# Group Theory and Computational Methods - GTCM 2016

November 5-14, 2016

## Finite simple groups and the Monster

N.S. Narasimha Sastry
Statistics and Mathematics Unit
Indian Statistical Institute
Bangalore

## Finite simple groups and the Monster
-a (very) brief introduction

**Contents:**

1. Introduction
2. Groups of Lie type
3. Sporadic groups

   - centralizers of involutions
   - transposition groups

4. Monster group

   - some of the striking properties
   - Discovery
   - Huristics for the $196,883$- dimensional representation Griess module

1. Classification of finite simple groups is a major achievement of twentieth century Mathematics. This programme has two aspects:

(a) Discovery of new simple groups;
(b) Proof of the completeness of the list of known simple groups.

From now on, “simple group” means “finite nonabelian simple group”.

**A.** *Before fifties:* Galois defined normal subgroups and simple groups.

- Jordan-Holder theorem, highlighting the central place of simple groups in the study of finite groups.
- In the first book on finite groups, Jordan listed the alternating groups and some matrix groups over fields of prime order.
- E. Galois (˜1832) work on $PSL(2,p)$ $p$ a prime and establishing the relation between solvability of a group and solvability of polynomial equations with integer coefficients.
- E. Mathieu's construction of the five highly transitive groups (1860-61).
  Sylow foundational theorems.
- L. E. Dickson's realization of a few groups as stabilizers of certain multilinear forms on finite dimensional vector spaces,

- J. Dieudonne's work on matrix groups,
- Representation theory developed by Frobenius, Burnside, Schur,...
- P. Hall's work on solvable groups and $p$-groups;
- Wielandt's work on permutation groups,
- Brauer's initiating the theory of modular representations;
- Grun's work on transfer,
- Hall-Highman theory,..

**B.** *The three major breakthrough in Fifties:*

**(i)** Richard Brauer's suggestion (in ICM 1954, at Amsterdam) that simple groups of even order could be classified by the centralizers of their involutions;

**(ii)** Claude Chevalley's 'algebraization of simple Lie groups' in his famous work in 1955 (Tohaku J.) and subsequent variations of his theme due to Steinberg, Hertzig and Ree.

This gave a uniform construction of the then known matrix simple groups.

Also, it constructed a few, then unknown, simple groups.

More significantly, it provided a general frame work to understand the structure and the representation theory of all these groups.

Using a very special double coset decomposition (called *Bruhat decomposition*) they all admit, Tits constructed a uniform geometric structure to study these groups. These structures are called *spherical buildings*.

A spherical building is a pair $(\Delta, \mathcal{A})$ consisting of a regular simplicial complex $\Delta$ of finite rank *n* together with a family $\mathcal{A}$ of pairwise isomorphic thin regular subcomplxes of rank *n* satisfying some properties.

**(iii).** John Thompson's thesis (1959) solving the Frobenius conjecture and thus starting local analysis in finite groups (that is, the study of finite groups from the normalizers of $p$-subgroups).

A *Frobenius group is a* transitive permutation group such that no nontrivial element of it fixes more than one symbol and there exist nontrivial elements that fix a symbol.

(i) (Frobenius) Let $G$ be a Frobenius group and $H$ be the stabilizer of a point. Then, the subset $K$ of $G$ consisting of identity together with those elements which do not fix any element is a normal subgroup of $G$ of order $[G : H]$. $K$ is called the *Frobenius group* and $H$ is called the Frobenius Kernel.

(ii) (Thompson,1959) The Frobenius kernel is nilpotent.

**C.** *Sporadic groups:* An important component of the classification programme was the discovery and the construction of finite (sporadic) simple groups.The most enigmatic of them all is the **Monster**.

These groups were discovered in a variety of ways:

Some as sections (that is, factor groups of subgroups) of groups of symmetries of some very special mathematical structures:

$*$partitions of $\mathbb{F}_q^n$ by spheres ( linear perfect Hamming codes);

$*$an exceptional lattice in $\mathbb{R}^{24}$ (the Leech lattice);

$*$Strongly regular graphs;

Some of them owe their existence to some very exceptional mathematical situations:

∗ exceptional nonsplit extensions;

∗ direct sum decompositions of the Lie algebra of type $E_8$ over complex numbers;

∗ groups generated by a conjugacy class of involutions with very few possibilities for the orders of the product of any two of them;

∗ exceptions to the general pattern of groups with a given class of involution centralizer.

In sixties and early seventies, simple groups satisfying some additional conditions ( for example, groups with bounds on lengths of flags of subgroups, groups with restrictions on the number of prime divisors, special choices for possible centralizers of involutions of finite simple groups, etc.) and some rather special configurations (lattices; geometric/combinatorial configurations; etc.) were examined in search of new simple groups.

Even as late as mid seventies, prominent players in classification (Brauer 1979, Conway, for example) were not sure if- and some even were hoping against - the number of the sporadic simple groups is finite.

## **Extra-special 2- groups play a significant role** in simple groups.

“Failure of arguments in the presence of extra-special 2- groups give rise to sporadic simple groups” -John G.Thompson (in essays for Phillip Hall)

Extra special 2-groups are finite anologues of Heisenberg groups.

A majority of sporadic simple groups have large extra-special groups. Not all though: $M(22)$ and $M(23)$, for example, don’t.

### Definition

An extraspecial 2-subgroup $Q$ of $G$ is said to be *large* in $G$ if

$$C_G(Q) = Z(Q) =: Z; \quad Q \lhd C_G(Z); \text{ and}$$

$$Q \nleqq N_G(K) \text{ for each } 1 \neq K < G \text{ and } |K| \text{ is odd.}$$

In his recent account of the theory of sporadic simple groups, Aschbaher characterizes many sporadic simple groups $G$ by the following property:

Let $L$ be a group and $n$ be a positive integer.

**Hypothesis** $\mathcal{H}(n, L)$**:** $G$ is a finite group containing an involution $z$ such that

$$
\begin{aligned}
(*) &\quad F^*(C_G(z)) = Q \simeq 2^{1+2n}, \\
(**) &\quad C_G(z)/Q \simeq L; \text{ and} \\
(***) &\quad z \text{ is not weakly closed in } Q \text{ with respect to } G.
\end{aligned}
$$

Here,

(i) $F^*(G) = F(G)E(G)$, called the *generalized Fitting subgroup* of $G$, where $F(G)$ is the *Fitting subgroup* of $G$ and $E(G)$ is the *layer* of $G$. $F(G)$ and $E(G)$ are characteristic subgroups of $G$, maximal subject to being nilpotent and semisimple, respectively.

   A group $X$ is said to be *semi-simple* if it is a product of quasi-simple groups $\{X_i\}$ with $[X_i, X_j] = 1$ for all $i \neq j$. A group is *quasi simple* if $X = [X, X]$ and $X/Z(X)$ is simple.

(ii) If $W < H < G$, then $W$ is said to be *weakly closed in* $H$ relative to $G$ if $W$ is the only $G$-conjugate of it contained in $H$.

Following groups are characterized as simple groups satisfying the hypothesis $H(n, L)$:

$$[M_{24}, \mathcal{H}(3, L_3(2))]$$

$$[J_2, \mathcal{H}(2, A_5)]$$

$$[Suz, \mathcal{H}(4, Sp_6(2))]$$

$$[J_4, \mathcal{H}(6, Aut(Z_3 \cdot M_{22}))]$$

$$\left[Co_1; \mathcal{H}\left(4, \Omega_8^+(2)\right)\right]$$

$$[F_3 = Th; \mathcal{H}(4, A_9)]$$

$$[F_5 = \text{Harada}; \mathcal{H}(4, A_5 2\mathbb{Z}_2]$$

$$[F_2 = BM, \mathcal{H}(11, Co_2)]$$

$$[F_1 = M, \mathcal{H}(12, Co_1)]$$

Unlike the unifying notion of Bruhat decomposition for the groups previously mentioned, a general unifying theme for all finite nonabelian simple groups is not yet known. As Ronald Solomon succinctly puts:

'A still elusive will-O-the wisp is an elegant set of axioms, in the spirit of Tits axioms for a building, defining a class of geometries for all finite simple groups and perhaps more, but not too much more!

**Some recent expository articles:**

1. Michael Aschbacher, Notices of AMS 51 (2), (2004) 736-740.
2. Ron Solomon, Notices of AMS 42 (2), (1995) 231-239.
3. Terry Gannon, Moonshine beyond Monster, CUP.
4. J. McKay, ed. *Finite groups coming of age*, AMS contemporary Mathematics V.45 (1982).
5. Ronald Solomon, BAMS, V. 38 (2), 315-352.

## Classification of finite simple groups

### Theorem

*Any finite simple group is isomorphic to one of the following:*

(i) *A cyclic group of prime order*

(ii) *An alternating group* $A_n$ $(n \geq 5)$

(iii) *A member of one of the 16 infinite families of groups of Lie type*

(iv) *26 sporadic simple groups*

## Remark

*(a) The definition of each of these groups makes it not a very simple statement.*

*(b) Every simple group contains an involution. Involutions play a very central role in the structure of simple groups. Remarkably, all simple groups, except for members of one infinite family of groups (the Suzuki groups), contain elements of order* 3*. Do they also play any major role?*

*(c) Most simple groups are of Lie type. They all admit uniform construction, subgroup structure, geometric structures they are symmetry groups of, representation theory. Also, they are particular cases of a much larger class of (reductive algebraic and Kac-Moody) groups, sharing all the above features.*

*In all groups of Lie type, the role of Coxeter groups is central.*

*(f)The dihedral groups and more generally the reflection groups, extra special groups and the algebra of octonions play major role in these groups.*

*(g) Most finite groups are nilpotent groups, but they exist in huge numbers.*

*Is there a theory of groups with a given set of simple groups as composite factors in analogy with the theory of solvable groups?*

## Consequences

Several basic questions in group theory are solved using classification. At least, the first two below are proved by case-by-case verification.

**Some examples:**

1. (Schrier's conjecture) The outer automorphism group of a finite simple group is solvable.
2. (Frobenius conjecture) Let $G$ be a finite group and $n$ be a divisor of $|G|$. If $G$ has exactly $n$ solutions for the equation $x^n = 1$, then these solutions form a subgroup of $G$.
3. Classification of $t$-transitive groups, $t \geq 2$.
4. Classification of certain classes of permutation polynomials.

Several questions are reduced to questions about simple groups (for example the O'Nan-Scott theorem about the maximal subgroups of symmetric groups and Aschbachers theorem about the maximal subgroups of the classical groups). However, no such reduction seems to be known about the question of realizing a finite group as the Galois group of an extension field of $\mathbb{Q}$.

