Group theory - Intro

- *group* is in general a set of some abstract elements with binary operations of specific properties
- one of our mains *goals* is to *represent* this set by some more tractable objects - usually matrices with the usual multiplication
- for physicist, group theory is mainly a tool to study symmetries & their consequences

- *symmetry* - usually invariance with respect to some kind of transformations:
  - spatial: translations, rotations, reflections, parity ($x_i \to -x_i \Leftrightarrow$ inversion)
  - translation in time
  - more abstract concepts: e.g. in particle physics
- *applications/usefulness* of the group theory

1, systematic tool to *search for dynamic laws* and conservation laws (Noether theorem)
   - translation in time $\Rightarrow$ energy conservation
     in space $\Rightarrow$ momentum conservation

2, tool to their *solution*
   - restrictions on possible solutions
   - decomposition of the solution space to independent subspaces $\Rightarrow$ reduction of dimensionality

$$(T + V(x))\psi(x) = E\psi(x)$$

$$V(x) = V(-x) \Rightarrow \psi(x) = \pm \psi(-x)$$ ... symmetric & antisymmetric solutions

3, *selection rules* for physical transitions (radiation $\Rightarrow$ change in parity)

Def: Group

A set with binary operation $(G, \cdot)$ forms a group if it satisfies for all $a, b, c \in G$:

1, $a \cdot b \in G$ (closure)

2, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity)

3, $\exists e : ea = ae = a$ (identity element)

4, $\forall a \in G \; \exists a^{-1} : aa^{-1} = a^{-1}a = e$ (inverse element)

note: • e & a^{-1} are determined unambiguously

→ let $e_1 \neq e_2$ are identity elements

$\Rightarrow e_1 e_2 = e_1$ & $e_1 e_2 = e_2$ ↯

→ let $b_1 \neq b_2$ are inverse to a:

$\Rightarrow ab_1 = e = ab_2 \quad / a^{-1}. \Rightarrow b_1 = b_2$ ↯

• $(ab)^{-1} = b^{-1}a^{-1}$

Examples

1, $S_n \equiv Sym(n)$ ... permutations of an n-element set

2, $(\mathbb{R} \setminus \{0\}, \cdot)$: $e = 1$, $a^{-1} = \frac{1}{a}$

- disconnected continuous group
- has simply connected subgroup $(\mathbb{R}^+, \cdot)$

3, $(\mathbb{R}, +)$: $e = 0$, $a^{-1} = -a$

- continuous group, connected

4, $GL(n, \mathbb{R}/\mathbb{C})$ ... $\mathbb{R}/\mathbb{C}$ regular $n \times n$ matrices with std. mat. multiplication

important subgroups:
$O(n) \leftrightarrow A^T A = \mathbb{1}$
$SO(n) \leftrightarrow A^T A = \mathbb{1}$ & $\det A = 1$
$U(n) \leftrightarrow A^+ A = \mathbb{1}$
$SU(n) \leftrightarrow$ -"- & $\det A = 1$

5, symmetry group (general concept) [of a system]

- group of transformations with respect to which the system (object) is invariant
- such transfs form a grup: composition of two transformations is again a transformation, $\exists$ inverse transf., ...

5a) Euclidean group – $E(n)$, $ISO(n)$

- isometries of E^n – transf. preserving distances

$$\vec{r}\,' = A\vec{r} + \vec{b} \qquad A \in O(n)$$

5b) point groups – finite subgroups of $E(3)$

- preserve distances + location/position of one point in space
- all finite subgr. of $E(3)$ are point groups!
  (Litzman, page 22, th. 1.3.5)
- describe molec. symmetries

5c) crystalographic groups : 5b + finite translations

- discrete groups ($E(3)$ is continuous)

5d) Lorentz group $O(3,1) \subset$ Poincaré group

P.g: isometries of Minkowski space-time

$$\left.\begin{array}{l}\text{• rotations in space}\\ \text{• boosts (LT without rotations)}\end{array}\right\} O(3,1)$$

