Lagrange's Theorem: Statement

Definition: The *Cardinality* of a set is how many objects it contains. Formally, two sets have the same cardinality if there exists a bijection between them. The *order* of a group is the amount of elements it contains.

Lemma: Let H be a subgroup of a finite group G. Then for any $g_1, g_2 \in G$, $|g_1H| = |g_2H|$. That is, any arbitrary pair of left cosets of H in G have the cardinality.

Proof:
Let $g \in G$, where G is a finite group and let $h \in H$, where H is a subgroup of G. It suffices to show that there exists a bijection between the elements of H and gH. Define the functions:

$$A: H \to gH, A(h) = gh$$
$$B: gH \to H, B(gh) = g^{-1}gh$$

It is easy to see that $A \circ B(gh) = A(g^{-1}gh) = A(h) = gh$ and $B \circ A(h) = B(gh) = g^1gh = h$. So, because both $A \circ B$ and $B \circ A$ are the identity mappings, they are inverses of each other. Hence, they are bijections between H and gH, so H and gH have the same cardinality.
Consequently, since the cardinality of any arbitrary left coset is equal to that of the subgroup it is formed by, any of this subgroup's cosets must have the same cardinality.

■

The advantage of defining equal cardinalities in this way rather than just counting them or defining it intuitively, is that this definition also generalises to infinite sets. However, we are not dealing with infinite sets here, as Lagrange's theorem doesn't apply to them. Infinity being divisible by some quantity does not have any rigorous meaning at this point.

Lemma: Given a subgroup $H \leq G$, the distinct cosets of H in G are disjoint, and their union covers G.

Proof:
Since H is a subgroup, it contains the identity element e. Then for any $g \in G$ we of course have $g = ge$. But since e is in H, we have $g = ge \in gH$. So any element of G is in at least one of the cosets of H. So the union of the cosets covers G.

To prove that the distinct cosets are disjoint, assume that g_1H and g_2H, where $g_1, g_2 \in G$, are distinct cosets of H in G which contain a common element x. Then for some $h_1, h_2 \in H$, it must be true that $x = g_1h_1 = g_2h_2$. Multiplying on both sides by the inverse of h_1, we have $g_1 = g_2h_2h_1^{-1}$. Then if we take any arbitrary element from the coset g_1H, which may be written as g_1h where h is an element of H, we have $g_1h = g_2h_2h_1^{-1}h$. But since H is closed under the operation, $h_2h_1^{-1}h$ is in H as well. So then $g_1h = g_2h_2h_1^{-1}h \in g_2H$. This shows that any element in the coset g_1H must also be contained in the coset g_2H. Using the same steps,

it is also easy to show that any element of g_2H must also be in g_1H. This means that the two cosets are exactly the same, so we have a contradiction.

■

Lagrange's Theorem: Let G be a finite group, and H be a subgroup of G. Then, the order of H divides that of G.

Proof:
This result easily follows from the previous lemma. Since the set of left cosets in G are a partition of G, the sum of each of their cardinality is that of G. But since we have shown that each left coset has the same cardinality, if follows that $|G| = [G:H]|H|$. Hence, $[G:H] = \frac{|G|}{|H|}$.

■

The converse of this theorem states that whenever d is a divisor of $|G|$, there exists a subgroup $H \leq G$ such that $|H| = d$. This is not in fact true in general. The smallest counterexample is in the group of rotational symmetries of a tetrahedron. The rotational symmetries form a group of order 12, but there is no subgroup of order 6.

Applications in number theory

It is not hard to see that the set of integers are closed under multiplication modulo n, the binary operation is associative, and that the integers $1\ (mod\ n)$ are the identity element. Is it also the case that there exists and identity and inverse for each element?
If m is coprime to n, then $\gcd(m,n) = 1$. Then by Bezout's lemma, there exist integers a and b such that $am + bn = 1$, and hence, $am = 1 - bn = 1\ (mod\ n)$. This makes a reduced modulo n the inverse for m, so all integers coprime to n have an inverse less than n. Moreover, a must also be coprime. It is also true that multiplying to integers coprime. to n and reducing modulo n, we arrive at another integer coprime to n. Since the set of integers less than and coprime to n under the operation of multiplication modulo n is closed under the operation, contains the identity element 1, and is closed under taking inverses, this set in fact forms a group. This is known as the multiplicative group of integers modulo n, and has an order of $\varphi(n)$.

Euler's Theorem: If a and n are coprime integers, then $a^{\varphi(n)} \equiv 1\ (mod\ n)$.

Proof:
Let a be an element of the multiplicative group of integers modulo n. Now consider the set $\{a, a^2, a^3, a^4, \dots\}$. Since the group was finite, this set must also be. So there exist smallest integers $q < r$ such that $a^q = a^r\ (mod\ n)$. Since a and n are coprime, a has an inverse element a^{-1}. We can multiply on both sides by this r times to arrive at $a^{q-r} = 1$. Let $k = q - r$ so a^k is the identity element. It is also evident that for any integer $m \leq k$, $a^m a^{k-m} = a^k = 1$. So a^{k-m} acts as an inverse to every a^m. It is now evident that $\{a, a^2, a^3, a^4, \dots, a^k\}$ is a subgroup of the multiplicative group of integers modulo n.

Then since the order of this subgroup is k, by Lagrange's theorem it must divide the $\varphi(n)$, the order of the multiplicative group of integers modulo n. So then it must be true that for some integer M, $kM = \varphi(n)$. We then have

$$a^{\varphi(n)} = a^{kM} = (a^k)^M = 1^M = 1 \ (mod\ n)$$

■

Note that this is a generalisation of Fermat's little theorem. Fermat's little theorem is the special case where n is prime, so that $\varphi(n) = n - 1$ and hence,

$$a^{n-1} = 1 \ (mod\ n)$$
$$a^n = a \ (mod\ n)$$