SYMMETRY AND THE MONSTER
The Classification of Finite 'Simple' Groups

Freshman Seminar
University of California, Irvine

Bernard Russo

University of California, Irvine

Spring 2015

The Enormous Theorem

In the summer of 1980, a mathematician at Ohio State University filled in the last piece of an enormous and highly complex puzzle:

The classification of symmetries (finite simple groups).

Originally 15,000 pages, 500 articles, 100 mathematicians (currently 5000 pages)

Along the way, discoveries were made that led to advances in the theory of computer algorithms, in mathematical logic, in geometry, in number theory, and (**speculation!**) the formulation of a unified field theory in physics.

The story had very humble beginnings (1600BC),

$$ax^2 + bx + c = 0 \quad , \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and similar solutions for higher-degree equations (1545 AD)

$$ax^3 + bx^2 + cx + d = 0 \text{ and } ax^4 + bx^3 + cx^2 + dx + e = 0$$

What about $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$?

In 1770 Joseph Louis Lagrange suggested that such a solution (by *radicals*) might not be possible, and in 1824, the Norwegian mathematician Niels Henrik Abel proved that this was indeed the case.

A **solution by radicals** uses only the basic algebraic operations of addition, subtraction, multiplication, and division, as well as the extraction of roots

A solution should be expressed in terms of the coefficients of the equation and must be valid for all values of the coefficients. It turns out that some quintic (5th degree) equations can be so solved and some cannot (as shown by Abel in 1824)

It was natural to ask whether there is any way of deciding whether or not a given quintic equation can be solved by radicals (without actually finding the solution).

Abel was working on this question when he died in 1829 at the age of 26.

The legacy of Évariste Galois (1811-1832)

A mathematical child prodigy whose repeated failure to gain entry into the Polytechnique and repeated rejection of his research drove him to reject the academic community and become a 'student radical.'

In spite of these troubles, his mathematics continued to flourish, and in 1831 he again submitted a paper to the French Academy of Sciences

When this paper was also ignored, the frustrated Galois turned his attention to revolutionary politics, was arrested twice, imprisoned once, and killed in a duel.

On the eve of the duel, from his prison cell, Galois wrote a long letter to a friend in which he outlined the current state of his mathematical theories.

A decade later, the French Academy found value in his last paper. The central concept that Galois had left to the world proved to be one of the most significant of all time, having applications in many fields of mathematics as well as in physics, chemistry, and engineering. The concept was that of a **group**.

Symmetry and symmetry groups

The symmetry of an isosceles triangle. Reflection (2 symmetries: Id, r)
The symmetry of a tripod. Rotation (3 symmetries: Id, v, w)
The symmetry of an equilateral triangle. (6 symmetries: Id, v,w, x,y,z)

It is the action of transforming the figure that is referred to as a reflection or rotation, not the result of that action.

Group: "Multiplication" table, identity, associativity, inverse

Some properties: commutative, finite, infinite, 'simple' (atom is better)

Other (familiar) examples

- Non-zero rational numbers, multiplication
- integers, addition
- integers modulo a prime number p, multiplication modulo p

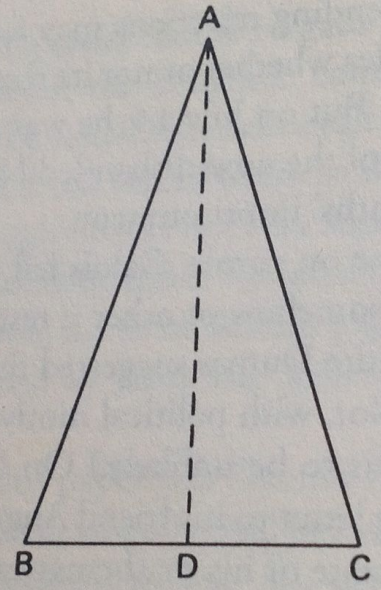


FIGURE 24 The symmetry of an isosceles triangle.

