Subgroups

**Definition:** Let \((G, \cdot)\) be a group. A subset \(H\) of \(G\) is called a **subgroup** of \(G\), if it has the following three properties:

(i) \(1 \in H\), the identity element of \(G\) is in \(H\).

(ii) \(a, b \in H\), \(ab \in H\), \(H\) is closed under the binary operation in \(G\).

(iii) \(a \in H\), \(a^{-1} \in H\), \(H\) is closed under inversion.

If \(H\) is a subgroup of \(G\), we indicate this by the notation

\[ H \leq G \quad \text{or} \quad H \subseteq G \text{ subgroup}. \]

If \(H\) is a subgroup of \(G\) and \(H \neq G\), then we call \(H\) a **proper subgroup** of \(G\).

The subgroup \(H = \{ e \}\) is called the **trivial subgroup** of \(G\).

**Remark:** A subgroup \(H\) of \(G\) is a group in its own right with the binary operation of \(G\) restricted to \(H\).

**Examples:**

1. \( \mathbb{Z} \) is a subgroup of \((\mathbb{Q}, +)\).

2. \( H = \{0 + 4\mathbb{Z}, 2 + 4\mathbb{Z}\} \subseteq \mathbb{Z}/4\mathbb{Z}\) is a subgroup of \(0 + 4\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z}\) if, and only if, the identity is there:

   \[
   \begin{align*}
   0 + 4\mathbb{Z} + 2 + 4\mathbb{Z} &\in 0 + 4\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} \\
   2 + 4\mathbb{Z} + 2 + 4\mathbb{Z} &\in 4 + 4\mathbb{Z} \subseteq 0 + 4\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} \\
   0 + 4\mathbb{Z} + 0 + 4\mathbb{Z} &\in 0 + 4\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z}
   \end{align*}
   \]

   \(-2 + 4\mathbb{Z} = 2 + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}\) is closed under inversion.

   \[ S = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}\} \subseteq \mathbb{Z}/4\mathbb{Z}\] is not a subgroup because \(S\) is not closed under the binary operation: \(1 + 4\mathbb{Z} + 2 + 4\mathbb{Z} = 3 + 4\mathbb{Z} \notin S\).

3. If \( M \subseteq N \), then the subset \( M / 4\mathbb{Z} = \{a + 4\mathbb{Z} : a \in M\} \) is a subgroup of \((\mathbb{Z}/4\mathbb{Z}, +)\).

4. If \( V \) is a vector space, then \((V, +)\) is a group, and if \(W \subseteq V\) is a subgroup, then \(W\) is a subgroup of \((V, +)\).
Prop. Let \( H, K \leq G \) be subgps of \( G \). Then \( HNK \leq G \) is a subgp of \( G \).

Proof:
1. \( I_G \in H \) and \( I_G \in K \) because \( H, K \) are subgps of \( G \). Therefore \( I_G \in HNK \).
2. Let \( x, y \in HNK \). Then \( xy \in H \) because \( H \) is a subgp of \( G \) and \( xy \in K \) because \( K \) is a subgp of \( G \). Therefore \( xy \in HNK \).
3. Let \( x \in HNK \). Then \( x^{-1} \in H \) because \( H \) is a subgp of \( G \) and \( x^{-1} \in K \) because \( K \) is a subgp of \( G \). Hence \( x^{-1} \in HNK \). \( \square \)

Remark: The proposition generalizes to any collection of subgps of \( G \).

Prop: Let \( G \) be a gp and let \( a \) be an element of \( G \). Then the subset \( H = \{ \alpha \in \mathbb{Z}^+ \mid \alpha a^n \in G \} \) is a subgp \( \leq G \) which contains \( a \). Moreover, \( H \) is the intersection of all subgps containing \( a \).

Proof:
1. \( a^0 = I_G \in H \)
2. Let \( x, y \in H \). Then \( x = a^m \) and \( y = a^n \) for some \( m, n \in \mathbb{Z} \), so \( xy = a^{m+n} \in H \).
3. Let \( x = a^n \in H \). Then \( x^{-1} = a^{-n} \in H \).

Therefore \( H \) is a subgp of \( G \).
Now we show that

\[ H = \bigcap_{K \in \mathcal{K}} K \]

\[ \text{if } a \in H, \text{ so } \bigcap_{K \in \mathcal{K}} K \subseteq H \quad \text{(by one of the } K's) \]

Conversely, if \( a \in \cap_{K \in \mathcal{K}} K \), then

1. \( a = 1a \in K \) because \( K \) is a subgroup, so has 1.
2. \( a^n \in \cap_{K \in \mathcal{K}} K \) because \( K \) is closed under group operation.
3. \( a^n = (a^n) \) for \( n \geq 0 \) because \( K \) is closed under inversion.

