BMC - Advanced: Groups and Symmetry

(2 hour crash course!)

Chris Overton

231120 - Handout, revised after lecture

We met on Nov 15 for a "crash course" on groups, motivated by thinking of their elements as symmetry operations.
These notes are not fully self-contained, but they should remind you of what we discussed (in some cases, what we **would have** discussed if time had permitted.)

To find out more, there are many excellent introductions to group theory - most taking over two hours to study.

Warm-up problems

What are all possible symmtries:
a) of an equilateral triangle?
b) of a regular tetrahedron?
c) of a 4-dimensional regular hyper-tetrahedron?

[More generally, the n-dimensional object with n+1 vertexes is called an n-simplex]

Here, by symmetry, we mean a rigid transformation (i.e. preserving lengths and angles) that maps corners to corners

In class, we demonstrated how we need to decide whether "symmetries" include mirror reflections, which we were regrettably not able to film for dimension >= 4.

Note:

- When you see: <---- SPOILER ALERT---->, (or just <----->), that means please don't look beyond this until you have thought about the question asked!
- Topics for thought are often marked by -->. These are less likely to have answers, and several were discussed in class
- <Done in class> material is not spelled out here

Topics for today

- Symmetries as a way to motivate groups & their axioms
- Group properties I - as illustrated on the symmetric group S_3
    - Properties of multiplication ("Cayley") tables
    - Subgroups, cosets, actions
- Where groups sit in math
- Speed-dating popular kinds of groups; some of their properties
    - Symmetric groups S_n
    - Linear groups
    - "Easy" groups: abelian (commutative)
    - p-groups
    - All finite groups
    - Free groups, and groups via presentations
- Crucial ways to understand how groups keep and break "symmetry":
    - Non-commutativity (related to non-identity commutators)
    - Homomorphisms
    - Conjugacy
    - **Normal subgroups**
- We violate the usual group intro by not showing a (standard) Rubik's cube
- More machinery & examples, as time permits

Symmetries as a way to motivate groups & their axioms

We'll write groups in capital letters like G, H and their elements in lowercase like $g_i, g_j \in G$

The first time I learned about groups, it seemed strange to have to memorize the weird set of defining rules. So lets "derive them" by considering the set of symmetries of an object.

<---- SPOILER ALERT---->

- a specified set of elements (Its cardinality is called the group's **order** and is written $|G|$)
- well defined operation: any $g_i, g_j \in G$ determine an element $g_i * g_j \in G$
- neutral element, which we'll call "1": for $g \in G, 1 * g = g * 1 = g$
- inverses (prove: left inverse = right inverse): for $g \in G$, there's an element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = 1$
- associativity

--> Question: what's a property we are used to from numbers that need not be true for symmetries?

<----->

Importantly, groups need **not** be commutative. This takes some getting used to, but allows for richer structure.

We demonstrated this by showing rotating a book by 90 degrees first around the x-axis and then around the y-axis turns out differently than for the other order of rotations

Group properties I - illustrated for S_3 - a symmetric group

To study this, we have to use notation from general permutation groups S_n.

Two notations, respectively "permutation" and "cycle" notations:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix} = (1\ 2\ 3)(4\ 5)(6) = (1\ 2\ 3)(4\ 5)$$

We prefer the second, because it is briefer and easier to read.
Elements not permuted (like 6 here) form their own cycle, which may be omitted.
Our convention: cycles multiply from left to right, e.g. (1 3)(2 3) = (1 2 3),
not (1 3 2)

Work out the **multiplication table** (called **Cayley table** for S_3. You just write rows and columns for all the elements $\{g_i\}$, and then in the (i,j)th position, write the product $g_i * g_j$

<---- SPOILER ALERT---->

$\circ$	e	(123)	(132)	(23)	(13)	(12)
e	e	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	e	(13)	(12)	(23)
(132)	(132)	e	(123)	(12)	(23)	(13)
(23)	(23)	(12)	(13)	e	(132)	(123)
(13)	(13)	(23)	(12)	(123)	e	(132)
(12)	(12)	(13)	(23)	(132)	(123)	e

What are some properties of this (kind of) table?

