GROUPS

OPERATION:

"Generalization" of the idea of sum, or product

DEF] Given a set A, every function $*: A \times A \longrightarrow A$ is called BINARY OPERATION on A.

(Usually we sign $*(a,b)$ as $a * b$
$+(a,b)$ $a+b$)

Example] (1) [redacted] $+: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
$(a,b) \longmapsto a+b$ is ~~an~~ operation on $\mathbb{Z}$

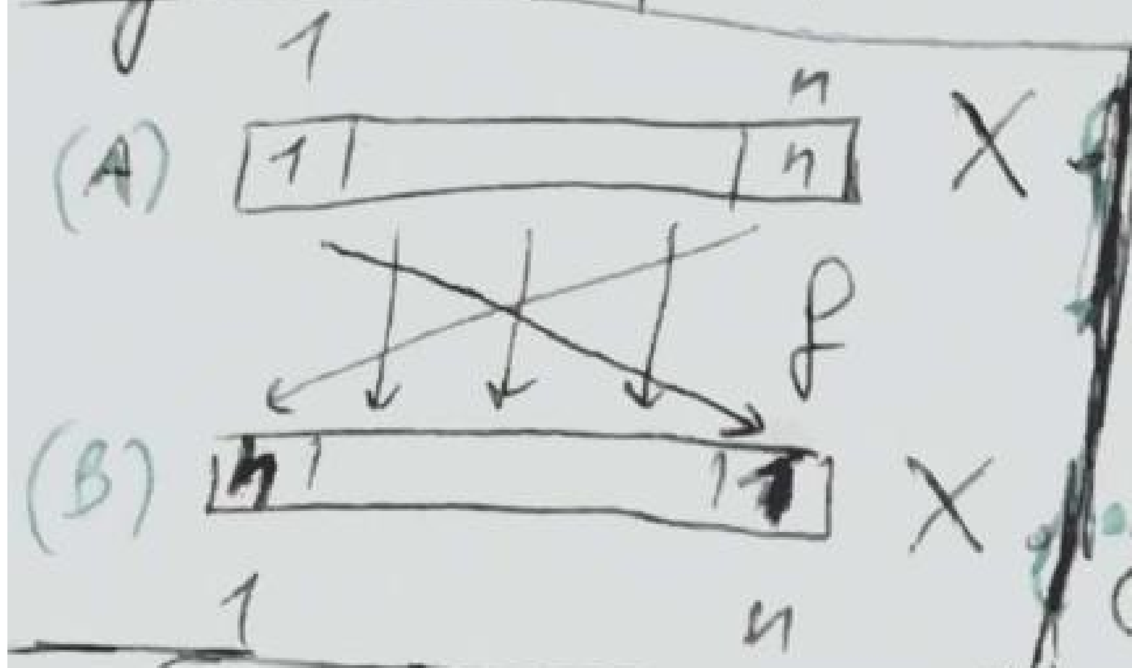
[$\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$

(2) Permutation Group, or Symmetric Group

Let's take $X_n = \{1, \text{—}, n\}$. We imagine it as the position of n people in a row:

We can define $S_n = \{f: X_n \to X_n \mid f \text{ is bijective}\}$.
The elements of S_n are called PERMUTATIONS and can be seen as the change of positions

