Cosets and Lagrange's Theorem

In this lecture we introduce the notion of a coset and prove the famous result of Lagrange regarding the divisibility of the order of a group by the orders of its subgroups.

Fix a group G and a subgroup $H \subset G$. Define a relation $\sim$ on the set G such that for $a, b \in G$:

$$a \sim b \quad \iff \quad ab^{-1} \in H$$

Keep in mind that $\sim$ depends on H. We show that this is an equivalence relation.

1. (Reflexivity) $a \sim a$ because $aa^{-1} = e$ and the identity is in any subgroup.
2. (Symmetry) $a \sim b$ implies $ab^{-1} \in H$. Since H is a subgroup, the inverse of this element is also in H: we have $(ab^{-1})^{-1} = ba^{-1} \in H$. Thus $b \sim a$.
3. (Transitivity) $a \sim b$ and $b \sim c$ imply $ab^{-1} \in H$ and $bc^{-1} \in H$. Since H is a subgroup, it is closed under the group operation. Thus $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, and $a \sim c$.

We have seen this construction before in a special case. Let $G = (\mathbb{Z}, +)$ and for a fixed positive integer n take the subgroup $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} \subset \mathbb{Z}$. Then $a \sim b$ if and only if "ab^{-1}" $= a - b \in n\mathbb{Z}$, i.e. $a \equiv b \pmod{n}$. This motivates the following general notation:

$$a \sim b \qquad \iff \qquad a \equiv b \pmod{H}$$

▸ **For $a \in G$, let $Ha = \{ha : h \in H\}$. Then Ha is called a *right coset* of H in G.**

The right cosets of H in G are the equivalence classes of the above relation:

$$Ha = \{b \in G : \; a \equiv b \pmod{H}\}$$

To see this, consider some $b \in Ha$. Then $b = ha$ where $h \in H$. From this we then find $ab^{-1} = h^{-1} \in H$ and so $a \equiv b \pmod{H}$. Thus Ha is a subset of the equivalence class of a. Conversely consider any $b \in G$ such that $a \equiv b \pmod{H}$. Then $ab^{-1} \in H$, so $ab^{-1} = h$ for some $h \in H$, and so $b = h^{-1}a \in Ha$.

▸ **There is a 1-1 correspondence between any two right cosets of H in G.**

Let Ha be a right coset. It suffices to show that Ha is in 1-1 correspondence with H itself. For this, we note that each $h \in H$ determines the element $ha \in Ha$, and every element in Ha is of this form. Thus the only thing to check is that if $ha = h'a$ then $h = h'$, and this just follows from multiplying by a^{-1} on the right.

We define the *index* of a subgroup H in G, written $[G : H]$, as follows:

$$[G : H] = \#\{\text{distinct right cosets of } H \text{ in } G\}$$

Of course it is possible that $[G : H]$ is infinite.

▶ **(Lagrange's Theorem) If G is a finite group, and H is a subgroup of G, then**

$$[G : H] = |G|/|H|$$

In particular, if G is finite, the order of any subgroup H divides the order of the group G. The proof follows from our discussion above: the right cosets in G are equivalence classes, and partition the set G into $[G : H]$ distinct subsets, each of which has size $|H|$. From this it follows that $|G| = [G : H] \cdot |H|$.

Let's see all of this in action. Take the symmetric group S_3 of orer 6:

$$S_3 = \{e, (12), (23), (31), (123), (132)\}$$

Let H be the order 2 cyclic subgroup $\{e, (12)\}$. Then the right cosets are

$$He = \{e, (12)\}, \qquad H(23) = \{(23), (123)\}, \qquad H(31) = \{(31), (132)\}$$

Any other right coset is one of the above 3: we have $H(12) = He = H$, $H(123) = H(23)$ and $H(132) = H(31)$. The number of distinct right cosets is $[S_3 : H] = 3$. We directly observe Lagrange's Theorem: $6/2 = |S_3|/|H| = [S_3 : H] = 3$.

For another example, consider the symmetric group S_4. This has order $|S_4| = 4! = 24$. We saw last lecture that the alternating group $A_4 \subset S_4$ has order 12. Thus

$$[S_4 : A_4] = |S_4|/|A_4| = 24/12 = 2$$

In particular, there are exactly two right cosets: $A_4 = A_4 e$ and $A_4\sigma$ where σ is any odd permutation, say, a transposition.

Assume $n \geqslant 2$. For the symmetric group S_n, and the subgroup $A_n \subset S_n$, there are exactly two right cosets. To see this, we note that $a \equiv b \pmod{A_n}$ if and only if ab^{-1} is even. Thus the two equivalence classes, i.e. right cosets, are the sets of even and odd permutations. (Assuming $n \geqslant 2$ ensures that these two cosets are both nonempty.) We conclude

$$|A_n| = |S_n|/[S_n : A_n] = n!/2.$$

Thus the alternating group A_n has order $n!/2$.