<----->

- The number $|G|$ of elements = # of rows = # of columns
- The neutral element appears exactly once in each row, and in each column
- Subgroups, cosets, actions...

Def: a subset $H \subset G$ is called a **subgroup**, written $H < G$ if H is also a group under the multiplication inherited from G.
[We could also write $H \leq G$ to explicitly allow the case $H = G$, but many authors use subset and subgroup notation as above to include this possibility.]

Def: the **right cosets** of H in G (for $H \leq G$) are the sets $\{h * g | h \in H\}$, namely for a fixed $g \in G$, with h ranging over (all) elements of H.

--> Work out the **subgroups** of S_3, including A = <(1 2 3)> and D = <(1 2)>, where the angle notation refers to the smallest group containing the elements shown. This is also called the subgroup **generated** by such elements.

--> Work out the **right** cosets of A.

Same question for right cosets of D, and **left** cosets of A and D.

--> Which sets of cosets are equal???

<----->

We saw A = <(1 2 3)>'s left and right cosets were identical, but not so for D.
Later, we see that this is equivalent to noting that A is **normal** in G.

Lagrange's theorem since the elements of G split into distinct cosets $\{Hg_i\}$ for a subgroup $H \leq G$, it follows that $|H| \ | \ |G|$, namely the order of a group is a multiple of the order of a subgroup

G **acts** on the $\frac{|G|}{|H|}$ cosets of H in G by permuting them. For example, for $g \in G$, any given coset Hg_i is turned into the coset $H(g_i g)$ (posibly a different coset)

This creates a map from G to the symmetric group $S_{|G|/|H|}$

--> If you only knew the image of this map, would that give you enough information to understand G as a group?

<----->

Answer:

- Definitely yes, if $H = 1$, because then you can reconstruct G's entire multiplication table from how its right multiplication permutes its elements, which are just cosets of {1}.
- No if H = G, because then you are just permuting a single object. (BUT: if G was already just 1, then yes, this shows the whole trivial structure of G.)
- If $1 \lneq H \lneq G$, it depends on how much structure of G gets obscured!

Where groups sit in math

Examples:

- **All** finite groups can be thought of as permutation groups. When you have a permutation of dimension (in a vector space), that is a particular kind of linear transformation. So group theory can sit inside linear algebra…
- Finite field extensions $f \subset F$ are characterized by the ways you can transform F while leaving f fixed. These form *Galois groups* and are a particularly clear application
- More generally, there are many cases in mathematics where elements of a group correspond to "maps" of elements in another space that respect certain properties of these elements, whether they are rigid transformations, differentiable maps, or many other possibilities. The group will depend on what kind of maps are allowed
- Another very general use for groups is as a way of describing elements of another set. For example, you can define groups that describe say the 217-dimensional structure of a space. This forms a map from spaces to groups, in which case problems about spaces can be turned into problems about groups - a very important part of **algebraic topology**

Speed-dating popular kinds of groups; some of their properties

The last two of these are intractable ("unsolvable", in certain senses.)
Much of the subject of group theory involves understanding "harder" groups by building them out of simpler ones.

- Symmetric groups S_n
- Linear groups - also, groups of "Lie type": linear-like groups over finite fields...
- "Easy" groups: abelian (commutative)
- p-groups
- All finite groups
- Free groups, and groups via presentations

<Explained more in class>

Some interesting facts about such types of group

Groups as maps:

- Every finite group is a subgroup of a symetric group
- Every symmetric group can be "represented" as a linear group
- Examples of linear groups: groups of certain n*n matrices with coefficients in a field F (like R, the reals...): $GL_n(F)$, $SL_n(F)$, $O_n(F)$, $SO_n(F)$

