CHAPTER II: GROUPS

Section 5: Cosets

Example 1: Consider the subgroup $H = \{(1),(12)\}$ of S_3. For each of the six elements $\pi \in S_3$, we can compute the set $\pi H = \{\pi\sigma : \sigma \in H\}$. For example, $(23)H = \{(23),(132)\}$. If you do the remaining computations, you will see that we get the following results:

$$\begin{gathered}(1)H = (12)H = H \\ (23)H = (132)H = \{(23),(132)\} \\ (13)H = (123)H = \{(13),(123)\}\end{gathered}$$

Definition: Let H be a subgroup of a group G. A subset of the form gH, where $g \in G$, is called a ***left coset*** (pronounced “CO-set”) of H. A subset of the form Hg, where $g \in G$, is called a ***right coset*** of H.

Example 2: Let $G = \mathbb{Z}_8$ (under addition modulo 8) and let H be the subgroup $\{0,2,4,6\}$. Since the group operation in this case is addition, we form the left cosets of H by adding the 8 elements of G to H.

$$\begin{array}{llll} 0+H=\{0,2,4,6\} & 1+H=\{1,3,5,7\} & 2+H=\{0,2,4,6\} & 3+H=\{1,3,5,7\} \\ 4+H=\{0,2,4,6\} & 5+H=\{1,3,5,7\} & 6+H=\{0,2,4,6\} & 7+H=\{1,3,5,7\} \end{array}$$

Even though we were multiplying (or adding) H by many elements (six in the first example and eight in the second), in both of these examples we only got a few different cosets (three in the first example, two in the second).

Theorem 1: If H is a subgroup of a group G and $a,b \in G$, then the following are equivalent:

(a) $a \in bH$
(b) $b \in aH$
(c) $aH = bH$
(d) $b^{-1}a \in H$
(e) $a^{-1}b \in H$

First I should say a word about this type of theorem. It states that "the following are equivalent" (often abbreviated TFAE). This doesn't mean that ANY of the conditions must be true, but if any one of them is true, the others are true also. They are all equivalent facts. There are several ways to prove a theorem of this type. One way is to show that (a)$\Rightarrow$(b)$\Rightarrow$(c)$\Rightarrow$(d)$\Rightarrow$(e)$\Rightarrow$(a). I'll provide the skeleton proof and let you fill in some details in the exercises.

Proof:
(a)$\Rightarrow$(b) Suppose $a \in bH$. Then there exists an $h \in H$ such that $a = bh$. But that implies that $ah^{-1} = b$, and hence $b \in aH$.

(b)$\Rightarrow$(c) If $b \in aH$, we want to show that $aH = bH$. Clearly $bH \subseteq aH$. (Why?) Now let $ah \in aH$ and since $b \in aH$, let's say $b = ah_0$. Then $ah = a(h_0 h_0^{-1})h \in bH$. (Why?) So $aH \subseteq bH$.

(c)$\Rightarrow$(d) Now if $aH = bH$, we can multiply both sides by b^{-1} and get $b^{-1}aH = H$. This implies that $b^{-1}a \in H$. (Why?)

(d)$\Rightarrow$(e) Since the inverse of $b^{-1}a$ is $a^{-1}b$, this must be in H also.

(e)$\Rightarrow$(a) Finally, $a^{-1}b \in H$ implies that $a^{-1}b = h$ for some $h \in H$. Therefore, $a \in bH$. (Why?)

Theorem 2: Let H be a subgroup of a group G. The collection of left cosets of H forms a partition of G. In other words, (a) each coset is nonempty, (b) for each $a, b \in G$, either $aH = bH$ or $aH \cap bH = \varnothing$, and (c) the union of left cosets is G.

Proof: For each $a \in G$, $a \in aH$. This proves parts (a) and (c). To show part (b), suppose $aH \cap bH \neq \varnothing$. Let $g \in aH \cap bH$. By the previous theorem, this means that $gH = aH$ and $gH = bH$. So $aH = bH$.

Theorem 3: Let H be a subgroup of a finite group G. Each coset of H has the same cardinality.

Proof: Let aH and bH be distinct cosets of H. The mapping sending x to $ba^{-1}x$ is a bijection from aH onto bH.

Definition: The number of distinct left cosets of H in G is called the ***index*** of H

in G, and is denoted by $[G:H]$.

Theorem 4 (Lagrange): Let H be a subgroup of a finite group G. Then the cardinality of G is the cardinality of H times the index of H in G. In particular, the cardinality of H divides the cardinality of G.

Proof: Suppose $[G:H]=n$. The distinct left cosets of H are pairwise disjoint by Theorem 2, each has the same size by Theorem 3, and $|gH|=|H|$ for all $g \in G$. Since the union of the distinct left cosets is G (again by Theorem 2), $|G|=|H| \cdot n$. Hence $|H|$ divides $|G|$.

Corollary: Let p be a prime number and suppose G is a group of order p. Then

(a) G has only two subgroups, itself and $\{e\}$.
(b) G is cyclic (generated by any non-identity element).
(c) Every homomorphism from G into another group is either trivial (i.e. every element getting mapped to the identity) or injective.

Proof: By Lagrange's Theorem, subgroups of G must be of order 1 or p, so part (a) follows. Similarly, if $a \neq e$ the subgroup generated by a must be the whole group, so (b) is true. Finally, part (c) follows from the fact that the kernel of a homomorphism is a subgroup of G, so it must be either $\{e\}$ (in which case the homomorphism is injective) or G (in which case the homomorphism is trivial).

Definition: The ***center of a group*** G, denoted $Z(G)$, is the set of all elements that commute with all elements of G, $Z(G)=\{a \in G : ag = ga \text{ for all } g \in G\}$.

Clearly this set is always nonempty and contains the identity of the group. You are asked in the exercises to show that the center of a group is always a normal subgroup.