THE UNIVERSITY OF ADELAIDE

The Monster

The Monster is the largest sporadic finite simple group.

School of Mathematical Sciences
The University of Adelaide
2009

2000BC ?? **"Quadratic formula"**

$$ax^2 + bx + c = 0$$

has solution

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

1540 ?? **Solution of Cubic**

$$x^3 + px + q = 0$$

has solution

$$x = x_1 + x_2, \qquad \rho x_1 + \rho^2 x_2, \qquad \rho^2 x_1 + \rho x_2$$

where

$$\rho, \rho^2 = \frac{-1 \pm \sqrt{-3}}{2} \quad \text{and} \quad x_1, x_2 = \frac{1}{3}\sqrt[3]{\frac{-27q \pm 3\sqrt{-3(-4p^3 - 27q^2)}}{2}}$$

1545 ?? **Solution of Quartic**

Published in *Ars Magna* by Geronimo Cardano,

but due to Luigi Ferrari.

Principal works in the development of Group Theory

1770	**Lagrange**	Study of the number of values of a function to solve the problem of algebraic solutions of equations.
1815	**Cauchy**	First systematic study of "substitutions" (permutations).
1824	**Abel**	Substitutions used to show the non-solvability of the 5th degree equation.
1830	**Galois**	Connected groups and solution of equations.
1845-6	**Cauchy**	Extensive study study of substitutions and groups of substitutions.
1854	**Cayley**	First definition of an abstract group.
1860	**Mathieu**	Discovery of five multiply transitive permutation groups, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.
1870	**Jordan**	First book on permutation groups (*Traité des Substitutions*).
1872	**Sylow**	Sylow Theorems.
1889	**Holder**	Completed the proof of the "Jordan-Holder Theorem". Problem: *Find all of the finite simple groups.*
1869	**Lie**	Study of infinite (Lie) groups.

Jordan - Holder Theorem

Definition A normal subgroup M in a group G is a *maximal normal subgroup* if whenever $M \leq N \leq G,\ N \lhd G$ then $M = N$ or $N = G$.

As there are no proper normal subgroups between M and G, the factor group G/M also contains no proper normal subgroups and so G/M is a simple group.

If G is a finite group then we can choose a maximal normal subgroup M_1 of G; and then choose a maximal normal subgroup M_2 of M_1 and eventually we will reach the identity subgroup $\langle 1 \rangle$ as G is a finite group. Thus we have a series of normal subgroups, called a *composition series*

$$\langle 1 \rangle = M_n \lhd M_{n-1} \lhd \ldots \lhd M_2 \lhd M_1 \lhd G = M_0$$

in which each of the factor groups $M_i/M_{i+1},\ i = 0, 1, \ldots, n-1$ is a simple group.

The Jordan - Holder Theorem states that if we choose any other composition series

$$\langle 1 \rangle = N_k \lhd N_{k-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd G = N_0$$

then $n = k$ and the two sets of simple factors are exactly the same:

$$\{M_i/M_{i+1} \mid\ i = 0, 1, \ldots, n-1\} = \{N_i/N_{i+1},\ i = 0, 1, \ldots, n-1\}.$$

As each finite group G has a uniquely determined set of simple groups "involved" in G, it is not surprising that Holder posed the problem: *Find all of the finite simple groups.*

Just knowing the simple factors will not (in general) determine the group.

Example Each of the following, non-isomorphic groups have the same set of composition (simple) factors: $C_2,\ A_5$.

1. The symmetric group S_5 has only one proper normal subgroup A_5 with $S_5/A_5 \cong C_2$.
2. The special linear group $SL(2,5)$ has only one proper normal subgroup $Z(SL(2,5)) \cong C_2$ with $SL(2,5)/Z(SL(2,5) \cong PSL(2,5) \cong A_5$.
3. The direct product $G = C_2 \times A_5$ has two proper normal subgroups, C_2 andA_5 with $G/C_2 \cong A_5$ and $G/A_5 \cong C_2$.