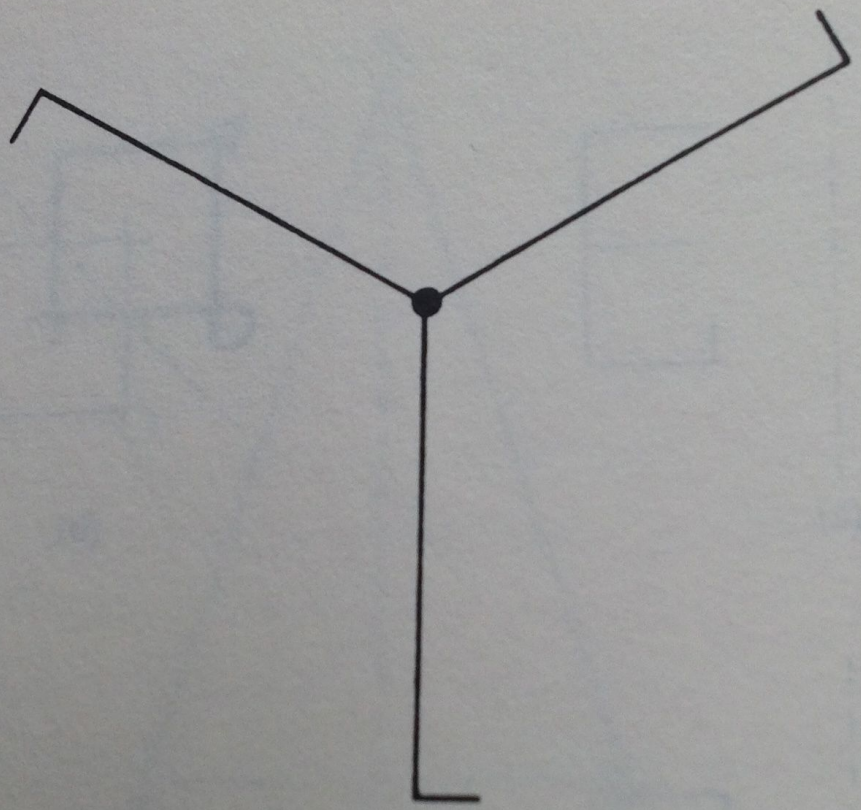


FIGURE 26 Rotational symmetry.

