One of the central problems in group theory is to understand the structure of a group by understanding the structure of its subgroups. Of course, this is a very difficult question to answer. Given a group G, how can we possibly hope to find all of its subgroups? Admittedly, we only have to check a finite number of sets, namely elements of $\mathcal{P}(G)$. We can even dispose of a bunch of sets quite fast (any sets not containing the identity). But that's still a lot! Can we narrow our search more?

We do have a sufficient condition for something to be a subgroup, namely, the definition. But that doesn't help us much, since we would still need to manually check whether something is a subgroup. What about a necessary condition? Do subgroups have any properties that they must satisfy? Turning our attention temporarily to cyclic groups, we notice that the subgroups of all cyclic groups have orders the divisor of the order of the whole group. So the orders of subgroups of cyclic groups divides the order of the group. Is this true in general?

The answer to this question is yes. 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? To find out how to do so, let us look at some examples.

Let $G = \mathbb{Z}_{10}$. We know all the subgroups of G, since G is cyclic. Let us consider the subgroup of G that consists of all the even numbers. Now, we know that there are just as many odd numbers. Indeed, if $H = \{0, 2, 4, 6, 8\}$, then the odd numbers would be $\{1, 3, 5, 7, 9\}$. Now, notice that if we take each element of H and add 1 to it, i.e. $1 + H$, we would arrive at the set of odd numbers. It also appears that $1 + H$ is disjoint from H. Motivated by this example, we turn our attention to the subgroup $H = \{0, 5\}$. In a similar fashion, we can consider $1 + H = \{1, 6\}$, $2 + H = \{2, 7\}$ as well as $3 + H, 4 + H$. What is $5 + H$? It appears that $5 + H$ is just H, and $6 + H$ is just $1 + H$. So it appears that if $h \in H$, then $h + H = H$. Another interesting observation we can make is that $g + H$ and $g' + H$ appear to be either equal to each other, or disjoint.

We summarize our observations:

1. The sets of the form $g + H$ seem to all have the same size
2. We either have $g + H = g' + H$ or they are disjoint

At this point, these are all conjectural. So let us now make this precise.

> **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. The language of partitions is equivalence relations, and we shall now talk about them.

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.

Note that we can declare a similar equivalence relation by saying that $a \sim b$ if and only if there is some $h \in H$ such that $a = hb$.

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 $a \in H$.
7. $aH = bH$ or aH is disjoint from bH

Proof.

1. Notice $a = ae \in aH$.
2. This follows from Proposition 0.2.
3. Follows from 2.
4. Exercise.
5. Define a bijection from aH to bH by sending $x \in aH$ to $ba^{-1}x$.
6. Use 2 and 3.
7. Being in the same coset is an equivalence relation.

□

Exercise 0.5. Fill in the details of the proof of 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. See Exercise 0.7. □

Exercise 0.7. Prove Theorem 0.6. You will need Proposition 0.2 and property 5 in Theorem 0.4.

We again direct our attention to the power of definitions. Having the correct choice of equivalence relation made the proof of Lagrange's Theorem very easy. As such, it would do a lot of good to understand how such an equivalence relation was chosen. Lagrange's theorem now motivates the following definition: the *index of a subgroup*. If H is a subgroup of G, then we let $[G : H]$ denote the number of left cosets of H. This is called the *index of H in G*. We leave it to the reader to verify that $[G : H]$ is the same number if we used right cosets instead of left. If there are infinitely many cosets, we write $[G : H] = \infty$.

We now state some corollaries of Lagrange's Theorem. While obvious, they are still good to mention.

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.

To really demonstrate the power of Lagrange's theorem, we shall see some applications of it. The first application is in number theory.

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 (divide it by p). □

Exercise 0.11. Fill in the details of Corollary 0.10.

Lagrange's theorem also gives us a useful counting theorem which tells us what the sizes of subgroups can be.