## (A) Finite simple groups of Lie type (Chevalley, Steinberg, Hertzig, Ree,Tits)

With an indecomposable root system

$$\Sigma \in \{A_n, B_n, C_n, D_n, F_4, G_2, E_6, E_7, E_8\}$$

in $\mathbb{R}^n$ and a field $k$, Chevalley associated a group $G_\Sigma(k)$ and all its central nonsplit extensions (using an integral Lie basis for the simple Lie algebra of type $\Sigma$ over $\mathbb{C}$), now called a *Chevalley group*. The nonabelian sections of these groups when $k$ is a finite field are finite. Except those of order less than 60, they are all simple. Explicitly, they are

**(i) The classical groups** ($q$, a prime power) :

$A_n(q) \simeq L_{n+1}(q)$ for $n \geq 1$ except $L_2(2)$ and $L_2(3)$
(general linear group)

$C_n(q) \simeq PSp_{2n}(q)$ for $n \geq 2$ except $PSp_4(2)$ (Symplectic group)

$B_n(q) \simeq P\Omega_{2n+1}(q)$ for $n \geq 3$, $q$ odd (orthogonal group)

$D_n(q) \simeq P\Omega_{2n}^{+}(q)$ for $n \geq 4$ (orthogonal group)

${}^2D_n(q) \simeq P\Omega_{2n}^{-}(q)$ for $n \geq 4$ (orthogonal group)

${}^2A_n(q) \simeq PSU_{n+1}(q)$ for $n \geq 2$ except $PSU_3(2)$ (unitary group)

## (ii) The exceptional groups

$$G_2\left(q\right), q \geq 3; \;\; F_4\left(q\right); \quad E_i\left(q\right) \;\; i \in \{6, 7, 8\}$$

(iii) **The twisted groups:** These are the fixed point subgroups of some specific outer automorphism of order 2 (of order 3 in the case of $D_4$) outer automorphisms of some of the groups

$$G \in \{A_n(q), B_2\left(2^{2n+1}\right), C_2\left(2^{2n+1}\right), D_4(q), F_4, G_2\left(3^{2n+1}\right), E_6\left(q\right)\}$$

are also simple. These are

$$\begin{aligned}
{}^2B_2\left(2^{2n+1}\right) \simeq \; {}^2C_2\left(2^{2n+1}\right), &\text{ The Suzuki groups } (n \geq 2)\\
{}^2G_2\left(3^{2n+1}\right), &\text{ Ree groups } (n \geq 1)\\
{}^2F_4\left(2^{2n+1}\right), &\text{ Ree groups}\\
{}^3D_4\left(q\right) &\text{ The Steinberg's triality groups}\\
{}^2E_6\left(q\right)&\\
{}^2F_4\left(2\right)' &\text{ The Tits group}
\end{aligned}$$

The groups listed in (i),(ii),(iii) are collectively called *Finite groups of Lie type.*

Except for some groups of “small” orders, they are all simple.

The isomorphisms among the above are:

$$L_2(4) \simeq L_2(5) \simeq A_5;\ L_2(7) \simeq L_3(2);$$
$$L_2(q) \simeq A_6;\ L_4(2) \simeq A_8;\ \ U_4(2) \simeq PSp_4(3)$$

These isomorphisms correspond to different geometric realizations of these groups.

- Steinberg (1968) gave a uniform construction and characterization of all finite groups of Lie type as groups of fixed points of endomorphisms of a linear Algebraic group over the algebraic closure of a finite field.
  The following embeddings hold:
- $G_2(q) < F_4(q) < E_6(q) < E_7(q) < E_8(q)$.

  The algebra of Octonions play a central role in the construction of (at least) the following groups: $G_2(q)$, $F_4(q)$, $E_6(q)$

**Geometrically, groups of Lie type are realized as nonabelian sections of the automorphism groups of the following geometries:**

- Finite Desarguesian projective spaces of rank at least two: the general linear group $L_{n+1}(q), n \geq 1$.
- Finite classical polar spaces of rank at least two (due to Fredenthal,Tits, Buekenhout-Shult): the symplectic, unitary and orthgonal groups)
- Thick generalized $n$-gons (Tits), $n = 6, 8$: $G_2(q)$ and ${}^3D_4(q)$ for $n = 6$; and ${}^2F_4\left(2^{2n+1}\right)$ with $n = 8$
- Finite metasymplectic spaces (Tits): $F_4(q)$ and ${}^2E_6(q)$
- Spherical buildings (Tits) for all groups of Lie type
- A (specific) inversive plane of order $q, q = 2^{2n+1}$; that is, a $3 - \left(q^2 + 1, q + 1, 1\right)$ design: the Suzuki group ${}^2B_2\left(2^{2n+1}\right)$
- A (specific) unital of order $q, q = 3^{2n+1}$; that is, a $2 - \left(q^3 + 1, q + 1, 1\right)$ design: the Ree group ${}^2G_2\left(3^{2n+1}\right)$

*Classification of generalized polygons, the inversive planes and the unitals are major problems in incidence geometry.*

- The group $G$ of isomorphisms of the poset $\mathcal{P}(V)$ of all nontrivial subspaces (that is, the *projective space* of dimension $n$ over $\mathbb{F}_q$ ) of a $n+1$ dimensional vector space $V$ over $\mathbb{F}_q$;
- The subgroup of $G$ consisting of all its elements commuting with a given, order reversing, involutory bijection of $\mathcal{P}(V)$

  (Equivalent, the stabilizer in $G$ of a nondegenerate symplectic, unitary or quadratic form on $V$.

  Also, from the order preserving bijections of the subposet of $\mathcal{P}(V)$ consisting of isotropic subspaces relative to the defining nondegenerate symplectic, hermitian or quadratic form.

- Some of the groups are also realized as the stabilizer in $G$ of a system of certain multilinear forms on $V$:

  $G_2(q)$ : $(V, f, T)$ with $\dim . V = 7$, $f$ is a specific n.d. symmetric bilinear, $T$ is Dicksons alternating trilinear form;

  $F_4(q)$ :

  $E_6(q)$ : $\left(\mathcal{M}_3(q)^3, N\right)$ with $N\ (A, B, C) = \det(A) + \det(B) + \det(C) - tr(ABC)$, a cubic form on $\mathcal{M}_3(q)^3$;

  $E_7(q)$ :

- $G_2(q)$ is the automorphism group of the algebra of octonions over $\mathbb{F}_q$; it is also a section of the automorphism group of the generalized hexagon $H(q)$.

  $F_4(q)$ is the automorphism group of the 27- dimensional exceptional Jordan algebra over $\mathbb{F}_q$;

  $E_6(q)$ is a section of the automorphism group of the octonion projective plane.

# Special features of groups of Lie type

- Most finite simple groups are of Lie type.
- They all admit $(B, N)-$ structure, i.e., each such group $G$ contains subgroups $B$ and $N$ such that:

  (i) $G = < B, N >$;

  (ii) $B \cap N = T \triangleleft N$ and $W = N/T$ is a Coxeter group with $s'_1, \cdots, s'_n$ as a basic set of generating involutions of $W$;

  (iii) if $s_i, i = 1, \cdots, n$, is a set of elements of $N$ such that their images $s_i^{'}$ in $W$ are as in (ii), then

  $$(Bs_iB)(BwB) \subseteq BwB \cup Bs_iwB$$

  for all $s_i$ and $w \in W$;

  (iv) $s_iBs_i \neq B$ for each $s_i$.

## Remark

*(a) (i) and (iii) imply that $G = BNB$.*

*(b) Invert (iii) and replace $w^{-1}$ by $w$ to get*
*$(BwB)(Bs_iB) \subseteq BwB \cup Bws_iB$ for all $s_i$ and $w \in W$.*

## Remark

*Let $X = G/B = \{gB : g \in G\}$. Then $BwB$ is the union of the elements of the $B$- orbit under the $G$- action on $X$ by left multiplication. Condition (iii) says that $s_i$ leaves this orbit invariant or takes it to the $B$- orbit containing $s_iwB$.*

*Groups admitting $(B, N)-$ structure share several uniform features: simplicity; poset of subgroups containing conjugates of $B$ leading to the construction of the corresponding building.*

## Bruhat decomposition

$$G = \cup_{\overline{w} \in W} BwB,$$

$$G = \cup_{\overline{w} \in W} BwB_w,$$

where $B_w$ is the subgroup of $B$ generated by the root subgroups corresponding to the positive roots which are mapped to negative roots by $\overline{w}$. In fact, each element of $G$ can be written *uniquely* as $bwb'$ with $b \in B, w \in W$ and $b' \in B_w$. In particular, if $k$ is finite, then

$$|G_\Sigma(q)| = |B| \sum_{w \in W} q^{n(w)}; |B| = q^{|\Sigma^+|}, \text{and } \sum_{w \in W} q^{n(w)} = \prod_{i=1}^{n} \frac{(1-q^{d_i})}{(1-q)}.$$

Here $n(w)$ is the number of positive roots which are mapped to negative roots by $w$; and $d_1, \cdots, d_n$ are the degrees of homogeneous, algebraically independent, polynomials $I_1, \cdots, I_n$ over $\mathbb{C}$ in $n$ variables which form a set of generators for the ring $I(V)$ of invariants for the action of the Weyl group on the symmetric algebra $S(V)$ via the faithful action of $W$ on the real vector space $V$. By a theorem of Chevalley, the action of $W$ on

**Some basic facts about $d_i' s$.**
The numbers $\{d_i\}$ are uniquely determined by $W$ and satisfy:

(a) $|W| = \prod_{i=1}^n d_i;$
$\sum_{i=1}^n (d_i - 1) = |\Sigma^+|$
$\prod_{i=1}^n (1 - t^{d_i})^{-1} = \frac{1}{|W|}(\sum_{w \in W} \det(1 - wt)^{-1}).$

These numbers
for $A_n$ are $(2, 3, \cdots, n+1)$
for $B_n$and $C_n$ are $(2, 4, \cdots, 2n)$
for $D_n$ are $(2, 4, \cdots, 2n-2, n)$
for $E_6$ are $(2, 5, 6, 8, 9, 12)$
for $E_7$ are $(2, 6, 8, 10, 12, 14, 18)$
for $E_8$ are $(2, 8, 12, 14, 18, 20, 24, 30)$
for $F_4$ are $(2, 6, 8, 12)$ and
for $G_2$ are $(2, 6)$

### Characteristic of a finite group:

- A prime number $p$ is defined to be a *characteristic of a finite group* $G$ if $C_H(O_p(H)) \subseteq O_p(H)$ for each $p$-local subgroups $H$ of $G$.
- A group may have several characteristics. If $G$ is of Lie type, its characteristic is that of the field over which it is defined and the parabolic subgroups of $G$ are characterized as the subgroups $Q$ of $G$ such that $Q = N_G(O_p(Q))$.
  We define a subgroup $Q$ of $G$ to be *$p-$parabolic* if $Q = N_G(O_p(Q))$.
- Some groups may have more than one characteristic associated with it, for example ${}^2A_3(2) \backsimeq U_4(2, 2^2) \backsimeq C_2(3)$ and some may not have a characteristic associated with it [example, $A_n$].
- However, if a group admits a characteristic, then taking $B = N_G(P) = PH$ and $N = N_G\,(H)$, we can try to construct a building-like geometry.

# (B) The 26 sporadic simple groups

- The five Mathieu groups: $M_{11}$, $M_{12}$, $M_{22}$, $M_{23}$, $M_{24}$;
- The seven groups from the Leech lattice: $\cdot 1, \cdot 2, \cdot 3$ (the Conway groups); $McL$; $HS$; $Suz$; $J_2$
- The five Monster groups: $\mathbb{M}$ (Monster); $BM$ (Baby Monster); $Th$ (Thompson group); $HN$ (Harada-Norton); $He$ (Held)
- Fischer's three transposition groups: $Fi_{22}, Fi_{23}, Fi'_{24}$(Fischer groups)
- The six groups not involved in $\mathbb{M}$: $J_1$, $J_3$, $J_4$, $O'N$ (O′nan group), $Ly$, $Ru$

## Methods of discovery:

**I The Mathieu groups:** They were discovered as automorphism groups of Witt designs:

$$\begin{array}{cccc} 2-(9,3,1) \rightarrow & 3-(10,4,1) \rightarrow & 4-(11,5,1) \rightarrow & 5-(12,6,1)\,; \\ 2-(21,5,1) \rightarrow & 3-(22,6,1) \rightarrow & 4-(23,7,1) \rightarrow & 5-(24,,8,1). \end{array}$$

Later, they were also realized as sections of automorphism groups of linear codes:

- $M_{11}$ from $[11,6,5]$ Golay code over $\mathbb{F}_3$ and $M_{12}$ from $[12,6,5]$ Golay code over $\mathbb{F}_3$
- $M_{22}$ from $[22,12,6]$ Golay code over $\mathbb{F}_2$; $M_{23}$ from $[23,12,7]$ Golay code over $\mathbb{F}_2$;

  $M_{24}$ from $[24,12,8]$ Golay code over $\mathbb{F}_2$.

Along with alternating and symmetric groups, these are the only $t$-transitive groups, $t \geq 4$.

