let $n = 8$. A '3-cycle' of H centralises a group $\cong \mathcal{A}_4$.

Hence there is a V_4 centralising the '3-cycle'.

The elements of $\mathcal{A}_8$ of cycle type $[3^2, 1^2]$ do not centralise a V_4.

Hence a '3-cycle' of H is a 3-cycle of $\mathcal{A}_8$.

Automorphisms of $\mathcal{A}_n$, II

- Thus for $n \geq 8$ the '3-cycles' of H map to 3-cycles of $\mathcal{A}_n$.
- For pairs of 3-cycles we have $\langle (a,b,c),(a,b,d) \rangle \cong \mathcal{A}_4$.
- Hence the subgroup

$$H \cong \mathcal{A}_{n-1} = \langle (1,2,3), \ldots, (1,2,n-1) \rangle$$

maps to a subgroup

$$\langle (a,b,c_1), \ldots, (a,b,c_{n-3}) \rangle \leq \mathcal{A}_n.$$

- The latter moves $n-1$ points.
- Hence $H \leq \mathrm{Stab}_{\mathcal{A}_n}(i)$ for some i, proving $(*)$ for $n \geq 8$.

- Now:
- Any automorphism permutes the subgroups isomorphic to $\mathcal{A}_{n-1}$.
- These subgroups are in natural bijection with $\{1, \ldots, n\}$.
- Hence any automorphism induces a permutation of $\{1, \ldots, n\}$. $\sharp$

- We have $\mathrm{Aut}(\mathcal{A}_n) = \mathcal{S}_n$ for $n \in \{4,5\}$.
- We have $\mathrm{Aut}(\mathcal{A}_6) \cong \mathcal{A}_6.2^2$.
- $\mathcal{A}_6$ has two conjugacy classes of subgroups isomorphic to $\mathcal{A}_5$.

Schur covers of $\mathcal{S}_n$ and $\mathcal{A}_n$

• A finite group H such that $Z(H) \leq H'$ and $H/Z(H) \cong G$ is called an $|Z(H)|$**-fold cover** of G.

○ Two maximal covers of G are **isoclinic**.

○ If G is perfect, its unique maximal cover is a **universal cover**.

• $\mathcal{A}_n$ has maximal 2-fold covers $\widetilde{\mathcal{A}}_n = 2.\mathcal{A}_n$, for $n \geq 4$,

○ except for $n \in \{6, 7\}$ where it has maximal 6-fold covers $6.\mathcal{A}_n$.

• $\mathcal{S}_n$ has two maximal 2-fold covers $\widetilde{\mathcal{S}}_n$ and $\widehat{\mathcal{S}}_n$, for $n \geq 4$,

○ both of shape $2.\mathcal{S}_n$, but we have $\widetilde{\mathcal{S}}_n \cong \widehat{\mathcal{S}}_n$ if and only if $n = 6$.

• The **Coxeter presentation** of $\mathcal{S}_n$, where $n \in \mathbb{N}$, is given as

$$\mathcal{S}_n \cong \langle s_1, \ldots, s_{n-1} \mid s_i^2 = (s_i s_{i+1})^3 = (s_i s_j)^2 = 1 \text{ for } |i-j| \geq 2 \rangle,$$

○ where **adjacent transpositions** $(i, i+1) \mapsto s_i$.

• For $\widetilde{\mathcal{S}}_n$ and $\widehat{\mathcal{S}}_n$, where $n \geq 4$, we have [Schur, 1911]:

$$\widetilde{\mathcal{S}}_n := \langle s_1, \ldots, s_{n-1}, z \mid z^2 = 1, \mathbf{s_i^2} = (\mathbf{s_i s_{i+1}})^\mathbf{3} = \mathbf{z}, (s_i s_j)^2 = z \rangle$$

$$\widehat{\mathcal{S}}_n := \langle s_1, \ldots, s_{n-1}, z \mid z^2 = 1, \mathbf{s_i^2} = (\mathbf{s_i z})^\mathbf{2} = (\mathbf{s_i s_{i+1}})^\mathbf{3} = \mathbf{1}, (s_i s_j)^2 = z \rangle$$

Subgroups of $\mathcal{S}_n$

∘ Describing all the subgroups of $\mathcal{S}_n$, for all $n \in \mathbb{N}_0$, is by

∘ **Cayley's Theorem** equivalent to classifying all finite groups:

∘ **hopeless**.

∘ But there are certainly are interesting prominent subgroups:

• for example, intransitive subgroups.

• Partition the set of $n = km$ points into m **blocks** of size k.

∘ The **wreath product** $\mathcal{S}_k \wr \mathcal{S}_m \cong \mathcal{S}_k^m : \mathcal{S}_m$ acts on this partition,

∘ where the **base group** $\mathcal{S}_k^m = \mathcal{S}_k \times \cdots \times \mathcal{S}_k$ consists of permutations of the various blocks,

∘ and the wreathing $\mathcal{S}_m$ permutes the blocks.

∘ $\mathcal{S}_k \wr \mathcal{S}_m < \mathcal{S}_n$ is an imprimitive transitive subgroup, for $k, m \geq 2$.

• $\mathcal{S}_k \wr \mathcal{S}_m$ acts on $\{1, \ldots, k\}^m$ by the **product action**, $n = k^m$,

∘ where $[\pi_1, \ldots, \pi_m] \in \mathcal{S}_k^m$ acts by $[a_1, \ldots, a_m] \mapsto [a_1^{\pi_1}, \ldots, a_m^{\pi_m}]$,

∘ and $\pi^{-1} \in \mathcal{S}_m$ acts by $[a_1, \ldots, a_m] \mapsto [a_{1^\pi}, \ldots, a_{m^\pi}]$.

∘ $\mathcal{S}_k \wr \mathcal{S}_m < \mathcal{S}_n$ is a primitive subgroup, for $k \geq 3$ and $m \geq 2$.

Maximal subgroups of $\mathcal{S}_n$

◦ One might try to describe the **maximal** subgroups of $\mathcal{S}_n$;

◦ the maximal subgroups of $\mathcal{A}_n$ are then obtained by intersection:

• **O'Nan-Scott Theorem [1979]:** Any proper subgroup of $\mathcal{S}_n$ different from $\mathcal{A}_n$ is contained in one of the following subgroups:

i) an intransitive group $\mathcal{S}_k \times \mathcal{S}_m$, where $n = k + m$;

ii) an imprimitive transitive group $\mathcal{S}_k \wr \mathcal{S}_m$, where $n = km$;

iii) a primitive wreath product $\mathcal{S}_k \wr \mathcal{S}_m$, where $n = k^m$;

iv) an affine group $\mathrm{AGL}_d(p) \cong p^d \colon \mathrm{GL}_d(p)$, where $n = p^d$;

v) a **diagonal type** group

$$T^m.(\mathrm{Out}(T) \times \mathcal{S}_m) \cong (T \wr \mathcal{S}_m).\mathrm{Out}(T),$$

where T is a non-abelian simple group,

acting on the cosets of a subgroup of index $n = |T|^{m-1}$, of shape

$$\Delta(T).(\mathrm{Out}(T) \times \mathcal{S}_m) \cong \mathrm{Aut}(T) \times \mathcal{S}_m;$$

vi) an almost simple group,

acting on the cosets of a maximal subgroup of index n.

◦ Describing the groups in class **vi)** requires complete knowledge of the maximal subgroups of all almost simple groups:

◦ **reducing an impossible problem to an even harder one**.

Linear groups

- ○ Let $\mathbb{F}_q$ be the field with $q = p^f$ elements, p a prime, $f \in \mathbb{N}$, $n \in \mathbb{N}$.

- • **General linear group** $\mathrm{GL}_n(q) := \{g \in \mathbb{F}_q^{n\times n}; \det(g) \neq 0\}$
- ○ Counting the number of ordered $\mathbb{F}_q$-bases of $\mathbb{F}_q^n$:
- ○ $|\mathrm{GL}_n(q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}) = q^{\binom{n}{2}} \cdot \prod_{i=1}^n (q^i - 1)$
- ○ Viewing q as an indeterminate,
- ○ this is an **order polyomial** in $\mathbb{Z}[q]$,
- ○ whose irreducible factors are q and cyclotomic polynomials.

- • **Special linear group** $\mathrm{SL}_n(q) := \{g \in \mathrm{GL}_n(q); \det(g) = 1\}$

- • **Projective** general linear group $\mathrm{PGL}_n(q) := \mathrm{GL}_n(q)/Z(\mathrm{GL}_n(q))$,
- ○ where $Z(\mathrm{GL}_n(q)) = \mathbb{F}_q^* \cdot E_n \cong C_{q-1}$.
- ○ $|\mathrm{SL}_n(q)| = |\mathrm{PGL}_n(q)| = \frac{1}{q-1} \cdot |\mathrm{GL}_n(q)|$

- • **Projective** special linear group $\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$,
- ○ where $Z(\mathrm{SL}_n(q)) = \{\lambda \cdot E_n; \lambda^n = 1\} \cong C_{\gcd(n,q-1)}$.
- ○ $|\mathrm{PSL}_n(q)| = \frac{1}{\gcd(n,q-1)} \cdot |\mathrm{SL}_n(q)| = \frac{1}{\gcd(n,q-1)} \cdot \frac{1}{q-1} \cdot |\mathrm{GL}_n(q)|$

Simplicity of $\mathbf{PSL}_n(q)$

- $\mathrm{PSL}_2(2) \cong \mathrm{GL}_2(2) \cong \mathcal{S}_3$:

○ $\mathrm{GL}_2(2)$ acts 2-transitively on the three vectors in $\mathbb{F}_2^2 \setminus \{0\}$.

