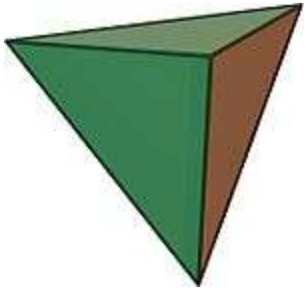
An Introduction to Group Theory

HWW Math Club Meeting (March 5, 2012)

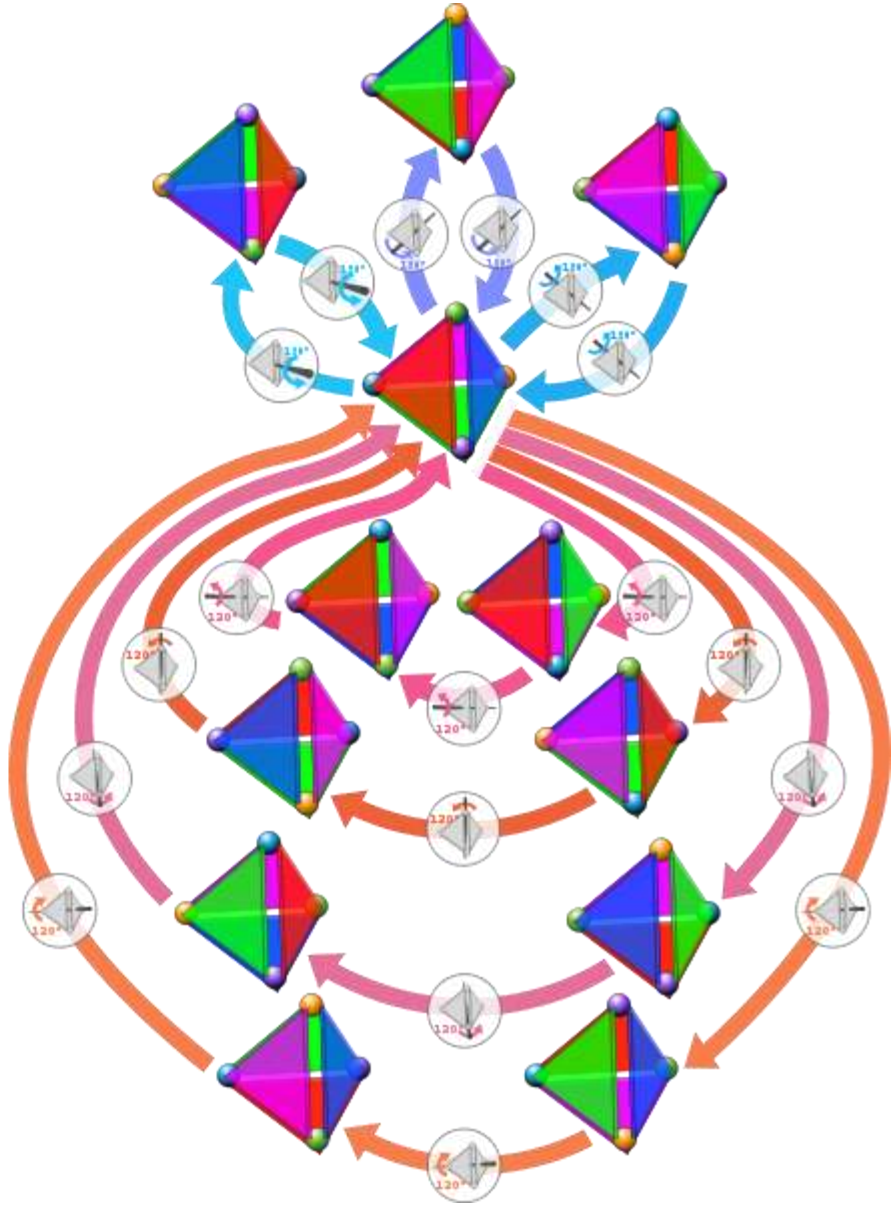
Presentation by Julian Salazar

Symmetry

How many rotational symmetries?



Symmetry



Symmetry

- So the 6-pointed snowflake, 12-sided pyramid, and the regular tetrahedron all have the same number of rotational symmetries…
- But clearly the “nature” of their symmetries are different!
- How do we describe this?

Symmetry

Numbers measure size.

Groups measure symmetry.

Terminology

- Set: A collection of items. Ex: $S = \{a, b, c\}$

- Element: An item in a set. Ex: $a \in S$

- Binary operator: An operation that takes two things and produces one result. Ex: $+$, $\times$

Formal Definition

A **group** is a set G with a binary operation $*$. We can notate as $(G,*)$ or simply G. We can omit the $*$ symbol.

It must satisfy these properties (axioms):

- Closed: If a, b are in G, ab is in G.
- Associative: $(ab)c = a(bc)$
- Identity: There exists e such that $ae = a = ea$ for every a in G. $(\exists\, e \in G : ae = e = ea\ \forall\, a \in G)$
- Inverse: For every a in G there exists a^{-1} such that $aa^{-1} = e = a^{-1}a$. $(\forall\, a \in G\ \exists\, a^{-1} \in G : aa^{-1} = e = a^{-1}a)$

EXAMPLE: $(\mathbb{Z},+)$

The integers under addition are a group.

- Closed: Adding two integers gives an integer
- Associative: It doesn't matter how you group summands; $(3+1)+4 = 3+(1+4)$
- Identity: Adding an integer to 0 gives the integer
- Inverse: Adding an integer with its negative gives 0

- Is $(\mathbb{R} - \{0\}, \times)$ a group?
- Is $(\{\pm 1, \pm i\}, \times)$ a group?

Identities are UNIQUE

Theorem: For any group, there's only one identity e.

