Math 412: Cosets

DEFINITION: Fix a group G and a subgroup K. A **right K-coset** of K is any subset of G of the form

$$K \circ b = \{k \circ b \mid k \in K\}$$

where $b \in G$. Similarly, a **left K-coset** of K is any set of the form $b \circ K = \{b \circ k \mid k \in K\}$.

PROPOSITION: Fix a group G and a subgroup K. The total number of right K-cosets is equal to the total number of left K-cosets.

DEFINITION: Fix a group G and a subgroup K. The **index** of K in G is the total number of *distinct* right K-cosets of K in G. We write this index $[G : K]$.

LAGRANGE'S THEOREM: Fix a group G and a subgroup K. Then $|G| = |K|[G : K]$.

DEFINITION: Let $a, b \in G$. We say a is **congruent** to b modulo K if $ab^{-1} \in K$.

Part 1: The essentials.

A. EXAMPLE IN THE GROUP OF INTEGERS. Let $G = (\mathbb{Z}, +)$ and let K be the subgroup generated by 7.

(1) Verify that $K = 7\mathbb{Z} = \{7k | k \in \mathbb{Z}\}$.
(2) Describe the right K-coset $K + 0$.
(3) Explain why the left/right K-coset containing a is the same as the set $[a]_7 \subseteq \mathbb{Z}$.
(4) Find the index $[G : K]$. Verify LaGrange's theorem.

Solution.

(1) The elements in this subgroup are the integers that can be obtained by adding or subtracting 7 any number of times, so the multiples of 7.
(2) $K + 0 = \{7k | k \in \mathbb{Z}\}$.
(3) $K + a = \{7k + a | k \in \mathbb{Z}\} = [a]_7$.
(4) $[G : K] = 7$, and $|G| = |H| = \infty$, so even though we have some orders that are infinite, Lagrange's Theorem still holds!

B. EXAMPLE IN S_3. Consider the subgroup K of S_3 generated by $(1\,2)$.

(1) List out all the elements of K. What does Lagrange's Theorem predict about the number of right cosets of K?
(2) Find the right K-coset Ke. Show that it is the same as the right coset $K(1\,2)$.
(3) Find the right coset $K(2\,3)$. Show that it is the same as the right coset $K(1\,2\,3)$.
(4) Find the right coset $K(1\,3)$. Show that it is the same as the right coset $K(1\,3\,2)$.
(5) Write out all the elements of S_3 explicitly, grouping them together if they are in the same right K-coset.
(6) Express S_3 as a disjoint union of right K-cosets. How many right K-cosets are there in total?
(7) Verify Lagrange's Theorem for $K \subseteq S_3$.

Solution.

(1) $Ke = \{e, (1\,2)\} = K\,(1\,2)$.
(2) $K\,(2\,3) = \{(2\,3), (1\,2)(2\,3)\} = \{(2\,3), (1\,2\,3)\} = \{(1\,2\,3), (1\,2)(1\,2\,3)\} = K\,(1\,2\,3)$.
(3) $K\,(1\,3) = \{(1\,3), (1\,2)(1\,3)\} = \{(1\,3), (1\,3\,2)\} = \{(1\,3\,2), (1\,2)(1\,3\,1)\} = K\,(1\,3\,2)$.

(4) $Ke = \{e, (1\,2)\}$, $K\,(2\,3) = \{(2\,3), (1\,2\,3)\}$, $K\,(1\,3) = \{(1\,3), (1\,3\,2)\}$
(5) $S_3 = Ke \cup K(1\,2) \cup K(1\,3)$.
(6) $|S_3| = 6 = 3 \times 2 = [S_3 : K]\,|K|$.

C. RIGHT K-COSETS AND CONGRUENCE MODULO K. Fix a group G and a subgroup K.

(1) Prove that a is congruent to b modulo K if and only if $a \in Kb$. So the set of all elements congruent to b mod K is precisely the right coset Kb.
(2) Prove that congruence modulo K is an equivalence relation.
(3) Discuss: the concept of "right K-coset" is the group analog of the concept of "congruence class modulo an ideal" for rings.
(4) Show that if $b \in Ka$, then $Ka = Kb$. Show also that if $b \notin Ka$, then $Ka \cap Kb = \emptyset$. That is, two cosets are either exactly the same subset of G or they do not overlap at all.