Therefore \( H = \bigcap_{K \in \mathcal{K}} K \), so \( H = \bigcap_{K \in \mathcal{K}} K \).

Hence \( H \) is the intersection of all the subgroups containing \( a \). \( \square \)

---

**Def:** Let \( G \) be a group.

1. For every element \( a \in G \), the subgroup \( \langle a \rangle = \{ a^n : n \in \mathbb{Z} \} \) is called the **subgroup generated by** \( a \) and is denoted by \( \langle a \rangle \). \( \langle a \rangle \) is the smallest subgroup of \( G \) containing \( a \).
2. A group \( G \) is called **cyclic** if \( \exists a \in G \) such that \( G = \langle a \rangle \). In this case, \( a \) is called a **generator** of \( G \).

**Note:** If \( G \) is a cyclic group there may be more than one generator of \( G \).
Prop: Every cyclic group is abelian.

Proof: Let $G$ be a cyclic group, so $G = \langle a \rangle$ for some $a \in G$. Let $xy \in G$.
Then $x = a^n$ and $y = a^m$ for some $n, m \in \mathbb{Z}$ and so
$$xy = a^n a^m = a^{n+m} = a^m a^n = yx$$

Example 1: $\mathbb{Z} = \langle 17 \rangle$. This is because for $n \in \mathbb{Z}$, $n = n \cdot 1$. Also, $\langle -1 \rangle = \langle 17 \rangle$.

2. $\mathbb{Z}/\mathbb{Z} = \langle 1 + \mathbb{Z} \rangle$. This is because for $m + n \in \mathbb{Z}/\mathbb{Z}$,
$$m + n \mathbb{Z} = m(1 + n \mathbb{Z})$$

Def: Let $G$ be a group.
(a) For any non-empty subset $X$ of $G$, we define $\langle X \rangle$ as the set of all elements of $G$ of the form
$$x_1 x_2 \cdots x_n$$
where $n \in \mathbb{N}$, $x_1, \ldots, x_n \in X$, and $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$. We extend this definition to the empty subset of $G$ by setting $\langle \phi \rangle = \{1_G\}$. We will prove that $\langle X \rangle$ is a subgroup of $G$, it is called the subgroup generated by $X$.
(b) If $X$ is a subset of $G$ such that $\langle X \rangle = G$, then we call $X$ a generating set of $G$. 
Prop: Let $X$ be a subset of a gp $G$. Then:
(a) $\langle X \rangle$ is a subgp of $G$ containing $X$.
(b) If $K$ is a subgp of $G$ and $X \subseteq K$, then $\langle X \rangle \subseteq K$.
(c) $\langle X \rangle = \bigcap_{K \leq G} X \subseteq K$

Proof: If $X = \emptyset$, then $\langle X \rangle = \{1_G\}$ and (a) - (c) are easy to verify.

Assume $X \neq \emptyset$.

(a) First $x \in \langle X \rangle$. Let $x \in X$. Then $x = x_1^n$ so $x \in \langle X \rangle$ by def of $\langle X \rangle$.

Now that $\langle X \rangle$ is a subgp of $G$.

1. Identity: $X \neq \emptyset$ implies $\exists x \in X$. Then $1_G = x \cdot x^{-1} \in \langle X \rangle$.

2. Closure: Let $y, z \in \langle X \rangle$. Then

$$y = y_{e_1}^{e_1} \cdots y_{e_n}^{e_n}$$
$$z = z_{s_1}^{s_1} \cdots z_{s_m}^{s_m}$$

for some $e_i, s_j \in \{1, \pm 1\}$, $y_i, z_j \in X$. Then

$$yz = y_{e_1}^{e_1} \cdots y_{e_n}^{e_n} z_{s_1}^{s_1} \cdots z_{s_m}^{s_m} \in \langle X \rangle$$

by def of $\langle X \rangle$.

3. Inverses: Let $x = x_{e_1}^{e_1} \cdots x_{e_n}^{e_n} \in \langle X \rangle$. Then

$$x^{-1} = x_{e_1}^{-e_1} \cdots x_{e_n}^{-e_n} \in \langle X \rangle$$
(b) Let \( K \) be a subgp of \( G \) st. \( X \subseteq K \). Then \( K \) contains

1. All elements of \( X \) by assumption.
2. All inverses of elements of \( X \) since \( K \) is closed under inversion.
3. All products of elements of \( X \) and inverses of elements of \( X \) because \( K \) is closed under mult.