- $\mathrm{PSL}_2(3) \cong \mathcal{A}_4$:

○ $\mathrm{GL}_2(3)$ acts on the four 1-dimensional $\mathbb{F}_3$-subspaces of $\mathbb{F}_3^2$,

○ the action is 2-transitive, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ fixes the standard $\mathbb{F}_3$-basis,

○ hence $\mathrm{GL}_2(3) \to \mathcal{S}_4$, with kernel $Z(\mathrm{GL}_2(3)) \cong C_2$,

○ thus $\mathrm{PGL}_2(3) \cong \mathcal{S}_4$ and $\mathrm{PSL}_2(3) \cong \mathcal{A}_4$.

○ Note: $\mathrm{GL}_2(3) \cong \widetilde{\mathcal{S}}_4$ and $\mathrm{SL}_2(3) \cong \widetilde{\mathcal{A}}_4$.

- **Theorem:** Let $n \geq 2$ and $(n, q) \neq (2, 2), (2, 3)$.

Then $\mathrm{PSL}_n(q)$ is simple.

- **Proof:**

○ $G := \mathrm{SL}_n(q)$ acts on the set of 1-dimensional subspaces of $\mathbb{F}_q^n$,

○ yielding a 2-transitive, hence primitive, action of $\mathrm{PSL}_n(q)$.

○ Let $x := \langle [1, 0, \ldots, 0] \rangle_{\mathbb{F}_q}$ and $H := \mathrm{Stab}_G(x)$,

○ then

$$H = \left\{ \begin{bmatrix} \lambda & 0_{n-1} \\ * & h \end{bmatrix} \in G; \lambda \in \mathbb{F}_q^*, h \in \mathrm{GL}_{n-1}(q), \lambda \cdot \det(h) = 1 \right\}.$$

Simplicity of $\mathbf{PSL}_n(q)$, II

∘ Use Iwasawa's Criterion:

∘ Let

$$A := \left\{ \begin{bmatrix} 1 & 0_{n-1} \\ * & E_{n-1} \end{bmatrix} \in H \right\},$$

∘ then $A \lhd H$ is abelian, consisting of **transvections**,

∘ that is $g \in G$ such that $\operatorname{rk}(g - E_n) = 1$ and $\operatorname{rk}((g - E_n)^2) = 0$.

∘ **Jordan normal form theorem** implies that

• any transvection is G-conjugate to some element of A.

• G is generated by transvections:

∘ Any $g \in G$ can be reduced to E_n by a sequence of elementary row operations of the form '$r_i \mapsto r_i + \lambda r_j$',

∘ that is multiplying g from the right with a series of transvections.

• G is perfect:

∘ For $n \geq 3$ any transvection is a commutator:

$$\left[\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{bmatrix} \right] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\lambda & 0 & 1 \end{bmatrix}$$

∘ For $n = 2$ and $q \geq 4$ there is $\lambda \in \mathbb{F}_q^*$ such that $\lambda^2 \neq 1$, then

$$\left[\begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}, \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \right] = \begin{bmatrix} 1 & 0 \\ \beta(\lambda^2 - 1) & 1 \end{bmatrix}$$

is an arbitrary element of A. ♯

Iwasawa's Criterion

- **Theorem: [Iwasawa, 1941]**
- ∘ Let G be a finite group, acting primitively on a set Ω,
- ∘ let $H := \mathrm{Stab}_G(x) < G$ for some $x \in \Omega$,
- ∘ and let $A \trianglelefteq H$ such that $\langle A^g; g \in G \rangle = G$.
- Then for any $N \trianglelefteq G$ we have
- ∘ either $N \leq \mathrm{Stab}_G(\Omega) = \bigcap_{g \in G} H^g \lhd G$,
- ∘ or G/N is isomorphic to a quotient of A.
- In particular:
- ∘ if A is abelian and G is perfect, then $G/\mathrm{Stab}_G(\Omega)$ is simple.

- **Proof:**
- ∘ We may assume that $N \not\leq H$.
- ∘ $H < G$ being maximal implies $G = HN$, thus
- ∘ any $g \in G$ can be written as $g = hn$, where $h \in H$ and $n \in N$.
- ∘ Hence $A^g = A^{hn} = A^n \leq AN$, for any $g \in G$,
- ∘ implying $G = \langle A^g; g \in G \rangle = AN$,
- ∘ thus $G/N = AN/N \cong A/(A \cap N)$. ♯

- ∘ **Despite its simplicity this is astonishingly powerful.**
- ∘ **Exercise:** Use it to prove the simplicity of $\mathcal{A}_n$, for $n \geq 5$.

Automorphisms of $\mathbf{SL}_n(q)$

- **Diagonal automorphisms:**

◦ induced by conjugation with diagonal matrices,

◦ that is by the conjugation action of $\mathrm{GL}_n(q)$.

◦ $\mathrm{GL}_n(q)/\mathrm{SL}_n(q) \cong C_{q-1}$, $\mathrm{PGL}_n(q)/\mathrm{PSL}_n(q) \cong C_{\gcd(n,q-1)}$

- **Field automorphisms:**

◦ induced by the **Frobenius automorphism** $\varphi_p \colon \lambda \mapsto \lambda^p$ of $\mathbb{F}_q$,

◦ where $q = p^f$, hence $\langle \varphi_p \rangle \cong C_f$.

◦ **Semilinear** groups

$$\Gamma\mathrm{L}_n(q) := \mathrm{GL}_n(q) : \langle \varphi_p \rangle, \quad \mathrm{P\Gamma L}_n(q) := \mathrm{PGL}_n(q) : \langle \varphi_p \rangle,$$

$$\Sigma\mathrm{L}_n(q) := \mathrm{SL}_n(q) : \langle \varphi_p \rangle, \quad \mathrm{P\Sigma L}_n(q) := \mathrm{PSL}_n(q) : \langle \varphi_p \rangle.$$

- **Graph automorphisms:**

◦ induced by a graph automorphism of the **Dynkin diagram**.

◦ **Duality** $\mathrm{GL}_n(q) \to \mathrm{GL}_n(q) \colon g \mapsto g^{-\mathrm{tr}}$;

◦ induces duality on $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$.

◦ Note: duality is not inner for $n \geq 3$.

- These are all the ‘outer’ automorphisms;

◦ in particular the outer automorphism group is soluble.

Covers of $\mathbf{PSL}_n(q)$

- $\mathrm{PSL}_n(q)$ has $\gcd(n, q-1)$-fold universal cover

$$\mathrm{SL}_n(q) \cong C_{\gcd(n,q-1)}.\mathrm{PSL}_n(q),$$

- except:

○ $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong \mathcal{A}_5$ has universal cover $2.\mathrm{PSL}_2(4)$;

○ $\mathrm{PSL}_2(9) \cong \mathcal{A}_6$ has universal cover $6.\mathrm{PSL}_2(9)$;

○ $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ has universal cover $2.\mathrm{PSL}_3(2)$;

○ $\mathrm{PSL}_4(2) \cong \mathcal{A}_8$ has universal cover $2.\mathrm{PSL}_4(2)$;

○ $\mathrm{PSL}_3(4)$ has universal cover $(3 \times 4^2).\mathrm{PSL}_3(4)$.

- Note:

○ generic universal covers have order coprime to the **defining characteristic** p of the Lie type group,

○ while exceptional parts of universal covers are p-groups.

Subgroups of $\mathbf{GL}_n(q)$

- **Borel subgroup** $B := \{g; g \text{ lower triangular}\} < G := \mathrm{GL}_n(q)$,
- ◦ the stabiliser of a **maximal flag** of $\mathbb{F}_q^n$;
- **monomial subgroup** $N := \{g \in G; g \text{ monomial}\} < G$;
- **maximal split torus** $T := B \cap N = \{g \in G; g \text{ diagonal}\}$,
- ◦ $T \cong C_{q-1}^n$, and $N = N_G(T)$ for $q \geq 3$;
- **unipotent subgroup** $U := \{g \in G; g \text{ lower unitriangular}\} \trianglelefteq B$,
- ◦ $U \in \mathrm{Syl}_p(G)$, and $B = U : T$ **split**;
- **Weyl group** $W := N/T \cong \mathcal{S}_n$, via $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto (1, 2)$,
- ◦ a **crystallographic real reflection group**:
- ◦ the adjacent transpositions act as **reflections**,
- ◦ that is $\dim_{\mathbb{Q}}(\ker(g - E_n)) = n - 1$ and $\dim_{\mathbb{Q}}(\ker(g + E_n)) = 1$.
- Flag stabilisers are called **parabolic subgroups**;
- ◦ $B \leq P = \begin{bmatrix} \mathrm{GL}_k(q) & 0 \\ * & \mathrm{GL}_{n-k}(q) \end{bmatrix} = U_P : L_P$ **maximal parabolic**,
- ◦ with **unipotent radical** $U_P = \begin{bmatrix} E_k & 0 \\ * & E_{n-k} \end{bmatrix}$, and
- ◦ **Levi** subgroup $L_P = \begin{bmatrix} \mathrm{GL}_k(q) & 0 \\ 0 & \mathrm{GL}_{n-k}(q) \end{bmatrix} \cong \mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$.