- translations in space & time

- cf structure of $E(3)$

Def: Order of the group

For a finite G, the number of elements (cardinality) is called order of the group

notation: $\#G$, $|G|$

- $Sym(n)$, point groups

Infinite groups:

- discrete (countable many elements) - same of 5b
- continuous - connected vs. disconnected

  2-4, 5a, 5d

- Lie groups $\subset$ topological groups

Multiplication table - definition of an abstract finite group

	e	a	b ...
e	ee	ea	eb
a	ae	aa	ab ...
b	be	ba	bb
⋮		⋮	⋱

$\equiv$

e	a	b
a	aa	ab
b	ba	bb

Example: $(\{e,a\},\cdot)$: $a^2 = e$

	e	a
e	e	a
a	a	e

... abstract group

- more "specific" groups with the same MT $\equiv$ same (isomorphic) groups:

1, $(\{1,-1\},\cdot)$

2, $Z_2 = (\{0,1\}, + \bmod 2)$

3, $C_s = \{e,\sigma\} \sim C_i = \{e,i\} \sim C_2 = \{e, C_2\}$

4, $\left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}, \text{matrix mult.}\right) = M_2$

5, $Sym(2) = \left(\left\{\begin{pmatrix}1&2\\1&2\end{pmatrix}, \begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}, \text{composition of perm.}\right)$

Def: Abelian (commutative) group

$$ab = ba \quad \forall a,b \in G$$

- group above is comm.
- in fact, all 2, 3, 4, 5 - elem. groups are abelian
- simplest non-abelian group is of order 6 & is isomorphic to C_{3v} - sym. group of ammonia (NH_3) - see tutorial 1

Theorem 1 (Rearrangement th.)

For any fixed element $h \in G$, the sets $\{hg \,|\, g \in G\}$ and $\{gh \,|\, g \in G\}$ both contain every element of G once and only once.

- g runs over the whole G, h is fixed
- in other words, each row & each col. of MT contain each element of G once & only once (this is not sufficient condition for "legality" of MT!)

Proof:
- let $g' \in G \Rightarrow \exists g = h^{-1}g' \Rightarrow g' = hg \Rightarrow g' \in \{hg \,|\, g \in G\}$
- let $\exists g_1 \neq g_2 : g' = hg_1 = hg_2 \Rightarrow / h^{-1} \cdot / \Rightarrow g_1 = g_2$ ↯

$\Rightarrow g'$ is there only once ☒

SUBGROUPS

Def: A subset H of a group G that is itself a group with the same bin. operation as G is called a subgroup of G.

→ closure, existence of e and a^{-1}

Examples: 1, $SO(2) \subset SO(3)$ ... rotations about one chosen axis
2, $Sym(2) \subset Sym(n > 2)$
3, cyclic subgroup

Def: The order of an element $g \in G$ is the smallest positive integer n such that $g^n = e$.

notes: such number always $\exists$ for every element of a finite group:

- repeatedly multiply g by itself $\Rightarrow$ in a finite group we have to arrive at the same element at one point
- let $g^p = g^q$ & $q < p = q + n \Rightarrow a^{q+n} = a^q \Rightarrow a^n = e$

$\Rightarrow$

Def: $\mathcal{G} = \{e, g, \dots, g^{n-1}\}$ is cyclic (sub)group generated by an element $g \in G$ of order n.

Lemma: Nonempty subset $H \subset G$ is a subgroup of G if and only if

$$gh^{-1} \in H \quad \forall g, h \in H$$

Proof: $\Rightarrow$/ obvious (H subgr. $\Rightarrow \exists h^{-1} \in H$ & closure of H)

$\Leftarrow$/ verify group axioms:

3, identity: $h = g \Rightarrow gg^{-1} = e \in H \quad \forall g \in H$

4, inversion: $g = e \Rightarrow eh^{-1} = h^{-1} \in H \quad \forall h \in H$

1, closure: $h^{-1} \in H \Rightarrow g(h^{-1})^{-1} = gh \in H \quad \forall g, h \in H$

2, associativity is a property of the operation. $\boxtimes$

Theorem 2: Intersection of two subgroups of G is again a subgroup of G.