Commutative (abelian) groups

- We will use the notation Z/n for the (additive) group of integers mod n
- Finite abelian groups G have a clear classification that's kind of like the unique factorization of integers: there is a unique way you can write $G = Z/n_1 * Z/n_2 * \ldots * Z/n_k$, where $n_1 | n_2 | \ldots | n_k$

p-groups

- p-groups are groups of order p^n. They can be very complicated, but if $p^n||G|$ (i.e. p^n divides the order of G), then G has a subgroup of this order. There are very important **Sylow** theorems about these
- p-groups allow rich structure, which has the side effect of there being so many different ones!
  A large majority of groups with order under 2000 have orders a power of 2 - of which the largest number have the highest such power, namely 1024

Free groups and presentations

<**Intended** for class, but barely mentioned>

- Free group, their presentations, and a presentation of the dihedral group D_n, with rotation a and reflection d: $< a, d | a^n = d^2 = 1, d * a * d^{-1} = a^{-1} >$
  Some authors write D_{2n} for this group of order 2n
  [We noted S_3 is the symmetry group D_3 of the regular 3-gon (aka triangle)]

Crucial ways to understand how groups keep and break "symmetry"

Non-commutativity (related to non-identity commutators)

Review asymmetry of multiplication table of S_3

Commutators $g * h * g^{-1} * h^{-1}$

We discussed how these would be 1 if g and h commuted, but how the deviation from 1 is a way to undertand how g and h "twist" each other.
Also discussed: how commutators are a great way to limit results in case g or h are within known normal subgroups [One key technique for solving Rubik's cube type problems]

Homomorphisms

In group theory, the only kinds of maps f we consider from a group H to a group G preserve products. So if $h_i, h_j \in H$, let $g_i = f(h_i), g_j = f(h_j)$.

For $f : H \to G$ to be a homomorphism, we need
$f(h_i *_H h_j) = f(h_i) *_G f(h_j) = g_i *_G g_j$,
so f must "translate" multipication within H into multiplication within G.
This is emphasized by showing the appropriate group as a subscript to each multiplication.

We can write this as a "commutative diagram." Note: everything in the top row happens in H, and everything in the bottom row (including its multiplication!) happens in G:

$$\begin{array}{ccc} h_i & \overrightarrow{*h_j} & h_i * h_j \\ \downarrow f & & \downarrow f \\ g_i & \overrightarrow{*g_j} & g_i * g_j \end{array}$$

--> Show this implies f(1) = 1' (for neutral elements $1 \in H, 1' \in G$), and
$f(h^{-1}) = f(h)^{-1}$

If you keep times'ing by g, you might get back to 1. If so, the smallest natural number n such that $g^n = 1$ is called its **order**. If not, $g's$ order is infinite.

This lets you define the subgroup $< g >$ generated by the set $\{g\}$.
$< g >$ is said to be **cyclic**, because it just consists of all integer powers g^i of g

--> If g has finite order n, show this is a subgroup. In particular, show $g^{-1} = g^{n-i}$.

--> If g's order is infinite, we use the notation $g^{-i} = (g^{-1})^i$, and then show $< g >$ again is just the set of all integer powers of g.

Conjugacy

--> Identify which elements g_i, g_j in S_3 are **conjugate**, namely, there exists an element $g \in G$ such that $g * g_i * g^{-1} = g_j$

--> Can you generalize this to higher S_n?

<Discussed in class>

--> Given elements $g_i, g \in S_n$ in cycle notation, how can you write down the conjugate above?

<----->

Answer - convince yourself this works! in the cycle notation of g_i, replace every symbol x by the symbol $g^{-1}(x)$, namely what the inverse of g takes x to!

Conjugation by a fixed element g is an isomorphism on G. From this cycle notation above, you have even more explicit evidence: since conjugates have the same cycle structure, they have the same order.

Normal subgroups

We saw above that left and right cosets differ for certain subgroups, but not for others.

Def: A subgroup $H < G$ is **normal**, written $H \lhd G$ if for any $g \in G$, $gHg^{-1} = H$.

