PMath 336 - Introduction to Group Theory with Applications

Course Notes, University of Waterloo

Tyrone Ghaswala

Spring 2025

Contents

"We need a super-mathematics in which the operations are as unknown as the quantities they operate on, and a super-mathematician who does not know what he is doing when he performs these operations. Such a super-mathematics is the Theory of Groups."

- Sir Arthur Stanley Eddington

These notes are for the Spring 2025 offering of PMath 336 - Introduction to Group Theory with Applications. They will be updated as I go, and are definitely not free of typos and mistakes. If you find any, please let me know about it (either by email or through Piazza)!

Lecture 1 - 05/05

1 Introduction

Group theory is one of the most rich and accessible topics in all of pure mathematics. It is very easy to get your hands on groups, and the area is full of mystery and enjoyment.

Groups first had some serious influence in the early 1800s, when Évariste Galois, a young French mathematician, developed what is now known as Galois Theory. One of the things he developed and used groups to do was to prove something amazing about solving equations.

We all know that if I have a quadratic equation $ax^2 + bx + c = 0$ for some numbers a, b, and c, then the values of x which satisfy this equation are

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Here is a way to write down the solutions for any quadratic, using only roots, and the four operations, plus, minus, divide and times. It's natural to ask, what about solving $ax^3 + bx^2 + cx + d = 0$? Is there a solution for that? It turns out the answer is yes, and one of the answers (there are three in total) is given by

$$x = \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} + \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) - \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}$$

This formula may be disgusting and unenlightening, but the important thing is that it exists! What about for a quartic equation (where the highest power of x that appears is 4)? Again, the answer is yes but the formula is an abomination! No one should ever have to use that formula to find roots, and making someone do that would be an effective form of torture.

At this point, it would be surprising if the answer was ever "no". Surprisingly, for a general quintic of the form $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$, there is no analogue of the quadratic formula. This is an easy consequence of some of the results from Galois theory, which is built upon the sturdy and industrious foundation of group theory.

Today group theory is used in elliptic curve cryptography, areas of chemistry, and most notably physics as illustrated by this quote.

"The importance of group theory was emphasized very recently when some physicists using group theory predicted the existence of a particle that had never been observed before, and described the properties it should have. Later experiments proved that this particle really exists and has those properties."
- Irving Adler

The idea that something as abstract as group theory could actually predict the existence of a particle with certain properties is mind blowing. We don't really know why, but for some reason the universe truly seems to be written in the language of mathematics.

Above all of these applications, the most important reason for studying group theory for me is the indescribable aesthetic beauty that exists in the subject. It really is one of the most beautiful areas of pure mathematics.

The power of group theory lies in its abstraction, and its focus on structure. This all sounds very vague right now, but it will become clear as we start playing with some groups. Throughout this whole course, it will pay for you to have your eyes open and your brain switched on. There are lots of connections to be made, too many to mention, and you will only make them if you're constantly looking out for them. That feeling when you find a connection is one of the great rewards of pure mathematics.

All of this might make group theory seem like some amazingly large and inaccessible mathematical object, but that's not the case. In fact, you already know a whole bunch of examples of groups, so let's get right into it.

2 Getting Your Toes Wet - Some Examples of Groups

When a child learns what a cat is, they do not learn it by being told "a cat is a quadruped, typically with fur, that is usually evil and meows". Instead they just keep seeing cats until they have a complete understanding of what a cat is. We will take the same approach to learning about groups. I will not at first tell you what a group is, but for now we will just amass some examples.

2.1 The Integers - $(\mathbb{Z}, +)$

This group is made up of all the integers, and the only thing we have other than the set of whole numbers is the operation "+". So recall that

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

and notice that $+$ is an operation that takes in two elements of $\mathbb{Z}$ and spits out another one. For example

$$\begin{aligned} 3 + 5 &= 8 \\ 5 + 3 &= 8 \\ 2 + (-1) &= 1 \\ 0 + 5 &= 5 \\ 0 + 6 &= 6 \\ (-10) + 0 &= -10 \\ 2 + (-2) &= 0. \end{aligned}$$

Notice that there appears to be something interesting going on with 0. It has the property that

$$a + 0 = a = 0 + a$$

for every a in $\mathbb{Z}$. An element like this in a group will be called the **identity**. In this group, is there more than one such element?

Let's take a closer look at the last equation above, $2 + (-2) = 0$. 2 and -2 have an interesting relationship to each other. Notice that they add together to make the identity. In this case, we say -2 is the **inverse** of 2, and of course, 2 is the inverse of -2.

2.2 $(\{1, -1\}, \cdot)$

The previous group $\mathbb{Z}$, had an infinite number of elements. Now, let's look at the group where the only elements are 1 and -1, and the operation is multiplication. Let's do something different here, and draw out a multiplication table.

$\cdot$	1	-1
1	1	-1
-1	-1	1

Just by looking at this table, we can identify that 1 is the identity, the inverse of -1 is -1 (since $-1 \cdot -1 = 1$), and the inverse of 1 is 1.

2.3 The rationals under addition - $(\mathbb{Q}, +)$

Here is another group: all the rational numbers $\mathbb{Q}$ under addition. Similar to the case above, if you add two rational numbers together you get another rational number. Furthermore, the identity again is given by 0. Think about what the additive inverse of $\frac{a}{b}$ is. Remember, it's a rational number that has the property that it adds to $\frac{a}{b}$ to equal the identity, which is 0.

Lecture 2 - 07/05

2.4 $(\mathbb{Q}^*, \times)$

Now things get a little more interesting. Here $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, the rational numbers without 0. Let's look at the group formed by taking all the rational numbers *except for* 0, and this time only being able to multiply them together. The first thing to notice here is that if you take any two non-zero rational numbers and multiply them together, you end up with another rational number, so that's certainly a good thing.

We can again ask, what element in $\mathbb{Q} \setminus \{0\}$ is the identity? Well, whatever the identity is, it better have the property that multiplying any other number by it doesn't change that other number. With a bit of thought we can convince ourselves that the identity here is given by $\frac{1}{1}$ since

$$\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b} = \frac{a}{b} \cdot \frac{1}{1}.$$

So, if 1 (we will just write it like this instead of $\frac{1}{1}$ from now on) is the identity, what do inverses look like? Well, as above, the inverse of, say $\frac{3}{5}$ is some element in $\mathbb{Q} \setminus \{0\}$, call it $\left(\frac{3}{5}\right)^{-1}$, such that $\frac{3}{5} \cdot \left(\frac{3}{5}\right)^{-1} = 1$. Again, a bit of thought and elbow grease, and you can convince yourself that $\left(\frac{3}{5}\right)^{-1} = \frac{5}{3}$. See if you can justify to yourself why this is the case!

In general, for any element $\frac{a}{b}$ in $\mathbb{Q} \setminus \{0\}$, we see that under the operation of multiplication, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, which should explain to you why you were always taught that the inverse of $\frac{7}{2}$ is $\frac{2}{7}$.

So far, we have a few things to notice. First, each group we've looked at so far has an identity, and every element has an inverse. A group seems to be made up of these things, and the *operation* (multiplication or addition above) has the property that it eats two elements in the set, and spits out another element in the set. All of this of course will be formalised in the next few lectures.

Let's look at a few more examples.

2.5 More examples of groups

Here are a few groups you should play with to become more comfortable with groups. When doing so, keep the following questions in the back of your mind: What is the identity? How many identities are there? For each element, what is its inverse? How many inverses does it have? What other properties does it have?

- $(\mathbb{C}, +)$, the complex numbers with addition.
- $(\mathbb{C}^*, \cdot)$, the complex numbers without 0, with the operation being multiplication.
- $(\{1, i, -1, -i\}, \cdot)$. Here i is the complex number i, which has the property that $i^2 = -1$.

2.6 The Integers Modulo n

The integers modulo n, which we will denote $\mathbb{Z}_n$, is a nice infinite family of examples of groups. In fact, for each n, we get two groups:

- $(\mathbb{Z}_n, +)$, the integers modulo n under addition.
- $(\mathbb{Z}_n^*, \cdot)$, the **group of units** modulo n. Remember that $\mathbb{Z}_n^*$ is the set of elements with a multiplicative inverse.

For example, let $n = 7$. Then $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, which is a group under addition, and $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, which is a group under multiplication. In $\mathbb{Z}_n$, the identity is always 0, and in $\mathbb{Z}_n^*$ the identity is always 1.

Recall from your 135 days, that $a \in \mathbb{Z}_n^*$ if and only if $\gcd(a, n) = 1$. This will be *very important.*

For example, $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. The reason we only include these elements when our operation is multiplication, is that these are the only elements that have an inverse! For example, there is no element $a \in \mathbb{Z}_{12}$ such that $2a = 1$, so 2 does not have an inverse, and hence it is not in $\mathbb{Z}_{12}^*$.

If you are a little rusty with your modulo arithmetic, try some of the problems in the extra exercises, and see the appendix at the end of this document.

Let's draw out the **Cayley table** for $(\mathbb{Z}_6^*, \cdot)$.

$\cdot$	1	5
1	1	5
5	5	1

Compare this with the group $(\{1, -1\}, \cdot)$, do you notice anything?

2.7 Some Definitions and Notation

From here on in, if we have a group, say $(\mathbb{Z}_n, +)$ where there is an obvious choice for an operation (in this case $+$ since $\mathbb{Z}_n$ is not a group under multiplication), we will simply denote the group by $\mathbb{Z}_n$. Furthermore, sometimes we will completely ignore the actual operation and write something like $a \cdot b$ as ab.

Definition. Let $(G, \cdot)$ be a group (which we will simply denote G). The **order of the group** G, denoted $|G|$, is the number of elements in the group.

So for example, $|\mathbb{Z}| = \infty$, $|\mathbb{Z}_n| = n$, and $|\mathbb{Z}_n^*| = \phi(n)$, where $\phi(n)$ is the **Euler phi function** or the totient function. If you don't know what the Euler phi function is, check your MATH 135 notes or look it up. It's pretty great, but we won't be talking too much about it in this course.

Definition. Let G be a group and let $e \in G$ be such that $ea = ae = a$ for all $a \in G$. Such an element is called an **identity** element.

Lecture 3 - 09/05

We will see later that in any group there exists exactly one identity element. In all the examples we have done so far, the order of multiplication (or addition) hasn't changed the outcome of an operation ab, that is $ab = ba$ always. However, we will see in a moment that this isn't always the case.

Here is one more definition to finish this section off.

Definition. Let G be a group and $e \in G$ the identity element. Suppose $a \in G$, and let $b \in G$ be such that $ab = ba = e$. The element b is called an **inverse** for a, and is denoted a^{-1}.

Again, we will see later that every element has a unique inverse.

2.8 Matrix Groups

Matrices are an excellent place to look for examples of groups, and will give us our first examples of what are called **non-abelian** groups.

The real general linear group

This group is called the **general linear** group over $\mathbb{R}$, and is defined as follows:

$$\mathrm{GL}_n(\mathbb{R}) := \{A \in M_{n\times n}(\mathbb{R}) : A \text{ is invertible}\}.$$

Remember that a matrix with entries in $\mathbb{R}$ is invertible if and only if its determinant is not equal to 0. The operation in this group is matrix multiplication.

Let's focus on the case $n = 2$ for a moment. The identity is given by the matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Recall that the inverse of a matrix, say $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, is given by

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = \frac{1}{-2} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & \frac{-1}{2} \end{bmatrix}.$$

We will now investigate something that makes this group fundamentally different to any of the groups we have seen so far. If we set matrices A and B as in the next line, you can check the following equiations.

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}, \quad AB = \begin{bmatrix} -1 & -3 \\ -1 & -7 \end{bmatrix} \quad \text{and} \quad BA = \begin{bmatrix} -2 & -2 \\ -4 & -6 \end{bmatrix}.$$

Notice here that the *order of multiplication matters* since $AB \neq BA$.

As we will define formally below, a group G where $ab = ba$ for all $a, b \in G$ is called **abelian**, and the group is **non-abelian** if it is not abelian (amazingly enough).

The general linear group, in general.

In principle, the matrices do not have to have entries in $\mathbb{R}$. We can replace $\mathbb{R}$ by anything which has both multiplication and addition (or some version of them). Such things are called **rings**. We won't formally define rings in this course, but some examples of rings are $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{C}$, and $\mathbb{Z}_n$ for all integers $n > 0$.

So, if we have a ring $\mathcal{R}$, $\mathrm{GL}_n(\mathcal{R})$ will be the set of $n \times n$ *invertible* matrices with entries from $\mathcal{R}$, and the group operation will be matrix multiplication.

You might wonder how you know if a matrix is invertible when it has entries in something like $\mathbb{Z}_n$. Well, as long as the determinant is in $\mathbb{Z}_n^*$, all will be fine. It turns out that you can always characterise when a matrix is invertible with entries from a ring in terms of the determinant, and we can replace the condition "A is invertible" from the definition of $\mathrm{GL}_n(\mathbb{R})$ above as follows.

$$\begin{aligned}
\mathrm{GL}_n(\mathbb{R}) &:= \{A \in M_{n\times n}(\mathbb{R}) : \det(A) \in \mathbb{R}^*\} \\
\mathrm{GL}_n(\mathbb{Q}) &:= \{A \in M_{n\times n}(\mathbb{Q}) : \det(A) \in \mathbb{Q}^*\} \\
\mathrm{GL}_n(\mathbb{C}) &:= \{A \in M_{n\times n}(\mathbb{C}) : \det(A) \in \mathbb{C}^*\} \\
\mathrm{GL}_n(\mathbb{Z}) &:= \{A \in M_{n\times n}(\mathbb{Z}) : \det(A) \in \mathbb{Z}^*\} \\
\mathrm{GL}_n(\mathbb{Z}_k) &:= \{A \in M_{n\times n}(\mathbb{Z}_k) : \det(A) \in \mathbb{Z}_k^*\}
\end{aligned}$$

where $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $\mathbb{Z}^* = \{1, -1\}$, and $\mathbb{Z}_k^*$ is the group of units modulo k.

Let's play with an example in $\mathrm{GL}_2(\mathbb{Z}_{15})$. Let $A \in \mathrm{GL}_2(\mathbb{Z}_{15})$ be the matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. You find the determinant in the usual way! Remember, for this whole example, the multiplication and addition occurs in $\mathbb{Z}_{15}$.

$$\det(A) = 1 \cdot 4 + (-(2 \cdot 3)) = 4 + (-6) = -2 = 13$$

in $\mathbb{Z}_{15}$. Notice that we used both addition and multiplication here, but that's all you need. Since $\gcd(13, 15) = 1$, $\det(A) \in \mathbb{Z}_{15}^*$ and A is invertible. So let's actually find the inverse! We find it in the way we used to back in the day.

$$A^{-1} = \frac{1}{13} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = 7 \begin{bmatrix} 4 & 13 \\ 12 & 1 \end{bmatrix} = \begin{bmatrix} 13 & 1 \\ 9 & 7 \end{bmatrix}.$$

Great, so we have a new matrix with entries in $\mathbb{Z}_{15}$, but is it really the inverse? Let's check!

$$AA^{-1} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 13 & 1 \\ 75 & 31 \end{bmatrix} = \begin{bmatrix} 31 & 15 \\ 75 & 31 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

It's magic! You can check that $A^{-1}A = I$ as well.

3 So what actually is a group?

3.1 Group Axioms

Now that we have seen a fair few examples of groups, it is time to formally define a group. Keep in mind, that a binary operation on a set is something that takes in two elements of the set, and gives back one. Multiplication, addition, and matrix multiplication are all examples of a binary operation.

Definition (Definition of a group)**.** A **group** is a set G with a binary operation operation $\cdot$ such that

1. For any elements $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (this says that $\cdot$ is **associative**).
2. There exists an element $e \in G$, which we call the **identity**, such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. We call such an element the **inverse** of a.

Definition. Two elements $a, b \in G$ for a group G are said to **commute** if $ab = ba$. If a and b commute *for all* $a, b \in G$, we say G is **abelian**. If G is not abelian, we say it is **non-abelian**.

As an exercise, come up with a few examples of both abelian and non-abelian groups. We have already seen both types of groups, which ones are which?

It is worth taking a moment here to discuss abstraction in mathematics. You might look at the list of axioms above and think, "why in the world would you make such an abstract definition?". This is a perfectly valid question, and it is often definitions like this that turn people off pure mathematics. As we will see, there is incredible power in stripping off everything except for these bare bones. Now, if we prove something only using the axioms of a group, then we have automatically proved it for anything that satisfies these properties. We've already seen an infinite number of groups, so if we prove something in this abstract setting, we've proved it for an infinite number of things. Amazing! We'll see this in all it's glory a little later.

After all, as Henri Poincaré once put it, *"Mathematics is the art of giving the same name to different things"*.

