One of the central problems in group theory is to understand the structure of a group by understanding the structure of its subgroups.

One cannot talk about finite group theory without mention of Lagrange's Theorem. This is arguably the most important theorem in finite group theory. In a sense, it restricts the sizes of the subgroups of a group. Lagrange's Theorem tells us that the order of a subgroup must divide the order of a group. Of course, this only holds for finite groups.

How should we prove something like this? Let G be a finite group and let H be a subgroup of G. If we can somehow bundle together the elements of a group into piles of $|H|$, the result should follow. But what is the correct way to bundle them? Here is one way.

Definition 0.1 (Coset)**.** Let G be a group and let H be a subgroup of G. A (left) coset of H, denoted gH is the set

$$gH = \{\, gh : h \in H \,\}.$$

Why are cosets important? It turns out that cosets form a partition of G, and that the size of a coset is precisely the size of the subgroup H.

Recall that an equivalence relation $\sim$ on G is a relation that is reflexive, symmetric and transitive. Equivalence relations give rise to partitions. If $\sim$ is an equivalence relation on G and $g \in G$, then the set

$$[g]_\sim = \{\, a \in G : a \sim g \,\}$$

denotes the equivalence class of g under $\sim$. If the equivalence relation is clear, we shall simply write $[g]$.

Proposition 0.2 (Coset is an equivalence relation)**.** *Let G be a finite group and H a subgroup of G. Define the equivalence relation $\sim$ on G by $a \sim b$ if and only if $a^{-1}b \in H$. Then, $\sim$ is an equivalence relation and $aH = [a]$, where $[a]$ is the equivalence class of a under $\sim$.*

Proof. Exercise. □

Exercise 0.3. Prove Proposition 0.2.

Theorem 0.4 (Properties of cosets)**.** Let G be a finite group and let H be a subgroup of G. Then, the following are true.

1. $a \in aH$.
2. $aH = H$ if and only if $a \in H$.
3. $aH = bH$ if and only if $a^{-1}b \in H$.
4. $aH = Ha$ if and only if $aHa^{-1} = H$.
5. $|aH| = |bH|$. In other words, different cosets have the same size.
6. aH is a subgroup if and only if $a \in H$.

Proof.

1. Obvious.
2. Clearly.
3. Follows from 2.
4. Easy to see.
5. Define a bijection from aH to bH by sending $x \in aH$ to $ba^{-1}x$.
6. Clearly.

□

Since writing "obvious" and "clearly" for a proof doesn't really constitute a proof, we have the following exercise.

Exercise 0.5. Prove Theorem 0.4.

Now, take a good look at property number 5 of Theorem 0.4. This is the key idea here. It tells us that the equivalence classes of the coset relation all have the same size. We are now ready to prove Lagrange's Theorem. With the coset equivalence relation, we cut up G into pieces of size $|H|$.

Theorem 0.6 (Lagrange's Theorem)**.** Let G be a finite group of order n. Let H be a subgroup of G. Then, $|H|$ divides n.

Proof. Exercise. □

Exercise 0.7. Prove Theorem 0.6

One thing you may have noticed is that the proof of Lagrange's Theorem was rather trivial. How does such a powerful theorem have such a trivial proof? The key answer lies in how the definitions were formulated.

We now state some corollaries of Lagrange's Theorem. These are obvious.

Corollary 0.8 (Consequences of Lagrange's Theorem)**.** Let G be a finite group. Then, the following are true.

1. If $g \in G$, $|g|$ divides $|G|$.
2. If G has prime order then it is cyclic.
3. If $g \in G$, then $g^{|G|} = e$.

Exercise 0.9. Prove Corollary 0.8.

Let us now see an application of Lagrange's Theorem.

Corollary 0.10 (Fermat's Little Theorem)**.** Let p be a prime, and let a be an integer. Then, $a^p \bmod p = a \bmod p$.

Proof. To do this, we study the behavior of an element of $U(p)$. Recall that $U(p) = \{1, \ldots, p-1\}$, which has order $p-1$. If $a \in U(p)$, we would have $a^{|U(p)|} = 1$, so $a^p = a$. If a is not in $U(p)$, then use the division algorithm on a. □

Exercise 0.11. Fill in the details of Corollary 0.10.