Cosets and Lagrange's theorem

These are notes on cosets and Lagrange's theorem some of which may already have been lecturer. There are some questions for you included in the text. You should write the answers in the boxes. And there is no need to stop completely if you can't answer one particular question—continue on to the next sections and come back to it later. If this was not lectured, it would be about one week's work—roughly 10 hours—so perhaps it will be 3–4 hours given your previous work. How long you actually need will depend on how thoroughly you want to study.

It might be useful to know the aims of this workbook. It is meant to help you to get used to working with a balance of abstract ideas and concrete calculations. I would like you to understand the statements of definitions and theorems a bit better from working with them in examples, and I would like you to become more comfortable with reading and writing abstract proofs.

There are six sections that have exercises. (Section 7 is optional.)

1. **Lagrange's theorem**
2. **Cosets**
3. **Cosets have the same size**
4. **Cosets partition the group**
5. **The proof of Lagrange's theorem**
6. **Case study: subgroups of** Isom(Sq)

Reminder about notation

When talking about groups in general terms, we always write the group operation as though it is multiplication: thus we write $gh \in G$ to denote the group operation applied to g and h (in that order). And we denote the identity element in G by 1_G.

However, in examples the group operation might be addition, or anything else. Our general statements cover that case, but must be interpreted correctly. If we prove that $ab^2 = 1_G$, then in the case where $G = \mathbb{Z}$, we realise this as $a+2b = 0$—the group operation is addition, and the identity element is $0 \in \mathbb{Z}$.

Cosets and Lagrange's theorem

1 Lagrange's theorem

Lagrange's theorem is about finite groups and their subgroups. It is very important in group theory, and not just because it has a name.

Theorem 1 (Lagrange's theorem) *Let G be a finite group and $H \subset G$ a subgroup of G. Then $|H|$ divides $|G|$.*

We will prove this theorem later in the workbook. But first we begin to see what the theorem means.

1.1 Understanding the statement

Remember that $|G|$ denotes the number of elements of the group G; it makes perfect sense because G is finite. Similarly, since $H \subset G$, certainly H is also finite and again writing $|H|$ makes sense.

Now Lagrange's theorem says that whatever groups $H \subset G$ we have, $|H|$ divides $|G|$. That's an amazing thing, because it's not easy for one number to divide another. For example, if we had a group G_1 with $|G_1| = 77$, then any subgroup of G_1 could only have size 1, 7, 11 or 77. So if you were working out the elements of a subgroup H_1 of G_1 and you could see 12 different elements of H_1 already, then in fact you would be finished: you would know that $|H_1| = 77$, and so the subgroup would *have to be* the whole of G.

That example is a bit artificial. Nevertheless, seeing how a theorem is used in practice helps you to understand it, so we look next at a true application of Lagrange's theorem.

1.2 A favourite application of Lagrange's theorem

The same counting argument as above (but easier) proves your favourite first corollary of Lagrange's theorem. Remember that 2 is the smallest prime—1 is not a prime.

Corollary 2 *If G is a finite group with $|G|$ prime, then G is cyclic.*

Proof Step 1: Show that $|G| \geq 2$ and conclude that there is some element $g \in G$ which is not equal to the identity 1_G.

Step 2: Using g from Step 1, show that the subgroup $H = \langle g \rangle \subset G$ also has $|H| \geq 2$.

Step 3: Since $|G|$ is prime, conclude from Lagrange's theorem that $|H| = |G|$.

Step 4: Conclude that $\langle g \rangle = G$.

Step 5: Write down the definition of cyclic group (from lecture notes or a textbook), and conclude from the definition that G is cyclic as claimed.

Q.E.D.

We worked that proof out in very close detail. I write it out again much more briefly below—it's merely a condensed version of what you wrote above. The two versions of the proof are equally valid since they follow the same logical course and address the same mathematical points. You can decide which you prefer to read and which you prefer to write for yourself.

Proof (of Corollary 2 again) Let $p = |G|$. Since $p \geq 2$, there is an element $g \in G$ with $g \neq 1_G$. Consider the subgroup $\langle g \rangle \subset G$ generated by g. We have $|\langle g \rangle| \geq 2$ since both $1_G, g \in \langle g \rangle$. So by Lagrange's theorem $|\langle g \rangle| = p$. Thus $\langle g \rangle = G$, and so, by definition, G is cyclic as claimed. Q.E.D.

We will prove Lagrange's theorem over the next few sections. We start by defining cosets, since they will be the main technical tool.

