The Mathematician's group theory - Introduction

What is a group?

Def:- A group is a set G together with a binary operation $*: G \times G \to G$ s.t.

(i) $a*(b*c) = (a*b)*c$, $\forall\ a,b,c \in G$

(ii) $\exists\ e \in G$ satisfying $a*e = e*a = a$ $\forall\ a \in G$

(iii) $\forall\ a \in G$, $\exists$ an element $a^{-1} \in G$, s.t.

$a*a^{-1} = a^{-1}*a = e$. a^{-1} is called the inverse of G.

These look like simple axioms, but there can be more general structures.

Monoids

Remove axiom (iii) and you get a monoid. In fact, monoids basically represent the matrices one gets for non-unitary quantum evolutions.

Semigroups

Remove axiom (ii) as well & what you get is called a semigroup

Can axiom (iii) hold without axiom (ii)? (You need e!!!)

Time for examples

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
2. $(\mathbb{Q}\setminus\{0\}, *)$, $(\mathbb{R}\setminus\{0\}, *)$
3. $(V, +)$ for any vector space V ("Modules") [$(N\times N)$ matrices]
4. $(GL_N(\mathbb{F}), *)$
   ↳ General linear transformations with entries from a field F

For a group, one needs only one operation. But all the sets we discussed had two. Is there a higher classification?

Is this a group $(\mathbb{Z}^+, +)$? Can it be any structure we have discussed till now?

Two terms very important to physicists

"Abelian" → A group is called abelian if $ab = ba \ \forall \ a, b \in G$.

"Non-abelian" → $ab \neq ba$ for atleast any one such pair.

How constrained is a group?

~~Say ax xxup Xax X elements. Box X~~

→ Right now, I can rename my elements & there can be infinite such groups.

What is fundamental to a group? A multiplication table.

(for finite groups, of course. but there are notions for infinite groups as well).

Let $e, a_1, \ldots, a_{n-1}$ be elements of the group, which has a total of n elements (distinct).

Write these down in a row & column like a table.

	e	a_1	. . . .	a_{n-1}
e				
a_1				
.				
.				
.				
a_{n-1}				

Let us do so, for $n=3$ & $n=4$. How many groups are possible for each case? (Without renaming, etc)

↳ Just remember the axioms.

→ What is this renaming? We need more info for that. Let us try to formalize this renaming.

Homomorphism

Let H & G be two groups with operations $*_H$ & $*_G$ respectively.

We say $\phi: G \to H$ is a homomorphism if

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) \quad \forall\ g_1, g_2 \in G.$$

Now, if ϕ is also a bijection, we call ϕ an isomorphism.

→ Formalized notion of "renaming".

Homomorphisms preserve the multiplication table. However, homomorphisms might not be injective or surjective. So, there might be missing entries or identical elements in place of different elements.

↙ $\phi(g_1) = \mathbb{1}\ \forall\ g_1 \in G$

↘ $\phi: \mathbb{Z} \to \mathbb{R}$ given by $\phi(z) = z$.

Isomorphisms 'exactly' preserve the multiplication table.

Now why study groups? Notion of symmetry, in exact terms. No handwavyness.

Before we go there, here are some "obvious" properties you can prove at your leisure.

(i) Identity is unique.

(ii) Inverse is unique.

(iii) Inverse of inverse is the element itself.

(iv) $(ab)^{-1} = b^{-1}a^{-1}$ (Matrices?)

∎

Permutation groups

Better known as S_n ("symmetric groups on n indices/letters")

$$S_n = \{ \text{bijections from } [n] \to [n] \}$$

How does one define the group operation.

Let $\sigma : [n] \to [n]$ & $g : [n] \to [n]$ be bijections.

Then $\sigma g : [n] \to [n]$ is also a bijection. Check that group axioms are satisfied.

Elements of S_3 are:-

{ }.

As you have studied earlier, tensors have multiple indices. The symmetry of such objects is dictated by the permutation group & its functions.

Take $\phi : S_n \to S_n$ given $\phi(\sigma) = \sigma$. Obviously homomorphism.