3.2 Some Basic Results

Proposition 1 (Uniqueness of identity elements)**.** *In a group G, there exists only one identity element.*

Proof. Suppose e and f both have the property that $ea = ae = a$ and $fa = af = a$ for all $a \in G$. Then $ef = f$, and $ef = e$ so $f = e$. Therefore there is only one identity element. ■

Proposition 2 (Uniqueness of inverses)**.** *Every element $a \in G$ has a unique inverse.*

Proof. This is an exercise. ■

Proposition 3 (Cancellation Property)**.** *Let $a, b, c \in G$ for a group G. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.*

Proof. This is an exercise. ■

Lecture 4 - 12/05

4 Even More Examples of groups

We finally have a definition of a group, and it's pretty abstract. Let's see some groups that are maybe a little more unfamiliar than the ones we have seen so far. Every time we explore a new group (or family of groups), make sure to keep the group axioms in mind, and check whether or not these examples are indeed groups.

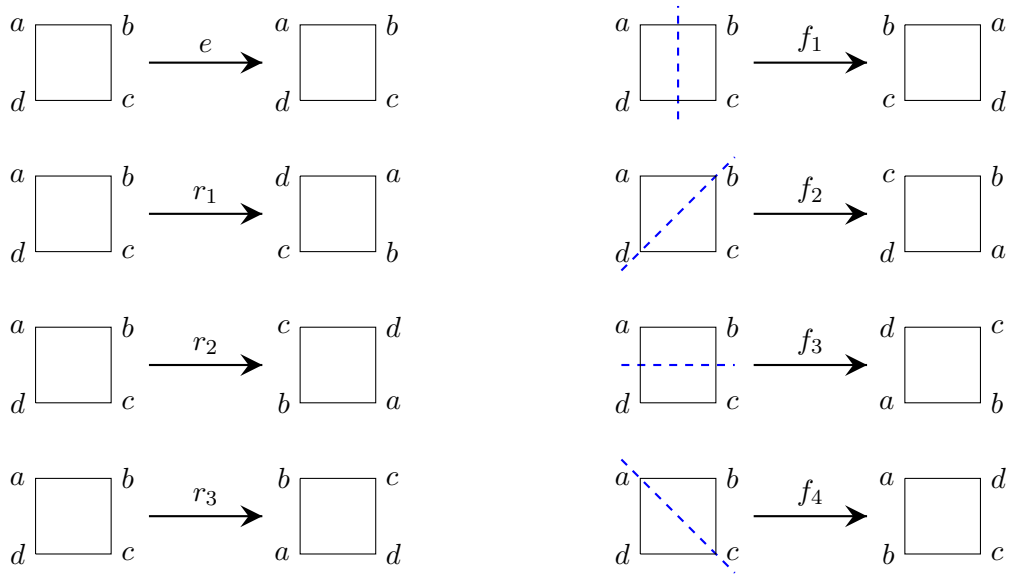
4.1 Dihedral Groups

The dihedral groups are a family of groups D_n, one for each integer $n \geq 3$. They are defined as the group of symmetries of a regular n-gon, and we will see exactly what this means in a moment. Remember that you can think of a symmetry of an object as something I can do to it while you're not looking, that you won't notice has happened! You are about to see why people often say that group theory is the study of symmetries.

Symmetries of the Square

Let's explore the group D_4, which is the group of symmetries of the square. A group comes with two things: a set of things, and an operation on those things.

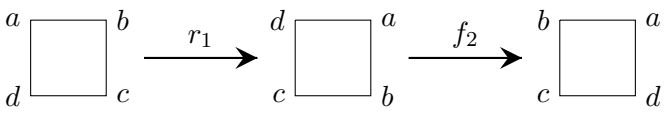
The set is the set of symmetries of the square, and we'll get to the operation later. First, let's count how many symmetries there are. We have 4 choices as to which corner goes in the top left corner, and then 2 choices as to which goes in the top right (you might have to draw out some pictures to convince yourself this is true). This gives us 8 symmetries, and here they are:



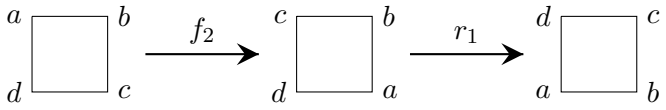
Note that the letters are only there as an aid to help us work out which symmetry has been performed, and the blue dotted lines are to indicate what axes we're flipping over. From now on, we will refer to each symmetry simply by the label that has been put above each arrow. Notice that the first column is made up of rotations, and the second of flips.

Ok, so we have our set of things, now for the operation. The operation will be composition of symmetries. What we mean by this is that if we want to work out what ab is where a an b are both symmetries, we first perform the symmetry b, and then perform the symmetry a. Since a and b are both symmetries, doing one after the other will be another symmetry!

For example, let's work out what $f_2 r_1$ is. By what we just said, it better be another symmetry, so we will just perform r_1 followed by f_2 and hope for the best!



This is the same symmetry as f_1, which means $r_1 f_2 = f_1$. On the other hand, if we do the same thing for $r_1 f_2$ we have



so $f_2 r_1 = f_3$. Notice that $f_2 r_1 \neq r_1 f_2$ so D_4 is non-abelian.

The set of symmetries of a square along with composition (which we will just denote $\cdot$ if we denote it at all), form a group D_4. Now that we know how the group operation works, we can draw out the Cayley table for D_4. Since it is non-abelian, we must be careful which order we perform the operation in. To set a convention, the element on the left of the table will come first, so the symmetry which appears in the row corresponding to r_1 and the column corresponding to f_2 will be $f_2 r_1$, which is f_1.

$\cdot$	e	r_1	r_2	r_3	f_1	f_2	f_3	f_4
e	e	r_1	r_2	r_3	f_1	f_2	f_3	f_4
r_1	r_1	r_2	r_3	e	f_4	f_1	f_2	f_3
r_2	r_2	r_3	e	r_1	f_3	f_4	f_1	f_2
r_3	r_3	e	r_1	r_2	f_2	f_3	f_4	f_1
f_1	f_1	f_2	f_3	f_4	e	r_1	r_2	r_3
f_2	f_2	f_3	f_4	f_1	r_3	e	r_1	r_2
f_3	f_3	f_4	f_1	f_2	r_2	r_3	e	r_1
f_4	f_4	f_1	f_2	f_3	r_1	r_2	r_3	e

.

There are lots of interesting things to notice in this table, too many to mention here. Stare at it for as long as you can and make a note of anything you find interesting. A good exercise to do is to work out why what you have noticed has happened.

One of the things worth noticing is that the identity is e (so my choice of name for that symmetry was a good one!). Another thing to notice is that the es appear symmetrically about the main diagonal. This will happen in every group since inverses are two sided (that is, $a^{-1}a = e$ if and only if $aa^{-1} = e$).

The Dihedral Group D_n

There is nothing special about the square. We can talk about the dihedral group of any regular polygon. The group of symmetries of a regular n-gon is the group D_n, and the operation is composition of symmetries just like in the example for $n = 4$ above.

Exercise. Compute the order of the group D_n.

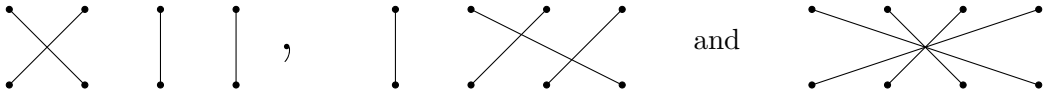
4.2 Symmetric Groups

The symmetric groups S_n (sometimes called permutation groups) are probably the most important finite groups. We will introduce them briefly here and come back to them later in the course for a more in depth study.

As you have probably guessed by the notation, there is a group S_n for every integer $n \geq 1$ (although the case $n = 1$ is pretty boring).

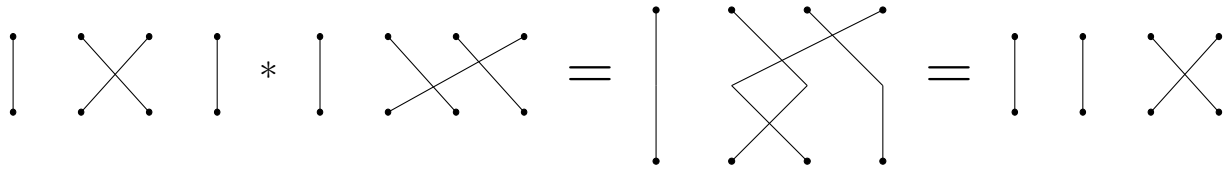
We will illustrate how S_n works by looking at the specific case of S_4. There are several different ways of looking at the elements in S_n, but we will start off with my favourite.

As usual, we must define the group elements, as well as the operation. An element in S_n can be thought of as a diagram consisting of two rows of n dots, joined together by n lines in such a way that every dot in the top row is joined to exactly one in the bottom row, and every dot in the bottom row is joined to exactly one in the top row. Here are some elements in S_4:



It is worthwhile to think of each of these diagrams as a permutation of the four dots. A **permutation** on a set is a function from the set to itself that is a bijection. If we think of it this way, then the group operation is simply composition of functions. If you prefer to draw diagrams (like I do), here is how the operation works.

We will denote the operation by $*$. We need a way of taking two of these diagrams and spitting out another diagram. Suppose a and b are two elements in S_4. Then $a * b$ is the diagram obtained by putting a below b, and simply combining them by looking at where each line starts and ends. For example,



We will not do it here, but it is worth checking that S_n with the operation $*$ satisfies the 3 group axioms and so S_n is indeed a group.

We can ask the usual questions: What is the identity? What is the inverse of any particular element? What is $|S_n|$? We will answer this one now, and the other questions are left as an exercise.

Proposition 4. *The order of S_n is $n!$.*

Proof. We wish to count how many possible diagrams we can draw. Consider the unique line that begins at the leftmost dot. There are n choices for where it finishes, so pick one.

Then move on to the second dot from the left. We now have $n-1$ choices for where that line ends (since one of the dots on the bottom row has been taken), so pick one of the remaining $n-1$ dots and connect the second dot from the left on the top row to that dot.

Continuing on this way, we see the total number of possible diagrams is $n(n-1)(n-2)\cdots(n-n-1) = n!$. ∎

4.3 Creating new groups from old - Direct Products

Given two groups G and H, we can form a new one called the direct product. This is sometimes called an external direct product, but we won't call it that.

Definition. Let $(G, *)$ and $(H, \circ)$ be groups. Define the **direct product** of G and H as the group $(G \times H, \cdot)$ where

$$G \times H := \{(g, h) : g \in G, h \in H\}$$

and $(g_1, h_1) \cdot (g_2, h_2) := (g_1 * g_2, h_1 \circ h_2)$.

Let's play around with an example. Consider $\mathrm{GL}_3(\mathbb{Z}) \times \mathbb{Z}_3$. Remember, the operation in $\mathbb{Z}_3$ is addition, and the operation in $\mathrm{GL}_3(\mathbb{Z})$ is matrix multiplication. Let's do a quick calculation in this group.

$$\left(\begin{bmatrix}1&2&3\\0&1&2\\0&0&1\end{bmatrix}, 2\right) \cdot \left(\begin{bmatrix}1&0&0\\4&1&0\\-1&0&-1\end{bmatrix}, 1\right) = \left(\begin{bmatrix}1&2&3\\0&1&2\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\4&1&0\\-1&0&-1\end{bmatrix}, 2+1\right)$$
$$= \left(\begin{bmatrix}6&2&-3\\2&1&-2\\-1&0&-1\end{bmatrix}, 0\right).$$

Notice that the operation takes in two elements of the form (A, x) for $A \in \mathrm{GL}_3(\mathbb{Z})$ and $x \in \mathbb{Z}_3$, and returns another element in the group.

As an exercise, prove that if G and H are groups, $G \times H$ is a group.

5 Classifying Groups

We will now introduce one of the big underlying questions in group theory: what groups can exist? This is pretty vague, so let's make the question a little more specific: What groups of order n can exist?

Let's start with the case $n = 2$. We have a few groups of order 2: $\mathbb{Z}_2$, $\{1, -1\}$, $\mathbb{Z}_6^*$. Let's look at the **Cayley table**s in order:

$+$	0	1
0	0	1
1	1	0

$\cdot$	1	-1
1	1	-1
-1	-1	1

$\cdot$	1	5
1	1	5
5	5	1

.

There are a few things to notice here. First, if you relabel the elements all the tables look the same. This isn't a coincidence because of the following result.

Lemma 5. *In any row or column of a Cayley table of a group, every element in that group appears exactly once.*

Proof. In Assignment 1 you will prove that $f_a : G \to G$ defined by $f_a(g) := ag$ is a bijection. In a similar manner you can prove that the function $h_a : G \to G$ defined by $h_a(g) := ga$ is also a bijection.

The function f_a being injective says that every entry in the row labelled by a can appear at most once, and f_a being surjective says that every element must appear. A similar argument with h_a completes the proof. ■

Let's use this to see that every group of order 2 must have a Cayley table like the one above. Let the two elements be e (since every group must have an identity) and a. Then immediately we know the table must at least look like

$\cdot$	e	a
e	e	a
a	a	

and since every row and column must have every element exactly once, the bottom right hand entry must be an e. That was a nice warm up, let's move on.

What about groups with 3 elements? Let's have a look at some examples of groups of order 3.

- Our good friend $\mathbb{Z}_3$.
- The group of rotations of a regular triangle. This is like the dihedral group D_3 except you are not allowed flips. The three rotations will be denoted $\{e, r_1, r_2\}$, r_1 is a rotation clockwise by 120 degrees, and r_2 by 240. We will call this group G_1.
- The group
$$G_2 := \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \right\}$$
where the operation is matrix multiplication. We will denote these three matrices I, A, B.

You can check that all three of these are groups (we already know the first one is!). Let's draw out the Cayley tables for them all in order:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	e	r_1	r_2
e	e	r_1	r_2
r_1	r_1	r_2	e
r_2	r_2	e	r_1

$\cdot$	I	A	B
I	I	A	B
A	A	B	I
B	B	I	A

.

Let's prove that this always happens. Suppose $\{e, a, b\}$ make up three elements of a group. The Cayley table must look like

$\cdot$	e	a	b
e	e	a	b
a	a		
b	b		

since one of the elements must be the identity, and we may as well let it be e. The middle entry can now be either e or b (since a already appears in the middle row). If it is e, then the middle right entry must be b, which is not possible since b already appears in the third column. Therefore the middle must be b. With b in the middle, that leaves one possibility for every other entry, giving us the Cayley table

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

What this tells us is that up to renaming elements, all groups of order 3 are the same! Notice that I didn't have to put the identity first, and if I switched the order of e and a in the previous table, the table would look different. Because of this, if we want to work out whether or not two groups are the same, we have to allow reordering of the elements in the Cayley table.

Lecture 6 - 16/05

This leads us to the following definition. We will later see another way to make the same definition, but this will do for now.

Definition. Two groups G and H are **isomorphic** if, after relabelling and reordering elements, both their Cayley tables are identical. In this case we write $G \cong H$.

Exercise. Prove that $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic. Also, prove that up to isomorphism, these are the *only* two groups of order 4.

Before we move on, it is worth noting that Lemma 5 is not the only restriction on Cayley tables. As we noted earlier with the Cayley table for D_4, the identities have to be symmetric about the main diagonal. There are also additional restrictions that come from the fact that the group operation must be associative (the first of the group axioms). These are for you to figure out!

6 Subgroups

One of the keys to understanding a group, is understanding its subgroups. They can tell you things about the group you never thought you wanted to know!

6.1 Examples and Definition

Subgroups are what they sound like, they are subsets of a group that also form a group. We have already seen a few examples of these, but let's focus on the integers for now.

Consider the set $2\mathbb{Z} := \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. This is a subset of $\mathbb{Z}$ and we can ask whether or not this forms a group, where the operation is the usual addition operation inherited from $\mathbb{Z}$. A quick check should convince you that $(2\mathbb{Z}, +)$ is indeed a group, and we say $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ and write $2\mathbb{Z} < \mathbb{Z}$.

Let's consider another subset, $\{3, 0, -3\} \subset \mathbb{Z}$. We can ask again, is this a group under addition? Well, it has an identity element, and everything has an inverse. We know addition is associative, so this looks like a group. However, addition is not actually a binary operation on this set, since $3 + 3$ is not in the set. Here, we say $\{3, 0, -3\}$ is not closed under addition, so it is not a subgroup of $\mathbb{Z}$.

Definition. Let $(G, \cdot)$ be a group. A subgroup $S < G$ is a subset $S \subset G$ such that $(S, \cdot)$ is a group.

It is worth pointing out that every group comes equipped with two subgroups: The group itself and the trivial subgroup.

The **trivial subgroup** is the subgroup consisting only of the identity element and nothing else. It may not be immediately clear why this is a subgroup, but you should convince yourself it always is.

Definition. Let $S < G$ be a subgroup of G. If S is not the whole group or the trivial subgroup, we say S is a proper subgroup of G.

The subgroup generated by a single element.

Given an element $a \in G$, there is a special subgroup associated to it. To begin this investigation, we must set some notation which we have informally been using already.

Definition. Let $a \in (G, \cdot)$. For any $k \in \mathbb{Z}$, define the element $a^k \in G$ by

$$a^k := \begin{cases} \overbrace{a \cdot a \cdots a \cdot a}^{k-\text{times}} & \text{if } k \text{ is a positive integer} \\ e & \text{if } k = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1} \cdot a^{-1}}_{k-\text{times}} & \text{if } k \text{ is a negative integer.} \end{cases}$$

As an exercise, prove that $a^n \cdot a^m = a^{n+m}$ and $(a^n)^{-1} = a^{-n}$ for all $n, m \in \mathbb{Z}$.

