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 keep repeating themselves with period \( n \),

of \( x \)
while \( 1, x, x^2, \ldots, x^{n-1} \) are distinct.

Ex: \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \) has order \( \infty \);
\( \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \) 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 \( r \in \{0, 1, \ldots, n-1\} \).
Then: (a) \( x^k = x^r \)  \( \parallel \) (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 **cyclic** 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:

$$V = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \in \text{GL}_2(\mathbb{R}) \mid \text{\pm's independent} \right\}$$

is a subgroup of $\text{GL}_2(\mathbb{R})$.

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:

<table>
<thead>
<tr>
<th>groups</th>
<th>$\leftrightarrow$</th>
<th>vector spaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>homomorphisms</td>
<td>$\leftrightarrow$</td>
<td>linear maps</td>
</tr>
<tr>
<td>isomorphisms</td>
<td>$\leftrightarrow$</td>
<td>invertible linear maps</td>
</tr>
<tr>
<td>subgroups</td>
<td>$\leftrightarrow$</td>
<td>subspaces</td>
</tr>
</tbody>
</table>
Def. Let $G$ and $H$ be two groups. Let $\varphi : G \rightarrow H$ 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) $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ is a homomorphism.

(b) $\text{sign} : S_n \rightarrow \{\pm 1\}$

(c) $\exp : \mathbb{R}^+ \rightarrow \mathbb{R}^*$ (since $\exp(a+b) = \exp a \cdot \exp b$).

(d) $|\cdot| : \mathbb{C}^* \rightarrow \mathbb{R}^+$ (since $|ab| = |a| \cdot |b|$).

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

(f) $S_n \rightarrow GL_n$, $\sigma \mapsto (\text{perm. matrix of } \sigma) = (s_{ij})_{1 \leq i, j \leq n}$ is a homomorphism.
(g) Given any group $H$ and any $a \in H$, the map
$$\mathbb{Z}^+ \to H, \quad n \mapsto a^n$$
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
$$G \to H, \quad g \mapsto 1_H$$
is a homomorphism, called the trivial homomorphism.

(i) Given a group $H$ & a subgroup $G$ of $H$, the inclusion map
$$G \to H$$
(that is, $G \to H, \quad g \mapsto g$)
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. (2) Assume axiom (a) holds. Then

\[ \psi(1 \cdot 1) = \psi(1) \psi(1) \]

i.e. \[ \psi(1) = \psi(1) \psi(1) \]

i.e. \[ 1 = \psi(1) \],

Thus axiom (b) holds.

Next, \( \forall a \in G \), we have

\[ \psi(a \cdot a^{-1}) = \psi(a) \psi(a^{-1}) \], so \[ \psi(a^{-1}) = \psi(a)^{-1} \].

Thus axiom (c) holds. Thus, part (2) follows. \( \square \)

(b) Induction on \( k \).

For any homomorphism \( \psi : G \rightarrow H \), we define two subgroups:

- The image \( \text{Im} \psi = \psi(G) \) of \( \psi \) is the subset \( \{ \psi(g) \mid g \in G \} \) of \( H \). This is a subgroup of \( H \).
(Ex) If $G$ is any group and $a \in H$, then 
$\text{Im}(\mathbb{Z}^+ \to H, \ n \mapsto a^n) = \langle a \rangle$. 

The kernel $\ker \varphi$ of $\varphi$ is the subset \{\(g \in G \mid \varphi(g) = 1_{H}\}\} of $G$. This is a subgroup of $G$.

(Ex) $\text{Ker}(\det: \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\times) = \text{SL}_n(\mathbb{R})$.

$\text{Ker}(\text{sign: } S_n \to \{\pm 1\}) = \{\text{even permutations in } S_n\}$

$= A_n$ (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 $H$-coset of $a$ in $G$.

**Prop. 2.5.8.** Let $\varphi: \text{G} \to \text{H}$ be a homomorphism of groups.

Let $a, b \in G$. Let $K = \ker \varphi$. Then, TFAE:

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

(3) \( b \in aK \).

(4) \( bK = aK \).

Proof.

(4) \( \Rightarrow \) (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): \( a^{-1}b \in K \) \( \Rightarrow \) \( b = a \cdot a^{-1}b \in aK \).

(3) \( \Rightarrow \) (4): \( b \in aK \) \( \Rightarrow \) \( bK \leq aK K \leq aK \).

(more rigorously: \( b \in aK \), so \( b = al \) for some \( l \in K \).

Now, \( bK = \{bk \mid k \in K \} = \{alk \mid k \in K \} \)

\( = \{al \} \) (since \( K \) is a subgroup)

\( \leq aK \).

But also, \( b = al \) for some \( l \in K \). Thus, \( a = bl^{-1} \in bK \).
Similarly \( aK \subseteq bK \), combined, this gives \( bK = aK \).

(4) \( \Rightarrow \) (1):
\[
\Rightarrow bK = aK \Rightarrow b = a_k \text{ for some } k \in K
\]
\[
\Rightarrow \varphi(b) = \varphi(a_k) = \varphi(a) \varphi(k) = \varphi(a) \cdot 1
\]
\[
\square
\]

Cor. 2.5.9. A \( \varphi \) homom. \( \varphi : G \rightarrow H \) is injective if \& only if \( \text{Ker } \varphi = \{1\} \).

Def. Let \( G \) be a group, let \( a \in G \).
The conjugates of \( a \) are the elements \( g \cdot a \cdot g^{-1} \) for \( g \in G \).

Conjugation by \( g \in G \) is the map \( G \rightarrow G, \; b \mapsto g \cdot b \cdot g^{-1} \).

Def. Let \( N \) be a subgroup of \( G \). We say that \( N \) is normal in \( G \) if every \( a \in N \) and \( g \in G \) satisfy \( g \cdot a \cdot g^{-1} \in N \).
Prop. 2.5.11. If \( \varphi : G \to H \) is a homomorphism, then
\[ \ker \varphi \] is a normal subgroup of \( G \).

\[ \text{Pf.} \] Let \( a \in \ker \varphi \) and \( g \in G \). Then,
\[ \varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1, \]
so \( gag^{-1} \in \ker \varphi \). \( \Box \)

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 \( SL_n = \ker \det \).

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

(c) Is \( \langle s_1 \rangle \) a normal subgroup of \( S_3 \)? No, since
\[ S_3 S_2 S_2^{-1} = \langle 1, 2, 3 \rangle \notin \langle s_1 \rangle. \]
(d) If $G$ is any group, then $\mathbb{Z}/3$ and $G$ are normal subgroups of $G$.

(e) Let $n \geq 2$.

$$O_n(\mathbb{R}) = \{ \text{orthogonal group of } \mathbb{R}^n \}$$

$$= \{ A \in GL_n(\mathbb{R}) \mid A^T A = I_n \}$$

$$= \{ \text{distance-preserving linear transformations } \mathbb{R}^n \to \mathbb{R}^n \}$$

$$= \{ \text{isometries of } \mathbb{R}^n \}. \tag{2}$$

E.g. $O_2(\mathbb{R}) = \{ \text{rotations around } (0) \}$

$\cup$ vertices of reflections in lines through $(0)$.

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 $g = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $g^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$.

$g^{-1} a g$ acts as

$\begin{pmatrix} \ast & \ast \\ \ast & \ast \end{pmatrix}$
Is $g \circ g^{-1} \in O_2(R)$?

not distance-preserving $\implies \notin O_2(R)$.

So, not normal.