Subgroups

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

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

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

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

If H is a subgp of G, we indicate this by the notation

$$H \leq G \quad \text{or} \quad H \subseteq G \text{ subgp.}$$

If H is a subgp of G and $H \neq G$, then we call H a proper subgp of G.

The subgp $H = \{1_G\}$ is called the trivial subgp of G.

Remark: A subgp 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 subgp of $(\mathbb{Q},+)$.

2. $H = \{0+4\mathbb{Z}, 2+4\mathbb{Z}\} \subseteq \mathbb{Z}/4\mathbb{Z}$ is a subgp: $0+4\mathbb{Z} \in H$ identity is there

$$\left.\begin{array}{l} 0+4\mathbb{Z} + 2+4\mathbb{Z} = 2+4\mathbb{Z} \in H \\ 2+4\mathbb{Z} + 2+4\mathbb{Z} = 4+4\mathbb{Z} = 0+4\mathbb{Z} \in H \\ 0+4\mathbb{Z} + 0+4\mathbb{Z} = 0+4\mathbb{Z} \in H \end{array}\right\} \text{closed under binary operation}$$

$-2+4\mathbb{Z} = 2+4\mathbb{Z} \in H$ 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 subgp because is not closed under the binary operation: $1+4\mathbb{Z} + 2+4\mathbb{Z} = 3+4\mathbb{Z} \notin S$.

3. If $m \in \mathbb{N}$, then the subset $m\mathbb{Z} := \{ma : a \in \mathbb{Z}\}$ is a subgp of $(\mathbb{Z},+)$.

4. If V is a vector space, then $(V,+)$ is a gp, and if $W \subseteq V$ is a subspace, then W is a subgp of $(V,+)$.

Prop: ~~H,K ≤ G subgp~~ Let $H, K \le G$ be subgps of G. Then $H \cap K \le G$ is a subgp of G.

proof: 1. $1_G \in H$ and $1_G \in K$ because H, K are subgps of G. Therefore $1_G \in H \cap K$.

2. Let $x, y \in H \cap K$. Then $xy \in H$ because H is a subgp of G and $xy \in K$ because K is a subgp of G. Therefore $xy \in H \cap K$.

3. Let $x \in H \cap K$. 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 $x^{-1} \in H \cap K$. $\square$

Remark: The proposition generalizes to the intersection of any collection of subgps of G.

Do the notation stuff from earlier.

Prop: Let G be a gp and let a be an element of G. Then the subset

$$H := \{ a^n : n \in \mathbb{Z} \}$$

is a subgp of G which contains a. Moreover, H is the intersection of all subgps containing containing a.

proof: 1. $a^0 = 1_G \in H$

2. Let $x, y \in H$. Then $x = a^n$, $y = a^m$ for some n, m, so $xy = a^{n+m} \in H$.

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

$$H = \bigcap_{\substack{a \in K \\ \text{and } K \le G}} K$$

$a \in H$, so $\bigcap_{\substack{a\in K \\ K \le G}} K \subseteq H$ (H is one of the K's)

Conversely, if $a \in K$, and K is a subgp of G, then

1. $a^0 = 1_G \in K$ because K is a subgp, so has id.
2. $a^n \in K$ $\forall n > 0$ because K is closed under gp operation.
3. $a^{-n} = (a^n)^{-1}$ $\forall n > 0$ because K is closed under inversion.

Therefore $H \subseteq K$, so $H \subseteq \bigcap_{\substack{a \in K \\ K \le G}} K$.

Hence H is the intersection of all the subgps containing a. $\square$

Def: Let G be a gp.

(a) For every element $a \in G$, the subgp $\{a^n : n \in \mathbb{Z}\}$ is called the subgp generated by a and is denoted by $\langle a \rangle$. $\langle a \rangle$ is the smallest subgp of G containing a.

(b) A gp 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 gp there may be more than one generator of G.

Prop: Every cyclic gp is abelian.

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

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$$

Example 1. $\mathbb{Z} = \langle 1 \rangle$. This is because for $n \in \mathbb{Z}$, $n = n1$. Also have $\mathbb{Z} = \langle -1 \rangle$.

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

$$m + n\mathbb{Z} = m(1 + n\mathbb{Z}).$$

~~Prop: Let X be a subset of a gp G~~

Def: Let G be a gp.