Solution.

(1) If a is congruent to b modulo K, then $ab^{-1} \in K$, and $a = ab^{-1}b \in Kb$. On the other hand, if $a \in Kb$, then $a = kb$ for some $k \in K$. Then $ab^{-1} = k \in K$.
(2) Reflexive: for any $a \in G$, $aa^{-1} = e \in K$, so a is congruent to a modulo K.
   Symmetric: for any $a, b \in G$, if $ab^{-1} = e \in K$, then $ba^{-1} = (ab^{-1})^{-1} \in K$. So if a is congruent to b modulo K, then b is congruent to a modulo K.
   Transitive: suppose that a is congruent to b modulo K and b is congruent to c modulo K. Then $ab^{-1}, bc^{-1} \in K$. Since K is closed for products, $ac^{-1} = (ab^{-1})(bc^{-1}) \in K$, so a is congruent to c modulo K.
(4) Suppose that $b \in Ka$, which we have shown is equivalent to a being congruent to b modulo K. Given any element $g \in G$, $g \in K$ if and only if $gab^{-1} \in K$ (why?). Then
$$Kb = \{kb \,|\, k \in K\} = \{(kab^{-1})b \,|\, k \in K\} = \{ka \,|\, k \in K\} = Ka.$$
   On the other hand, if $b \notin Ka$, then by (1) we know $ab^{-1} \notin K$, and so for every $k_1, k_2 \in K$, $k_1 a \neq k_2 b$, or else we could write $ab^{-1} = k_1^{-1}k_2 \in K$. Therefore, $Ka \cap Kb = \emptyset$.

D. THE PROOF OF LAGRANGE'S THEOREM. Fix a group G and a subgroup K. Let $a, b \in G$.

(1) Prove that there is a bijection
$$Ka \to Kb$$
   given by right multiplication by $a^{-1}b$.
(2) Prove that G is the disjoint union of its distinct right K-cosets, all of which have cardinality $|K|$.
(3) Prove that if G is finite, then $|G| = [G : K]|K|$.
(4) Conclude that the order of any subgroup K must divide the order of G.
(5) Conclude that the order of any element in G must divide the order of G.

Solution.

(1) The map $Ka \to Kb$ given by right multiplication by $a^{-1}b$ has inverse $Kb \to Ka$ given by right multiplication by $b^{-1}a$. This is easy to check: $na \mapsto (na)(a^{-1}b) \mapsto (na)(ab^{-1})(b^{-1}a) = na$ and $nb \mapsto (nb)(b^{-1}a) \mapsto (nb)(b^{-1}a)(a^{-1}b) = nb$ so these maps are mutually inverse.
(2) We already know that every element of G is in one coset, so G is the disjoint union of its cosets. By (1), each coset has the same cardinality as K.
(3) Each coset has $|K|$ elements. so $|G| = |K|[G : K]$.
(4) Lagrange's Theorem says that $|K|$ divides $|G|$.

(5) The order of an element g is the same as the order of the cyclic subgroupof G generated by g.

A good self-check.

E. LEFT VS RIGHT COSETS. Let G be a group and K be a subgroup of G.

(1) With the notation we used in A, is $K+0=0+K$? How about $K+a$ and $a+K$ for some $a \in \mathbb{Z}$?
(2) With the notation we used in B, is $K(1\,2\,3)=(1\,2\,3)K$?
(3) TRUE OR FALSE: In an arbitrary group G, for any subgroup K, $Kg=gK$ for all $g \in G$.
(4) TRUE OR FALSE: In an arbitrary abelian group G, for any subgroup K, $Kg=gK$ for all $g \in G$.
(5) TRUE OR FALSE: In an arbitrary group G, every right K-coset is a subgroup of G.

Solution.

(1) Yes! In particular, because this group is abelian.
(2) $K\,(1\,2\,3)=\{(2\,3),(1\,2\,3)\}$ and $(1\,2\,3)\,K=\{(1\,2\,3),(1\,3)\}$.
(3) False. For a counterexample, consider the subgroup generated by $(1\,2)$ in S_3.
(4) True, because g commutes with all the elements in K.
(5) False. In particular, only one of the cosets contains the identity.