Two examples of simple groups of finite order

1. If G is an abelian simple group then G is cyclic of order p, where p is a prime number. That is, $G \cong C_p \cong (\mathbf{Z}_p, +)$.
2. The Alternating groups A_n, $n \geq 5$ are simple.
   The Alternating group A_n is the subgroup of even permutations in the symmetric group S_n, the group of all permutations on n objects, $\{1, 2, \ldots, n\}$.
   The order of A_n, $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

   The Alternating group A_5 of order 60 is the smallest non-abelian simple group.

Solution of polynomial equations

A polynomial equation with integer coefficients is *soluble by radicals* if the solutions can be obtained by successively taking $\sqrt{\ }$, $\sqrt[3]{\ }$, etc in some order.

Galois Corresponding to every polynomial equation there is a (finite) group (of permutations of the roots of the equation). The equation is soluble by radicals if and only if the corresponding (Galois) group has all of its composition factors abelian (i.e. cyclic of prime order).

Examples

1. The polynomial equation $x^5 - 2$ is soluble by radicals.
   The corresponding Galois group has all of its composition factors abelian.
2. The polynomial equation $x^5 - 4x + 2$ is **not** soluble by radicals.
   The corresponding Galois group has one of its composition factors a non-abelian simple group, namely A_5.

Examples of simple groups of finite order - known around 1900

1. The abelian simple groups C_p, p a prime number.

2. The Alternating groups A_n, $n \geq 5$ are simple.

3. The *General Linear group* $(GL(n, F), \cdot)$, F a field, is a non-abelian group, where $(GL(n, F), \cdot)$ denotes the invertible $n \times n$ matrices under multiplication with entries in the field F.

   Besides the finite fields $\mathbf{Z}_p$ there is a (unique) finite field $GF(p^n)$ for every prime power $q = p^n,\ n \geq 1$.

   Notation: For finite fields $GF(q)$ we often write $GL(n, q)$ for $GL(n, F)$.

   Note that $GL(n, F)$ can also be thought of as the group of invertible linear transformations $GL(V)$ on a finite vector space V of dimension n over the finite field F.

   $GL(n, F)$ is not simple and contains a normal subgroup $SL(n, F)$, the *Special Linear group* which consists of all of the $n \times n$ matrices with determinant 1.

   In general $SL(n, F)$ is also not simple, but the factor group

   $$PSL(n, F) = SL(n, F)/Z(SL(n, F))$$

   is a non-abelian simple group for all n, F (except for a couple of cases in which both n and $|F| = q$ are very small).

4. Other "classical groups" - orthogonal, unitary and symplectic groups.

5. The five Mathieu groups, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

Group Representations

A *representation* of a group G is a (group) homomorphism

$$f : G \to GL(V) = GL(n, F)$$

where V is a vector space of dimension n over the field F.

The representation f is *irreducible* if V has no $f(G)-$ invariant subspace.

When $F = \mathbf{C}$, the complex numbers, the function $\chi(x) =$ trace $(f(g))$ is called an (ordinary) character of G. Note that $\chi(x) = \chi(g^{-1}xg)$.

The number of (distinct) irreducible representations (and hence characters) is equal to the number of conjugacy classes of G.

For a simple group, as $\ker f \lhd G$, $\ker f = \langle 1 \rangle$ or G. Thus either $f : G \to \langle 1 \rangle$ or f is an isomporphism.

In any case $f(1) = I_n$ and $\chi(1) = n$ called the *degree* of the representation.

The Character Table of a group G

A square array which gives the values of the irreducible characters on the different conjugacy classes.

Character Table of A_5, the Alternating group of order 60.

Class	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	α_1	α_2
χ_5	3	-1	0	α_2	α_1

where $\alpha_1 = \dfrac{1+\sqrt{5}}{2}$ and $\alpha_2 = \dfrac{1-\sqrt{5}}{2}$.

What is known about the finite simple groups?

p-groups (groups of order $p^n,\ p$ a prime) are not simple (unless $n = 1$).

