**Recall:** If $H \leq G$ is a subgroup, then for any $g \in G$ we have the left coset

$$gH = \{gH \mid h \in H\}.$$

We proved:

- the left cosets of $H$ partition $G$
- each coset has size $|gH| = |H|$.

**Note:** When the group operation is $+$, we write

$$g+H = \{g+h \mid h \in H\}$$

instead.

**Warm-Up:** Find all left cosets of

- $\langle s \rangle$ in $D_4$
- $\langle 2 \rangle$ in $\mathbb{Z}_6$
- $3\mathbb{Z}$ in $\mathbb{Z}$

Recall that we defined $[G:H]$, the <u>index of $H$ in $G$</u>, to be the number of distinct left cosets of $H$ in $G$.

<u>Thm</u> (Lagrange): Let $G$ be a finite group, and let $H \leq G$ be a subgroup. Then $|H|$ divides $|G|$, and

$$\frac{|G|}{|H|} = [G:H].$$

<u>Proof</u>: $G$ is partitioned into $[G:H]$ cosets, each of which has cardinality $|H|$. Hence,

$$|G| = |H| \cdot [G:H].$$

$\blacksquare$

## Two important corollaries:

**Cor 1:** Let $G$ be a finite group. Then for any $g \in G$, $|g|$ divides $|G|$.

Hence, $g^{|G|} = e$.

**Proof:** Since $|g| = |\langle g \rangle|$, we have $|g|$ divides $|G|$ by Lagrange's theorem. $\blacksquare$

**Cor 2:** Every group of prime order is cyclic.

**Proof:** Let $G$ be a group with $|G| = p$ for some prime $p$.

Since $p \geq 2$, there is some $g \in G$ with $g \neq e$. Then $|g| \neq 1$ divides $p$, by Lagrange, so $|g| = p$.

Therefore, $\langle g \rangle = G$. $\blacksquare$

# Two famous theorems

**Thm** (Fermat's little theorem):

Let $p$ be a prime. If $a \in \mathbb{Z}$ and $p \nmid a$, then

$$a^{p-1} \equiv a \pmod{p}.$$

**Thm** (Euler): Let $n \in \mathbb{N}$. If $a \in \mathbb{Z}$ and $\gcd(a,n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

$\phi(n) = |U(n)|$

These are both instances of Corollary 1!

Take $G = U(n)$ to get Euler, and Fermat is the special case where $n = p$.

# Homomorphisms

**Def:** Let $G$ and $H$ be groups. A homomorphism is a function $\varphi : G \to H$ such that for all $g_1, g_2 \in G$,

$$\varphi(\underbrace{g_1 g_2}_{\text{product in } G}) = \underbrace{\varphi(g_1)\,\varphi(g_2)}_{\text{product in } H}$$

If a homomorphism $\varphi : G \to H$ is also a bijection, then $\varphi$ is an isomorphism and we write $G \cong H$. ("$G$ is isomorophic to $H$")