Therefore \( \langle X \rangle \subseteq K \).

(c) \( X \subseteq \langle X \rangle \), so \( \bigcap_{K \subseteq G} \langle X \rangle \)

Conversely, by (b), if \( X \subseteq K \), then \( \langle X \rangle \subseteq K \), so

\( \langle X \rangle \subseteq \bigcap_{K \subseteq G} \langle X \rangle \). Hence \( \langle X \rangle = \bigcap_{K \subseteq G} \langle X \rangle \). \( \square \)

Note: By prop, the subgp generated by a set \( X \) is the intersection of all gps containing \( X \).

Def: Let \( f : G \to H \) be a gp hom. Define the kernel of \( f \) to be the set

\[ \ker(f) = \{ g \in G : f(g) = e_H \} \]

Prop: \( \ker(f) \) is a subgp of \( G \) and \( \text{im}(f) \) is a subgp of \( H \).

Proof: 1. Identity: \( f(e_G) = e_H \), so \( e_G \in \ker(f) \).
2. Closed under mult: Let \( xy \in \ker(f) \), then

\[ f(xy) = f(x)f(y) = e_H e_H = e_H \]

so \( xy \in \ker(f) \).
3. Closed under inversion: Let \( x \in \ker(f) \), then \( f(x^{-1}) = f(x)^{-1} = e_H \), so \( x^{-1} \in \ker(f) \).
Example: Define

$$\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

$$a \mapsto a + n\mathbb{Z}$$

$$\pi$$ is a group homomorphism:

$$\pi(a + b) = \pi(a) + \pi(b)$$

$$= a + n\mathbb{Z} + b + n\mathbb{Z}$$

$$= \pi(a) + \pi(b)$$

$$\ker(\pi) = \{ a \in \mathbb{Z} : \pi(a) = 0 + n\mathbb{Z} \}$$

$$\pi(a) = a + n\mathbb{Z}, \quad a + n\mathbb{Z} = 0 + n\mathbb{Z}$$

if and only if $$a \equiv 0 \mod n$$

if and only if $$n$$ divides $$a$$.

$$\ker(\pi) = n\mathbb{Z} = \{ kn : k \in \mathbb{Z} \}$$

Example: Vector space.

Let $$V$$ be a vector space. Then

$$\{ v_i \} \subset V$$

is a basis for $$V$$ if and only if

$$\forall x \in V : x = \sum_{i=1}^{n} a_i v_i, \quad a_i \in \mathbb{R}$$

$$\{ v_i \} \subset V$$

is a basis for $$V$$ if and only if

$$\text{Span} \{ v_1, \ldots, v_n \} = V$$.
Example: Symmetric Group

Let $X = \{1, 2, \ldots, n\}$. Then $\text{Sym}(X)$ is denoted $\text{Sym}(n)$ or $S_n$, and called the symmetric group.

Elements of $\text{Sym}(n)$ are bijections

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

Composition of functions makes $\text{Sym}(n)$ a group.

Representing elements of $\text{Sym}(5)$: Let $\sigma \in \text{Sym}(5)$

$$\sigma : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$$

1. $\sigma(1) = \text{can be anything}$
2. $\sigma(2) = \text{anything but } \sigma(1)$
3. $\sigma(3) = \text{anything but } \sigma(1), \sigma(2)$
4. $\sigma(4) = \text{anything but } \sigma(1), \sigma(2), \sigma(3)$
5. $\sigma(5) = \text{element that is left}$

There are $5!$ elements of $\text{Sym}(5)$.

Let $\sigma, \tau \in \text{Sym}(5)$ be two elements, $\tau \in \text{Sym}(5)$

$$\sigma : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}, \quad \tau : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}, \quad \tau \circ \sigma : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$$

\[
\begin{align*}
\sigma(1) &= 3 \\
\sigma(2) &= 4 \\
\sigma(3) &= 1 \\
\sigma(4) &= 2 \\
\sigma(5) &= 5
\end{align*}
\]

\[
\begin{align*}
\tau(1) &= 1 \\
\tau(2) &= 3 \\
\tau(3) &= 2 \\
\tau(4) &= 9 \\
\tau(5) &= 5
\end{align*}
\]

Represent $\sigma$ as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$