Chapter 2

Essential concepts of group theory

2.1 Lagrange's Theorem

Recall the following terminology and notation. Suppose that a and b are natural numbers (positive integers). We say that a *divides* b if $b = ka$ for some integer k, i.e. if b is a multiple of a or equivalently if a is a factor of b.

Examples: 3 divides 12: we write $3|12$. However 3 does not divide 14: we can express this by writing $3 \not| 14$.

Note: Make sure you are using this language and notation accurately (many people don't). The statement "a divides b" means that a is a factor of b. It has nothing to do with the number "a divided by b". The written shorthand for this statement is $a|b$; the symbol in it is a vertical bar, it is not a forward slash or a backslash or a hyphen. In particular it has no connection to the slash that is used in fractions as in a/b.

The purpose of this section is to explore and prove the following theorem, known as Lagrange's Theorem. This theorem was not actually proved by Lagrange, but it was observed by him in 1771 the case of certain groups of permutations arising from his study of solutions of polynomial equations. It was proved in more generality by Gauss in 1801. We have already observed it in the examples of the dihedral groups, and maybe you noticed it also in some of the problems on the first homework sheet.

Theorem 2.1.1 (Lagrange's Theorem)**.** *If* G *is a finite group and* H *is a subgroup of* G*, then the order of* H *divides the order of* G*.*

So for example, Lagrange's Theorem tells us that there is no point in looking for a subgroup with 7 elements in a group with 24 elements; no such subgroup exists.

The rest of this section will be devoted to a proof of Theorem 2.1.1, with some supporting examples and some new concepts that will be needed for the proof. It is not immediately obvious how we could possibly go about trying to prove this theorem, in the absence of any specific information about the groups in question. The fact that this can be done at all demonstrates the power of the axiomatic approach to algebra. Nevertheless it is worth mentioning that the statement of Lagrange's Theorem was noticed for specific examples (by Lagrange) before being stated in a general context. New mathematical theory very frequently comes from observations about particular examples (that are later found to apply more generally) rather than reasoning with completely abstract concepts. The finished product is often stated and described in terms of an abstract setting, so that it can be applied as widely as possible. This is great if what you want to do is apply it as generally as possible, but the downside is that you can get the impression that it came from nowhere. It probably came from (maybe decades or centuries of) an accumulation of observations and examples, but that can sometimes be erased from the record when it is presented in a concise and general form.

So how could we possibly go about proving that the order of a subgroup must be a factor of the order of the whole group? How can we even relate these two numbers when we are not talking

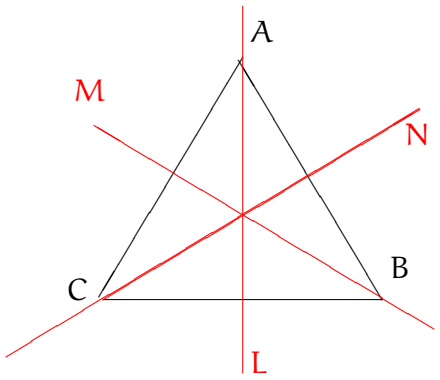
about a specific example? The basic idea is to show that the whole group G can be represented as the union of a number of "shifted copies" of the subgroup H, in such a way that each copy has the same number of elements as H and every element of G belongs to exactly one of them. We are going to break the group into disjoint pieces each of which has the same number of elements as H and somehow "resembles" H. The pieces, or "shifted copies" are called *cosets*.

Definition 2.1.2. *Let G be a group and let H be a subgroup of G. Let g be an element of G. Then the* left coset *of H determined by g is defined to be the set*

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

Note: In the last line above, g is a specified element of G and h is running through all the elements of H. So gH is the subset of G consisting of those elements that can be obtained by multiplying an element of H on the left by g.

Example 2.1.3. Let D_6 be the set of symmetries of the equilateral triangle, with rotations id, R_{120}, R_{240} and reflections T_L, T_M and T_N as shown.



