Subgroups

Suppose G is a group. (written multiplicatively) We say that a non-empty subset $H \subseteq G$ is a **subgroup** of G if:

i) $\forall g, h \in H$, $gh \in H$, and (closed under multiplication)

ii) $\forall g \in H$, $g^{-1} \in H$. (closed under inverses)

Notation: $H \leqslant G$

These conditions guarantee that H is a group with respect to the binary operation on G:

- Condition i) guarantees that the restriction of the binary operation to H is well defined.
  - Associativity in $(H, \cdot)$: follows from associativity in $(G, \cdot)$.
- Existence of identity: ($e_H = e_G$)

$$H \text{ is nonempty} \Rightarrow \exists g \in H$$

$$\text{Condition ii)} \Rightarrow g^{-1} \in H$$

$$\text{Condition i)} \Rightarrow gg^{-1} = e_G \in H$$

$$\forall h \in H, \quad e_G h = h e_G = h$$

- Existence of inverses: follows from condition ii).

Exs:

1a) $G = \mathbb{Z}$, $H = 2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$

$\forall g, h \in H$, $\exists k, \ell \in \mathbb{Z}$ s.t. $g = 2k$, $h = 2\ell$.

So $g + h = 2(k + \ell) \in H$ ✓

and $-g = 2(-k) \in H$ ✓

1b) $G = \mathbb{Z}$, $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, where $n \in \mathbb{Z}$.

2) $G = C_6 = \langle x : x^6 = e \rangle = \{e, x, x^2, x^3, x^4, x^5\}$

$H_1 = \{e, x^3\}$, $H_2 = \{e, x^2, x^4\}$

3) $G = V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$

$= \{e, a, b, ab\}$

$H_1 = \{e, a\}$, $H_2 = \{e, b\}$, $H_3 = \{e, ab\}$

4) $G = D_{2n} = \langle r, s \mid r^n = s^2 = e, rs = sr^{-1} \rangle$ $(n \geq 3)$

$= \{e, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$

$H_1 = \{e, r, r^2, \ldots, r^{n-1}\}$

$H_2 = \{e, s\}$ (... and more)

Some facts and terminology:

Let G be a group.

1) $G \leq G$ and $\{e\} \leq G$. (trivial subgroup)

2) If $H \leq G$ and $H \neq G$ then H is called a proper subgroup of G.

3a) Subgroup criterion:

If $H \subseteq G$ is non-empty then

$H \leq G$ if and only if $\forall g, h \in H$, $gh^{-1} \in H$.

Pf: $H \neq \phi \Rightarrow \exists g \in H$. Then:

- $e = gg^{-1} \in H$.
- $\forall h \in H$, $h^{-1} = eh^{-1} \in H$. (closed under inverses)
- $\forall g, h \in H$, $h^{-1} \in H$, so $g(h^{-1})^{-1} = gh \in H$. $\blacksquare$
(closed under mult.)

3b) Subgroup criterion for finite sets

If $H \subseteq G$ is non-empty and $|H| < \infty$ then

$H \leq G$ if and only if $\forall g, h \in H$, $gh \in H$.

Pf: Only need to show that H is closed under taking inverses. For any $g \in H$, $\{g, g^2, g^3, \ldots\} \subseteq H$. But $|H| < \infty \Rightarrow \exists\, i, j \in \mathbb{N}$, $j \geq i+2$, with $g^i = g^j$. Then $g \cdot g^{j-i-1} = g^{j-i} = e \Rightarrow g^{-1} = g^{j-i-1}$,

and $j-i-1 \geq 1 \Rightarrow g^{j-i-1} \in H$. ∎

4) Intersections of subgroups of G are subgroups:

If $\{H_i\}_{i \in I}$ is a non-empty collection of subgroups of G, then $\bigcap_{i \in I} H_i$ is also a subgroup of G.

Pf: Write $H = \bigcap_{i \in I} H_i$. Then:

- $\forall i \in I$, $e \in H_i \Rightarrow e \in H \Rightarrow H \neq \emptyset$.
- If $g, h \in H$ then, since $g, h \in H_i$, $\forall i \in I$, we have that $gh^{-1} \in H_i$, $\forall i \in I$. (subgroup crit.)
  Therefore $gh^{-1} \in H$.

It follows from the subgroup criterion that $H \leq G$. ∎

Subgroup generated by a subset

If $S \subseteq G$ then the <u>subgroup generated by S</u>, denoted $\langle S \rangle$ is the intersection of all subgroups of G which contain S.