F. Fix a subgroup K of a group $(G,\circ)$.

(1) Show that $Ke=K=eK$.
(2) Show that for any $a \in G$, there is a bijection $K \longrightarrow Ka$.
(3) Prove that $|K \circ a|=|a \circ K|$, even if in general $K \circ a \neq \circ K$.
(4) Prove that if G is finite, the number of left K-cosets is the same as the number of right K-cosets.

Solution.

(1) $Ke=\{ke|k \in K\}=\{ek|k \in K\}=eK$.
(2) The map $k \mapsto ka$ is a bijection, with inverse $b \mapsto ba^{-1}$.
(3) The bijection $k \mapsto ka$ shows that $|K \circ a|=|K|$. Similarly, there is a bijection between K and aK.
(4) We have shown that the right K-cosets partition G into subsets of the size $|K|$; that means there must be $\frac{|G|}{|K|}$ right K-cosets. Similarly, the left K-cosets partition G into subsets all of size $|K|$, so there must be $\frac{|G|}{|K|}$ left K-cosets.

Part 2: Foreshadowing.

G. A CAUTIONARY EXAMPLE. Let G be a group and let K be a subgroup. Consider the set G/K of all right K-cosets. It is tempting to try to define a quotient group as we defined quotient rings. That is, we can try to define a binary operation $\star$ on G/K by $(K \circ g) \star (K \circ h) := K(g \circ h)$.

(1) Show that in the example of $7\mathbb{Z}$ in $\mathbb{Z}$ from A, $\star$ is a well-defined binary operation.
(2) Show that in the example of $K=\langle(1\,2)\rangle$ in S_3 as in B, $\star$ is **not** a well-defined binary operation. In fact, there is *no natural way to induce a quotient group structure on the set of cosets* G/K.
(3) For R_4 in D_4 in A, is $\star$ a well-defined binary operation on the set of right cosets D_4/R_4? Is $(D_4/R_4,\star)$ a group?

Solution.

(1) The operation $\star$ is the operation $+$ we have previously defined on $\mathbb{Z}_7$, and we have shown that is well-defined.
(2) $(1\,2\,3)(1\,2\,3) = (1\,3\,2)$, so if $\star$ is well-defined we should have $K(1\,2\,3) \star K(1\,2\,3) = K(1\,3\,2) \neq Ke$. However, $(2\,3) \in K(1\,3\,2)$ as well, and $(2\,3)(2\,3) = e$, which should mean that $K(1\,2\,3) \star K(1\,2\,3) = Ke$.
(3) Yes! We will come up with a better justification for this soon; for now, the best we can do is check all possible products.

H. A MATRIX EXAMPLE. Consider $G = GL_2(\mathbb{R})$, the subgroup $K = SL_2(\mathbb{R})$, and $A = \begin{bmatrix} 1 & 17 \\ 0 & \pi \end{bmatrix}$.

(1) Prove that the right K-coset KA in $GL_2(\mathbb{R})$ is $\{B \in GL_2(\mathbb{R}) \mid \det B = \pi\}$.
(2) Prove that the left K-coset $AK = KA$.
(3) Prove that the right K-cosets KC and KD are the same in this case if and only if $\det C = \det D$.
(4) What is the index $[GL_2(\mathbb{R}) : SL_2(\mathbb{R})]$?

Solution.

(1) A matrix B is in KA if and only if B is congruent to A modulo K, which means that $AB^{-1} \in K$. Equivalently,
$$1 = \det(BA^{-1}) = \det(B)\pi^{-1},$$
which is equivalent to $\det(B) = \pi$.
(2) A matrix B is in AK if and only if $A^{-1}B \in K$. Equivalently,
$$1 = \det(A^{-1}B) = \pi^{-1}\det(B),$$
which is equivalent to $\det(B) = \pi$.
(3) We have shown that $KC = KD$ if and only if C is congruent to D modulo K. So $KC = KD$ if and only if $\det(CD^{-1}) = 1$, or equivalently, by 217, $\det(C)\det(D)^{-1} = 1$.
(4) It's infinite: there is one coset for each real number.