of the people in the row: 1

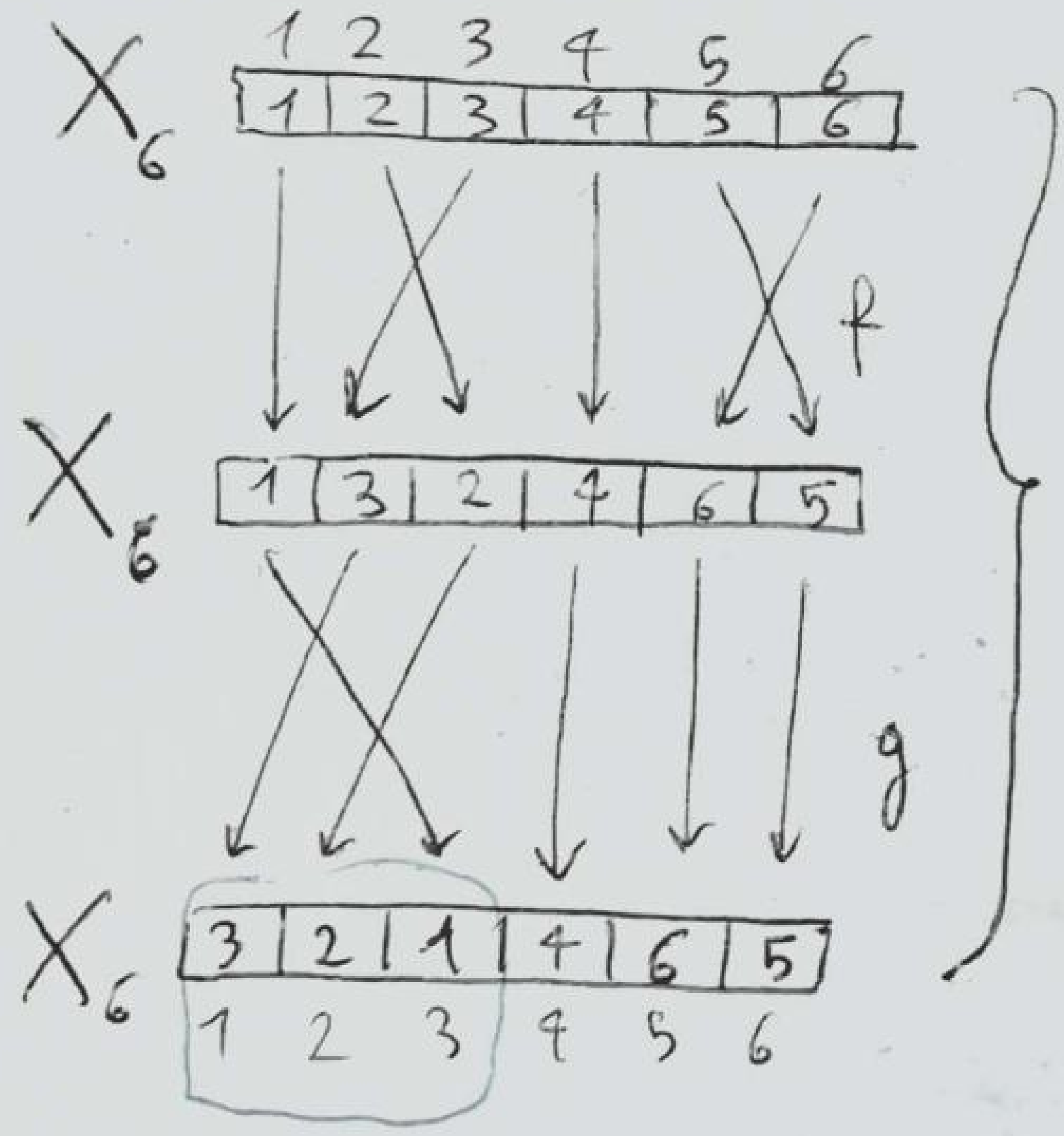


- f is surjective: every person from row (B) was a person in row (A)
- f is injective: 2 people from row (A) cannot ~~finish~~ end up in the same place in row (B)

Functions can be composed. (Fig 2)

If f, g are bijective, $f \circ g$ is bijective (Trust me).

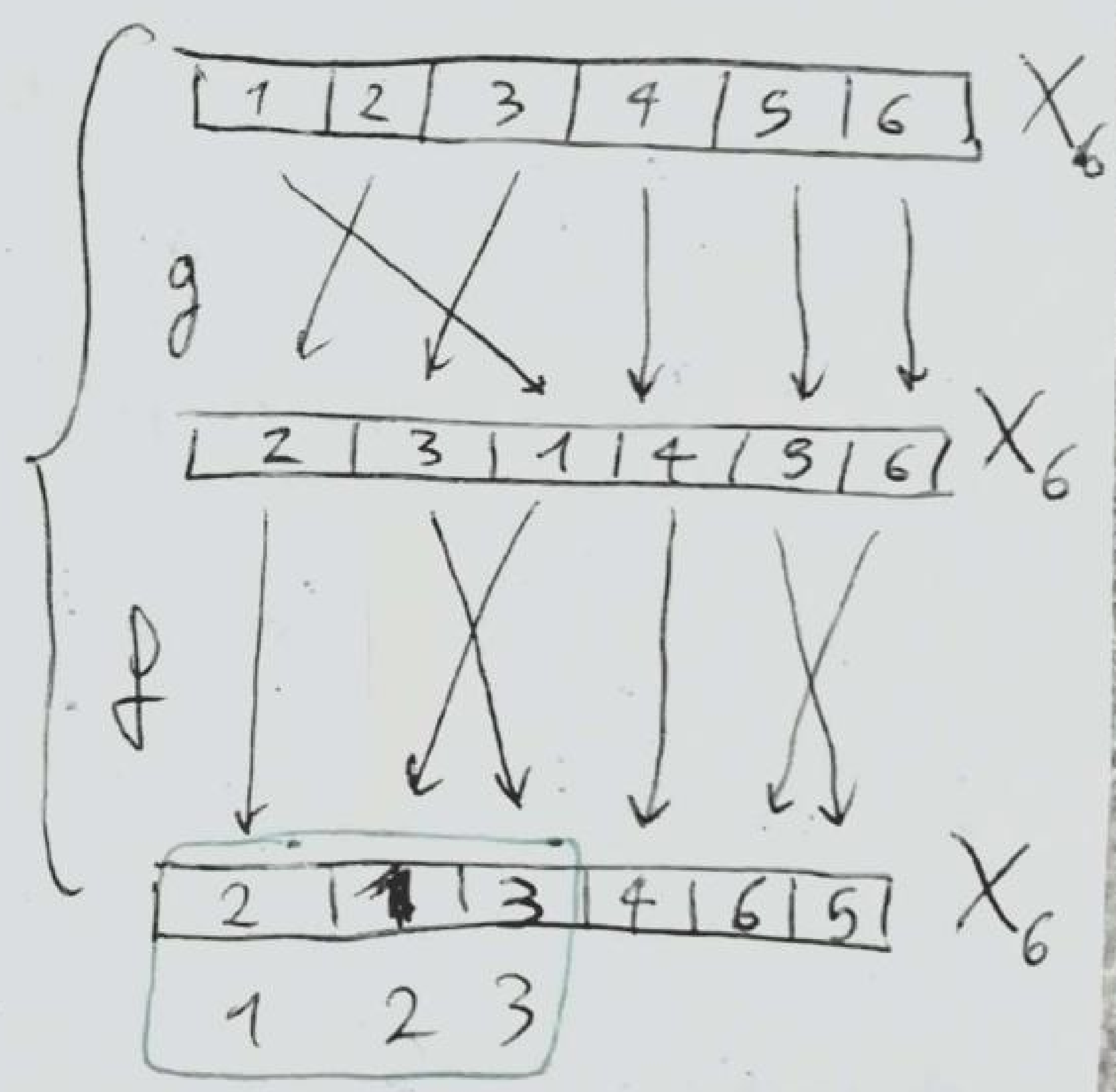
It means, if $f, g: X \longrightarrow X$ are bijective, $f \circ g : X \longrightarrow X$ is bijective.



$g \circ f \neq f \circ g$

↑

NOT COMMUTATIVE



So $\circ$ is an operation on S_n!

We want to study "beautiful" operation.

Example: Given a set A, $f: A \times A \longrightarrow A$, $(a,b) \longmapsto a$ is an operation.