2 Cosets

2.1 The definition of left coset

We want to understand the following definition—it is very important in group theory (and in abstract algebra more generally). Incidentally, this definition talks about left cosets. Right cosets are important too, but we will consider them another time.

Definition 3 *Let G be a group and $H \subset G$ a subgroup. A* left coset of H in G *is a subset of G of the form gH for some $g \in G$.*

For a left coset gH, the element $g \in G$ is referred to as a representative *of the coset.*

2.2 Multiplying elements and sets

Of course, the expression gH does not make immediate sense from the group axioms. What it means, by definition, is

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

To put this another way, **the golden rule is this**: if you know that $f \in gH$, then you can conclude that there is some $h \in H$ so that $f = gh$.

Here is an example of how the golden rule works.

Applying the golden rule

Consider $G = S_4$ and $H = \{\mathrm{id}, (1,2)\}$. If $g = (2,3,4)$, then $gH = \{(2,3,4), (2,3,4)(1,2)\} = \{(2,3,4), (1,3,4,2)\}$. Now let $f = (3,4,2,1)$—this is an element of gH. Which $h \in H$ satisfies $f = gh$?

Or if $g = (1,3)(2,4)$, then $gH = \{(1,3)(2,4), (1,4,2,3)\}$. If you let $f = (1,4,2,3)$, which $h \in H$ satisfies $f = gh$ this time?

In the box below, compute the two cosets $g_1H \subset S_4$ and $g_2H \subset S_4$ for

$$H = \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \quad \text{and} \quad g_1 = (1,3,2), \quad g_2 = (1,2,3,4).$$

Computing cosets

One of these two cosets is equal to H itself; the other is disjoint from H. We consider why this happens in section 4 below.

2.3 One coset can have many representatives

Compute another example—in this case the group operation is addition, so we write $a+b$ rather than ab, and similarly cosets are written $a+H$ rather than aH.

Cosets in $\mathbb{Z}$

Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\} = \{\dots, -5, 0, 5, 10, \dots\}$. The coset $2 + H$ is the set $\{2 + 5n \mid n \in \mathbb{Z}\} = \{\dots, -8, -3, 2, 7, 12, \dots\}$, which is of course just the set of numbers congruent to 2 mod 5.

We say that 2 is a *representative* of the coset $2 + H$.

Which of the numbers 17, 152, 21, -18, -2 lie in the set $2 + H$?

Now calculate $7 + H =$

You should see that $7 + H$ is exactly the same subset of $\mathbb{Z}$ as $2 + H$. Therefore we can also say that 7 is a representative of $2 + H$. The point is that 7 and 2 are the same mod 5. In fact, so are -8, 12, 152, or indeed any other element of the set $2 + H$. We can refer to any of them as a representive of this coset.

3 Cosets have the same size

The precise statement of the proposition below is what this section title really means.

Proposition 4 *Let G be a group and $H \subset G$ a subgroup. If H is a finite group, then every left coset of H in G is finite, and moreover $|gH| = |H|$ for any $g \in G$.*

In other words, any (left) coset of H in G has exactly the same number of elements as H does. Your first thought is to see whether this is true in examples. In section 4.1 you computed all cosets of a particular subgroup of S_3, so you should look back there to see that indeed in that case every coset has exactly 2 elements.

3.1 Why do cosets all have the same size?

Proposition 4 follows from an even better result—it's better because it doesn't need to talk about finiteness at all.

Proposition 5 *Let G be a group and $H \subset G$ a subgroup. Fix $g \in G$. Then the map*

$$\varphi_g \colon H \longrightarrow gH \quad \textit{defined by} \quad \varphi_g(h) = gh$$

(which is a map of sets) is a bijection.

This proof is easy: as you'll see below, the map is surjective by the golden rule and injective by left cancellation, and we use nothing more complicated than that.

Proof Step 1: Show that if $f \in gH$, then there is an $h \in H$ with $\varphi_g(h) = f$.

Step 2: Show that if $h_1, h_2 \in H$ satisfy $\varphi_g(h_1) = \varphi_g(h_2)$, then $h_1 = h_2$.

Step 3: Triumphant declaration! (I'll do this—I have to do everything round here.)

So φ_g is bijective because it is surjective by Step 1 and injective by Step 2.

Q.E.D.

Finally, observe that Proposition 4 follows from Proposition 5 because if there is a bijection between H and gH then these two sets have the same number of elements.