- Axiomatic: BN**-pairs** [Tits, 1962]

Maximal subgroups $\mathbf{GL}_n(q)$

• **Aschbacher-Dynkin Theorem: [1984/1952]**

∘ Any proper subgroup of $\mathrm{GL}_n(q)$ different from $\mathrm{SL}_n(q)$ is contained in one of the following subgroups:

i) a **reducible** group $q^{km}: (\mathrm{GL}_k(q) \times \mathrm{GL}_m(q))$, where $n = k + m$,

the stabiliser of a k-dimensional $\mathbb{F}_q$-subspace;

ii) an **imprimitive** group $\mathrm{GL}_k(q) \wr \mathcal{S}_m$, where $n = km$,

the stabiliser of a direct sum decomposition into m k-subspaces;

iii) a **tensor product** $\mathrm{GL}_k(q) \circ \mathrm{GL}_m(q)$, where $n = km$,

the stabiliser of a tensor product decomposition $\mathbb{F}_q^k \otimes \mathbb{F}_q^m$;

iv) a **wreathed tensor product**,
the preimage in $\mathrm{GL}_n(q)$ of $\mathrm{PGL}_k(q) \wr \mathcal{S}_m$, where $n = k^m$,

the stabiliser of a tensor product decomposition $\mathbb{F}_q^k \otimes \cdots \otimes \mathbb{F}_q^k$;

v) the preimage in $\mathrm{GL}_n(q)$ of $r^{2k}: \mathrm{Sp}_{2k}(r)$, where $n = r^k$,

or of $2^{2k}.\mathrm{GO}_{2k}^{\epsilon}(2)$, for $r = 2$ and $q \equiv \epsilon \pmod 4$;

vi) an almost quasi-simple group acting irreducibly.

• Aschbacher: looks more closely at case **vi)** ,

∘ in particular considers subfields and extension fields of $\mathbb{F}_q$.

Proof of the Aschbacher-Dynkin Theorem

- **Proof:**

∘ Let $\mathrm{PSL}_n(q) \not\leq H < G := \mathrm{PGL}_n(q)$,

∘ and let $\widehat{H} < \widehat{G} := \mathrm{GL}_n(q)$ be its preimage.

- We may assume that $\widehat{H}$ acts **irreducibly**, otherwise case **i)** .

∘ Let $N \trianglelefteq H$ be the **socle** of H,

∘ that is the product of its minimal non-trivial normal subgroups.

∘ By **Clifford theory** $\widehat{N}$ acts **completely reducibly**.

- We may assume that $\widehat{N}$ has only one **isotypic component**, otherwise case **ii)** .

- We may assume that $\widehat{N}$ acts irreducibly, otherwise $\widehat{H} \leq \widehat{N} \circ C_{\widehat{G}}(\widehat{N})$ implies case **iii)** .

- We may assume that N is the only minimal normal subgroup, otherwise $\widehat{N} \leq \widehat{N}_1 \circ \widehat{N}_2$ implies case **iii)** again.

- If $N \cong C_r \times \cdots \times C_r$ is (elementary) abelian we get case **v)** .

- If $N \cong T$ is non-abelian simple we get case **vi)** .

- If $N \cong T \times \cdots \times T$ is non-abelian non-simple we get case **iv)** . $\sharp$

Geometric algebra

- ○ Let F be a field, with automorphism $\sigma\colon F \to F$ such that $\sigma^2 = \mathrm{id}$,
- ○ and let V be a finitely generated F-vector space.

- • A **σ-bilinear form** is a map $f\colon V \times V \to F$ such that
- ○ $f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$,
- ○ $f(u, \lambda v + w) = \lambda^\sigma f(u, v) + f(u, w)$.

- • f is called
- ○ **symmetric** if $\sigma = \mathrm{id}$ and $f(w, v) = f(v, w)$,
- ○ **hermitian** if $\sigma \neq \mathrm{id}$ and $f(w, v) = f(v, w)^\sigma$,
- ○ **symplectic** if $\sigma = \mathrm{id}$ and $f(w, v) = -f(v, w)$,
- ○ **alternating** if $\sigma = \mathrm{id}$ and $f(v, v) = 0$.

- ○ Any alternating form is symplectic,
- ○ if $\mathrm{char}(F) \neq 2$ then any symplectic form is alternating;
- ○ if $\mathrm{char}(F) = 2$ then being symmetric or symplectic coincide.

- • A **quadratic form** is a map $q\colon V \to F$ such that
- ○ $q(\lambda v + w) = \lambda^2 q(v) + q(w) + \lambda f(v, w)$,
- ○ where the associated bilinear form $f\colon V \times V \to F$ is symmetric.

- ○ If $\mathrm{char}(F) \neq 2$ then q is recovered from f as $q(v) = \frac{1}{2} f(v, v)$,
- ○ if $\mathrm{char}(F) = 2$ then f is alternating.

Geometric algebra, II

• A σ-bilinear form f is called **non-degenerate**, if

$$\mathrm{rad}(f) := \{w \in V; f(v,w) = 0 \text{ for all } v \in V\} = \{0\}.$$

∘ $v \in V$ is called **isotropic** if $f(v,v) = 0$.

∘ A map $A \in \mathrm{GL}(V)$ is called an **isometry** of f, if

$$f(vA, wA) = f(v,w) \text{ for all } v,w \in V;$$

∘ the set of all isometries is a subgroup of $\mathrm{GL}(V)$.

• A quadratic form q is called **non-degenerate**, if

$$\mathrm{rad}(q) := \{v \in \mathrm{rad}(f); v \text{ singular}\} = \{0\},$$

∘ where $v \in V$ is called **singular** if $q(v) = 0$.

∘ The **Witt index** is the dimension of a maximal singular subspace;

∘ by **Witt's Theorem** this is independent of the subspace chosen.

∘ A map $A \in \mathrm{GL}(V)$ is called an **isometry** of q, if

$$q(vA) = q(v) \text{ for all } v \in V;$$

∘ the set of all isometries is a subgroup of $\mathrm{GL}(V)$.

• No classification of non-degenerate forms for arbitrary F is known.

Unitary groups

• **Theorem:** Any non-degenerate φ_q-hermitian form over $\mathbb{F}_{q^2}$ has an orthonormal $\mathbb{F}_{q^2}$-basis,

∘ that is the associated **Gram matrix** is E_n.

• Thus $g \in \mathrm{GL}_n(q^2)$ is an isometry if and only if $g \cdot E_n \cdot \overline{g}^{\mathrm{tr}} = E_n$.

∘ **General unitary group** $\mathrm{GU}_n(q^2) := \{g \in \mathrm{GL}_n(q^2); \overline{g}^{-\mathrm{tr}} = g\}$,

∘ that is the **fixed points** of the concatenation of the graph automorphism (the duality) and a field automorphism of $\mathrm{GL}_n(q^2)$.

• Counting the number of ordered orthonormal $\mathbb{F}_{q^2}$-bases:

∘ $|\mathrm{GU}_n(q^2)| = q^{\binom{n}{2}} \cdot \prod_{i=1}^{n}(q^i - (-1)^i) = (-q)^{\binom{n}{2}} \cdot \prod_{i=1}^{n}((-q)^i - 1)$

∘ **Ennola duality** $|\mathrm{GU}_n(q^2)| = |\mathrm{GL}_n(-q)|$

• As in the linear case: $\mathrm{SU}_n(q^2)$, $\mathrm{PGU}_n(q^2)$, $\mathrm{PSU}_n(q^2)$,

∘ where $Z(GU_n(q^2)) \cong C_{q+1} = C_{|(-q)-1|}$.

∘ $|\mathrm{PSU}_n(q^2)| = \frac{1}{\gcd(n,q+1)} \cdot \frac{1}{q+1} \cdot |\mathrm{GU}_n(q^2)| = |\mathrm{PSL}_n(-q)|$

• **Simplicity of PSU$_n(q^2)$:** Apply Iwasawa's Criterion

∘ to the action on the set of isotropic 1-dimensional subspaces,

∘ and use **unitary transvections**,

∘ that is $V \to V : v \mapsto v + \lambda f(v, w)w$, where $w \in V$ is isotropic.

∘ Exceptions: $\mathrm{PSU}_2(q^2) \cong \mathrm{PSL}_2(q)$, and $\mathrm{PSU}_3(2^2)$ is soluble.

Symplectic groups

• **Theorem:** Any (necessarily even-dimensional) non-degenerate alternating form over $\mathbb{F}_q$ is an orthogonal sum of **hyperbolic planes**;

◦ that is the latter have **Gram matrix** $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

• **Symplectic group** $\mathrm{Sp}_{2n}(q)$

◦ Counting the number of ordered **symplectic** $\mathbb{F}_q$-bases:

◦ $|\mathrm{Sp}_{2n}(q)| = q^{n^2} \cdot \prod_{i=1}^{n}(q^{2i} - 1)$

◦ We have $\mathrm{Sp}_{2n}(q) \leq \mathrm{SL}_{2n}(q)$.

• **Projective** symplectic group $\mathrm{PSp}_{2n}(q) := \mathrm{Sp}_{2n}(q)/Z(\mathrm{Sp}_{2n}(q))$,

◦ where $Z(\mathrm{Sp}_{2n}(q)) = \{\pm E_n\}$.

