8. Lagranges Theorem

Definition 8.1. *Let G be a group and let H be a subgroup.*

*The **index of** H **in** G, denoted $[G : H]$, is equal to the number of left cosets of H in G.*

Note that even though G might be infinite, the index might still be finite. For example, suppose that G is the group of integers and let H be the subgroup of even integers. Then there are two cosets (evens and odds) and so the index is two.

We are now ready to state our first Theorem.

Theorem 8.2 (Lagrange's Theorem)**.** *Let G be a group. Then*

$$|H|[G : H] = |G|.$$

In particular, if G is finite then the order of H divides the order of G.

Proof. Since G is a disjoint union of its left cosets, it suffices to prove that the cardinality of each coset is equal to the cardinality of H.

Suppose that gH is a left coset of H in G. Define a map

$$\alpha \colon H \longrightarrow gH$$

by sending $h \in H$ to $\alpha(h) = gh$. α is clearly well-defined. Define a map

$$\beta \colon gH \longrightarrow H$$

by sending $k \in gH$ to $\beta(k) = g^{-1}k$. The image of β surely lands in G and it is not too hard to check it lands in H. Thus β is well-defined.

We show that β is the inverse of α. We first compute

$$\beta \circ \alpha \colon H \longrightarrow H.$$

Suppose that $h \in H$, then

$$\begin{aligned}(\beta \circ \alpha)(h) &= \beta(\alpha(h)) \\ &= \beta(gh) \\ &= g^{-1}(gh) \\ &= h.\end{aligned}$$

Thus $\beta \circ \alpha \colon H \longrightarrow H$ is certainly the identity map. Now consider

$$\alpha \circ \beta \colon gH \longrightarrow gH.$$

Suppose that $k \in gH$, then

$$\begin{aligned}(\alpha \circ \beta)(k) &= \alpha(\beta(k)) \\ &= \alpha(g^{-1}k) \\ &= g(g^{-1}k) \\ &= k.\end{aligned}$$

Thus β is indeed the inverse of α. In particular α must be a bijection and so H and gH must have the same cardinality. □

Lemma 8.3. *Let G be a group and let H_i, $i \in I$ be a collection of subgroups of G.*

Then the intersection

$$H = \bigcap_{i \in I} H_i$$

is a subgroup of G

Proof. First note that H is non-empty, as the identity belongs to every H_i. We have to check that H is closed under products and inverses.

Suppose that g and h are in H. Then g and h are in H_i, for all i. But then $gh \in H_i$ for all i, as H_i is closed under products. Thus $gh \in H$.

Similarly as H_i is closed under taking inverses, $g^{-1} \in H_i$ for all $i \in I$. But then $g^{-1} \in H$.

Thus H is indeed a subgroup. □

Definition-Lemma 8.4. *Let G be a group and let S be a subset of G.*

*The **subgroup** $H = \langle S \rangle$ **generated by** S is equal to the smallest subgroup of G that contains H.*

Proof. The only thing to check is that the word smallest makes sense.

Suppose that H_i, $i \in I$ is the collection of subgroups that contain S. By (8.3), the intersection H of the H_i is a subgroup of G.

On the other hand H obviously contains S and it is contained in each H_i.

Thus H is the smallest subgroup that contains S. □

Lemma 8.5. *Let S be a non-empty subset of G.*

Then the subgroup H generated by S is equal to the smallest subset of G, containing S, that is closed under taking products and inverses.

Proof. Let K_i, $i \in I$ be the collection of all subsets of G closed under taking products and inverses. Then the intersection K is closed under products and interses. Let K be the smallest subset of S, closed under taking products and inverses.

As H is closed under taking products and inverses, it is clear that H must contain K. On the other hand, as K is a subgroup of G, K must contain H.

But then $H = K$. □

Definition 8.6. *Let G be a group. We say that a subset S of G **generates** G, if the smallest subgroup of G that contains S is G itself.*

Definition 8.7. *Let G be a group. We say that G is **cyclic** if it is generated by one element.*

Let $G = \langle a \rangle$ be a cyclic group. By (8.5)

$$G = \{\, a^i \mid i \in \mathbb{Z} \,\}.$$

Definition 8.8. *Let G be a group and let $g \in G$ be an element of G.*

*The **order** of g is equal to the cardinality of the subgroup generated by g.*

Lemma 8.9. *Let G be a finite group and let $g \in G$.*

Then the order of g divides the order of G.

Proof. Immediate from Lagrange's Theorem. □

Lemma 8.10. *Let G be a group of prime order.*

Then G is cyclic.

Proof. One is not a prime so we may pick an element g of G not equal to the identity. As g is not equal to the identity, its order is not one. As the order of g divides the order of G and this is prime, it follows that the order of g is equal to the order of G.

But then $G = \langle g \rangle$ and G is cyclic. □

It is interesting to go back to the problem of classifying groups of finite order and see how these results change our picture of what is going on.

Now we know that every group of order 1, 2, 3 and 5 must be cyclic. Suppose that G has order 4. There are two cases. If G has an element a of order 4, then G is cyclic.

We get the following group table.

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	a	a
a^3	a^3	e	a	a^2

Replacing a^2 by b, a^3 by c we get

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	a	a
c	c	e	a	b

Now suppose that G does not contain any elements of order 4. Since the order of every element divides 4, the order of every element must be 1, 2 or 4. On the other hand, the only element of order 1 is the identity element. Thus if G does not have an element of order 4, then every element, other than the identity, must have order 2.

In other words, every element is its own inverse.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	?	
b	b		e	
c	c			e

Now ? must in fact be c, simply by a process of elimination. In fact we must put c somewhere in the row that contains a and we cannot put it in the last column, as this already contains c. Continuing in this way, it turns out there is only one way to fill in the whole table

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(We will check later that there is a group of order 4 which is not cyclic; since we have just shown this is the only possible non cyclic group of order 4, multiplication must be associative).

So now we have a complete classification of all finite groups up to order five (it easy to see that there is a cyclic group of any order; just take the rotations of a regular n-gon). If the order is not four, then the only possibility is a cyclic group of that order. Otherwise the order is four and there are two possibilities.

Either G is cyclic. In this case there are two elements of order 4 (a and a^3) and one element of order two (a^2). Otherwise G has three elements of order two. Note however that G is abelian.

So the first non-abelian group has order six (equal to D_3).