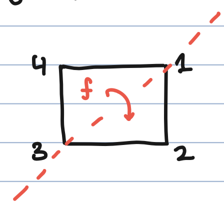
Subgroups



- Symmetry group for this is D_4
- What if we only want the motions that fix 1?
  - $\rightarrow$ Then $H = \{id, f\}$ is a group under composition and is a subset of D_4.

We refer to H as a subgroup of D_4.

Definition: Let $(G, *)$ be a group. We say a nonempty subset $H \subseteq G$ is a subgroup if $(H, *)$ is a group.

For H to be a group, we need:
- nonempty
- identity
- associative (for free if it is a subset of a group.)
- inverses
- closed

However, suppose we know $H \neq \emptyset$ and whenever $x, y \in H$, then $x * y^{-1} \in H$. This implies the following:
- $x \in H$, $x * x^{-1} \in H \Rightarrow e_G \in H$. (identity)
- $x \in H$, $e_G * x^{-1} \Rightarrow x^{-1} \in H$ (inverse)
- $x \in H$, $y^{-1} \in H$, $x * (y^{-1})^{-1} \Rightarrow x * y \in H$. (closure)

Proposition: If $H \subseteq G$, where $(G, *)$ is a group. if $\underline{H \neq \emptyset}$ and $\underline{x * y^{-1} \in H}$ for all $x, y \in H$, then H is a subgroup

Example: Let $G = \mathbb{Z}$, $* = +$.
Fix $n \in \mathbb{Z}$. Consider $H = n\mathbb{Z} = \{m \in \mathbb{Z} : n \mid m\}$
$= \{nk : k \in \mathbb{Z}\}$
Note $H \neq \emptyset$ b/c $n \in H$.
Let $a, b \in H$. We can write $a = ns$ and $b = nt$ for some $s, t \in \mathbb{Z}$.
We have $a - b = ns - nt = n(s-t) \in H$.
So H is a subgroup of G.

Example: Consider the group D_3. Its subgroups are:
- D_3
- $\{e\}$
- $H_1 = \{e, r, r^2\}$
- $H_2 = \{e, \sigma\}$
- $H_3 = \{e, \sigma r\}$

- $H_4 = \{e, \sigma r^2\}$

Suppose we have a subgroup H_* with $\sigma r, \sigma r^2 \in H$.
Note that:

$$\begin{aligned} \sigma r \sigma r^2 \in H &\Leftrightarrow \sigma r^2 r^2 \sigma \in H \\ &\Leftrightarrow \dots \\ &\Leftrightarrow r^2 \in H \end{aligned}$$

So H_* also contains r^2. But:

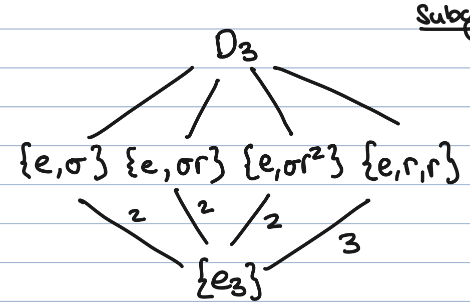
$$\sigma r r^2 \in H \Leftrightarrow \sigma \in H$$

So H_* also contains σ. But:

$$\begin{aligned} \sigma \in H &\Leftrightarrow \sigma(\sigma r) \in H \\ &\Leftrightarrow r \in H \\ \text{and } &\Leftrightarrow \sigma(\sigma r^2) \in H \\ &\Leftrightarrow r^2 \in H. \end{aligned}$$

So $H_* = D_3$.

Subgroup lattice



Exercise: • What are the subgroups of $\mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$

$\longrightarrow$ Clearly $\mathbb{Z}/6\mathbb{Z}$ and $\{0\}$ are.

If H is a subgroup and $1 \in H$, then $H = \mathbb{Z}/6\mathbb{Z}$

If $2 \in H$, then $4 \in H$, and $0 \in H$. So $H = \{0,2,4\}$.

If $3 \in H$, then $0 \in H$. So $H \in \{0,3\}$.

