Subgroups

Definition

Definition 1

Let $(G, \star)$ denote a group. A **subgroup** *$H < G$ is a subset of G such that $(H, \star)$ is also a group.*

Example 1

The set $6\mathbb{Z} \subset \mathbb{Z}$ of multiples of 6 forms a subgroup of $\mathbb{Z}$.

Proof: We must verify the group axioms:

- Is $+$ binary on $6\mathbb{Z}$? (Verifying this condition is sometimes called "showing $6\mathbb{Z}$ is **closed under addition**".)

  Suppose $g, h \in 6\mathbb{Z}$. Since g and h are multiples of 6 then there exist (integers) n and m such that $g = 6n$ and $h = 6m$. We must show $g + h \in 6\mathbb{Z}$:

$$\begin{aligned} g + h &= 6n + 6m \\ &= \underbrace{n + \cdots + n}_{\text{6 times}} + \underbrace{m + \cdots + m}_{\text{6 times}} \\ &= \underbrace{(n + m) + \cdots + (n + m)}_{\text{6 times}} \text{ (by associativity in } G) \\ &= 6(n + m). \end{aligned}$$

Since $\mathbb{Z}$ is a group $n + m \in \mathbb{Z}$ and hence $g + h = 6(n + m)$ is an integer multiple of 6. Therefore $g + h \in 6\mathbb{Z}$.

- Is $+$ associative in $6\mathbb{Z}$?

  In general we never have to prove this property since $6\mathbb{Z} \subset \mathbb{Z}$ and therefore $+$ inherits associativity from $\mathbb{Z}$.

- Does $6\mathbb{Z}$ contain the identity element?

  In our case we need to show the identity element is a multiple of 6. The additive identy of $\mathbb{Z}$ is $0 = 6 \cdot 0$, so $0 \in 6\mathbb{Z}$.

- Does every element in $6\mathbb{Z}$ have an inverse in $6\mathbb{Z}$ (i.e., is $6\mathbb{Z}$ is "closed under inverses")?

  Suppose $g \in 6\mathbb{Z}$, and write $g = 6n$ for some integer n. Then $g + (-g) = (6n) + (-6n) = 0 = (-6n) + (6n)$. We conclude $-g = -6n$. And, $-g = -6n = 6(-n) \in 6\mathbb{Z}$.

$\square$

The following is a shortcut for proving a subset is a subgroup.

Proposition 1

Suppose $G = (G, \star)$ is a group and H is a non-empty subset of G. Then $H < G$ if $gh^{-1} \in H$ for every $g, h \in H$.

Question

Why do we suppose H is non-empty?

Exercise 1

Prove Proposition 1. Is the converse true?

Example 2 (cf. Problem 49)

Suppose H is a subset of $G = (G, \star)$ satisfying the following:

(i) H is closed under $\star$.

(ii) If $g \in H$ then $g^{-1} \in H$.

Then $H < G$.

Proof: Suppose $g, h \in H$. By (i) $h^{-1} \in H$ and by (ii) $gh^{-1} \in H$. It follows from Proposition 1 that $H < G$. $\square$

Exercise 2 (cf. Problem 50)

Let $G = \mathbb{Z}_{12}$, as defined in Exercise **??**. Show that $H = \{0, 3, 6, 9\}$ is a subgroup of G.

Cyclic subgroups

Definition 2

Suppose G is a group and $g \in G$. Define

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

as the **cyclic subgroup** *of G* **generated by** *g.*

Exercise 3

For Definition 2 to make sense, we must check $\langle g \rangle$ actually is a subgroup.

As alternative notation, authors may write $gG = \langle g \rangle$ to denote the subgroup in G generated by g (see Example 1).

Example 3

For any integer k, the subgroup $k\mathbb{Z} < \mathbb{Z}$ is cyclic.

(Recall, from Section **??**, the subgroups $0\mathbb{Z} < \mathbb{Z}$ and $1\mathbb{Z} < \mathbb{Z}$.)

Question

What is $0\mathbb{Z}$? What is $1\mathbb{Z}$?

We can define subgroups with more than one generator, though we do not describe such subgroups as cyclic.

Definition 3

Let $S = \{s_1, \ldots, s_k\}$ denote some set of elements in the group G. The subgroup generated by S is defined as

$$\langle S \rangle := \{s_1^{n_1} \cdots s_k^{n_k} \mid n_i \in \mathbb{Z} \text{ for all } i = 1, \ldots k\}.$$

Elements in $\langle S \rangle$ are called **words**.

Question

How would you rewrite Definition 3 in additive notation?

Exercise 4 (cf. Problem 51)

Prove $\langle S \rangle$ in Definition 3 is a subgroup of G.

Example 4 (cf. Problem 52)

In $\mathbb{Z}_{12}$, we list the elements of the subgroup $H = \langle 2, 3 \rangle$ by writing down **$\mathbb{Z}$-linear combinations** of the generators, i.e., all possible elements of the form $n_1 \cdot 2 + n_2 \cdot 3$ for $n_1, n_2 \in \mathbb{Z}$:

$$
\begin{array}{llll}
1 \cdot 2 + 0 \cdot 3 = 2 & 0 \cdot 2 + 1 \cdot 3 = 3 & 1 \cdot 2 + 1 \cdot 3 = 5 & (-1) \cdot 2 + 1 \cdot 3 = 1 \\
2 \cdot 2 + 0 \cdot 3 = 4 & 0 \cdot 2 + 3 \cdot 3 = 9 & 2 \cdot 2 + 1 \cdot 3 = 7 & \\
3 \cdot 2 + 0 \cdot 3 = 6 & & 4 \cdot 2 + 1 \cdot 3 = 11 & \\
4 \cdot 2 + 0 \cdot 3 = 8 & & & \\
5 \cdot 2 + 0 \cdot 3 = 10 & & & \\
6 \cdot 2 + 0 \cdot 3 = 0 & & &
\end{array}
$$

Having exhausted all possible elements, we conclude $\langle 2, 3 \rangle = \mathbb{Z}_{12}$.