◦ $|\mathrm{PSp}_{2n}(q)| = \frac{1}{\gcd(2,q-1)} \cdot |\mathrm{Sp}_{2n}(q)|$

• **Simplicity of PSp$_{2n}(q)$:** Apply Iwasawa's Criterion

◦ to the action on the set of 1-dimensional subspaces,

◦ and use **symplectic transvections**,

◦ that is $V \to V : v \mapsto v + \lambda f(v,w)w$.

◦ Exceptions: $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$, and $\mathrm{Sp}_4(2) \cong \mathcal{S}_6$.

Orthogonal groups

• **Theorem:** Any $(2n+1)$-dimensional non-degenerate quadratic form over $\mathbb{F}_q$ is equivalent to $X_0^2 + \sum_{i=1}^n X_i X_{-i}$.

• **Theorem:** Any $2n$-dimensional non-degenerate quadratic form over $\mathbb{F}_q$ is equivalent

∘ either to $\sum_{i=1}^n X_i X_{-i}$, having maximal Witt index n,

∘ or to, where $T^2 + T + a \in \mathbb{F}_q[T]$ is irreducible,

$$(X_0^2 + X_0 X_{-0} + aX_{-0}^2) + \sum_{i=1}^{n-1} X_i X_{-i},$$

having non-maximal Witt index $n-1$.

• **General orthogonal groups** $\mathrm{GO}_{2n+1}(q)$, $\mathrm{GO}_{2n}^+(q)$, $\mathrm{GO}_{2n}^-(q)$

• Counting the number of isotropic vectors,

∘ which are acted on transitively by $\mathrm{GO}_n(q)$, and induction:

∘ $|\mathrm{GO}_{2n}^\epsilon(q)| = 2q^{\binom{n}{2}} \cdot (q^n - \epsilon) \cdot \prod_{i=1}^{n-1}(q^{2i} - 1)$

∘ $|\mathrm{GO}_{2n+1}(q)| = 2q^{n^2} \cdot \prod_{i=1}^{n}(q^{2i} - 1)$,

• As in the linear case: $\mathrm{SO}_n(q)$, $\mathrm{PGO}_n(q)$, $\mathrm{PSO}_n(q)$,

∘ where $Z(\mathrm{GO}_n(q)) = \{\pm E_n\}$,

∘ and where $g \cdot J \cdot g^{\mathrm{tr}} = J$, for J being the Gram matrix,

∘ implies $\det(g)^2 = 1$ for all $g \in \mathrm{GO}_n(q)$.

• **But:** $\mathrm{PSO}_n(q)$ is in general not perfect.

Orthogonal groups in odd characteristic

∘ Let q be odd.

• **Spinor norm** $\nu\colon \mathrm{GO}_n(q) \to \mathbb{F}_q^*/\mathbb{F}_q^{*2} \cong C_2$:

∘ write $g \in \mathrm{GO}_n(q)$ as a product of **reflections**

∘ $r_w\colon V \to V\colon v \mapsto v - \frac{f(v,w)}{q(w)} \cdot w$, where $w \in V$ is non-singular,

∘ and let $\nu(r_w) := q(w) \cdot \mathbb{F}_q^{*2} \in \mathbb{F}_q^*/\mathbb{F}_q^{*2}$.

∘ Note the similarity to the definition of the sign of a permutation.

• Let $\Omega_n(q) := \ker(\nu) \cap \mathrm{SO}_n(q)$ and $\mathrm{P}\Omega_n(q) := \Omega_n(q)/Z(\Omega_n(q))$,

∘ then $\mathrm{GO}_n(q)/\ker(\nu) \cong \mathrm{SO}_n(q)/\Omega_n(q) \cong C_2$.

• $\mathrm{SO}_{2n+1}(q) \cong \mathrm{PSO}_{2n+1}(q)$ and $\Omega_{2n+1}(q) \cong \mathrm{P}\Omega_{2n+1}(q)$,

∘ hence $|\Omega_{2n+1}(q)| = \frac{1}{4} \cdot |\mathrm{GO}_{2n+1}(q)|$.

• $-E_{2n} \in \Omega_{2n}^\epsilon(q)$ if and only if $q^n \equiv \epsilon \pmod 4$,

∘ hence $|\mathrm{P}\Omega_{2n}^\epsilon(q)| = \frac{1}{2\cdot\gcd(4,q^n-\epsilon)} \cdot |\mathrm{GO}_{2n}^\epsilon(q)|$.

• **Simplicity of $\mathrm{P}\Omega_n(q)$:** Apply Iwasawa's Criterion

∘ to the action on the set of 1-dimensional singular subspaces,

∘ and use **Siegel transformations**.

∘ Exceptions: $\mathrm{GO}_2^\epsilon(q) \cong D_{2(q-\epsilon)}$, and $\mathrm{P}\Omega_3(3) \cong \mathrm{PSL}_2(3) \cong \mathcal{A}_4$, and $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$.

∘ Note: $|\Omega_{2n+1}(q)| = |\mathrm{PSp}_{2n}(q)|$, but $\Omega_{2n+1}(q) \not\cong \mathrm{PSp}_{2n}(q)$.

Orthogonal groups in characteristic 2

∘ Let $q = 2^f$.

∘ $\mathrm{GO}_n(q) = \mathrm{SO}_n(q) = \mathrm{PGO}_n(q) = \mathrm{PSO}_n(q)$

• **Theorem:** $\mathrm{GO}_{2n+1}(q) \cong \mathrm{Sp}_{2n}(q)$

∘ Hence only consider the even-dimensional case:

• **Quasideterminant** $\nu\colon \mathrm{GO}_{2n}^{\epsilon}(q) \to \{\pm 1\} \cong C_2$:

∘ write $g \in \mathrm{GO}_{2n}^{\epsilon}(q)$ as a product of **orthogonal transvections**

∘ $t_w\colon V \to V\colon v \mapsto v + f(v,w)\cdot w$, where $w \in V$,

∘ and let $\nu(t_w) := -1$.

∘ Kantor: Then $\nu(g)$ is the sign of the permutation induced by g on the set of maximal isotropic subspaces.

• Let $\Omega_{2n}^{\epsilon}(q) := \ker(\nu)$.

∘ Then the order formulae and the simplicity proof are still valid;

∘ the latter with the exceptions $\mathrm{GO}_2^{\epsilon}(q) \cong D_{2(q-\epsilon)}$, and $\mathrm{P}\Omega_4^{+}(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$, and $\mathrm{P}\Omega_5(2) \cong \mathrm{Sp}_4(2) \cong \mathcal{S}_6$.

• Note: For arbitrary q we have, using **Klein correspondence**,

∘ $\mathrm{GO}_2^{\epsilon}(q) \cong D_{2(q-\epsilon)}$, $\mathrm{P}\Omega_3(q) \cong \mathrm{PSL}_2(q)$,

∘ $\mathrm{P}\Omega_4^{+}(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$, $\mathrm{P}\Omega_4^{-}(q) \cong \mathrm{PSL}_2(q^2)$,

∘ $\mathrm{P}\Omega_5(q) \cong \mathrm{PSp}_4(q)$, $\mathrm{P}\Omega_6^{+}(q) \cong \mathrm{PSL}_4(q)$, $\mathrm{P}\Omega_6^{-}(q) \cong \mathrm{PSU}_4(q)$.

Structure of classical groups

- **Subgroups:**

◦ groups with BN-pairs,

◦ tori, Borels, and parabolics described in terms of **geometry**;

◦ entailing a generic 'Iwasawa type' simplicity argument.

◦ Moreover:

- **Automorphisms:**

◦ diagonal, field, and graph automorphisms

- **Covers:**

◦ generic p'-fold covers, and finitely many p-power-fold exceptions

- **Maximal subgroups:**

◦ Dynkin [1952]: complex classical groups

◦ Aschbacher [1984]: finite classical groups

◦ Kleidman, Liebeck [1990]: explicit lists

Modern view of classical groups

• **Linear and classical groups:** described in terms of

∘ **geometry**,

∘ **Lie theory**,

∘ **algebraic groups**.

• **Example:** $\mathrm{SL}_n(q)$ is described by

∘ its **natural** faithful action on the n-dimensional space $\mathbb{F}_q^n$;

∘ the **conjugation** action on the (n^2-1)-dimensional **Lie algebra**

$$\mathfrak{sl}_n(q) := \{A \in \mathbb{F}_q^{n\times n}; \mathrm{Tr}(A) = 0\},$$

yielding an action of $\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$;

∘ **polynomial equations** defining the **algebraic group**

$$\mathrm{SL}_n(\overline{\mathbb{F}}) := \{A \in \overline{\mathbb{F}}^{n\times n}; \det(A) = 1\},$$

where $\mathbb{F}_q \subseteq \overline{\mathbb{F}}$ is an algebraic closure with **Frobenius morphism**

$$F := \varphi_q \colon \overline{\mathbb{F}} \to \overline{\mathbb{F}} \colon \lambda \mapsto \lambda^q,$$

yielding the set of fixed points

$$\mathrm{SL}_n(q) = \mathrm{SL}_n(\overline{\mathbb{F}})^F := \{g \in \mathrm{SL}_n(\overline{\mathbb{F}}); F(g) = g\}.$$

• **Starting point:** Classification of simple complex Lie algebras

∘ by **Dynkin types** A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2.