## Definition of the $[24, 8, 5]$ Golay code over $F_2$ and $M_{24}$:

- $\Omega = \mathbb{F}_{23} \cup \{\infty\}$
- $\mathcal{P}(\Omega) \simeq \mathbb{F}_2^{24}$, the power set of $\Omega$ considered an abelian group with symmetric difference as group operation;
- $\pi : \mathcal{P}(\Omega) \times \mathcal{P}(\Omega) \to \mathbb{F}_2$ taking $(A, B)$ to $|A \cap B| \pmod 2$, a symmetric nondengerate bilinear form.
- $N = \{xr : x \in \mathbb{F}_{23}\}$
  $\Omega = \{N - i : i \in \mathbb{F}_{23}\} \subset P(\Omega)$
- $\mathcal{G}_{12} := \langle A : A \in \mathcal{O} \rangle \leq \ \mathcal{P}(\Omega)$, the Golay code; a self-dual, binary $[24, 12, 8]$-code with weight enumerator

$$0^1 \ 8^{759} \ 12^{2576} \ 8^{759} \ 24^1$$

- $M_{24} :=$ Stab $(\mathcal{O})$ in Sym $(\Omega)$, the Mathieu-group; it is a simple group and acts 5-transitively on $\Omega$.

## II. The Conway groups: $\cdot 1, \cdot 2, \cdot 3$; the Maclaughlin group and the Highman-Sims group

Recall that a *lattice* of rank $n$ is a free abelian groups of rank $n$ with an integer valued, positive definite, symmetric bilinear form.

By Neumier's classification, among the 26 mutually nonequivalent lattices of rank 24 , the Leech lattice $\Lambda$ is the unique one (up to, equivalence) such that

(a) $||x||^2 \in 2\mathbb{Z}$ for each $x \in \Lambda$ (i.e, *even*);

(b) det $(\langle x_i, x_j \rangle_{1 \leq i,j \leq 24}) = \pm 1$ for any basis $x_1, \cdots, x_n$ of $\Lambda$ ( i.e., *unimodular*; equivalently, this means that $\Lambda$ has only one point per unit volume);

(c) $||x||^2 \neq 2$ for each $x \in \Lambda$ and there are elements $x \in \Lambda$ with $||x||^2 = 4$ (i.e., *without roots*)

(d) there is no $y \in \mathbb{R}^n \setminus \Lambda$ with $\langle x, y \rangle \in \mathbb{Z}$ for each $x \in \Lambda$.

Explicitly: Let

$$V = \bigoplus_{x\in\Omega} \mathbb{R}_x$$

$$\begin{aligned} \left(\sum_{x\in\Omega} \lambda_x x, \sum_{y\in\Omega} \mu_y y\right) &= \sum \lambda_x \mu_x, \text{ a nondegenerate symmetric bilinear form} \\ q\left(v\right) &= \left(v, v\right)/16, \text{ a positive definite quadratic form on } V \end{aligned}$$

For $A \subseteq \Omega$, define $e_A = \sum_{a\in A} \in V$.

For $x \in \Omega$, define $\lambda_x = e_\Omega \setminus 4x$.

Then, the *Leech lattice* $\Lambda$ is can be taken as the set of all vectors $v = \sum n_x x \in V$ such that:

(i) $n_x \in \mathbb{Z}$ for all $x \in \Omega$.

(ii) $m(v) = \left(\sum n_x\right)/4 \in \mathbb{Z}$.

(iii) $n_x \equiv m(v) \bmod 2$ for all $x \in \Omega$.

(iv) $C(v) = \{x \in \Omega : n_x \neq m(v) \bmod 4\} \in \mathcal{G}$.

For $n = 1, 2, 3, \ldots$, define

$$\Lambda_n = \{v \in \Lambda : q(v) = n\}$$

Then,

$$\Lambda = \Lambda_1 \cup \Lambda_2 \cup \cdots$$

and the isometry group $\cdot 0$ of $\Lambda$ is a nonsplit extension of the simple group $\cdot 1$ by its centre $\langle -Id \rangle$ of order 2.

The simple groups $\cdot 2$, $\cdot 3$, $McL$, $HS$ appear as follows:

$$C_2 \times \cdot 2 = Stab_{\cdot 0}(x) \text{ for } x \in \Lambda_2; \; C_2 \times \cdot 3 = Stab_{\cdot 0}(x) \text{ for } x \in \Lambda_3$$
$$McL = Stab_{\cdot 0}(x) \text{ for } x \in \Lambda_5; \qquad HS = Stab_{\cdot 0}(x) \text{ for } x \in \Lambda_7$$

**III.** *Centralizers of involutions (Brauer's programme)*

Some time in the late 40's, Richard Brauer realized that some very simple properties of involutions lead to deep insights into the structure of finite groups.

The following simple, but very unique, property of a pair of involutions of a group is very significant:

(a) **(Brauer and Fowler,1953)** If $t$ and $u$ are involutions in a group $G$, then the subgroup $H$ of $G$ generated by them is a dihedral group of order $2n$, where $n = |tu|$.

- If $n$ is odd, then $t$ and $u$ are conjugate in $H$.
- If $n$ is even, then $\langle tu \rangle$ contains a unique involution.

This and a very simple counting argument leads to:
(b) (**Thompson's order formula**) Let $G$ be a finite group with at least two conjugacy classes $u^G$, $v^G$ of involutions. Let $u_1 = u$, $u_2 = v$, $u_3, \ldots, u_t$ be representatives of distinct conjugacy classes of involutions in $G$. For every pair $(x, y) \in u^G \times v^G$, there is a unique integer $n(x, y)$ and a unique $i \in \{1, 2, \ldots, t\}$ such that

$$w = (xy)^{n(x,y)} \in u_i^G$$

Define

$$R(u, v, u_i) = \left\{(x, y) \in u^G \times v^G : (xy)^{n(x,y)} \in u_i^G\right\}.$$

Then,

(i) $R(u, v, u_i) =$
$\left\{(x, y) \in [u^G \cap C_G(u] \times [v^G \cap C_G(v))] : (xy)^{n(x,y)} = u_i\right\}$

(ii) $|G| = \sum_{i=1}^{t} |R(u, v, u_i)| \ \frac{|C_G(u)||C_G(v)|}{|C_G(u_i)|}$.

Thus, the order of $G$ can be computed from the character table of $C_G(u_i)$ and the fusion pattern of the conjugacy classes of their involutions.

Proof.

$$\frac{|G|}{|C_G(u)|} \cdot \frac{|G|}{|C_G(v)|} = \left|u^G\right| \left|v^G\right| = \sum_{i=1}^{t} |R(u, v, u_i)| \cdot \left|u_i^G\right| = \sum_{i=1}^{t} |R(u, v, u_i)$$

□

*The case when $G$ has a single class of involutions is more involved:*

(3) (Michler) Let $G$ be a finite group with a unique conjugacy class $z^G$, $z \neq 1$, of involutions. Let $H = C_G(z)$. Let $\pi$ be the smallest set of primes $p$ dividing $|H|$ and is such that $C_G(g)$ is a $\pi$-subgroup of $G$ for each $\pi$-element $1 \neq g \in G$. Let

- $r_1, \ldots, r_s$ be a set of representatives of strongly real conjugacy classes of $\pi$- elements of $G$; and
- $b_1, \ldots, b_t$ be a set of representatives of the strongly real conjugacy classes of $\pi'$-elements of $G$.

Then, the following holds:

(a) $d\left(r_i\right) = \left|\left\{(x, y) \in z^G \times z^G : xy = r_i\right\}\right| \leq \left|C_G\left(r_i\right)\right|$ for $1 \leq i \leq s$.

(b) $d\left(b_j\right) = \left|\left\{(x, y) \in z^G \times z^G : xy = b_j\right\}\right| = \left|C_G\left(b_j\right)\right|$ for $1 \leq j \leq t$.

(c) $c = 1 + \sum_{i=1}^{s} d\left(r_i\right) \frac{|H|}{|C_G(r_i)|}$ is a positive integer and is uniquely determined by $H$ are the $s$ extended centralizer $C_G^*\left(r_i\right)$.

(d) $|G| = C\,|H| + t\,|H|^2$.

The following result is elementary and fundamental:

### Theorem

*(Brauer and Fowler, Annals 1953) If $t$ is an involution of a nonabelian simple group $G$ and $|C_G(t)| = n$, then $G$ can be embedded in $A_{n^2-1}$. In particular, there are only a finite number of finite simple groups with a given involution centralizer.*

In view of this, Brauer initiated the programme to determine all finite simple groups with a given centralizer of an involution. This programme, along with the plethora of new ideas introduced in the monumental works

- proving that a finite group admitting a fixed point free automorphism of prime order is nilpotent (Thompson, Math. Zeit. 1959);
- that each nonabelian finite simple group contains an involution (W. Feit and J. Thompson, PJM1963); and
- the classification of nonabelian simple groups such that the normalizer of each $p$-subgroup is solvable ( the so called N-groups) (J. Thompson, I to VI, 1968-1974)

brought in a sea change in the approach to the study of simple groups. The methods of local analysis introduced were central to the whole classification programme.

While some of the earlier theorems (for example, Grun's theorems) gave conditions under which a group admits a nontrivial homomorphism, some of the later theorems (for example, Thompson's factorization theorems, Glauberman's $Z^*$-theorem) gave conditions for the existence of normal subgroups.

### Theorem

*(Thompson's theorem on N-groups) Let $G$ be a simple group in which the normalizer of any solvable subgroup of order greater than 1 is solvable. Then $G$ is one of the following groups*

(i) $L_2(q), q > 3$
(ii) $Sz\left(2^{2m+1}\right), m \geq 1$
(iii) $PSL_3(3)$
(iv) $M_{11}$
(v) $A_7$
(vi) $PSU_3(3)$
(vii) ${}^2F_4(2)'$

An interesting consequence is the following characterizations of solvable groups:

### Theorem

*(Thompson) The following conditions are equivalent for a group $G$.*
*(i) $G$ is solvable.*
*(ii) Every pair of elements of $G$ generate a solvable group.*
*(iii) If $x, y, z$ are three nonidentity elements of $G$ of pairwise coprime order, then $xyz \neq 1$.*
*(iv) If $x_1, x_2, \ldots$ are nonidentity elements of $G$ of coprime order, then $x_1 x_2 \ldots \neq 1$.*
*(v) For any nonprincipal irreducible character $\chi$ of $G$, there exists a prime $p$ and a Sylow $p$-subgroup $P$ of $G$ such that the restriction of $\chi$ to $P$ does not contain the principal character of $P$ as a constituent.*

Brauer's programme turned out to be so successful that many new sporadic simple groups were discovered in pursuit of this programme and many sporadic simple groups were characterized by their involution centralizers.

Many sporadic groups appeared as exceptions to general patterns. Here is an example of an early result in this programme:

## Theorem

*(Brauer,1966), Let $G$ be a finite group satisfying the following properties:*

*(i) There exists an involution $t$ such that $C_G(t) \simeq GL_2(q)$.*

*(ii) If $s$ is an element of the centre of $C_G(t)$, $s \neq 1$, then $C_G(t) = C_G(s)$.*

*(iii) $G = G'$.*

*If $q \equiv -1 \pmod 4$, $q \neq 1 \pmod 3$, then either $G$ is isomorphic to $PSL_3(q)$ or $q = 3$ and $G$ is isomorphic to $M_{11}$.*

Commenting on this insight that it is far from obvious, W. Feit (ICM 74) mentions that this eluded even a mathematician of the calibre of Burnside, particularly after he had proved the following beautiful

### Theorem

*$SL_2(2^a)$, $a > 1$, are the only simple groups of even order in which the order of each element is either 2 or odd.*

(Burnside, Trans. of Cambr. Phil. Soc. 18 (1900), 269-276).
(Feit, BAMS 1 (1979),1-20).
The following groups were discovered as a part of this programme:

$$J_1, J_2, J_3, J_4, He, Ly, \mathbb{M}$$

and the following groups are uniquely determined by the centralizer of involution:

$$J_1, H_5, Ha, Th, M_{22}, M_{23}, Co_3, J_4, Ru, McL, Suz, ON, Fi_{22}, Fi'_{24}.$$

Determination of all finite groups with a given centralizer of an involution, particularly the classical groups, is still incomplete.

