Subgroup \((G \text{ a group})\)

If \(H \leq G\) and \(H\) is a group under the operation of \(G\), then \(H\) is a subgroup of \(G\).
e.g. \( \exists e \in \mathbb{Z} \) is always a subgroup of any \( G \) (called the trivial subgroup).

e.g. \( \exists \mathbb{Z}, \mathbb{Z}^3 \) is a subgroup of \( \mathbb{U}(12) \).
Subgroup tests:

I. $H$ is non-empty and
   $a, b \in H \Rightarrow ab^{-1} \in H$

II. $H$ is non-empty and
    $a, b \in H \Rightarrow ab \in H$
    $a \in H \Rightarrow a^{-1} \in H$
III if $H$ is non-empty

and \text{FINITE}

and $a, b \in H \Rightarrow ab \in H$
Some ways to show $H$ is NOT a subgroup—do any one of the following:

A. Show $e \notin H$

B. Find $a \in H$ with $a^{-1} \notin H$

C. Find $a, b \in H$ with $ab \notin H$
Proof of Subgroup Tests:

(i.e. show if $H$ satisfies the conditions of the test, then it is itself a group — i.e. assoc., closed, e, inverses)
I. H "inherits" associativity from G.

is \( e \in H \)?

H is non-empty, so \( \exists x \in H \)

we let \( a = x, b = x, \) so

\( ab^{-1} \in H, \) so \( xx^{-1} = e \in H \)
Inverses? If $x \in H$, is $x^{-1}$ in $H$?

Yes, let $a=e$, $b=x$, so then $ab^{-1} = ex^{-1} = x^{-1} \in H \checkmark$
Closure? \( x, y \in H \) is \( xy \in H \)?

Let \( a = x \) \( b = y^{-1} \) since we know \( y \in H \Rightarrow y^{-1} \in H \) from previous step.

\[ ab^{-1} = x(y^{-1})^{-1} = xy \in H \]

So yes \( H \) is a subgroup.
Test II

We've proven closed inverses are all given.

$H$ is non-empty, so $x \in H$.
$x \in H \Rightarrow x^{-1} \in H$

Let $a = x$, $b = x^{-1}$, so $ab = xx^{-1} = e \in H$. 


Test III

$H$ is finite and $a, b \in H \Rightarrow ab \in H$

Assoc. is given, closed is given.

Need to show $x \in H \Rightarrow x^{-1} \in H$

(this will give $e \in H$ as above)
So let $X$ be any element of $H$. Look at the set

$\exists x, x^2, x^3, \ldots, 3 \leq H$

But $H$ is finite, so there must be $i \neq j$ such that
$x^i = x^j$

Then (operating in $G$)

$e = x^{j-1} = x \cdot x^{-1}$

i.e.

$x^{-1} = x^{j-i-1} \in \{x^1, x^2, x^3, \ldots \} \subseteq H$

Inverses are in $H$, and since closed

$x \cdot x^{-1} = e \in H \checkmark$
Notation

for $x \in G$

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

$X$ is called a generator of $\langle x \rangle$
eg in \( \mathbb{Z}^+ \)

\[
\langle 4 \rangle = \langle 3, 4, 8, 2, 6, 0 \rangle = \langle 2 \rangle = \langle 6 \rangle = \langle 8 \rangle \\
\langle 5 \rangle = \langle 3, 0, 5 \rangle \\
\langle 7 \rangle = \mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 9 \rangle
\]

(all relatively prime to 10)
Theorem: \( \langle x \rangle \) is always a subgroup of \( G \).

Proof: (Use Test I)

Take \( a, b \in \langle x \rangle \)

So \( a = x^n, b = x^m \) for some \( m, n \in \mathbb{Z} \)
Then \( ab^{-1} = x^n x^{-m} \)

\[ = x^{n-m} \in \langle x \rangle \]

since \( n-m \in \mathbb{Z} \).
Def

\[ Z(G) = \{ a \in G \mid a x = x a \quad \forall x \in G \} \]

"The Center of G"
Theorem: $Z(G) \leq G$

Proof (Test II)

Let $x, y \in Z(G)$, is $xy \in Z(G)$
\[ xg = gx \quad \forall g \in G, \]
\[ yg = gy \quad \forall g \in G, \]

Show \((xy)g = g(xy)\) \quad \forall g \in G, \]
\[ xyg = xgy = gx'y \]
Now show if $x \in Z(q)$
then $x^{-1} \in Z(q)$.

Know $xg = gx$  show  $x^{-1}g = gx^{-1}$

$x^{-1}xg = x^{-1}gx \\
g = x^{-1}g x \\
g = g x^{-1}x^{-1}$

$g x^{-1} = x^{-1}g x^{-1}$

Q.E.D.