Definition. Let $a \in G$. Define the **order of** a, denoted $|a|$ as the smallest positive integer k such that $a^k = e$. If there is no such k, we say the order of a is infinite and $|a| = \infty$.

Definition. Let $a \in G$. Define the **subgroup generated by** a, denoted $\langle a \rangle$, as

$$\langle a \rangle := \{a^k : k \in \mathbb{Z}\}.$$

As an exercise, prove that $\langle a \rangle$ is indeed a subgroup. Even though $\langle a \rangle$ appears to be an infinite set, it can be finite as we will see now.

Consider the group $\mathbb{Z}_8$, and the element $2 \in \mathbb{Z}_8$. Let's write out all the powers of 2. This is kind of weird, because 2^4 for example, means $2 + 2 + 2 + 2$ since the group operation is addition.

k	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
2^k	$\cdots$	0	2	4	6	0	2	4	6	0	$\cdots$

This pattern keeps repeating, so $\langle 2 \rangle = \{0, 2, 4, 6\} \subset \mathbb{Z}_8$. Notice that the order of 2 is 4, and the order of the subgroup generated by 2 is also 4. Coincidence? No! Here is another exercise for you: prove that for an element $a \in G$, $|a| = |\langle a \rangle|$.

It is worth noting here that not all subgroups are the subgroup generated by a single element.

Indeed, consider the group $G = \mathbb{Z}_4 \times \mathbb{Z}_4$. Consider the subgroup $H = \{(0,0), (0,2), (2,0), (2,2)\} < G$. It turns out that this is not the subgroup generated by a single element. This is because

$$\begin{aligned}
\langle (0,0) \rangle &= \{(0,0)\} \\
\langle (2,0) \rangle &= \{(0,0), (2,0)\} \\
\langle (0,2) \rangle &= \{(0,0), (0,2)\} \\
\langle (2,2) \rangle &= \{(0,0), (2,2)\}
\end{aligned}$$

and none of these are all of H.

Lecture 7 - 21/05

6.2 The Subgroup Test

Suppose we have a subset of a group and we want to know whether or not it forms a subgroup. There are a few things we can check. For example, we could check if the identity is in there. If it isn't, we can immediately rule out the possibility of that subset being a group.

However, so far the only way we know how to check whether or not a subset $H \subset G$ forms a group is to check that the binary operation on G restricts to a binary operation on H, and that it satisfies the 3 group axioms. This can get tedious, and if you do it a few times you will realize that some of it comes for free from the fact that G is a group.

Here is a quick test that can take a bit of the work out of checking whether or not something is a subgroup.

Theorem 6 (The Subgroup Test)**.** *Let $(G, \cdot)$ be a group and $H \subset G$ a non-empty subset of the group. Suppose the following two conditions hold:*

1. *For all $a, b \in H$, $a \cdot b \in H$, and*
2. *For all $a \in H$, $a^{-1} \in H$.*

Then H is a subgroup of G.

Proof. To show something is a group, we need to show it satisfies the three group axioms. Condition 1 tells us that $\cdot$ is a binary operation on H, since if we take any two elements of H, $\cdot$ gives us back an element of H.

Since G is a group, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$, so in particular it is true for all $a, b, c \in H$.

To see there is an identity element in H, take an element $a \in H$ (which exists since H is non-empty). By condition 2 above, $a^{-1} \in H$, and by property 1 we have $e = a \cdot a^{-1} \in H$. Since $e \cdot a = a \cdot e = a$ for all $a \in G$, it is true for all $a \in H$.

Lastly, property 2 tells us that every element has an inverse, completing the proof. ■

It is important that $H \subset G$ is non-empty, otherwise it definitely isn't a group, so this needs checking as well!

6.3 Towards Lagrange's Theorem

Lagrange's theorem is a strong candidate for the most important theorem in mathematics (if such a title even makes sense). It is one of the main reasons group theory is so beautiful and powerful.

To see what it says, let's first look at a bunch of examples of subgroups that we have seen so far. We will denote the group by G and the subgroup by H.

G	H	$\lvert G\rvert$	$\lvert H\rvert$
$\mathbb{Z}_8$	$\langle 2 \rangle$	8	4
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\{(0,0),(0,2),(2,0),(2,2)\}$	16	4
D_n	$\langle f \rangle$ where f is any flip	$2n$	2
D_n	All rotations	$2n$	n
$\mathbb{Z}_9^*$	$\langle 2 \rangle$	6	6
$\mathbb{Z}_9^*$	$\langle 8 \rangle$	6	2
$\mathrm{GL}_2(\mathbb{Z}_3)$	$\{A \in \mathrm{GL}_2(\mathbb{Z}_3) : \det(A) = 1\}$	48	24.

Lecture 8 - 23/05

For any of the subgroups listed above that we haven't seen already, it's a good exercise to convince yourself that they are indeed subgroups and the orders are as they are listed above. Let's also focus our attention on $\mathbb{Z}_{12}$, and find the orders of each of the elements (which is the same as finding the orders of the subgroups generated by the elements).

x	0	1	2	3	4	5	6	7	8	9	10	11
$\lvert x\rvert = \lvert\langle x\rangle\rvert$	1	12	6	4	3	12	2	12	3	4	6	12.

There is something a little bit striking about both of these tables. Every single subgroup has an order that divides the order of the group it sits inside. Of course, this is not a coincidence and is essentiality the statement of Lagrange's theorem.

6.4 Cosets

In order to prove Lagrange's theorem, we have to talk about cosets of a subgroup. Intuitively, cosets of a subgroup are translations of the subgroup, and it turns out that they partition the group. Let's take a look at a couple of examples.

Example. Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z}$. We create the cosets of $4\mathbb{Z}$ by adding elements of $\mathbb{Z}$ to the entire group. It turns out there are only 4 cosets, and they are

$$\begin{aligned}
0 + 4\mathbb{Z} &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
1 + 4\mathbb{Z} &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
2 + 4\mathbb{Z} &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
3 + 4\mathbb{Z} &= \{\ldots, -5, -1, 3, 7, 11 \ldots\}.
\end{aligned}$$

We could add any other element of $\mathbb{Z}$ to $4\mathbb{Z}$, but we would just end up with one of the cosets already listed. For example, $7 + 4\mathbb{Z} = -1 + 4\mathbb{Z} = 3 + 4\mathbb{Z}$. There are two important things to notice here. First, is that every element of $\mathbb{Z}$ lies in one of the 4 cosets. Second is that all 4 cosets are disjoint, that is they share no elements in common.

Example. Let $G = \mathbb{Z}_9$, $H = \langle 3 \rangle = \{0, 3, 6\}$. Then the cosets are

$$\begin{aligned}
\{0, 3, 6\} &= 0 + H = 3 + H = 6 + H \\
\{1, 4, 7\} &= 1 + H = 4 + H = 7 + H \\
\{2, 5, 8\} &= 2 + H = 5 + H = 8 + H.
\end{aligned}$$

Again, notice that the cosets partition the whole group, that is every element of the group is in a coset, and the cosets are disjoint. There is something else worth noticing about this example: every coset has the same size.

Let's make this idea of a coset formal and define the index of a subgroup.

Definition. Let G be a group and $H < G$ a subgroup, and $a \in G$. The set $aH := \{ah : h \in H\}$ is called a **left coset** of H in G. The set $Ha := \{ha : h \in H\}$ is called a **right coset** of H in G.

Definition. Let G be a group and $H < G$ a subgroup. The **index** of H in G, denoted $|G : H|$, is the number of left cosets of H in G.

There are a couple of questions that naturally arise from these definitions. First, why do we define both left and right cosets?

Exercise. Find an example of a group G, a subgroup H, and an element $a \in G$ with the property that $aH \neq Ha$.

Second, what if we use right cosets to define the index?

Exercise. Prove that there is a bijection between the set of left cosets and the set of right cosets of a subgroup H in a group G. Conclude that the definition of index is independented of whether or not we choose to use right or left cosets.

6.5 Lagrange's theorem

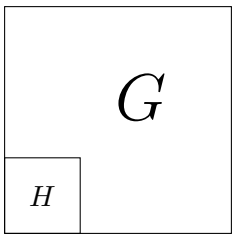
We now have the language and definitions to prove Lagrange's theorem, what my officemate calls "the most important theorem in mathematics." I don't entirely disagree with him either!

Here is the statement. There is a more general one for infinite groups, but we will only be concerned with the finite group case.

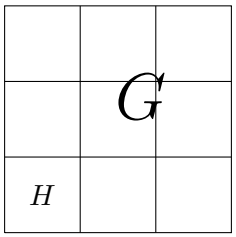
Theorem 7 (Lagrange's Theorem)**.** *Let G be a finite group, and $H < G$ a subgroup. Then $|H| \,\big|\, |G|$.*

Before we prove this, let's outline a road map. We will arbitrarily choose to work with left cosets, although right cosets would work just as well. The object is to show that left cosets partition the group: which means every group element appears in a coset, and no element occurs in two or more. Once we have shown this, we will then argue that all the cosets have the same size, and that will be enough. Let's see why.

Suppose our group G is represented by the square below, with H sitting inside it.



If the left cosets of H partition the group, and they are all the same size, then we can fill up the group by subsets of equal size as represented in



where each little square is a left coset of H. In this picture, $|G : H| = 9$ and therefore $|G| = 9\,|H|$ and $|H|$ divides $|G|$.

So, let's get proving! Until we prove Lagrange, G will be a finite group with a subgroup H.

Lemma 8. *Any left coset aH is the same size as the subgroup H.*

Proof. Let $a \in G$. Since left multiplication by an element is a bijection, we see $|H| = |aH|$. ■

Lecture 9 - 26/05

Lemma 9. *Suppose aH and bH are two left cosets of H in G. Then either they are equal or disjoint.*

Proof. Suppose $aH \cap bH = \emptyset$, then we are done. If not, there exists some element in both, call it x.

Then $x = ah_1 = bh_2$ for some elements $h_1, h_2 \in H$. This tells us that $b^{-1}ah_1 = h_2$. Now we wish to show that aH is contained in bH. Let ah be an arbitrary element of aH. Then

$$ah = bb^{-1}ah_1h_1^{-1}h = bh_2h_1^{-1}h$$

and since $h_1, h_2, h \in H$, and H is a group, $h_2h_1^{-1}h \in H$. Therefore $ah \in bH$ and we can conclude $aH \subset bH$.

A similar argument shows $bH \subset aH$ and we have $bH = aH$, completing the proof. ■

Lemma 10. *Every element $g \in G$ is in some left coset of H.*

Proof. This is an exercise. ■

These last two lemmas are what it means for the left cosets of H to **partition** the set G. Notice that nowhere in the last two lemmas did we use that G was a finite group. The fact that the cosets of a subgroup partition a group is true in infinite groups as well.

Proof of Lagrange's theorem. Let $\{a_1H, \ldots, a_kH\}$ be a complete set of left cosets of H in G. Since the left cosets of H partition G, we have

$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH| .$$

Since all cosets have the property that $|a_iH| = |H|$ we have

$$|G| = k\,|H|$$

completing the result. ■

Porism 11. *Let G be a finite group and H a subgroup. Then $|G| / |H| = |G : H|$.*

Proof. This is an exercise. ■

Fun fact: A porism is a result that follows from something in the proof of a theorem, whereas a corollary is something that follows from the statement of the theorem.

Let's now use Lagrange to investigate groups of order 15.

Example. We will prove that if G is a group of order 15, then any two distinct proper subgroups H and K must be such that $H \cap K = \{e\}$.

The divisors of 15 are 1,3,5, and 15, so any two proper subgroups must have order 3 or 5. Since $H \cap K$ is a subgroup of G (this is an exercise for the reader to justify), $|H \cap K|$ divides 15. Since $H \cap K$ is a subgroup of both H and K (this is also an exercise) we must have $|H \cap K|$ divides the orders of both H and K. Since $3 \nmid 5$ and both subgroups are distinct, neither one is entirely contained in the other. Therefore $|H \cap K| < |H|$ and $|H \cap K| < |K|$. Since both 3 and 5 are prime, the only way this can happen is if $|H \cap K| = 1$ and thus $H \cap K = \{e\}$.

We will now state a couple of corollaries which are very useful, and follow immediately from Lagrange's theorem. Their proofs are short exercises.

Corollary 12. *Let G be a finite group and $a \in G$. Then $|a|$ divides $|G|$.*

Corollary 13. *Let G be a finite group and $a \in G$. Then $a^{|G|} = e$.*

Corollary 14. *Any group of prime order is cyclic.*

Cyclic groups were introduced on Assignment 1, but I will give a formal definition here. The definition in the assignment is only valid for finite groups, but this one is valid for all groups. As an exercise, convince yourself that the two definitions agree when the group is finite.

Definition. A group G is **cyclic** if there exists an element $a \in G$ such that $\langle a \rangle = G$. Such an element is called a **generator** of G.

We will now look at an important application to elementary number theory.

Theorem 15 (Fermat's Little Theorem)**.** *If p is prime, then for any integer a we have $a^p \equiv a \mod p$.*

Proof. If $p \mid a$, then $a \equiv 0 \mod p$ so $a^p \equiv a \mod p$. If not, then $a \in \mathbb{Z}_p^*$. We know $\left|\mathbb{Z}_p^*\right| = p-1$ so by Lagrange, $a^{p-1} \equiv 1 \mod p$. Multiplying both sides by a gives us our result. ■

Lecture 10 - 28/05

Magic! Lagrange's theorem can also tell us interesting things about the Rubik's cube.

The Rubik's Cube

The Rubik's cube forms a group where the group elements are the moves (turn a face 90 degrees, for example, or rotate the whole cube), and the group operation is composition of moves (do one after the other). If you start at the solved state, and do two different moves which take you to the same state on the cube, then they are the same element in the group. Another way to think of this is to simply say that the group is the group of symmetries of the Rubik's cube.

With a bit of thought you can convince yourself that the group is finite (although that finite number is pretty damn big), since there are only finitely many positions and ways each little cube can sit inside the big cube. Because of this, we can use Lagrange to deduce some facts about this group.

Rotating a face by 90 degrees is an element of order 4 in the group (since doing it 4 times returns you back to where you started). This immediately tells us that the total size of the Rubik's cube group is a multiple of 4. As it happens, the move $\mathbf{RU}$ (this is standard notation for a cube, and can be found on the Wikipedia site for the Rubik's cube) has order 105, and the move $\mathbf{RU^{-1}}$ has order 63. This tells us the total order of the cube must be a multiple of both 105 and 63 (as well as 4). It turns out that the highest order element is an element of order 1260, given by $\mathbf{RU^2D^{-1}BD^{-1}}$.

Amazingly, these orders come nowhere close to the size of the actual group, which is of size $(11!)(8!)(2^{12})(3^8) \approx 42 \times 10^{18}$.

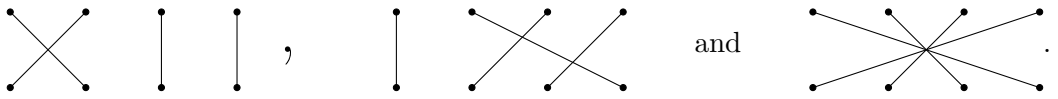
We have now done a decent amount of theory and built up this beautiful framework around groups. Let's shift our attention back to symmetric groups and investigate them a little more.

7 Symmetric Groups

So far symmetric groups have been irritating to deal with because of the notation, but they are an incredibly powerful and useful part of finite group theory. We will now present two other ways of thinking about the symmetric group.

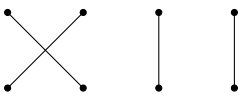
7.1 New perspectives on S_n

We will introduce two new ways to talk about elements of S_n. Up to now, the elements of S_4 for example, are diagrams that look like



As we mentioned earlier, these diagrams are representing permutations of the 4 dots. If we number the dots 1,2,3,4 from left to right, we can think of each element as a function $\sigma : \{1,2,3,4\} \to \{1,2,3,4\}$ which is a bijection.

The element of S_4 given by



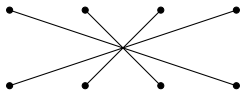
corresponds to the permutation σ where $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$, and $\sigma(4) = 4$.

Definition. A **permutation** on a set X is a bijection $\sigma : X \to X$.

We really want to think as elements of S_n as permutations on the set $\{1, \ldots, n\}$. Repeating a permutation repeatedly does different things to different elements of $\{1, \ldots, n\}$. This information is what will be captured in cycle notation for permutations.

7.2 Cycle Notation

Consider the element



in S_4. Viewing this as a permutation (as we should!) we see that 1 goes to 4 and 4 goes to 1, so if we keep performing the permutation we get a cycle

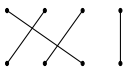
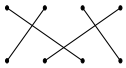
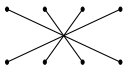
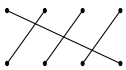
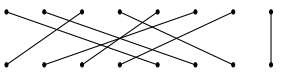
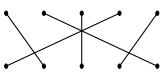
$$1 \to 4 \to 1 \to 4 \to 1 \to 4 \to 1 \cdots$$

and similarly

$$2 \to 3 \to 2 \to 3 \to 2 \to 3 \to 2 \cdots .$$

Notice that these two cycles are disjoint, and they tell us exactly what the permutation does. Because of this, we can denote sigma in what is called **cycle notation** by (14)(23). It turns out, and it will be an exercise for you to prove, that every permutation can be written like this.