**Suzuki's (partial) list of satellites, 1969:**
In the following, $z$ is an involution in the centre of a Sylow 2-subgroup of the simple group $G$. A *satellite* is defined as a, not necessarily simple, group having an isomorphic involution centralizer.

| $G$ | $C_G(z)$ | Satellites of $G$ |
|---|---|---|
| $M_{11}$ | $2 \cdot S_4$ | $L_3(3)$ (Brauer) |
| $M_{24}$ | $2^{1+6} : L_3(2)$ | $L_5(2)$, $He$ (Held) |
| $J_2$ | $2^{1+4} : A_5$ | $J_3$ (Janko) |
| $A_6$ | $D_8$ | $L_2(7) \simeq L_3(2)$ (Suzuki) |
| $A_8$ | $2^3 : S_4$ | $A_9$ (Held) |
| $A_{12}$ | $2^5 : S_6$ | $A_{13}, Sp_6(2)$ (Yamaki) |
| $A_{4k}$ | $2^{2k-1} : S_{2k}$ | $A_{4k+1}$, $k = 4, 5, \ldots$ (Kondo) |

**IV.** *Transposition groups:*

In an attempt to characterize the symmetric groups, Bernd Fischer studied finite groups generated by a conjugacy class of involutions.

Motivated by the fact that $S_n$ is generated by a conjugacy class of involutions (namely, transpositions) such that the product of any two of them is $1, 2$ or $3$, Fischer started investigating groups generated by a conjugacy class of involutions with restrictions on the orders of the product of pairs of its elements.

### Definition

A conjugacy class $D$ of involutions of $G$ is said to be a class of $p$-transpositions, $p$ an odd prime, if $|xy| \in \{1, 2, p\}$ for all $x, y \in D$. If $G = \langle D \rangle$, $G$ is said to be a $p$-transposition group.

## Example

The set of transpositions in $S_n$ ($\backsimeq A_{n-1}$). More generally, for any finite irreducible root system with only one root length (i.e. those of types $A_n, D_n, E_n$), the Weyl group $W$ is a 3-transposition group and the set $D$ of all reflections is a class of 3-transpositions.

Fischer's classification of 3-transposition groups led to three new simple groups $Fi_{22}, Fi_{23}, F'i_{24}$.

Specifying the orders to be at most 4 (respectively, at most 6) includes Baby Monster $BM$ ( respectively, $BM$ and the Monster $\mathbb{M}$).

These investigations by Fischer, and also later by Aschbacher and Timmesfeld, lead them naturally to introduce geometric methods in group theory.

The results listed below are due to Fischer and are all about a group $G$ generated by a conjugacy class $D$ of involutions. They clearly indicate the natural emergence of geometric ideas.

### Theorem

*(Fischer) If $D$ is a class of p-transpositions such that:*
*(i) no three elements of $D$ generate a 2-group;*
*(ii) $C_D(x) \neq x$ for each $x \in D$,*
*then, $G = S_4$ or $S_5$ and $p = 3$.*

### Theorem

*Suppose that there is an odd prime $p$ such that $|xy|$ is a power of $p$ for each pair $x, y$ of distinct elements of $D$. Then, $G'$ is nilpotent.*

## Theorem

*Suppose that distinct elements of $D$ do not commute and*

$$C_G(x) = O_2(C_G(x)) \times O(C_G(x))$$

*for all $x \in D$. Then, $G$ is solvable.*

## Theorem

*Let $E$ be a set of pairwise commuting involutions of $D$ of maximum size $n$. Then:*
*(i) $N_G(E)$ contains a Sylow 2-subgroup of $G$;*
*(ii) $N_G(E)$ acts 2- transitively on $E$;*
*(iii) $N_G(E)/C_G(E)$ is isomorphic to one of:*

$S_n, A_n, GL(n,2), L_m(4)\, S_n, A_n, GL(n,2), L_m(4)$ *with*
$m = [n/2], S_{2^n} \cdot GL(n,2), M_{22}, M_{23}, M_{24}.$

## Theorem

*For* $x \in D$*, set* $D_x = C_D(x) \setminus \{x\}$ *and* $F_x = D \setminus (D_x \cup \{x\})$*. Then:*

*(i)* $\langle D_x \rangle$ *acts transitively on* $D_x$ *as well as on* $F_x$*.*

*(ii)* $G$ *acts on* $D$*, by conjugation, as a rank* $3$ *permutation group with stabilizer* $\langle D_x \rangle = C_G(x)$ *having* $C_G(x)$*-orbits* $\{x\}$*,* $E_x$ *and* $F_x$*.*

*(iii) If* $O(\langle D_x \rangle) \nleq Z(\langle D_x \rangle)$*, then* $G \simeq S_5$*. If* $O_2(\langle D_x \rangle) \nleq Z(\langle D_x \rangle)$*, then* $G \simeq Sp(n,2)$ *or* $U_m(2)$*. If* $\langle D_x \rangle$ *is solvable, then*

$$G \simeq S_5, S_6, U_4(2) \, or U_3(2).$$

## Theorem

*( Main Theorem) Let $G$ be generated by a conjugacy class $D$ of 3-transpositions. Assume that $Z(G) = \langle 1 \rangle$ and $G'$ is simple. Then, one of the following holds:*

(i) $G \simeq S_n$ and $D$ is the set of transpositions of $G$.
(ii) $G \simeq Sp_{2n}(2)$ and $D$ is the set of transvections.
(iii) $G \simeq U_n(2)$, the projective unitary group defined over a field of order 4 and $D$ is the set of transvections.
(iv) $G \simeq PO_n^{\mu,\pi}(3)$ is the subgroup of an $n$-dimensional orthogonal group over a field of 3 elements generated by a conjugacy class $D$ of reflections.
(v) $G$ is a (Fischer) simple group of type $M(22)$, $M(23)$ or $M(24)$, uniquely determined up to isomorphism and $D$ is a uniquely determined conjugacy class of involutions.

**Definition of** $PO_n^{\mu,\pi}(3)$: $V = V_n(3)$, $Q$, a nondegenerate quadratic form on $V$. For $v \in V$ with $Q(v) \neq 0$, define the reflection $t(v) : v \to V$ by $xt(v) = x - (x,v)\,v/Q(v)$. For $\pi = \pm 1$, let $D = D(\pi)$ be the set of reflections $t(v)$, $Q(v) = \pi$. Let $\mu(V) = \mu((V,Q)) := \det(J(X,f))$, the discriminant of the space $(V,Q)$. Here, $X$ is a basis of $V$ and $f$ is the bilinear form for $Q$ and $J(x,f)$ is the matrix $(f(x_i,x_j))$.

**Note:** $\mu(V) = \pm 1$ and $\mu(V) = (-1)^{n/2}\,Sgn(V)$ if $n$ is even. Here, $\mathrm{Sgn}(V) = +1$ if $Q$ is hyperbolic and -1 if elliptic.
$G := O_n^{\mu,\pi}(3) := \langle D_\pi \rangle$, where $\mu(V) = \pi$.

- $[O_n(3) : O_n^{\mu,\pi}(3)] = 2$
- $O_n^{\mu_1,\pi_1}(3) \simeq O_n^{\mu_2,\pi_2}(3)$ iff $\mu_1\pi_1^n = \mu_2\pi_2^n$
- $G$ is transitive on $D$ unless $n = 2$ and $\mathrm{Sgn}(V) = -1$.

The following result due to Aschbacher gives a converse to Fischer's theorem **??** :

### Theorem

*(Aschbacher, 72-73) Let $G$ be a group with $Soc\,(G) = 1$ and generated by a conjugacy class $D$ of involutions. If $G$ is a rank $3$ permutation group on $D$, then $D$ is a class of $3$-transpositions of $G$.*

### Definition

A conjugacy class of involutions is said to be a *class of odd transpositions* if the product of any two of its noncommuting elements is of odd order.

### Theorem

*(Baer and Suzuki) If $D$ is a conjugacy class of elements of prime order $p$ with the property that $\langle x, y\rangle$ is a $p$-group for each pair $x, y \in D$, then $D \leq O_p(G)$.*

### Corollary

*If $G$ is generated by a conjugacy class $D$ of involutions such that $|xy|$ is a power of $2$ for each $x, y \in D$, then $G$ is a $2$-group.*

### Definition

A conjugacy class $D$ of involutions is said to be a *class of* $\{3,4\}$*-transpositions* if the product of any 2 of them has order $1, 2, 3$ or 4. It is said to be *nondegenerate* if $|xy| = 4$ for some $x, y \in D$.

It is said to be a *class of* $\{3,4\}^+$*-transpositions* if, further, whenever $x, y \in D$ and $|xy| = 4$, then $(xy)^2 \in D$.

### Theorem

*(Timmesfeld, 70, 75) Let $G$ be a group with $Z(G) = 1$, $O(G) = 1$ and generated by a class of $\{3,4\}^{+}$-transpositions. Then, $G$ is isomorphic to one of the following:*

$$GL(n,2), n \geq 3; Sp(2n,2), n \geq 3; O_{2n}^{\pm}(2), n \geq 4$$
$$G_2(2)', {}^3D_4(2), F_4(2), {}^2E_6(2), E_6(2), E_7(2), E_8(2)$$

*Moreover, in each case, $D$ is uniquely determined by a class of 2-central involutions.*

Fischer developed a method to form, from a class $E$ of transpositions of a group $H$, a larger group $G$ containing $H$ and generated by a class $D$ of transpositions containing $E$.

The passage from $U_6(2)$ to $M(22)$, from $M(22)$ to $M(23)$ and $\mathbb{Z}_2 \times M(23)$ to $M(24)$.

$\mathrm{Aut}(M_{22}) = M_{22} \cdot \mathbb{Z}_2$ (split) is a generated by a class $D$ of $\{3, 4\}$-transpositions. The elements of $D$ necessarily induce outer automorphisms of $M(22)$.

## Theorem

*(Fischer/Leon-Sims) The baby monster BM is generated by a class $D$ of $\{3, 4\}$-transpositions such that $C_{BM}(x) \simeq {}^2\widehat{E}_6(2) \cdot 2$ for all $x \in D$.*

**V.** *Suzuki chain:*

**VI.** *Thompson's factorization:* An exceptional decomposition of Lie algebra of type $E_8$ over $\mathbb{C}$ as a direct sum $\oplus_{i=1}^{31} E_i$ of Cartan subalgebras such that, for $1 \leq i \neq j \leq 31$, there exists $k$ such that $[E_i, E_j] \subseteq E_k$.

- Existence of $\mathbb{M}$ that it is independently predicted by Bernard Fischer and Robert Griess in 1973. Griess constructed $\mathbb{M}$ in 1980 as the (full) automorphism group of a commutative, nonassociative, algebra of dimension $196,883$ over $\mathbb{Q}$. This algebra now is called the *Griess Algebra*.

- $\mathbb{M}$ is the largest of the 26 sporadic finite simple groups. Its order

$$8080,1742,4794,5128,7588,6459,9049,6171,0757,0057,5436,$$

$$8000,0000,00$$

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

is very large: appropriately $8 \times 10^{53}$ (15 prime factors!).

- $Out(\mathbb{M}) = 1$ and its Schur multiplier is trivial. That is, it is a perfect group and admits no nonsplit central extensions.
- Degrees of the two smallest complex irreducible representations are $196,883$ and $21296876$. It has a unique complex irreducible representation of degree $196,883$. Assuming its existence (conjectured by Griess and proved later by Norton), the character table of $\mathbb{M}$ was calculated by B.Fischer, D. Livingston, and M.P. Thorne.
- Thompson's uniqueness proof of this group (1979) as the group satisfying some conditions forced by the internal structure, and its subsequent construction due to Griess (1980), started with the assumption that it has an irreducible representation of degree $196,883$ and it is the smallest degree.