- Since $S \subseteq G$, there is always at least one subgroup of G containing S, so $\langle S \rangle \leq G$.
- $\langle S \rangle$ is the smallest subgroup of G containing S, in the sense that,

$$\text{if } H \leq G \text{ and } S \subseteq H, \text{ then } \langle S \rangle \leq H.$$

- If $S = \{g_1, \dots, g_n\}$ then we also write

$$\langle S \rangle = \langle g_1, \dots, g_n \rangle.$$

This is consistent with our previous notation $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$, $(g \in G)$.

(cyclic subgroup generated by g)

- If $G = \langle S \rangle$ for a finite set $S \subseteq G$, then we say that G is <u>finitely generated</u>.

Note: $|G| < \infty \Rightarrow G$ finitely generated $(G = \langle G \rangle)$

However, in general,

$$|G| = \infty \not\Rightarrow G \text{ not finitely generated}.$$

Exs:

0) For any group G, if we take $S=\phi$, then $\langle S\rangle=\{e\}$.

1) $G=\mathbb{Z}$, $H=n\mathbb{Z}=\{nk : k\in\mathbb{Z}\}=\langle n\rangle$, $(n\in\mathbb{Z})$.

(Note: $|G|=\infty$ but G is finitely generated.)

2) $G=C_6=\{e, x, x^2, x^3, x^4, x^5\}=\langle x\rangle$

$H_1=\{e, x^3\}=\langle x^3\rangle$ $\quad ((x^4)^2=x^8=x^2)$

$H_2=\{e, x^2, x^4\}=\langle x^2\rangle=\langle x^4\rangle$

3) $G=V_4=\{e, a, b, ab\}=\langle a,b\rangle$

$H_1=\{e, a\}=\langle a\rangle$

$H_2=\{e, b\}=\langle b\rangle$

$H_3=\{e, ab\}=\langle ab\rangle$

4) $G=D_{2n}=\{e, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}=\langle r,s\rangle$

$H_1=\{e, r, r^2, \dots, r^{n-1}\}=\langle r\rangle$

$H_2=\{e, s\}=\langle s\rangle$

5) $\mathbb{Q}$ is not finitely generated

Pf: Suppose $S = \{r_1, r_2, \ldots, r_n\} \subseteq \mathbb{Q}$, write $r_i = \frac{p_i}{q_i}$, with $p_i \in \mathbb{Z}$, $q_i \in \mathbb{N}$. Let

$$H = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n : a_1, \ldots, a_n \in \mathbb{Z}\}.$$

Then:
- $H \leq \mathbb{Q}$ (subgroup crit.)
- $S \subseteq H \Rightarrow \langle S \rangle \leq H$ (def. of $\langle S \rangle$)
- $H \subseteq \langle S \rangle$ (subgroup crit. applied to $\langle S \rangle$)

Therefore $\langle S \rangle = H$.

Now let $q = \operatorname{lcm}(q_1, \ldots, q_n)$. Then $\forall x \in H$, since

$$x = \sum_{i=1}^{n} a_i \left(\frac{p_i}{q_i}\right) \quad \text{for some } a_1, \ldots, a_n \in \mathbb{Z},$$

we have that

$$qx = \sum_{i=1}^{n} a_i p_i \underbrace{\left(\frac{q}{q_i}\right)}_{\in \mathbb{Z}} \in \mathbb{Z}.$$

But then, since $q \cdot \left(\frac{1}{2q}\right) = \frac{1}{2} \notin \mathbb{Z}$, we find that $\frac{1}{2q} \notin H \Rightarrow H \neq \mathbb{Q}$. $\blacksquare$

Thm: If G is a group and $S \subseteq G$ then

$$\langle S \rangle = \{ \underbrace{g_1^{u_1} g_2^{u_2} \cdots g_n^{u_n}}_{\text{(order matters, in general)}} : n \in \mathbb{N}, \underbrace{g_1, \ldots, g_n}_{\text{(not necessarily distinct)}} \in S, u_1, \ldots, u_n \in \{\pm 1\} \}.$$

Pf: Let $H = \{ g_1^{u_1} g_2^{u_2} \cdots g_n^{u_n} : n \in \mathbb{N}, g_1, \ldots, g_n \in S, u_1, \ldots, u_n \in \{\pm 1\} \}$.