If $4 \in H$, then $2 \in H$, and $0 \in H$. So $H = \{0,2,4\}$.

If $5 \in H$, then $H = \mathbb{Z}/6\mathbb{Z}$.

• Is $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$ a subgroup of $GL_2(\mathbb{R})$?

$\longrightarrow$ H is clearly nonempty since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$.

Let $A, B \in H$. WTS $AB^{-1} \in H$.

So $AB^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \in H$.

So H is a subgroup.

- Let G be a group, where H, K are subgroups. We denote this as $H, K \leq G$. Show $H \cap K \leq G$.
  - $\rightarrow$ Since H, K are subgroups, $e_G \in H$ and $e_G \in K$. So $e_G \in H \cap K$.
    Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$.
    Since $H \leq G$, $a * b^{-1} \in H$
    Since $K \leq G$, $a * b^{-1} \in K$.
    So $a * b^{-1} \in H \cap K$.
    Thus $H \cap K$ is a subgroup.

- Is $H \cup K$ a subgroup?
  - $\rightarrow$ Not in general. Suppose $H = \{id, \sigma r\}$ and $K = \{id, \sigma r^2\}$
    Then $H \cup K = \{id, \sigma r, \sigma r^2\}$, which is not closed under multiplication because $\sigma r \sigma r^2 = \ldots = r^2 \notin H \cup K$.

Cyclic Groups:

Let $(G, *)$ be a group. We say G is cyclic if there exists $g \in G$ so that $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$

For any group $(G, *)$ and $a \in G$, set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ as the cyclic subgroup generated by a.

Example: Let $G = D_3$. $H = \langle r \rangle = \{r^k : k \in \mathbb{Z}\} = \{r, r^2, r^3 = e\}$

Definition: Let $a \in G$ with $a^n = e$ for some $n \in \mathbb{Z}_{\geq 1}$. If $a^m \neq e$ for all $0 < m < n$, we say n is the order of a and write $|a| = n$ or $\text{ord}_G(a) = n$.

If there is no such n, we say a has infinite order and write $|a| = \infty$.

Example: $G = \mathbb{Z}$, then $|2| = \infty$
$G = D_3$, then $|r| = 3$

$a^n = e$
$a^k = e$ iff $n | k$

Proposition: Let $a \in G$ with $|a| = n$.

1) $a^k = e$ iff $n \mid k$ iff $k \equiv 0 \pmod n$
2) $a^i = a^j$ iff $i \equiv j \pmod n$
3) $\# \langle a \rangle = |a|$
4) $\langle a^k \rangle = \langle a \rangle$ iff $\gcd(k,n) = 1$
5) $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$
6) $|a^k| = n / \gcd(k,n)$

$\langle a \rangle \quad | \quad |$

$\langle a \rangle \quad | \quad |$

$| \langle e \rangle |$

proof: 1) is a special case of 2).

For 2) ($\Rightarrow$) suppose $a^i = a^j$.

So $a^i a^{-j} = e \Leftrightarrow a^{i-j}$

Using the division algorithm, write $i - j = nq + r$ for some $q, r \in \mathbb{Z}$, where $0 \leq r < n$.

$a \mid b$

$\exists c \in \mathbb{Z}$ s.t. $b = ac$.

So we have
$$\begin{aligned} e &= a^{i-j} \\ &= a^{nq+r} \\ &= (a^n)^q a^r \\ &= e^q a^r \\ &= a^r \end{aligned}$$

Thus $a^r = e$. However, $r < n$ and n is the smallest positive integer with $a^n = e$. So $r = 0$.

how?

$r = 0$

$\Rightarrow i - j = nq$

$n \mid (i-j)$

Thus, $n \mid (i-j)$, i.e. $i \equiv j \pmod n$

($\Leftarrow$) Assume $i \equiv j \pmod n$.

So there exists $k \in \mathbb{Z}$ with $i - j = nk$.

We have
$$\begin{aligned} a^i &= a^i \\ &= a^{j+nk} \\ &= a^j (a^n)^k \\ &= a^j e^k \\ &= a^j \quad \square \end{aligned}$$

225 236 62
112 81 71
62 33 23