--> Show $H \lhd G$ is equivalent to left and right cosets of H corresponding for all $g \in G$: $gH = Hg$

This is a very special and important condition that distinguishes subgroups you can "divide by", giving the sequence of two homomorphisms: $H \hookrightarrow G \twoheadrightarrow G/H$, because of a surprising fact:

Def in a homomorphism $f : G \to H$, the set $N = \{n \in G | f(n) = 1\}$ is called the **kernel**

Theorem: "**kernels are normal, and all normals are kernels**":
A) The kernel N of a such a homomorphism f is a normal subgroup of G.
B) Every normal subgroup N is the kernel of an isomorphism from G onto the group of cosets of N in G

Def: G always has "trivial" normal subgroups $1 \lhd G$ and $G \lhd G$.
If G has no other normal subgroups, we say it is **simple**

We are not near to being able to classify all finite groups. But one of the major math triumphs of the 20th century was to work out all the finite simple groups

- Examples of simple groups: Z/p for p prime
- A_n for $n \geq 5$ (Here A means the "alternating group", namely the elemends of S_n of "even parity")

"Parity" is just the number mod 2 of of 2-cycles in a cycle representation of an element $s \in S_n$ (which turns out to be well-defined.)
In symmetries of simplexes, we say that parity captures whether a mirror reflection is needed.

--> Try to show A_5 is simple by noting that and normal subgroup $H \lhd A_5$ would have to consist of complete conjugacy classes of elements of A_5. Why is this tricker than just considering conjugacy classes as we have worked out for S_5?

<----->

Caution: just because x_i, x_j are conjugate in S_n does that mean they're conjugate in A_n?

A better way is to show A_n is simple (for $n \geq 5$) is to show there is a "parity" homomorphism from $S_n \to Z/2$ with kernel A_n.

We violate usual introduction to groups by not showing a (standard) Rubik's cube

[In class, however, we did trot out a whole box full of Rubik's variants, including ones that were surprisingly isomorphic or non-isomorphic]

Some ideas we discussed

- The "unreasonable" success of commutators
- Subgroup structure
- Characterizing the complexity and solution of the tetrahedral puzzle of "size 3"

More machinery & examples, but ran out of time...

Sylow theorems

If $|G| = p^n * m$ for prime p that does not divide m, any subgroup of order p^n is called a p-**Sylow** subgroup

- G always has these for any prime that divides its order
- The p-Sylow subgroups for G are all conjugate
- Their number is 1 mod p and divides m

These sound like very specific and technical, but they allow many conclusions, such as:
==> Show there is no simple group of order 28, by proving 7-Sylow subgroups are normal

p-groups

- p-groups have nontrivial **center** (elements that commute with everything.) A center is normal, so p-groups can be "decomposed"

Group presentations

==> Try the group presentation challenge in section 2.2 of "Crash course" (p.32)

Conclusion

- You now know enough group theory defs to be dangerous
- More reliable use comes from practice with standard facts and working though many examples (e.g. finding all the groups up to order 15)
- But you do know enough about symmetric groups to be able to work with any group that can be described with permutations - which all groups can! Downside: symmetric groups still have a lot of mystery.
- You will see groups all over the place in math, and even in unexpected places like crystal structures in chemistry. Hopefully, today's talk has whetted your appetite

References:

- Cameron, 2016: "A Crash Course on Group Theory" (omits proofs, but a useful guide for study)
- Goodwin/Morrow?, 2019: "An introduction to the classification of finite groups" (19 pages, so omits proofs)
- Kurzweil & Stellmacher, 2004: "the theory of finite groups" There are many, many introductions to group theory, including in almost any intro text on ("modern") algebra. This is just one reasonable & reasonably recent text.)
- Interestingly, the "Princeton companion to mathematics" (Gowers, ed., 2008) doesn't have a major section **just** on groups, because they come up in so many other places. They do introduce groups first as symmetries.