Ex: $3 * 4 = 3$, $4 * 3 = 4$, $7 * 3 = 7$

We call this the SHIT OPERATION.

~~We der~~ We will not study operation like the shit operation.

DEF Given G, set, and $*$, operation on G, we say $(G;*)$ is a group if:

(1) $*$ is associative: $\boxed{(a*b)*c = a*(b*c)}$ for every $a,b,c \in G$

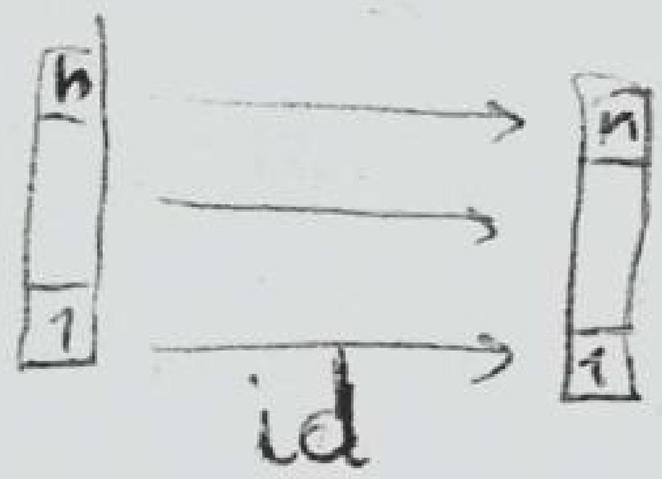
[not associative operation? Octanions] [$*(*(a,b);c) = *(a;*(b,c))$]

(2) $*$ has an element identity e:

for every a $\boxed{a*e = e*a = a}$

[Example: in S_n e is the "identity function

in the drawing:

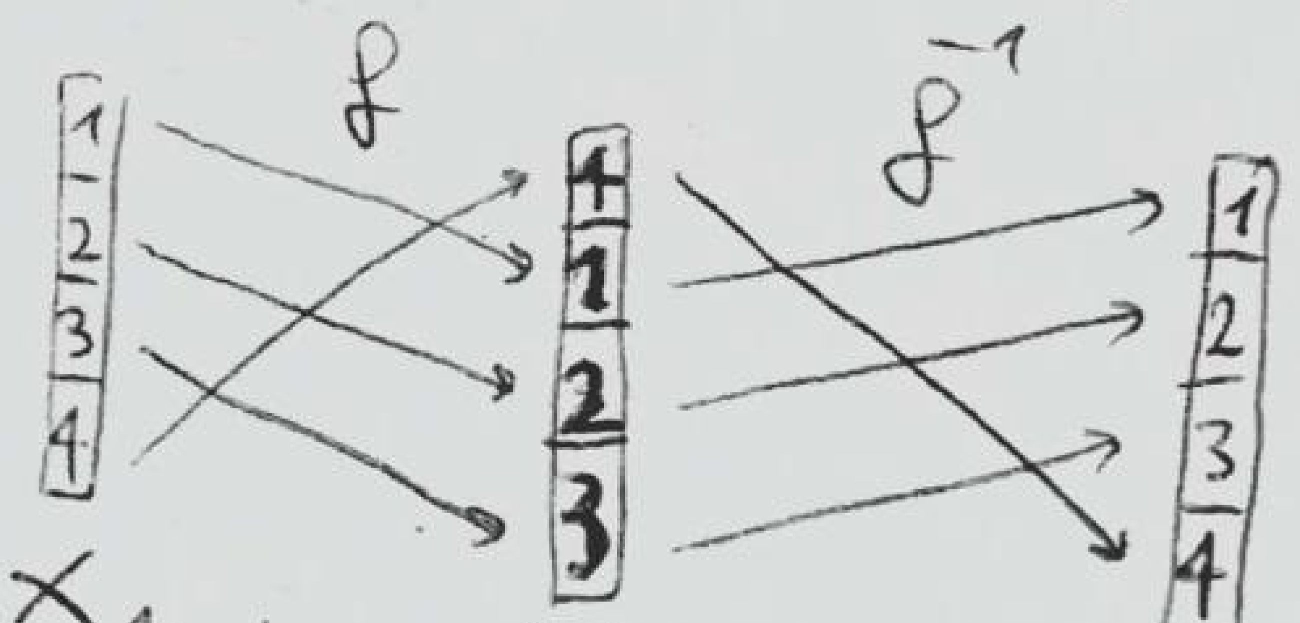

]

(3) for every a exists its inverse a^{-1}:

just notation (no real power)

$\boxed{a*a^{-1} = a^{-1}*a = e}$

[In S_n the inverse of f the inverse function f^{-1}


]