- Griess construction involves some very remarkable mathematical structures: binary $[24, 12, 8]$- Golay code, extra-special 2-group $2_+^{1+24}$, the Leech lattice.
- It is also the automorphism group of a Monster vertex algebra. It also appears as a subgroup of the diagram automorphisms of the Monster Lie algebra.
- Its permutation representation of smallest degree can be realized on a conjugacy class $\mathcal{F}$ of involutions of $\mathbb{M}$ ( the so called Fischer involutions). The degree is $|\mathcal{F}| = 97, 239, 461, 142, 990, 186, 000$ (approximately$10^{20}$).

## 2. Some striking properties of $\mathbb{M}$

**2.1** $\mathbb{M}$ has 194 conjugacy classes (as Cameron notes, a very small number for a group of this size). It has maximal subgroups of very large indices. These properties makes it a ‘highly’ nonsoluable group. Many features of the sporadic groups is in full display in this group.

**2.2**. **Its structure is very intricate:**

Not just because of its size : $Alt_{47}$ has a comparable order!

(2.2.a) **Twenty** of the **twenty six** sporadic simple groups appear as sections in $\mathbb{M}$.

Following simple groups are involved in $\mathbb{M}$ as subgroups of $C_{\mathbb{M}}(\sigma)/O_2(C_{\mathbb{M}}(\sigma)) \backsimeq \cdot 1$, where $\sigma$ is a (Conway) involution of $\mathbb{M}$ :

$\cdot 1, \cdot 2, \cdot 3, Suz, Mcl, HiS, HJ = J_2,$ the 5$-$Mathieu groups

Following simple groups appear as $C_{\mathbb{M}}\langle x\rangle / \langle x\rangle$ for $x \in \mathbb{M}$ with with $|x| = 1, 2, 3, 3, 5, 7$ respectively:

$\mathbb{M}= F_1, F_2\,(= BM)\,, F_3\,(= Th)\,, F'_{24}, F_5\,(= Harada)\,, F_7\ (=$

$C_{\mathbb{M}}\langle x\rangle$ splits over $\langle x\rangle$ in all cases except when $|x| = 2$.

$F_{22}, F_{23}$ appear as subgroups of $F'_{24}$.

(2.2.b) **Simple groups whose order divides $|\mathbb{M}|$ and their involvement in $|\mathbb{M}|$**

- $A_n (5 \leq n \leq 12)$ : $A_6$ is involved in, but not as a subgroup of $\mathbb{M}$; unique conjugacy class in all other cases.
- $L_2(q)$  For $q \in \{7, 8, 11, 13, 16, 17, 19, 31\}$ classification is known only partially. For $q \in \{23, 25, 49, 59\}$, complete classification is known. For $q = 29$, only a computer proof is known. There is a unique conjugacy class of subgroups in $\mathbb{M}$ which are isomorphic to $L_2(41)$; any such subgroup is self normalizing and maximal in $\mathbb{M}$. $L_2(27)$ and $L_2(71)$ are doubtful; $L_2(81)$ is involved, but not contained in $\mathbb{M}$.
- $L_3(3)$ partially classified; $L_3(4)$ is doubtful; $L_3(5)$ and $L_5(2)$ are involved, but not contained; unique conjugacy class of $L_4(3)$.
- $U_3(3), U_3(4), U_3(8), U_4(2)$ partially classified. $U_3(5)$ and $U_5(2)$ unique up to conjugacy.

- $U_4(2), U_4(3), U_6(2)$ are involved, but not contained.
- $S_4(4), S_6(2), S_8(2), O_7(3), O_8^+(2), O_8^-(2), O_8^+(3)$ are completely determined cases;
- $O_8^-(3), O_{10}^+(2), O_{10}^-(2)$ are involved but not contained.
- $G_2(3),^3 D_4(2),^2 F_4(2)'$ are completely determined;
- $G_2(4), F_4(2),^2 E_6(2)$ are involved, but not contained; $Sz(8)$ is doubtful.
- $M_{11}, M_{22}, M_{23}, M_{24}, (\cdot 1), (\cdot 2), (\cdot 3), Fi_{22}, Fi'_{24}, J_2, Suz, HS$, $McL, BM$ are involved, but are not contained.The case of $M_{12}, Fi_{23}, He, HN, Th, \mathbb{M}$ are completely determined. $J_1$ is not involved.

(2.2.c) The following nonsplit extensions appear as sections of $\mathbb{M}$:

$$2^{\cdot}F_2; \quad 2\cdot 2\cdot\ {}^2E_6(2); \quad 2^{5\cdot}GL(5,2), \quad 3^{\cdot}F'_{24},$$
$$3^{\cdot}B_3(3); \quad 3^{\cdot}G_2(3); \quad 3^{8\cdot\cdot}0^{-}(8,3); \quad 5^{3\cdot}SL(3,5) \text{ in } Mcl$$

Construction of $\mathbb{M}$ provides existence proof for the sporadic groups and the nonsplit extensions mentioned above.

**2.3. Prime divisors of $\mathbb{M}$:** (Ogg's observation 1975) For a prime number $p$, $X_{\Delta(p)}$ is of genus zero if and only if $p$ divides $|\mathbb{M}|$.

**2.4.** (J. Thompson) $\mathbb{M} = Gal\,(F/\mathbb{Q})$ for some algebraic extension of $\mathbb{Q}$.

(The degree of the polynomial is expected to be more than 1,200.)

**2.5.** A *p*- group in which every characteristic abelian subgroup is cyclic is called a *group of symplectic type*. Any such group is either the central product of an extraspecial group and a group which is either cyclic or is a 2 -group of maximal class (P. Hall).

For any finite group $G$, define

$$\sigma(G) = \{p : p \text{ a prime such that there is an element } x \in G \text{ with } F^*(C_G(x)) \text{ is of symplectic type }\}.$$

For example, $\sigma(\mathbb{M}) = \{2, 3, 5, 7, 13\}$.
**Conjecture (Thompson)**: If $(\sigma(G)) \geq 5$, then $G \simeq \mathbb{M}$.

In $\mathbb{M}$, the centralizers are:

$2^{1+24} \cdot (\cdot 1)$; $3^{1+12} \cdot 2Sz$; $5^{1+6} \cdot 2J_2$; $7^{1+4} \cdot 2A_7$; $13^{1+2} \cdot 2S_4$

## 2.6. Some remarkable coincidences occur:

The following sets of primes are equal:

$A_1 = \{p : (p-1) \text{ divides } 24\} = \{2,3,5,7,13\}$

$A_2 = \{p : \Gamma_0(p) \text{ is of genus zero}\}$

$A_3 = \{p : \cdot O$ contains an element of order $p$

which acts without fixed points on the Leech lattice and $p.G_p$ is its cer

$A_4 = \{p : \mathbb{M}$ contains an element of order $p$ such that its centralizer

is isomorphic to $p^{1+2d} \cdot G_p$, where $2d(p-1) = 24$ and $G_p$ is as in $A_3\}$

$\mathbb{M}$ has two conjugacy classes of involutions:

- $\mathcal{F} = \tau^{\mathbb{M}}$, the set of *Fischer involutions*; $C = C_{\mathbb{M}}(\tau) \backsimeq 2^{\cdot} F_2$ (nonsplit);
- $\mathcal{C} = \sigma^{\mathbb{M}}$, the set of *Conway involutions*; $C_{\mathbb{M}}(\sigma) \backsimeq 2_+^{+124} C_0$;
- $|\mathcal{C}| = N \times |\mathcal{F}|$, where $N$ is almost 100 million.

It also has elements $t$ of order 3 with $C_{\mathbb{M}}(t) \simeq 3^{1+12} \cdot 2\,\mathrm{Suz}$.

In fact: for each prime $p$ such that $p-1$ divides 24, there exist elements $t_p$ of order $p$ in $\mathbb{M}$ and $g_p \in (\cdot 0)$ of order $p$ such that

- the action of $g_p$ on $\Lambda$ is fixed point free;
- $C_p = C_{\mathbb{M}}(t_p) \simeq p^{1+d} \cdot G_p$, where $d = \frac{24}{p-1}$, $G_p \simeq C_{(\cdot 0)}(g_p)/\langle g_p \rangle$; $E_p \subseteq C_p$ is isomorphic to $p^{1+d}$ and $C_{C_p}(E_p) = Z(E_p)$.
- The action of $C_p$ on $E_p$ by conjugation induces a faithful representation of $G_p$ on $E_p/Z(E_p) \simeq \mathbb{F}_p^d$.

The number 24 seems to occur in different contexts. The following characterization of 24 have been useful:

The divisors $h$ of are precisely those integers for which $xy = 1 (\mathrm{mod}\ h)$ implies $x = y \pmod{h}$.

## 2.7. Involutions of $\mathbb{M}$

**(A) $\mathbb{M}$ as a $6$ -transposition group:**

$\mathbb{M}$ acts transitively on $\mathcal{F} = \tau^{\mathbb{M}}$ by conjugation.

The centralizer $C = C_{\mathbb{M}}(\tau)$ has 9 orbits $\mathcal{F}_i$, $i = 0, \cdots, 8$, on $\mathcal{F}$. Thus, $\mathbb{M}$ has a permutation representation of rank 9 on $\mathcal{F}$.

Fix $t_i \in \mathcal{F}_i$, let $n_i = |tt_i|$ and $t = t_0$. Then, $n_i$ is independent of the choice of $t_i$ in $\mathcal{F}_i$ (since $tt_i^x = (tt_i)^x$ for each $x \in C$) and

$$n_0, n_1, \cdots, n_8 \equiv 1, 2, 3, 4, 5, 6, 3, 4, 2.$$

Thus, $\mathbb{M}$ is a 6 -transposition group. Further, these are exactly the degrees of the irreducible representations of the binary icosahedral group.

1) Products of distinct elements of $\mathcal{F}$ are in 8 different conjugacy classes of $\mathbb{M}$ (using the Atlas notation):

$$1, 2A, 2B, 3A, 3C, 4A, 4B, 5A, 6A$$

The structure of the respective centralizers of elements in $\mathbb{M}$ are: $2^{\cdot}F_2$; $2^{2\ .2}E_6(2)$; $2^{2+22.}((\cdot 2))$; $M(23)$; $Th$; $2^{1+21.}Mcl$; $2.F_4(2)$; $HN$ ; $2.M(2)$ (This information was used to calculate the order of $\mathbb{M}$.)

2) Norton determined the number of tripes $\{x, y, z\}$ in $\mathcal{F}$ such that $xy, yz, zx$ are in specific conjugacy classes. This gives the intersection numbers of the centralizer algebra of the action of $\mathbb{M}$ on $\mathcal{F}$.

This algebra has a primitive idempotent of dimension 196883.

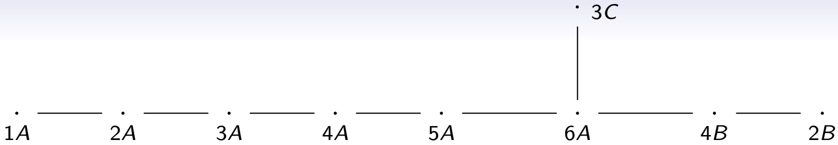
## (B) Connections with affine $\widetilde{E}_8$-lattice: McKay's observation:

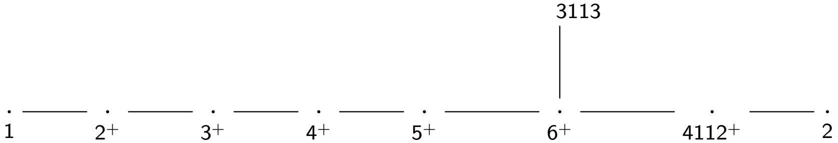
Let $\alpha_1, \cdots, \alpha_8$ be the fundamental roots in the root system $\Phi$ of type $E_8$ and $\alpha_M$ be the maximal root in $\Phi$. Set $\alpha_0 = -\alpha_M$. Then,

$$\alpha_M = \Sigma_{i=1}^{8} c_i \alpha_i = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8.$$

That is,

$$\Sigma_{i=0}^{8} c_i \alpha_i = 0 \text{ with } c_0 = 1.$$





$n^{+}\Gamma_0(n)^{+}$

$n\|h+$ for $\Gamma_0(n\|h)+$

McKay's observation was that after, rearranging the indices if necessary,

$$c_i = |tt_i|, \; i = 0, \cdots, 8,$$

Thus, we can associate a conjugacy class of elements of $\mathbb{M}$ with each vertex of $\widetilde{E}_8$.