Theorem 0.12 (HK theorem). Let H, K be finite subgroups of some group G. Define $HK = \{hk : h \in H, k \in K\}$. Then,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Let's talk strategy. Of course, HK has $|H| \cdot |K|$ products, but they may not be distinct group elements. What this means is that we could have $hk = h'k'$ where $h \neq h', k \neq k'$. The formula suggests that duplicates occur in multiples of $|H \cap K|$. We need some way to tie each product in HK to every single element of $|H \cap K|$. The first observation comes from noticing that if $t \in H \cap K$, then $hk = (ht)(t^{-1}k)$.

Proof. Let $h \in H, k \in K$. If $t \in H \cap K$, then $hk = (ht)(t^{-1}k)$. This tells us that every element of HK is represented by at least $|H \cap K|$ products in HK. Suppose $hk = h'k'$, then,

$$tt^{-1} = h^{-1}h'k'k^{-1}.$$

So if $t = h^{-1}h' = kk'^{-1}$, then it all works out. This shows that every element in HK is represented by precisely $|H \cap K|$ products. □

The proof here actually leads to a proof of a more general fact, which is outlined in Exercise 0.19.

Let us now see another application of Lagrange's theorem. This time, we classify all groups of order $2p$ where p is some odd prime.

Theorem 0.13 (Classification of groups of order $2p$). Let p be a prime such that $p > 2$. Let G be a group of order $2p$. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.

Proof. See Exercise 0.16. □

Counting can be useful. We now make use of Lagrange's theorem to prove a fact about group actions.

Theorem 0.14 (Orbit-Stabilizer Theorem). Let G be a finite group acting on a set S. Then,

$$|G| = |\mathrm{orb}_G(s)||\mathrm{stab}_G(s)|.$$

Proof. The stabilizer of s is a subgroup of G. It will suffice to provide a bijection between left cosets of $\mathrm{stab}_G(s)$ and elements in $\mathrm{orb}_G(s)$. The map $\varphi : g\,\mathrm{stab}_G(s) \mapsto g \cdot s$ will do. We leave the details to the reader in Exercise 0.17. □

0.0.1 Exercises and Problems

Exercise 0.15. Suppose that G is finite. Let $H \leq G$ and $K \leq H$. Show that $[G : K] = [G : H][H : K]$.
Exercise 0.16. Prove Theorem 0.13 by following the steps below.

1. Assume that G has no element of order $2p$. Show that G must have an element of order p, call it a.
2. Find an element of order 2, call it b.
3. Show that a and b satisfy the relations of D_p: in particular, $a^j b = ba^{-j}$ for $j \in \{1, \ldots, p-1\}$.

4. Show that every element of G can be uniquely expressed in the form $a^j b^k$.

5. Conclude that G is isomorphic to D_p.

Exercise 0.17 (Orbit-Stabilizer Theorem)**.** Complete the proof of Theorem 0.14. In particular, show that the map φ as defined is well-defined and a bijection. Note that the facts in **??** will be needed.

Exercise 0.18. Prove that the rotation group of a cube is S_4.

Exercise 0.19 (Generalization of HK theorem)**.** Let H, K be subgroups of G, and $\alpha : H \times K \to G$ be the map defined by $\alpha(h, k) = hk$. Prove that $\alpha^{-1}(hk) = \{\, (ht, t^{-1}k) : t \in H \cap K \,\}$, and that additionally the cardinality of $\alpha^{-1}(hk)$ equals to the cardinality of $H \cap K$. Conclude that if H, K are finite, then $|HK| = |H||K|/(|H \cap K|)$.

See [Jac09, Exercise 9, p. 58]

Exercise 0.20 (Index is multiplicative)**.** Let G be a group (not necessarily finite) and let $H \leq K \leq G$. Prove that $[G : H] = [G : K][K : H]$. Do not assume that any of the indices are finite.

Hint: There is a canonical surjection p from left cosets of H to left cosets of K. Consider the size of $p^{-1}[\{gK\}]$.