Recall: If $G$ is a group & $x \in G$, then

either all powers of $x$ are distinct, and we say $x$ has order $\infty$,

or $x$ has order $n$ for some integer $n$, and the powers of $x$ keep repeating themselves with period $n$, while $1, x, x^2, \dots, x^{n-1}$ are distinct.

Ex: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$ has order $\infty$;

$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in GL_n(\mathbb{R})$ has order 6.

Prop: 2.4.3. Let $G$ be a group. Let $x \in G$ have order $n < \infty$, Let $k = nq + r$ be an integer with $q \in \mathbb{Z}$ and $r \in \{0, 1, \dots, n-1\}$.

Then: (a) $x^k = x^r$. || (b) $x^k = 1$ if & only if $r = 0$.

(c) Let $d = \gcd(k, n)$. Then the order of $x^k$ is $n/d$.

**Def.** A group $G$ is called <u>cyclic</u> if $\exists x \in G$ such that $G = \langle x \rangle$.

**Ex:** $\mathbb{Z}^+$ is cyclic: $\mathbb{Z}^+ = \langle 1 \rangle = \langle -1 \rangle$.

**Ex:** Smallest non-cyclic group:

$$V = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \in GL_2(\mathbb{R}) \;\middle|\; \pm\text{'s independent} \right\}$$

is a subgroup of $GL_2(\mathbb{R})$,

Each elt. of $V$ has order $1$ or $2$, but $|V| = 4$.
$V$ is called Klein's 4-group. (Later: $V \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$.)
So $V$ is not cyclic.

## §2.5. Homomorphisms

Idea:

| | | |
|---|---|---|
| groups | $\longleftrightarrow$ | vector spaces |
| homomorphisms | $\longleftrightarrow$ | linear maps |
| isomorphisms | $\longleftrightarrow$ | invertible linear maps |
| subgroups | $\longleftrightarrow$ | subspaces |

**Def.** Let $G$ and $H$ be two groups. Let $\varphi : G \to H$ be a map. Then, $\varphi$ is called a homomorphism (of groups) if & only if it satisfies

(a) $\varphi(ab) = \varphi(a)\varphi(b)$ $\quad \forall a, b \in G$;

(b) $\varphi(1_G) = 1_H$ ;

(c) $\varphi(a^{-1}) = (\varphi(a))^{-1}$ $\quad \forall a \in G$.

**Rmk.** Conditions (b) & (c) follow from (a). Why? See Prop. 2.5.3.

**Examples:** (a) $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism.

(b) $\mathrm{sign} : S_n \to \{\pm 1\}$ — // —.

(c) $\exp : \mathbb{R}^+ \to \mathbb{R}^\times$ — // — (since $\exp(a+b) = \exp a \cdot \exp b$).

(d) $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$ — // — (since $|ab| = |a| \cdot |b|$).

(e) $|\cdot| : \mathbb{C}^+ \to \mathbb{R}^+$ is not (since $|a+b| \neq |a| + |b|$ in general),

(f) $S_n \to GL_n$, $\sigma \mapsto$ (perm. matrix of $\sigma$) $= \left( \begin{cases} 1 & \text{if } i = \sigma(j) \\ 0 & \text{else} \end{cases} \right)_{1 \le i,j \le n}$

is a homomorphism.

(g) Given any group $H$ and any $a \in H$, the map $\mathbb{Z}^+ \to H$, $n \mapsto a^n$ is a homomorphism.
(because $a^{n+m} = a^n a^m$, $a^{-n} = (a^n)^{-1}$, etc).

(h) Given any groups $G$ & $H$, the map $G \to H$, $g \mapsto 1_H$ is a homomorphism, called the trivial homomorphism.

(i) Given a group $H$ & a subgroup $G$ of $H$, the inclusion map ~~(that is, $H \to G$, $h \mapsto$~~
$G \hookrightarrow H$ (that is, $G \to H$, $g \mapsto g$)
is a homomorphism.

Prop. 2.5.3. (a) In the def. of homomorphisms, axiom (a) implies (b) & (c).