(about points) th

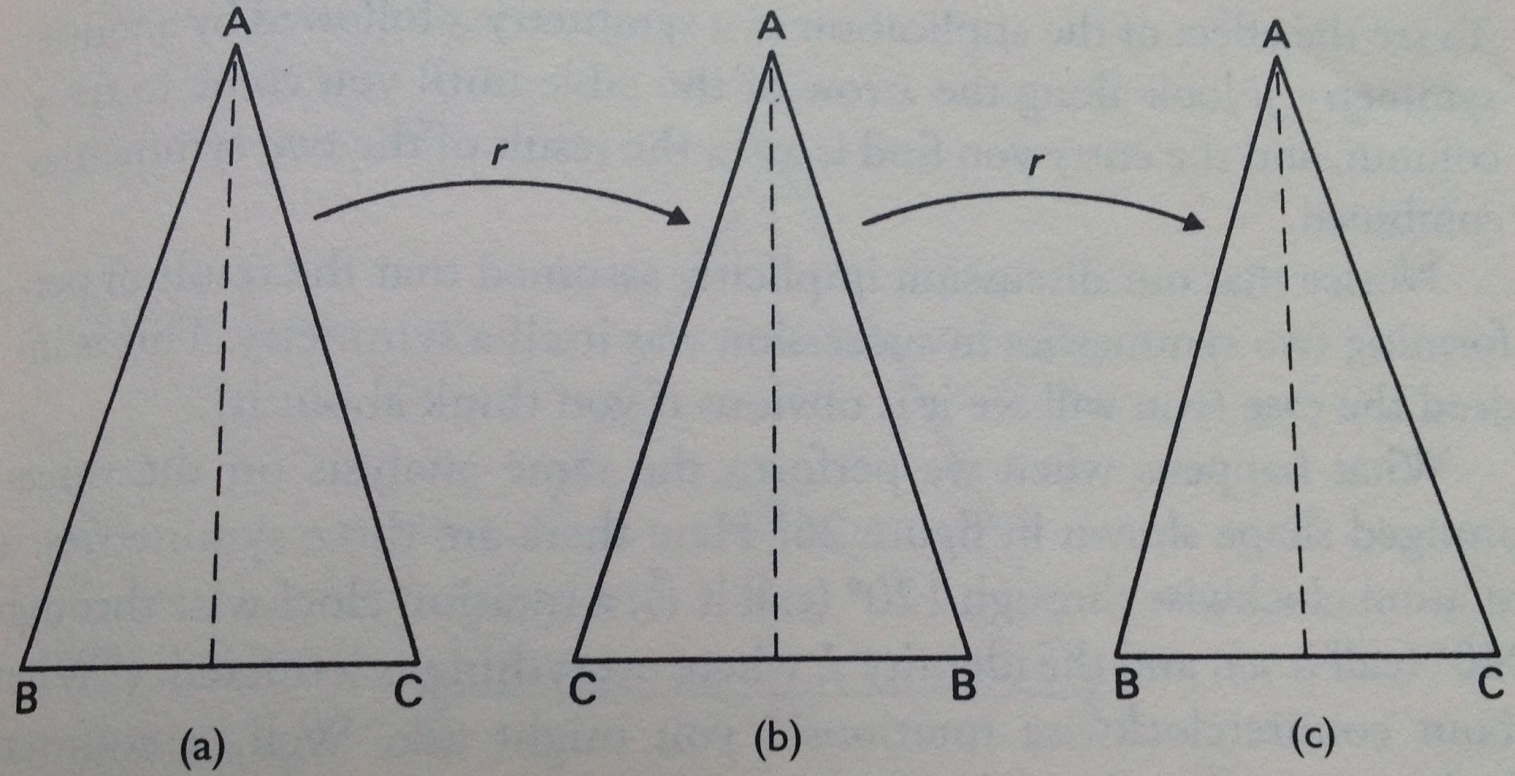


FIGURE 27 Successive reflections.

$$r * r = I,$$

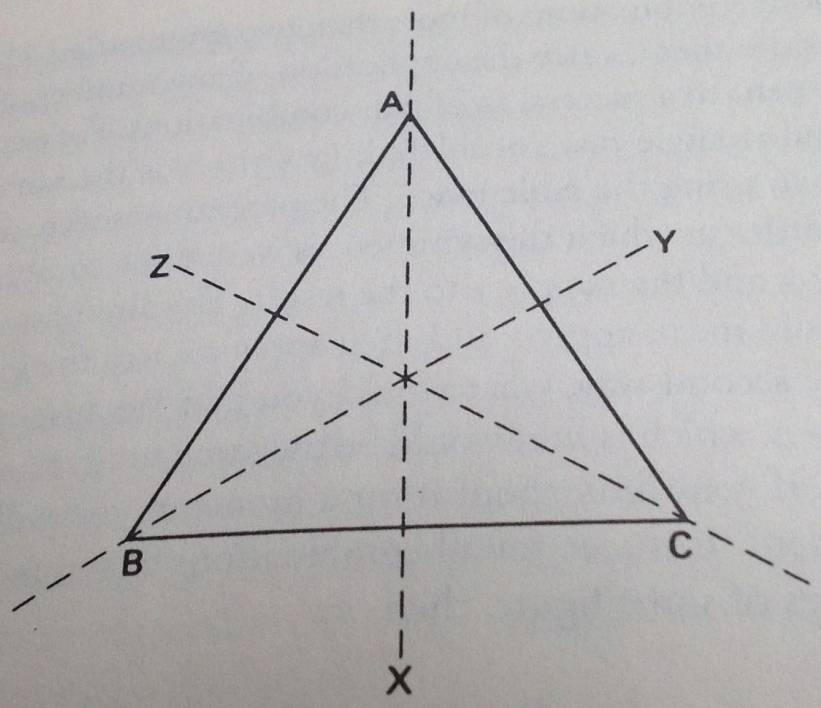


FIGURE 28 Symmetries of an equilateral triangle.

moves.) These symmetries combine as indicated by the following

and then applying b to the result.) Using the same notation, we may describe the (in this case trivial) effects of performing other sequences of symmetries, thus:

$$r * I = r,$$

$$I * r = r,$$

$$I * I = I.$$

These four identities may be summarized in a table:

Isosceles triangle:

$*$	I	r
I	I	r
r	r	I

Similarly, two 240° rotations are equivalent to one 120° rotation, so

$$w * w = v.$$

The full table of successive symmetries is

Tripod:

$*$	I	v	w
I	I	v	w
v	v	w	I
w	w	I	v

more example. The equilateral triangle (see fig
metries. There is the identity, I, clockwise rotati
120° and 240°, respectively, and reflections x,

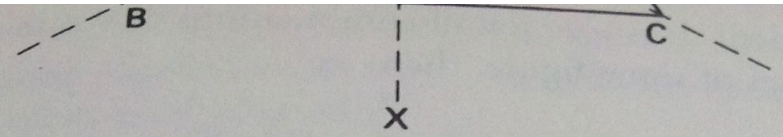


FIGURE 28 Symmetries of an equilateral triangle.