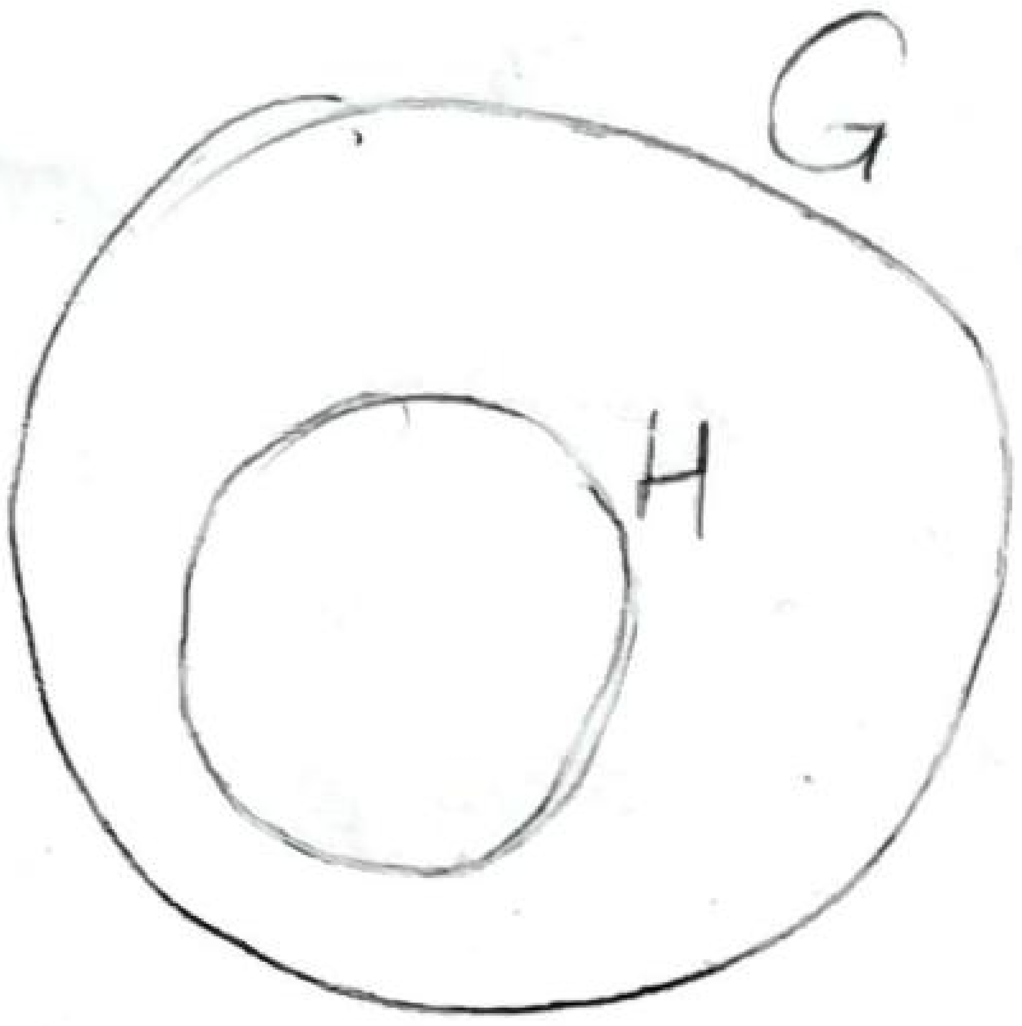
Ex • $(S_n;\circ)$ is a group (not commutative)

• $(A$; the shit operation$)$ is not a group (no identity)

$a*b=a$ but $b*a=b$ for every b. So no identity from the left

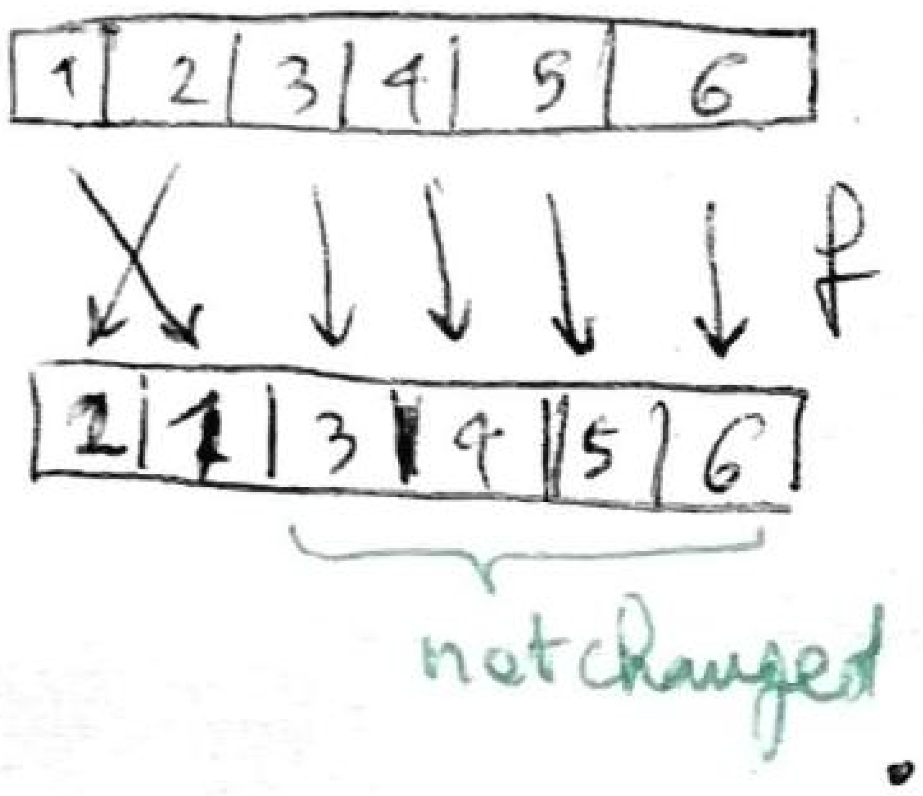
• $(\mathbb{Z};+)$ is a group:

$$a+(b+c) = (a+b)+c$$
$$a+0 = 0+a = a$$
$$a+(-a) = (-a)+a = 0$$



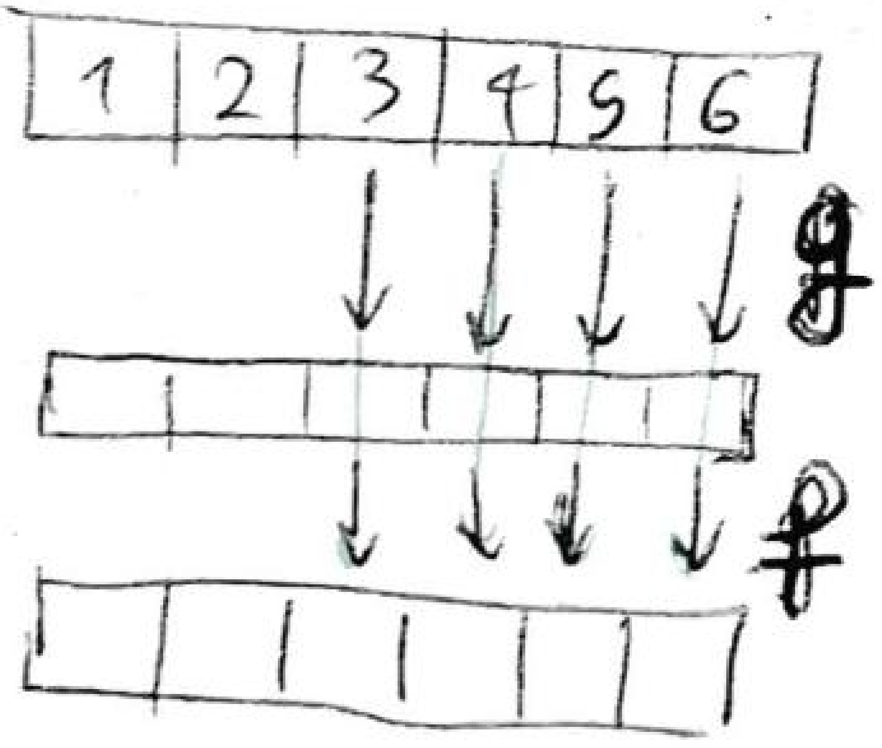
Def] Given $(G,+)$ group, and $H \subseteq G$ subset of G, we say that <u>H is a SUBGROUP OF G</u> if $(H,+)$ is a group.

Examples] • Let's take $S_6 (=G)$. S_6 is our group



We define $H=\{f\in S_6 \mid f(3)=3,\ f(4)=4,\ f(5)=5,\ f(6)=6\}$

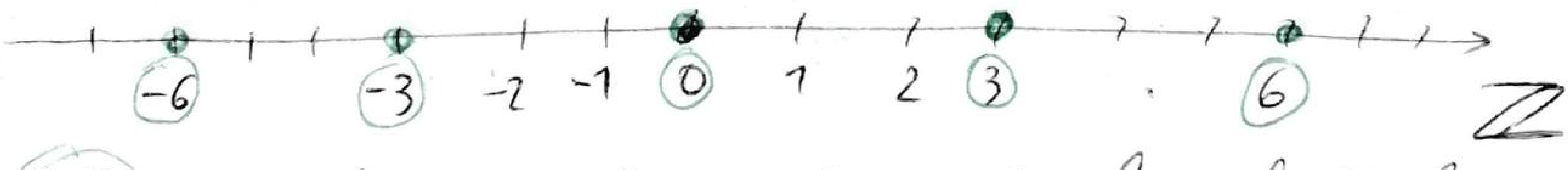
• If $f,g\in H$, $f\circ g$ will always be inside H, as we can see in the drawing.



Besides, if $f\in H$, f^{-1} will not change 3, 4, 5, 6, so $f^{-1}\in H$.

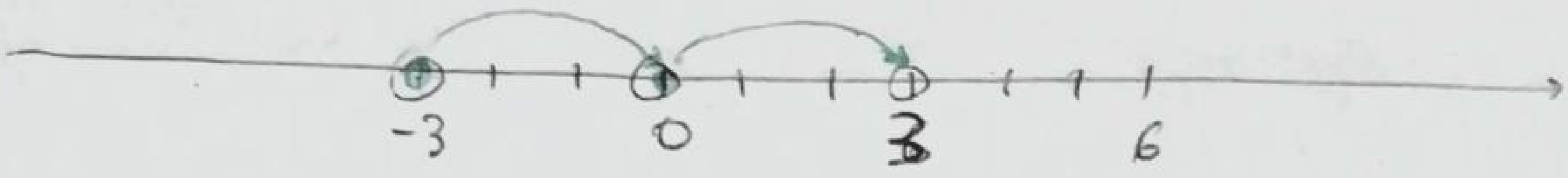
So $(H,\circ)$ is a subgroup of S_6

• Let's take $\mathbb{Z}$. We define $3\mathbb{Z}=\{3n \mid n\in\mathbb{Z}\}$



$3\mathbb{Z}$ is the set of all the multiple of 3 (negative and positive). We see:

(2.A) $3n+3m = 3(n+m) \Rightarrow [h_1, h_2 \in 3\mathbb{Z} \Rightarrow$
$\Rightarrow h_1 + h_2 \in 3\mathbb{Z}]$



So $+$ is an operation on $3\mathbb{Z}$.
¿But does $3\mathbb{Z}$ is a group with $+$?
So does $+$ respect the 3 condition of group?

(2.B) $(a+b)+c = a+(b+c)$ (ASSOCIATIVITY)
because ~~this~~ law is valid for every $a,b,c \in \mathbb{Z} \Rightarrow$
$\Rightarrow$ is valid for every $\underset{\overset{\cup}{\mathbb{Z}}}{}$ $a,b,c \in 3\mathbb{Z}$

(2.C) $0 \in 3\mathbb{Z}$ in fact $3 \cdot \underset{\overset{\cup}{\mathbb{Z}}}{0} = 0$ (identity)

(2.D) if $3n \in 3\mathbb{Z}$, $-3n = 3(\underset{\overset{\cap}{\mathbb{Z}}}{-n}) \in 3\mathbb{Z}$ (inverse)
$\Rightarrow 3n + 3(-n) = 0$

So $(3\mathbb{Z}; +)$ is subgroup of $(\mathbb{Z}; +)$!

Ex. 3] Given $(G; +)$ group, $(\{e\}; +)$ is always a subgroup, called the trivial group.