(b) If $\varphi : G \to H$ is a homomorphism, then
$$\varphi(a_1 a_2 \cdots a_k) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_k) \quad \forall a_1, a_2, \ldots, a_k \in G.$$

**Proof.** (a) Assume axiom (a) holds. Then

$$\varphi(1\cdot 1) = \varphi(1)\,\varphi(1).$$

ie $\cancel{\varphi(1)} = \cancel{\varphi(1)}\,\varphi(1)$

ie $1 = \varphi(1)$. Thus axiom (b) holds.

Next, $\forall a \in G$, we have

$$\underbrace{\varphi(a a^{-1})}_{\varphi(1) = 1} = \varphi(a)\varphi(a^{-1}), \quad \text{so} \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

Thus axiom (c) holds. Thus, part (a) follows. $\square$

(b) Induction on $k$.

For any homomorphism $\varphi: G \to H$, we define two subgroups:

- The *image* $\operatorname{Im}\varphi = \varphi(G)$ of $\varphi$ is the subset $\{\varphi(g) \mid g \in G\}$ of $H$. This is a subgroup of $H$.

(Ex: If ~~G~~ $H$ is any group and $a \in H$, then
$\mathrm{Im}(\mathbb{Z}^+ \to H,\ n \mapsto a^n) = \langle a \rangle$.)

- The kernel $\mathrm{Ker}\,\varphi$ of $\varphi$ is the subset $\{g \in G \mid \varphi(g) = 1_H\}$ of $G$. This is a subgroup of $G$.

(Ex: $\mathrm{Ker}(\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times) = SL_n(\mathbb{R})$.
$\mathrm{Ker}(\mathrm{sign} : S_n \to \{\pm 1\}) = \{\text{even permutations in } S_n\}$
$=: A_n$ (the "alternating group").)

**Def.** Let $H$ be a subgroup of a group $G$. Let $a \in G$.
Then, $aH := \{ah \mid h \in H\}$ is called the ~~left coset~~ left $H$-coset of $a$ in $G$.

**Prop. 2.5.8.** Let $\varphi :$ ~~G~~ $G \to H$ be a homom. of groups. Let $K = \ker\varphi$. Then, TFAE:
Let $a, b \in G$.

(1) $\varphi(a) = \varphi(b)$.

(2) $a^{-1}b \in K$.

(3) $b \in aK$.

(4) $bK = aK$.

<u>Proof.</u> (1) $\Rightarrow$ (2): $\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) = \varphi(b)^{-1}\varphi(b)$
$= 1$, so $a^{-1}b \in K$.

(2) $\Rightarrow$ (3): $a^{-1}b \in K \Rightarrow$ ~~...~~ $b = a \cdot \underbrace{a^{-1}b}_{\in K} \in aK$.

(3) $\Rightarrow$ (4): $b \in aK \Rightarrow \underbrace{b}_{\in aK}K \subseteq a\underbrace{KK}_{\subseteq K} \subseteq aK$

(more rigorously: $b \in aK$, so $b = al$ for some $l \in K$.
Now, $bK = \{\underbrace{b}_{=al}k \mid k \in K\} = \{\underbrace{a\underbrace{lk}_{\in K \text{ (since } K \text{ is a subgroup)}}}_{\in aK} \mid k \in K\}$

$\subseteq aK$.)

But also, $b = al$ for some $l \in K$. Thus, $a = b\underbrace{l^{-1}}_{\in K} \in bK$.

$\Rightarrow$ similarly $aK \subseteq bK$. Combined, this gives $bK = aK$.

$(4) \Rightarrow (1)$: $\quad bK = aK$.

$\Rightarrow b = b\underbrace{1}_{\in K} \in bK = aK \Rightarrow b = ak$ for some $k \in K$

$\Rightarrow \varphi(b) = \varphi(ak) = \varphi(a)\underbrace{\varphi(k)}_{=1} = \varphi(a)$. $\square$

<u>Cor. 2.5.9.</u> A homom. $\varphi : G \to H$ is injective if & only if $\operatorname{Ker}\varphi = \{1\}$.

<u>Def.</u> Let $G$ be a group. Let $a \in G$.
The <u>conjugates</u> of $a$ are the elements $gag^{-1}$ for $g \in G$.