moves.) These symmetries combine as indicated by the following table:

Equilateral triangle:

*	I	v	w	x	y	z
I	I	v	w	x	y	z
v	v	w	I	z	x	y
w	w	I	v	y	z	x
x	x	y	z	I	v	w
y	y	z	x	w	I	v
z	z	x	y	v	w	I

If you wish to check these entries, you could try cutting out an equilateral triangle from cardboard, marking the corners A, B, C, and placing it on a sheet of paper on which the lines X, Y, Z are drawn. Then you

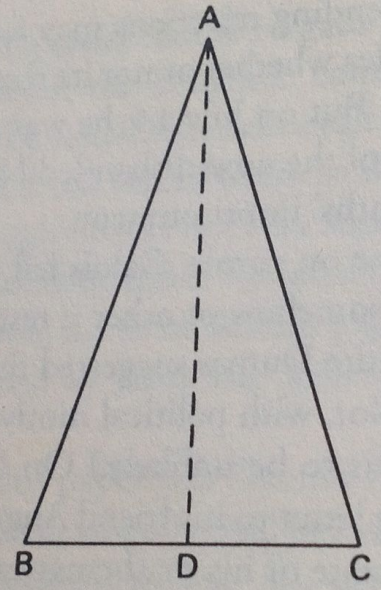


FIGURE 24 The symmetry of an isosceles triangle.

More examples of groups

Symmetry groups in 3 dimensions

• Symmetries of the five Platonic solids (cube 48 symmetries, dodecahedron 120 symmetries). In each case half are rotational and half are reflections (in a plane)
• The rotational symmetries of a dodecahedron form the smallest simple group which is not noncommutative.

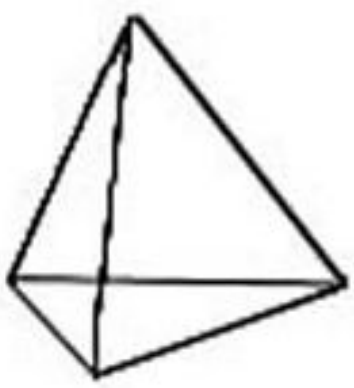
Sets of matrices, under **matrix multiplication** provide examples of both finite and infinite noncommutative groups.

• Mathematicians developed and studied matrices with certain applications in mind (in particular, the solution of large systems of simultaneous linear equations) and those applications required the complicated definition of matrix multiplication.
• Matrix arithmetic is probably the numerical task most often performed by present-day computers

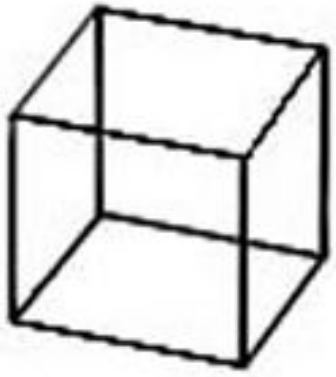
Another important class of groups is the *clock groups*, that is, the integers modulo n under addition modulo n (n need not be a prime number)

POLYHEDRA

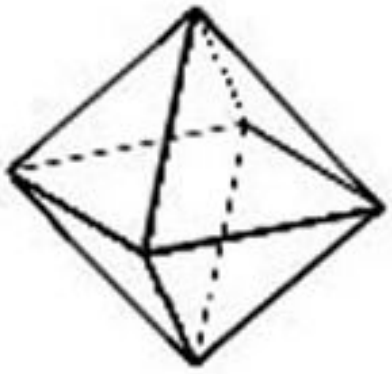
regular polyhedra (Platonic solids) --all sides are congruent regular polygons that meet the same way



