Coset's and Lagrange's Theorem

Goal for this week: understand platonic solids examples in a more general context ("group actions")

Definition: G a group, H a subgroup. The subset

$$gH = \{ gh \mid h \in H \} \subset G \qquad (\text{fixed } g \in G)$$

is called (the) left coset of H in G (containing g)

Examples:

1) $(\mathbb{Z}, +)$ group of integers, H the subgroup of even integers.

Then H has 2 cosets in $\mathbb{Z}$:

- H itself, the even numbers
- $1+H = \{1+n \mid n \in H\}$ – odd numbers.

2) D_n dihedral group. $H = \{e, r, r^2, \dots, r^{n-1}\}$ the subgroup of rotations. Again 2 cosets of H in D_n:

- H itself
- $sH = \{ sr^k \mid k = 0, 1, \dots, n-1\}$

reflection $= \{s_1, \dots, s_n\}$ set of reflections.

Proposition 1: For all $g \in G$, we have $|gH| = |H|$.

Proof: The map $M_g : H \to gH$ is clearly surjective.
$h \mapsto gh$

It is also injective: if $gh_1 = gh_2$ then

$g^{-1}(gh_1) = g^{-1}(gh_2)$, so $h_1 = h_2$.

Hence M_g is a bijection $\therefore$ $|gH| = |H|$. ∎

Proposition 2: For two cosets g_1H and g_2H, either

- $g_1H = g_2H$ (cosets are equal), or
- $g_1H \cap g_2H = \emptyset$ (cosets are disjoint).

Proof: Suppose $g_1H \cap g_2H$ is not the empty set.

Need to prove $g_1H = g_2H$.

Since $g_1H \cap g_2H \neq \emptyset$ there exist $h_1, h_2 \in H$

such that $g_1h_1 = g_2h_2$. Then

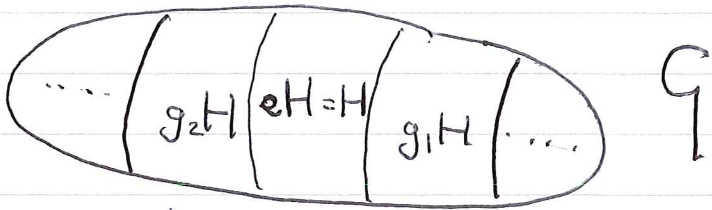
$g_2 = (g_1h_1)h_2^{-1} = g_1(h_1h_2^{-1})$.

So for any $h \in H$, we have $g_2h = g_1(h_1h_2^{-1}h) \in g_1H$.

So $g_2H \subset g_1H$. Similarly we can show

$g_1H \subset g_2H$, hence $g_1H = g_2H$ ∎

This means we have a partition of G into disjoint cosets of H:



Notation: Write G/H to denote the set of left cosets of H in G.

Theorem (Lagrange's Theorem, LT)

The order of a subgroup divides the order of the group.

Proof: Since the cosets $g_1H, \dots, g_nH$ partition G, we have $|G| = |g_1H| + \dots + |g_nH|$.

But $|g_iH| = |H|$ for all i, so we get

$$|G| = n|H| \quad \text{where } n = \#\text{ cosets} = |G/H|.$$

■

Corollary 1: For every $g \in G$, $\operatorname{ord}(g)$ divides $|G|$.

Proof: Consider $H = \langle g \rangle = \{e, g, \dots, g^{k-1}\}$

Then $|H| = k = \operatorname{ord}(g)$.

So LT $\Rightarrow$ $\operatorname{ord}(g) \mid |G|$.

"divides"

Corollary 2: For any $g \in G$ we have $g^{|G|} = e$.

Proof: Let $k = \text{ord}(g)$. Then $|G| = kn$ for some n (Corollary 1)

So $g^{|G|} = g^{kn} = (g^k)^n = e^n = e$. ■

Corollary 3: If $|G| = p$, prime, then G is cyclic.

Proof: For any $g \in G$, $\text{ord}(g) \mid |G|$ so $\text{ord}(g) = 1$ or p.

If $g \neq e$ then $\text{ord}(g) \neq 1$, so $\text{ord}(g) = p$.

Therefore $|\langle g \rangle| = p = |G|$ and so $\langle g \rangle = G$. ■

Corollary 4: "Fermat's Little Theorem".

Let p be prime. For every a not divisible by p,

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

Proof: Let $b = a \bmod p$. Then $a^{p-1} \bmod p = b^{p-1} \bmod p$

so we can prove the result for b instead.

Now $b \in \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$.

This group has order $p-1$ so Corollary 2 implies

$b^{p-1} = 1$ in $\mathbb{Z}_p^\times$, that is

$b^{p-1} \equiv 1 \bmod p$. ■

operation is mult. mod p

Example: Let $p = 13$, $a = 2$.

Then $a^{p-1} = 2^{12} \equiv 1 \mod 13$: we calculate

$2^4 = 16 \equiv 3 \mod 13$

$\Rightarrow 2^{12} = (2^4)^3 = 3^3 = 27 \equiv 1 \mod 13$.

Example LT saves us time in computing orders of elements in finite groups. E.g. what is $\mathrm{ord}(2)$ in $\mathbb{Z}_{13}^\times$?

[Just showed $2^{12} = 1$ in $\mathbb{Z}_{13}^\times$ but $\mathrm{ord}(2)$ could be smaller!]

Now $|\mathbb{Z}_{13}^\times| = 12$, so LT $\Rightarrow \mathrm{ord}(2) \mid 12$

hence $\mathrm{ord}(2) = 2, 3, 4, 6$ or 12.

$2^2 = 4 \neq 1 \Rightarrow \mathrm{ord}(2) \neq 2$

$2^3 = 8 \neq 1 \Rightarrow \mathrm{ord}(2) \neq 3$

$2^4 = 3 \neq 1 \Rightarrow \mathrm{ord}(2) \neq 4$

$2^6 = 2^2 \cdot 2^4 = 4 \cdot 3 = 12 \neq 1 \Rightarrow \mathrm{ord}(2) \neq 6$.

So in fact we must have $\mathrm{ord}(2) = 12$

Exercise: What is $\mathrm{ord}(2)$ in $\mathbb{Z}_{11}^\times$?