1897 **Burnside** First book on abstract groups (*Theory of groups of finite order*).

Theorem: *Groups of order $p^a q^b$ are not simple.*

Theorem: *A simple group of even order has order divisible by* 4.

Conjecture: *A non-abelian simple group must have even order.*

Finite groups of even order

Definitions Let G be a finite group.

An element $x \in G$ is an *involution* if x has order 2.

The centralizer of x in $G,\ C_G(x) = \{g \in G \mid g^{-1}xg = x \text{ (or } gx = xg) \ \forall g \in G\}$.

1954 **Brauer** There are only a finite number of non-abelian simple groups with a given centralizer of an involution.

Theorem: If G is a non-abelian simple group which contains an involution z with $C_G(z) \cong GL(2, q),\ q$ odd, then $G \cong PSL(3, q)$ or $q = 3$ and $G \cong M_{11}$.

Programme: If G is a known non-abelian simple group containing an involution z, show that $C_G(z)$ characterizes G.

Algebras

An *algebra* is a vector space A over a field F in which there is a product defined on the vectors in A. The product satisfies certain distributive conditions and may/may not be associative or commutative depending on the algebra.

Associative algebras

1. The $n \times n$ matrices over a field F.
2. The group algebra.

Lie algebras

An algebra A is a Lie Algebra if, for all $x, y, z \in A$,

(i) $x^2 = 0$

(ii) $x(yz) + z(xy) + y(zx) = 0$

The semi-simple complex Lie algebras were classified late in the 19th Century. These Lie algebras consist of 4 infinite families :

$A_n, \quad B_n, \quad C_n, \quad D_n$

and 5 "exceptional" Lie algebras:

$G_2, \quad F_4, \quad E_6, \quad E_7, \quad E_8$

The simple groups of Lie type

1956 **Chevalley**

$A_n(q)$		$PSL_{n+1}(n, q)$
$B_n(q)$	$n > 1$	Orthogonal groups
$C_n(q)$	$n > 2$	Symplectic groups
$D_n(q)$	$n > 3$	Orthogonal groups
$G_2(q)$		
$F_4(q)$		
$E_6(q)$		
$E_7(q)$		
$E_8(q)$		

"Twisted Lie groups"

1959 **Steinberg**
1962 **Suzuki**
1961 **Ree**

${}^2A_n(q)$	$n > 1$	Unitary groups
${}^2D_n(q)$	$n > 3$	Orthogonal groups
${}^3D_4(q)$		Steinberg groups
${}^2E_6(q)$		Steinberg groups
${}^2B_2(q)$	$q = 2^{2m-1}$	Suzuki groups
${}^2G_2(q)$	$q = 3^{2m-1}$	Ree groups
${}^2F_4(q)$	$q = 2^{2m-1}$	Ree groups

A_n	$n \geq 5$	Alternating groups

"Sporadic groups" - the Mathieu groups

M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	4-transitive
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	5-transitive
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	3-transitive
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	4-transitive
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	5-transitive

The Odd Order Theorem

1963 **Feit, W. & Thompson, J.G.**

There are no non-abelian finite simple groups of odd order.

1965 **Janko, Z**

There is (another) sporadic non-abelian simple group of order

$$175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$$

This group, now denoted by J_1 is a subgroup of $GL(7, 11)$ and is generated by the matrices Y and Z:

$$Y = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{bmatrix}$$

The Character table for J_1 is a 15×15 array.

The matrices given above were derived by taking a complex representation and "reducing" (mod 11) - that is by finding a representation from J_1 to $GL(7, 11)$.

The 26 Sporadic groups

Group	Order	Name
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Janko
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Janko
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Janko
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman-Sims
Mc	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLaughlin
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Rudvalis
$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	Suzuki
.3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
.2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
.1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway
$M(22)$	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Fischer
$M(23)$	$2^{18} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer
$M(24)'$	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	Fischer
F_3	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson
F_5	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Harada
F_2	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	Baby Monster
F_1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	Monster

All but the Mathieu groups were discovered in the period from 1963−1975.

