Order

Recall: Let G be a group and $g \in G$.

For $n \in \mathbb{N}$, we will write

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}$$

and

$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}.$$

We will also write $g^0 := e$.

Thm: Let G be a group and $g \in G$. Then

① $g^m g^n = g^{m+n}$ for all $n, m \in \mathbb{Z}$.

② $(g^m)^n = g^{mn}$ for all $n, m \in \mathbb{Z}$.

③ $(g^n)^{-1} = g^{-n}$ for all $n \in \mathbb{Z}$.

This should be fairly intuitive, but the proof is tricky!

Outline:
- First prove for $n, m \in \mathbb{N}$ by induction.
- Then consider cases where n and/or m are 0 or negative.

WARNING: Since G may not be abelian, $(gh)^n \neq g^n h^n$ in general.

Potentially confusing convention

While we use multiplicative notation in general, there are some groups (e.g., $\mathbb{Z}$, $\mathbb{Z}_n$) where we use $+$ for the group operation.

Note: We only use $+$ for abelian groups.

In these groups, we will write

$$ng := \underbrace{g + \cdots + g}_{n \text{ times}}$$

and

$$-ng := \underbrace{(-g) + \cdots + (-g)}_{n \text{ times}}$$

for $n \in \mathbb{N}$.

Also, $0g := e$.

<u>Def</u>: Let G be a group and $g \in G$.

The <u>order</u> of g is the smallest positive integer n such that $g^n = e$. We write $|g| = n$.

If no such positive integer exists, we say g has <u>infinite order</u> and write $|g| = \infty$.

<u>Def</u>: Let G be a group.

If $|G| = n$ for some $n \in \mathbb{N}$, then we say G is a <u>finite group</u> and that G has <u>order n</u>.

If $|G|$ is infinite, we say G is an <u>infinite group</u>. We also say that it is a group of <u>infinite order</u>.

Ex: $|\mathbb{Z}_4| = 4$, and

$$|0| = 1, \quad |1| = 4, \quad |2| = 2, \quad |3| = 3.$$

Ex: $|U(8)| = 4$, and

$$|1| = 1, \quad |3| = 2, \quad |5| = 2, \quad |7| = 2.$$

Ex: $\mathbb{Z}$ is infinite.

$$|0| = 1, \text{ and } |n| = \infty \text{ if } n \neq 0.$$

Ex: $GL_2(\mathbb{R})$ is infinite.

$$\left|\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right| = 4, \quad \left|\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\right| = \infty.$$

Check these!

Subgroups

Def: Let G be a group. A <u>subgroup</u> of G is a subset $H \subseteq G$ which is also a group <u>under the same operation</u>.

Notation: $H \leq G$.

If $H \leq G$ and $H \neq G$, write $H \lneq G$.

Ex:

- $\mathbb{Z} \lneq \mathbb{Q} \lneq \mathbb{R} \lneq \mathbb{C}$ (as groups under $+$)

- $\{1,-1\} \lneq \underset{\mathbb{Q}\setminus\{0\}}{\mathbb{Q}^\times} \lneq \underset{\mathbb{R}\setminus\{0\}}{\mathbb{R}^\times} \lneq \underset{\mathbb{C}\setminus\{0\}}{\mathbb{C}^\times}$ (as groups under $\cdot$)

- For any group G, the subset $\{e\}$ containing only the identity is a subgroup, called the <u>trivial subgroup</u> of G.

<u>Observation</u>: Let $(G, *)$ be a group and $H \subseteq G$ a subset.

In order for H to be a subgroup, we must check both

① <u>$*$ is a binary operation on H</u>.

That is, for all $h_1, h_2 \in H$, we have $h_1 * h_2 \in H$.

Also say H is <u>closed under $*$</u>.

② <u>$(H, *)$ is a group</u>.

$*$ is already known to be associative, so need to check 2 things:

- $e \in H$.

and

- for all $h \in H$, we have $h^{-1} \in H$

i.e., H is <u>closed under inverses</u>

Ex: Let $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$ be the set of multiples of 3. Then

- $3\mathbb{Z}$ is closed under $+$

  $3k_1 + 3k_2 = 3(k_1 + k_2)$ ✓

- $0 \in 3\mathbb{Z}$

  $0 = 3(0)$ ✓

- $3\mathbb{Z}$ is closed under additive inverses

  $-(3k) = 3(-k)$ ✓

Therefore, $3\mathbb{Z} \leq \mathbb{Z}$.

Ex: By the exact same reasoning, the set

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

of all multiples of some fixed $n \in \mathbb{Z}$ is also a subgroup of $\mathbb{Z}$.

Ex: Two groups of order 4, $\mathbb{Z}_4$ and $U(8)$

<u>Subgroups of $\mathbb{Z}_4$</u>

- $\mathbb{Z}_4$
- $\{0\}$
- $\{0,2\}$

<u>Subgroups of $U(8)$</u>

- $U(8)$
- $\{1\}$
- $\{1,3\}$
- $\{1,5\}$
- $\{1,7\}$

We can organize this information by drawing the <u>subgroup lattice</u> for each group.

$$\begin{tikzcd}[arrows=dash]
\mathbb{Z}_4 \arrow[d] \\
\{0,2\} \arrow[d] \\
\{0\}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[arrows=dash]
& U(8) \arrow[dl] \arrow[d] \arrow[dr] & \\
\{1,3\} \arrow[dr] & \{1,5\} \arrow[d] & \{1,7\} \arrow[dl] \\
& \{1\} &
\end{tikzcd}$$

Here, upward paths indicate inclusions.