(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

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$$

where $n \in \mathbb{N}$, $x_1, \dots, x_n \in X$, and $\varepsilon_1, \dots, \varepsilon_n \in \{1, -1\}$. 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 subgp of G, it is called the <u>subgp generated by X</u>.

(b) If X is a subset of G such that $\langle X \rangle = G$, then we call X a <u>generating set</u> 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) $$\langle X \rangle = \bigcap_{X \subseteq K \leq G} K$$

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

Assume $X \neq \phi$.

(a) First $X \subseteq \langle X \rangle$. Let $x \in X$. Then $x = x^1$, so $x \in \langle X \rangle$ by def. of $\langle X \rangle$.

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

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

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

$$y = y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}$$
$$z = z_1^{\delta_1} \cdots z_m^{\delta_m}$$

for some $\varepsilon_i, \delta_j \in \{\pm 1\}$, $y_i, z_j \in X$. Then.

$$yz = y_1^{\varepsilon_1} y_2^{\varepsilon_2} \cdots y_n^{\varepsilon_n} z_1^{\delta_1} \cdots z_m^{\delta_m} \in \langle X \rangle$$

by def of $\langle X \rangle$.

3. Inverses: Let $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \langle X \rangle$. Then

$$x^{-1} = x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1} \in \langle X \rangle$$

(b) Let K be a subgp of G s.t. $X \subseteq K$. 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 $\bigcap_{X \subseteq K \leq G} K \subseteq \langle X \rangle$

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

$\langle X \rangle \subseteq \bigcap_{X \subseteq K \leq G} K$. Hence $\langle X \rangle = \bigcap_{X \subseteq K \leq G} K$. $\square$

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 $\operatorname{im}(f)$ is a subgp of H.

proof: 1. Identity: $f(e_G) = e_H$, so $e_G \in \ker(f)$.

2. Closed under mult: Let $x, y \in \ker(f)$, 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 $f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in \ker(f)$.

Example: Define

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$a \longmapsto a + n\mathbb{Z}$$

π is a gp hom:

$$\pi(a+b) = (a+b) + n\mathbb{Z}$$
$$= a+n\mathbb{Z} + b+n\mathbb{Z}$$
$$= \pi(a) + \pi(b)$$

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

$\pi(a) = a+n\mathbb{Z}$, $a+n\mathbb{Z} = 0+n\mathbb{Z}$ iff $a \equiv 0 \mod n$

iff n divides a.

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

~~Example: V - vector space (over R), [illegible] is (V, +) is a gp~~

~~Let $v_1, \dots, v_k \in V$. Then~~

~~$\langle v_1, \dots, v_k \rangle = \{ \sum_{i=1}^{k} \lambda_i v_i : \lambda_i \in \mathbb{R} \} = \mathrm{Span}(v_1, \dots, v_k)$~~

Example: Symmetric Group

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

Elements of $Sym(n)$ are bijections

$$\sigma : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$$

Composition of functions ~~may~~ makes $Sym(n)$ a group.

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

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

$1 \longmapsto \sigma(1) =$ can be anything — 5 choices

$2 \longmapsto \sigma(2) =$ anything but $\sigma(1)$ — 4 choices

$3 \longmapsto \sigma(3) =$ anything but $\sigma(1), \sigma(2)$ — 3 choices

$4 \longmapsto \sigma(4) =$ anything but $\sigma(1), \sigma(2), \sigma(3)$ — 2 choices

$5 \longmapsto \sigma(5) =$ element that is left — 1 choice

There are $5!$ elements of $Sym(5)$.

Let $\sigma \in Sym(5)$ be the element, $\tau \in Sym(5)$

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

$\sigma(1) = 3$	$\tau(1) = 1$	$\tau \circ \sigma(1) = 2$
$\sigma(2) = 4$	$\tau(2) = 3$	$\tau \circ \sigma(2) = 4$
$\sigma(3) = 1$	$\tau(3) = 2$	$\tau \circ \sigma(3) = 1$
$\sigma(4) = 2$	$\tau(4) = 4$	$\tau \circ \sigma(4) = 3$
$\sigma(5) = 5$	$\tau(5) = 5$	$\tau \circ \sigma(5) = 5$

represent σ as

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