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 $a*b$
$+(a,b)$ $\quad a+b$)

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

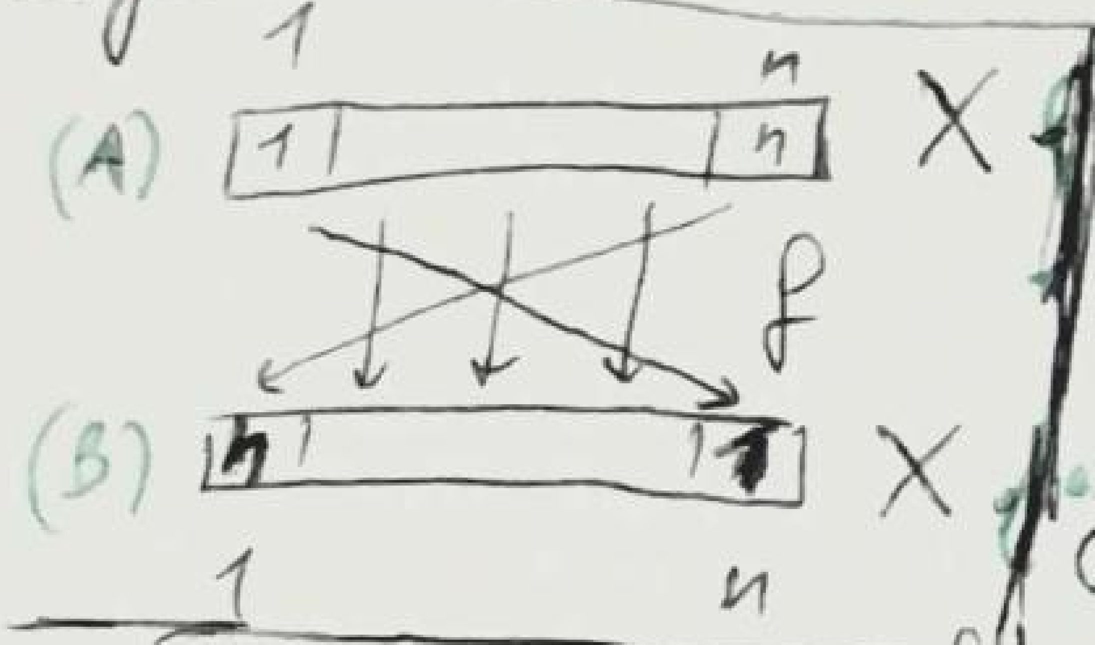
[$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

(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:



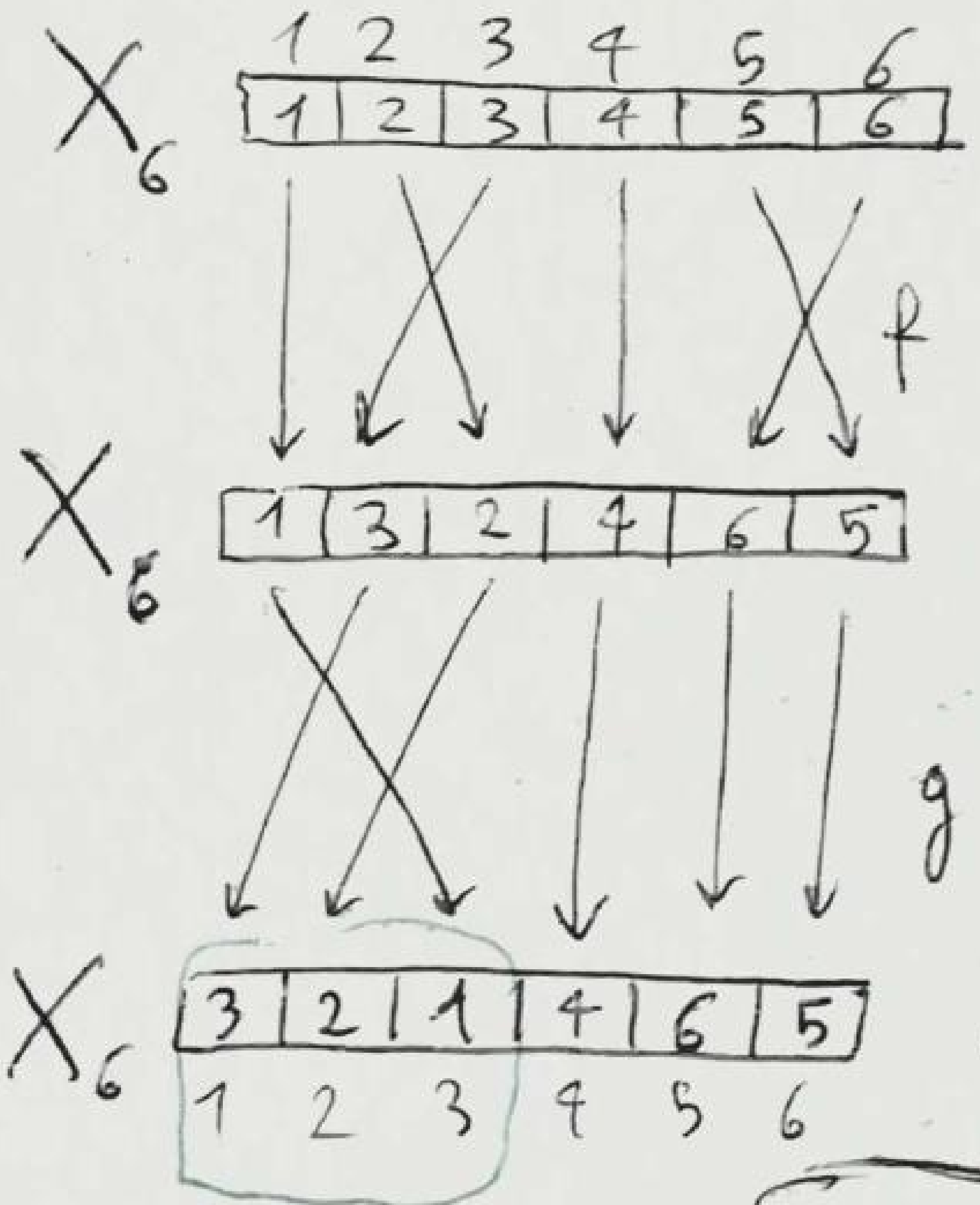
f is surjective: every person from row (B) was a person in row (A)
f is injective: 2 people from row (A) cannot ~~finish~~ end up in the same place in row (B)