Discovery of the sporadic simple groups

Janko's four groups and a number of other sporadic groups were discovered by considering the centralizer of an involution of a known group or one having a similar structure to one of the sporadic groups.

The three Conway groups arose as subgroups of the automorphism group .0 of the "Leech Lattice". The Leech lattice is associated with a very good example of sphere packing in 24-dimesional space.

The last seven groups on the list were discovered due to work by Fischer who considered finite groups in which a class of involutions has certain properties. If x, y are involutions then $x^2 = y^2 = 1$ and if $xy = yx$ then $(xy)^2 = 1$.

Now consider a finite group of even order in which a conjugacy class K of involutions has the property that if $x, y \in K$ the the order of xy is either 1, 2 or 3.

An example of groups containing such a class of involutions is the symmetric groups $S_n, n \geq 3$ and the conjugacy class of transpositions

$$K = \{(a,\, b) \mid a,\, b = 1, 2, \ldots, n,\ a \neq b\}.$$

The groups $M(22), M(23), M(24)$ also satisfy this condition and contain the respective Mathieu groups (as suggested by Fischer's notation).

The "Baby Monster" F_2 arose from an extension of the above problem. Namely, suppose that the possible orders for the product of two involutions is either 1, 2, 3 or 4.

The existence of the Monster F_1 was then conjectured as being a simple group G containing a class of involutions K_1 with $C_G(t)/\langle t \rangle \cong F_2$ for $t \in K_1$ and another class of involutions K_2 such that if $z \in K_2$ then $C_G(z)$ contains a normal subroup N with $C_G(z)/N \cong .0$ and $|N| = 2^{25}$.

The Monster or Friendly Giant

The Monster has order

$$\begin{aligned} & 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ = \; & 808017424794512875886459904961710757005754368000000000 \\ \approx \; & 8 \cdot 10^{53}. \end{aligned}$$

The Monster has 194 conjugacy classes and so its Character Table is a 194×194 array.

The smallest non-trivial irreducible (complex) representation (character) has degree 196883.

Although the Monster was conjectured to exist as early as 1972, its existence was not proved until 1980 by Griess. Griess constructed a 196884-dimensional algebra (as the sum of the trivial and smallest representations) and, using properties derived from the character table, showed it possessed certain "forms" and that the Monster was the automorphism group of this algebra.

Amazingly Griess did not use the computer in his calculations - it was all done by hand and induced him to name the monster as the "Friendly Giant".

Exactly 20 of the 26 sporadic groups occur in the Monster.

Monstrous Moonshine

Shortly after the possible existence of the Monster was first suggested, the likely degrees of the irreducible representations were calculated. John McKay made the observation that 196883 was "almost equal" to the coefficient 196884 in the elliptic modular function, well known in number theory:

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots$$

where $q = e^{2\pi i\tau}$. Shortly afterwards John Thompson observed that the second coefficient 21493760 is the sum of the degrees (dimensions) of the first three irreducible representations of the Monster (and similarly all other coefficients seemed to be simple linear combinations of the dimensions of the irreducible representations of the Monster).

It has since been shown that the Monster acts on an infinite dimensional algebra and a number of the moonshine conjectures have been shown, but even today some of the remarkable coincidences are still not fully understood.

Classification of finite simple groups - announced 1980

A non-abelian simple group is one of the groups appearing above in the list of 17 infinite series or one of the 26 sporadic groups.

1984 **Thompson, J.G.**

The Monster is the Galois group of a certain polynomial with integer coefficients.

For a brief, up to date summary of Moonshine and the Monster the following book review is worth reading.

Book review by **Richard Borcherds**, Bulletin Amer Math Soc Vol 45, p. 675, 2008:

Terry Gannon, *Moonshine beyond the Monster: The bridge connecting algebra, modular forms and physics*, C.U.P.

For more information on the classification of the simple groups and the sporadic groups, the following is a good reference.

Daniel Gorenstein, *Finite Simple Groups*, Plenum