Discuss in your group:

Consider the *additive* group $\mathbb{Z}_{12}$ and its subgroup $H = \{0, 4, 8\}$. How many *distinct* cosets of H do you expect? Find all of them.

Example:
$6 + H = \{6, 10, 2\}$

- $0 + H = 4 + H = 8 + H = \{0, 4, 8\}$ (original subgroup)
- $1 + H = 5 + H = 9 + H = \{1, 5, 9\}$
- $2 + H = 6 + H = 10 + H = \{2, 6, 10\}$
- $3 + H = 7 + H = 11 + H = \{3, 7, 11\}$

Notation. $[G : H]$ denotes the number of distinct (left) cosets of H in G.

- In the above example, $[G : H] = 4$.
- $[G : H]$ is called the *index* of H in G.

When two cosets are equal:

$$a + H = b + H \iff a - b \in H \text{ and } b - a \in H \quad \text{(additive groups)}$$

$$aH = bH \iff b^{-1}a \in H \text{ and } a^{-1}b \in H \quad \text{(multiplicative groups)}$$

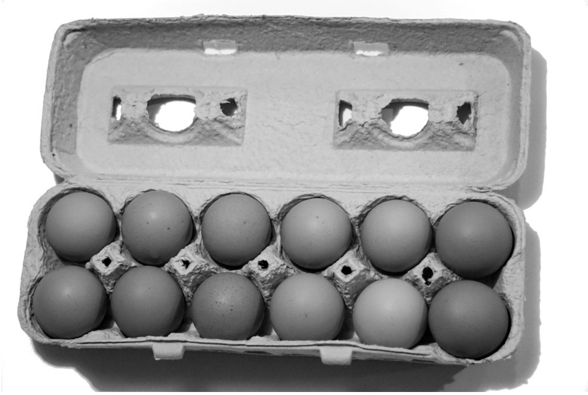
(Not $ab^{-1}, ba^{-1} \in H$.)

Mnemonic. $aH = bH \overset{* b^{-1}}{\iff} b^{-1}aH = H \iff b^{-1}a \in H$.

(This is *not* a proof!)

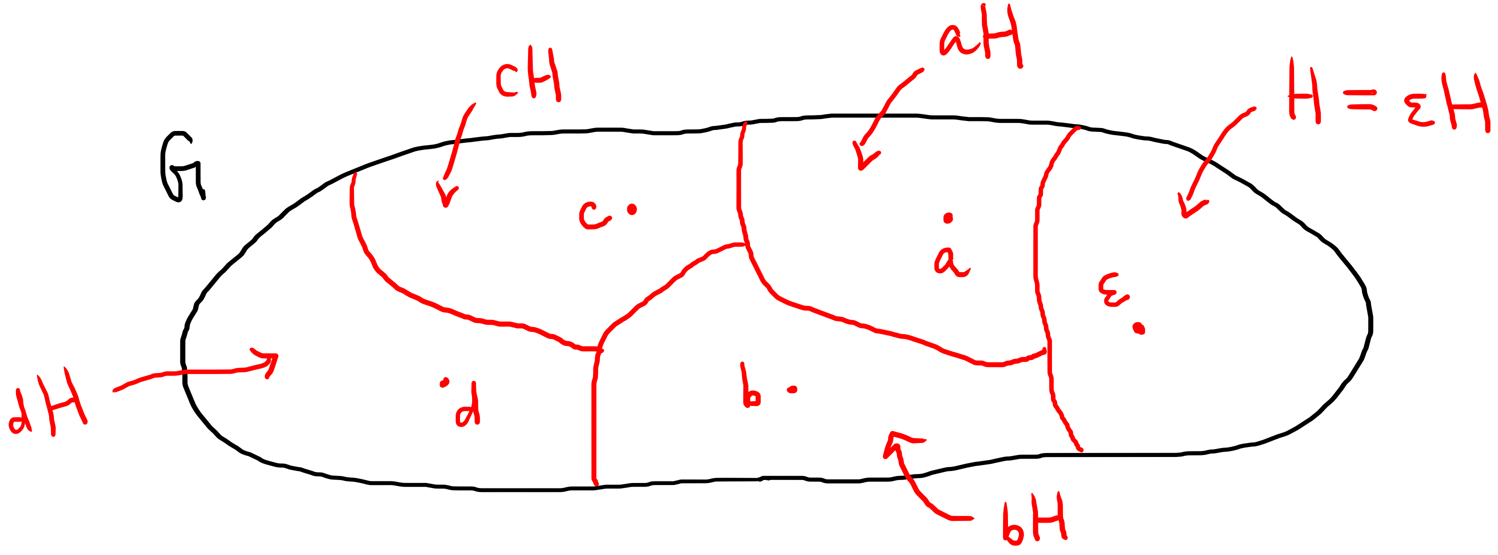
Problem #1, part (b):

With $\#H = 12$, the group G cannot contain 1000 elements, because 12 is *not* a divisor of 1000.



Lagrange's Theorem: Let H be a subgroup of a finite group G. Then $\#H$ is a divisor of $\#G$.