Functions can be composed. (Fig 2)

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

It means, if $f, g : X_n \longrightarrow X_n$ are bijective,

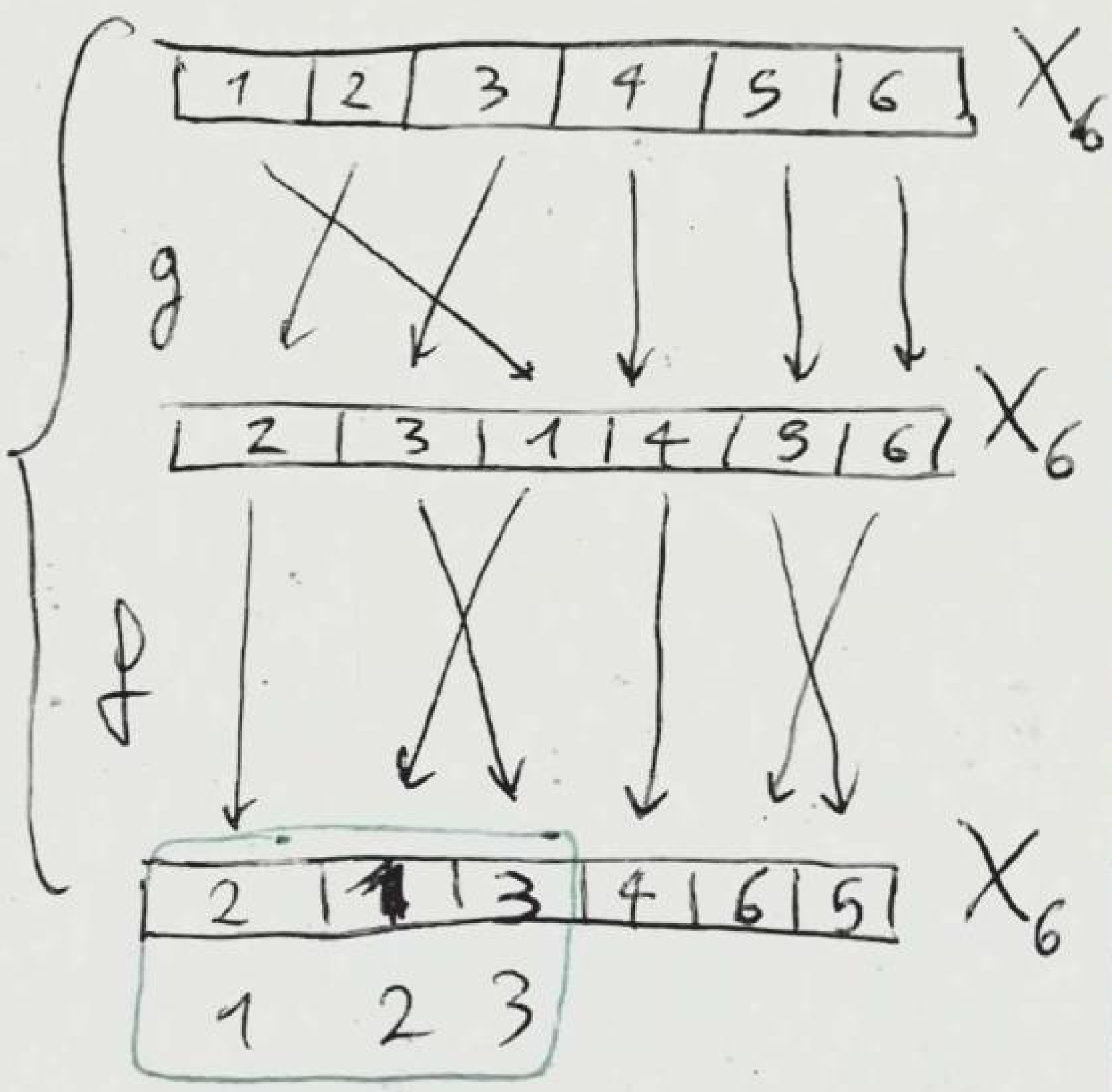
$f \circ g : X_n \longrightarrow X_n$ is bijective. $\Rightarrow f \circ g \in S_n$



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

↑

NOT COMMUTATIVE



$$\boxed{\begin{aligned} \circ : S_n \times S_n &\longrightarrow S_n \\ (f, g) &\longmapsto f \circ g \end{aligned}}$$

So $\underline{\circ}$ is an operation on $\underline{S_n}$!

We ~~want~~ to study "beautiful" operation.

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

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

We call this the SHIT OPERATION.

We want to study more beautiful example, example like S_6, and not like the shit operation.
We take all the set A, with all the operation $*$, and we select just some of them. DISCRIMINATION.

