Abstract Algebra
Lecture 6
Monday, 9/20/2010

1 Quotient Groups, Continued

Recall: Let $N \leq G$. Then $N \trianglelefteq G$ (N is a normal subgroup of G) if $xNx^{-1} \subseteq N$ for all $x \in G$. If $N \trianglelefteq G$, then the quotient group G/N is a group, where

$$G/N = \{Ng \mid g \in G\}$$

under the operation $NxNy = Nxy$ and the map $\pi : G \to G/N$ defined by $\pi(g) = Ng$ is a homomorphism with $\ker(\pi) = N$.

Proof: We begin by showing that G/N is a group by showing that it is closed under its binary operation, associative, contains an identity element, and is closed under inverses. Since we have $1 \in G$, that implies $N1 \in G/N$. Then we have $NxN1 = Nx1 = Nx = N1x = N1Nx$, so $N1 = N$ is the identity. For all $x, y \in G$, we know that $xy \in G$. So $NxNy = Nxy \in G/N$, so it is closed. For all $x, y, z \in G$, $Nx(NyNz) = NxNyz = Nx(yz) = N(xy)z = NxyNz = (NxNy)Nz$, so we have associativity. Finally, for some $Nx \in G/N$, the inverse is $(Nx)^{-1} = N(x^{-1})$, so we have inverses.

Now, inspect π. Let $x, y \in G$. Then $\pi(xy) = Nxy = NxNy = \pi(x)\pi(y)$, so π is a homomorphism. Now we need to show that $\ker(\pi) = N$. Note that $1_{G/N} = N$. We know that $\ker(\pi) = \{x \in G \mid \pi(x) = N\}$. But $\pi(x) = Nx$. So we want to show that $\ker(\pi) = \{x \mid Nx = N\}$. Want to show $\ker(\pi) \subseteq N$ and $N \subseteq \ker(\pi)$ to show this equality. Let $n_0 \in N$. Then $\pi(n_0) = Nn_0 = \{nn_0 \mid n \in N\}$, so $nn_0 \in N$. But what we really want to show is that $Nn_0 = N$, so we are going to show $Nn_0 \subseteq N$ and $N \subseteq Nn_0$. We just showed that $Nn_0 \subseteq N$ above. Now, let $m \in N$. Then $mn_0^{-1} \in N$. Then $mn_0^{-1}n_0 = m$, where $n_0^{-1}n_0 \in Nn_0$, so $N \subseteq Nn_0$. Thus, $Nn_0 = N$, and now, $N \subseteq \ker(\pi)$. We now show that $\ker(\pi) \subseteq N$. Let $x \in \ker(\pi)$. Then $\pi(x) = Nx = N$, and recall that $Nx = \{nx \mid n \in N\}$. But $1 \in N$, so $1x \in Nx$, so $1x \in N$. Therefore, $\ker(\pi) \subseteq N$, and hence $\ker(\pi) = N$. QED. ∎

Theorem: Let $H \leq G$. The number of right cosets of H equals the number of left cosets of H.

Proof: Let $R = \{Hx \mid x \in G\}$ and $L = \{xH \mid x \in G\}$. Then $f : R \to L$ defined by $f(Hx) = x^{-1}H$ and $g : L \to R$ defined by $g(xH) = Hx^{-1}$ are mutually inverse, and therefore bijections. ∎

Defn: The **index** of $H \leq G$ is the number of its distinct right (or left) cosets. We denote this $[G : H]$.

Defn: A **partition** P of a set S is a collection of subsets $S_1, S_2, \ldots, S_n, \ldots \subseteq S$ that are exhaustive and disjoint:

1. $\cup S_i = S$,
2. $S_i \cap S_j = \emptyset$ if $i \neq j$.

Remark: Any equivalence relation $\sim$ on a set S **partitions** S into equivalence classes.

Recall: For any $H \leq G$, we have an equivalence relation $x \sim y \iff xy^{-1} \in H$ for any $x, y \in G$. Let $[x]$ denote the equivalence class of $x \in G$. Then

$$G = \bigcup_{x \in G} [x].$$

Note: Therefore,

$$xy^{-1} \in H \iff x \in Hy.$$

Theorem: Any two cosets of a group are either equal or disjoint.

Proof: Left as an exercise for the reader. ∎

2 Lagrange's Theorem

Theorem: If $H \leq G$, then $\boxed{|G| = |H| \cdot [G : H].}$

Corollary: If G is finite, then $|H|$ and $[G : H]$ divide $|G|$.

Proof: We claim that for any $x \in G$, $|H| = |Hx|$. Consider the map $H \to Hx$ given by right multiplication by x (this is clearly a bijection, with inverse of right multiplying by x^{-1}). We also know that $G = \cup_{x \in G} Hx$. But there are $[G : H]$ distinct cosets of H. So the total number of elements in the group is equal to the number of cosets, multiplied by the number of elements in each coset, or $|G| = |H|[G : H]$, as desired. ∎

Corollary: In a finite group, the order of every element divides the order of G.

Proof: The order of an element a is the order of the cyclic subgroup generated by that element, or $|a| = |\langle a \rangle|$, but $\langle a \rangle \leq G$. QED. ∎

Corollary: A group of prime order is cyclic (generated by a single element).

Proof: For all $a \in G$, $|a| = 1$ or $|a| = p = |G|$. Let $a \neq 1_G$. Then $|a| = |\langle a \rangle| = p$. QED. ∎

Corollary: Let G be finite, and let $a \in G$. Then $a^{|G|} = 1$.

Proof: Since $|a|$ divides $|G|$, $a^{|G|} = 1^n$ for some integer n. ∎