Applications of Groups:

(1) Chemistry: symmetries of molecule
(2) Cryptography: (Galois Theory) A.E.S., R.S.A.
(3) Image processing in informatics
(4) Music Theory: everywhere
(5) Physics, symmetries
(6) ALL OVER MATHEMATICS

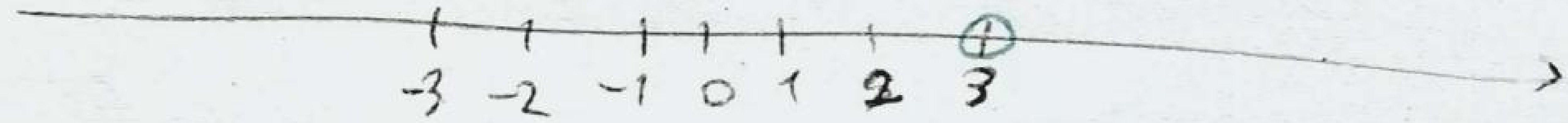
GENERATORS

DEF] Given $(G;+)$ group, ~~and $g_1, \ldots, g_n \in G$~~ and $g \in G$, we call $H = \langle g \rangle$ the smallest subgroup of G that contains $g, -g$.

[**Practically:** $\langle g \rangle$ is made by all the possible elements we can obtain summing g and $-g$]

You didn't understand? Let's see an example

Ex] Let's take $(\mathbb{Z};+)$. Let's take 3.



$\langle 3 \rangle$ is the smallest subgroup of $(\mathbb{Z};+)$ that contains $3, -3$. Is composed by:

$$\underbrace{3+3+3+\ldots+3}_{n \text{ times}} + \underbrace{(-3)+(-3)+\ldots+(-3)}_{m \text{ times}} =$$