Also, Glauberman and Norton observe that

$$\text{for } 1 \leq i \neq j \leq 8, tt_i \text{ is not conjugate to } tt_j \text{ under } \mathbb{M}. \qquad (1)$$

Thus, we can index the nodes of the $\widetilde{E}_8$ diagram by the conjugacy classes $tt_i$.

An interpretation of the edges of $\widetilde{E}_8$, if any, is not known.

Clearly, $c_i$ is the index of the sublattice of the $E_8-$ lattice spanned by the nodes $\alpha_j$, $j \neq i$,in the $\widetilde{E}_8-$diagram.

Thus, $c_i$ can be seen with in the lattice $\mathbf{E}_8$ .

There are other connections which tell how to associate each node with a suborbit. Using the atlas notation,

DIAGRAM

2) Let $K$ be the smallest conjugacy of the baby monster $\mathbb{B}$. The conjugacy classes in $K^2 = \{xy : x, y \in K\}$ has orders $1, 2, 2, 3, 4$ (Note: $\mathbb{B}$ is a 4-transposition group). These are the labels of $\widehat{\mathbb{F}}_4$, the affine diagram of type $F_4$:

Mackay observed that an order 2folding of the affine $E_7$-diagram gives the affine $F_4$-diagram $\widehat{F}_4$. An order two centre extension of $\mathbb{B}$ is the centralizer of an element $g \in M$ of order 2. The three-folding of affine $E_6$-diagram is affine $G_2$-diagram $\widehat{G}_2$ $M$ has 3 conjugacy classes f elements of order 3. The smallest of these (‘$3A'$) has a centralizer which is a triple cover of $F_{i_2 4} \cdot 2'$. Taking the smallest conjugacy class $\mathcal{C}$ of $F_{i_2 4} \cdot 2'$, $\mathcal{C}^2$ gives conjugacy classes of order $1, 2, 3$ and these are the labels for $\widehat{G}_2$. Note that $F_{i_2 4} \cdot 2'$is a 3-transposition group

## 2.8. It is very close to an infinite Coxeter group:

## 2.9. Moonshine conjectures: Modular connection:

This aspect has drawn most attention from mathematicians in other areas and string theorists.

**Moonshine properties**

‘Moonshine’ means ‘crazy or foolish ideas’. A typical example of its use is the following quote from E. Rutherford (discoverer of the nucleus of an atom) “The energy produced by the breaking down of the atom is a very poor kind of thing. Any one who expects a source of power from the transformations of these atoms is talking moonshine”.

‘Moonshine’ is also a name for corn whisky, especially if it is smuggled or distilled illegally.

1. In the expression for $j(q)$, the constant term could be arbitrary.
2. ‘Moonshine’ started when John McKay wrote to J. Thompson that

$$196,884 = 1 + 196,883$$

The coefficient of $q$ in the elliptic modular function $j(q)$ is $1+$ minimum of the dimensions of nontrivial complex representations of $\mathbb{M}$

1. Thompson (1979) pointed out that:

   *the next few coefficients of $j(q)$ are also simple positive integral linear combinations of the degrees of some irreducible representations of $\mathbb{M}$.* He suggested that there might be an infinite dimensional graded $\mathbb{C}[M]$-module

   $$W = \oplus_{n\in\mathbb{Z}} W_n = W_{-1} \oplus W_1 \oplus W_2 \oplus \cdots$$

   such that

   $$\dim(W_n) = \text{ coefficient of } q^{n-1} \text{ in } j(q) - 744$$

   for each $n \neq 0$. To charectarize $W$, Thompson suggested studying the modular transformation properties of the graded traces

   $$T_g\left(\tau\right) = \sum_n Tr\left(g\mid_{W_n}\right) q^{n-1}$$

   for each element $g$ of the Monster. For example $T_g\left(1\right) = j\left(\tau\right)$.

1. Conway and Norton (1979) calculated the first few terms of the McKay-Thompson series above by making reasonable guesses for the decomposition for the first few $W_n$ 's into direct sums of irreducible representations of $\mathbb{M}$.

$$\begin{aligned} 1 &= 1 \\ 196844 &= 196843 + 1 \\ 21493760 &= 21296876 + 196883 + 1 \\ 864299970 &= 842609326 + 21296876 + 2 \times 196883 + 2 \times 1 \end{aligned}$$

Here, numbers on the left side are the coefficients of powers of $q$ in $j(\tau)$ and the numbers on the right side are the dimensions of some irreducible representations of the monster. By calculating the first few terms, they found that the McKay-Thompson series

$$T_g(\tau) = q^{-1} + \sum_{n=0}^{\infty} Tr\left(g \mid_{W_n}\right) q^n, \qquad \tau \in \mathbb{H}, g \in \mathbb{M}$$

seemed to be hauptmodules of genus zero. On the basis of this, they made the famous Moonshine conjectures (1979) . They were proved by Borcherds in 1992 for which he got the Fields medal.

## Theorem

*Let $\tau \in \mathbb{H}$ and $q = e^{2\pi i\tau}$. Then, for each $g \in \mathbb{M}$, there is a formal q-expansion*

$$j_g(q) = q^{-1} + \sum_{n=1}^{\infty} a_n(g)q^n, \; a_n(g) \in \mathbb{Z}, n \geq 1$$

*such that: (i) for each integer $n \geq 1$, $g \mapsto a_n(g)$ is a character of* $\mathbb{M}$;
*(ii) For each $g \in \mathbb{M}$, there is a congruence subgroup $\Delta(g)$ of $SL(2, \mathbb{R})$ and a divisor h of the greatest common divisor of 24 and the order of g such that*
$\Gamma_0(o(g)h) \leq \Delta(g) <?\Delta(o(g)h)$ *and* $\frac{\Delta(g)}{\Gamma_0(o(g)h)}$ *is of exponent atmost 2*
*(iii) The genus of $X_{\Delta(g)}$ is zero.*
*(iv) $j_g$ is the Fourier expansion of a function $f_g(\tau)$ which is analytic on $\mathbb{H}$. The field of modular functions of weight zero with respect to $\Delta(g)$ is $\mathbb{C}(f_g)$.*

Conway and Norton wrote down a list of 194 normalized generators

$$T_g(\tau) = \sum_n c_n(g)\, q^n$$

of genus zero function fields arising from certain discrete subgroups of $PSL_2(\mathbb{R})$ such that for the first few integers $n$, $c_n$ were the characters of $W_n$.
For each $g \in \mathbb{M}$, there exists a genus zero subgroup $K$ of $PSL_2(\mathbb{R})$ such that $T_g(\tau)$ is the normalized main modular function for $K$ .
Note that

$$T_g(\tau) = T_{g^{-1}}(\tau) = T_{g^x}(\tau)$$

for all $g, x \in \mathbb{M}$. Thus, we have a genus zero subgroup $H$ for each of such 171 (of atmost 194) rational conjugacy classes of elements of $\mathbb{M}$. Recall that $x, y$ in $\mathbb{M}$ are *rationaly conjugate* if $x$ is conjugate to $y$ or $y^{-1}$. Since the coeffecients $a_n(g)'$s in $T_g$ are all integers, it follows that $T_g = T_h$ if and only if $\langle g \rangle = \langle h \rangle$.

There are 171 Thompson-Mackey series $T_g$ and 172 conjugacy classes of cyclic subgroups in $\mathbb{M}$ .The correspondence $\langle g \rangle \to T_g$ is one-to-one except that two distinct rational conjugacy classes of elements of order 27 (namely $27A$ and $27B$) correspond to the same Hauptmodule of genus zero. This exception is unexplained.Though there are no further equalities between the series, there are certain dependencies, like, for example,

$$T_{6+} + 2T_{6-} = T_{6+2} + T_{6+3} + T_{6+6}$$

and other similar relations found for 4-groups.

## Discovery of $\mathbb{M}$

In November 1973, B. Fischer suggested that the following configuration in a finite group $\mathbb{M}$ might be interesting:

- $\mathbb{M}$ contains an element $\rho$ of order 3 which is conjugate to its inverse;
- $O_3(C_{\mathbb{M}}(\rho))$ is an extra special group of order $3^{13}$ and exponent 3;
- $D = C_{\mathbb{M}}(\rho)$ is 3-constrained and $D = O_3(D)\cdot\ S$, where $S$ is the full covering group (here, a double covering) of the simple group $Suz$, and $Z(S) = \langle \rho \rangle \times \langle z \rangle\,, |z| = 2$ and $z$ inverts $O_3(D)/\langle \rho \rangle$.

Recall that, given a prime $p$, a finite group $G$ with $O_{p'}(G) = 1$ is said to be *p-constrained* if $C_G(O_p(G)) \subseteq O_p(G)$. A finite group $G$ is *p-constrained* if $G/O_{p'}(G)$ is $p$-constrained.

A group satisfying the above hypothesis is called a *group of type* $F_1$.

Thompson showed that under the above hypothesis, $\mathbb{M}$ contains involutions $z$ and $t$ such that

1. $D = C_{\mathbb{M}}(z)$ is $2-$constrained
2. $Q = O_2(D) \backsimeq 2_+^{1+24}$ and $D/Q \backsimeq (\cdot 1)$
3. $H = C_{\mathbb{M}}(t)$ has the property that $H = H', Z(H) = \langle t \rangle$ and $H/\langle t \rangle \backsimeq F_2$, Fischer's $\{3,4\}^+-$ transposition group, the 'baby Monster'.

**(a)** Starting with Fischer's hypothesis, Thompson, Conway, Norton and others in Cambridge started finding information about $\mathbb{M}$ like the structure of local subgroups, order of the group, etc.

Using the 24- dimensional representation of $(\cdot 1)$ over $\mathbb{F}_2$, Thompson determined the centralizers of $p$ elements of $\mathbb{M}$ and hence the $p$-share of $|\mathbb{M}|$ for the primes $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ and 47; that is, he determined $m$, where $|\mathbb{M}| = mn, (m, n) = 1$ and $n$ is coprime to the primes above.

Using Sylow theorem, Conway and Thompson showed that

$$n \geq 41 \times 57 \times 71$$

The order of $\mathbb{M}$ was finally determined by Griess using the Thompson order formula.

**(b)** Thompson showed that a group $\mathbb{M}$ of type $F_1$ contains elements $\tau_i$ of orders $i \in \{2, 3, 5\}$ such that $F_i = C_{\mathbb{M}}(\tau_i)/\langle \tau_i \rangle$ is simple. Here, $C_{\mathbb{M}}(\tau_i)$ is split over $\langle \tau_i \rangle$ for $i = 3, 5$ and nonsplit for $i = 2$. He also determined the structure of the centralizer of an involution in $C_{\mathbb{M}}(\tau_i)$:

$$\begin{aligned} {}^2\widetilde{E}_6(2) \cdot 2 &\text{ if } i = 2, \\ 2^{1+8}.A_9 &\text{ if } i = 3 \\ \widehat{HS} \cdot 2 &\text{ if } i = 5. \end{aligned}$$

The group $F_2$ had been proposed by Fischer in the summer of 1973 as a group generated by a class of $\{3, 4\}$-transpositions and was constructed by Lyons and Sims with the aid of a computing machine (1977). It has multiplier 2 and $out(F_2) = 1$.

