Example: Theorems and Proofs

WriteLaTeX

February 8, 2014

Definition 1. Let H be a subgroup of a group G. A *left coset* of H in G is a subset of G that is of the form xH, where $x \in G$ and $xH = \{xh : h \in H\}$. Similarly a *right coset* of H in G is a subset of G that is of the form Hx, where $Hx = \{hx : h \in H\}$

Note that a subgroup H of a group G is itself a left coset of H in G.

Lemma 1. *Let H be a subgroup of a group G, and let x and y be elements of G. Suppose that $xH \cap yH$ is non-empty. Then $xH = yH$.*

Proof. Let z be some element of $xH \cap yH$. Then $z = xa$ for some $a \in H$, and $z = yb$ for some $b \in H$. If h is any element of H then $ah \in H$ and $a^{-1}h \in H$, since H is a subgroup of G. But $zh = x(ah)$ and $xh = z(a^{-1}h)$ for all $h \in H$. Therefore $zH \subset xH$ and $xH \subset zH$, and thus $xH = zH$. Similarly $yH = zH$, and thus $xH = yH$, as required. □

Lemma 2. *Let H be a finite subgroup of a group G. Then each left coset of H in G has the same number of elements as H.*

Proof. Let $H = \{h_1, h_2, \ldots, h_m\}$, where $h_1, h_2, \ldots, h_m$ are distinct, and let x be an element of G. Then the left coset xH consists of the elements xh_j for $j = 1, 2, \ldots, m$. Suppose that j and k are integers between 1 and m for which $xh_j = xh_k$. Then $h_j = x^{-1}(xh_j) = x^{-1}(xh_k) = h_k$, and thus $j = k$, since $h_1, h_2, \ldots, h_m$ are distinct. It follows that the elements $xh_1, xh_2, \ldots, xh_m$ are distinct. We conclude that the subgroup H and the left coset xH both have m elements, as required. □

Theorem 1. (Lagrange's Theorem) *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof. Each element x of G belongs to at least one left coset of H in G (namely the coset xH), and no element can belong to two distinct left cosets of H in G (see Lemma 1). Therefore every element of G belongs to exactly one left coset of H. Moreover each left coset of H contains $|H|$ elements (Lemma 2). Therefore $|G| = n|H|$, where n is the number of left cosets of H in G. The result follows. □