$$= n \cdot 3 + m \cdot (-3)$$

$$= (n-m) \cdot 3$$

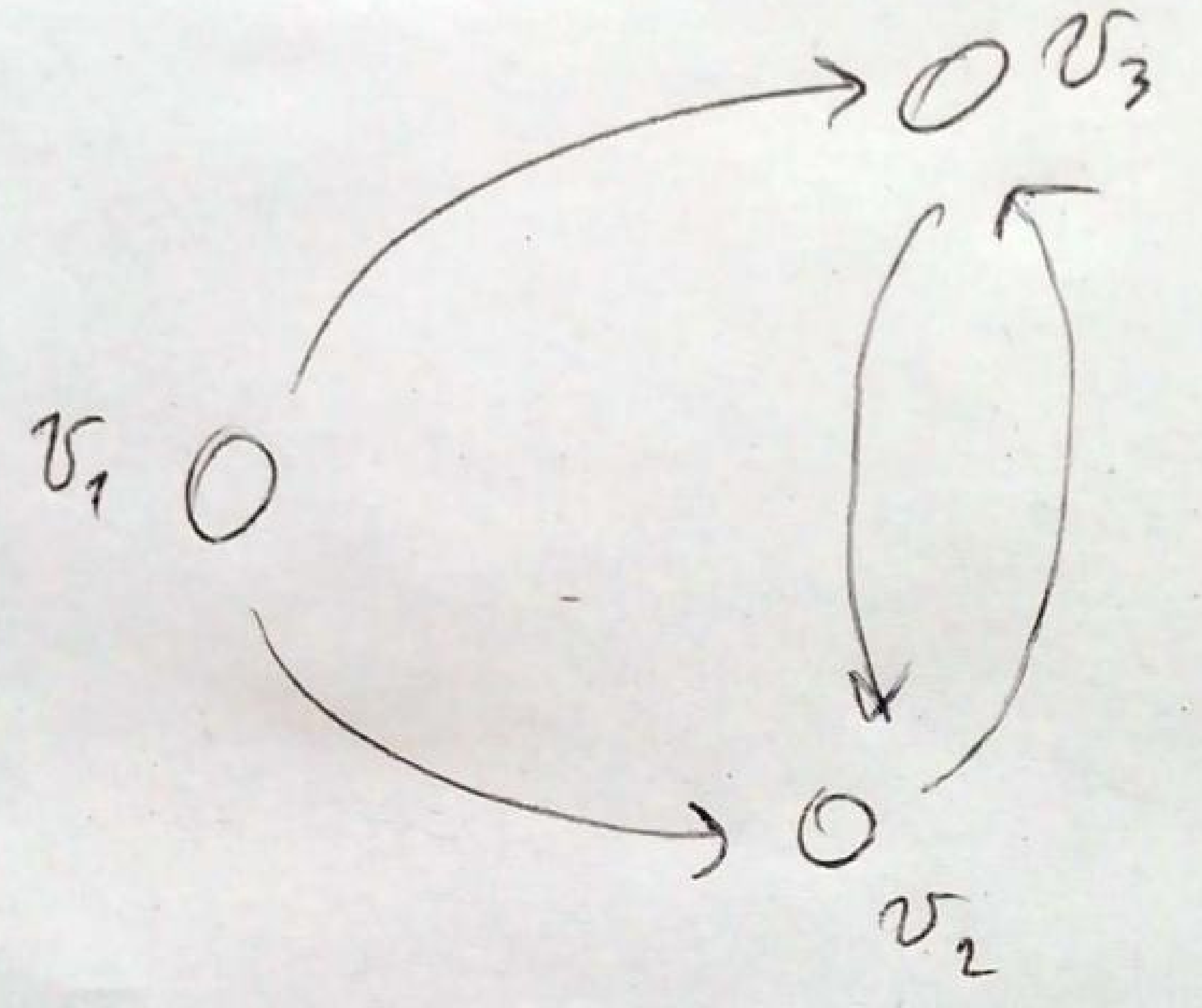
We could ~~easily~~ find out that

$\langle 3 \rangle = 3\mathbb{Z}$

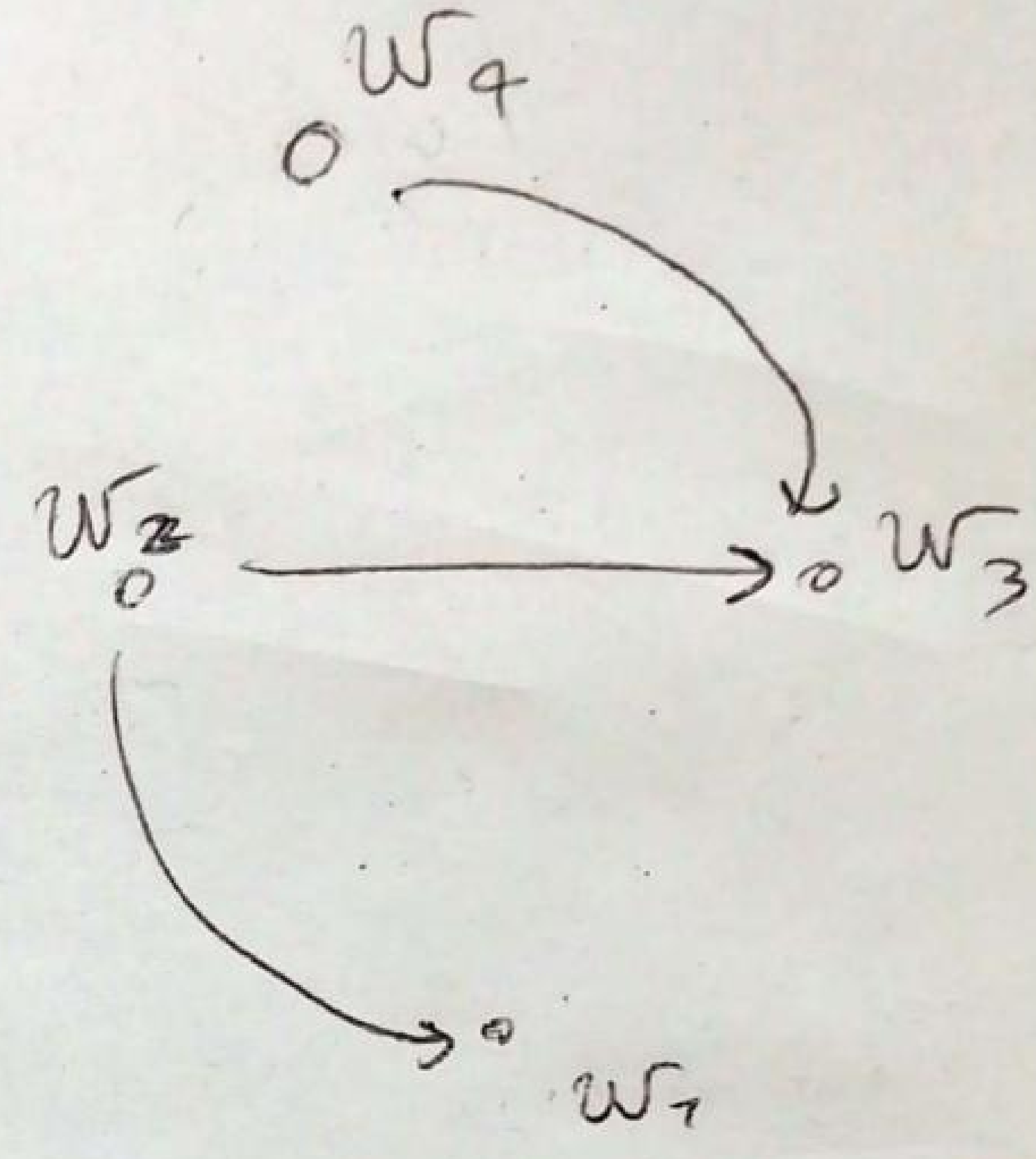
I'm not gonna demonstrate that

GRAPHS

Graphs are basically little drawings of balls and arrows:



G_1



G_2

G_2

<u>formally</u>: $G=(V,E)$, where V are the "balls", <u>vertexes</u>, and E are the arrows, usually called <u>EDGES</u>.

$E \subseteq V \times V$, so ~~for~~ example in G_1:

$G_1 = (V, E_1)$, where $V = \{v_1, v_2, v_3\}$

$E = \{(v_1, v_2), (v_1, v_3), (v_3, v_2), (v_2, v_3)\}$

So an element $(v_i, v_j) \in E$ tells us that exists an arrow from v_i to v_j.

~~Dimen~~ Lenght and dimensions don't count here.

Search on google:
- Schreier graph
- Social graph

(7)

TREES:

Informally a tree is a graph of this type (fig 1 or Fig 2). The top is called the ROOT.