The existence and uniqueness of $F_3$ was proved by Thompson and Peter Smith (as a linear group of degree 248) and $F_5$ by Harada . We have

$$|F_2| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47, \text{ Fischer group}$$

$$|F_3| = 2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19, \text{ Thompson group}$$

$$|F_5| = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31, \text{ Harada group}$$

## Theorem

*(S. Smith, 1979) Let $G$ be a finite group containing an involution $z$ such that:*
*(i)* $O_2(C_G(z)) \simeq 2^{1+24}_{+}$;
*(ii)* $C_G(z) / O_2(C_G(z)) \simeq (\cdot 1)$; *and*
*(iii)* $C_G(O_2(C_G(z))) = \langle z \rangle$.

*Then, either :*

*(i) $G$ contains an involution $t \in O_2(C_G(t))$ such that $C_G(t) \backsimeq \widehat{F_2}$, the double cover of $F_2$, and*
$|G| = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$,*or*
*(ii)* $G = O(G)\, C_G(z)$.

Thus, the structure of $C_t$ follows from that of $C_z$ . So, a group of type $F_1$ can be defined in terms of $C_z$ alone. Thus,

## Theorem

*If $G$ is a finite simple group containing an involution $y$ such that $C_G(y) \simeq (2_+^{1+24})^{\cdot}(\cdot 1)$, then $G$ is a group of type $F_1$.*

Griess was independently, and simultaneously, studying finite groups $G$ containing involutions $x$ and $y$ such that:

- $C_x \simeq \widehat{F}_2$, the covering group of the baby monster $F_2$ by $\mathbb{Z}_2$ and
- $C_y \cong (2_+^{1+24})^{\cdot}(\cdot 1)$.

## Theorem

*(Griess) Let $G$ be a finite simple group containing involutions $\sigma$ and $\tau$ such that $C_\sigma \cong 2_+^{1+24} \cdot (\cdot 1).C_\tau \simeq \widehat{F}_2$, the covering group of $F_2$ by $\mathbb{Z}_2$. Then, $G$ has exactly 2 conjugacy classes of involutions and*
$|G| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Thus, Fischer and Griess arrived at the same group.

Griess also showed that:
(i) A group $G$ of type $F_1$ has only two conjugacy classes of involutions.
(ii) $G$ has trivial multiplier.
Involutions of $\mathbb{M}$ which are conjugate to $\sigma$ are called *Conway involutions (*also called *long involutions)* and those conjugate to $\tau$ are called *Fischer involutions (*also called *transpositions* or *short involutions)*.

## Theorem

*(Griess, Meirfrankenfeld, and Segev,1989) Let $G$ be a finite group containing two involutions $\sigma$ and $\tau$ such that $C_G(\sigma) \backsimeq 2_+^{1+24} \cdot Co_1$ and $C_G(\tau) \backsimeq 2 \cdot F_2$. Then, $G$ is unique up to isomorphism.*

Let $\Gamma_{\mathcal{F}}$ be the graph whose vertices are the involutions of $\mathbb{M}$ of type $F_2$ and the edges are pairs of commuting involutions whose product also is of type $F_2$. The conditions on the centralizers of involutions is strong enough to uniquely determine this graph. Aschbacher and Segev (1992) used this information to show that this graph is triangulable.

## Construction of $\mathbb{M}$

The construction of $\mathbb{M}$ is due to Griess with simplifications of some parts of the Griess argument due to Conway and Tits. It makes constructive the uniqueness proof, independently due to Thompson, of $\mathbb{M}$ assuming some of its then known properties. $\mathbb{M}$ is constructed as the amalgam of the groups

$$G_1 \backsimeq 2_+^{1+24} \cdot (\cdot 1)\,;$$
$$G_2 \backsimeq 2^{2+11+22} \cdot (M_{24} \times S_3)\,; \text{ and}$$
$$G_3 \backsimeq 2^{3+6+12+18} \cdot (3^{\cdot} S_6 \times L_3(2)) \text{ with}$$
$$[G_2 : G_1 \cap G_2] = 3; \text{ and } [G_3 : G_1 \cap G_3] = [G_3 : G_2 \cap G_3] = 7$$

**Definition of an amalgam and its completion:**

Let $(G_i, \odot_i)$ be groups, $i = 1, 2, 3$. Assume that the sets of elements of $G_i$ have pairwise nontrivial intersections and that, for $x, y \in G_i \cap G_j$, $1 \leq i \neq j \leq 3$,

$$x \odot_i y = x \odot_j y$$

holds. A *completion* of the system $\{G_i, \odot_i\}$ is a pair $((G, \odot), \psi)$, where $(G, \odot)$ is a group and $\psi$ is a map from $G_1 \cup G_2 \cup G_3$ to $G$ such that, for all $x, y \in G_i$, $1 \leq i \leq 3$,

$$\psi(x \odot_i y) = \psi(x) \odot \psi(y).$$

$(G, \odot)$ is called a *completion group* and $\psi$ *is called* the *completion map*.

The completion is said to be:

- *faithful* if $\psi$ is injective;
- *generating* if the image of $\psi$ generates $(G, \odot)$;
- *universal* if for any other completion $((H, \triangle), \theta)$, there is a surjective homomorphism $\eta : G \to H$ such that $\theta = \eta \circ \psi$.

Note that:

- The universal completion is necessarily generating;
- A faithful completion exists if, and only, the universal completion is faithful.
- All universal completions of a given amalgam are isomorphic.

One needs to prove that:

- Up to isomorphism, there is a unique monster amalgam (Thompson).
- $\mathcal{M}$ possesses a faithful completion. This is answered by producing a faithful 196,883-dimensional representation.
- The only faithful completion of $\mathcal{M}$ is the universal one and the completion group is the Monster, that is the nonabelian simple group with Monster, that is the nonabelian simple group with $G_1$ as the centralizer of an involution.

**Motivation for the construction of the Griess algebra $B$:**

Given

- $A$, an algebra over a field $k$,
- $\langle -, - \rangle$ a bilinear form on $A$,
- $B$, a linear subspace of $A$,
- $p : A \to B$, the orthogonal projection of $A$ onto $B$; that is, restriction of $p$ to $B$ is the identity, and $\langle \ker p, B \rangle = \langle B, \ker p \rangle = 0$. If $B$ is nonsingular with respect to $\langle -, - \rangle$, such a map is unique;
- $G$, a group of algebra automorphisms of $A$ preserving $\langle -, - \rangle$

we can define a $G$ -algebra structure on $B$ by defining: for $x, y \in A$, define $x \cdot y = p(xy)$.

The resulting algebra structure on $B$ is called the *restriction* of the algebra (structure of) $A$ to $B$, and is denoted by $\mathrm{Ret}(A, B)$. If the form $\langle -, - \rangle$ on $A$ is associative (i.e., $\langle x \cdot y, z \rangle = \langle x, y \cdot z \rangle$, then the restriction of the form to $B$ is also associative, i.e., for $x, y, z \in B$

$$(p(xy), z) = (xy, z) = (x, yz) = (x, p(yz)).$$

## Example

Let $A = M_n(k)$, characteristic of $k$ is not 2. Consider the bilinear map taking $(M, N) \in A^2$ to $tr(MN)$. Let $A^+$ and $A^-$ be the symmetric and the skew symmetric matrices in $A$. The above bilinear form is nondegenerate on $A$ and remains so when restricted to $A^+$ and $A^-$. Let $p^\pm : A \to A^\pm$ be the relevant projection maps; i.e., $p^\pm(M) = (M \pm M^{tr})/2$. Then, $A^+$ is the Jordan algebra of symmetric matrices and $A^-$ is the Lie algebra of skew-symmetric matrices.

### Deformation of a $G$ -Algebra $\mathbb{B}$

Suppose $A = A_1 \oplus A_2$ with $A_i$ being $G$ -invariant subalgebras. Let $I_i : A_i \to A$ and $p_i : A \to A_i$ be the inclusion and projection maps, $i = 1, 2$. Then there are maps $F_{ijk} : A_i \otimes A_j \to A_k$ defined by this set of maps. A deformation $A$ is an algebra $A^*$ which is $A_1 + A_2$ as a vector space and the product is given by $F^*_{ijk} = C_{ijk} F_{ijk}$, where $C_{ijk}$ are scalars and the notation has obvious meaning.

### Heuristics for the construction of the Griess algebra $\mathbb{B}$

**a)** Assuming the existence of an irreducible representation $\theta$ of $\mathbb{M}$ on a complex vector space $V$ of dimension 196883, Norton showed that the character $\chi$ of $V$ satisfies:

i. $\chi(g) \in \mathbb{Q}$ for each $g \in \mathbb{M}$;
ii. $\langle \chi, s^2\chi \rangle = 1$; and
iii. $\langle \chi, s^3\chi \rangle = 1$.

(i) Recall that, if $\psi$ is a representation of a group $X$ on a vector space $W$ over $\mathbb{C}$, then the map $h : W \times W^* \to \mathbb{C}$ taking $(v, f)$ to $f(v)$ is a $\psi(W)$-invariant, nondegenerate bilinear form; and that, two irreducible complex representations are equivalent if their characters are identical.

Since the representation $\theta$ of $\mathbb{M}$ on $V$ is irreducible and its character $\chi$ is equal to its dual$\chi^*$ by (i), $\theta$ is equivalent to its dual representation $\theta^*$ of $\mathbb{M}$ on $V^*$. So, $V^*$ can be identified with $V$. *This identification allows us to assume that $V$ admits a $\theta(\mathbb{M})$-invariant, symmetric, nondegenerate bilinear form.*

(ii) A multiplication on a $k$ -algebra $A$ is a map $\alpha : A \times A \to A$.

- The map $\alpha$ is distributive if, and only if, it factors through $A \otimes_k A$ (if, and only if, there is a map $\beta : A \otimes_k A \to A$ such that $\alpha = \pi \circ \beta$, where $\pi : A \times A \to A \otimes_k A$ is the natural map).
- The multiplication $\alpha$ is commutative if, and only if, it factors through $S^2 A = A \otimes A / \langle v \otimes w - w \otimes v \rangle$.

Thus, any $k$-linear map $\gamma : S^2 A \to A$ defines a commutative multiplication on $A$. If $A$ is a $G$-module and $\gamma$ is a $kG$-module morphism, then the multiplication also satisfies $\phi(g)u \cdot \phi(g)v = \phi(g)(uv)$.

Since $\left\langle S^2(\chi), \chi \right\rangle = 1$, the projection map $p$ from $S^2V$ to $V$ induced by the direct sum decomposition $S^2V = V \oplus V'$ commutes with the action of $\mathbb{M}$.

So, $V$ admits the structure of a commutative $\mathbb{M}$ -invariant algebra, i.e., there exists a symmetric bilinear multiplication $\cdot$ on $V$ such that

$$x \cdot \lambda y = \lambda x \cdot y; \text{ and } \varphi(g)x \cdot \varphi(g)(y) = \varphi(x \cdot y)$$

(iii) Similarly, considering $S^3(V)$ as the image of $S^2(V) \otimes V$ as well as of $V \otimes S^2(V)$, we see hat $\left\langle \chi, S^3\chi \right\rangle = 1$ implies that $V$ admits an $\mathbb{M}$ -invariant associative form on $V$; i.e. a map $f : V \times V \to V$ such that

$$f(x \cdot y, z) = f(x, y \cdot z) =: f(x, y, z) \text{ and}$$
$$f(x \cdot y, z) = f(g(x) \cdot g(y), g(z))$$

**Existence of a 196883- dimensional module**

Norton deduced the existence of the smallest irreducible representation from the local information on $\mathbb{M}$.