Let's see some more examples of how to write permutations in cycle notation.

Old Notation	**Cycle Notation**
	(132)
	(1342)
	(14)(23)
	(1432)
	(153)(26)(47)(8)
	(1254)

There are two important remarks that need to be made about this new notation.

Remark.

1. The number we write first in each cycle has no effect on the actual permutation. For example, the cycle (123) is the same as (231) is the same as (312). Because of this, we choose to start each cycle with the lowest number.

2. If a cycle has length 1, we will omit it. In the last example in the table above, (1254) should have been (1254)(3), but it is understood that the 3 is sent to itself if it is left out. Likewise, the second last example in the table could have simply been (153)(26)(47), and context would have told us we are in S_8 so the 8 is sent to itself. The only time we must put in cycles of length 1 is when we are talking about the identity element, in which case we denote it by (1) regardless of which S_n we are working in.

Definition. An n**-cycle** is a cycle of the form $(a_1\, a_2\, \ldots\, a_{n-1}\, a_n)$. A 2-cycle is called a **transposition**.

To use this new language in a sentece, we would say that the second last example in the table above is a product of a 3-cycle and two transpositions.

Example. Here are all the elements of S_3 in cycle notation.

(1) (12) (13) (23) (123) (132)

We see that S_3 consists of the identity, three transpositions and two 3-cycles.

The group operation

Since elements of S_n are permutations $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, the group operation will be performed in reverse. For example, $\sigma\tau$ will be the permutation obtained by performing τ first, and then σ. "Why do something this ludicrous?" I hear you ask? Well, let's take a look at an example.

In the table below, we define σ and τ in S_4, and compute $\sigma\tau$ viewing them as functions.

$\sigma(1) = 3$	$\tau(1) = 4$	$\sigma\tau(1) = \sigma(4) = 2$
$\sigma(2) = 1$	$\tau(2) = 2$	$\sigma\tau(2) = \sigma(2) = 1$
$\sigma(3) = 4$	$\tau(3) = 3$	$\sigma\tau(3) = \sigma(3) = 4$
$\sigma(4) = 2$	$\tau(4) = 1$	$\sigma\tau(4) = \sigma(1) = 3.$

When the permutations are presented as functions (which is what they are), it is natural to do the one on the right first, and then the one on the left. Because of this, the group operation in S_n will go in the opposite order than usual.

The same calculation using cycle notation would look like

$$\sigma = (1342) \qquad \tau = (14) \qquad \sigma\tau = (1342)(14) = (12)(34).$$

Becoming fluent in performing group operations in S_n using cycle notation is an important skill, and takes a little getting used to. As a general method, here's how I like to do it (of course, you're welcome to do whatever works for you, even if it involves converting the permutations into function notation or the old cumbersome notation and then back again).

1. Pick the lowest number that hasn't appeared in your answer yet, and write it as the first number of a new cycle.

2. Start from the right most cycle and move left. At each cycle, work out where the number you have gets sent to.

3. Once you have moved through all the cycles, write down the number you are left with next to the first number you have written down.

4. Repeat with the new number.

5. If you end up with the number you started that cycle with, close the bracket.

6. Repeat all the steps until you have written down every number in $\{1, \ldots, n\}$, leaving out any numbers that form a 1-cycle.

These instructions are dificult to follow (and to write down!). Becuase of this, the best way for you to become comfortable with cycle notation is to practice, practice, and then practice some more. Here are a few examples for you to work through.

$$(12)(13)(14) = (1432)$$
$$(142)(123)(12)(23) = (13)(24).$$

There are more examples in the exercises for you to work through, or just make some up!

Each group S_n comes with an index-2 subgroup A_n. In order to talk about this group, we need the following few lemmas.

Lemma 16. *Every cycle can be written as a product of transpositions.*

Proof. We claim that $(a_1 \cdots a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_2)$. The proof will be by induction on n. If $n = 2$, $(a_1\, a_2)$ is already a transposition, which is our base case. For $n > 2$, notice that $(a_1\, a_2 \ldots a_n) = (a_1\, a_n)(a_1\, a_2 \ldots a_{n-1})$. By the inductive assumption we have $(a_1\, a_2 \ldots a_{n-1}) = (a_1\, a_{n-1}) \cdots (a_1\, a_2)$ so

$$(a_1\, a_2 \ldots a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_2)$$

completing the proof. ■

Lemma 17. *Every permutation can be written as a product of disjoint cycles.*

Proof. This is an exercise. ■

Although this is an exercise, here is a sketch of the idea of the proof. Given a number $k \in \{1, \ldots, n\}$ and $\sigma \in S_n$, we can look at where k is sent under repeated application of σ. This is called the orbit of k under σ. The idea is to prove that the orbits of all the numbers in $\{1, \ldots n\}$ partition the set $\{1, \ldots, n\}$, and these partitions are the disjoint cycles.

Lecture 11 - 30/05

Theorem 18. *Every permutation can be written as a product of transpositions.*

Proof. Since every cycle is a product of transpositions and every permutation is a product of cycles, the result follows. ■

7.3 Odd and Even Permutations and the Alternating Group

We just showed that every permutation can be written as a product of transpositions, so we can ask the following question: How many transpositions do we need to write any particular element?

For example, consider the element $(123) \in S_4$. From the proof of lemma 16, we know $(123) = (13)(12)$. But we could also write $(123) = (13)(14)(23)(14)(23)(12)$, or $(123) = (24)(13)(24)(12)$. Here we have the three cycle (123) written as a product of $2, 6$ and 4 transpositions respectively. However, since a transposition only moves 2 things in $\{1, 2, 3, 4\}$, it cannot be written as 1 transposition.

Let's look at another example, $(12) \in S_4$. This can clearly be written as a product of 1 transpositions, but we also have $(12) = (34)(12)(34)$ and $(12) = (12)(34)(12)(12)(34)$. Here we have this element written as a product of 3 and 5 transpositions.

Notice that in both examples it seems like we might be able to write each permutation as a product of however many transpositions as you like. However, if you try, you will find that you can only seem to write the first permutation as a product of an even number of transpositions, and the second as an odd number. This is no coincidence, and is an indication of what happens in general.

Fact 19. *The identity $(1) \in S_n$ cannot be written as a product of an odd number of transpositions.*

The proof of the above fact is surprisingly involved, and I'll lead you through it in the exercises.

Proposition 20. *No permutation in S_n can be written as a product of both an even and an odd number of transpositions.*

Proof. Suppose you could write σ as both an even and an odd number of transpositions. Say

$$\sigma = (a_1\ b_1)\cdots(a_n\ b_n) = (c_1\ d_1)\cdots(c_m\ d_m)$$

with n odd and m even. Since for any transposition $(a\ b)^{-1} = (a\ b)$ we have

$$\begin{aligned}(1) &= ((a_1\ b_1)\cdots(a_n\ b_n))^{-1}\,(c_1\ d_1)\cdots(c_m\ d_m)\\ &= (a_n\ b_n)\cdots(a_1\ b_1)(c_1\ d_1)\cdots(c_m\ d_m).\end{aligned}$$

However, here we have the identity written as a product of $n + m$ transpositions, which is an odd number of transpositions. This is not possible by Fact 19, completing the proof. ■

Because of this result, the following definition makes sense.

Definition. If a permutation $\sigma \in S_n$ can be written as a product of an even number of transpositions, we say σ is an **even permutation**. If $\sigma \in S_n$ can be written as a product of an odd number of transpositions, we say σ is an odd permutation.

Let's write down all the even and odd permutations in S_3.

Even	Odd
(1)	(12)
(123)	(13)
(132)	(23).

Notice that there are the same number of even permutations as there are odd ones, and that in this case the set of even permutations form a subgroup.

Proposition 21. *Let $A_n := \{\sigma \in S_n : \sigma \text{ is even}\}$. A_n is a subgroup of S_n.*

Proof. The set A_n is non-empty since $(1) \in A_n$. Since an even number plus an even number is an even number, the product of two even permutations is even. Since $((a_1\ b_1)\cdots(a_n\ b_n))^{-1} = (a_n\ b_n)\cdots(a_1\ b_1)$ we see that the inverse of a product of n transpositions is a product of n transpositions. Therefore the inverse of an even permutation is even. Alas, by the subgroup test, A_n is a subgroup. ■

We can now define the alternating group.

Definition. The subgroup $A_n < S_n$ is called the **alternating group on n letters**.

Here are a couple of important exercises:

Exercise. 1. Prove that an n-cycle is even if and only if n is odd.

2. Prove that if σ is even and τ is odd, then $\sigma\tau$ is odd.

3. Prove that if σ and τ are odd permutations, then $\sigma\tau$ is an even permutation.

4. Prove that there are the same number of even permutations as there are odd permutations in S_n. Deduce that $|S_n : A_n| = 2$.

7.4 The Futurama Problem

This problem arises in the plot of Futurama Episode 10 in Season 6: The Prisoner of Benda. In the episode Professor Farnsworth and Amy build a machine that allows them to switch minds, but stay in the same bodies. They decide this would make for an excellent episode, so they agree to do so. With Professor Farnsworth's skinny body, Amy is free to gorge on food as she once could, and Professor Farnsworth can relive his youth in her body.

However, when they try to switch back, they realise that the machine cannot work on the same two people! To get around this, they bring Bender in and he switches minds with Professor Farnsworth (in Amy's body), but they run into the same problem (and hilarity ensues).

Spoiler alert: They end up bringing the whole crew in and eventually everything ends up alright.

An interesting question arises from this hilarious episode: How many more people did they actually need? Here is a more general way to state the problem:

Question: Let $\sigma \in S_n$ be any permutation. How many more numbers do you need to add to the set $\{1, \ldots, n\}$ so that you can undo the permutation σ only using distinct transpisitions, each involving at least one of the new numbers?

With a bit of thought, you can see that adding Bender was not enough, so the answer is at least 2 for $n = 2$.

Lecture 12 - 02/06

8 Cyclic Groups

8.1 Subgroups of cyclic groups

We have mentioned cyclic groups a few times up until now, and we will now focus on them for a little while. The goal of this section is to prove that every subgroup of a cyclic group is cyclic, and

that in a finite cyclic group of order n, there is exactly one subgroup of order d for all integers $d \mid n$ (Theorems 23 and 26 below).

We have already seen the definition of a cyclic group, but let's write it down again for completeness.

Definition. A group G is **cyclic** if there exists an element $a \in G$ such that $\langle a \rangle = G$. Such an element is called a **generator** of G.

Here are some examples of cyclic groups:

- $\mathbb{Z}_n = \langle 1 \rangle = \langle n-1 \rangle$.
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^2, 3^3\} = \langle 3 \rangle$.
- $\mathbb{Z} = \langle 1 \rangle$.
- $3\mathbb{Z} = \langle 3 \rangle$.
- $\{1, -1, i, -i\} = \langle i \rangle$.
- $\{(1), (123), (132)\} = \langle (123) \rangle < S_3$.
- $\langle a \rangle < G$ is cyclic for any group G and any element $a \in G$.

Notice that cyclic groups do not necessarily have to be finite, as demonstrated by the existence of $\mathbb{Z}$ and $3\mathbb{Z}$. All of these examples are abelian, which is a quick consequence of the definition and the first axiom from the definition of a group.

Proposition 22. *Cyclic groups are abelian.*

Proof. This is an exercise. ■

To motivate our first main theorem, let's look at the subgroups of $\mathbb{Z}$. We know that for each element $n \in \mathbb{Z}$ we get $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$, and these are all cyclic. It is natural to ask whether or not we can have a subgroup of $\mathbb{Z}$ which is not a cyclic group. It will turn out that the answer is no, but let's try to get an idea why this might be the case.

Suppose you had two elements in a subgroup H, say 8 and 12. Then since $4 = \gcd(8, 12)$, we know 4 must also be in this subgroup (in fact $4 = 8 + 8 - 12$). Because of this, we know our subgroup must contain every multiple of 4. Suppose every other element in the subgroup was a multiple of 4, then we would have $H = \langle 4 \rangle$. If there was another element that's not a multiple of 4, take the greatest common divisor of that with 4 and repeat the argument. You will eventually arrive at the conclusion that $H = \langle 2 \rangle$ or $H = \mathbb{Z}$. This is the idea that the proof of the next theorem will follow.

Theorem 23. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle$, and let $H < G$. If $H = \{e\}$, then $H = \langle e \rangle$, so assume H is non-trivial.

Pick an element $b \in H$ such that $b \neq e$. Then $b = a^s$ for some integer $s \neq 0$. Note that since H is a subgroup, $b^{-1} = a^{-s} \in H$. Therefore, H contains a positive power of a. Let m be the smallest positive integer such that $a^m \in H$. We will now show that $H = \langle a^m \rangle$.

Let $y \in H$ be an arbitrary element, so $y = a^n$ for some n. We can perform the division algorithm and we have $n = qm + r$ for some integers q, r with $0 \leq r < m$. Then

$$y = a^{qm+r} = a^{qm} a^r$$

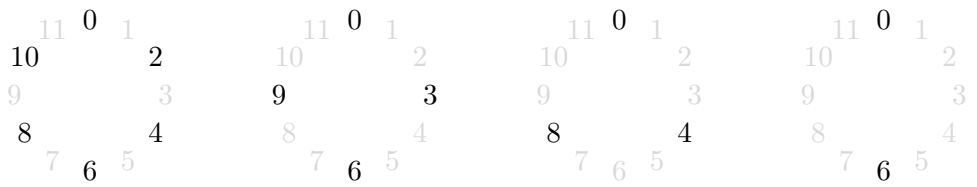
so $a^r = y(a^m)^{-q}$. Since $y, a^m \in H$, $a^r \in H$. But $r < m$, so $r = 0$ and $y = (a^m)^q$. Since every element in H is a power of a^m, $H = \langle a^m \rangle$. ■

The proof of this result is almost as important as the result itself. Suppose you have a cyclic group G and you know $a \in G$ generates G. If you are given a subgroup H, you know it is cyclic but you might want to be able to write down a generator for H. Then, as indicated in the proof, you simply find the first power of a that is in H, and that is your generator!

We now shift our gaze to proving that there exists exactly one subgroup of a finite cyclic group of every order allowed by Lagrange. Let's take a look at all the subgroups of $\mathbb{Z}_{12}$. Since we know all the subgroups must be cyclic, we can find them all by just taking the subgroup generated by a single element. Here are all the subgroups:

$$\begin{aligned} \langle 0 \rangle &= \{0\} \\ \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle &= \mathbb{Z}_{12} \\ \langle 2 \rangle = \langle 10 \rangle &= \{0, 2, 4, 6, 8, 10\} \\ \langle 3 \rangle = \langle 9 \rangle &= \{0, 3, 6, 9\} \\ \langle 4 \rangle = \langle 8 \rangle &= \{0, 4, 8\} \\ \langle 6 \rangle &= \{0, 6\}. \end{aligned}$$

Let's have a look at these on the clock! From left to right we have the proper subgroups $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, and $\langle 6 \rangle$ respectively.



Lecture 13 - 06/04

If you play around with these pictures, you will see that this is the only way you could possibly get a subgroup of order 4 (for example). These examples also give us a hint as to what the generator of each subgroup should be. We would guess that if G was a cyclic group of order n and $d \mid n$, then the subgroup of order d is generated by $a^{n/d}$, which is exactly what turns out to be true!

In order to prove the theorem, we first need a couple of lemmas.

Lemma 24. *Let G be a group and $a \in G$ an element of finite order $|a| = n$. Then for any $k \in \mathbb{Z}$, $a^k = e$ if and only if k is a multiple of n.*

Proof. This is an exercise. ■

Lemma 25. *Let $G = \langle a \rangle$ be a cyclic group of order n. Then for any element $a^s \in G$, $|a^s| = n/\gcd(n, s)$.*

Proof. Let $|a^s| = k$. Then k is the smallest number such that $a^{sk} = e$. However, we know sk is a multiple of n, so sk is the smallest number that is a multiple of both s and n, or $sk = \operatorname{lcm}(n, s)$. We then have

$$sk = \operatorname{lcm}(n, s) = \frac{ns}{\gcd(n, s)}$$

and so $k = n/\gcd(n, s)$. ■

Lecture 14 - 6/6

Theorem 26. *Let $G = \langle a \rangle$ be a cyclic group of order n. For every positive integer d that divides n, there exists a unique subgroup of order d, the subgroup $H = \langle a^{n/d} \rangle$.*

Proof. For $d = 1$, $H = \{e\}$ is the only subgroup of order 1, so suppose $d > 1$. Note $\left|a^{n/d}\right| = d$, so $H = \langle a^{n/d} \rangle$ is a subgroup of order d. It remains to show this is the only subgroup of order d.

Suppose K is a subgroup of order d. As in the proof above, $K = \langle a^s \rangle$ where s is the smallest positive integer such that $a^s \in K$. We would like to show $s = n/d$.