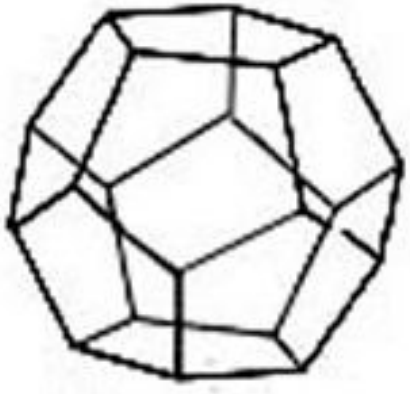
tetrahedron



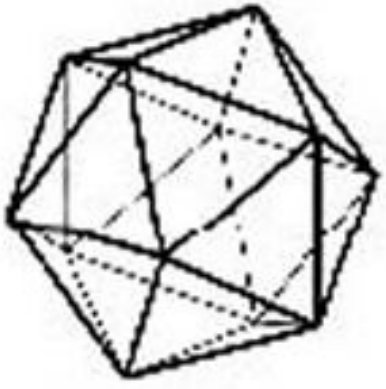
cube



octahedron



dodecahedron



icosahedron

example of a (square) matrix of order 2 is

$$\begin{bmatrix} 21 & -5 \\ 3{\cdot}8 & 20 \end{bmatrix}.$$

Matrices have their own arithmetic. The rule for adding two matrices (of the same order) is straightforward: you simply add corresponding entries. Thus

$$\begin{bmatrix} 1 & 3 \\ -2 & 6 \end{bmatrix} + \begin{bmatrix} 2 & 5 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 8 \\ 1 & 7 \end{bmatrix}.$$

Multiplication is a little more complicated. Briefly, you multiply the rows of the first matrix by the columns of the second, term by term, adding the answers as you go. For matrices of order 2, this is perhaps best explained by means of an algebraic example followed by a numerical one:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} v & w \\ x & y \end{bmatrix} = \begin{bmatrix} (av + bx) & (aw + by) \\ (cv + dx) & (cw + dy) \end{bmatrix},$$

$$\begin{bmatrix} 1 & 3 \\ -2 & 5 \end{bmatrix} \times \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} (2 + 9) & (4 + 3) \\ (-4 + 15) & (-8 + 5) \end{bmatrix}$$

$$= \begin{bmatrix} 11 & 7 \\ 11 & -3 \end{bmatrix}.$$

One of the primary aims in any branch of science is to identify and study the "basic objects" from which all other objects are constructed.

- In biology, these are the cells
- In chemistry, the atoms
- In physics, the fundamental particles

The same is true in many branches of mathematics.

- In number theory, it is the prime numbers
- In group theory, it is the 'simple' groups

In each of these examples, the basic objects of the theory are *structurally simple*, in the sense that they cannot be 'decomposed' into smaller entities of the same kind.

What the heck is a 'simple' group?

Simple groups, simplified

Suppose we have two groups A and B, each contained in a third bigger group G. The 'product' of A and B is the set C consisting of all products of one element of A with one element of B.

It is easy to verify the axioms of a group hold in C and that any two groups can be replaced by 'equivalent' groups which sit in a common bigger group.

A group is said to be **simple** if it is not the product of two smaller groups each with at least two elements. In fact, every finite group can be decomposed into a unique product of one or more simple groups, analogous to the fundamental theorem of arithmetic.

The integers modulo 6 is not simple: $\mathbf{Z}_6$ is the product of $\mathbf{Z}_2$ and $\mathbf{Z}_3$. In fact $\mathbf{Z}_n$ is simple if and only if n is a prime number

The analogy with prime numbers breaks down: recall that the rotational symmetries of the dodecahedron has 60 elements, which is not a prime number.

Which groups are simple and which are not?

Clock groups of prime order are simple; clock groups of composite order are not.

Clock groups are the only examples of commutative simple groups.

Is there a 'periodic table,' or atlas, of simple groups?

The short answer is YES.
There are 18 'regular' families (each containing infinitely many groups), and 26 highly irregular groups (also called one-off, or sporadic) that did not fit any pattern.

- Clock groups of prime order constitute one of the regular families.
- Alternating groups of degree 5 or more constitute another regular family.

The remaining 16 families are more complicated. They all consist of matrices.

The first 5 of these strange sporadic simple groups were discovered in the 1860s. The orders of these 5 groups range from 7920 to 244,823,040.

A century later, in 1965, a 6th sporadic group was found of order 175,560. It was a group of matrices of size 7 by 7.

Shortly, two more sporadic groups were found, of orders 604,800 and 50,232,960.

In 1980, the last of the 26 sporadic groups was found. It is by far the largest of the sporadic groups, a fact that earned it the name of "the Monster."

The monster consists of 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 matrices of size 196,883 by 196,883.

It is now known that the finite simple groups consist of the groups that make up the 18 regular families of groups, together with the 26 sporadic groups, *and no more*. This is the **Classification Theorem of finite simple groups**