DEF] Given G set, and $*$, operation on G, we say that $(G, *)$ is a GROUP if $*$ ~~respects thi~~ has all these properties:

(1) Property of associativity: $*$ is associative if

$$\boxed{\forall a, b, c \in G \quad (a * b) * c = a * (b * c)}$$

Example] $(\mathbb{Z}; +)$ $(n+m)+k = n+(m+k)$ [+ is associative] for every $n+m+k$ $\Rightarrow$ we can avoid to put parenthesis $a+b+c$

(2) Property of the identity: $*$ has the identity, if exists $e \in G$, such that:

$$\boxed{e * a = a * e = a \quad \text{for every } a \in G}$$

e is called the identity

Example] $(\mathbb{Z}; +)$, + has the identity! $e = 0 \in \mathbb{Z}$:

$n + 0 = 0 + n = n$ for every $n \in \mathbb{Z}$

(3) Property of the inverse: $*$ has this property if:

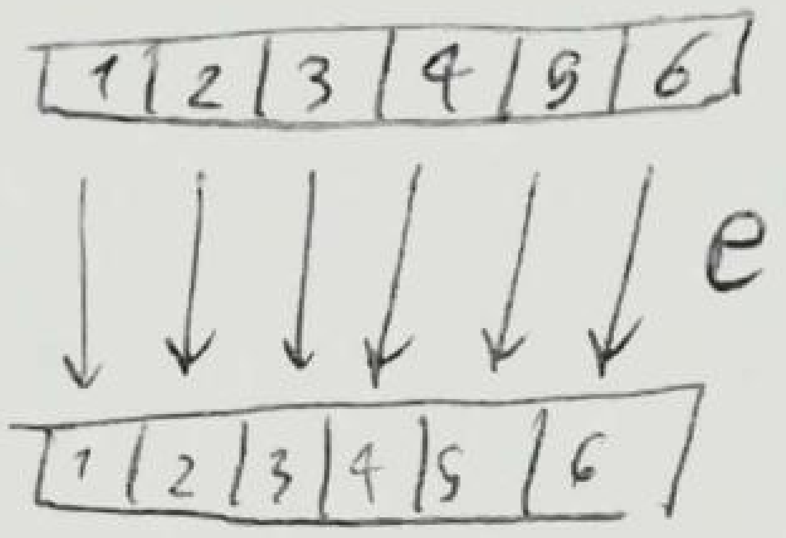
$$\boxed{\forall a \in G \quad \exists b \in G \quad \text{s.t.} \quad a * b = b * a = e}$$

(Usually the inverse of a is signed as a^{-1})

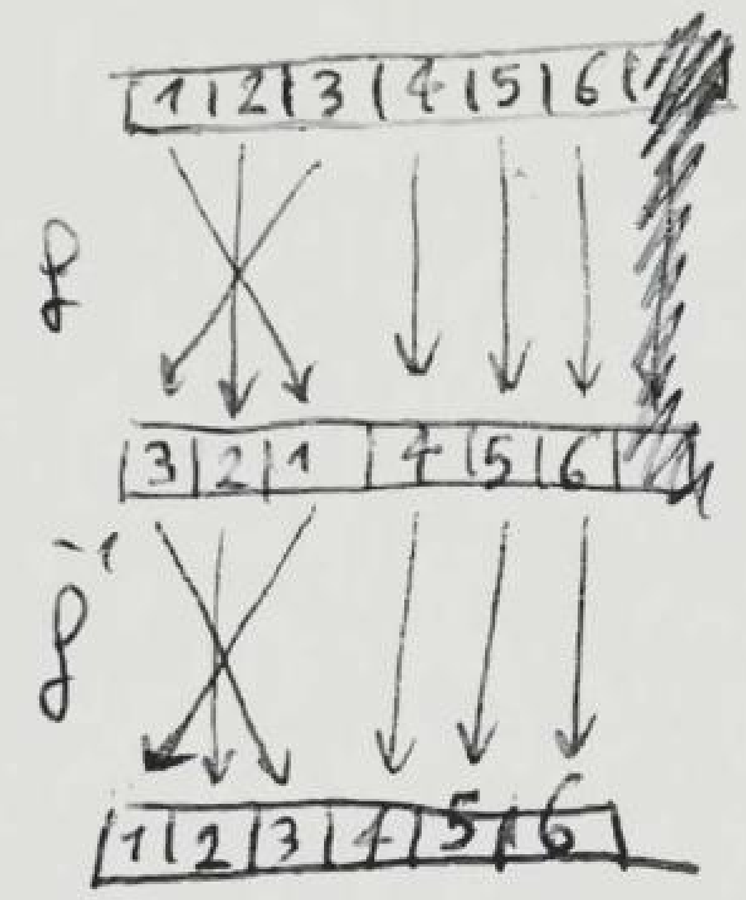
Example] $(\mathbb{Z}, +)$ If we take n, we can find $-n$,