Then:
- $H \leq G$ (subgroup crit.)
- $S \subseteq H \Rightarrow \langle S \rangle \subseteq H$ (def. of $\langle S \rangle$)
- $H \subseteq \langle S \rangle$ (subgroup crit. applied to $\langle S \rangle$)

Therefore $\langle S \rangle = H$. ∎

Cor: If G is Abelian and $S \subseteq G$ then

$$\langle S \rangle = \{ g_1^{a_1} \cdots g_n^{a_n} : g_1, \ldots, g_n \in S, a_1, \ldots, a_n \in \mathbb{Z}, g_i \neq g_j \text{ for } i \neq j \}.$$

In particular, if $S = \{g_1, \ldots, g_n\}$ then

$$\langle S \rangle = \{ g_1^{a_1} \cdots g_n^{a_n} : a_1, \ldots, a_n \in \mathbb{Z} \}.$$

Cyclic subgroups and orders of elements

If $g \in G$ then the order of g, denoted $|g|$ or $o(g)$, is defined to be the smallest $k \in \mathbb{N}$ satisfying $g^k = e$, or ∞ if there is no such k.

Exs: 1) $G = C_6 = \{e, x, x^2, x^3, x^4, x^5\} = \langle x \rangle$

$|e| = 1$

$|x| = 6$

$|x^2| = 3$ $\quad (x^2)^1 = x^2, \quad (x^2)^2 = x^4, \quad (x^2)^3 = x^6 = e$

$|x^3| = 2$ $\quad (x^3)^1 = x^3, \quad (x^3)^2 = x^6 = e$

$|x^4| = 3$ $\quad (x^4)^1 = x^4, \quad (x^4)^2 = x^8 = x^2, \quad (x^4)^3 = x^{12} = e$

$|x^5| = 6$ $\quad x^5 = x^{-1} \Rightarrow (x^5)^i = x^{-i}, \quad 1 \le i \le 6$

x^5, x^4, x^3, x^2, x, e

2) $G = D_6 = \langle r, s \mid r^3 = s^2 = e, \; rs = sr^{-1} \rangle = \{e, r, r^2, s, sr, sr^2\}$

$|e| = 1, \quad |r| = |r^2| = 3, \quad |s| = 2$

$|sr| = 2$

$$(sr)^2 = (sr)(sr) = s(rs)r = s(sr^{-1})r = s^2(r^{-1}r) = e.$$

$|sr^2| = 2$

$r^2s = r(rs) = r(sr^{-1}) = (rs)r^{-1} = sr^{-2}$

$$(sr^2)^2 = (sr^2)(sr^2) = s(r^2s)r^2 = s^2r^{-2}r^2 = e$$

3) $G=\mathbb{Z}$, $n\in\mathbb{Z}$, $|n|=\begin{cases} 1 & \text{if } n=0, \\ \infty & \text{if } n\neq 0. \end{cases}$

Theorem: $\forall g\in G$, $|g|=|\underbrace{\langle g\rangle}_{=\{g^n:\, n\in\mathbb{Z}\}}|$. More precisely:

i) If $|g|=\infty$ then $g^i\neq g^j$, $\forall\, i,j\in\mathbb{Z}$ with $i\neq j$.

ii) If $|g|=k\in\mathbb{N}$ then $\langle g\rangle=\{e,g,g^2,\dots,g^{k-1}\}$, and $g^i=g^j$ for $i,j\in\mathbb{Z}$ iff $i\equiv j \bmod k$.

Pf: To prove i), consider the contrapositive. Suppose that $g^i=g^j$ for some $i,j\in\mathbb{Z}$ with $i\neq j$. W.L.O.G., suppose $i<j$. Then $g^{j-i}=e$ and $j-i\in\mathbb{N}$ $\Rightarrow |g|<\infty$. This establishes i).

To prove ii), suppose $|g|=k$ and $g^i=g^j$ for some $i,j\in\mathbb{Z}$. Then $g^{j-i}=e$. By the Division Algorithm, $\exists\, q,r\in\mathbb{Z}$ with $0\le r<k$ s.t. $j-i=qk+r$. Since

$$e=g^{j-i}=g^{qk+r}=(\underbrace{g^k}_{e})^q g^r=g^r,$$

and since k is the smallest element of $\mathbb{N}$ satisfying $g^k=e$, it follows that $r=0$.