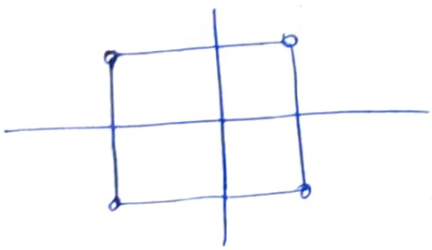
Is $\phi(\sigma) = \sigma^{-1}$ a homomorphism?

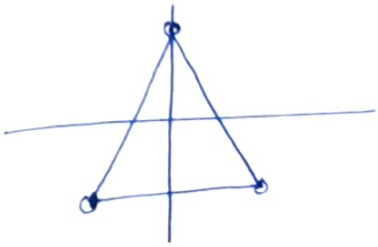
Is $\phi(\sigma) = \sigma^2$ a homomorphism?

Counterexamples/Pf ? → Insert order of group & order of element

A more "physical" example

① D_{2n} is the set of symmetries of a regular n-gon drawn symmetrically about the origin & the y-axis. This is called the dihedral group





Define actions r & s

r → rotates the diagram by $2\pi/n$, n is the n-gon.

s → flips it w.r.t. the y-axis

It is clear that applying r & s does not do anything to the diagrams i.e. these are symmetries.

Now, we'll see how r & s generate the symmetries.

We now write the generator form of the group.

$$D_{2n} = \langle r, s \mid s^2 = r^n = 1,\ rsr = s \rangle.$$

What does this mean? Take as many products of r & s in whatever order you like, following these rules.

You get all the elements of D_{2n} (distinct).

Some easy things to see —

(i) $1, r, \ldots, r^{n-1}$ are distinct. } Physically very easy to see.

(ii) $s^2 = 1$.

(iii) $s \neq r^i$ for any i. } Slightly hard

(iv) $rs = sr^{-1}$

(v) $r^i s = sr^{-i}$

Subgroups

A subset of the group, which is closed under taking products & inverses / just closed. denoted $G \leq H$, where G is a subgroup of H.

Cayley's theorem

Every finite group is isomorphic to a subgroup of some symmetric group. In particular, if $|G| = n$, then $G \leq S_n$. ⟶ Shows why S_n is so important.

↳ subgroup

↳ Very rich in properties.

Now, we come to some more interesting definitions.

Kernel – Let $\phi: G \to H$ be a homomorphism.

$$\text{Ker}(\phi) = \{ x \in G \mid \phi(x) = e_H \}.$$

Some important facts.

1. $e_G \in \text{Ker}(\phi)$.
2. If $\text{Ker}(\phi) = \{e_G\}$, then ϕ is an isomorphism.
3. $\text{Ker}(\phi) \trianglelefteq G$.

Why define kernel? (Other than fun)
So that we can define

Normal subgroup (denoted $N \trianglelefteq G$)

$N \leq G$ is called a normal subgroup if the set

$$gNg^{-1} \equiv \{ gng^{-1} \mid n \in N \} = N.$$

This operation is called conjugation.

All Abelian subgroups are normal.

Connection

$N \trianglelefteq G$ iff $N = \text{ker}(\phi)$, for some ϕ.

A definition we'll use later.

Center

Center of a group is defined as.

$$Z(G) = \{ g \in G \mid gxg^{-1} = x \ \forall \ x \in G \}$$

As per physical understanding, symmetries act on some set of objects. There is a general mathematical notion to this. Let us understand this.

Group action

A (left) group action of a group G on a set A is a map $\cdot : G \times A \to A$ with the following axioms:-

i) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \quad \forall \; g_1, g_2 \in G \;\&\; \forall \; a \in A$

ii) $1_G \cdot a = a \quad \forall \; a \in A.$

→ Looks like a homomorphism, right?

Important consequence

$S_A = \{$ bijections: $A \to A \}$.

Let $\sigma \in S_A$.

Then $\sigma . a \equiv \sigma(a), \quad \sigma \in S_A, \; a \in A.$

Suppose G acts on A. Then, define $\forall \; g \in G$,

$\sigma_g : A \to A$ by $\sigma_g(a) = g . a$.

Then

i) $\forall \; g \in G$, σ_g is a permutation of A.

ii) $\phi : G \to S_A$ given by $\phi(g) = \sigma_g$ is a homomorphism.

So the group action is basically a permutation on the set A, which is exactly what a symmetry does to its object set.