<u>Conjugation</u> by $g \in G$ is the map

$$G \to G, \quad b \mapsto gbg^{-1}.$$

<u>Def.</u> Let $N$ be a subgroup of $G$. We say that $N$ is <u>normal</u> in $G$ if every $a \in N$ and $g \in G$ satisfy $gag^{-1} \in N$.

**Prop. 2.5.11.** If $\varphi: G \to H$ is a homom., then $\operatorname{Ker}\varphi$ is a normal subgroup of $G$.

**Pf.** Let $a \in \operatorname{Ker}\varphi$ and $g \in G$. Then,

$$\varphi(gag^{-1}) = \varphi(g)\underbrace{\varphi(a)}_{=1}\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1,$$

so $gag^{-1} \in \operatorname{Ker}\varphi$. $\square$

**Rmk.** Let $a \in G$, $b \in G$. Then TFAE:

- $ab = ba$.
- $aba^{-1} = b$.
- $bab^{-1} = a$.

**Examples:** (a) Is $SL_n$ a normal subgroup of $GL_n$?
Yes, since $SL_n = \operatorname{Ker}\det$.

(b) Is $A_n$ a normal subgroup of $S_n$? Yes, since $A_n = \operatorname{Ker}\operatorname{sign}$.

(c) Is $\langle s_1 \rangle$ a normal subgroup of $S_3$? No, since

$$s_2 s_1 s_2^{-1} = \boxed{1\ 2\ 3} \notin \langle s_1 \rangle.$$

(d) If $G$ is any group, then $\{1\}$ and $G$ are normal subgroups of $G$.

(e) Let $n \geq 2$.

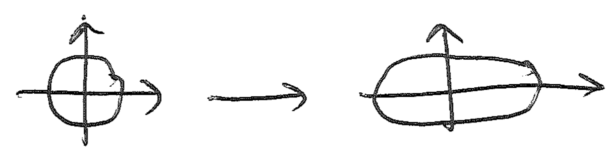
$$\begin{aligned} O_n(\mathbb{R}) &= \{\text{orthogonal group of } \mathbb{R}^n\} \\ &= \{A \in GL_n(\mathbb{R}) \mid A^T A = I_n\} \\ &= \{\text{distance-preserving linear transformations } \mathbb{R}^n \to \mathbb{R}^n\} \\ &= \{\text{isometries of } \mathbb{R}^n\}. \end{aligned}$$

E.g. $O_2(\mathbb{R}) = \{\text{rotations around } \begin{pmatrix}0\\0\end{pmatrix}\}$
$\cup \{\text{reflections in lines through } \begin{pmatrix}0\\0\end{pmatrix}\}$.

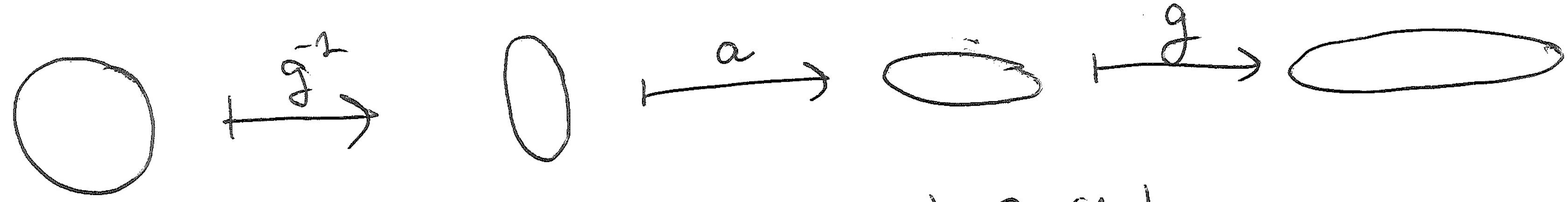
Is $O_2(\mathbb{R})$ a normal subgroup of $GL_2(\mathbb{R})$?

E.g. let $a = (90^\circ \text{ rotation}) = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \in O_2(\mathbb{R})$.

Let $g = \begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}$.
$\in GL_2(\mathbb{R})$



Is $gag^{-1} \in O_2(\mathbb{R})$?




not distance-preserving $\Rightarrow \notin O_2(\mathbb{R})$.

So, not normal.