Math 403 Chapter 7: Cosets and Lagrange's Theorem

1. **Introduction:** The concept of a coset, and how it leads to Lagrange's Theorem and to the notion of a normal subgroup and then quotient groups, is essential to the analysis of groups.

2. **Cosets:**

   (a) **Definition:** Let G be a group and let $H \leq G$. For any $a \in G$ we define:

$$\begin{aligned} aH &= \{ah \,|\, h \in H\} = \text{The left coset of } H \text{ containing } a. \\ Ha &= \{ha \,|\, h \in H\} = \text{The right coset of } H \text{ containing } a. \\ aHa^{-1} &= \{aha^{-1} \,|\, h \in H\} \end{aligned}$$

   We also define:

$$\begin{aligned} |aH| &= \text{The number of elements in the left coset.} \\ |Ha| &= \text{The number of elements in the right coset.} \end{aligned}$$

   Mostly we'll focus on left-cosets as it turns out that the two situations are essentially mirror images of one another. As we will see, cosets are not distinct.

   Example: Consider $G = S_3$ and $H = \{(), (2\,3)\}$. Here are all the left cosets:

$$\begin{aligned} ()H &= (\,)\{(), (23)\} = \{(), (23)\} \\ (12)H &= (12)\{(), (23)\} = \{(12), (123)\} \\ (13)H &= (13)\{(), (23)\} = \{(13), (132)\} \\ (23)H &= (23)\{(), (23)\} = \{(23), ()\} \\ (123)H &= (123)\{(), (23)\} = \{(123), (12)\} \\ (132)H &= (132)\{(), (23)\} = \{(132), (13)\} \end{aligned}$$

   We see that there are only three distinct cosets, those are $()H$, $(12)H$ and $(13)H$.

(b) **Theorem:** Let $H \leq G$ and let $a, b \in G$. Then:

(i) $a \in aH$.

(ii) $aH = H$ iff $a \in H$.

(iii) $(ab)H = a(bH)$.

(iv) $aH = bH$ iff $a \in bH$.

(v) $aH = bH$ or $aH \cap bH = \emptyset$.

(vi) $aH = bH$ iff $a^{-1}b \in H$.

(vii) $|aH| = |bH|$.

(viii) $aH = Ha$ iff $aHa^{-1} = H$.

(ix) $aH \leq G$ iff $a \in H$.

Proof: These are all fairly straightforward:

(i) $a = ae \in aH$.

(ii) $\Rightarrow$: If $aH = H$ then $a \in aH = H$. We use (i) here.
$\Leftarrow$: If $a \in H$ then first note that $aH \subseteq H$ by the closure of H as a subgroup. To show that $H \subseteq aH$ let $h \in H$ and note that since $a \in H$ we have $a^{-1} \in H$ and so $a^{-1}h \in H$ and then $h = eh = a(a^{-1}h) \in aH$.

(iii) Follows from associativity in G.

(iv) $\Rightarrow$: If $aH = bH$ then $a \in aH = bH$. We use (i) here.
$\Leftarrow$: If $a \in bH$ then $a = bh$ for some $h \in H$ and then $aH = bhH = bH$ where $hH = H$ by (ii).

(v) If they are disjoint then we're done. If not then there is some $c \in aH \cap bH$ and then by (iv) we know $cH = aH$ and $cH = bH$ and so $aH = bH$.

(vi) We have $aH = bH$ iff $a^{-1}bH = H$ and then apply (ii).

(vii) The mapping $aH \to bH$ given by $ah \mapsto bh$ is onto by construction and 1-1 by the cancelation property.

(viii) We have $aH = Ha$ iff $aHa^{-1} = Haa^{-1}$ and $Haa^{-1} = H$.

(ix) $\Rightarrow$: If $aH \leq H$ then $e \in aH$ since aH is a subgroup and then $aH \cap eH \neq \emptyset$ and so by (v) we have $aH = eH = H$ and then by (ii) we have $a \in H$.
$\Leftarrow$: If $a \in H$ then by (ii) we have $aH = H$ and we know $H \leq G$.

This theorem, especially (v), helps us be more systematic about finding cosets.

Example: Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and $H = \{1, 4\}$ we know that $1H = \{1, 4\}$ and $4H$ is the same. By disjointness pick another element not already accounted for and find its coset. For example $2H = \{2, 8\}$. Repeat until done, giving $7H = \{7, 13\}$ and $11H = \{11, 14\}$. Then we're done because there are no elements left.

3. **Lagrange's Theorem and Consequences:**

(a) **Definition:** The number of cosets of H in G is called *the index of H in G* and is denoted $|G : H|$.
Example: We have $|S_3 : \{(), (23)\}| = 3$.

(b) **Lagrange's Theorem:** If G is finite and $H \leq G$ then $|H|\big||G|$ and $|G : H| = |G|/|H|$.
Proof: This follows immediately from the fact that the cosets are disjoint or identical, the union is the entire group, and that they are all the same size, that size being $|H|$. $\mathcal{QED}$

Note: The Fundamental Theorem of Cyclic Groups told us that for cyclic groups this is the case, and even that such subgroups exist and are unique. This is not quite as good as it does not guarantee existance or uniqueness, but it certainly provides restrictions.

Example: A group of order 15 may only have subgroups of orders $1, 3, 5, 15$. This is not to say it must have such subgroups but this is all that it could have.

(c) **Corollary 1:** If G is finite and $g \in G$ then $|g|\big||G|$.
Proof: Follows from the fact that $|g| = |\langle g \rangle|$. $\mathcal{QED}$

Example: If $|G| = 28$ then the order of any element could only be $1, 2, 4, 7, 14, 28$.

(d) **Corollary 2:** If $|G|$ is prime then G is cyclic.
Proof: Pick $g \in G$ with $g \neq e$. Then $|g| \neq 1$ so $|g| = |G|$ and so $\langle g \rangle = G$. $\mathcal{QED}$

Example: This is a strong statement. For example if a group has order 7 then it must be cyclic and we know therefore it is isomorphic to $\mathbb{Z}_7$, or to $\{e, g, g^2, g^3, g^4, g^5, g^6\}$.

(e) **Corollary 3:** If G is finite and $g \in G$ then $g^{|G|} = e$.
Proof: Follows from the fact that $|g|\big||G|$. $\mathcal{QED}$