Now, we use conjugation and see how it is able to create a partition on the group.

i) $\bigcup_i P_i = G$

ii) $P_i \cap P_j = \phi$ if $i \neq j$

Conjugacy classes

We say $a, b \in G$ are conjugate if $\exists\, g \in G$ s.t. $a = gbg^{-1}$. Let

Now, say,

$a \sim b$ if a & b are conjugate.

We show that these form a partition of G. (or rather, equivalence classes) i.e. $\sim$ is an equivalence relation.

See that $a \sim a$ as $a = eae^{-1} = a$.

Now, suppose

$$a \sim b \Rightarrow \exists\, g \text{ s.t. } a = gbg^{-1}$$
$$\Rightarrow b = g^{-1}ag \;\&\; g^{-1} \in G \text{ as } g \in G$$
$$\Rightarrow b \sim a$$

Finally, suppose $a \sim b$ & $b \sim c$

$$\Rightarrow \exists\, g_1 \text{ s.t. } a = g_1 b g_1^{-1}$$
$$\& \exists\, g_2 \text{ s.t. } b = g_2 c g_2^{-1}$$
$$\Rightarrow a = g_1 g_2 c g_2^{-1} g_1^{-1}$$
$$= g_1 g_2 c (g_1 g_2)^{-1} \;\&\; g_1 g_2 \in G \text{ as } g_1, g_2 \in G$$
$$\Rightarrow a \sim c.$$

So, $\sim$ is an equivalence relation on G. Suppose $[a]$ represent the equivalence class of a, where $a \in G$. This is called a conjugacy class.

How do conjugacy classes look for an Abelian group?

Conjugacy class of e = $\{e\}$ always.

Conjugacy classes of S_3 are $\{e\}$, $\{(123), (132)\}$, $\{(12), (23), (13)\}$.

Let us recall the generator form of D_{2n}.

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1 \rangle$$

Here r & s are called the generators of D_{2n}.

Finally, the most trivial family of groups !!!

Cyclic groups

Def] A group G is cyclic if there is some $x \in G$ s.t

$$G = \{x^n \mid n \in \mathbb{Z}\}$$

Clearly, G is abelian.

$G \simeq$ nth roots of unity.

Finally, we go to a higher structure

Rings

A ring is a set R together with two operations $+, * : R \times R \to R$ called addition & multiplication resp., which satisfy the following -

(i) $(R, +)$ is an Abelian group.

(ii) $(a * b) * c = a * (b * c), \quad \forall\ a, b, c \in R$

iii) $(a+b) * c = a * c + b * c$

$a * (b+c) = a * b + a * c$

R is said to be commutative if $a * b = b * a \ \forall\ a, b \in R$.

R is said to be have an identity if $\exists\ e \in R$ s.t.

$a * e = e * a = a \ \forall\ a \in R$

→ A commutative ring s.t. every non-zero element has a multiplicative inverse is a field.

Ex a) $(\mathbb{Z}, +, *)$ b) $(2\mathbb{Z}, +, *)$ c) $(GL_n(\mathbb{F}), +, *)$

Wedderburn's theorem (fun fact)

All finite "division" rings are commutative & thus are finite fields.

Modules — "Generalized" vector spaces

Remember that vector spaces use a field $\mathbb{F}$. Vector spaces are defined over said field $\mathbb{F}$. This can also can also be done over a ring. The vector space is then called a module.

Def Let R be a ring. A left module over R is a set M together with

(1) A binary operation $+$ on M under which M is an abelian group.

(2) A map $rm : R \times M \to M$, which satisfies $\forall r \in R, m \in M$,

(a) $(r+s)(m) = rm + sm$ $\quad \forall\ r, s \in R,\ m \in M$

(b) $(rs)m = r(sm)$ $\quad \forall\ r, s \in R,\ m \in M$

(c) $r(m+n) = rm + rn$ $\quad \forall\ r \in R,\ m, n \in M.$

If the ring has an identity, we impose

(d) $1m = m$ $\forall\ m \in M$.

If R is a field, the left module is just a vector space over R.

Examples

" $\mathbb{Z}$-modules are the same as Abelian groups. "

Def: $R = \mathbb{Z}$, M is any Abelian group, $rm \equiv \begin{cases} m+m+\cdots+m \ (r \text{ times}) & r>0 \\ 0 & \\ -m-m-m-\cdots-m \ (r \text{ times}) & r<0 \end{cases}$

See that these satisfy all the axioms.