4 Cosets partition the group

The title of this section is an important slogan that we want to understand properly and then prove—at the moment it may mean very little to us.

4.1 What does 'cosets partition the group' mean?

Consider $G = S_3$ and let $H = \{\mathrm{id}, (1,2)\} \subset G$. Compute *all* left cosets of H in G in the boxes below; the first couple are already done.

$\mathrm{id}\, H = H$	$(1,2)H =$
$(1,3)H = \{(1,3),(1,2,3)\}$	$(1,2,3)H =$
$(2,3)H =$	$(1,3,2)H =$

What you should have found is that if you look at any two of the boxes, then the results are either exactly the same or disjoint. (Check your answers if that's not true.)

The subsets of S_3 computed above form a partition of S_3. In words: a partition is a division of the whole of a set into mutually disjoint subsets. The mathematical definition is more precise.

Definition 6 *If X is a set, then a* partition of X *is a collection of subsets $Y_\alpha \subset X$, for some indexing set $\alpha \in A$, for which*

(i) $X = \cup Y_\alpha$, *where the union is taken over all $\alpha \in A$, and*

(ii) if $\alpha_1, \alpha_2 \in A$, then either $Y_{\alpha_1} = Y_{\alpha_2}$ or $Y_{\alpha_1} \cap Y_{\alpha_2} = \emptyset$.

Another example. Consider the set $X = \{1, 2, \ldots 8\}$ of the first 8 positive integers. Here are several randomly-chosen subsets of X:

$$Y_1 = \{1,2,3\}, \quad Y_2 = \{2,4,6,8\}, \quad Y_3 = \{4,6,8\},$$
$$Y_4 = \{1,3,5,7\}, \quad Y_5 = \{5,7\}, \quad Y_6 = \{8\}, \quad Y_7 = \{4,6\}.$$

The collection of three subsets Y_1, Y_3, Y_5 form a partition of X since

(i) $X = Y_1 \cup Y_3 \cup Y_5$, and

(ii) each of $Y_1 \cap Y_3$, $Y_1 \cap Y_5$ and $Y_3 \cap Y_5$ is empty.

Find two other collections of subsets from among the Y_i listed above that also form partitions of X.

4.2 Why do cosets partition the group?

Proposition 7 *Let G be a group and $H \subset G$ a subgroup. The set of all left cosets of H in G is a partition of G.*

For the proof, we must check conditions (i) and (ii) of Definition 6.

Show that if $g \in G$ then there is some coset that contains g. [Hint: $1 \in H$.]

The box above confirms condition (i)—it says that G is a subset of the union of all cosets, and so it must be equal to the union of all cosets.

The following lemma checks condition (ii).

Lemma 8 *(Notation as in Proposition 7.) Let $g_1, g_2 \in G$. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.*

This statement says that in the given circumstances one (or both) of two events, P and Q say, must happen. A typical method of proof for such statements is to see what happens if you assume that Q does *not* happen. If you can show that P *must* happen, then you are done. That will be our strategy: we will imagine that $g_1H \cap g_2H \neq \emptyset$ and then we will prove that $g_1H = g_2H$.

Before we start the proof, let's think through an important point: if there is an element $f \in g_1H \cap g_2H$, then by the golden rule there are elements $h_1, h_2 \in H$ so that

$$f = g_1h_1 \quad \text{and} \quad f = g_2h_2.$$

In particular, this shows that $g_1h_1 = g_2h_2$, and we can rearrange this equation to prove that $g_1 \in g_2H$. With those thoughts in mind, we are ready for the proof.

Proof (of Lemma 8)

Step 1: Show that if $g_1H \cap g_2H \neq \emptyset$, then there are $h_1, h_2 \in H$ so that $g_1h_1 = g_2h_2$.

Step 2: Show that $g_1h_1 = g_2h_2$ implies that $g_1 \in g_2H$.

Step 3: Show that $g_1 \in g_2H$ implies that $g_1H \subset g_2H$. [Hint: golden rule again.]

Step 4: Explain why you are finished. (I'll do this.)

Repeating Steps 2 and 3 with g_1 and g_2 exchanged shows that $g_2H \subset g_1H$. Together with Step 3, this implies that $g_1H = g_2H$. The proof is complete.

Q.E.D.

5 The proof of Lagrange's theorem

The idea is that the cosets of H divide G up into equal-sized pieces; and since the size of each piece is $|H|$, the result follows. But that's just the executive summary—we'll take it more slowly.

First recall the statement of Lagrange's theorem.