Chevalley groups

- Chevalley [1955]:
  - **integral forms** of simple complex Lie algebras
  - yield simple Lie algebras L over any field F;
  - consider **adjoint representation**

$$\mathrm{ad}\colon L \to \mathrm{End}_F(L)\colon x \mapsto (L \to L\colon y \mapsto [x, y]),$$

  - and **integrate** suitable **roots** $x \in L$,
  - obtain **one-parameter subgroups** of $\mathrm{Aut}(L)$, given by

$$\exp(\lambda \cdot \mathrm{ad}(x)) := \sum_{i \geq 0} \frac{\lambda^i}{i!} \cdot \mathrm{ad}(x)^i \in \mathrm{GL}_F(L).$$

- **Chevalley group**

$$G_n(F) := \langle \exp(\lambda \cdot \mathrm{ad}(x)); x \in L \text{ root}, \lambda \in F \rangle \leq \mathrm{Aut}(L)$$

- This uniformly yields finite field analoga of
  - the classical Lie groups,
  - and the exceptional groups G_2, F_4, E_6, E_7, E_8.
- $G_n(F)$ is a group with BN-pair.

Chevalley group of type A_1

• $\mathfrak{sl}_2(F) = \langle f, h, e \rangle_F$, with **Chevalley basis**

$$f := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad h := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad e := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

∘ Adjoint action of e is nilpotent:

$$\operatorname{ad}(e) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{bmatrix}, \quad \operatorname{ad}(e)^2 = \begin{bmatrix} 0 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \operatorname{ad}(e)^3 = 0 \cdot E_3.$$

∘ Integration $\lambda \cdot \operatorname{ad}(e)$ and $\lambda \cdot \operatorname{ad}(f)$ is well-defined:

$$\exp(\lambda \cdot \operatorname{ad}(e)) = E_3 + \lambda \cdot \operatorname{ad}(e) + \frac{\lambda^2}{2} \cdot \operatorname{ad}(e)^2 = \begin{bmatrix} 1 & \lambda & -\lambda^2 \\ 0 & 1 & -2\lambda \\ 0 & 0 & 1 \end{bmatrix}$$

$$\exp(\lambda \cdot \operatorname{ad}(f)) = E_3 + \lambda \cdot \operatorname{ad}(f) + \frac{\lambda^2}{2} \cdot \operatorname{ad}(f)^2 = \begin{bmatrix} 1 & 0 & 0 \\ 2\lambda & 1 & 0 \\ -\lambda^2 & -\lambda & 1 \end{bmatrix}$$

• $\mathrm{SL}_2(F) = \langle x(\lambda), y(\lambda); \lambda \in F \rangle$, with transvections

$$x(\lambda) := \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}, \quad y(\lambda) := \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}.$$

∘ Adjoint action of $\mathrm{SL}_2(F)$ on $\mathfrak{sl}_2(F)$ is conjugation:

$$x(\lambda)\colon f \mapsto f + \lambda h - \lambda^2 e, \quad h \mapsto h - 2\lambda e, \quad e \mapsto e;$$
$$y(\lambda)\colon f \mapsto f, \quad h \mapsto h + 2\lambda e, \quad e \mapsto \lambda^2 f - \lambda h + e.$$

• Thus we have $\mathrm{SL}_2(F) \to A_1(F)$, implying

$$A_1(F) := \langle \exp(\lambda \cdot \operatorname{ad}(e)), \exp(\lambda \cdot \operatorname{ad}(f)); \lambda \in F \rangle \cong \mathrm{PSL}_2(F).$$

Twisted groups

○ Generalise the construction of unitary groups from linear groups,

○ as fixed point sets under suitable graph automorphisms:

• completes the list of classical groups;

• yields twisted exceptional groups

○ ${}^2E_6(q^2)$ and ${}^3D_4(q^3)$ [Steinberg, 1959];

• yields 'sporadic' twisted exceptional groups

○ ${}^2B_2(2^{2f+1})$ [Suzuki, 1962],

○ ${}^2G_2(3^{2f+1})$ [Ree, 1961],

○ ${}^2F_4(2^{2f+1})$ [Ree, Tits, 1961/1964].

• These also are groups with BN-pair.

• **Are there geometrical interpretations of these groups?**

○ Mostly there are, elucidating more of the group structure;

○ and leading to **natural** representations

○ smaller than the **adjoint** representations.

• For $E_7(q)$ the smallest representation has dimension 56,

○ while the adjoint representation has dimension 133.

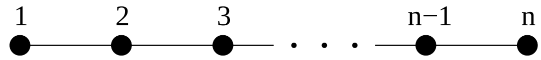
• For $E_8(q)$ the adjoint representation is smallest, of dimension 248.

Classical Dynkin types

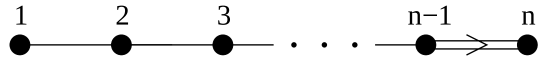
∘ Six series of classical groups:

• Classical Chevalley groups:

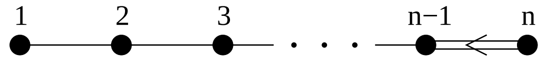
∘ Type A_n: $\mathrm{PSL}_{n+1}(q)$, for $n \geq 1$



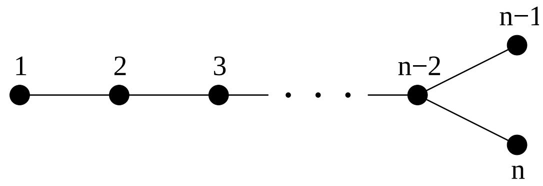
∘ Type B_n: $\Omega_{2n+1}(q)$, for $n \geq 3$



∘ Type C_n: $\mathrm{PSp}_{2n}(q)$, for $n \geq 2$

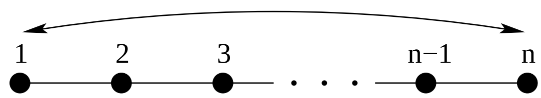


∘ Type D_n: $\mathrm{P}\Omega^{+}_{2n}(q)$, for $n \geq 4$

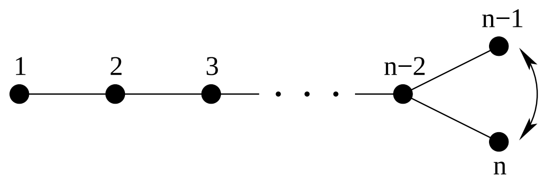


• Twisted classical groups:

∘ Type ${}^2A_n$: $\mathrm{PSU}_{n+1}(q)$, for $n \geq 2$



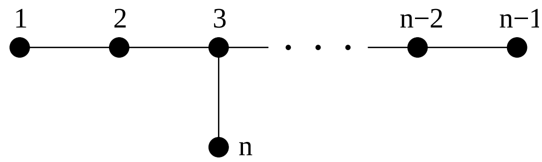
∘ Type ${}^2D_n$: $\mathrm{P}\Omega^{-}_{2n}(q)$, for $n \geq 4$



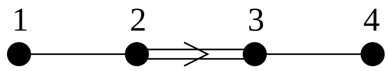
Exceptional Dynkin types

○ Ten series of exceptional groups:

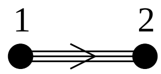
• Exceptional Chevalley groups:



○ Type E_n, for $n \in \{6, 7, 8\}$

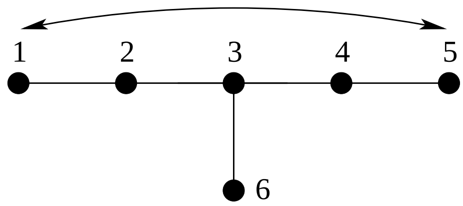


○ Type F_4

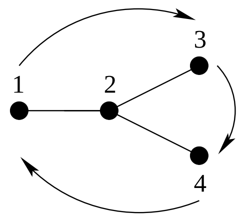


○ Type G_2

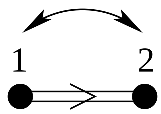
• Twisted exceptional groups:



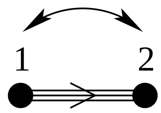
○ Type ${}^2E_6(q^2)$



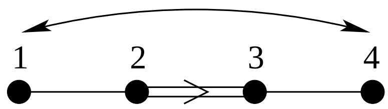
○ Type ${}^3D_4(q^3)$



○ Type ${}^2B_2(2^{2f+1})$



○ Type ${}^2G_2(3^{2f+1})$



○ Type ${}^2F_4(2^{2f+1})$

Suzuki groups

- ◦ Let $q := 2^{2f+1}$ for $f \in \mathbb{N}_0$.
- • Consider the exceptional isomorphism $\mathcal{S}_6 \cong \mathrm{Sp}_4(2) = B_2(2)$:
- ◦ Natural permutation representation of $\mathcal{S}_6$ over $F := \mathbb{F}_q$
- ◦ has $\mathcal{S}_6$-invariant form $f([x_1, \ldots, x_6], [y_1, \ldots, y_6]) := \sum_{i=1}^{6} x_i y_i$.
- ◦ Then $V := \langle v \rangle_F^{\perp} / \langle v \rangle_F$, where $v := [1, \ldots, 1]$,
- ◦ has $\mathcal{S}_6$-invariant non-degenerate alternating form,
- ◦ hence we have $\mathcal{S}_6 \leq \mathrm{Sp}_4(q)$; now compare orders for $q = 2$.
- • V has hyperbolic basis

$$e_1 := [1,1,0,0,0,0],\ \ f_1 := [0,1,1,0,0,0],$$
$$e_2 := [0,0,0,1,1,0],\ \ f_2 := [0,0,0,0,1,1].$$

- ◦ **Exterior square** $V' := \Lambda^2(V)$ has
- ◦ non-degenerate symplectic form f' **(Klein correspondence)**
- ◦ given by $f'(a \wedge b, c \wedge d) = 1$ if and only if $\dim(\langle a, b, c, d \rangle_F) = 4$.
- ◦ $\langle v' \rangle_F^{\perp} / \langle v' \rangle_F$, where $v' := e_1 \wedge f_1 + e_2 \wedge f_2$, has hyperbolic basis

$$e_1' := e_1 \wedge e_2, \quad f_1' := f_1 \wedge f_2, \quad e_2' := e_1 \wedge f_2, \quad f_2' := e_2 \wedge f_1.$$

- • $\gamma \colon e_i \mapsto e_i',\ f_i \mapsto f_i'$ defines a graph automorphism of $\mathrm{Sp}_4(q)$
- ◦ such that $\gamma^2 = \varphi_2$, hence $(\gamma\varphi_2^f)^2 = \varphi_2^{1+2f} = \mathrm{id}$.
- • **Suzuki group** $Sz(q) := {}^2B_2(q) := C_{\mathrm{Sp}_4(q)}(\gamma\varphi_2^f)$ [Ono, 1962]
- ◦ Note: γ extends $\mathcal{A}_6 < \mathcal{S}_6 \cong \mathrm{Sp}_4(2)$ to $\mathrm{PGL}_2(9) \not\cong \mathcal{S}_6$.