Then $H = \{\mathrm{id}, T_L\}$ is a subgroup of D_6 of order 2, and left cosets of H in D_6 determined by the six elements are:

1. $\mathrm{id}H = \{\mathrm{id} \circ \mathrm{id}, \mathrm{id} \circ T_L\} = \{\mathrm{id}, T_L\} = H$
2. $T_L H = \{T_L \circ \mathrm{id}, T_L \circ T_L\} = \{T_L, \mathrm{id}\} = H$ again.
3. $R_{120}H = \{R_{120} \circ \mathrm{id}, R_{120} \circ T_L\} = \{R_{120}, T_M\}$.
4. $T_M H = \{T_M \circ \mathrm{id}, T_M \circ T_L\} = \{T_M, R_{120}\} = R_{120}H$ again.
5. $R_{240}H = \{R_{240} \circ \mathrm{id}, R_{240} \circ T_L\} = \{R_{240}, T_N\}$
6. $T_N H = \{T_N \circ \mathrm{id}, T_N \circ T_L\} = \{T_N, R_{240}\} = R_{240}H$ again.

Note that there are only three distinct cosets (although each appears twice in the list). Each of these cosets has two elements (same as H) and every element of D_6 appears in exactly one of these three distinct cosets. It follows that the number of elements in D_6 is 3×2, which means in particular that it is a multiple of 2 which is what Lagrange's Theorem says. This example contains the key idea for our proof of Lagrange's Theorem, all we have to do is express the same idea in abstract terms and establish some properties of left cosets.

The concept of a coset is an extremely important one in mathematics, not only in group theory. It is worth spending some time making sure that you understand it well. Here is another example.

Example 2.1.4. If $G = GL(2, \mathbb{Q})$, let H denote the subgroup $SL(2, \mathbb{Q})$. Recall that this means H is the group of all matrices with determinant 1, and the group operation here is matrix multplication. *Question*: What are the cosets of H in G?

For example, choose A to be some specific element of G, say $A = \begin{pmatrix} -1 & 2 \\ 3 & 4 \end{pmatrix}$.

Then the coset of H in G determined by A is the set of all matrices of the form AB, where $B \in H$.

This means the set of all matrices AB, where $\det B = 1$.
If $\det B = 1$, what can we say about $\det(AB)$? It is the same as $\det A$, which in this example is -10. This means the coset of H determined by A consists entirely of matrices whose determinant is -10.
Does it contain *every* such matrix?
To answer this, suppose that C is a matrix in G with $\det C = 10$. Does C belong to AH? To answer this we have to write C as a product with A as the left factor, and see if we can figure out whether the right factor belongs to H. We can write

$$C = AA^{-1}C = A(A^{-1}C).$$

Since A and C both have determinant -10, we have $\det(A^{-1}C) = \det A^{-1} \times \det C = -\frac{1}{10} \times -10 = 1$. So $A^{-1}C \in H$, and C belongs to the coset AH.
(Note: if the above reasoning doesn't make sense to you, try it with a specific matrix of determinant -10 in place of C).
We conclude that AH is exactly the set of matrices in G whose determinant is -10, the same as that of A. So the distinct cosets of H in G are exactly the sets of matrices with the same (specified) determinant. There is one coset for every rational number - one consisting of those matrices with determinant 1 (this is H itself), one with those of determinant -10, etc. Apart from H itself, the cosets of H in G are *not* subgroups of G (why?) - but they do have some recognizable structure, namely in this case that they are the maximal subsets on which the determinant has a constant value. Finally note that if A and A' have the same determinant, then the cosets AH and $A'H$ are the same set.

Example 2.1.5. Suppose that $5\mathbb{Z}$ denotes the subgroup of $(\mathbb{Z}, +)$ consisting of all multiples of 5. What are the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$? How many of them are there? Remember that the group operation here is addition, so (for example) the coset of $5\mathbb{Z}$ in $\mathbb{Z}$ determined by 7 is

$$7 + 5\mathbb{Z} = \{\dots, 7 + (-10), 7 + (-5), 7 + 0, 7 + 5, 7 + 10, \dots\} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

If two integers a and b determine the same coset of $5\mathbb{Z}$ in $\mathbb{Z}$, what is the relationship between a and b?

We have the following important observations.