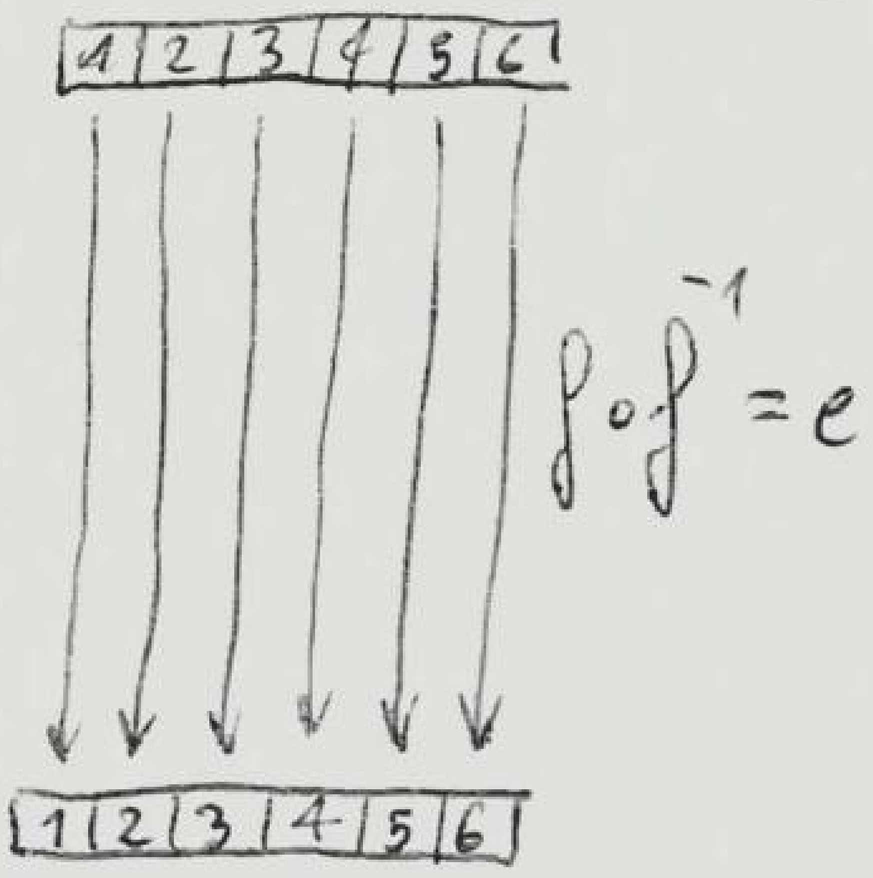
$n + (-n) = (-n) + n = 0 \leftarrow$ identity of $\mathbb{Z}$

- So $(\mathbb{Z}, +)$ is a group (seen in examples)
- We could demonstrate also that S_6 is a group, with the operation $\circ$:



- $\circ$ is ASSOCIATIVE
- $e \circ f = f \circ e = f$ for every $f \in S_6$
- $f \in S_6$, we can take the inverse $f^{-1} \in S_6$ and have $f \circ f^{-1} = e$



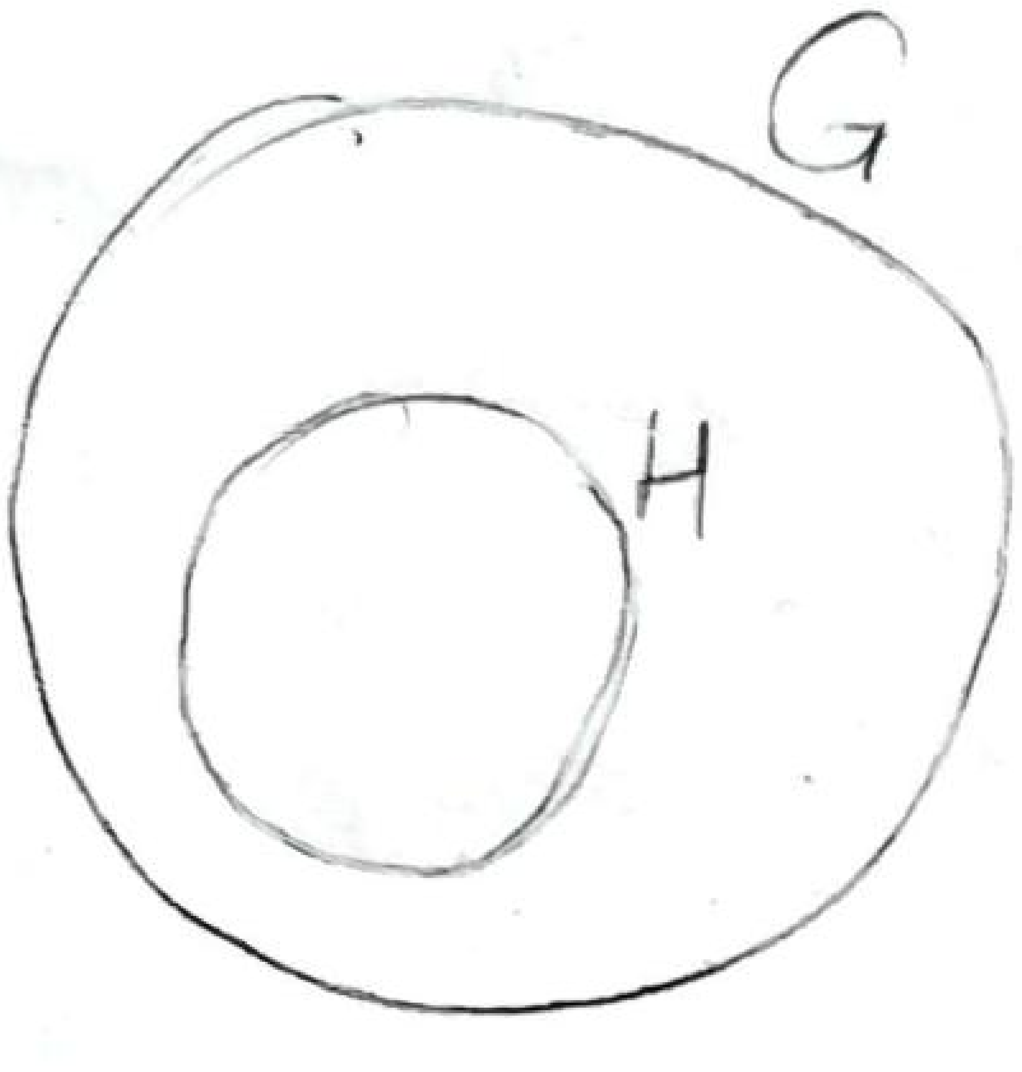


- (A, the shit operation) is not a group!