Suzuki groups, II

- $Sz(q)$ acts 2-transitively on the **Tits oval** [Suzuki, 1962],
  - a certain set of q^2+1 many 1-dimensional subspaces of V,
  - with point stabiliser $q^{1+1}\colon C_{q-1}$,
  - whose central involutions are commutators and generate $Sz(q)$.
  - This yields $|Sz(q)| = (q^2+1)q^2(q-1)$,
  - and Iwasawa's Criterion implies simplicity,
  - with the exception $Sz(2) \cong 5\colon 4$.
- **Automorphisms:** only field automorphisms
- **Covers:** generically trivial,
  - with the exception $2^2.Sz(8)$.
- **Maximal subgroups**, for $f \geq 1$: [Suzuki]
  - $q^{1+1}\colon C_{q-1}$,
  - $D_{2(q-1)}$,
  - $C_{q+\sqrt{2q}+1}\colon 4$,
  - $C_{q-\sqrt{2q}+1}\colon 4$,
  - $Sz(q')$, where $q = (q')^r$ for r a prime and $q' \neq 2$.
  - Note: If $2f+1$ is a prime, $Sz(q)$ is a **minimal simple group**.

Octonion algebras

∘ Let F be a field such that $\mathrm{char}(F) \neq 2$.

• **Hamilton quaternions** $\mathbb{H}(F) = \langle 1, i, j, k \rangle_F$ [1843]

∘ are obtained from F by adjoining three orthogonal $\sqrt{-1}$'s,

∘ such that $i \cdot j = k$, $j \cdot k = i$, $k \cdot i = j$.

∘ $\mathbb{H}(F)$ is a skew-field such that $\dim_F(\mathbb{H}(F)) = 4$.

• Letting $\mathbb{H}(F)' := \langle i, j, k \rangle_F = \langle 1 \rangle_F^{\perp}$,

∘ with respect to the natural symmetric form,

∘ we have $\dim_F(\mathbb{H}(F)') = 3$,

• yielding $\mathrm{Aut}(\mathbb{H}(F)) = \mathrm{Aut}(\mathbb{H}(F)') \cong \mathrm{SO}_3(F) \cong \mathrm{PGL}_2(F)$.

• **Cayley octonions** $\mathbb{O}(F)$ [Cayley, Graves, 1845/1843]

∘ are obtained from F by adjoining seven orthogonal $\sqrt{-1}$'s

∘ $\{i_0, \ldots, i_6\}$, where any triple $[i_t, i_{t+1}, i_{t+3}]$

∘ fulfills the multiplication rules of $i, j, k \in \mathbb{H}(F)$.

∘ $\mathbb{O}(F)$ is a non-associative algebra such that $\dim_F(\mathbb{O}(F)) = 8$.

• Letting $\mathbb{O}(F)' := \langle i_0, \ldots, i_6 \rangle_F = \langle 1 \rangle_F^{\perp}$,

∘ with respect to the natural symmetric form,

∘ we have $\dim_F(\mathbb{O}(F)') = 7$.

• Replacing by a suitable form yields a characteristic-free definition:

Octonion algebras, II

- **Chevalley group**

$$G_2(F) \cong \mathrm{Aut}(\mathbb{O}(F)) = \mathrm{Aut}(\mathbb{O}(F)') < \mathrm{SO}_7(F)$$

∘ The geometric approach yields, for example,

$$|G_2(q)| = q^6(q^6-1)(q^2-1);$$

∘ $G_2(F)$ has a 7-dimensional natural representation,

∘ while the adjoint representation has dimension 14.

∘ Exception to simplicity: $G_2(2) \cong \mathrm{PSU}_3(3):2$

- **Small Ree group** ${}^2G_2(3^{2f+1}) < G_2(3^{2f+1})$**:**

∘ fixed points under a suitable graph automorphism,

∘ similar to $Sz(2^{2f+1}) \cong {}^2B_2(2^{2f+1}) < B_2(2^{2f+1}) \cong \mathrm{Sp}_4(2^{2f+1})$.

∘ Exception to simplicity: ${}^2G_2(3) \cong \mathrm{PSL}_2(8):3$

- **Steinberg triality group** $G_2(q) < {}^3D_4(q^3) < \mathrm{P}\Omega_8^+(q^3)$**:**

∘ automorphism group of **twisted** octonions.

∘ Note: ${}^3D_4(q^3) < D_4(q^3) \cong \mathrm{P}\Omega_8^+(q^3)$ fixed points under

∘ **Steinberg's triality automorphism**,

∘ which hence can be understood in terms of octonions.

Albert algebras

○ Let F be a finite field such that $\mathrm{char}(F) \not\in \{2, 3\}$.

• **Jordan product** $A \circ B := \frac{1}{2}(AB + BA)$ on an associative algebra

○ is commutative, non-associative, and fufills the **Jordan identity**

$$((A \circ A) \circ B) \circ A = (A \circ A) \circ (B \circ A).$$

○ A **Jordan algebra** is a commutative, non-associative algebra fullfing the Jordan identity.

• Any simple Jordan F-algebra arises from an associative F-algebra,

• except the **Albert algebra**

$$\mathbb{A}(F) := \{A \in \mathbb{O}(F)^{3\times 3}; A^{\mathrm{tr}} = \overline{A}\},$$

○ where $\bar{\ }\colon \mathbb{O}(F) \to \mathbb{O}(F)$ denotes **octonion conjugation**;

○ we have $\dim_F(\mathbb{A}(F)) = 27$.

• Letting $\mathbb{A}(F)' := \{A \in \mathbb{A}(F); \mathrm{Tr}(A) = 0\} = \langle E_3 \rangle^{\perp}$,

○ with respect to the natural symmetric form,

○ we have $\dim_F(\mathbb{A}(F)') = 26$.

• Replacing by a suitable form yields a characteristic-free definition:

Albert algebras, II

- **Chevalley group $F_4(q) \cong \mathrm{Aut}(\mathbb{A}(\mathbb{F}_q))$:**
  - has a 26-dimensional natural representation,
  - while the adjoint representation has dimension 52.

- **Large Ree group $^2F_4(2^{2f+1}) < F_4(2^{2f+1})$:**
  - fixed points under a suitable graph automorphism;
  - similar to $^2G_2(3^{2f+1}) < G_2(3^{2f+1})$.
  - Exception to simplicity: **Tits group** $^2F_4(2)'$

- **Chevalley group $E_6(q)$:** [Dickson, 1901]
  - leaves invariant a **cubic 'determinant' form** on $\mathbb{A}(\mathbb{F}_q)$;
  - $E_6(q)$ has a 27-dimensional natural representation,
  - while the adjoint representation has dimension 78.

- **Steinberg group $^2E_6(q^2) < E_6(q)$:**
  - fixed points under a suitable graph automorphism;
  - twisting the symmetric form on $\mathbb{A}(\mathbb{F}_q)$ yields a hermitian form,
  - similar to $\mathrm{PSU}_n(q) < \mathrm{PSL}_n(q)$.

Golay codes

- A **Steiner system** $S(t, k, v)$ on the set $\{1, \ldots, v\}$
- ◦ is a set of k-subsets, called **blocks**, such that
- ◦ any subset of size t is contained in precisely one block.
- ◦ Hence there are $|S(t, k, v)| = \binom{v}{t} / \binom{k}{t}$ blocks.

- **Example:** The finite **projective plane** of order q
- ◦ is a Steiner system $S(2, q + 1, q^2 + q + 1)$,
- ◦ the blocks being the projective lines.

- **Theorem:** There is a unique Steiner system $S(5, 8, 24)$.

- ◦ **Existence:** Three successive one-point extensions of $S(2, 5, 21)$
- ◦ coming from the projective plane of order 4 [Witt, 1938];

- ◦ **or:** the blocks are the 759 words of **weight** 8 of the
- ◦ self-dual **extended binary Golay** $[24, 12, 8]_2$-code $\mathcal{G}_{24} < \mathbb{F}_2^{24}$.

