Section 10: Lagrange's Theorem

Theorem 0.1 (Lagrange's Theorem)**.** *Let H be a subgroup of a finite group G. Then, the order of H divides the order of G.*

With the example from the worksheet, we see that D_4 has order 8 and is a subgroup of S_4, and there are 3 distinct cosets, and $24 = 8 \cdot 3$. Lagrange's Theorem says this always happens: (size of group) = (size of subgroup) $\times$ (number of cosets).

Definition 0.2. Let H be a subgroup of a finite group G. The **index** of H in G, denoted $(G : H)$, is the number of left cosets of H in G.

With this, Lagrange's Theorem could be stated as $|G| = |H|(G : H)$.

Corollary 0.3. If G is a finite group and $a \in G$ is any element, then the order of a divides the order of G.

Proof. The order of a is the smallest positive integer such that $a^m = e$, which is equivalent to saying the order of the subgroup $\langle a \rangle$ is m. By Lagrange's Theorem, m divides the order of G. □

Example 0.4. Let G be a group with six elements. This corollary says that, for any $a \in G$, the order of a divides 6. So, $\text{ord}(a) = 1, 2, 3$ or 6. We an actually say even more: if $\text{ord}(a) = 1$, then $a = e$. If $\text{ord}(a) = 6$, then $\langle a \rangle = \{e, a, a^2, a^3, a^4, a^5\} \subset G$, so $\langle a \rangle = G$ and G is cyclic.[1]

We know another group of order 6: S_3! All of the elements of S_3 have order $1, 2$, or 3 (order 1: ι, order 2: transpositions, like (12), order 3: cycles of length 3, like (123)). Here is a fact that you should think about: if G is a group of order 6 and no element of G has order 6, then $G \cong S_3$.

Corollary 0.5. If G is a finite group of prime order p, then G is cyclic.

Proof. The previous corollary implies that, if a is any non-identity element of G, then $\text{ord}(a) = p$, so $\langle a \rangle = G$, so G is cyclic. □

Corollary 0.6. If G is a group of order n, then $a^n = e$ for any element $a \in G$.

Proof. We know $\text{ord}(a)$ divides n, so $n = \text{ord}(a)k$ for some integer k, so $a^n = a^{\text{ord}(a)k} = e^k = e$. □

Example 0.7. We have talked a lot about $\mathbb{Z}_n$, and today we will introduce a new variant.

Let $M_n \subset \mathbb{Z}_n$ be the subset $U_n = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. Prove that $(M_n, \cdot_n)$ is a group.

To show this is a group, we observe that 1 is the identity and the binary operation is well defined: if a and b are two elements such that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$. (In words, this is just saying that if a and n have no common divisors and b and n have no common divisors, then ab and n can have no common divisors.) Finally, we show that inverses exist: if $\gcd(a, n) = 1$, then $1 = ar + ns$ for some integers r and s (this is from the definition of gcd we gave when we were talking about subgroups of cyclic groups!). So, modulo n, $ar = 1 \mod n$, so $r = a^{-1}$. So, a^{-1} exists, and we need to show $\gcd(a^{-1}, n) = 1$ so

[1] Fact: we've seen this before, but let's say it again: a group G of order n is cyclic if and only if G contains an element of order n.

that a^{-1} is actually in the group. But this is true: $aa^{-1} = 1 \mod n$, so $\gcd(aa^{-1}, n) = 1$, and $\gcd(a, n) = 1$, so we must have $\gcd(a^{-1}, n) = 1$.

How many elements does M_n have? We give a new definition.

Definition 0.8. For any integer n, the number of elements in $\mathbb{Z}_n$ that are relatively prime to n is called the **Euler totient function** of n, denoted $\phi(n)$.

With this definition, $|M_n| = \phi(n)$.

Corollary 0.9. For any integer a, n such that $\gcd(a, n) = 1$, then $a^{\phi(n)} = 1 \mod n$.

Proof. It suffices to show this for $a \in M_n$, and by the previous corollary of Lagrange's Theorem, we know that $a^{|M_n|} = a^{\phi(n)} = 1 \mod n$. □

Corollary 0.10. For any integer a and prime number p, if $\gcd(a, p) = 1$, $a^{p-1} = 1 \mod p$.

Proof. If p is prime, $\phi(p) = p - 1$, so $a^{p-1} = a^{\phi(p)} = 1 \mod p$. □

This can work as a cool primality test. In general, it is hard to look at a number and determine the prime factorization. But, if we have some big number n that we think might be prime, we can pick a number a such that a is not a multiple of n and compute $a^{n-1} \mod n$. If it is not 1, then n can't be prime.

We'll close with asking if Lagrange's Theorem has a converse:

Question 0.11. If $|G| = n$ and d is a divisor of n, if there a subgroup of G of size d?

The answer is no in general, but yes in some cases. We have already seen this is true for any finite cyclic group (because then $G \cong \mathbb{Z}_n$ and we got one subgroup for each divisor of n). Here is some practice.

Example 0.12. Let $G = S_3$. Show that G has a subgroup of size d for every divisor d of 6.

Example 0.13. Let $G = A_4$. Show that G does not have a subgroup of size 6 (even though 6 is a divisor of $12 = |G|$).