BUSM: Introductory Lecture on Group Theory

What is a group?

Mathematician:

def: Group $(G,\cdot)$ is an ordered pair $(G,\circ)$, with a set G and a binary product $\cdot : G\times G \to G$ s.t. $\forall f,g,h \in G$,

1) $\exists I \in G$: $I\cdot g = g$
2) $\exists g^{-1} \in G$: $g^{-1}\cdot g = e$
3) $g\cdot f \in G$
4) $(f\cdot g)\cdot h = f\cdot(g\cdot h)$

Why? what is this useful for?

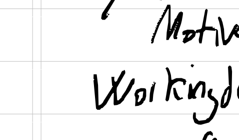
Motivation for def. of group

Working def.

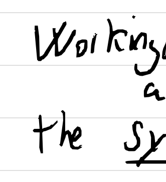
a group is a mathematical representation of the <u>Symmetries</u> of an object.

A symmetry of an object is an action which leaves some aspect of that object unchanged:

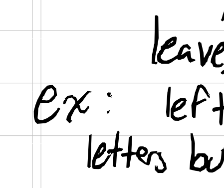
ex: left-right symmetry of stop sign, changes letters but keeps shape the same, so it is a 'geometrical symmetry'



Translations: changes location, keeps everything else the same



Homeomorphisms: changes geometry, keeps topology the same 'topological symmetry'



Symmetries have structure which we will show behave like a 'group'. Take the geometric symmetries of a triangle [shape needs to be exactly the same, no translations or 30° turns]

A
/ \
C — B

what are symmetries of a Δ?

I: keep Δ the same

r_1, r_2: rotate Δ by 120°, 240°

m_1, m_2, m_3 reflect about axis 1,2,3: | , \ , /

(m_1 A C—B = A B—C, m_2 A C—B = C A—B, etc)

what about 'compound' symmetries, Ex:

$m_1\cdot m_3\cdot\Delta \to$ first, m_3, then m_1.

$m_1 m_3$ A C—B $\to m_1$ B C—A $\to$ C B—A $\stackrel{?}{=}$ r_1 A C—B

We say

$m_1 m_3 = r_1$ because they do the same thing

this defines 'multiplication' of symmetries. do each in order from right to left (like function)

2 reflections = a rotation or I

what about $r_1 m_1$ A C—B $= r_1$ A B—C $=$ B C—A $= m_3$ A C—B

is this eq. to

$m_1 r_1$? no: $m_1 r_1$ A C—B $= m_1$ C B—A $=$ C A—B $= m_2$ A C—B

I) In general: properties of symmetries:

there is an 'Identity symmetry' which does nothing: $I\cdot g\cdot\Delta = g\cdot\Delta \Rightarrow I\cdot g = g$

II) it is always possible to undo symmetries: no matter what I do to triangle I can restore it to it's initial state by undoing everything $\Rightarrow$ inverses exist, $\exists g^{-1}$: $g^{-1}\cdot g = I$

III) say I have enumerated all symmetries of an object: $I, s_1, s_2, s_3 \dots s_N$. then, it must be that $s_i s_j = s_k$: composing two symmetries always gives you another symmetry, since you are keeping e.g. the geometry the same, & $a=b=c \Rightarrow a=c$

IV if $g\cdot f = h$, I can always replace $g\cdot f$ with h anywhere I see it, so

$g\cdot f\cdot l = h\cdot l$. from this, we have $g\cdot(f\cdot l) = (g\cdot f)\cdot l$

We can easily check that this holds for triangle symmetries:

I) ✓ II) $r_1^{-1} = r_2$, $r_2^{-1} = r_1$, $m_i^{-1} = m_i$, $I^{-1} = I$

III $r_1 r_1 = I$, $r_1 m_i = m_{i+1}$, $r_2 m_i = m_{i+2}$, etc

IV check this @ home.

In general a group is any set & binary product so that all of these hold. the usefulness of having such an abstract definition is that even when it is not obvious what symmetry there is, you can spot a group by just checking the axioms. but know that in general, every group can be thought of as the symmetry of <u>some</u> abstract object.

Examples of groups that don't at first seem like groups:

i) trivial: $\{I\}$, $I\cdot I = I$ (symmetries of a computer)
ii) integers: $\mathbb{Z}^+$ (symmetries of an infinite comb)
iii) set of 3D matrices w/ determinant 1 which are also orthogonal (so $M^T = M$): $SO(3)$ (symmetries of a sphere)
iv) functions $f: \mathbb{R}\to\mathbb{R}$ which are bijective and monotonically increasing (symmetries of a stretchy rope (that preserve 'rope-ness'))

exercises: is it a group: yes or no:

1) $\mathbb{Z}^\times$ (no)
2) $\mathbb{R}^\times$ (no)
3) $\mathbb{R}^n[x]^+$ (polynomials of order n under addition) (yes)
4) the set $\{s_1, s_2, s_3, \dots s_N\}$ with product $\cdot$ which multiplies every two elements $s_i s_j = s_1$ $\forall i,j$ (no)
5) the permutations of the set $\{1,2,3,4\}$ (yes)

Some definitions:

<u>def</u>: <u>Groups</u> G_1 & G_2 are 'isomorphic' if they are the same group (related by 'relabeling')

<u>def</u>: <u>subgroup</u>. $G_1 \subset G_2$ if G_1 is a group and all of it's elements are in G_2 & the multiplication is the same:

$I, r_1, r_2 \subseteq \{I, r_1, r_2, m_1, m_2, m_3\}$

but not

$\{I, m_1, m_2, m_3\}$

<u>def</u>: <u>Abelian group</u> (makes you sound smart)

a group where $ab = ba$, commutative group

fun fact: named after neils abel, who proved that quintic formula is impossible, <u>not</u> galois. died @ 26 from tuberculosis, was incredibly poor. Charles Hermite of 'Hermite polynomials' fame, said 'Abel has left mathematicians enough to keep them busy for 500 years'

<u>def</u>: <u>Generators of a group</u>

minimal subset S of G s.t. every element of G can be made by multiplying together elements of S: for Δ $S = \{r_1, m_1\}$: $r_2 = r_1 r_1$, $I = m_1 m_1$, $m_2 = r_1 m_1$, $m_3 = r_1 r_1 m_1$

A brief detour into representation theory (if time permits)

$\to$ All groups can be represented by sets of matrices over $\mathbb{C}$ or $\mathbb{R}$ w/ matrix multiplication

this is a theorem in math. for finite groups, this follows from the fact that every finite group is a subgroup of S_n, and that one can find a matrix rep of S_n since they are permutations.

This should make sense: matrix multiplication is not commutative & matrices act like transformations of the $\mathbb{R}^n$ or $\mathbb{C}^n$

here, representation means that there is an isomorphism

Finite groups: Δ group (D_3), C_n, $\mathbb{Z}$ mod n

Infinite groups: $\mathbb{Z}^+$

Continuous groups/lie groups: $SO(2)$

Cameron part