10 Cosets and Lagrange's Theorem

10.1 Cosets

Theorem. *Suppose $H \leq G$. Define the relation $\sim_L$ as*

$$a \sim_L b \iff a^{-1}b \in H.$$

Similarly,

$$a \sim_R b \iff ab^{-1} \in H.$$

Then both $\sim_L$ and $\sim_R$ are equivalence relations on the group G.

We may prove the theorem by showing that $\sim_L$ is reflexive, symmetric, and transitive. Similar procedure proves the theorem for $\sim_R$.

Recall that every equivalence relation on a set S partitions S into equivalence classes. For the equivalence relation $\sim_L$, what is the equivalence class for an element $g \in G$?

If $x \in G$ is in the same class as g, then $g \sim_L x$, which means $g^{-1}x \in H$. That is, $g^{-1}x = h$ for some $h \in H$. If we solve this equation for x, we obtain $x = gh$. Thus the equivalent class of $g \in G$ is $\{gh \mid h \in H\}$. We use the notation gH for this equivalence class.

Similarly, the equivalent class of $g \in G$ for the equivalence relation $\sim_R$ is $Hg = \{hg \mid h \in H\}$.

Definition. *Suppose $H \leq G$. The **left coset** of H containing $g \in G$ is $gH \subseteq G$. The **right coset** of H containing $g \in G$ is $Hg \subseteq G$.*

Example 1. *Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.*

Remark. *If $H \leq G$ and G is abelian, then $gH = Hg$ for all $g \in G$.*

Remark. *The equivalence classes of $\sim_L$ and $\sim_R$ in $n\mathbb{Z}$ for an integer n are called* cosets modulo $n\mathbb{Z}$.

Example 2. *Find the partitions of $\mathbb{Z}_6$ into cosets of the subgroup $H = \langle 3 \rangle$.*

Solution. The cosets are $0 + \langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle$.

If we use the notation:

$$0 = \begin{matrix} 0 & 3 \\ 3 & 0 \end{matrix}$$

$$1 = \begin{matrix} 1 & 4 \\ 4 & 1 \end{matrix}$$

$$2 = \begin{matrix} 2 & 5 \\ 5 & 2 \end{matrix}$$

then we may rewrite the table for $\mathbb{Z}_6$ as the following:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We observe that this *coset group* is isomorphic to $\mathbb{Z}_3$. Section 14 of the textbook shows that a partition of an *abelian* group into cosets always results in a coset group. □

Example 3. *S_3 is nonabelian and we do not get a coset group from the left cosets and right cosets of $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$.*

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

The left cosets of $H = \langle \mu_1 \rangle$ are

$$\begin{aligned} H &= \{\rho_0, \mu_1\} \\ \rho_1 H &= \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, \mu_3\} \\ \rho_2 H &= \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, \mu_2\}. \end{aligned}$$

The partition of S_3 into right cosets of H is

$$\begin{aligned} H &= \{\rho_0, \mu_1\} \\ H\rho_1 &= \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, \mu_2\} \\ H\rho_2 &= \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, \mu_3\}. \end{aligned}$$

Remark. *For the nonabelian group S_3, the left cosets of $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ and the right cosets of $\langle \rho_1 \rangle$ are the same:*

$$\begin{aligned} H &= \{\rho_0, \rho_1, \rho_2\} \\ \mu_1 H &= \{\mu_1, \mu_2, \mu_3\} = H\mu_1 \end{aligned}$$

These cosets do form a coset group that is isomorphic to $\mathbb{Z}_2$. The reason is that the partition of S_3 into left cosets is the same as the partition of S_3 into right cosets. Thus we may simply say the cosets of H and omit the the adjective left or right.

10.2 Lagrange's Theorem

Theorem (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$ and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.*

Proof. Let $|H| = n$ and let the number of left cosets of H in G equal k. The set of left cosets of H in G partition G. By definition of a left coset, the map

$$H \to gH \quad \text{defined by} \quad h \mapsto gh$$

maps H onto the left coset gH. The left cancellation law implies this map is 1-1 because $gh_1 = gh_2$ implies $h_1 = h_2$. This proves that H and gH have the same order.

$$|gH| = |H| = n.$$

Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = nk$. Thus $k = \frac{|G|}{n} = \frac{|G|}{|H|}$. □

The proof of Lagrange's Theorem is the result of simple counting! Lagrange's Theorem is one of the most important combinatorial results in finite group theory and will be used repeatedly.

Corollary. *If G is a group of prime order p, then G is cyclic and $G \cong \mathbb{Z}_p$.*

Proof. Let $x \in G$ and $x \neq 1$. Thus $|\langle x \rangle| > 1$ and $|\langle x \rangle|$ divides G. Since $|G|$ is prime, we must have $|\langle x \rangle| = |G|$. Therefore $G = \langle x \rangle$ is cyclic (with any non-identity element x as generator). Since every two cyclic groups of the same order are isomorphic, $G \cong \mathbb{Z}_p$. □

Thus there is only one group structure, up to isomorphism, of a given prime order p.

Corollary. *If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular, $x^{|G|} = 1$ for all x in G.*

Proof. We have $|x| = |\langle x \rangle|$. The first part of the corollary follows from Lagrange's Theorem applied to $H = \langle x \rangle$. The second statement is clear since now $|G|$ is a multiple of the order of x. □

Definition. *If G is a group and $H \leq G$, the number of left cosets of H in G is called the **index** of H in G and is denoted by $(G : H)$.*

If G is finite, then $(G : H) = |G|/|H|$ because every coset of H contains $|H|$ elements.

Theorem. *Suppose G is a group and $K \leq H \leq G$. Furthermore, suppose $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.*

Example 4. *Find the index of $\langle \mu_2 \rangle$ in the group D_4.*

Example 5. *Let $\sigma = (1, 2, 5, 4)(2, 3)$ in S_5. Find the index of $\langle \sigma \rangle$ in S_5.*

Example 6. *Let H be a subgroup of a group G and let $a, b \in G$. Prove*

$$aH = bH \Longrightarrow Ha^{-1} = Hb^{-1}$$

or give a counterexample.

Example 7. *Show that if a group G with identity element e has finite order n, then $g^n = e$ for all $g \in G$.*