Now use Proposition 7 to conclude that G is the disjoint union of finitely many cosets $g_1H, \ldots, g_kH$, for some $g_1, \ldots, g_k \in G$.

Finally, using Proposition 4, deduce that $|G| = k|H|$ and observe that this proves the theorem.

6 Case study: subgroups of Isom(Sq)

We know that Isom(Sq) is a group with exactly 8 elements. By Lagrange's theorem, any subgroup $H \subset \text{Isom(Sq)}$ must have $|H|$ dividing 8—that is, H must have 1, 2, 4 or 8 elements. The only subgroup of order 1 is the trivial subgroup $\{\text{id}\}$. And if $|H| = 8$, then H is the whole group. So we only have to think about subgroups of order 2 or 4.

Before we start, it's worth noting the order of each element of Isom(Sq)—remember, the *order* of $g \in G$ is the least integer $n > 0$ for which $g^n = 1_G$. (You may need to remind yourself of the notation used in lectures for elements of Isom(Sq).)

element	id	R	R^2	R^3	ρ_x	ρ_y	α	β
order								

6.1 Subgroups of order 2

If $\{\text{id}, \sigma\}$ is an order 2 subgroup of Isom(Sq), show that $\sigma^2 = \text{id}$.

List all elements of Isom(Sq) of order 2.

Finally list all subgroups of Isom(Sq) of order 2.

6.2 Subgroups of order 4

Let $H \subset G = \text{Isom(Sq)}$ be a subgroup of order 4. There are two cases to distinguish. If H contains an element $g \in H$ of order 4, then $H = \langle g \rangle \subset G$. Using the table of element orders above, list all such subgroups of order 4.

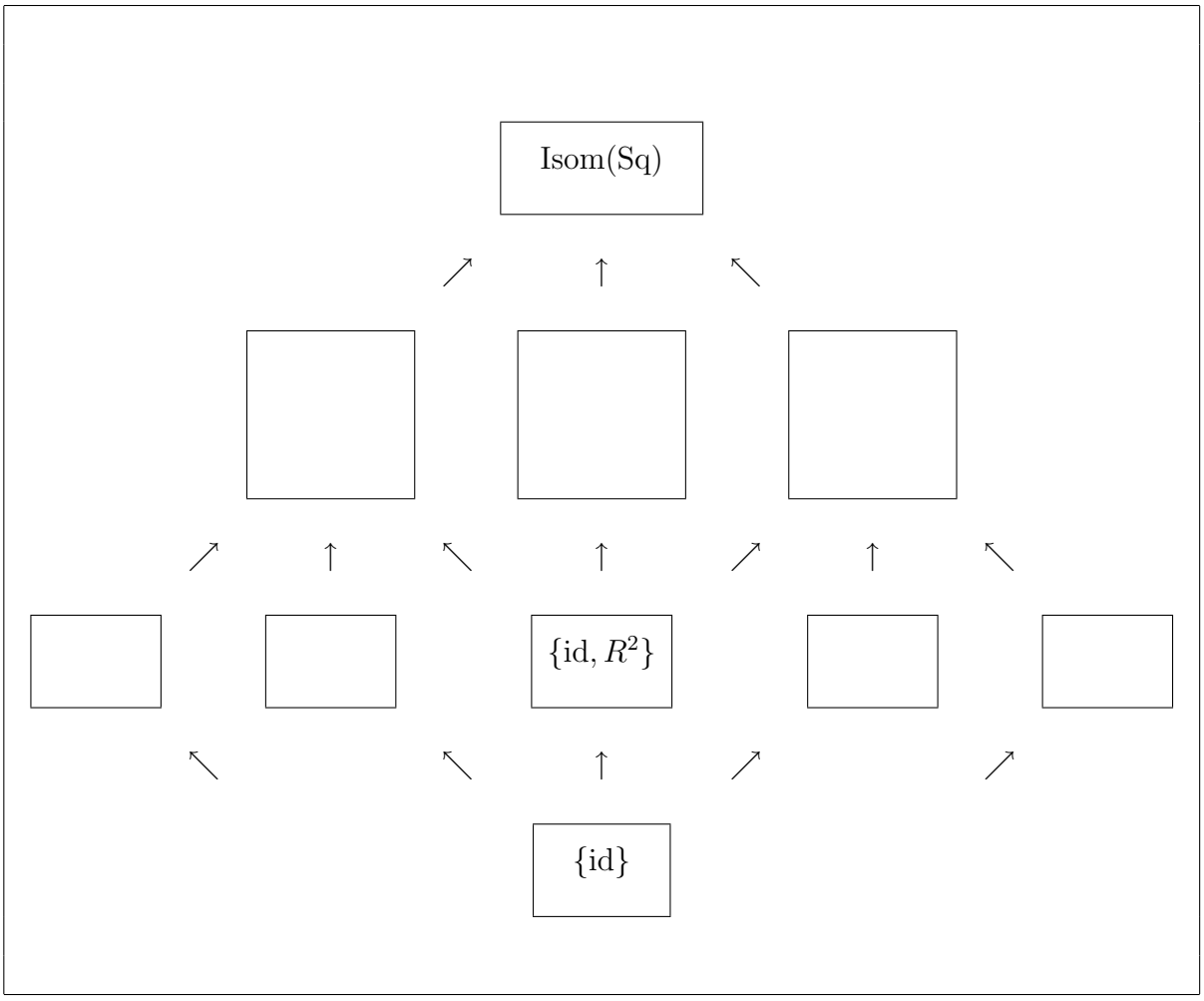
The second case is when H does not contain any element of order 4. In that case—looking at the table of element orders again—it must consist of the identity and three elements of order 2.

