Two ways to get subgroups in a general group $(G, *)$

(1) Given two subgroups $H, K \subseteq G$, then $H \cap K \subseteq G$ is a subgroup

Pf • Since H, K are subgroups, $e \in H, e \in K \Rightarrow e \in H \cap K$.
• If $a \in H \cap K \Rightarrow a^{-1} \in H, a^{-1} \in K \Rightarrow a^{-1} \in H \cap K$
• $a, b \in H \cap K \Rightarrow a * b \in H, a * b \in K \Rightarrow a * b \in H \cap K$

(2) Cyclic group: Given $a \in G$, the set $\{a^n : n \in \mathbb{Z}\}$ with operation $*$ is a subgroup of G. Usually called the cyclic group generated by a and is denoted by $\langle a \rangle$.

Pf • $a^0 = e \in \langle a \rangle$
• $a^n \in \langle a \rangle \Rightarrow a^{-n} \in \langle a \rangle$
• all elements of $\langle a \rangle$ are of the form a^{i_1}, a^{i_2} and thus $a^{i_1} * a^{i_2} = a^{i_1 + i_2} \in \langle a \rangle$.

Ex. $3\mathbb{Z}, 2\mathbb{Z} \subseteq \mathbb{Z}$ and $3\mathbb{Z} \cap 2\mathbb{Z} = 6\mathbb{Z}$.

• $0 \in \mathbb{Z} \rightsquigarrow \langle 0 \rangle$ has exactly one element
$a \in \mathbb{Z} \rightsquigarrow \langle a \rangle = a\mathbb{Z}$.

• Consider $(\mathbb{C}^*, \times)$ ~~and let i be a square root of~~
What is $\langle i \rangle$?

Pf As a set $\langle i \rangle = \{\dots, i^{-2}, i^{-1}, i^0, i^1, i^2, \dots\}$.
But $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i \dots$. More precisely $i^k = i^{k-4}$.
Thus $\langle i \rangle = \{1, i, -i, -1\}$ and has size 4.

- Similarly given an n^{th} root ω_n of 1, the subgroup $\langle \omega_n \rangle$ has size n.

• $\left\langle \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{A} \right\rangle \subseteq GL_2(\mathbb{R})$

$A^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Cosets and $\mathbb{Z}/m\mathbb{Z}$

Given a subgroup $H \leq G$ we can define two equivalence relations on G as follows

(1) $a \sim_L b \iff a^{-1} * b \in H$

(2) $a \sim_R b \iff a * b^{-1} \in H$

Let's check (1) is an equivalence relation.

- Reflexive: $a \sim_L a$ because $a^{-1} * a = e \in H$
- Symmetric: $a \sim_L b \Rightarrow a^{-1} * b \in H \Rightarrow (a^{-1} * b)^{-1} \in H$
  $\Rightarrow b^{-1} * a \in H \quad (= b^{-1} * (a^{-1})^{-1})$
  $\Rightarrow b \sim_L a$
- Transitive: $a \sim_L b$ and $b \sim_L c \Rightarrow a^{-1} * b,\ b^{-1} * c \in H \Rightarrow (a^{-1} * b) * (b^{-1} * c) \in H$
  $\Rightarrow a^{-1} * (b * (b^{-1} * c)) \in H$
  $\Rightarrow a^{-1} * e * c \in H$
  $\Rightarrow a^{-1} * c \in H$ ∎

Defn The equivalence classes of $\sim_L$ are called <u>left cosets</u> and the equivalence classes of $\sim_R$ are called <u>right cosets</u>.

Prop For $x \in G$, the left coset (equivalence class) containing x is
$xH = \{x * h : h \in H\} \subseteq G$.

Pf We need to show $[x] = xH$.