- Words of weight 8 are called **octads** [Todd, 1966].
- ◦ Computational combinatorial tool: [Curtis, 1976]
- ◦ **Miracle Octad Generator (MOG)**

- **Weight enumerator** $T^{24} + 759 \cdot T^{16} + 2576 \cdot T^{12} + 759 \cdot T^8 + 1$,
- ◦ the 2576 words of weight 12 are called **dodecads**.

Golay codes, II

- Given a dodecad,
- ∘ $S(5,8,24)$ induces a Steiner system $S(5,6,12)$ on it,
- ∘ being unique up to isomorphism,
- ∘ having 132 blocks, called **hexads**.

- Attaching signs, the blocks yield the words of weight 6 of the
- ∘ self-dual **extended ternary Golay** $[12,6,6]_3$-code $\mathcal{G}_{12} < \mathbb{F}_3^{12}$;
- ∘ weight enumerator $2 \cdot (12 \cdot T^{12} + 220 \cdot T^9 + 132 \cdot T^6 + 1)$.

- Any word of weight 4 determines a coset in the
- ∘ **Golay cocode (Todd module)** $\mathbb{F}_2^{24}/\mathcal{G}_{24}$,
- ∘ where 6 mutually disjoint words determine the same coset.
- ∘ Hence any word of weight 4 yields a **sextet**,
- ∘ a partition of $\{1,\ldots,24\}$ into 6 subsets of size 4,
- ∘ the union of any two of which is an octad;
- there are $\frac{1}{6} \cdot \binom{24}{4} = 1771$ sextets.

Mathieu groups [1861/1873]

- **Mathieu group** $M_{24} := \mathrm{Aut}(S(5,8,24)) \cong \mathrm{Aut}(\mathcal{G}_{24})$,
- ∘ acts 5-transitively on $\{1,\ldots,24\}$:

- **Mathieu group** $M_{23} := \mathrm{Stab}_{M_{24}}(1) \cong \mathrm{Aut}(\mathcal{G}_{23})$,
- ∘ where $\mathcal{G}_{23} < \mathbb{F}_2^{23}$ is the perfect **binary Golay** $[23,12,7]_2$-code;

- **Mathieu group** $M_{22} := \mathrm{Stab}_{M_{24}}(1,2)$;
- ∘ $M_{21} := \mathrm{Stab}_{M_{24}}(1,2,3) \cong \mathrm{PSL}_3(4)$, in natural 2-transitive action.

- $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
- Simplicity of M_{24}: Apply Iwasawa's Criterion
- ∘ to the transitive action on the sextets, with stabiliser $2^6 \colon (3.\mathcal{S}_6)$.

- ∘ M_{24} acts transitive on the dodecads, with point stabiliser
- **Mathieu group** $M_{12} \cong \mathrm{Aut}(S(5,6,12))$, $\mathrm{Aut}(\mathcal{G}_{12}) \cong 2.M_{12}$;
- ∘ $|M_{12}| = \frac{|M_{24}|}{2576} = 95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$.
- ∘ M_{12} acts sharply 5-transivitely on $\{1,\ldots,12\}$:

- **Mathieu group** $M_{11} := \mathrm{Stab}_{M_{12}}(1)$, $\mathrm{Aut}(\mathcal{G}_{11}) \cong 2 \times M_{11}$,
- ∘ where $\mathcal{G}_{11} < \mathbb{F}_3^{11}$ is the perfect **ternary Golay** $[11,6,5]_3$-code;

- $M_{10} := \mathrm{Stab}_{M_{12}}(1,2) \cong \mathcal{A}_6.2$,
- ∘ where $\mathrm{Aut}(\mathcal{A}_6) \cong \mathcal{A}_6.2^2$ and $\mathcal{S}_6 \not\cong \mathcal{A}_6.2 \not\cong \mathrm{PGL}_2(9)$.

Leech lattice

- $2^{12} \colon M_{24}$ afforded by the Golay code $\mathcal{G}_{24}$,
- ◦ acts monomially on

- **Leech lattice $\mathcal{L}$:** [Leech, Witt, 1967/1940]
- ◦ the set of all $x := [x_1, \ldots, x_{24}] \in \mathbb{Z}^{24}$ such that
- ◦ $x_i \equiv \frac{1}{4} \sum_{i=1}^{24} x_i \equiv m \pmod 2$, for some m,
- ◦ and $\{i; x_i \equiv k \pmod 4\} \in \mathcal{G}_{24}$, for each k;
- ◦ with scalar product $\langle x, y \rangle := \frac{1}{8} \cdot \sum_{i=1}^{24} x_i y_i \in \mathbb{Z}$.

- **Theorem:** $\mathcal{L}$ is the unique **unimodular even** lattice in $\mathbb{R}^{24}$
- ◦ without **roots**, that is vectors of norm 2.

- $\mathcal{L}_n := \{x \in \mathcal{L}; \langle x, x \rangle = n\}$, for $n \in 2\mathbb{N}_0$.
- ◦ **Weight function** $\Theta_{\mathcal{L}} := \sum_{n \in \mathbb{N}_0} |\mathcal{L}_{2n}| \cdot T^n \in \mathbb{Z}[[T]]$**:**

$$\Theta_{\mathcal{L}} = 1 + 196560 \cdot T^2 + 16773120 \cdot T^3 + 398034000 \cdot T^4 + \cdots$$

- $\mathcal{L}_8$ falls into classes of 48 mutually orthogonal vectors,
- ◦ called **coordinate frames**,
- ◦ hence there are $\frac{398034000}{48} = 8292375$ coordinate frames.

Conway groups [1969]

• **Conway group** $2.Co_1 := \mathrm{Aut}(\mathcal{L})$

∘ $|Co_1| = \frac{1}{2} \cdot 8292375 \cdot 2^{12} \cdot |M_{24}| = 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$

∘ Simplicity: Apply Iwasawa's Criterion to

∘ the transitive action on coordinate frames, with stabiliser $2^{12}\colon M_{24}$.

∘ Smallest representation of dimension 24 is **globally irreducible**.

∘ **Sublattice groups:** $2.Co_1$ acts transitively on $\mathcal{L}_4$ and $\mathcal{L}_6$.

• **Conway group** $Co_2 := \mathrm{Stab}_{2.Co_1}(v)$ where $v \in \mathcal{L}_4$;

• **Conway group** $Co_3 := \mathrm{Stab}_{2.Co_1}(w)$ where $w \in \mathcal{L}_6$.

∘ $2.Co_1$ acts transitively on $\{[v, v'] \in \mathcal{L}_4 \times \mathcal{L}_4; v + v' \in \mathcal{L}_6\}$,

• **McLaughlin group [1969]** $McL := \mathrm{Stab}_{2.Co_1}(v, v')$.

∘ $2.Co_1$ acts transitively on $\{[w, w'] \in \mathcal{L}_6 \times \mathcal{L}_6; w + w' \in \mathcal{L}_4\}$,

• **Higman-Sims group [1968]** $HS := \mathrm{Stab}_{2.Co_1}(w, w')$.

• **Higman-Sims graph** on $\{z \in \mathcal{L}_4, \langle z, w\rangle = 3, \langle z, w'\rangle = -3\}$,

∘ vertices z, z' being adjacent if $\langle z, z'\rangle = 1$,

∘ size $n = 100$, regular of valency $k = 22$;

∘ HS primitive of rank 3, with stabiliser M_{22}.

Suzuki chain

• Let $3D \in Co_1$ [Atlas]

∘ have order 3 and centraliser $C_{Co_1}(3D) \cong 3 \times \mathcal{A}_9$.

∘ Letting

$$\mathcal{A}_9 > \mathcal{A}_8 > \mathcal{A}_7 > \mathcal{A}_6 > \mathcal{A}_5 > \mathcal{A}_4 > \mathcal{A}_3 > \mathcal{A}_2$$

∘ yields corresponding centralisers $C_{Co_1}(\mathcal{A}_i)$

$\mathcal{S}_3 < \mathcal{S}_4 < \mathrm{PSL}_3(2) < \mathrm{PSU}_3(3) < J_2 < G_2(4) < 3.Suz < Co_1$.

• **Suzuki group [1969]** Suz

• **Hall-Janko group [1968]** J_2

∘ has two classes of involutions and $C_{J_2}(2A) \cong 2_-^{1+4} \colon \mathcal{A}_5$.

• $6.Suz < 2.Co_1$ induces a **complex** structure $\mathcal{L}_\mathbb{C}$ on $\mathcal{L}$,

∘ such that $6.Suz = \mathrm{Aut}(\mathcal{L}_\mathbb{C})$ acts irreducibly.

• $2.\mathcal{A}_5 < \mathbb{H}(\mathbb{R})$ **binary icosahedral group** [Hamilton, 1857],

∘ hence $2.\mathcal{A}_5 \circ 2.J_2 < 2.\mathcal{A}_4 \circ 2.G_2(4) < 2.Co_1$

∘ induces a **quaternionic** structure $\mathcal{L}_\mathbb{H}$ on $\mathcal{L}$,

∘ such that $2.J_2 < 2.G_2(4) = \mathrm{Aut}(\mathcal{L}_\mathbb{H})$ act irreducibly;

∘ note: this yields the exceptional 2-fold cover $2.G_2(4)$.

Fischer groups

- A finite group G generated by
- ◦ a conjugacy class of involutions, called 3-**transpositions**,
- ◦ such that the product of two transpositions has order at most 3,
- ◦ $G' = G''$, and any normal 2- or 3-subgroup is central,
- ◦ is called a 3-**transposition group**.