From an elementary number theory course we know there exists integers $u, v \in \mathbb{Z}$ such that $\gcd(n, s) = un + vs$, so

$$a^{\gcd(n,s)} = (a^n)^u (a^s)^v = (a^s)^v$$

and $a^{\gcd(n,s)} \in K$. Since $1 \leq \gcd(n, s) \leq s$ we must have $\gcd(n, s) = s$. By Lemma 25 we have

$$d = |a^s| = \frac{n}{\gcd(n, s)} = \frac{n}{s}$$

and so $s = n/d$, completing the proof. ■

This theorem is incredibly useful. For example, we immediately know what all the subgroups $H < \mathbb{Z}_{100}$ are. Here they are with their orders.

$\lvert H \rvert$	100	50	25	20	10	5	4	2	1
H	$\langle 1 \rangle = \mathbb{Z}_{100}$	$\langle 2 \rangle$	$\langle 4 \rangle$	$\langle 5 \rangle$	$\langle 10 \rangle$	$\langle 20 \rangle$	$\langle 25 \rangle$	$\langle 50 \rangle$	$\langle 0 \rangle = \{0\}$.

It is worth noting that the converse of this theorem is amazingly also true! We won't prove it, but it turns out that something slightly stronger is true.

Fact 27. *Let G be a group of order n. The following are equivalent.*

1. *G is cyclic.*
2. *For any positive divisor d of n, G has at most one subgroup of size d.*
3. *For any positive divisor d of n, G has exactly one subgroup of size d.*

Amazing! We proved that 1 implies 3 above, and 3 implies 2 by definition. If you are interested in why 2 implies 1, the book *Advanced Modern Algebra* by Joseph J. Rotman has 2 proofs at the end of §2.6.

8.2 Orders of elements and generators

Now that we know pretty much exactly what subgroups of cyclic groups look like, we wish to answer the following question: How do we know which elements generate a cyclic group? We have already seen that 1 and $n - 1$ always generate $\mathbb{Z}_n$, but often there are other generators as well.

On the way to proving the last theorem, we proved Lemma 25: If $G = \langle a \rangle$ and $|G| = n$, then $|a^s| = n/\gcd(n, s)$. This turns out to be the main tool to answer questions about generators.

Notice that if $\gcd(n, s) = 1$, then $|a^s| = n = |G|$ and so a^s generates G. In fact, we have the following result.

Proposition 28. *Let $G = \langle a \rangle$ with $|G| = n$. Then a^s generates G if and only if $\gcd(s, n) = 1$.*

Proof. This is an exercise. ■

Example. Let's find all the generators of $\mathbb{Z}_{15}$. We know $\mathbb{Z}_{15} = \langle 1 \rangle$, so the generators will be 1^s where $\gcd(15, s) = 1$. Remember here that 1^s means $\underbrace{1 + \cdots + 1}_{s\text{-times}}$. From this we see that the generators are $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

Example. Let $G = \langle (1234) \rangle = \{(1), (1234), (13)(24), (1432)\}$, which is a subgroup of S_4. Note that $|(1234)| = 4$, so the generators will be $(1234)^s$ where $\gcd(s, 4) = 1$. Since $(1234)^t = (1234)^{t+4k}$ for all $t, k \in \mathbb{Z}$ we only need to find powers $0 \leq s \leq 3$ so that $\gcd(s, 4) = 1$. These powers are 1 and 3, so there are two generators for G, $(1234)^1 = (1234)$ and $(1234)^3 = (1432)$.

8.3 An interesting fact about the Rubik's cube

If you have ever played around with a Rubik's cube, you will find that it is incredibly complicated. However, if you have ever learnt (or figured out) how to solve it, you realise that you can memorise a short list of moves that you can apply at certain times to solve the cube from any state.

This gives rise to an interesting question: Is there a single move, however long it may be, that if repeated over and over again will eventually solve any cube, regardless of its starting position?

If you think about it, this is the same as asking if there is a generator of the Rubik's cube group. This is because that move, if repeated enough times, will eventually pass through every state of the Rubik's cube. Another way of saying this is that every element of this group is a power of that particular element. So, if there was such a move, the Rubik's cube group would be cyclic.

However, if you play around with a cube you will realise this can't possibly be the case! There are a few reasons why. First, the group is non-abelian since (in standard Rubik's cube notation) $\mathbf{RU} \neq \mathbf{UR}$. Another reason is that both $\mathbf{R}$ and $\mathbf{L}$ have order 4, however $\langle \mathbf{R} \rangle \neq \langle \mathbf{L} \rangle$ and so there is more than one subgroup of order 4.

9 Homomorphisms

9.1 Examples

So far we have looked at individual groups, but if you think about different examples of groups, it becomes clear that they don't exist in isolation. There are copies of groups living inside other groups, and there is evidence of the structure of one group hiding in another. Let's take a look at some examples.

- There is a copy (whatever that means) of $\mathbb{Z}_4$ in S_4. The copy is

  $$\{(1), (1234), (13)(24), (1432)\} = \{(1234)^0, (1234)^1, (1234)^2, (1234)^3\}.$$

  We can think of this as a function $\phi : \mathbb{Z}_4 \to S_4$ given by $\phi(n) = (1234)^n$. This has the property that the structure of $\mathbb{Z}_4$ is preserved. That is $\phi(n + m) = (1234)^{n+m} = (1234)^n(1234)^m = \phi(n)\phi(m)$.

- There is a copy of $\mathbb{Z}_n$ in D_n, given by all the rotations. Another way of saying this is to let $\{r_0 = e, r_1, \ldots, r_{n-1}\}$ be all the rotations in D_n. Define a function $\phi : \mathbb{Z}_n \to D_n$ by $\phi(n) = r_n$. Again we see that $\phi(n + m) = \phi(n)\phi(m)$.

- Group together all the odd numbers in $\mathbb{Z}$ and all the even numbers in $\mathbb{Z}$, and label the odd numbers by 1 and the even numbers by 0. If you add an odd to an odd you get an even, an even to an odd you get an odd, and an even to an even you get an even. This translates to

$1+1=0$, $0+1=1$, $0+0=0$, which is exactly how the addition works in $\mathbb{Z}_2$. Formally, this is just a special case of a function coming up. Deifne $\phi : \mathbb{Z} \to \mathbb{Z}_2$ given by $\phi(a) = 0$ if a is even, and $\phi(a) = 1$ if a is odd. Then we see $\phi(a+b) = \phi(a) + \phi(b)$.

- There are 3 cosets of $3\mathbb{Z}$ in $\mathbb{Z}$, they are all the numbers that are 0 mod 3, 1 mod 3 and 2 mod 3. For ease of notation call these 0, 1, and 2 respectively. The sum of any two numbers from 0 give you a number back in 0, a number from 1 and a number from 2 give you a number from 0, and two numbers from 2 give you a number from 1 (for example). In fact, you will see that the entire structure of $\mathbb{Z}_3$ can be recovered like this. Again, this information can be packaged in the existence of a function $\phi : \mathbb{Z} \to \mathbb{Z}_3$ given by $\phi(n) = n \mod 3$.

- The addition in $\mathbb{Z}_n$ is the same in some sense as the addition in $\mathbb{Z}$. More formally, define a map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(k) = k \mod n$. By the definition of how addition works in $\mathbb{Z}_n$, this map preserves the group structure of $\mathbb{Z}$.

- Consider all the odd and even permutations in S_n. Since an odd permutation composed with an odd permutation is an even permutation, even with even is even, and even with odd is odd, the same structure of $\mathbb{Z}_2$ arises. Again, we can formalise this by defining a function $\phi : S_n \to \mathbb{Z}_2$ by $\phi(\sigma) = 0$ if σ is an even permutation, and 1 if it is an odd permutation.

- The Cayley table for D_4 is given by

$\cdot$	e	r_1	r_2	r_3	f_1	f_2	f_3	f_4
e	e	r_1	r_2	r_3	f_1	f_2	f_3	f_4
r_1	r_1	r_2	r_3	e	f_4	f_1	f_2	f_3
r_2	r_2	r_3	e	r_1	f_3	f_4	f_1	f_2
r_3	r_3	e	r_1	r_2	f_2	f_3	f_4	f_1
f_1	f_1	f_2	f_3	f_4	e	r_1	r_2	r_3
f_2	f_2	f_3	f_4	f_1	r_3	e	r_1	r_2
f_3	f_3	f_4	f_1	f_2	r_2	r_3	e	r_1
f_4	f_4	f_1	f_2	f_3	r_1	r_2	r_3	e

  If you ignore the subscripts, you see that two rotations give you a rotation, a rotation and a flip give you a flip, and two flips give you a rotation. Again, the structure of $\mathbb{Z}_2$ is lurking somewhere in the structure of D_4. The same goes for D_n. What would be a function we could define here to capture this observation?

Lecture 15 - 09/06

9.2 Definitions and Basic Results

Each of these examples involves comparing two groups, and it appears that the way to do this is to talk about functions between groups. We could talk about any old functions between two groups, but we want to pay attention to the fact that they are in fact groups! The functions we defined in the examples above are group homomorphisms. Informally, a group homomorphism is a function between groups that preserves the structure of a group.

Definition. Let $(G, \cdot)$ and $(H, *)$ be groups. A **group homomrophism from G to H** is a function $\phi : G \to H$ that satisifies $\phi(a \cdot b) = \phi(a) * \phi(b)$ for all $a, b \in G$.

Here are a few more examples of group homomorphisms.

- Let $\phi : \mathbb{R} \to \mathbb{R}^*$ be given by $\phi(x) = e^x$. This is a homomorphism since $\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$.
- Let $\det : \mathrm{GL}_n(\mathbb{Z}_k) \to \mathbb{Z}_k^*$ be the determinant map. Since $\det(AB) = \det(A)\det(B)$, this is a group homomorphism.
- Let V and W be vector spaces. If you ignore scalar multiplication, then V and W are groups. Any linear map $L : V \to W$ is a group homomorphism. This is because one of the conditions of being a linear map is that $L(v_1 + v_2) = L(v_1) + L(v_2)$ for all $v_1, v_2 \in V$.
- Consider the map $|\cdot| : \mathbb{Q}^* \to \mathbb{Q}^*$ given by taking the absolute value. Since $|ab| = |a|\,|b|$ this is a group homomorphism from $\mathbb{Q}^*$ to itself.
- Consider the map $|\cdot| : \mathbb{C}^* \to \mathbb{R}^*$ given by taking the norm of a complex number. Again, since $|ab| = |a|\,|b|$, this is a group homomorphism.

Here are some basic facts about group homomorphisms.

Proposition 29. *Let $\phi : G \to H$ be a group homomorphism. Then $\phi(e) = e$ and $\phi(a^{-1}) = \phi(a)^{-1}$.*

Proof. We have $\phi(a) = \phi(ea) = \phi(e)\phi(a)$. Multiplying on the right by $\phi(a)^{-1}$ we get $e = \phi(e)$. The proof of the second statement is an exercise. ■

Proposition 30. *Let G, H, and K be groups and let $\phi : G \to H$ and $\varphi : H \to K$ be homomorphisms. Then $\varphi\phi : G \to K$ is also a homomorphism.*

Proof. This is an exercise. ■

What homomorphisms exist between two groups can actually give us information about the structure of both groups! In order to see this, we must first define two important subgroups that come with a homomorphism.

Definition. Let $\phi : G \to H$ be a homomorphism. The **kernel** of ϕ is defined to be

$$\ker(\phi) := \{g \in G : \phi(g) = e\}.$$

The **image** of ϕ is defined to be

$$\mathrm{im}(\phi) := \{h \in H : \text{ there exists } g \in G \text{ such that } \phi(g) = h\}.$$

It is important to remember that $\ker(\phi)$ lives in G, and $\mathrm{im}(\phi)$ lives in H.

Example. Let $\det : \mathrm{GL}_3(\mathbb{Z}_9) \to \mathbb{Z}_9^*$ be the homomorphism that takes a matrix to its determinant. Since the identity in $\mathbb{Z}_9^*$ is 1, we have

$$\ker(\det) = \{A \in \mathrm{GL}_3(\mathbb{Z}_9) : \det(A) = 1\}.$$

The image is the set of all elements in $\mathbb{Z}_9^*$ that is the determinant of some matrix. For any $a \in \mathbb{Z}_9^*$, notice that

$$\det\left(\begin{bmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = a$$

so $\mathrm{im}(\det) = \mathbb{Z}_9^*$.

Example. Consider the homomorphism $\phi : \mathbb{Z}_4 \to S_4$ given by $\phi(n) = (1234)^n$. This is a homomorphism with $\ker(\phi) = \{0\}$ and $\text{im}(\phi) = \{(1), (1234), (13)(24), (1432)\} = \langle (1234) \rangle$.

Lecture 16 - 11/06

Example. Let G be a group, and $a \in G$. Define the homomorphism $\phi_a : \mathbb{Z} \to G$ given by $\phi_a(n) = a^n$. Notice that this is a homomorphism since $\phi_a(n+m) = a^{n+m} = a^n a^m = \phi_a(n)\phi_a(m)$. As an exercise, show that $\text{im}(\phi_a) = \langle a \rangle$. As another exercise, show

$$\ker(\phi_a) = \begin{cases} \{0\} & \text{if } |a| = \infty \\ n\mathbb{Z} & \text{if } |a| = n. \end{cases}$$

This homomorphism is sometimes called the **exponential map**.

Example. Let G and H be groups. Then there is always the **trivial homomorphism** $\phi : G \to H$ defined by $\phi(g) = e$ for all $g \in G$. It is easy to check this is a homomorphism. In this case we have $\text{im}(\phi) = \{e\}$ and $\ker(\phi) = G$.

In all the examples we have seen so far, both the image and kernel of a homomorphims are subgroups. As you might expect (especially since I'm pointing it out!), this is not a coincidence.

Proposition 31. *Let $\phi : G \to H$ be a homomorphism. Then $\text{im}(\phi)$ is a subgroup of H.*

Proof. Since $\phi(e) = e$ always, $e \in \text{im}(\phi)$ so $\text{im}(\phi)$ is non-empty.

Let $h_1, h_2 \in \text{im}(\phi)$. Then there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Since ϕ is a homomorphism, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = h_1 h_2$, so $h_1 h_2 \in \text{im}(\phi)$.

Finally, let $h \in \text{im}(\phi)$, and let $g \in G$ be such that $\phi(g) = h$. Then $\phi(g^{-1}) = \phi(g)^{-1} = h^{-1} \in \text{im}(\phi)$. Therefore by the subgroup test, $\text{im}(\phi)$ is a subgroup of H. ■

Proposition 32. *Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi)$ is a subgroup of G.*

Proof. Note that $e \in \ker(\phi)$ since $\phi(e) = e$, so $\ker(\phi)$ is non-empty.

Let $g_1, g_2 \in \ker(\phi)$. Then $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = ee = e$ so $g_1 g_2 \in \ker(\phi)$.

Finally, let $g \in \ker(\phi)$. Then $\phi(g^{-1}) = \phi(g)^{-1} = e^{-1} = e$ so $g^{-1} \in \ker(\phi)$. Alas, by the subgroup test, $\ker(\phi)$ is a subgroup of G. ■

Since homomorphisms are functions, we can talk about them being injective and surjective (sometimes called one to one and onto, even though the latter is grammatically questionable). It is easy to see that a homomorphism $\phi : G \to H$ is surjective if and only if $\text{im}(\phi) = H$. There is a characterisation of being injective as well, although it does not just follow immediately from the definitions.

Proposition 33. *Let $\phi : G \to H$ be a homomorphism. Then ϕ is injective if and only if $\ker(\phi) = \{e\}$.*

Proof. Suppose ϕ is not injective. Then there exist $g_1 \neq g_2$ in G such that $\phi(g_1) = \phi(g_2)$. Then

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1)\phi(g_1)^{-1} = e$$

so $g_1 g_2^{-1} \in \ker(\phi)$. However, since $g_1 \neq g_2$, $g_1 g_2^{-1} \neq e$ and therefore $\ker(\phi) \neq \{e\}$.

Conversely, if ϕ is injective then only one element in G can be sent to e. Since $\phi(e) = e$ always, this one element must be the identity. Therefore $\ker(\phi) = \{e\}$. ■

This is an extremely useful tool, especially when we start talking about isomorphisms and isomorphism theorems.

Lecture 17 - 13/06

9.3 Isomorphisms

In an age gone by, we introduced the notion of two groups being isomorphic. Recall that if the groups were G and H, this meant a relabelling of the elements of G by the elements of H, such that the Cayley graphs were identical. Intuitively, two groups being isomorphic means that they have the same structure, regardless of what we call the individual elements.

We now have the technology to make a slightly slicker definition of groups being isomorphic. If we think about the notion of relabelling the elements of G by elements of H, this is simply a bijection from G to H. The requirement that after the relabelling the Cayley graphs are identical, is stated another way by saying that the bijection must be a homomorphism.

Definition. An **isomorphism** between two groups G and H is a homomorphism $\phi : G \to H$ such that ϕ is a bijection. If there exists an isomorphism $\phi : G \to H$ we say G and H are **isomorphic** and denote it $G \cong H$.

It is important to note that to show two groups G and H are isomorphic, you need to construct a homomorphism $\phi : G \to H$ (or the other way around), and then show it is a bijection.

Example. Let's take a look at something we already know in our hearts: that $\mathbb{Z}_5 \cong \langle(12345)\rangle$, where (12345) is in S_5 (although it doesn't really matter, we can take any S_n with $n \geq 5$).