fig. 1

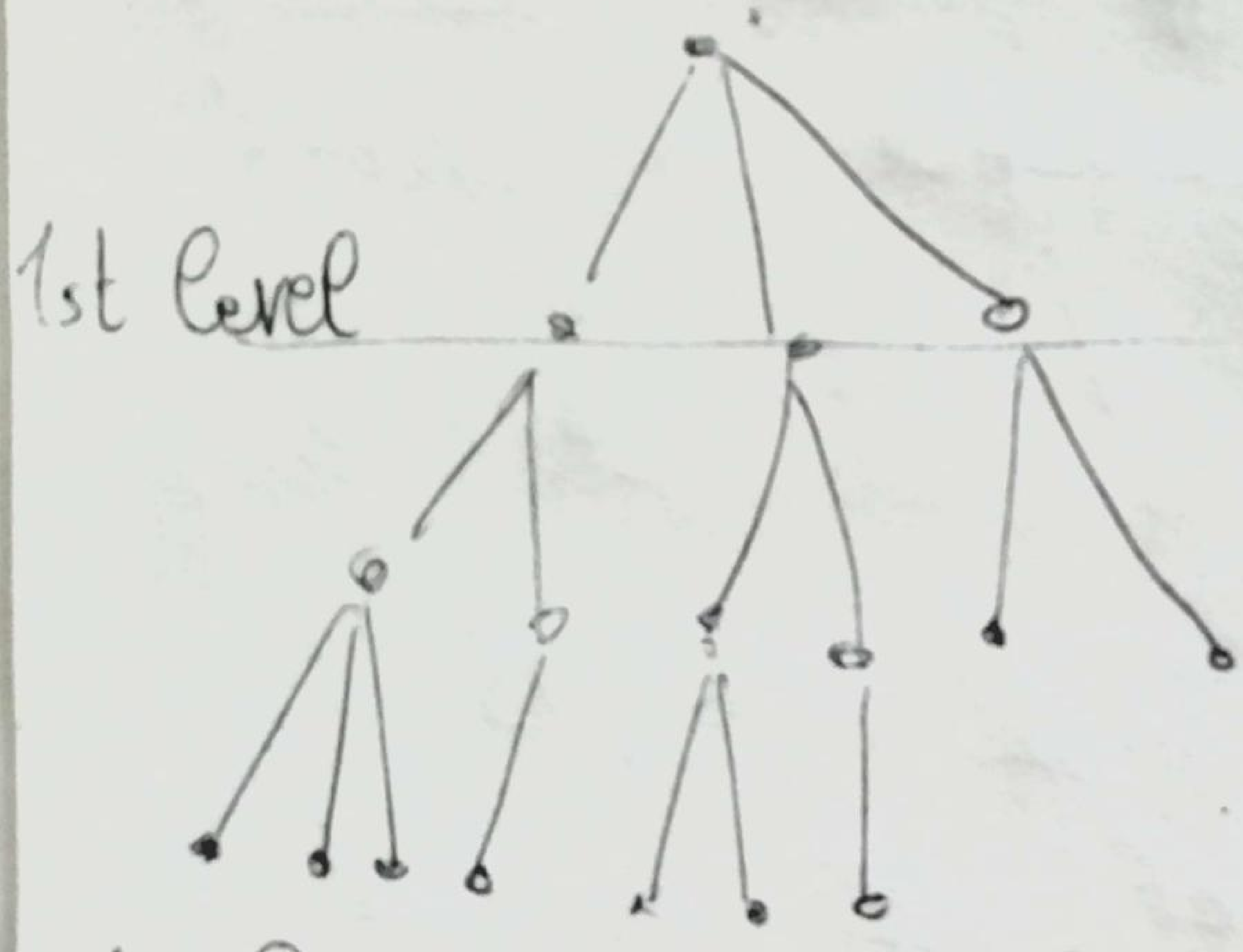
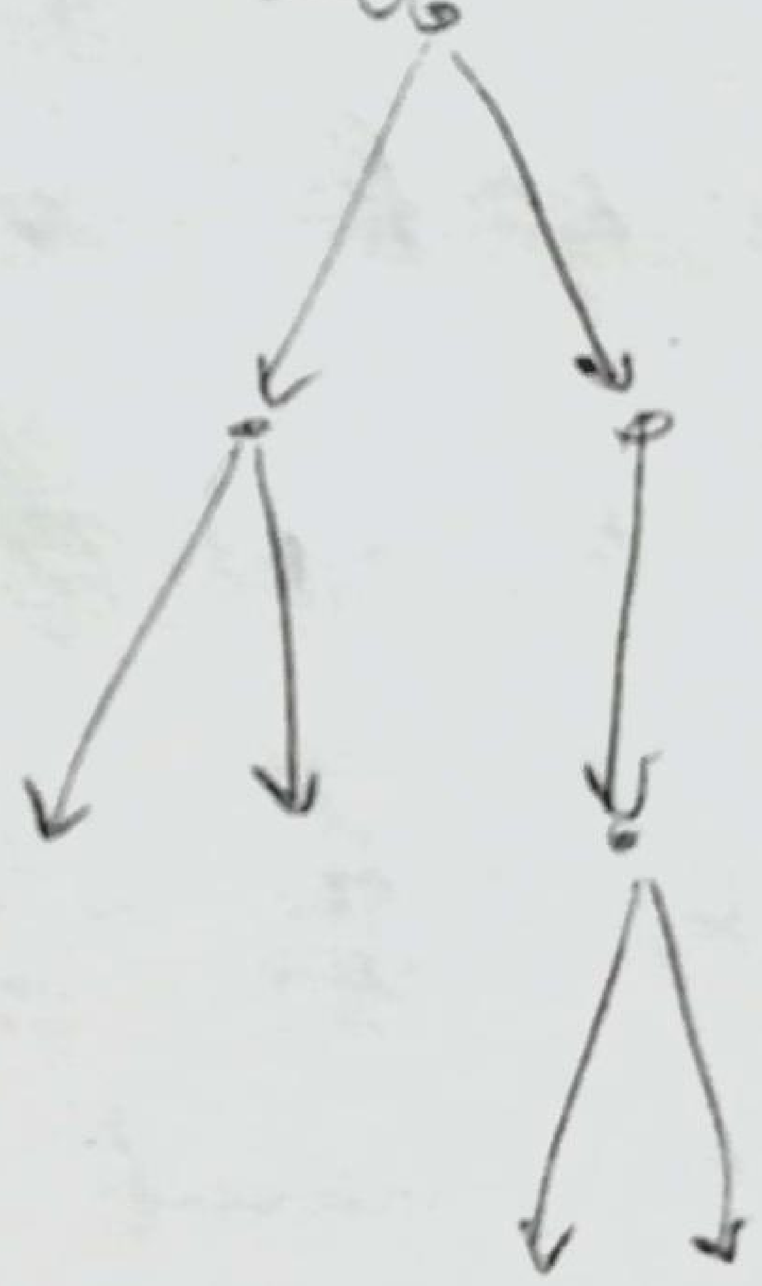


Fig. 2



Applications of Graph: (1) Modelling relations in a group of people (facebook, Insta etc...)

(2) Linguistics

Search images online