- $[x] \subseteq xH$: Well $x \sim y \Rightarrow x^{-1} * y \in H \Rightarrow \exists\ h \in H$ such that $x^{-1} * y = h$
  $\Rightarrow y = x * h$
  $\Rightarrow y \in xH$
  Thus $[x] \subseteq xH$ ∎
- $xH \subseteq [x]$: If $y \in xH \Rightarrow y = x * h$ for some $h \in H$
  $\Rightarrow x^{-1} * y = h$
  $\Rightarrow x^{-1} * y \in H$
  $\Rightarrow x \sim y$ ∎

Corollary $\forall x, y \in G$, $xH = yH$ if and only iff $x^{-1} * y \in H$.

Pf Use the previous proposition

This says there are many possible representatives that give the same left coset.

- $[e] = eH = H$
- If $H = \{e\}$, then every left coset $[g] = \{g\}$ $\forall g \in G$.

Ex • Consider $3\mathbb{Z} \leq \mathbb{Z}$. From above, cosets of $3\mathbb{Z}$ are just of the form $x + 3\mathbb{Z}$ for $x \in \mathbb{Z}$.

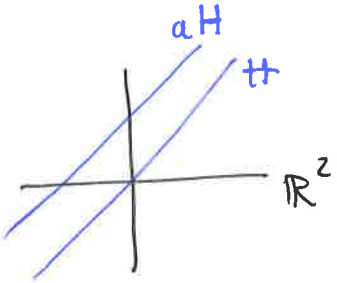
- $0 + 3\mathbb{Z} = [0]$
- $1 + 3\mathbb{Z} = [1]$
- $2 + 3\mathbb{Z} = [2]$
- $3 + 3\mathbb{Z} = [0]$

Thus $3\mathbb{Z}$ partitions $\mathbb{Z}$ into 3 cosets.

~~Exercise: More generally $n\mathbb{Z}$ partitions $\mathbb{Z}$ into n cosets.~~

Ex $(G, *) = (\mathbb{R}^2, +)$, $H = \{(x, x) : x \in \mathbb{R}\}$

Given $a \in \mathbb{R}^2$, aH or $a + H$ is a left coset that geometrically corresponds to translation by a.



Defn Let $(G, *)$ be a group and H a subgroup. We denote G/H to mean the set of left cosets of H in G. If $|G/H|$ is finite, we say H has finite index in G and write

$$[G : H] := |G/H|$$

Remark Given a group G, $|G|$ is called the order of G.

Construction of $\mathbb{Z}/m\mathbb{Z}$, $\forall m \geq 1$

Thm [Division algorithm] Given $n, m \in \mathbb{Z}$, $m > 0$, $\exists$ unique $q, r \in \mathbb{Z}$ s.t.

$$n = mq + r \quad \text{and} \quad 0 \leq r < m.$$

Ex $(3, 13) \rightsquigarrow 13 = 3 \cdot 4 + 1$.

As a consequence, $m\mathbb{Z} \subseteq \mathbb{Z}$ has exactly m cosets i.e. $|\mathbb{Z}/m\mathbb{Z}| = m$. Each coset can be represented by the remainder of division by m:

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}.$$

Note: Given $a, b \in \mathbb{Z}$, $a - b \in m\mathbb{Z} \iff m$ divides $a - b$

$$\iff a - b = m \cdot q + 0$$

$$\iff a = m \cdot q_1 + r \text{ and } b = m q_2 + r$$

i.e. same remainder

In fact we can put a group structure on $\mathbb{Z}/m\mathbb{Z}$:

Defn $(\mathbb{Z}/m\mathbb{Z}, +)$ is defined by

$$[a] + [b] := [a + b] \quad \forall\, a, b \in \mathbb{Z}.$$

① Is this well defined? : Yes, if $[a] = [a']$ and $[b] = [b']$, then

$$[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$$

② It's associative

③ It has an identity $[0]$: $[0] + [a] = [a] = [a] + [0]$

④ It has inverses : $[a]^{-1} := [-a]$.

Ex • $(\mathbb{Z}/3\mathbb{Z}, +) = \{[0], [1], [2]\}$

- $[0] + [1] = [1]$
- $[0] + [2] = [2]$
- $[1] + [2] = [0]$ or $[1] + [-1] = [0]$