Proof:
- $H_1, H_2 \subset G$ are subgr. $\Rightarrow e \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 \neq \emptyset$
- $g, h \in H_1 \cap H_2 \Rightarrow$ /they are subgr./ $\Rightarrow h^{-1} \in H_1 \cap H_2$ & $gh^{-1} \in H_1 \cap H_2$

$\Rightarrow$ /lemma/ $\Rightarrow \boxtimes$

LEFT/RIGHT COSETS

Def: Let H be a subgroup of G. Then for any fixed $g \in G$ the set of elements $gH \equiv \{gh | h \in H\}$ is called the left coset with respect to H. Similarly for right coset Hg.

- gH is in general not a subgroup, unless $g \in H$
  $\Rightarrow gH = Hg = H$ ($\Leftarrow$ rearrangement)

Lemma
1, Every $g \in G$ is a member of some left coset.
2, If H is finite of order $\#H$ then gH contains $\#H$ elements
3, Two left cosets with respect to H are either identical or disjoint.
4, $g' \in gH \Rightarrow g'H = gH$

Proof:
1, $g \in G \Rightarrow g = ge \Rightarrow g \in gH$
2, • let $h \neq h'$ & $gh = gh' \Rightarrow / g^{-1} \cdot / \Rightarrow h = h'$ ↯ (rearr.)
   • gH obviously can't contain more than $\#H$ elem.
3, let $gh = g'h'$ is common element of gH & $g'H$
   $(h, h' \in H)$
   $\Rightarrow (g')^{-1} g = h' h^{-1} \in H \Rightarrow$ /rearr./ $\Rightarrow (g')^{-1} g H = H$
   $\Rightarrow / g' \cdot / \Rightarrow gH = g'H$
4) $g' \overset{(1)}{\in} g'H$ & $g' \in gH \overset{(3)}{\Rightarrow} g'H = gH$

$\boxtimes$

Theorem 3 (Lagrange)

If G is a finite group of order $\#G$ and H is its subgroup of order $\#H$ then $\#H$ is a divisor of $\#G$.

Def: Integer $m = \#G/\#H$ is called index of a subgroup.

Proof (Lagrange)

- let m is the number of distinct left cosets with resp. to H

$\overset{(2)}{\Rightarrow}$ each has $\#H$ elements
$\overset{(3)}{\Rightarrow}$ they have no common element

$\Big\} \Rightarrow$ contain $m\#H$ elements

$\overset{(1)}{\Rightarrow}$ every $g \in G$ belongs to same $g'H$ $\Rightarrow \#G = m\#H$

$\boxtimes$

Example: • the only 5-element group is cyclic:

$\Leftarrow$ let there be an element of order $<5 \Rightarrow$ it generates cyclic subgroup of the same order which would divide 5 ↯

Met:

e	a	b	c	d
a	e	c	d	b
b	c	d	a	e
c	d	e	b	a
d	b	a	e	c

• satisfies the rearrangement th.

• contains $\{e, a\}$ subgroup

$\Rightarrow$?

$(ab)c = cc = b \neq a(bc) = aa = e$

$\Rightarrow$ it's not a group!

CONJUGACY CLASSES

Def: An element $g' \in G$ is said to be conjugate to $g \in G$ if $\exists h \in G: g' = hgh^{-1}$

note: conjugation is an equivalence relation (reflexivity $a \sim a$, symmetry $a \sim b \Rightarrow b \sim a$; transitivity $a \sim b$ & $b \sim c \Rightarrow a \sim c$)