To prove this statement, we will construct an isomorphism $\phi : \mathbb{Z}_5 \to \langle(12345)\rangle$. Define $\phi(n) = (12345)^n$. You can check that this is a homomorphism.

To see it is injective, notice that the only integer $n \in \{0, 1, 2, 3, 4\}$ such that $(12345)^n = (1)$ is 0. Therefore $\ker(\phi) = \{0\}$ and ϕ is injective.

To see it is surjective, notice

$$\begin{aligned}\langle(12345)\rangle &= \{(1), (12345), (13524), (14253), (15432)\} \\ &= \{(12345)^0, (12345)^1, (12345)^2, (12345)^3, (12345)^4\}.\end{aligned}$$

Since $\phi(n) = (12345)^n$ and $n \in \{0, 1, 2, 3, 4\}$ we see $\text{im}(\phi) = \langle(12345)\rangle$ and ϕ is surjective.

Therefore $\phi : \mathbb{Z}_5 \to \langle(12345)\rangle$ is an isomorphism and $\mathbb{Z}_5$ and $\langle(12345)\rangle$ are isomorphic.

Remember that if two groups are isomorphic, then they have the same structure. It feels right that a cyclic group should not be isomorphic to a group that is not cyclic, or that an abelian group should not be isomorphic to a non-abelian group. This formal definition of groups being isomorphic that we are dealing with allows us to nail down these intuitions.

Example. If we play with $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, we feel like they are different in some sense. Although they are both abelian and they both have order 4, the first doesn't have an element of order 4, whereas the second one does! Let's see how this allows us to prove that $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

Suppose there was an isomorphism $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$. Since ϕ is surjective, there is some $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $\phi(a) = 1$. Notice that all $g \in \mathbb{Z}_2 \times \mathbb{Z}_2$ is such that $g^2 = e$.

Therefore we have $\phi(e) = \phi(a^2) = 1 + 1 = 2$, which cannot happen since ϕ is a homomorphism. Therefore ϕ cannot be an isomorphism and $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

It is worth noting that in this argument, what we actually proved is that there is no homomorphism $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ such that $1 \in \text{im}(\phi)$.

Example. We will now show that $\mathbb{Z}_6 \ncong S_3$. We could argue this similarly to the argument above since $\mathbb{Z}_6$ has an element of order 6 but S_3 does not. However, we will take a slightly different approach, and exploit the fact that $\mathbb{Z}_6$ is abelian whereas S_3 is not.

Suppose $\phi : \mathbb{Z}_6 \to S_3$ is an isomorphism. Since ϕ is surjective, there are $a, b \in \mathbb{Z}_6$ such that $\phi(a) = (12)$ and $\phi(b) = (23)$. Notice that $a + b = b + a$ but $(12)(23) = (123) \neq (132) = (23)(12)$. This will be the key.

Since ϕ is a homomorphism, $\phi(a + b) = \phi(a)\phi(b) = (123)$. We also have $\phi(b + a) = \phi(b)\phi(a) = (132)$. However, since $a + b = b + a$, $\phi(a + b) = \phi(b + a)$, contradicting the previous computation.

Therefore ϕ cannot be an isomorphism, and $\mathbb{Z}_6 \ncong S_3$.

The argument we just used can be generalised to prove the following.

Proposition 34. *Let G be an abelian group and H a non-abelian group. Then $G \ncong H$.*

Proof. This is an exercise. ■

Proposition 35. *Let $G = \langle a \rangle$ and $H = \langle b \rangle$ be cyclic groups. Then $G \cong H$ if and only if $|G| = |H|$.*

Proof. First note that if G and H are isomorphic, then there is a bijection $\phi : G \to H$ which implies $|G| = |H|$. This is true even if we allow $|G| = \infty$.

We will now prove the converse, first for finite cyclic groups and then for infinite ones.

Suppose now that $|G| = |H| = n$. Then

$$G = \{e = a^0, a^1, \ldots, a^{n-1}\} \quad \text{and}$$
$$H = \{e = b^0, b^1, \ldots, b^{n-1}\}.$$

Notice that in G we have $a^s a^t = a^{(s+t \mod n)}$, and the same with H. We wish to find an isomorphism $\phi : G \to H$.

Define $\phi(a^i) = b^i$ for all $i \in \{0, \ldots, n-1\}$. Then

$$\phi(a^t a^s) = \phi(a^{(t+s \mod n)}) = b^{(t+s \mod n)} = b^t b^s = \phi(a^t)\phi(a^s).$$

Therefore ϕ is a homomorphism. Notice that $\ker(\phi) = \{a^0\} = \{e\}$ so ϕ is injective. Given a $b^t \in H$, $\phi(a^t) = b^t$ so $\mathrm{im}(\phi) = H$.

This proves that ϕ is an isomorphism, and $G \cong H$.

Suppose now that $|G| = |H| = \infty$. Then

$$G = \{a^k : k \in \mathbb{Z}\} \quad \text{and}$$
$$H = \{b^k : k \in \mathbb{Z}\}.$$

Define

$$\begin{aligned} \phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \end{aligned}$$

for all $k \in \mathbb{Z}$. Then

$$\phi(a^t a^s) = \phi(a^{t+s}) = b^{t+s} = b^t b^s = \phi(a^t)\phi(a^s)$$

so ϕ is a homomorphism. The identity in H is given by b^0 so $\ker(\phi) = \{a^0\} = \{e\}$ and ϕ is injective. Given $b^k \in H$, $\phi(a^k) = b^k$ so $\mathrm{im}(\phi) = H$ and ϕ is surjective.

Finally, ϕ is an isomorphism and $G \cong H$. ■

Corollary 36. *Let G be a cyclic group. Then if $|G| = n$, $G \cong \mathbb{Z}_n$. If $|G| = \infty$, $G \cong \mathbb{Z}$.*

Corollary 37. *Let p be a prime and let G and H be groups of order p. Then $G \cong H$.*

Proof. This is an exercise. ■

This next proposition is another way of thinking about isomorphisms. It is akin to the idea from linear algebra that a linear map is an isomorphism if and only if it is invertible. In the proposition below, φ plays the role of the inverse of ϕ.

Proposition 38. *Let G and H be groups. A homomorphism $\phi : G \to H$ is an isomorphism if and only if there exists a homomorphism $\varphi : H \to G$ such that $\phi\varphi(h) = h$ for all $h \in H$ and $\varphi\phi(g) = g$ for all $g \in G$. We call such a φ the* **inverse** *of ϕ, and denote it $\varphi = \phi^{-1}$.*

Proof. This is an exercise. ■

Let's take a moment to talk about this proposition, because it is something typical that happens in mathematics. Here we have a definition of a concept (isomorphism), and then a proposition which says the definition is equivalent to some other set of conditions. We could just have easily defined an isomorphism to be a homomorphism with an inverse, and then proved that this is the same as being a bijective homomorphism. The point is that with a result like this, we can now use whichever definition is most convenient or enlightening to us.

10 Normal Subgroups and Quotient Groups

This section will be about the study of very special subgroups called normal subgroups, and their use in the formation of what are called quotient groups. My favourite treatment of this subject is in a blog post by Timothy Gowers (https://gowers.wordpress.com/2011/11/20/normal-subgroups-and-quotient-groups/), and I will be more or less following this post for this section.

We have just defined images and kernels of homomorphisms, and we know they are both subgroups. There is a natural question to ask: can all subgroups of a group arise as the image or kernel of a homomorphism?

It turns out that the question is easy to answer for images of homomorphisms. Let $H < G$ be a subgroup and define the map

$$\begin{aligned} \phi : H &\longrightarrow G \\ h &\longmapsto h. \end{aligned}$$

A quick check will convince you that this is a homomorphism with $\mathrm{im}(\phi) = H$. This is called the **inclusion homomorphism**, and it shows that the question about which subgroups are images is not very interesting.

What about for kernels? Can all subgroups of a group arise as the kernel of a homomorphism? It turns out the answer is a little more involved.

Let's take a look at $H = \{(1), (12)\} < S_3$. Suppose it were the kernel of a homomorphism $\phi : S_3 \to G$ for some group G. Then we can do a trick, and **conjugate** (12) to show that if (12) is in the kernel, then (13) must also be in the kernel.

Consider $(23)(12)(23)^{-1} = (23)(12)(23) = (13)$. Then we see

$$\phi((13)) = \phi((23)(12)(23)) = \phi((23))\phi((12))\phi((23)) = \phi((23))\phi((23)) = \phi((23)(23)) = \phi((1)) = e.$$

This shows us that if (12) is in the kernel, then (13) is in the kernel. Therefore H cannot be the kernel of a homomorphism.

In general, we can show that if $\phi : G \to K$ is a homomorphism and $\phi(a) = e$, then $\phi(gag^{-1}) = e$ for all $g \in G$. So, if a subgroup $H < G$ is a kernel of some homomorphism, it must have the property that $ghg^{-1} \in H$ for all $h \in H$ and for all $g \in G$. This property is super important for a subgroup to have, so let's give it a name.

Definition. Let $H < G$ be a subgroup. We say H is a **normal subgroup** of G if for all $g \in G$, $ghg^{-1} \in H$ for all $h \in H$. We write this $H \triangleleft G$.

Another way to write this definition is to say $H < G$ is normal if for all $g \in G$, $gHg^{-1} \subset H$ for all $g \in G$. The following proposition tells us we could also have defined a subgroup H to be normal if $gHg^{-1} = H$ for all $g \in G$.

Proposition 39. *Let $H < G$ be a subgroup and $g \in G$. Then $gHg^{-1} \subset H$ if and only if $gHg^{-1} = H$.*

Proof. This is an exercise. ■

The discussion above shows us that if a subgroup $H < G$ is a kernel of a homomorphism, then it is normal (we will formally prove this below, but you pretty much already know how that goes).

So, we can now ask the natural question: Is a subgroup being normal the only restriction we need to conclude a subgroup is a kernel?

At first glance, this question seems to be quite difficult. If I give you a subgroup $H < G$, there is no other group in sight, let alone any homomorphism to it, how can we possibly prove it is the kernel of some homomorphism? We will approach this the only way we can, by pretending we've already found the homomorphism and see what we can say about it.

Let's assume G is a group with $H \triangleleft G$ and a homomorphism $\phi : G \to K$ for some group K with $\ker(\phi) = H$. Let's see what we can say about ϕ.

We already know that $\phi(h) = 0$ for all $h \in H$ so if $g_1 = g_2h$ we have $\phi(g_1) = \phi(g_2)$. So if two elements belong to the same left coset, ϕ sends them to the same place. Conversely, if $\phi(g_1) = \phi(g_2)$ then $\phi(g_2^{-1}g_1) = e$ so $g_2^{-1}g_1 = h$ for some $h \in H$ and $g_1 = g_2h$. This exactly says $g_1 \in g_2H$.

So, we can say that ϕ sends two elements in the same left coset to the same place, and elements from different cosets to different places. However, we just as well could have argued the same for right cosets. These observations are incompatible unless $gH = Hg$ for all $g \in G$.

Our major assumption is that $gHg^{-1} = H$ for all $g \in G$, so $gH = Hg$ and the observations we have made above about ϕ make sense. It is worth convincing yourself that if $gHg^{-1} = H$ then $gH = Hg$. The notation suggests it should be correct, but there is something to show!

Remember, at this point we don't actually know that ϕ exists, we have just deduced that if it does exist, then it sends elements in the same left coset to the same place, and elements in different left cosets to different places. Furthermore, we know we don't need to worry about whether or not we talk about left or right cosets. So, let's keep investigating.

We can now ask how the values obtained from different cosets play with each other. Suppose $\phi(g_1h_1) = a_1$ and $\phi(g_2h_2) = a_2$. We need $\phi(g_1h_1g_2h_2) = a_1a_2$ since ϕ is a homomorphism, so we can ask which coset $g_1h_1g_2h_2$ belongs to. Since H is normal we know $g_2^{-1}h_1g_2 = h_3$ for some $h_3 \in H$, which means $h_1 = g_2h_3g_2^{-1}$. Therefore we have

$$g_1h_2g_2h_2 = g_1g_2h_3h_2 \in g_1g_2H.$$

What this shows is that a element in g_1H times an element in g_2H ends up in g_1g_2H, which is about as nice as we could want!

At this point, let's take a breath. We now know a fair bit about ϕ, but we know almost nothing about the group which ϕ lands in, so let's try to construct that group. We would like a group which has an element for each coset of H in G, and the multiplication works as we want it to.

Lecture 19 - 18/06

Well, this seems tricky, but we can simply take the elements of the group to be the cosets themselves! What should the multiplication be? We showed above that $(g_1H)\cdot(g_2H) = g_1g_2H$ makes sense. We will call this group the quotient group G/H. Furthermore, $\phi : G \to G/H$ given by $\phi(g) = gH$ is a homomorphism with $\ker(\phi) = H$ which we will call the quotient map.

Definition. Let G be a group and $H \triangleleft G$. Define the **quotient group** $(G/H, \cdot)$ where G/H is the set of all left cosets of H in G, and $(g_1H)\cdot(g_2H) := g_1g_2H$. We will sometimes write gH as $[g]$ so with this notation, the operation is given by $[g_1]\cdot[g_2] = [g_1g_2]$.

As an exercise (and we essentially did it above) prove that if $[g_1] = [g_1']$ and $[g_2] = [g_2']$ then $[g_1g_2] = [g_1'g_2']$. This shows that the operation defined on G/H makes sense. As another exercise, show that this multiplication doesn't make sense when $H < S_3$ is the subgroup $H = \{(1), (12)\}$.

Whenever we have a group, we should ask what the identity is, and what inverses look like. The identity is given by the coset H itself, which is the coset $[e]$. This is because $[e][g] = [g]$ for all $g \in G$. It is not hard to show that inverses obey $[g]^{-1} = [g^{-1}]$. As an exercise, prove that $[g] = [e]$ if and only if $g \in H$.

Definition. Let G be a group and $H \triangleleft G$. Define the **quotient map** $\pi : G \to G/H$ by $\pi(g) = gH$.

With these definitions in mind, and the discussion above, it is an exercise for you to prove the following.

Proposition 40. *Let G be a group and H a subgroup. H is a normal subgroup if and only if $H = \ker(\phi)$ for some homomorphism $\phi : G \to K$ for some group K.*

Proof. This is an exercise. ∎

Because of this, you can use either condition to be the definition of normal. If you want to show a subgroup $H < G$ is normal, you can either show $gHg^{-1} = H$ for all $g \in G$, or you can show that H is a kernel of some homomorphism.

Lecture 20 - 20/06

Let's take a look at an example very familiar to us.

Example. Consider $\mathbb{Z}$ and $3\mathbb{Z} \triangleleft \mathbb{Z}$. Since $\mathbb{Z}$ is abelian, this subgroup is normal. The cosets are

$$\begin{aligned} 0 + \mathbb{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ 1 + \mathbb{Z} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ 2 + \mathbb{Z} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

So the quotient group $\mathbb{Z}/3\mathbb{Z}$ has three elements so we know $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$. In fact, the isomorphism is given by $\phi(n + \mathbb{Z}) = n$.

The quotient map $\pi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ is given by $\pi(x) = [x]$. Under the isomorphism $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}_3$, π is exactly the map $\pi(n) = n \mod 3$.

In general, $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(x + \mathbb{Z}) = x$ is an isomorphism. In fact, this is the way the group $\mathbb{Z}_n$ can be defined.

Here are some facts about normal subgroups and quotients that are exercises for you to prove.

Exercise. Prove the following.

- If G is abelian, then every subgroup is normal.
- Suppose $H < G$ is the only subgroup such that $|G : H| = n$ for some n. Then H is normal.
- The **centre of a group** $Z(G) := \{a \in G : ag = ga \text{ for all } g \in G\}$ is a normal subgroup of G.
- Let H be a normal subgroup of G. If G is finite, $|G/H| = |G| / |H|$.
- Let H be a normal subgroup of G. If G is abelian, then G/H is abelian.
- Let H be a normal subgroup of G. If G is cyclic, then G/H is cyclic.

We will prove one important fact about normal subgroups.

Proposition 41. *Suppose $H < G$ is such that $|G : H| = 2$. Then $H \triangleleft G$.*

Proof. If H is an index 2 subgroup, then there are two left and two right cosets. $H = eH = He$ is a left and right coset. Since the left cosets partition G, the other left coset must be $\{g \in G : g \notin H\}$. Since the right cosets partition G, the other right coset must be the same.

If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then

$$gH = \{g \in G : g \notin H\} = Hg.$$

So, for all $g \in G$, $gH = Hg$ so $gHg^{-1} = H$ and H is normal in G. ■

Corollary 42. *In S_n, A_n is a normal subgroup.*

Proof. We know that there are the same number of odd and even permutations, so $|S_n : A_n| = 2$ and $A_n \triangleleft S_n$. ■

10.1 The Quaternions

This is a natural place in the course to introduce a group called the quaternions. They were first discovered by William Hamilton in 1843 when he was looking for a way to multiply points in space. In the complex plane, we have a way of multiplying points in 2-dimensional space, so the desire was to find a way to multiply points in 3-dimensional space. The story goes that Hamilton was on a walk with his wife and they were on a bridge (Brougham Bridge, now known as Broom Bridge in Dublin) when it hit him. He stopped and carved the rules for the multiplication in the bridge:

$$i^2 = j^2 = k^2 = ijk = -1.$$

It turns out that this was actually a way to multiply points in 4-dimensional space. As it happens, this is what he was actually after! The cross product in $\mathbb{R}^3$ arises from the existence of the quaternions. There is a natural group which comes out of this setup, which we will call the **quaternion group** or just the quaternions.

