Group theory - basic concepts

Def: A group is a set G with binary operation $\circ$
1 satisfying group axioms:

1) G is closed under $\circ$, i.e. $a \circ b \in G$ for all $a, b \in G$
2) associative property: for all $a, b, c \in G$: $(a \circ b) \circ c = a \circ (b \circ c)$
3) identity : there exists $e \in G$: $e \circ a = a \circ e = a$ for all $a \in G$
4) inverse element : for all $a \in G$ exists $a^{-1} \in G$: $a^{-1} \circ a = a \circ a^{-1} = e$

- the binary or group operation can be addition, multiplication, composition of mappings etc., often not denoted at all : ab

- the identity e and the inverse element a^{-1} are unique:
  Proof by contradiction: 1) if e_1 and e_2 are two different identities then $e_1 \cdot e_2 = e_1$ and also $e_1 \cdot e_2 = e_2$. Thus $e_1 = e_2$ (contradiction)
  2) if b_1 and b_2 are two inverse elements to a, then $b_1 \cdot a = e = b_2 a$. Thus $b_1 = b_2$ (again contradiction)

- clearly $(a^{-1})^{-1} = a$ and $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ as $(a \cdot b)(a \cdot b)^{-1} = a \cdot b \cdot b^{-1} \cdot a^{-1} = e$

- note: the group axioms can be relaxed, for example to have only left identity $(e \cdot a = a)$ etc., but we used ~~the~~ standard definition

- order of the group = number of elements in the group, $\#G$ or $|G|$
  - it can be finite or infinite
  - infinite groups can be discrete, e.g. crystallographic or continuous - all Lie groups or with several continuous (connected) components (e.g. $O(3)$ has two separate parts - one consists of proper rotations, the other of improper rotations)

- we talk about an abstract group (given by relations among elements) (also called presentation) and its realizations (all have the same structure as a group, they are „isomorphic", but consists of elements of different nature, e.g. rotations or matrices or operators)

Def: A group isomorphism is a bijection between two groups,
2 satisfying the condition: if we have $\varphi : G_1 \xrightarrow{\text{onto}} G_2$

and $\varphi : a_1 \mapsto a_2$
$\varphi : b_1 \mapsto b_2$ then $\varphi : a_1 b_1 \mapsto a_2 b_2$

or $\varphi(a_1 b_1) = \varphi(a_1)\varphi(b_1)$, i.e. the structure of both groups is the same

- we say that such two groups are isomorphic, $G_1 \sim G_2$

Examples: The simplest finite group (besides the trivial one $\{e\}$)
1 is a two-element group $\{e, a\}$ with $a^2 = a \cdot a = e$

- it is given by this multiplication table:

	e	a
e	e·e	e·a
a	a·e	a·a

or

	e	a
e	e	a
a	a	e

or simply

e	a
a	$e = a^2$

- this abstract group has many realizations, all isomorphic

1) $G = (\{1, -1\}, \cdot)$ - a group of multiplications of 1 and -1, $e = 1$
2) $\mathbb{Z}_2 = (\{0, 1\}, + \bmod 2)$ - $1 + 1 \bmod 2 = 0$, $e = 0$
3) $S_2 = \left(\left\{\underbrace{\begin{pmatrix}1&2\\1&2\end{pmatrix}}_{e}, \underbrace{\begin{pmatrix}1&2\\2&1\end{pmatrix}}_{\text{transposition}}\right\}, \circ\right)$ - a group of permutations of two elements with composition of permutations as group operation
4) several point groups with the composition of transformations
$C_s = \{E, \sigma\}$ $(= m)$ - identity and reflection
$C_i = \{E, i\}$ $(= \bar{1})$ - identity and inverse
$C_2 = \{E, C_2\}$ $(= 2)$ - identity and rotation by 180°
(more on point groups later in the first tutorial)
5) groups of matrices with standard matrix multiplication
e.g. $M_1 = \left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}, \cdot\right)$ or $M_2 = \left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}, \cdot\right)$
inverze in the plane — reflection in the plane by $x = y$
6) parity (inversion in space), time reverse etc.

