Discuss in your group: Consider the subgroup $H = \{1, 3, 9\}$ of U_{13}.

Multiplicative group

(a) Quick! How many distinct cosets of H are there?

(b) Find all distinct cosets of H. (Example: $2H$.)

- $1H = \{1, 3, 9\} = 3H = 9H$
- $2H = \{2, 6, 5\} = 6H = 5H$
- $4H = \{4, 12, 10\} = 12H = 10H$
- $7H = \{7, 8, 11\} = 8H = 11H$

Remarks:

- $a \in aH$.
- The cosets form a *partition* of U_{13}.

Set of cosets

Consider again the subgroup $H = \{1, 3, 9\}$ of U_{13}.

Notation. We define U_{13}/H (read "U_{13} mod H") to be the set of distinct cosets of H. Thus,

$$U_{13}/H = \{1H,\ 2H,\ 4H,\ 7H\}.$$

Crazy idea.

- We want to turn U_{13}/H into a group.
- We need an operation, i.e., a way to "multiply" cosets.

Definition. Let S and T be subsets of a group G. Then the *product* of S and T is the set

$$S \cdot T = \{s \cdot t \mid s \in S, t \in T\},$$

where the multiplication $s \cdot t$ is done in G.

Example. To multiply the cosets $2H$ and $4H$...

$$2H \cdot 4H = \{2,\ 6,\ 5\} \cdot \{4,\ 12,\ 10\}$$

$$= \{2 \cdot 4,\ 2 \cdot 12,\ 2 \cdot 10,\ 6 \cdot 4,\ 6 \cdot 12,\ 6 \cdot 10,\ 5 \cdot 4,\ 5 \cdot 12,\ 5 \cdot 10\}$$

$$= \{8,\ 11,\ 7,\quad 11,\ 7,\ 8,\quad 7,\ 8,\ 11\}$$

$$= 7H$$

The group U_{13}/H

$\cdot$	$1H$	$2H$	$4H$	$7H$
$1H$	$1H$	$2H$	$4H$	$7H$
$2H$	$2H$	$4H$	$7H$	$1H$
$4H$	$4H$	$7H$	$1H$	$2H$
$7H$	$7H$	$1H$	$2H$	$4H$

Key:

Treat each coset aH as an *element* of U_{13}/H.

Group properties:

1. U_{13}/H is closed under coset multiplication.
2. Coset multiplication is associative. (See Chapter 21 reading.)
3. U_{13}/H contains the identity, namely $1H$.
4. Every element in U_{13}/H has an inverse.

The group U_{13}/H

$\cdot$	$1H$	$2H$	$4H$	$7H$
$1H$	$1H$	$2H$	$4H$	$7H$
$2H$	$2H$	$4H$	$7H$	$1H$
$4H$	$4H$	$7H$	$1H$	$2H$
$7H$	$7H$	$1H$	$2H$	$4H$

Key:

Treat each coset aH as an *element* of U_{13}/H.

Using this table, we find

4H $(2H)^2 \cdot (2H)$ 7H $(2H)^3 \cdot (2H)$

$$(2H)^1 = 2H, \quad (2H)^2 = 4H, \quad (2H)^3 = 7H, \quad (2H)^4 = 1H \implies \text{ord}(2H) = 4.$$

Thus, U_{13}/H is *cyclic* with generator $2H$, i.e., $U_{13}/H = \langle 2H \rangle$.

Coset multiplication shortcut

Problem #2: Elizabeth claims she can compute $4H \cdot 7H$ *without* multiplying each element of $4H$ by those of $7H$.

How? Can you *justify* her claim?

Key: $4H \cdot 7H = (4 \cdot 7)H = 2H$.

$aH \cdot bH = (a \cdot b)H \quad \longleftarrow$ True in a *commutative* group.

Question: When does the coset multiplication shortcut work?

Theorem: Let G be a *commutative* group, H a subgroup, and $a, b \in G$. Define $aH \cdot bH = \{\alpha \cdot \beta \mid \alpha \in aH,\ \beta \in bH\}$. Then $aH \cdot bH = (ab)H$.

Proof: We must show that $aH \cdot bH \subseteq (ab)H$ and $(ab)H \subseteq aH \cdot bH$.

True for *any* group G.

Let $\alpha \cdot \beta \in aH \cdot bH$, where $\alpha \in aH$ and $\beta \in bH$.

Thus, $\alpha = ah$ and $\beta = bk$ for some $h, k \in H$.

Since G is commutative, we have

$$\alpha \cdot \beta = (ah)(bk) = (ab)(hk) \in (ab)H.$$

Therefore, $\alpha \cdot \beta \in (ab)H$, so that $aH \cdot bH \subseteq (ab)H$.

Next, let $\gamma \in (ab)H$ so that $\gamma = (ab)h$ for some $h \in H$.

Then, $\gamma = (ab)h = (a\varepsilon)(bh) \in aH \cdot bH$.

Thus, $\gamma \in aH \cdot bH$, so that $(ab)H \subseteq aH \cdot bH$.

Therefore, $aH \cdot bH = (ab)H$ as desired.