Lagrange's Theorem: Let H be a subgroup of a finite group G. Then $\#H$ is a divisor of $\#G$.



Here $[G : H] = 5$, as 5 cosets of H are needed to fill up G.

Proof ingredients:

1. All the cosets of H have the same size, namely $\#H$.
2. The distinct cosets of H form a *partition* of G, i.e.,
   (a) they cover all of G, and
   (b) they do not overlap with each other.

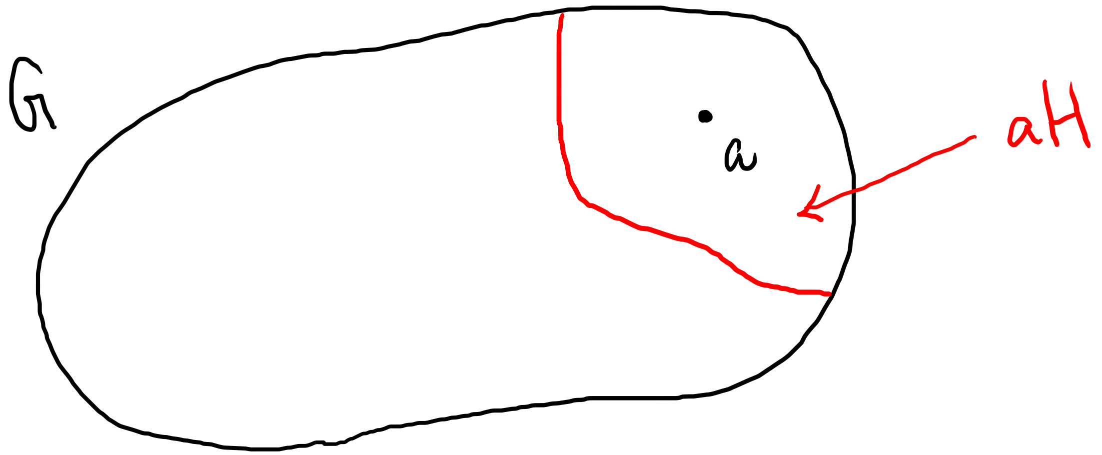
Key: These two ingredients prove Lagrange's Theorem.

Theorem. The distinct cosets of H form a *partition* of G, i.e.,

(a) They cover all of G.

We'll show that every element of G is contained in *some* coset.

Let $a \in G$. Then $a \in aH$, i.e., a is contained in the coset aH.



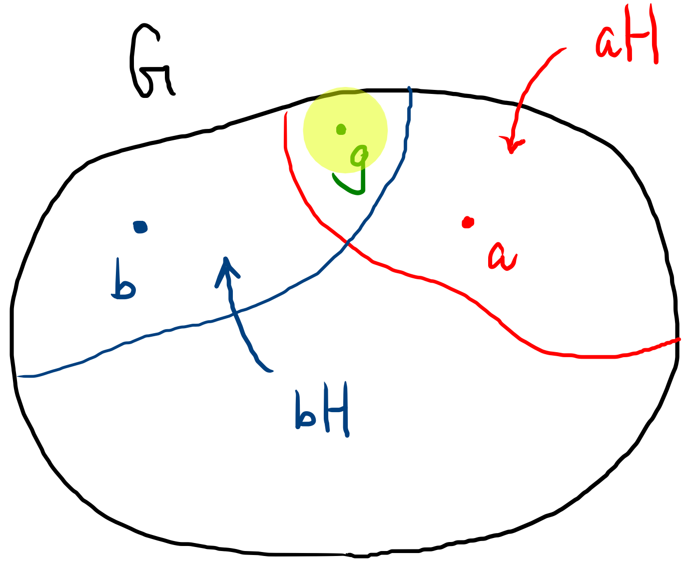
Theorem. The distinct cosets of H form a *partition* of G, i.e.,

(b) They do not overlap with each other.

We must show: if $aH \neq bH$, then aH and bH do *not* overlap.

We *will* show: if aH and bH do overlap, then $aH = bH$. (Contrapositive!)

- Assume that the cosets aH and bH overlap.
- Let g be an element in both aH and bH.
- Thus, $g = ah$ and $g = bk$ for some $h, k \in H$.
- Then, $ah = bk$ which implies $b^{-1}a = kh^{-1} \in H$.
- Since $b^{-1}a \in H$, we obtain $aH = bH$.



An old conjecture proved

Question: Let $g \in G$ be a group element.

If $\mathrm{ord}(g) = 12$, can G contain 1000 elements? Why or why not? No.

Conjecture: Let G be a finite group and $g \in G$.

Then $\mathrm{ord}(g)$ is a divisor of the number of elements in G.

Proof steps.

- Let $n = \mathrm{ord}(g)$.
- Since $\langle g \rangle = \{\varepsilon, g^1, g^2, g^3, \ldots, g^{n-1}\}$, we have $\#\langle g \rangle = n$.
- **Lagrange:** $\langle g \rangle$ is a subgroup of $G \implies \#\langle g \rangle \mid \#G$.
- Thus, n is a divisor of $\#G$.