- **Theorem:** [Fischer, 1968/1971]

Let G be a 3-transposition group. Then $G/Z(G)$ is isomorphic to:

- ◦ $\mathcal{S}_n$; $\mathrm{PSU}_n(2^2)$, $\mathrm{Sp}_{2n}(2)$, $\mathrm{GO}^{\epsilon}_{2n}(2)$; $\mathrm{P}\Omega^{\epsilon}_{2n}(3) : 2$, $\Omega_{2n+1}(3)$, $\mathrm{SO}_{2n+1}(3)$;
- ◦ or one of the **Fischer groups** Fi_{22}, Fi_{23}, $Fi'_{24}.2$.

- **Key tool: Transposition graph** Δ,
- ◦ with vertices corresponding to the 3-transpositions,
- ◦ being adjacent if the 3-transpositions commute.
- Hence Δ is regular, and $G \leq \mathrm{Aut}(\Delta)$ is vertex-transitive.

- ◦ Fi_{22}: $n = 3510$, $k = 693$, $H \cong 2.\mathrm{PSU}_6(2)$;
- ◦ Fi_{23}: $n = 31671$, $k = 3510$, $H \cong 2.Fi_{22}$;
- ◦ $Fi'_{24}.2$: $n = 306936$, $k = 31671$, $H \cong 2 \times Fi_{23}$

- Simplicity: Apply Iwasawa's Criterion
- ◦ to the above primitive rank 3 actions on the vertices of Δ.

The Monster

- ○ 3-transposition groups $2^2.\mathrm{PSU}_6(2^2) < 2.Fi_{22} < Fi_{23} < Fi'_{24}.2$
- ○ embedding $2.Fi_{22} < 2^2.{}^2E_6(2^2){:}\ 2$ into a 4**-transposition group**
- ○ $2^{11}.M_{24} < Fi'_{24}$ Todd action, $2^{11}{:}\ M_{24} < Co_1$ Golay action
- ○ FISCHER, CONWAY [1968]:

$$2^2.{}^2E_6(2^2){:}\ 2 \overset{?}{<} 2.B \overset{?}{<} M \overset{?}{<} \ ?$$

- **Fischer-Griess Monster (Friendly Giant)** M [1973]:
- ○ a 6**-transposition group** of order

$$808017424794512875886459904961710757005754368000000000$$
$$= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$
$$\sim 8 \cdot 10^{53}$$

- ○ Smallest representation V has dimension 196883,
- ○ carrying structure of non-associative **Griess algebra** [1980].
- ○ Construction needs a thorough analysis of $\mathcal{L}$ and $\mathcal{G}_{24}$.
- ○ The Leech lattice and Fischer groups are **involved** in M.

Monstrous Moonshine

- McKay, Thompson [1979]:
  - ○ Fourier expansion of the elliptic modular j-function

$$j - 744 = q^{-1} + 196884 \cdot q + 21493760 \cdot q^2 + 864299970 \cdot q^3 + \cdots ,$$

  - ○ has coefficients being character degrees of M.
- **Moonshine Conjectures:** [Conway, Norton, 1979]
  - ○ There is an infinite-dimensional graded M-module
  - ○ inducing a relation between conjugacy classes of M
  - ○ and modular functions of genus 0.
- Frenkel, Lepowsky, Meurman [1988]:
  - ○ construction of moonshine module,
  - ○ using **vertex operators** from **conformal field theory**.
- Borcherds [1992]:
  - ○ M-invariant **vertex algebra** on moonshine module,
  - ○ proving the Moonshine Conjectures.

How to construct a Monster?

[Griess, Conway, 1980/1985]

- $G_1 := C_M(2B) \cong 2_+^{1+24}.Co_1$,
- ∘ where $2^{24} \cong \mathcal{L}/2\mathcal{L}$ and $G_1/Z(G_1) \cong 2^{24}\colon Co_1$.
- Let $\widetilde{G}_1$ be the universal cover of G_1, then $Z(\widetilde{G}_1) \cong V_4$,
- ∘ giving rise to groups $G_1^s \ncong G_1^t \cong G_1$ of shape $2_+^{1+24}.Co_1$,
- ∘ with smallest faithful representations of dimension 2^{12} and $24 \cdot 2^{12}$.
- $V|_{G_1} \cong 98304 \oplus 98280 \oplus 299$, where
- ∘ $98304 \cong 4096 \otimes 24 = 2^{12} \otimes \mathcal{L}$, acted on by G_1^s and $2.Co_1$;
- ∘ $2^{24}|_{Co_2} = [1, 22, 1]$ uniserial, $2^{24}\colon Co_2$ having linear character 1^-,

$$98280 \cong (1^-_{2^{24}.Co_2}) \uparrow^{2^{24}.Co_1} \text{ monomial action;}$$

- ∘ $1 \oplus 299 \cong S^2(\mathcal{L}) < \mathcal{L} \otimes \mathcal{L}$, acted on by Co_1.
- Restrict to $G_1 > G_{12} \cong 2_+^{1+24}.(2^{11}\colon M_{24}) \cong 2^{2+11+22}.(2 \times M_{24})$,
- **triality symmetry** yields $G_{12} < G_2 \cong 2^{2+11+22}.(\mathcal{S}_3 \times M_{24})$.
- ∘ $V|_{G_2} \cong 147456 \oplus 48576 \oplus 828 \oplus 23$
- ∘ $98304|_{G'_{12}} \cong 49152 \oplus 49152$ and $552|_{G'_{12}} \cong 276 \oplus 276$

G_1	98304		98280			299
	↓	↙	↓	↘	↙	↓
G_{12}	98304	49152	48576	552	276	23
	↑	↗	↑	↖	↑	↑
G_2	147456		48576		828	23

Monstrous groups

- $C_M(2B) \cong 2_+^{1+24}.Co_1$
- $C_M(3A) \cong 3.Fi'_{24}$

- **Baby Monster B:** [Fischer, 1973]

∘ a 4-**transposition group**, arising as $C_M(2A) \cong 2.B$.

∘ Smallest representation has dimension 4371,

∘ is irreducible except in characteristic 2,

∘ and contains a vector with stabiliser $2.{}^2E_6(2^2){:}\,2$, yielding

∘ smallest permutation representation on 13 571 955 000 points

∘ [Leon, Sims, 1980].

- **Thompson group [1973] Th:**

∘ $3C \in M$ preimage of $3D$ with respect to $2_+^{1+24}.Co_1 \to Co_1$

∘ gives rise to $C_M(3C) \cong 3 \times Th$.

∘ $C_{Th}(2A) \cong 2_+^{1+8}.\mathcal{A}_9$

∘ Smallest representation has dimension 248,

∘ is globally irreducible,

∘ and yields an embedding $Th < E_8(3)$.

Monstrous groups, II

- **Harada-Norton group [1973]** HN**:**
- ◦ $5A \in M$ preimage of $5B$ with respect to $2_+^{1+24}.Co_1 \to Co_1$
- ◦ gives rise to $C_M(5A) \cong 5 \times HN$.
- ◦ $C_{HN}(2B) \cong 2_+^{1+8}.(\mathcal{A}_5 \times \mathcal{A}_5).2$
- ◦ Smallest representation has dimension 133 over $\mathbb{Q}[\sqrt{5}]$,
- ◦ is irreducible except in characteristic 2,
- ◦ and **does not** yield an embedding into $E_7(5)$.

- **Held group [1968]** He**:**
- ◦ arises as $C_M(7A) \cong 7 \times He$.
- ◦ Any simple group having an involution centraliser $2^{1+6}{:}\,\mathrm{PSL}_3(2)$
- ◦ is isomorphic to $\mathrm{PSL}_5(2)$, M_{24}, or He.

Pariahs

∘ There are just six sporadic groups not involved in M.

∘ Wilson: 'The behaviour of these six groups is so bizarre that any attempt to describe them ends up looking like a disconnected sequence of unrelated facts — it is simply the nature of the subject.'

• **Janko group [1965]** J_1**:**

∘ $C_{J_1}(2A) \cong 2 \times \mathcal{A}_5$;

∘ $J_1 < G_2(11)$,

∘ $|J_1| = 11 \cdot (11^3 - 1)(11 + 1)$.

∘ Wilson [1986]: J_1 is **not** a subgroup of M.

• **Janko group [1968]** J_3**:**

∘ has a single class of involutions and $C_{J_3}(2A) \cong 2_-^{1+4} \colon \mathcal{A}_5$;

∘ while J_2 has two classes of involutions and $C_{J_2}(2A) \cong C_{J_3}(2A)$.

• **Rudvalis group [1972]** Ru

Pariahs, II

- **O'Nan group [1973]** ON**:**
- ○ Parker, Ryba [1988]: $3.ON < \mathrm{GL}_{452}(\mathbb{F}_7)$
- ○ Soicher [1990]: action on 122760 points

- **Lyons group [1969]** Ly**:**
- ○ $C_{Ly}(2A) \cong 2.\mathcal{A}_{11}$
- ○ Meyer, Neutsch, Parker [1985]: $Ly < \mathrm{GL}_{111}(\mathbb{F}_5)$

- **Janko group [1975]** J_4**:**
- ○ $C_{J_4}(2A) \cong 2_+^{1+12}.(3.M_{22}:2)$
- ○ Norton, Parker, Thackray [1980]: $J_4 < \mathrm{GL}_{112}(\mathbb{F}_2)$,
- ○ **the original motivation to develop the MeatAxe.**

Computational techniques play an important role in the construction and analysis of the sporadic simple groups.