

The Orders of Elements and Subgroups: Lagrange's Theorem

From September 16:

Euler's Generalization of Fermat's Little Theorem: If $a \in \mathbb{Z}_n^\times$, then $a^{\phi(n)} = 1$. In particular, the multiplicative order of a divides $\phi(n)$.

Let's recall how we proved this.

Definition: Let $m \in \mathbb{Z}_n^\times$. We will say two elements $a, b \in \mathbb{Z}_n^\times$ are *congruent modulo m* if $a \cdot b^{-1}$ is some positive power of m . Another way to say this is $a = b \cdot m^i$ for some positive integer i .

The set of all b which are congruent to a modulo m will be written $[a]_m$.

#1: Show that the number of elements in $[m]_m$ is the order of m .

#2: Show that each $[a]_m$ has the same number of elements, no matter what $a \in \mathbb{Z}_n^\times$ we look at.

#3: Show that different ones don't overlap, i.e., $[a]_m \cap [b]_m = \emptyset$ if $[a]_m \neq [b]_m$.

#4: Conclude that the number of elements in $[m]_m$, i.e., the order of m , divides the total number of elements in \mathbb{Z}_n^\times . (By definition, this is $\phi(n)$.)

We can now restate this using the notions and tools we've studied since then.

For one, this “congruence” is an equivalence relation, and we can write it as $a \sim b$ if ab^{-1} is in the cyclic subgroup generated by m :

$$a \sim b \text{ if } ab^{-1} \in \langle m \rangle = \{m^1, m^2, \dots, m^{o(m)} = 1\}.$$

The four points above make perfect sense from a group-theoretic standpoint, and from our knowledge of equivalence relations.

Let's put it all into a general framework.

Lagrange's Theorem: If G is a finite group and H is a subgroup of G , then the order of H divides the order of G . In particular, if a is an element of G , then the order of a divides the order of G .

Suppose we take our group G and subgroup H and define an equivalence relation on G by saying

$$a \sim b \text{ if } ab^{-1} \in H.$$

We should check that this is, indeed, an equivalence relation.

- For any $a \in G$, $aa^{-1} = e \in H$ (reflexivity)
- For any $a, b \in G$, if $ab^{-1} \in H$, then $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} \in H$ (symmetry)
- For any $a, b, c \in G$, if $ab^{-1} \in H$ and $bc^{-1} \in H$, then $ab^{-1}bc^{-1} = ac^{-1} \in H$ (transitivity)

Then this equivalence relation will partition the group G into subsets (the equivalence classes).

Why are these subsets all the same size?

Definition: Suppose G is a group and H is a subgroup of G . A *right coset* of H is a subset of G of the form

$$Hx = \{hx : h \in H\},$$

where x is a fixed element of G . A *left coset* of H is a subset of the form

$$xH = \{xh : h \in H\},$$

All these cosets (both left and right) have the same number of elements: $o(H)$. Here's why.

Fix an element $x \in G$. Use this element to define a function $f: G \rightarrow G$:

$$f(g) = gx \quad \text{for all } g \in G.$$

Notice that by left cancellation, this function is *one-to-one*. Thus, the right coset Hx , which is $f(H)$, has $o(H)$ elements. Similar reasoning works for the left cosets.

Suppose a and b are in the same right coset of H : $a, b \in Hx$. This means that $a = h_1x$ and $b = h_2x$ for some elements h_1 and h_2 of H . Then $ab^{-1} = h_1x(h_2x)^{-1} = h_1xx^{-1}h_2^{-1} = h_1h_2^{-1} \in H$. So $a \sim b$ if a and b are in the same coset.

Conversely, suppose $a \sim b$. Since $b = eb$, b is in the coset Hb . Since $ab^{-1} \in H$, $ab^{-1} = h$ for some $h \in H$. So $a = hb \in Hb$, too. So a and b are in the same coset if $a \sim b$.

In other words, the equivalence classes here are exactly the right cosets of H .

Examples: 1. The subgroup H itself is a coset; just use $x = e$ (or any other element of H , for that matter). In other words, H is the equivalence class of the identity element $[e]$.

2. $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. Here there are three cosets: integers divisible by 3 (H itself), integers congruent to 1 modulo 3 ($H + 1$), and integers congruent to 2 modulo 3 ($H + 2$).

3. $G = S_4$ and $H = A_4$. Here there are two cosets: even permutations (H itself) and odd permutations ($H(1, 2)$).

4. $G = \mathbb{Z}_{13}^\times$ and $H = \langle 8 \rangle = \{1, 8, 12, 5\}$. Here there are three cosets: H itself, $H2 = \{2, 3, 11, 10\}$, and $H4 = \{4, 6, 9, 7\}$.

Back to Lagrange's Theorem: If G is a finite group, so is the subgroup H . The cosets of H all have the same number of elements: $o(H)$. The cosets are equivalence classes, so they give a partition of the group G . Thus,

the number of cosets of H times the order of H equals the order of G .