Use Lagrange's theorem to show that if $g_1, g_2 \in G$ are distinct elements of order 2, then $\langle g_1, g_2 \rangle$ either has order 4 or actually equals G.

By considering pairs of elements of order 2, list the remaining subgroups of order 4.

6.3 The subgroup lattice of Isom(Sq)

We can draw all the subgroups on one very beautiful picture. Here, the bigger the group, the higher it is in the diagram. The arrows are inclusions from a smaller subgroup to a larger one. It's a bit of a jigsaw puzzle to get the subgroups in the right boxes, but see if you can fit your lists of subgroups into the picture. To make it easier, I've drawn it so that subgroups of the same order lie at the same height on the page: from the top, therefore, you see rows of subgroups of size 8, 4, 2 and 1.



This is a very well-known picture, although I stole it from David Mond at Warwick; you can find it on page 12 of his lecture notes

`www.warwick.ac.uk/~masbm/Lectures/groups.pdf`

if you would like to see a more geometric derivation of these subgroups (and, happily, he too has left the boxes blank so it doesn't spoil the exercise).

7 When is a coset also a subgroup? (Optional)

Here's an extra thought about cosets if you've got time for more work.

We stick to the notation $H \subset G$. Obviously a left coset of H is a subset of G—by the closure axiom, if you like. However a typical left coset is not a subgroup of G: just look at the examples above—most of the cosets do not even contain the identity. In fact,

Proposition 9 *Let G be a group, $H \subset G$ a subgroup and $g \in G$. The coset gH is a subgroup of G if and only if $g \in H$.*

I want to prove this. The statement is an 'if and only if', which often—although not always—means that the proof is best done in two stages. I'm even going to split the statement into two halves to make this clearer. Here's the first half; it's the 'only if' part of Proposition 9.

Lemma 10 *Let G be a group, $H \subset G$ a subgroup and $g \in G$. If the coset gH is a subgroup of G, then $g \in H$.*

Proof Since gH is a group in its own right, gH must contain the identity element 1. That is, $1 \in \{gh \mid h \in H\}$. So there is some element $h \in H$ for which $gh = 1$. This implies that $g = h^{-1}$, and h^{-1} is certainly an element of H. Q.E.D.

The second half is the 'if' part of Proposition 9.

Lemma 11 *Let G be a group, $H \subset G$ a subgroup. If $g \in H$, then the coset gH is a subgroup of G.*

The proof below is slightly sneaky. We could simply run through the group axioms and check that they hold for gH—that's fine and will work, but it's slightly awkward. Instead, we find a short-cut by proving that $gH = H$—for that is indeed a subgroup of G.

Proof First observe that $gH \subset H$; this follows from the closure axiom for H because $g \in H$. To complete the proof, we show that $H \subset gH$, for then $gH = H$ is a subgroup as claimed.

Pick $h \in H$. We can write $h = g(g^{-1}h)$. Since $g \in H$, also $g^{-1} \in H$ and so also $g^{-1}h \in H$. So $h = g(g^{-1}h) \in gH$. We have shown that every $h \in H$ is also in gH; in other words $H \subset gH$, as required. Q.E.D.

Gavin Brown, Clare Dunning
Kent, January 2006