Formalizing Lagrange's Theorem

Max Hildebrand

05/05/2024

Solution.

We are looking to prove Lagrange's Theorem, which states that if G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Let's begin by defining what it means to be a group. A group is a set G with a binary operation $\cdot$ that satisfies the following properties:

(a) Closure: For all $a, b \in G$, $a \cdot b \in G$.

(b) Associativity: For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(c) Identity: There exists an element $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$.

(d) Inverses: For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Now, let's define what it means to be a subgroup. A subgroup is a subset with some extra properties.

We can think of a subgroup as a non-empty subset H of a group G that is itself a group under the same operation. In other words, H is a subgroup of G if it satisfies the following properties:

(a) Closure: For all $a, b \in H$, $a \cdot b \in H$.

(b) Identity: There exists an element $e \in H$ such that for all $a \in H$, $a \cdot e = e \cdot a = a$.

(c) Inverses: For all $a \in H$, there exists an element $a^{-1} \in H$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

It is important to note some important facts about subgroups, that follow from the fact that it is itself a group with respect to the original group's operation.

(a) The identity element of G is also the identity element of H.

(b) The inverse of an element in H is also in H.

(c) The associativity of the group operation is inherited by H.

Now, we can introduce the idea of a coset. There are both left and right Cosets, but we will only be discussing left cosets, as they are all that is needed for the proof of Lagrange's Theorem.

Let G be a group and H be a subgroup of G. For any $a \in G$, the left coset of H in G is defined as $aH = \{ah | h \in H\}$.

In order to make sure that we are thinking properly about these, I'll define a general example of a coset:

Let G be a group, with H a subgroup of G. Lets say that $H = \{e, h_1 \dots h_n\}$, and $a \in G$ is an element that is in G but not in H.

Then, the left coset of H in G is $aH = \{a, ah_1 \dots ah_n\}$.

Let's define some important properties of cosets:

(a) The left coset of H in G is a subset of G.

(b) for any $a, b \in G$, $aH = bH \iff a^{-1}b \in H$.

Note that this second property is very important, as it will be the key to proving Lagrange's Theorem, and is the basis of our sameLeftCoset Inductive in the Coq proof.

Great, now we have our basic structure set up, let's prove some other useful Lemmas that will help us prove Lagrange's Theorem.

Lemma 1. *Let G be a group, and $h, g \in G$. Then, $gh = e \implies g = h^{-1}$.*

Proof. So, let's start with our assumption:

$$g \cdot h = e$$

Now, let's multiply both sides by h^{-1}:

$$g \cdot h \cdot h^{-1} = e \cdot h^{-1}$$

$$g \cdot e = h^{-1}$$

$$g = h^{-1}$$

And we're done. □

We can see that this proof also extends to subgroups, as they are themselves groups.

Lemma 2. *Let G be a group, and H be a subgroup of G. Then, for any $a \in G$, $aH = aH$.*

Proof. Lets use our sameLeftCoset property to show this:

$$aH = aH \iff a^{-1}aH = a^{-1}aH$$

$$eH = eH$$

$$H = H$$

Okay, this one was a little silly, but let's go look at Coq. □

Lemma 3. *Let G be a group, and H be a subgroup of G. Then, for $g_1, g_2 \in G$, $g_1H = g_2H \implies g_2H = g_1H$.*

Proof. Let's use our sameLeftCoset property to show this:

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H$$

$$g_2H = g_1H \iff g_2^{-1}g_1 \in H$$

But, we know that $g_1^{-1}g_2 \in H \implies g_2^{-1}g_1 \in H$, because H is closed under inverses.

Notice how $(g_1^{-1}g_2) \cdot (g_2^{-1}g_1) = e$, so these two elements are inverses of each other. □

Lemma 4. *Let G be a group, and H be a subgroup of G. Then, for $g_1, g_2, g_3 \in G$, $g_1H = g_2H \wedge g_2H = g_3H \implies g_1H = g_3H$.*

Proof. Let's use our sameLeftCoset property to show this:

$$g_1H = g_2H \wedge g_2H = g_3H \iff g_1^{-1}g_2 \in H \wedge g_2^{-1}g_3 \in H$$

$$g_1H = g_3H \iff g_1^{-1}g_3 \in H$$

But, we know that $g_1^{-1}g_2 \in H \wedge g_2^{-1}g_3 \in H \implies g_1^{-1}g_3 \in H$, because H is closed under inverses.

Notice how $(g_1^{-1}g_2) \cdot (g_2^{-1}g_3) = g_1^{-1}g_3$, so these two elements are inverses of each other. □

So now, we have proven three named properties about sameLeftCoset:

(a) Reflexivity: $aH = aH$.

(b) Symmetry: $g_1H = g_2H \implies g_2H = g_1H$.

(c) Transitivity: $g_1H = g_2H \wedge g_2H = g_3H \implies g_1H = g_3H$.

These properties combine to prove that the left cosets of H in G form an equivalence relation.

Lemma 5. *Let G be a group, then $g \in G \implies g$ is in come coset of H, where H is a subgroup of G.*

Proof. Let's just look at the left coset of H in G corresponding to g, gH. We know that $g \in gH$, since $e \in H$, and $g \cdot e = g$ so we're done. □

So, we have now proven that every element of G is in some left coset of H in G.

Lemma 6. *Cosets of H, where H is a subset of G are either disjoint or equal.*

Proof. Let's assume that aH and bH are not disjoint, and that there is some element c that is in both aH and bH.

This means that $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$.

So, we can write $a = b \cdot h_2 \cdot h_1^{-1}$.

But, we know that $h_2 \cdot h_1^{-1} \in H$, so $aH = bH$. □

Lemma 7. *There exists a bijection between any two left cosets of H in G.*

Proof. Let's assume that aH and bH are two left cosets of H in G.

Let's define a function $f : aH \mapsto bH$ such that $f(x) = b \cdot a^{-1} \cdot x$.

We can see that this function is bijective, as it has an inverse $f^{-1}(x) = a \cdot b^{-1} \cdot x$. □

Lemma 8. *Let G be a group, and H be a subgroup of G. Then, the left cosets of H in G partition G.*

Proof. We know that the left cosets of H in G are either disjoint or equal. We also know that every element of G is in some left coset of H in G.

So, we have shown that the left cosets of H in G partition G. This means that the union of all left cosets of H in G is equal to G. □

Now, we have proven that all of our cosets are disjoint, and that they partition G, and are also all of the same size, as they are bijective.

A little bit of notation before we prove the theorem, $|G| = n$ means that G has cardinality n, or n items in the group.

Now, we can prove Lagrange's Theorem.

Theorem 9. *Let G be a finite group, and H be a subgroup of G. Then, the cardinality of H divides the order of G, ie $|G| = n|H|$.*

Proof. Let's start by defining the left cosets of H in G as $a_1H, a_2H, \ldots, a_nH$, where n is the order of G.

We know that the union of all left cosets of H in G is equal to G, so we can write:

$$G = a_1H \cup a_2H \cup \ldots \cup a_nH$$

Now, let's look at the cardinality of G:

$$|G| = |a_1H| + |a_2H| + \ldots + |a_nH|$$

$$|G| = n|H|$$

So, we have shown that the order of H divides the order of G. □

□