  Let's take $a \in A$ $\quad a * b = a$

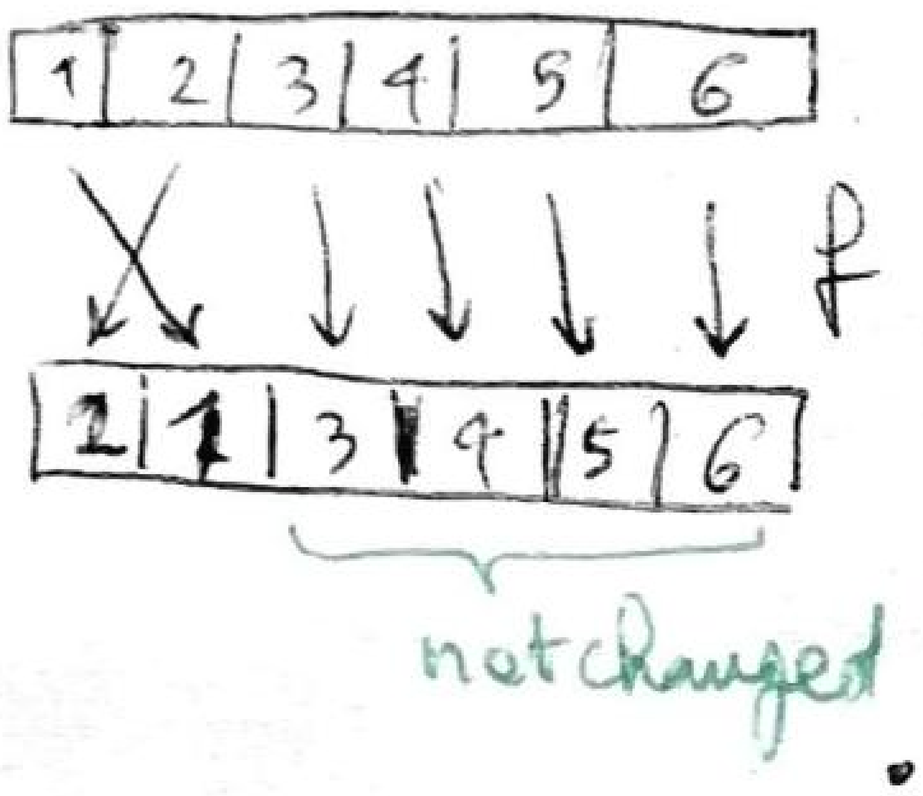
  It seems the identity is b. But if we do $b * a = b$, and if $b \neq a$, ~~again~~ we have no identity!

Now we will see another idea: we can nest (= incapsulare) groups one inside each other, like Matrioške, respect to the same operation.



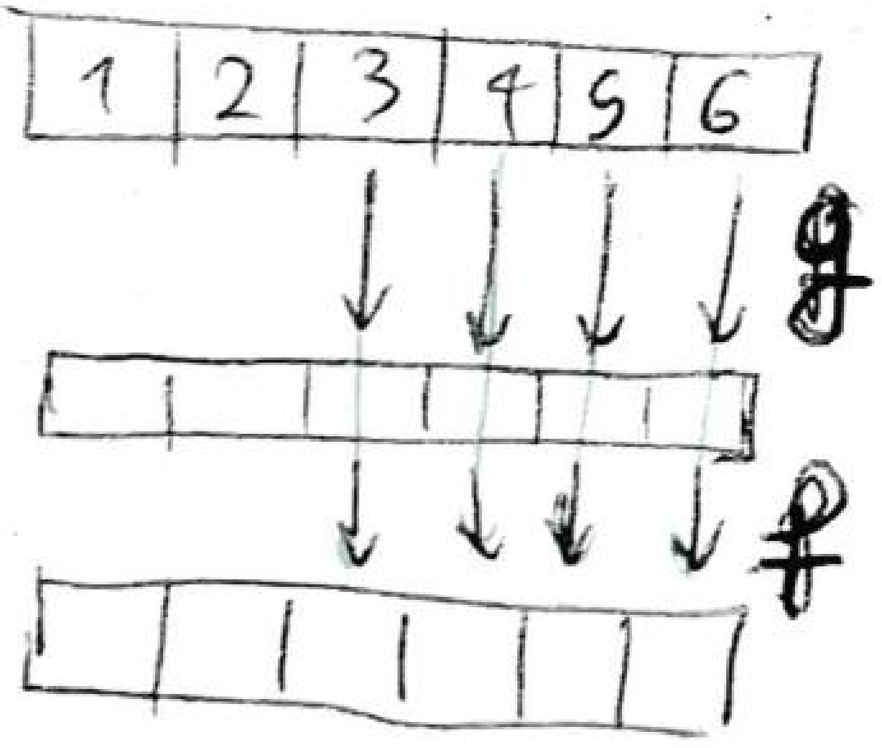
DEF Given $(G, +)$ group, and $H \subseteq G$ subset of G, we say that H is a SUBGROUP OF G if $(H, +)$ is a group.

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



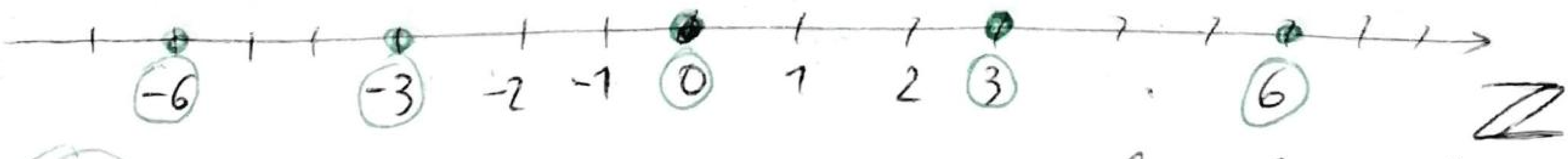
We define $H = \{ f \in S_6 \mid f(3) = 3,\ f(4) = 4,\ f(5) = 5,\ f(6) = 6 \}$