Then $j-i=qk \Rightarrow i\equiv j \bmod k$. Therefore $\langle g\rangle=\{e,g,g^2,\dots,g^{k-1}\}$ and $|\langle g\rangle|=k$. $\blacksquare$

(Also, $i\equiv j \bmod k \Rightarrow j-i=qk \Rightarrow g^{j-i}=e \Rightarrow g^j=g^i$)

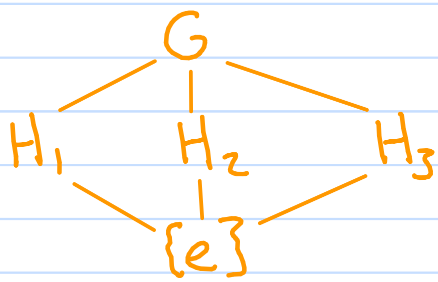
Lattice of subgroups of a group

The **lattice of subgroups** of a group is a diagram illustrating the subgroups of the group.

Exs:

1) $G = V_4 = \{e, a, b, ab\} = \langle a, b \rangle$

$H_1 = \{e, a\} = \langle a \rangle$, $H_2 = \{e, b\} = \langle b \rangle$, $H_3 = \{e, ab\} = \langle ab \rangle$

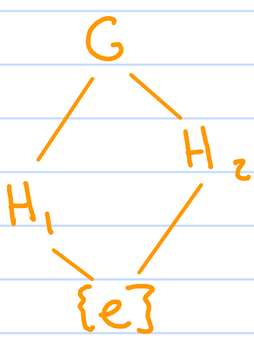


(line segments indicate set containments)

2) $G = C_6 = \{e, x, x^2, x^3, x^4, x^5\} = \langle x \rangle$

$H_1 = \{e, x^3\} = \langle x^3 \rangle$ $(|H_1| = 2)$

$H_2 = \{e, x^2, x^4\} = \langle x^2 \rangle = \langle x^4 \rangle$ $(|H_2| = 3)$



(For finite groups: Relative vertical position indicates differences in order.)

3) $G = D_6 = \langle r, s \mid r^3 = s^2 = e, \; rs = sr^{-1} \rangle = \{e, r, r^2, s, sr, sr^2\}$

$H_1 = \langle r \rangle = \{e, r, r^2\} = \langle r^2 \rangle$

$H_2 = \langle s \rangle = \{e, s\}$

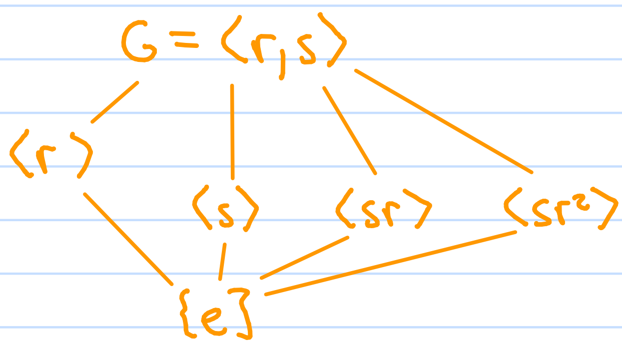
$H_3 = \langle sr \rangle = \{e, sr\}$

$(sr)^2 = (sr)(sr) = s(rs)r = s(sr^{-1})r = s^2(r^{-1}r) = e.$

$H_4 = \langle sr^2 \rangle$

$r^2 s = r(rs) = r(sr^{-1}) = (rs)r^{-1} = sr^{-2}$

$(sr^2)^2 = (sr^2)(sr^2) = s(r^2 s)r^2 = s^2 r^{-2} r^2 = e$



(... next page →)

This is the complete list of subgroups of G because:

- A subgroup $H \leq G$ which contains an element of $\{r, r^2\}$ and an element of $\{s, sr, sr^2\}$ will have to contain $\langle r \rangle$, and therefore also s. Then $\langle r, s \rangle \subseteq H \Rightarrow H = G$.

  Scratch work: $(sr)r^2 = sr^3 = s$

  $(sr^2)r = sr^3 = s$

- A subgroup $H \leq G$ which contains more than one element of $\{s, sr, sr^2\}$ will then have to contain r or r^2, so again $H = G$.

  Scratch work: $s(sr) = s^2 r = r$

  $s(sr^2) = s^2 r^2 = r^2$

  $\underbrace{(sr^2)}_{\text{" } sr^{-1}}(sr) = (rs)(sr) = rs^2 r = r^2$