Every Abelian group is a $\mathbb{Z}$-module & vice-versa.

There are various interesting topological results about modules.

Abstraction levels are getting pretty high!!

Representation theory comes to the rescue.

The Physicist's group theory – deep dive

Motivation →

Every symmetry is group-theoretic

(1) Lorentz transformations form a group, called the Lorentz group.

(2) Strong interactions have SU(3) flavour symmetry – group theoretic models explain why proton & neutron masses are so close.

(3) Weak interactions have a SU(2) symmetry & electromagnetic interactions have a U(1) symmetry.

(4) Wigner's classification – classification of the $E \geq 0$ irreducible unitary representations of the Poincare group, gives a classification of all particles
↳ 10 dimensional Lie group. (Next lecture)

(5) I mean, it is cool regardless of use. But its uses are what make it even cooler.
↑ Howard Georgi thinks so.

Hence, we begin representation theory of finite groups

Firstly, what is a representation of a group G?

↳ It is a map from $D: G \to$ space of linear operators (↳ Matrices form a vector space)
which satisfies the following:-

i) $D(e) = \mathbb{1}$ (identity map)

ii) $D(g_1 g_2) = D(g_1) D(g_2)$.

What is the simplest representation? $D(g) = \mathbb{1} \ \forall g \in G$.

↳ Trivial representation.

Since we have linear operators of any size, we also can act them on vectors. We can be very creative with representations.

(1) Enumerate all the group elements, say $g_1, \dots, g_N$. Say $g_i = e_i$ where e_i is the ith basis vector of a N-dimensional vector space

Define D s.t. $D(g_i)|g_j\rangle = |g_i g_j\rangle$.

For example, if I do this for $Z_3 = \mathbb{Z}/3\mathbb{Z}$, i.e. $\{0,1,2\}$

$$D(0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad D(1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad D(2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

↓ identity

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

This is called the regular representation.

It is of dimension of the order of the group, i.e. N.

So, for something like the permutation group S_4, which has 24 elements, each matrix here is 24-dimensional.

Not a very useful representation, right?

We move on to other representations.

Defn Two representations D', D are said to be equivalent if $\exists\, S$ s.t.

$$D'(g) = S^{-1} D(g) S \quad \forall\ g \in G.$$

Defn A representation is unitary if each $D(g)$ is unitary i.e.

$$D(g)^\dagger D(g) = D(g) D^\dagger(g) = \mathbb{1} \quad \forall\ g \in G.$$

Nice result: All representations of finite groups are equivalent to unitary representations. (We'll prove this later)

Reducible & irreducible representations

A representation is reducible if it has an invariant subspace, i.e.:

$\exists$ P projection operator

s.t.

$$PD(g)P = D(g)P \quad \forall \; g \in G.$$

Try this out!!

Take $P = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

See that $D(g)P = P$ where $D(g)$ is the regular representation for Z_3 we just discussed.

- If $D(g)$ is not reducible, it is irreducible. (irrep)

This is the only group of 3 elements, up to isomorphism.

	1	a	b
1	1	a	b
a	a	b	e
b	b	e	a

a needs an inverse.

$a^{-1} \neq e$,

so

$a^{-1} = a$

or $a^{-1} = b$

Suppose $a^{-1} = a$

$\Rightarrow a^2 = e$.

But then what is ab ?

If $ab = a^2$, $b = a$ (which is not possible)

so, $ab \neq e$, $ab \neq a$ ($\Rightarrow b = e$) not possible

That only leaves $ab = b$, which is again not possible,

which implies $a = e$ (again not possible).

So $ab \neq e, a, b$. ($\Rightarrow\Leftarrow$ to group definition)

So, $a^2 \neq e$.

But $a^2 \neq a \Rightarrow a = e$, not possible.

So $a^2 = b$.

Then $ab = e$.

Similarly, $b^2 \neq e$. So, $b^2 = a$ ($b^2 \neq b$, see that you understand)

Now, that automatically sets

$ab = ba = e$. (Again, see that you understand why!!)

Also, see that commutativity is forced i.e. fixed by definition.