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



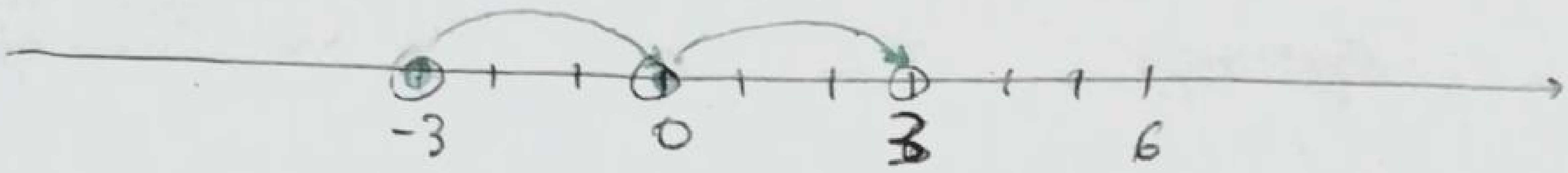
Besides, if $f \in H$, f^{-1} will not change 3, 4, 5, 6, so $f^{-1} \in H$.
So $(H, \circ)$ is a subgroup of S_6

• 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: ~~a + b~~

(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 $\forall a,b,c \in \mathbb{Z} \Rightarrow$
$\Rightarrow$ is valid for every $a,b,c \in 3\mathbb{Z}$

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

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

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

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

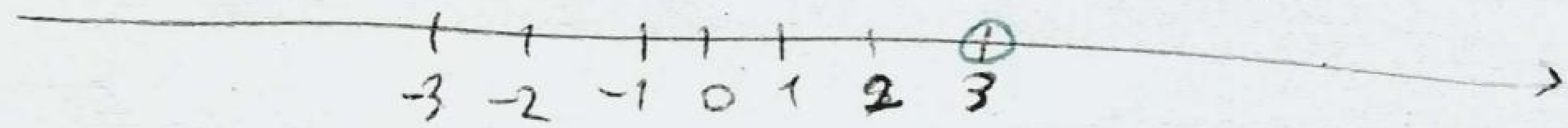
GENERATORS

DEF Given $(G, +)$ group, ~~and $g_1, \dots, g_n \in G$~~ 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:

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

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

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

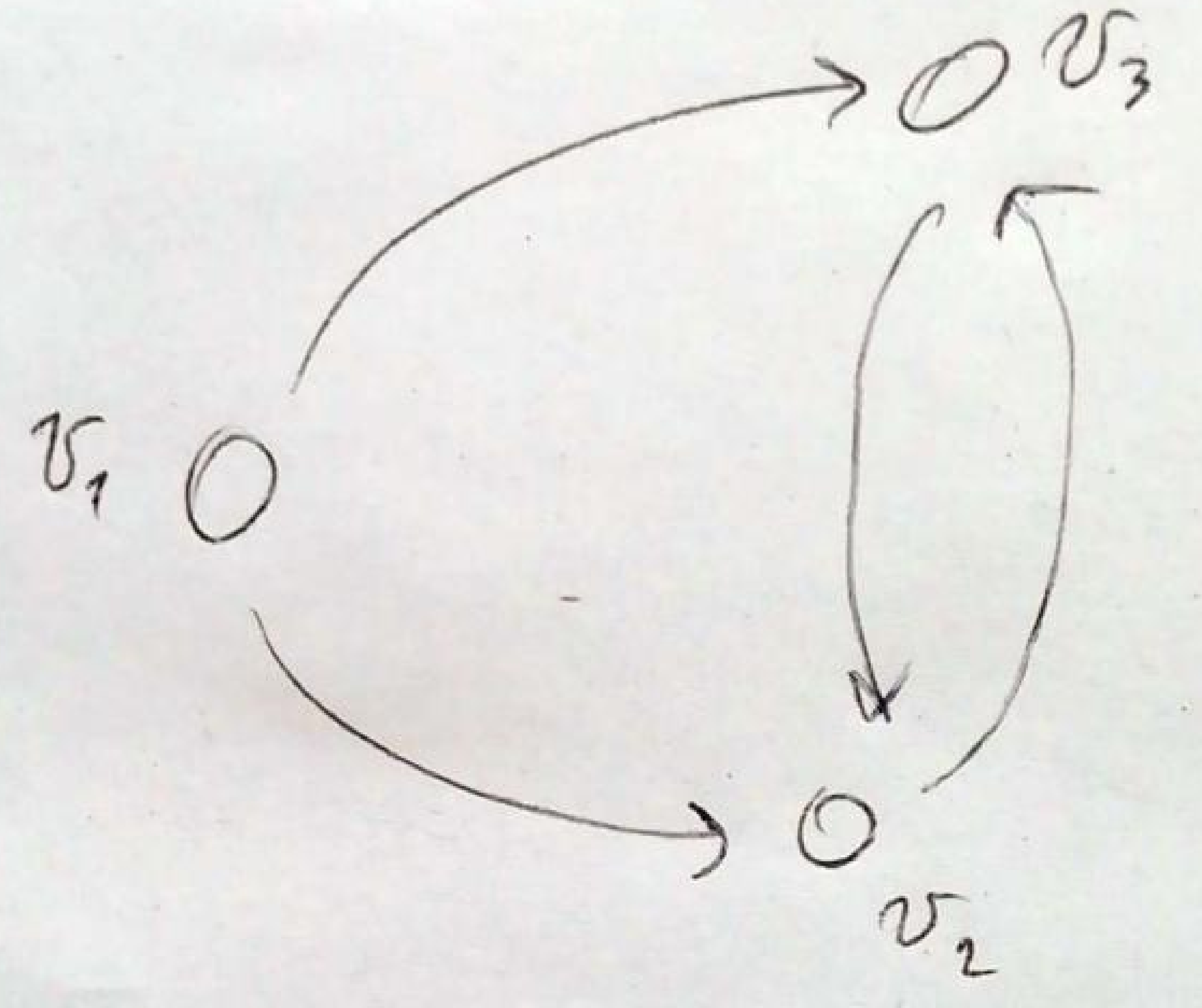
We could ~~easily~~ find out that

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

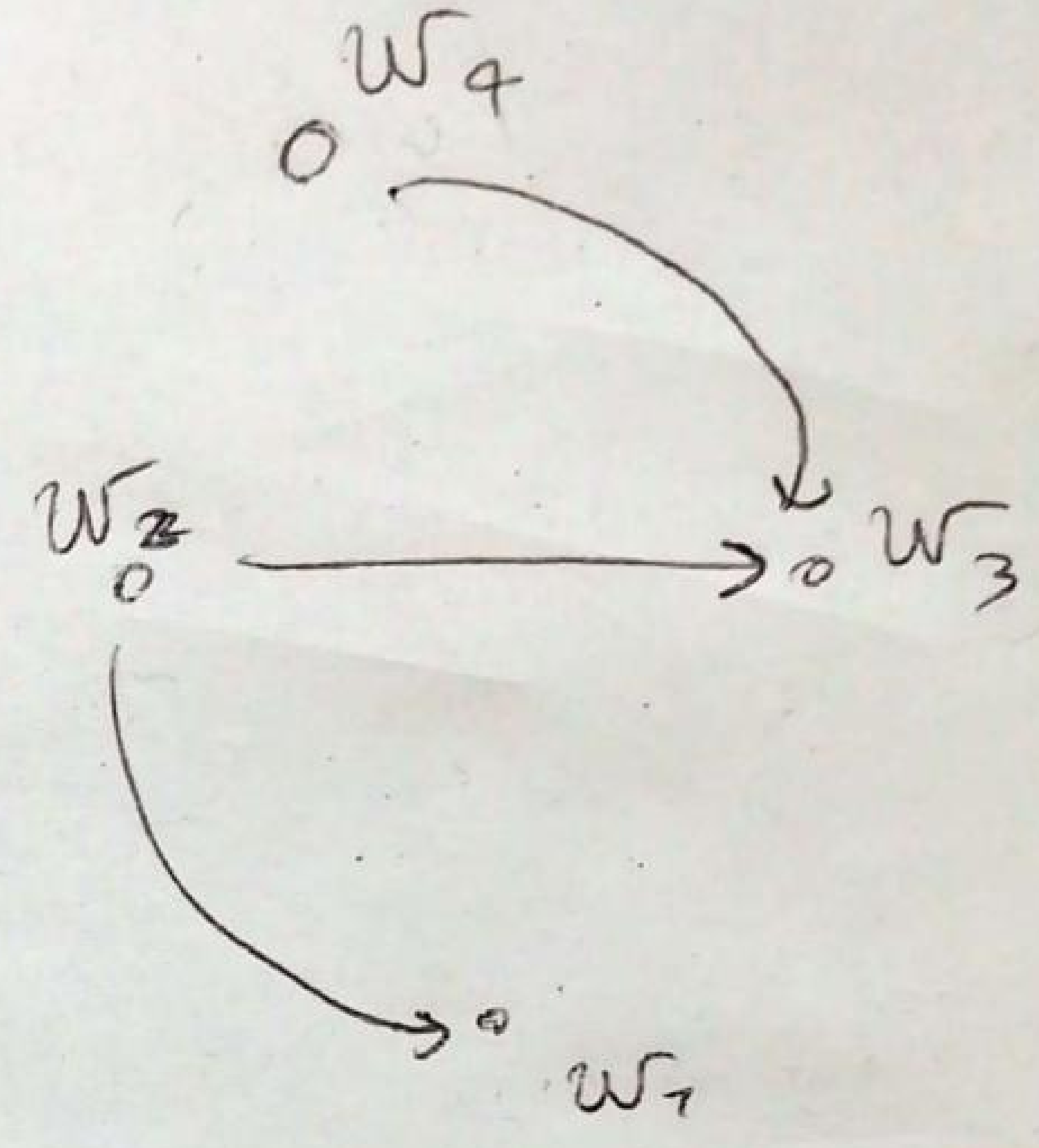
I'm not gonna demonstrate that

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 :
- Schreike 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