Def. ③ A group G is <u>commutative</u> (or abelian) if for all $a,b \in G$: $ab = ba$

- all <u>cyclic groups</u> given by $a^n = e$ with n elements are commutative, $G = \{e, a, a^2, \dots, a^{n-1}\}$ has $\#G = n$ different elements
  e.g. it is realised as a group of rotations "generated" by C_n = rotation by the angle $\varphi = \frac{2\pi}{n}$, thus C_n^2 is rotation by 2φ etc. and C_n^n by $n\varphi = 2\pi$ (identity)

<u>Rearrangement theorem</u> (RT later for short)

① For any fixed $g \in G$, two sets

$$L_g(G) = \{ g \cdot h \mid h \in G \} = \text{left multiplication of } G \text{ by } g$$
and $$R_g(G) = \{ h \cdot g \mid h \in G \} = \text{right multiplication of } G \text{ by } g$$

contain all elements of G and each element only once.

<u>Proof:</u> 1) every element of G is in $L_g(G)$ and also in $R_g(G)$:
consider <u>any</u> $h' \in G$ and multiply it by g^{-1} from the left,
<u>then</u> $g^{-1}h' = h \in G$ is a certain element of G and
$gh = g(g^{-1}h') = h' \in L_g(G)$ as gh belongs to $L_g(G)$
(in a similar way $h' \in R_g(G)$, from $h'g^{-1} = h$)

2) uniqueness of elements in $L_g(G)$ and $R_g(G)$:
consider two different $h_1 \neq h_2$ from G giving the same element of $L_g(G)$, then $gh_1 = gh_2$, but by multiplying this equation by g^{-1} from the left, we get $h_1 = h_2$ which is contradiction

- the second part is important in the case of infinite groups
- it follows that the <u>multiplication table</u> of any <u>finite group</u> must have all elements of the group in each row and column, only permutated, i.e. there cannot be the same elements in any row or column
- warning: this is not a sufficient condition for a table to define a group (see a counter example later for $\#G = 5$)

Examples: (2) 1) a group with three elements

- there is just one group with 3 elements - the cyclic group given by

$$a^3 = e \iff$$

e	a	b
a	b	e
b	e	a

here, e or a cannot be placed

$\sim C_3 = \{E, C_3, C_3^2\}$ - rotations by $\pm \frac{2\pi}{3} = \pm 120°$

2) two diffent groups with 4 elements

the cyclic group $a^4 = e$

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

$\sim C_4 = \{E, C_4, \underset{\overset{\|}{C_4^2}}{C_2}, C_4^3\}$

- rotations by multiples of 90°

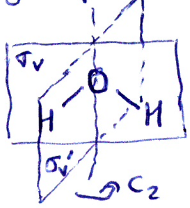
Klein four-group (abelian)

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

$\iff$ $a^2 = e$, $b^2 = e$, $c^2 = (ab)^2 = e$

$\sim C_{2v} = \{E, C_2, \sigma_v, \sigma_v'\}$

= symmetry group for H_2O



but also

$\sim D_2 \sim C_{2h}$

(see tutorial on point groups)

3) there is only one group with 5 elements - the cyclic group

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

$\iff a^5 = e$

$\sim C_5$

note that this „multiplication" table is not a group

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

because

$(ab)d = cd = a$

but $a(bd) = ac = d$ $\not\Rightarrow$

(associative property is not fulfilled)

Note: we could continue like this but we will see some examples later (as C_{3v} - the first non-abelian group with 6 elements)

let us just say that there is always just one group if $\#G$ is a prime number

and that mathematicians completed the classification of finite simple groups (with no nontrivial normal subgroup - see below)

(the proof is several thousand pages long and these groups include 27 sporadic groups (not in any sequence of groups) including Monster group of order $\approx 10^{53}$

Subgroups

Def: A subgroup H of a group G (denoted as $H \leq G$) is a subset
4 of G that forms a group itself with the same group operation.