Proof: Suppose e, e' are both identities of G.
Then $e = ee' = e'$.

Ex: For $(\mathbb{Z},+)$, only 0 can be added to an integer to leave it unchanged.

INVERSES ARE UNIQUE

Theorem: For every a there is a unique inverse a^{-1}.

Proof: Suppose y, z are both inverses of x.
Then $xy = yx = e$ and $zx = xz = e$.

$$y = ey = (zx)y = z(xy) = ze = z$$

Ex: In (ℤ,+), each integer has a unique inverse, its negative. If $a = 3$, $a^{-1} = -3$.

Composition (A note on notation)

Composition is a binary operator.

Take functions $f(x)$ and $g(x)$.

We compose f and g to get fg.

$fg(x) = f\big(g(x)\big)$, so we evaluate from right to left.

fg means g first, then f.

Let's "Group" our Symmetries

- Let e be doing nothing (identity)
- Let the binary operation be composition
- Let r be rotation 1/12th clockwise
- So $rr = r^2$ means…
- rotating 1/6th of the way clockwise!

- $G = \{e, r, r^2, r^3, \ldots, r^{11}\}$

Let's "Group" our Symmetries

- $G = \{e, r, r^2, r^3, \ldots, r^{11}\}$
  - Closed: No matter how many times you rotate with r, you'll end up at another rotation
  - Associative: Doesn't matter how you group the rotations
  - Identity: You can do nothing
  - Inverse: If you rotate by r^n, you must rotate r^{12-n} to return to the original state

Let's "Group" our Symmetries

- $G = \{e, r, r^2, r^3, \dots, r^{11}\}$
  - What is rotating counter-clockwise then?
  - It's r^{-1} (the inverse of r).
  - But wait! $r^{-1} = r^{11}$.
  - So $r(r^{11}) = e$. In plain words, rotating 1/12th twelve times gets you back to where you started =O

Let's "Group" our Symmetries

- $G = \{e, r, r^2, r^3, \ldots, r^{11}\}$
  - But inverses aren't unique! $r(r^{23}) = e$, right?
  - Yeah, but the net effect of r^{23} is the same as that of r^{11}.
  - So in our set, we only have r^{11}.
  - We only count "unique" elements for our group.

Let's "Group" our Symmetries

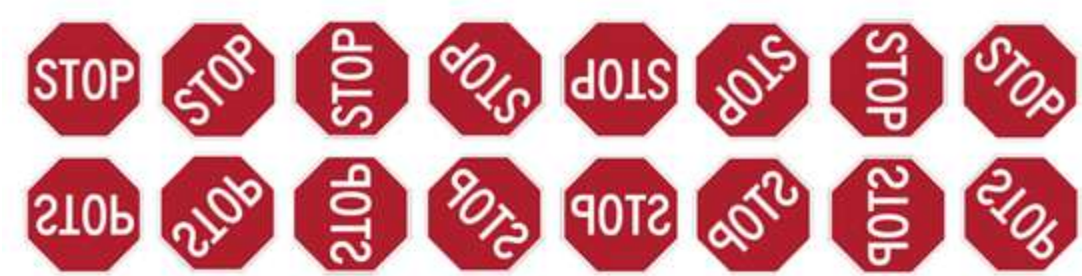
- Let e be doing nothing (identity)
- Let the binary operation be composition
- Let r be rotating the sign 1/8th clockwise
- Let s be flipping the sign over
- $G = \{e, r, r^2, \dots r^7, s, rs, r^2 s, \dots, r^7 s\}$

LET'S "GROUP" OUR SYMMETRIES

- $G = \{e, r, r^2, \dots r^7, s, rs, r^2s, \dots, r^7s\}$
  - Closed: No matter which rotations you do, you'll end up at one of the 16 rotations
  - Associative: Doesn't matter how you group the rotations
  - Identity: You can do nothing
  - Inverse: You can always keep rotating to get back to where you started

LET'S "GROUP" OUR SYMMETRIES

- $G = \{e, r, r^2, \ldots r^7, s, rs, r^2s, \ldots, r^7s\}$
  - What is s^{-1}?
  - What is $(r^2s)^{-1}$?
  - What is r^2sr^2s?
  - What is r^4s^2?
  - $r^2sr^2s \neq r^4s^2$.
  - We're not multiplying (ab not necessarily $= ba$)



Categorizing Groups

Cyclic groups: Symmetries of an *n*-sided pyramid.

Note: ($\mathbb{Z}$,+) is an *infinite* cyclic group.

Dihedral groups: Symmetries of a *n*-sided plate.

Other:

Permutation groups: The permutations of *n* elements form a group.

Lie groups, quaternions, Klein group, Lorentz group, Conway groups, etc.

Isomorphism

Consider a triangular plate under rotation.

Consider the ways you can permute 3 elements.

Consider the symmetries of an ammonia molecule.

They are ALL the same group, namely

$$\{e, r, r^2, s, rs, r^2s\}$$

Thus the three are isomorphic.

They fundamentally have the same symmetry.

Groups are NOT arbitrary!

Order: # of elements in a group

There are only 2 groups with order 4:
$\{e, r, r^2, r^3\}$, $\{e, r, s, rs\}$

There are only 2 groups with order 6:
$\{e, r, r^2, r^3, r^4, r^5\}$, $\{e, r, r^2, s, rs, r^2 s\}$

But there′s only 1 group with order 5!?
$\{e, r, r^2, r^3, r^4\}$

Using Groups

With groups you can:

- >>Measure symmetry<<
- Express the Standard Model of Physics
- Analyze molecular orbitals
- Implement public-key cryptography
- Formalize musical set theory
- Do advanced image processing
- Prove number theory results (like Fermat's Little Theorem)
- Study manifolds and differential equations
- And more!