

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

- The set of distinct cosets of H is: $U_{13}/H = \{1H, 2H, 4H, 7H\}$.
- The set U_{13}/H is a **quotient group** under coset multiplication.

For example...

$$\begin{aligned} 2H \cdot 7H &= \{2, 5, 6\} \cdot \{7, 8, 11\} \\ &= \{2 \cdot 7, 2 \cdot 8, 2 \cdot 11, 5 \cdot 7, 5 \cdot 8, 5 \cdot 11, 6 \cdot 7, 6 \cdot 8, 6 \cdot 11\} \\ &= \{1, 3, 9, 9, 1, 3, 3, 9, 1\} \\ &= 1H \end{aligned}$$

Group table for U_{13}/H

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

Group properties:

- Closure.
- Associativity. (Chapter 21 reading.)
- $1H$ is the identity element of U_{13}/H .
- **Inverses:**
 - $7H = (2H)^{-1}$ and $2H = (7H)^{-1}$.
 - Also, $1H$ and $4H$ are self inverses.

Coset multiplication shortcut: For $aH, bH \in U_{13}/H$,

$$aH \cdot bH = (ab)H.$$

For example, we *should* have $2H \cdot 7H = 14H$, and we've seen indeed that $2H \cdot 7H = 1H$. (Note that $14H = 1H$.)

What we know so far:

ex $G = U_{13}$

- We proved:

G is commutative

\implies

Shortcut holds in G/H

- But we saw that the shortcut also holds in D_4/Z ,
where $Z = \{\varepsilon, r_{180}\}$, **even though D_4 is non-commutative.**

Consider the subgroup $H = \langle 10 \rangle$ of the multiplicative group U_{37} .

Problem #4: Find the inverse of $15H$ in U_{37}/H .

- In U_{37} : $15 \cdot 5 = 1 \implies 15^{-1} = 5$.

- In U_{37}/H : $15H \cdot 5H = (15 \cdot 5)H = 1H \implies (15H)^{-1} = 5H = 15^{-1}H$

Conclusion: $(15H)^{-1} = 15^{-1}H$.

Generalize: $(aH)^{-1} = a^{-1}H$.

Verify: U_{37}/H is a **quotient** group

$$aH \cdot bH = (ab)H$$

Since U_{37}/H satisfies the coset multiplication shortcut...

1. U_{37}/H is closed under coset multiplication, i.e.,

$$aH \cdot bH = (ab)H \in U_{37}/H \text{ for all } aH, bH \in U_{37}/H.$$

2. Coset multiplication is associative. (See Chapter 21.)

3. U_{37}/H contains an identity element $1H$ such that

$$1H \cdot aH = (1 \cdot a)H = aH \text{ for all } aH \in U_{37}/H. \text{ (Also, } aH \cdot 1H = aH.)$$

4. Each $aH \in U_{37}/H$ has an inverse $a^{-1}H \in U_{37}/H$ where

$$aH \cdot a^{-1}H = (a \cdot a^{-1})H = 1H. \text{ (Also, } a^{-1}H \cdot aH = 1H.)$$

What we know so far (again)

- So we just proved:

Shortcut holds in $G/H \implies G/H$ is a quotient group

- **Question:** When does the shortcut hold?

(When G is commutative, yes. But there's more to the story... Stay tuned!)