The set is given by

$$\mathcal{Q}_8 := \{1, -1, i, -i, j, -j, k, -k\}$$

and the operation is multiplication. The multiplication works exactly as it does in the complex numbers, but with a few more rules. In $\mathbb{C}$, the multiplication works exactly the same as it does in $\mathbb{R}$, except wherever you see i^2 you replace it with -1. The multiplication in $\mathcal{Q}_8$ also works exactly the same as it does in $\mathbb{R}$, except with the following rules:

$$\begin{aligned} i^2 &= -1 \\ j^2 &= -1 \\ k^2 &= -1 \\ ijk &= -1. \end{aligned}$$

These rules are enough to multiply any two elements of Q_8 together. Notice that $i(-i) = -i^2 = 1$ so $i^{-1} = -i$. Similarly $j^{-1} = -j$ and $k^{-1} = -k$. With this in mind, suppose we wanted to find out what ji was. Well

$$ji = -ji(ijk) = -ji^2jk = j^2k = -k.$$

Similarly

$$ijk = -1 \quad \text{so } ij = -k^{-1} = k.$$

Therefore $\mathcal{Q}_8$ is non-abelian.

Exercise.

1. Prove that in an abelian group, all subgroups are normal.
2. Prove that all subgroups of $\mathcal{Q}_8$ are normal.

Lecture 21 - 23/06

11 The First Isomorphism Theorem

The first isomorphism theorem appears in many different areas of mathematics. Basically any time you can take a quotient, there is an isomorphism theorem. In fact, the rank-nullity theorem from linear algebra is a corollary of the linear algebra version.

Let's recall a few examples before we get stuck in.

Example. Consider the homomorphism $\phi : S_3 \to \mathbb{Z}_2$ given by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Note that $\ker(\phi) = A_3$ and $\text{im}(\phi) = \mathbb{Z}_2$. Since $|S_3 : A_3| = 2$, $S_3/A_3 \cong \mathbb{Z}_2$. Furthermore, the isomorphism is given by $\overline{\phi} : S_3/A_3 \to \mathbb{Z}_2$ where

$$\overline{\phi}([\sigma]) = \begin{cases} 0 & \text{if } \sigma \in A_3 \\ 1 & \text{if } \sigma \notin A_3. \end{cases}$$

Therefore we have $S_3/\ker(\phi) \cong \text{im}(\phi)$.

Example. Consider the homomorphism

$$\begin{aligned}\phi : \mathbb{Z}_9 &\longrightarrow \mathbb{Z}_3 \\ n &\longrightarrow n \mod 3.\end{aligned}$$

Then $\ker(\phi) = \{0, 3, 6\}$ and $\text{im}(\phi) = \mathbb{Z}_3$. Then $|\mathbb{Z}_9/\ker(\phi)| = |\mathbb{Z}_9| \,/\, |\ker(\phi)| = 3$ so it is isomorphic to $\mathbb{Z}_3$. However, we may build the isomorphism from ϕ as follows. Define

$$\begin{aligned}\overline{\phi} : \mathbb{Z}_9/\ker(\phi) &\longrightarrow \mathbb{Z}_3 \\ \overline{\phi}([n]) &\longrightarrow \phi(n).\end{aligned}$$

Suppose $[n] = [m]$, does $\phi(n) = \phi(m)$? If it doesn't, then $\overline{\phi}$ doesn't make any sense! Well if $[n] = [m]$, then $[n][m]^{-1} = [n-m] = [e]$, so $n - m \in \ker(\phi)$. Therefore $\phi(n-m) = \phi(n) - \phi(m) = 0$ so $\phi(n) = \phi(m)$. Now that we have checked that $\overline{\phi}$ is well defined, it is not too hard to see $\overline{\phi}$ is an isomorphism and $\mathbb{Z}_9/\ker(\phi) \cong \text{im}(\phi)$.

These two examples are an indication of what is true in general. This theorem is fantastically powerful.

Theorem 43 (The First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism. Then $G/\ker(\phi) \cong \text{im}(\phi)$.*

Proof. Let $\ker(\phi) = K$. Define the function

$$\begin{aligned}\overline{\phi} : G/K &\longrightarrow \text{im}(\phi) \\ [g] &\longmapsto \phi(g).\end{aligned}$$

We must first show that this is well defined, that is it doesn't depend on our choice of $g \in G$ we use to denote the element in G/K. Suppose $[g_1] = [g_2]$. We wish to show $\phi(g_1) = \phi(g_2)$. Since $[g_1] = [g_2]$, we have $[e] = [g_1][g_2]^{-1} = [g_1 g_2^{-1}]$ and therefore $g_1 g_2^{-1} \in K$. Then we have

$$e = \phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1}$$

so $\phi(g_1) = \phi(g_2)$. So $\overline{\phi}$ is well defined.

To see it is a homomorphism,

$$\overline{\phi}([a][b]) = \overline{\phi}([ab]) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}([a])\overline{\phi}([b]).$$

For injectivity, notice that $\phi(g) = e$ if and only if $g \in K$. Therefore $\overline{\phi}([g]) = e$ if and only if $[g] = [e]$ so $\ker(\overline{\phi}) = \{[e]\}$ and $\overline{\phi}$ is injective.

Since everything in $\text{im}(\phi)$ is of the form $\phi(g)$ for some $g \in G$, $\text{im}(\overline{\phi}) = \text{im}(\phi)$ and $\overline{\phi}$ is surjective.

Therefore $\overline{\phi}$ is an isomorphism and $G/K \cong \text{im}(\phi)$. ■

Corollary 44. *Let $\phi : G \to H$ be a homomorphism with G and H finite groups. Then $|\text{im}(\phi)|$ divides both $|G|$ and $|H|$.*

Proof. Since $\text{im}(\phi)$ is a subgroup of H, Lagrange's theorem tells us $|\text{im}(\phi)| \mid H$. The first isomorphism theorem tells us $G/\ker(\phi) \cong \text{im}(\phi)$. Then we have

$$|\text{im}(\phi)| = |G/\ker(\phi)| = |G| \,/\, |\ker(\phi)|$$

and so $|G| = |\ker(\phi)|\,|\text{im}(\phi)|$. Therefore $|\text{im}(\phi)|$ divides $|G|$. ■

The first isomorphism theorem is one of your most useful tools in proving that groups are isomorphic, especially if one of the groups is a quotient group.

Example. Let $H = \{1, -1\} \triangleleft \mathcal{Q}_8$. We want to show $\mathcal{Q}_8/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Define the map $\phi : \mathcal{Q}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$\begin{aligned}\phi(1) = \phi(-1) &= (0,0)\\ \phi(i) = \phi(-i) &= (1,0)\\ \phi(j) = \phi(-j) &= (1,1)\\ \phi(k) = \phi(-k) &= (0,1).\end{aligned}$$

This is a surjective homomorphism with $\ker(\phi) = \{1, -1\}$. Therefore by the first isomorphism theorem $\mathcal{Q}_8/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Lecture 22 - 25/06 and Lecture 23 - 27/06

12 Subgroup Lattices and the Correspondence Theorem

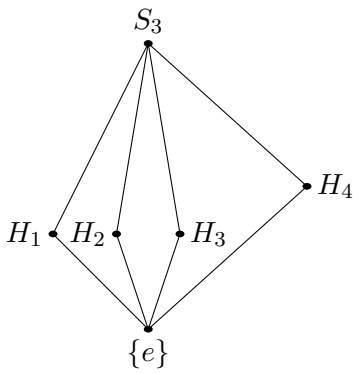
12.1 Subgroup Lattices

We can discover interesting things about a group by looking at its quotients. One of the things we can use quotients to learn more about is a group's subgroup lattice.

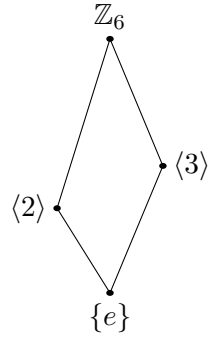
Example. Let $G = S_3$. We know from assignment 1 that all the subgroups are

$$\begin{aligned}\{e\} &= \{(1)\}\\ H_1 &= \{(1), (12)\}\\ H_2 &= \{(1), (13)\}\\ H_3 &= \{(1), (23)\}\\ H_4 &= \{(1), (123), (132)\} \quad \text{and}\\ S_3&.\end{aligned}$$

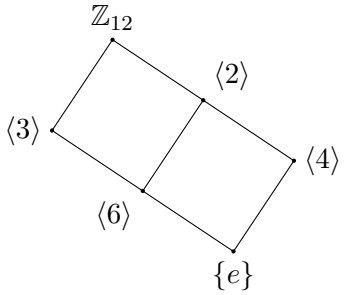
We can represent the way these subgroups relate to each other in a **subgroup lattice**. We will join one subgroup to another if one is contained in the other, with the larger subgroup higher up in the diagram. Here is the subgroup lattice for S_3.



Example. Again from assignment 1, we know the subgroups of $\mathbb{Z}_6$ are $\{e\}$, $\langle 2\rangle$, $\langle 3\rangle$, and $\mathbb{Z}_6$. The subgroup lattice in this case is



Example. We know what all the subgroups of a cyclic group of order n look like; there is exactly one subgroup subgroup of order d for all $d \mid n$, and all the subgroups are cyclic. As an exercise, deduce that the subgroup lattice of $\mathbb{Z}_{12}$ is



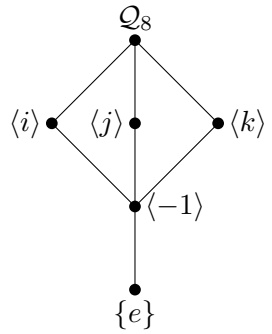
Notice that $|\langle 4\rangle| = 3$ and $|\langle 2\rangle| = 6$. Since $\langle 2\rangle$ is a cyclic group of order 6, it has a subgroup of order 3. Since there is only one subgroup of order 3 in $\mathbb{Z}_{12}$ it must be contained in $\langle 2\rangle$. Similar arguments can help you recover the entire lattice above.

There is one thing worth noticing in this example. Since $\mathbb{Z}_{12}$ is abelian, $\langle 6\rangle \triangleleft \mathbb{Z}_{12}$ so we can take the quotient. Since $\mathbb{Z}_{12}$ is cyclic, $\mathbb{Z}_{12}/\langle 6\rangle$ is a cyclic group of order 6 (since $|6| = 2$). Notice that the part of the lattice above $\langle 6\rangle$ is exactly the same as the lattice of $\mathbb{Z}_6$ (if you ignore the labels of the subgroups).

Example. From a practice exercise, the subgroups of $\mathcal{Q}_8$ are

$$\begin{aligned} \{e\} &= \{1\} \\ \langle -1\rangle &= \{1, -1\} \\ \langle i\rangle &= \{1, i, -1, -i\} \\ \langle j\rangle &= \{1, j, -1, -j\} \\ \langle k\rangle &= \{1, k, -1, -k\} \quad \text{and} \\ \mathcal{Q}_8. & \end{aligned}$$

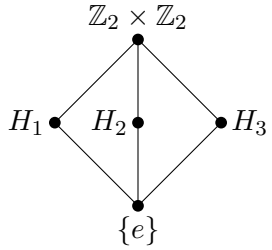
This gives us the subgroup lattice



Example. For $\mathbb{Z}_2 \times \mathbb{Z}_2$, since it is a group of order 4, all the proper subgroups have order 2. The subgroups are

$$\begin{aligned} \{e\} &= \{(0,0)\} \\ H_1 &= \{(0,0),(1,0)\} \\ H_2 &= \{(0,0),(0,1)\} \\ H_3 &= \{(0,0),(1,1)\} \quad \text{and} \\ \mathbb{Z}_2 \times \mathbb{Z}_2&. \end{aligned}$$

This gives us the subgroup lattice



We know from a while back that $\mathcal{Q}_8/\langle -1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Notice that the part of the lattice of $\mathcal{Q}_8$ above $\langle -1 \rangle$ is the same as the subgroup lattice of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

As an exercise, find the subgroup lattice of $\mathbb{Z}_n$ for your favourite positive integers n. Also do it for $\mathbb{Z}$, although don't do the whole thing (since it's infinite), and start from the top!

Let's keep these examples in mind while we talk about the next major theorem.

12.2 The Correspondence Theorem

To help with stating the next theorem, we first have to establish a bit of notation and prove a quick lemma.

Definition. Let $\phi : G \to H$ be a homomorphism between groups. Let $S \subset G$ be a subset. Then

$$\phi(S) := \{\phi(s) : s \in S\}$$

which is a subset of H. For a subset $T \subset H$,

$$\phi^{-1}(T) := \{g \in G : \phi(g) \in T\}.$$

Lemma 45. *Let $\phi : G_1 \to G_2$ be a homomorphism. If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2. If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*

Proof. This is an exercise. ■

The correspondence theorem is all about relating subgroups of quotients of a group, to subgroups of the group itself. This is sometimes called the fourth isomorphism theorem or the lattice isomorphism theorem.

Theorem 46 (The Correspondence Theorem)**.** *Let $\phi : G_1 \to G_2$ be a surjective homomorphism, and let $K = \ker(\phi)$. There is a one to one correspondence*

$$\begin{aligned} \{\textit{Subgroups } H \textit{ of } G_1 \textit{ such that } K < H < G_1\} &\longrightarrow \left\{\textit{Subgroups } \overline{H} \textit{ of } G_2\right\} \\ H &\longmapsto \phi(H) \\ \phi^{-1}(\overline{H}) &\longmapsfrom \overline{H}. \end{aligned}$$

Furthermore, this bijection has the following properties.

1. *For subgroups $K < H_1, H_2 < G_1$, $H_1 < H_2$ if and only if $\phi(H_1) < \phi(H_2)$.*
2. *For $K < H < G_1$, $|G_1 : H| = |G_2 : \phi(H)|$.*
3. *A subgroup H containing K is normal in G_1 if and only if $\phi(H)$ is normal in G_2.*

Proof. We will first show that both $H \to \phi(H)$ and $\overline{H} \to \phi^{-1}(\overline{H})$ are both well defined functions.

By the previous lemma, if H is a subgroup then $\phi(H)$ is a subgroup, so this function makes sense. Also by the previous lemma, since $\overline{H}$ is a subgroup of G_2 we know $\phi^{-1}(\overline{H})$ is a subgroup of G_1. It remains to check that $K < \phi^{-1}(\overline{H})$. However, $\phi(k) = e \in \overline{H}$ for all $k \in K$, and so $K < \phi^{-1}(\overline{H})$. Therefore both functions are well defined.

We will now show that the map $H \mapsto \phi(H)$ is a bijection between the set of subsets of G_1 containing H and the set of subgroups of G_2. We will do this by showing $\phi^{-1}\phi(H) = H$ and $\phi\phi^{-1}(\overline{H}) = \overline{H}$ for all subgroups H of G_1 containing K and all subgroups $\overline{H}$ of G_2.

Fix a subgroup $K < H < G_1$ and let $a \in \phi^{-1}\phi(H)$. Then $\phi(a) \in \phi(H)$, so there exists $b \in H$ such that $\phi(b) = \phi(a)$. Then we have $\phi(ab^{-1}) = e$ so $ab^{-1} \in K$. Since H contains K, $ab^{-1} \in H$. Since H is a subgroup we have $(ab^{-1})b \in H$ so $a \in H$. Therefore $\phi^{-1}\phi(H) \subset H$.

Conversely, let $a \in H$. Then $\phi(a) \in \phi(H)$ so $a \in \phi^{-1}\phi(H)$ and we conclude that $\phi^{-1}\phi(H) = H$ for all subgroups $K < H < G_1$.

The proof that $\phi\phi^{-1}(\overline{H})$ for all subgroups $\overline{H} < G_2$ is left as an exercise.

We can now conclude that $H \mapsto \phi(H)$ is a bijection (or a one to one correspondence) between subgroups of G_1 containing K and subgroups of G_2.

We must now prove that properties 1 and 2 hold. The proof that property 1 holds is left as an exercise. To prove property 2, we will construct a bijection between the set of left cosets of a subgroup H of G_1 containing K and the set of left cosets of $\phi(H)$ in G_2.

Fix a subgroup $K < H < G_1$ and define

$$\begin{aligned} \varphi : \{gH : g \in G_1\} &\longrightarrow \{g'\phi(H) : g' \in G_2\} \\ gH &\longrightarrow \phi(g)\phi(H). \end{aligned}$$

To see this is well defined, suppose $g_1H = g_2H$, so $g_2^{-1}g_1 \in H$. Then $\phi(g_2^{-1}g_1) \in \phi(H)$ so $\phi(g_1)\phi(H) = \phi(g_2)\phi(H)$. Therefore $\varphi(g_1H) = \varphi(g_2H)$ so φ is well defined.