Lemma 2.1.6. *Suppose H is a finite subgroup of a group G and that $g \in G$. Then gH has the same number of elements as H.*

Proof. Write k for the order of H and write $h_1, h_2, \dots, h_k$ for the elements of H.
So the elements of gH are $gh_1, gh_2, \dots, gh_k$. It looks like gH has k elements, to confirm this we just have to confirm that there is no repetition in this list. So suppose that $gh_i = gh_j$ for some i and j in the range $1, \dots, k$. We can multiply both sides of this equation on the left by g^{-1} to deduce that this means $h_i = h_j$ and hence $i = j$. So the gh_i are distinct for $i = 1, \dots, k$ and the coset gH has the same number of elements as H. □

Lemma 2.1.7. *Suppose that g_1 and g_2 are elements of a group G and that H is a subgroup of G. Then either the cosets g_1H and g_2H are equal to each other or they are disjoint from each other, i.e. their intersection is empty, they have no element in common.*

Note: Since g_1H and g_2H are *sets* (subsets of G), what it means to say that they are equal is that they contain exactly the same elements. A standard approach to presenting a proof that two sets A and B are equal is to show that every element of A belongs to B (so $A \subseteq B$) and that every element of B belongs to A (so $B \subseteq A$).

Proof. If g_1H and g_2H have no element in common then there is nothing to do. So suppose that these two sets *do* have at least one element in their intersection. This means that there are elements h_1 and h_2 of H for which

$$g_1h_1 = g_2h_2.$$

(To see this, note that elements of g_1H have the form g_1h where $h \in H$, and elements of g_2H have the form g_2h where $h \in H$. An element that belongs to both of these sets must simultaneously be equal to g_1h_1 and to g_2h_2, for some elements h_1, h_2 of H).

Now that g_1H and g_2H have non-empty intersection, we need to show that these sets must actually be equal. We must make use of the fact that H is a group. First we show that $g_1H \subseteq g_2H$.

Let $h \in H$. We want to show that $g_1h \in g_2H$. We know that $g_1 = g_2h_2h_1^{-1}$, so we can write

$$g_1 = g_2h_2h_1^{-1} \implies g_1h = g_2h_2h_1^{-1}h = g_2(h_2h_1^{-1}h).$$

Now since H is closed under the operation of G and under taking inverses, we know that the element $h_2h_1^{-1}h$ belongs to H, and hence that g_1h belongs to the left coset g_2H. Thus $g_1H \subseteq g_2H$.

A similar argument, using the fact that $g_2 = g_1h_1h_2^{-1}$, shows that $g_2H \subseteq g_1H$. Hence $g_1H = g_2H$ as required. □

Lemma 2.1.7 says that two left cosets of a subgroup H in a group G are equal to each other if they intersect at all. This (and our proof above) applies to all groups not just finite groups. Note that the proof uses both the fact that H is closed under the group operation and the fact that it contains the inverse of each of its elements.

Lemma 2.1.8. *If* g *is an element of a group* G *and* H *is a subgroup of* G*, then* g *belongs to* some *left coset of* H *in* G*.*

Proof. For example, g belongs to the left coset gH, since $\mathrm{id}_G \in H$. □

The significance of Lemma 2.1.8 is that it shows that the union of the various left cosets of H in G is the full group G.

We are now in a position to prove Lagrange's Theorem by putting all of these facts together in the context where G is a finite group. In this case we know that G is the union of the distinct left cosets of H, that each of these has the same number of elements, and that they don't intersect each other. So to count the elements of G we just need to add up the numbers in each coset - this is essentially the proof.

Theorem 2.1.1. *If* G *is a finite group and* H *is a subgroup of* G*, then the order of* H *divides the order of* G*.*

Note: We will use the notations $|G|$ and $|H|$ respectively for the orders of G and H. (This is standard in group theory).

Proof. Since G is a finite group there are finitely many left cosets of H in G. Let $H, g_2H, \ldots, g_kH$ be the *distinct* left cosets of H in G. (We have seen that two elements of G may determine the same left coset - what the word *distinct* here means is that each coset is counted only once). By Lemma 2.1.6, each of these cosets has exactly $|H|$ elements. By Lemmas 2.1.7 and 2.1.8, each element of G appears in exactly one of them. Thus the number of elements of G is

$$\underbrace{|H| + |H| + \cdots + |H|}_{k} = k|H|.$$

So the order of G is an integer multiple of H. □

Definition 2.1.9. *If* H *is a subgroup of a finite group* G*, then the integer* $\frac{|G|}{|H|}$ *is called the* index *of* H *in* G *and denoted by* $[G : H]$*.*