**Generalities on permutation modules:**

Let

- $G$, a permutation group acting on a set $\Omega$;
- $\mathcal{W} = \bigoplus\limits_{\alpha \in \Omega} \mathbb{C}\alpha$, free vector space on the left cosets $\{gH : g \in G\}$ of the stabilizer $H$ of an element $\alpha \in \Omega$ with a $G$-module structure by the left multiplication by elements of $G$;
- $\Omega \times \Omega = \overset{r}{\underset{i=0}{}} \mathcal{O}_i$, the $G$-orbit decomposition;
- $A_i, 0 \leq i \leq r$, the $(0,1)$-matrix corresponding to the characteristic function of $\mathcal{O}_i$;
- $\mathcal{A} := \{h \in End(\mathcal{W}) : hg(\alpha) = gh(\alpha)$ for each $g \in G, \alpha \in \Omega\}$, commuting algebra of the permutation action of $G$; thus,

$$\mathcal{A} = \mathbb{C}A_0 \oplus \cdots \oplus \mathbb{C}A_r.$$

Then, $\mathcal{W}$ and $\mathcal{A}$ are semi-simple $\mathbb{C}G$-modules; and the degrees of irreducible constituents appearing in $\mathcal{W}$ are the multiplicities of irreducible representation of $\mathcal{A}$ and vice-versa. Further, $\mathcal{W}$ is multiplicity-free if and only if $\mathcal{A}$ is commutative.

Let $\mathcal{O}_0$ be the diagonal in $\Omega \times \Omega$. Then, $A_0 = Id$. For each $i > 0$, $A_i$ generates $\mathcal{A}$ as a subalgebra of $\mathcal{A}$.

For $i, j \in \{0, 1, \cdots, r\}$, let

$$A_i A_j = \Sigma_{k=0}^{r} h_{ijk} A_k.$$

The $(r+1)$-matrices $\{H^{(i)} = ((h_{ijk}))\}$ are called the *Highman invariants* of the permutation group $(G, \Omega)$.

The multiplicities and the dimensions of the simple modules of $\mathcal{A}$ and hence the dimensions and the multiplicities of the components of the irreducible representations of the permutation module are determined by these Highman matrices.

**Permutation module $(\mathbb{M}, \mathcal{F})$ and the structure constants of $\mathcal{A}$:**

$\mathbb{M}$ acts by conjugation on the set $\mathcal{F}$ Fischer involutions and $|\mathcal{F}| = 97,239,461,142,990,186,000$. The order of the product of 2 distinct elements of $\mathcal{F}$ is one of : $1,2,3,4,5,6$. These products are in 8 different conjugacy classes of $\mathbb{M}$:

$$1, 2A, 2B, 3A, 3C, 4A, 4B, 5A, 6A$$

A pair of elements of $\mathcal{F}$ is uniquely determined by the conjugacy class of their product. Thus, $\mathbb{M}$ has a permutation representation of rank 9 on $\mathcal{F}$. Norton determined the number of tripes $(x, y, z) \in \mathcal{F}^3$ such that $xy, yz, zx$ are in specific conjugacy classes. This gives the intersection numbers of the centralizer algebra of the permutation action of $\mathbb{M}$ on $\mathcal{F}$. Thus, the structure of the permutation algebra $\mathcal{A}$ is determined.

Norton determined the primitive idempotents of the algebra $\mathcal{A}$. One of them has rank $196,883$. So, $\mathbb{M}$ has an irreducible representations of degree $196,883$. Thus the decomposition of the space $\mathbb{C}^{\mathcal{F}}$ into $\mathbb{M}$ -invariant subspaces has a component isomorphic to $V$. Thus the existence of a $196,883$-dimensional faithful representation of $\mathbb{M}$ was deduced from local information (i.e., properties of centralizers of certain elements). These proofs due to Norton were not published. (The methods in Griess, Meirfrankrnfeld, Segev were different.)

The Griess algebra can be realized as the projection to $V$ of the point-wise multiplication in $\mathbb{C}^{\mathcal{F}}$. However, the algebra itself is not associative.

### Problem

$196883 = 47 \times 59 \times 71 = 299 + 98304 + 98280$. *Is there a tensor product decomposition of the Griess algebra of dimensions* $47, 59, 71$ *which are* $G-$*invariant modules for an appropriate subgroup* $G$ *of* $\mathbb{M}$.

# The Witt design, the Golay code $\mathcal{G}_{12}$ and the Mathieu group $M_{24}$

- Define

$$\begin{aligned} \mathcal{P}_0(\Omega) &:= \{\phi, \Omega\} \simeq \mathbb{F}_2 \ \text{ and } \mathcal{P}^0(\Omega) := \{A \subseteq \Omega : |A|\,, \text{ even}\} \simeq \mathbb{F}_2^{23} \\ \mathcal{G}_{11} &:= \mathcal{G}_{12}/\mathcal{P}_0(\Omega)\,; \\ \overline{\mathcal{G}}_{12} &:= \mathcal{P}(\Omega)/\mathcal{G} \ \text{ (called \textit{the Todd module}); and} \\ \overline{\mathcal{G}}_{11} &:= \mathcal{P}^0(\Omega)/\mathcal{G} \end{aligned}$$

*Weight* of an element of $\overline{\mathcal{G}}_{12}$ is the cardinality of the smallest element in that coset.

$$0^1\ 1^{24} 2^{276} 3^{2024} 4^{1771}$$

Distinct subsets of $\Omega$ of cardinality less than 4 are in distinct cosets.

A subset of $\Omega$ of size 4 is one of six 4-subsets of $\Omega$ forming a partition of $\Omega$ and such that the union of any two of them is an octad. Any such six $4-$ sets is called a *sextet*.

- $$\{\phi\} < \mathcal{P}_0\left(\Omega\right) < \mathcal{G}_{12} < \mathcal{P}_0\left(\Omega\right) < \mathcal{P}\left(\Omega\right),$$
  unique $\mathbb{F}_2 M_{24}$-composition series of $\mathcal{P}\left(\Omega\right)$.
- $\pi$ induces well-defined maps
  $$\pi : \mathcal{G}_{12} \times \overline{\mathcal{G}}_{12} \to \mathbb{F}_2 \text{ (since } \mathcal{G}_{12} = \overline{\mathcal{G}}_{12}\text{)}$$
  and $\pi : \mathcal{G}_{11} \times \overline{\mathcal{G}}_{11} \to \mathbb{F}_2$ (since $Rad\left(\pi\right)$ in $\mathcal{P}^0\left(\Omega\right)$ is $\mathcal{P}_0\left(\Omega\right)$).
- $H^1\left(C_{11}, M_{24}\right) = 1$; this means ...

## Extra special $p$-groups (P. Hall)

A $p$ -group $Q$ is called *extra-special* if

$$Q' = Z(Q) = \Phi(Q) = \langle z \rangle \simeq C_p$$

- finite analogue of the Heisenberg group.

- $(xZ(Q), yZ(Q)) = [x, y], x, y \in Q$ defines a nondegenrate alternating form on $\overline{Q} := Q/Z(Q) \simeq V(2m, p)$.
- If $p = 2$, $q : \overline{Q} \to \mathbb{F}_2$ taking $xZ(Q)$ to $x^2$ is a quadratic form with $(\cdot, \cdot)$ as the associated bilinear form

**Notation:**

$$Q \text{ is written as } 2_{+}^{1+2n} \text{ or } 2_{-}^{1+2n}$$

according to as $q$ is of $(+)$-type or of $(-)$-type.

- If $p$ is odd, $Q$ is written as $p_{+}^{1+2n}$ if it is of exponent $p$. (most common occurrence is simple groups)
  $\mathbb{C}$characters of $Q \simeq p^{1+2n}$
- $p^{2n}$ linear characters
- $p-1$ irreducible complex characters of degree $p^n$ each. Each of them is faithful.

## Modular forms

Consider the action of $SL_2(\mathbb{R})$ on the upper half plane

$$\mathbb{H} = \{z \in \mathbb{C} \colon im(z) > 0\}$$

via the Mobius transformations:

$$g = \left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \in SL_2(\mathbb{R}) \text{ takes } z \in \mathbb{H} \text{ to } \frac{az+b}{cz+d}.$$

For a positive integer $n$, let

$$\Gamma(n) = \{\left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \in SL_2(\mathbb{Z}) : \left[\begin{array}{cc} a & b \\ c & d \end{array}\right] = I_2 (\operatorname{mod} n)\}$$

$$\Gamma_0(n) = \{\left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \in SL_2(\mathbb{Z}) : c \equiv 0 (\operatorname{mod} n)\}$$

$$\Gamma_1(n) = \{\left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \in \Gamma_0(n) : a \equiv d \equiv 1 (\operatorname{mod} n)\}$$

$$\Delta(n) = N_{SL_2(\mathbb{R})}(\Gamma_0(n)) = \left\langle \Gamma_0(n), \left[\begin{array}{cc} 0 & -\frac{1}{\sqrt{n}} \\ \sqrt{n} & 0 \end{array}\right] \right\rangle$$

## Note

1. $\Gamma/\Gamma(n) \backsimeq PSL_2(\mathbb{Z}_n)$
2. $\Delta(n)/\Gamma_0(n) \backsimeq 2^t$ for small (Specify!) $t$. Further, $t = 1$ if $n$ is a prime.
3. $\Delta(p) = \langle \Gamma_0(p), \omega_p(\tau) \rangle$ if $p$ is a prime, where $\omega_p(\tau)$ is the Fricke involution defined for any integer $n$ by

$$\omega_n(\tau) = -\frac{1}{n\tau}, \text{ where } \tau \in \mathbb{H}.$$

Recall that a subgroup of $SL_2(\mathbb{R})$ is said to be *discrete* if its orbits in $\mathbb{H}$ have no accumulation points. A *congruence subgroup* of $SL_2(\mathbb{R})$ is a discrete subgroup of $SL_2(\mathbb{R})$ containing $\Gamma(n)$ for some integer $n$.

Let $G$ be a congruence subgroup of $SL_2(\mathbb{R})$. It acts on the extended complex plane

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$$

by Mobius transformations and $\mathbb{H}^*/G$ has the structure of a compact Riemann Surface $X_G$. The significant invariant of $X_G$ is its genus (define). The genus is zero if and only if $X_G$ is homeomorphic to a sphere in $\mathbb{R}^3$. We then say that the group $G$ is of genus zero.
Surprisingly, genus of $\Gamma_0(n)$ tends to infinity as $n$ tends to infinity. So there are only a finite number of integers $n$ such that $\Gamma_0(n)$ has genus zero.Thompson has shown that there are only a finite number of conjugacy classes of congruence subgroups of $PSL_2(\mathbb{R})$ of genus zero.There are in fact about 370 of them.

# Definition

A *modular function of weight* zero for a discrete subgroup $G$ of $SL_2(\mathbb{R})$ is a meromorphic function $f$ on the upper half plane $\mathbb{H}$ (i.e., $f$ is analytic except at a discrete set of points) such that

$$f(g(z)) = f(z) \text{ for each } g \in G \text{ and } \ z \in \mathbb{H}.$$

A modular function of weight zero for $G$ defines a meromorphic function on $\mathbb{H} \setminus \Gamma$.

If $G$ is a congruence subgroup of $SL_2(\mathbb{R})$ such that $X_G$ is of genus zero, then the set $\mathcal{F}(X_G)$ of all modular functions of weight zero with respect to $G$ is a field, isomorphic to the field $\mathbb{C}(X)$ of rational functions with complex coefficients in one variable .

We write $\mathcal{F}(n)$ for $\mathcal{F}(X_{\Gamma_0(n)})$.

**Definition:** A modular function $f$ is called a *Haupt module* for $G$ if:

- $\mathcal{F}(X_G) = \mathbb{C}\,(f)$, *i.e.*,any modular function of weight 0 with respect to $G$ is a rational functions of $f$ ; and
- $f$ has a simple pole at $\infty$.

Example

If $G = SL_2(\mathbb{Z})$, then $X_G$ is homeomorphic to the unit sphere in $\mathbb{R}^3$ and a Haupt module is the classical elliptic modular function

$$j(\tau) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + \cdots,$$

$$q = e^{2\pi i\tau}, \tau \in \mathbb{H}.$$