3.2: Cosets and Lagrange's Theorem

Alex L.

October 12, 2024

Def: The **order** of a finite group is how many elements are in the group. The order is an important group invariant to study.

Theorem: Lagrange's Theorem If G is a finite group and $H \leq G$, then the order of H divides the order of G, and the number of cosets of G/H is equal to $\frac{|G|}{|H|}$

Proof: Let the order of H be n, and the number of left cosets of H in G be k. The left cosets of H, gH, form k disjoint subsets, each with size n, so the total size of G is kn, therefore, if $|H| = n$, and $|G/H| = k$ (because the quotient group is the group of cosets), then $|G/H| = \frac{|G|}{|H|}$.

Def: If G is a group and $H \leq G$, the number of left cosets of H in G is called the **index** of H in G, and is denoted $|G : H|$.

Corrolary: If G is a finite group and $x \in G$, the order of x divides the order of G. Additionally, $x^{|G|} = 1$ for all $x \in G$

Proof: The order of x is equal to the order of the group generated by x, $| < x > |$. If we let that group equal H, then by Lagrange's Theorem, $|G|$ is a multiple of the order of x, meaning the second statement holds.

Corrolary: If G is a group of prime order p, then G is cyclic, hence $G \simeq Z_p$

Proof: Cyclic means a group that can be generated by a single element, and by extension, that element has the same order as the entire group. Let $x \in G$ and $x \neq 1_G$. Then, by the previous corrolary, the order of the group generated by x must divide $|G|$, but it can't be 1 because x is not the identity. Therefore, since $|G|$ is prime, $| < x > | = |G|$, and the group is cyclic.

Ex: Let H be a subgroup of G with H in G having an index of 2 (there are two cosets of H in G). Then, we will prove that H is normal in G

Proof: Let $g \in G - H$, then, we have two subgroups, $1H$ and gH, which together, partition G. $1H = H1$, so therefore, $gH = Hg$, and as we proved in section 3.1, $gH = Hg$ indicates H is normal in G.

Theorem: If G is a finite group and p is a prime which divides $|G|$, then there is an element of order p in G

Theorem: If G is a finite group of order $p^\alpha m$, where p is a prime and p doesn't divide m, then G has a subgroup of order p^α.

Def: Let H, K be subgroups and define

$$HK = \{hk \mid h \in H, k \in K\}$$

Prop: If H and K are finite subgroups, then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof: HK is actially the set of left cosets of K with elements of H. We want to find how many distinct left cosets of K there are.

Prop: If H and K are subgroups of a group, then HK is a subgroup if and only if $HK - KH$.

Proof: HK is the group of one element of H multiplied by another element from K. Forward Proof: Let h_1k_1, h_2k_2 be elements in HK. HK has an identity because both H and K have an identity. We want to show that $h_1k_1(h_2k_2)^{-1}$ is in HK. First, note that $(h_2k_2)^{-1}$ is equal to $k_2^{-1}h_2^{-1}$. Substituting, we get $h_1k_1k_2^{-1}h_2^{-1}$. Since K is a group, $k_1k_2^{-1}$ is equal to another element in K, k_3. Substituting, we get $h_1k_3h_2^{-1}$. Since $HK = KH$, for every element kh in KH, there is a corresponding hk in HK. As such, $k_3h_2^{-1}$ is equal to h_3k_4 in HK. Then, we get $h_1h_3k_4$, and since H is a group, the equation evaluates to h_4k_4. This is obviously in HK, so our proof is done.

Reverse Proof: We want to show that given the conditions that HK is a group, then $HK = KH$. To show equality of groups, we need to show they are subgroups of each other. Since $K \leq HK$ because 1_Hk, and $H \leq HK$, we know that $KH \subseteq HK$. To show the opposite, note that $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1}$, which is in KH, so every element of HK is in KH. We have established our two inclusions, so these sets are equal.

Corrolary: If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. If $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

Proof: Since H normalizes K, hk is in KH because $kh = hkh^{-1}h = hk$. Also, kh is in HK because $kh = hh^{-1}kh = hk$.

0.1 Exercises:

1. Which of the following are permissible orders for subgroups of order 120: $1, 2, 5, 7, 9, 15, 60, 240$, and what is the index of each order?
   Solution: The order of a subgroup must divide the order of the parent group. The index is the order of the parent group divided by the order of a subgroup. $(\text{order}, \text{index}) : (1, 120), (2, 60), (5, 12), (15, 8), (60, 2)$.

2. Prove the lattice of subgroup of S_3 is correctly drawn in Section 2.5.
   Solution: We want to show that all of the nodes are actually subgroups of S_3 and their parents. The order of S_3 is 6, and we have four subgroups drawn: $(1, 2, 3)$, $(1, 2)$, $(2, 3)$, $(1, 3)$. The order of these is $3, 2, 2, 2$ respectively. They are all indeed subgroups. None of them link to each other, which is also correct, so they are drawn correctly.

3. Proce the lattice of subgroups of Q_8 is correctly drawn in Section 2.5.
   Solution: The quaternion group has an order of 8, and the drawn subgroups are $(i), (j), (k), (-1)$, having orders of $4, 4, 4, 2$ respectively, and (-1) is a group of the former three, which all checks out.

4. Show that if $|G| = pq$ for some primes p and q, then either G is abelian or $Z(G) = 1$
   Solution: The center of a group, $Z(G)$ is always a subgroup of G, so by Lagrange's Theorem, $Z(G)$ has order $1, p, q$ or pq. If $Z(G)$ has order p or q, then it has index q or p respectively. Therefore, $G/Z(G)$ has a prime order, and by the corrolary above, it will be cyclic and therefore abelian. If the quotient group is abelian, so is the main group, so G is abelian. The only other cases are when $Z(G)$ has order pq, which means $Z(G) = G$ and so it is abelian, or when $Z(G)$ has order 1, in which case it is the trivial group, $\{1\}$, because it is the only group with order 1.