1st level

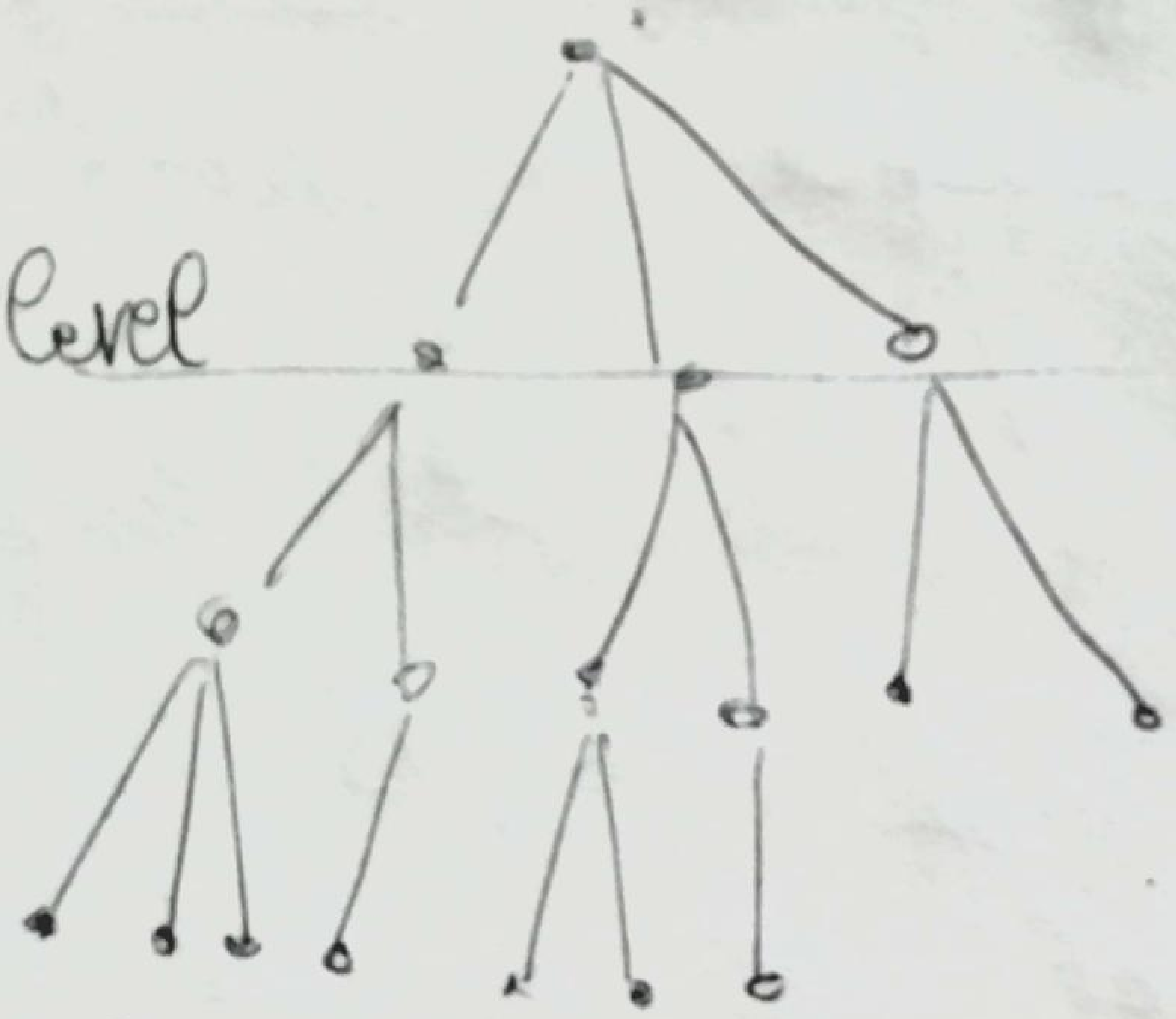
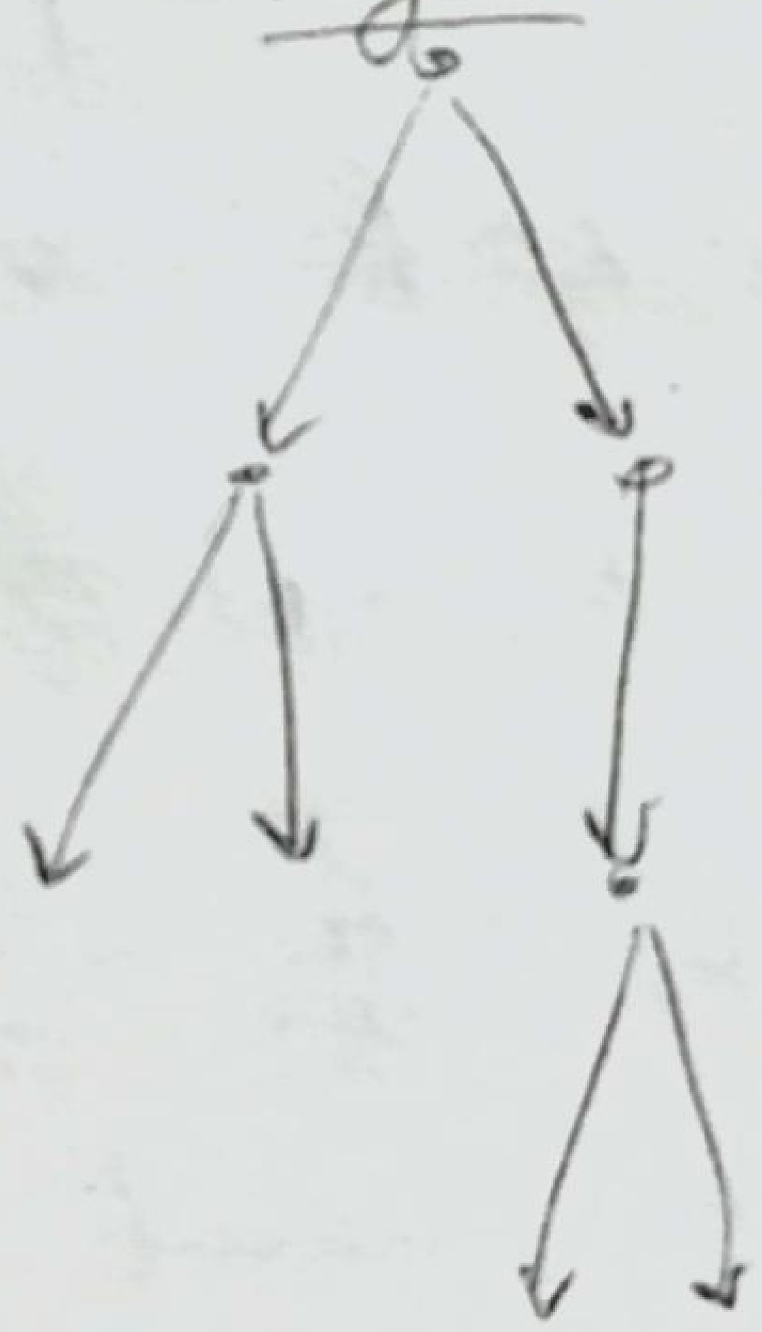


Fig. 2



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

Search images online