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 $g + h \in 6\mathbb{Z}$:

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

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, $-g = -6n = 6(-n) \in 6\mathbb{Z}$.

$\square$

Example 1 also holds when we replace 6 with any integer k (see also, Example 3).

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: We must verify the group axioms. Item (i) implies $\star$ is binary on H and associativity is inherited from G. We must check the identity element e is in H. From (ii), if an element g is in H, then so is its inverse. Combine that with (i) then $gg^{-1} = e \in H$. Finally, the existence of inverse elements is given by (i). $\square$

Quicker 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

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

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 $n_1, n_2 \in \mathbb{Z}$:

$1 \cdot 2 + 0 \cdot 3 = 2$	$0 \cdot 2 + 1 \cdot 3 = 3$	$1 \cdot 2 + 1 \cdot 3 = 5$	$(-1) \cdot 2 + 1 \cdot 3 = 1$
$2 \cdot 2 + 0 \cdot 3 = 4$	$0 \cdot 2 + 3 \cdot 3 = 9$	$2 \cdot 2 + 1 \cdot 3 = 7$	
$3 \cdot 2 + 0 \cdot 3 = 6$		$4 \cdot 2 + 1 \cdot 3 = 11$	
$4 \cdot 2 + 0 \cdot 3 = 8$			
$5 \cdot 2 + 0 \cdot 3 = 10$			
$6 \cdot 2 + 0 \cdot 3 = 0$			

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

Solutions to exercises

Exercise 1 (cf. notes)

Solution: Take $g, h \in H$. We shall exploit the hypothesis statement: $gh^{-1} \in H$. In the case where $g = h$, we have $gg^{-1} = e \in H$. Using the hypothesis again, $e, h \in H$ implies $eh^{-1} = h^{-1} \in H$. Therefore every element in H has an inverse in G. Finally, we must show closure of the binary operation, i.e., that $gh \in H$. Since $h \in H$, so is h^{-1}. Then the hypothesis says $g(h^{-1})^{-1} = gh \in H$. $\square$

The converse states that if H is a subgroup then for all $g, h \in H$, we have $gh^{-1} \in H$. This statement is **true** and follows directly from the group axioms for H.

Exercise 2 (cf. Problem 50)

Solution: By Example 2 it suffices to show closure under $\oplus_{12}$ and the presence of inverse elements. H consists of multiples of 3 modulo 12, and so adding two of them results in a multiple of 3 as well. The inverses are $-0 = 0$, $-3 = 9$, $-6 = 6$. $\square$

Exercise 3

Solution: We appeal to Example 2. Take $g^n, g^m \in \langle g \rangle$. Then $g^n g^m = g^{n+m} \in G$, i.e., $\langle g \rangle$ is closed under the operation in G. For inverses, the definition of $\langle g \rangle$ includes inverses, since $(g^n)^{-1} = g^{-n}$. $\square$

Exercise 4 (cf. Problem 51)

Solution: We modify the arguments used in Exercise 3. If $s_1^{n_1} \cdots s_k^{n_k}$ and $s_1^{m_1} \cdots s_k^{m_k}$ are in $\langle S \rangle$, then their product is

$$(s_1^{n_1} \cdots s_k^{n_k}) \cdot (s_1^{m_1} \cdots s_k^{m_k}) = s_1^{n_1+m_1} \cdots s_k^{n_k+m_k} \in \langle S \rangle.$$

For the presence of inverses, put

$$s := (s_1^{n_1} \cdots s_k^{n_k})^{-1} = s_k^{-n_k} \cdots s_1^{-n_1}.$$

By definition, each of $s_i^{-n_i} \in \langle S \rangle$, for $i = 1, \ldots, k$. Since we showed closure under the group operation, $s \in \langle S \rangle$. $\square$