Warm-Up: ① List the elements of $U(12)$.

② Find the order of each element.

③ Draw the subgroup lattice.

Def: The Euler totient function

$$\phi : \mathbb{N} \to \mathbb{N}$$

is defined by

$$\phi(n) = \left|\{a \in \mathbb{N} \mid a < n \text{ and } \gcd(a,n) = 1\}\right|$$

$$= |U(n)|$$

Facts: ① If p is prime, then $\phi(p) = p - 1$.

② If $\gcd(m,n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

Thm (Subgroup criterion)

Let G be a group.

A subset $H \subseteq G$ is a subgroup of G if and only if both

- $H \neq \emptyset$

and

- For all $g, h \in H$, we have $gh^{-1} \in H$.

Proof: ($\Rightarrow$) Suppose $H \leq G$. Then $e \in H$, so $H \neq \emptyset$.

If $g, h \in H$, then $h^{-1} \in H$ (closure under inverses) so $gh^{-1} \in H$ also (closure under group operation).

($\Leftarrow$) Conversely, suppose the two conditions in the theorem hold.

Since $H \neq \emptyset$, there is some $x \in H$. Then $xx^{-1} = e \in H$. Identity ✓

For all $h \in H$, since $e \in H$ we get $eh^{-1} = h^{-1} \in H$. Closure under inverses ✓

Lastly, suppose $h_1, h_2 \in H$. By above, $h_2^{-1} \in H$. Thus,

$$h_1(h_2^{-1})^{-1} = h_1 h_2 \in H.$$

closure under group operation ✓

So $H \leq G$.

$\boxtimes$

Cyclic Groups

Thm: Let G be a group. Then

$$\langle a \rangle := \{ a^k \mid k \in \mathbb{Z} \}$$

is a subgroup of G, called the cyclic subgroup generated by a.

Moreover, it is the smallest subgroup of G containing a, in that if $H \leq G$ and $a \in H$, then $\langle a \rangle \leq H$.

Proof: We use the subgroup criterion.

- $\langle a \rangle \neq \emptyset$, since $a^0 = e \in \langle a \rangle$.

- If $g, h \in \langle a \rangle$, then $g = a^k$ and $h = a^l$ for some $k, l \in \mathbb{Z}$. Thus,

$$gh^{-1} = a^k a^{-l} = a^{k-l} \in \langle a \rangle.$$

So $\langle a \rangle \leq G$.

Now, suppose $a \in H$ for some subgroup $H \leq G$. Then

- $a^0 = e \in H$ (Identity)
- $a^k \in H$ for all $k \in \mathbb{N}$ (Closure)
- $a^{-1} \in H$ (Inverses)
- $a^{-k} = (a^{-1})^k \in H$ for all $k \in \mathbb{N}$ (Closure)

So $\langle a \rangle \leq H$.

$\blacksquare$

<u>Note</u>: In an additive group (like $\mathbb{Z}$ or $\mathbb{Z}_n$),

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}.$$

<u>Ex</u>: In $\mathbb{Z}$, $\langle n \rangle = n\mathbb{Z} = \langle -n \rangle$.

<u>Ex</u>: In $\mathbb{Z}_{10}$, $\langle 1 \rangle = \mathbb{Z}_{10}$, $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$, $\langle 5 \rangle = \{0, 5\}$, etc.

<u>Ex</u>: In $U(12)$, $\langle 1 \rangle = \{1\}$

$\langle 5 \rangle = \{1, 5\}$

$\langle 7 \rangle = \{1, 7\}$

$\langle 11 \rangle = \{1, 11\}$.