Examples: 1) the cyclic group C_4 has two trivial ($\{E\}$ and itself)
3 and one non-trivial subgroup $\{E, C_2\}$

2) Klein four-group (C_{2v}) has 3 non-trivial subgroups
$\{E, C_2\}$, $\{E, \sigma_v\}$ and $\{E, \sigma_v'\}$
but for example $\{E, \sigma_v, \sigma_v'\}$ is not a subgroup: $\sigma_v \sigma_v' = C_2$

Theorem: A non-empty subset H of G is a subgroup of G,
2 if and only if (iff) $g \cdot h^{-1} \in H$ for all $g, h \in H$.

Proof: $\Rightarrow$ obvious (as $h^{-1} \in H \Rightarrow gh^{-1} \in H$)

$\Leftarrow$ let us show that H satisfies the axioms of the group

1) if $g \in H$ then $g \cdot g^{-1} = e \in H$ (identity)

2) take $g = e \in H$, then $e \cdot h^{-1} \in H$, that is $h^{-1} \in H$ for all $h \in H$ (inverse el.)

3) we know $h^{-1} \in H \Rightarrow g(h^{-1})^{-1} = gh \in H$ for all $g, h \in H$
(H is closed under the group operation)

- associative property follows immediately from G

Theorem: An intersection of two subgroups H_1 and H_2 of G
3 is also a subgroup of G.

Proof: It follows from the previous theorem. If $H_1 \leq G$ and $H_2 \leq G$ then $e \in H_1 \cap H_2$ (i.e. it is a non-empty subset) and if g and $h \in H_1 \cap H_2$ then $gh^{-1} \in H_1 \cap H_2$
(as H_1 and H_2 are subgroups)

Theorem: For every element g of a finite group G,
4 there exists $n \in \mathbb{N}$ such that $g^n = e$ (order of the element)

Proof: In any finite group, there must exist $p > q$ such that $g^p = g^q$. If we set $p = q + n$, then $g^p = g^q \cdot g^n = g^q \Rightarrow g^n = e$.

Generators of groups and subgroups

- if $g \in G$ is of order n, then $\{e, g, g^2, \dots, g^{n-1}\}$ forms a subgroup of G generated by g that is cyclic
- in general, we can generate subgroups of G from more elements $g_1, \dots, g_m \in G$ if we take all their products and also products of their inverse elements and with them (note that for finite groups, it would be enough to consider only products of the elements, not their inverses, as for $g_i^n = e$ we set $g_i^{-1} = g_i^{n-1}$ but for infinite groups it is important to include inverse elements)

Theorem 5: For any subset $X \subset G$, there exists the smallest subgroup of G containing X. Its elements consist of all finite products of elements from X and their inverses.

Proof: Let $H_i \leq G$ be all subgroups containing X, i.e. $X \subset H_i$ for all i, then $S = \bigcap_i H_i \leq G$ (see Theorem 3) that is clearly the smallest subgroup containing X.

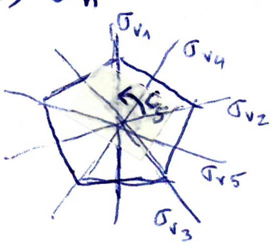
- we use $S = \langle X \rangle$ for a subgroup generated by X
- if $\langle X \rangle = G$, we say that X generates G
- the smallest subset of elements that generate the whole group is called generators of the group (useful concept, for example, for finding matrix representations for all elements if we know representations for generators)

(**Note**: generators of Lie groups will be elements of its Lie algebra not elements of the group itself)

Examples:

1) $\langle \emptyset \rangle = \{e\}$
2) $\langle g \rangle = \{e, g, \dots g^{n-1}\}$

3) $D_n = \langle \{C_n, \sigma_{v1}\} \rangle$ – the group of symmetries of the regular polygon with n sides



- the whole group is defined by relations

$$C_n^n = E \Rightarrow C_n^{-1} = C_n^{n-1}$$
$$\sigma_{v1}^2 = E \Rightarrow \sigma_{v1}^{-1} = \sigma_{v1}$$
$$\sigma_{v1} C_n \sigma_{v1} = C_n^{-1} \Rightarrow \sigma_{v1} C_n = C_n^{n-1} \sigma_{v1}$$
$$\sigma_{v1} C_n^2 = C_n^{n-1} \sigma_{v1} C_n = C_n^{n-2} \sigma_{v1} \text{ etc.}$$

or abstractly

$$D_n = \langle \{r, s\} \mid r^n = s^2 = e, \; srs = r^{-1} \rangle$$

this is called presentation of D_n

Left and right cosets

Def: (5) Let H be a subgroup of G ($H \leq G$). Then a set of all products $g \cdot H = \{gh \mid h \in H\}$ is called a left coset of G and similarly $H \cdot g = \{hg \mid h \in H\}$ is a right coset

Theorem: (6) Two left (or right) cosets $g_1 H$ and $g_2 H$ for a subgroup H are either the same, or disjoint sets (they have no common element)

Proof: $g_1 H$ and $g_2 H$ are either disjoint or they have at least one common element, but then

$g_1 h_k = g_2 h_e$ for certain h_k and h_e from H

and thus $g_2^{-1} g_1 = h_e h_k^{-1} \in H$ and $g_2^{-1} g_1 H = H$

and by Theorem (1) (Rearr. t.) $g_1 H = g_2 H$

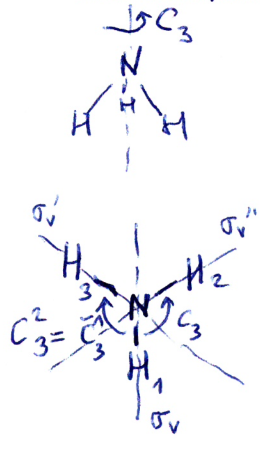
- each element g of G belongs to one coset, specifically gH and Hg
- if $g' \in gH$ then $g'H = gH$ as they have at least one common element g'
- if H is a finite subgroup then $\#(g \cdot H) = \#H$ and thus it follows

Lagrange's theorem: (7) If G is a finite group of order $\#G$ and H is subgroup of order $\#H$ then $\#H$ divides $\#G$

and $m = \dfrac{\#G}{\#H}$ is called the index $[G:H]$ of H in G

Corollary: The order of an element divides $\#G$ and thus all groups of prime order are necessarily cyclic.

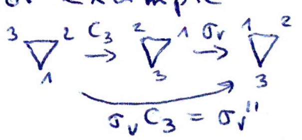
Example: C_{3v} - the only group with 6 elements besides the cyclic group C_6



$\underbrace{E \quad C_3 \quad C_3^2}_{C_3 \text{ subgroup}}$

E	C_3	C_3^2	σ_v	σ_v'	σ_v''
C_3	C_3^2	E	σ_v'	σ_v''	σ_v
C_3^2	E	C_3	σ_v''	σ_v	σ_v'
σ_v	σ_v''	σ_v'	E	C_3^2	C_3
σ_v'	σ_v	σ_v''	C_3	E	C_3^2
σ_v''	σ_v'	σ_v	C_3^2	C_3	E

for example



etc.

left cosets for $C_3 \leq C_{3v}$:

$\sigma_v C_3 = \{\sigma_v, \sigma_v'', \sigma_v''\} = \sigma_v' C_3 = \sigma_v'' C_3$

and for $C_s \sim \{E, \sigma_v\} \leq C_{3v}$:

$C_3 C_s = \{C_3, \sigma_v'\}$, $C_3^2 C_s = \{C_3^2, \sigma_v''\}$