For injectivity, suppose $\varphi(g_1H) = \varphi(g_2H)$, so $\phi(g_1)\phi(H) = \phi(g_2)\phi(H)$. This means $\phi(g_2)^{-1}\phi(g_1) \in \phi(H)$ or $\phi(g_2^{-1}g_1) \in \phi(H)$. Therefore $g_2^{-1}g_1 \in \phi^{-1}\phi(H) = H$ so $g_1H = g_2H$ and φ is injective.

For surjectivity, pick an arbitrary $g'\phi(H)$ of $\phi(H)$ in G_2. Since ϕ is surjective, there exists $g \in G$ such that $\phi(g) = g'$. Then $\varphi(gH) = \phi(g)\phi(H) = g'\phi(H)$ so φ is surjective.

Since φ is a bijection, the number of left cosets of H in G_1 is equal to the number of left cosets of $\phi(H)$ in G_2. Written another way, this says $|G_1 : H| = |G_2 : \phi(H)|$.

Property 3 is also an exercise. ■

Notice that if $\phi : G \to H$ is not a surjective homomorphism, we can simply replace H by $\text{im}(\phi)$ and then apply the correspondence theorem.

Corollary 47. *Let G and H be groups such that $G \cong H$. Then*

1. *G and H have the same subgroup lattices.*
2. *G and H have the same number of subgroups of index k for every k.*

Proof. Let $\phi : G \to H$ be an isomorphism, and note that $\ker(\phi) = \{e\}$. As an exercise, prove that the first statement follows from Property 1 of the correspondence theorem, and the second follows from Property 2. ■

Corollary 48. *Let G be a group and $K \triangleleft G$ a normal subgroup. Then there is a one to one correspondence between subgroups of G containing K and subgroups of G/K. Furthermore, this bijection preserves inclusion and index.*

Proof. This is an exercise in applying the correspondence theorem to $\pi : G \to G/K$ where π is the quotient map. ■

Notice that this corollary proves what we noticed earlier. That is, if $K \triangleleft G$, then the subgroup lattice of G/K is exactly the subgroup lattice of G that lies above K.

As an exercise to finish this section off, the correspondence theorem can be applied to finite cyclic groups to give a different proof a result we've already seen. It is more complicated and uses the unproven results in Fact 27, but it's always nice to have another way to prove a result.

Corollary 49. *Quotients of finite cyclic groups are cyclic.*

Proof. This is an exercise. ■

13 Automorphism Groups

Automorphisms of a group are best thought of as a symmetry of a group. Remember that a symmetry is something I can do to my object (in this case the group) that if you weren't looking when I did it, you wouldn't ever know it happened. Let's look at some examples to illustrate this.

Example. Consider the group

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \right\} = \{I, A, B\} < \text{GL}_2(\mathbb{Z}).$$

Notice that this group is isomorphic to $\mathbb{Z}_3$ since it has 3 elements. Let's take a closer look at it. We notice the following equalities hold:

$$A^2 = B, \quad B^2 = A, \quad \text{and} \quad AB = BA = I.$$

If you looked away, and I switched A and B, you would be none the wiser! This is an example of an automorphism of G.

Example. Consider S_3, and view the elements as bijections from $\{1,2,3\}$ to $\{1,2,3\}$. Intuitively, the element (12) should be no different to the element (13) because on some level, they both just switch two things, and it really shouldn't matter what we call those two things.

More formally, we can fix a $\tau \in S_3$, say $\tau = (23)$ and we can simply apply that to every permutation. So, we could create the map

$$\begin{aligned} \phi : S_3 &\longrightarrow S_3 \\ (1) &\longmapsto (1) \\ (12) &\longmapsto (13) \\ (13) &\longmapsto (12) \\ (23) &\longmapsto (23) \\ (123) &\longmapsto (132) \\ (132) &\longmapsto (123). \end{aligned}$$

Notice that we just switched the roles of 2 and 3 everywhere. This turns out to be a homomorphism, and can more succinctly be written as

$$\begin{aligned} \phi : S_3 &\longrightarrow S_3 \\ \sigma &\longmapsto \tau\sigma\tau^{-1}. \end{aligned}$$

This is an example of an inner automorphism, because it is intrinsic to the group in some sense.

Let's formally define an automorphism.

Definition. Let G be a group. An **automorphism** of G is an isomorphism $\phi : G \to G$. The set of all automorphisms is denoted $\mathrm{Aut}(G)$.

When you define something in mathematics there are always some questions you must ask. One of the most important questions is whether or not the thing you just defined actually exists. If we have a group, we can ask whether or not there actually is an automorphism of G.

Definition. Given a group G, define the **identity automorphism**

$$\begin{aligned} \mathrm{id}_G : G &\longrightarrow G \\ g &\longmapsto g. \end{aligned}$$

As an exercise, you can check that this is an automorphism regardless of the group. Because of this, we know that $\mathrm{Aut}(G)$ actually has at least one element, regardless of what G is.

Since this is a group theory course, it would be a shame if $\mathrm{Aut}(G)$ weren't a group. Thankfully, it is!

Proposition 50. *Let G be a group. Then $\mathrm{Aut}(G)$ is a group under composition. That is, for $\phi, \varphi \in \mathrm{Aut}(G)$, define $\phi\varphi \in \mathrm{Aut}(G)$ by $\phi\varphi(g) := \phi(\varphi(g))$.*

It is tempting when you have to prove that something is a group to just use the subgroup test. However, $\mathrm{Aut}(G)$ is *not* a subset of some larger group, so that won't work. We have no choice but to prove it is a group using the group axioms.

Proof. The composition of two automorphism is an automorphism (this is an exercise), so composition is a binary operation on $\mathrm{Aut}(G)$.

An exercise also shows that for $\phi, \varphi, \rho \in \mathrm{Aut}(G)$, $(\phi\varphi)\rho(g) = \phi(\varphi\rho)(g)$ for all $g \in G$ so $(\phi\varphi)\rho = \phi(\varphi\rho)$. Therefore composition is associative.

Another exercise shows that id_G plays the role of the identity in $\mathrm{Aut}(G)$.

The part of this proof I won't just leave as an exercise is the existence of inverses. Let $\phi \in \mathrm{Aut}(G)$. Define

$$\begin{aligned} \varphi : G &\longrightarrow G \\ g &\longmapsto g' \end{aligned}$$

where g' is the unique element in G such that $\phi(g') = g$. Let's first see that this is a homomorphism. Notice that for all $a, b \in G$,

$$\phi(\varphi(ab)) = ab = \phi(\varphi(a))\phi(\varphi(b)) = \phi(\varphi(a)\varphi(b)).$$

Since ϕ is injective, this implies $\varphi(ab) = \varphi(a)\varphi(b)$ so φ is a homomorphism. To see it is a bijection, for all $g \in G$ we have

$$\phi(\varphi(g)) = \phi(g') = g \quad \text{and} \quad \varphi(\phi(g')) = \varphi(g) = g'.$$

Since every element of G can be written as g' for some $g \in G$, this is enough to show that φ is a bijection and thus an automorphism. Furthermore, we have also just shown that $\phi\varphi(g) = \mathrm{id}_G(g)$ and $\varphi\phi(g) = \mathrm{id}_G(g)$ for all $g \in G$, so $\phi\varphi = \varphi\phi = \mathrm{id}_G$ and $\varphi = \phi^{-1}$.

We have now checked all the group axioms and therefore can conclude that $\mathrm{Aut}(G)$ is a group under composition. ■

The elements of $\mathrm{Aut}(G)$ are functions, so if you want to show that two automorphism $\varphi, \phi \in \mathrm{Aut}(G)$ are the same, you must show $\varphi(g) = \phi(g)$ for all $g \in G$. It doesn't matter what we call the functions, if they do the same thing they are the same function. Conversely if there exists a $g \in G$ such that $\varphi(g) \neq \phi(g)$, then $\varphi \neq \phi$.

Let's take a look at one of my favourite examples, $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

Example. Here is an outline of the fact that $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$. We know the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are $\{(0,0), (1,0), (0,1), (1,1)\}$, or $\{e, a, b, c\}$. Notice that $a^2 = b^2 = c^2 = e$, and a product of any two of $\{a, b, c\}$ results in the remaining element of a, b, or c. These observations give tell us that the three non-identity elements are indistinguishable in some sense, so we should be able to permute the three elements $\{a, b, c\}$ in any way we like and end up with an automorphism. As an exercise, use this idea to formally write down a proof that $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

An interesting thing to notice is that $\mathrm{GL}_2(\mathbb{Z}_2) \cong S_3$, so one might ask how can you think of a matrix in $\mathrm{GL}_2(\mathbb{Z}_2)$ as an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$? Well, we can think of an element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ as a column $\begin{bmatrix} a \\ b \end{bmatrix}$. Then for a matrix in $\mathrm{GL}_2(\mathbb{Z}_2)$, we can simply treat this is a linear map. For example, the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ gives us

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a+b \\ b \end{bmatrix}$$

so this matrix corresponds to the automorphism given by $(1,0) \mapsto (1,0)$, $(1,1) \mapsto (0,1)$, and $(0,1) \mapsto (1,1)$.

13.1 Conjugation, Inner Automorphisms and Outer Automorphisms

Any group comes with a bunch of automorphisms that are given by elements of the group itself. These automorphisms are called conjugation.

When you apply an automorphism to a group, you can think of it as looking at the group from another perspective, or in another language. However, a general automorphism sometimes seems to come out of the blue, and it's not always obvious how to translate (in the language sense) between the point of view you're used to (the Queen's English), and this new language (French). However, when this automorphism comes from conjugation, the group provides you with a translator. After all, viewing something in English and viewing it in French should give you the same information, and it's sometimes useful to move back and forth between the two.

Let's bring up the example we looked at earlier, with $\tau = (23)$ in S_3, and the automorphism

$$\begin{aligned} \phi_\tau : S_3 &\longrightarrow S_3 \\ \sigma &\longmapsto \tau\sigma\tau^{-1}. \end{aligned}$$

We say that we could think of this automorphism as simply switching the roles of 2 and 3, which is precisely what τ does. Looking at this automorphism, it is hard to believe that there are any other automorphisms besides ones that come from conjugation, at least in S_3 (or S_n). It turns out that this intuition is correct, for every S_n except for 6! Weird, I know.

In order to propertly define conjugation as an automorphism, we first need the following proposition, which you proved on assignment 3.

Proposition 51. *Let G be a group and $a \in G$. Then*

$$\begin{aligned} \phi_a : G &\longrightarrow G \\ g &\longmapsto aga^{-1} \end{aligned}$$

is an automorphism of G.

Proof. This is an exercise. ■

Definition. Let G be a group and $a \in G$. Define **conjugation by** a to be the automorphism

$$\begin{aligned} \phi_a : G &\longrightarrow G \\ g &\longmapsto aga^{-1}. \end{aligned}$$

Such an automorphism is called an **inner automorphism** and the set of all inner automorphisms is denoted $\mathrm{Inn}(G)$.

Since I defined something like this, you would hope it were a subgroup! You will not be disappointed.

Proposition 52. *The inner automorphism group* $\mathrm{Inn}(G)$ *is a subgroup of* $\mathrm{Aut}(G)$.

Proof. This is an exercise. ■

Remember that two automorphisms φ, ϕ are the same if $\varphi(g) = \phi(g)$ for all $g \in G$. With this in mind, it could be the case that $\phi_a = \phi_b$) for two different elements $a, b \in G$. Let's see this in an example.

Example. Consider $\text{Inn}(\mathcal{Q}_8)$. Notice that $\phi_1 = \text{id}_{\mathcal{Q}_8}$ is the identity in $\text{Inn}(\mathcal{Q}_8)$. Let's conisder ϕ_{-1}. For any $g \in \mathcal{Q}_8$, we have

$$\phi_{-1}(g) = (-1)g(-1) = g$$

so $\phi_{-1} = \phi_1 = \text{id}_{\mathcal{Q}_8}$. We also have $\phi_i(g) = ig(-i) = (-i)gi = \phi_{-i}(g)$ for all $g \in G$ so $\phi_i = \phi_{-i}$. Similarly we get $\phi_j = \phi_{-j}$ and $\phi_k = \phi_{-k}$.

Since these are all the inner automorphisms, we see that $|\text{Inn}(\mathcal{Q}_8)| = 4$, and it turns out that $\text{Inn}(\mathcal{Q}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Recall that $\mathcal{Q}_8/\langle -1\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and as an exercise, check that the center (defined below) of $\mathcal{Q}_8$ is $Z(\mathcal{Q}_8) = \langle -1\rangle$.

Lecture 24 - 02/07

From this example, it's believable that if an element a commutes with everything in a group, then $\phi_a = \text{id}_G$. This leads us to the definition of the center.

Definition. Let G be a group. Define the **center** of G by $Z(G) := \{a \in G : ag = ga \text{ for all } g \in G\}$.

In other words, the center of a group is the set of things that commute with everything. We saw above that the center should contain all the things that induce trivial inner automorphisms. So intuitively, it should be the case that if we ignore these (or quotient out by them), we get the inner automorphism group.

Proposition 53. *Let G be a group. Then $G/Z(G) \cong \text{Inn}(G)$.*

Proof. The strategy of this proof is to find a surjective homomorphism from G to $\text{Inn}(G)$ with kernel equal to $Z(G)$, and then the result will follow from the first isomorphism theorem.

First note that

$$\phi_a\phi_b(g) = \phi_a(bgb^{-1}) = (ab)g(ab)^{-1} = \phi_{ab}(g)$$

for all $g \in G$, so $\phi_a\phi_b = \phi_{ab}$. With this in mind, define the potential homomorphism

$$\begin{aligned} \Psi : G &\longrightarrow \text{Inn}(G) \\ g &\longmapsto \phi_g. \end{aligned}$$

Notice that $\Psi(ab) = \phi_{ab} = \phi_a\phi_b = \Psi(a)\Psi(b)$ so Ψ is a homomrophism. It is surjective since every inner automorphism is of the form ϕ_g for some $g \in G$. It remains to show $\ker(\Psi) = Z(G)$.

If $a \in \ker(\Psi)$, then $\phi_a(g) = g$ for all $g \in G$. That is $aga^{-1} = g$ for all $g \in G$, and rearranging we get $ag = ga$ for all $g \in G$ so $a \in Z(G)$.

Conversely, if $a \in Z(G)$, $\phi_a(g) = aga^{-1} = gaa^{-1} = g$ for all $g \in G$, so $a \in \ker(\Psi)$.

By the first isomorphism theorem, $G/Z(G) \cong \text{Inn}(G)$. ■

Corollary 54. *If G is abelian, $\text{Inn}(G) \cong \{e\}$.*

Proof. This is an exercise. ■

We now shift our attention to the automorphisms that are not inner automorphisms. Inner automorphisms are relatively easy to understand, so what about the rest? Well, in order to do this, we would like to ignore the inner automorphisms, and see what's left. The way to do this is to quotient out by the inner automorphisms. If only whenever we wanted to ignore something in real life we could just take a quotient!

In order to take the quotient, we must first show that $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

Proposition 55. *The inner automorphism group* $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$ *is a normal subgroup.*

Proof. Let $\psi \in \mathrm{Aut}(G)$ and $\phi_a \in \mathrm{Inn}(G)$. Then for all $g \in G$ we have

$$\psi\phi_a\psi^{-1}(g) = \psi(a\psi^{-1}(g)a^{-1}) = \psi(a)\psi\psi^{-1}(g)\psi(a^{-1}) = \psi(a)g\psi(a)^{-1} = \phi_{\psi(a)}(g)$$

so $\psi\phi_a\psi^{-1} \in \mathrm{Inn}(G)$. Therefore $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. ■

We can now define the outer automorphsim group.

Definition. Define the **outer automorphism group** of a group G to be

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G).$$

Studying outer automorphisms in general is extremely difficult, as is studying automorphism groups. Here are some fun facts about outer automorphism groups and automorphism groups to get a taste of what is out there.

- $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.
- $\mathrm{Aut}\left(\underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{k \text{ times}}\right) \cong \mathrm{GL}_k(\mathbb{Z}_p)$.
- There is no G such that $\mathrm{Aut}(G) \cong \mathbb{Z}$.
- There is no G such that $\mathrm{Aut}(G) \cong \mathbb{Z}_n$ for odd n.
- This is the weirdest one of all. $\mathrm{Out}(S_n) \cong \{e\}$ if $n \neq 6$, and $\mathrm{Out}(S_6) \cong \mathbb{Z}_2$.

14 Group Actions

So far in the course, we have been abstracting things left, right, and center, and reaping the rewards! However, there are many more rewards to be reaped by taking a group, and having it act (whatever that means) on a concrete set. Properties of this action can tell us imporant things about the group.

Timothy Gowers has an excellent series of blog posts on this subject (the first of four is at https://gowers.wordpress.com/2011/11/06/group-actions-i/), and these are a large influence on the way I present the material.

As usual, before defining a group action, let's take a look at some examples.

Example. The group D_5 acts on the vertices of a pentagon. Each element of D_5 can be viewed as a bijection from the set of vertices of a pentagon to the set of vertices of a pentagon. If we let X be the set of vertices of a pentagon, and S_X the group of bijections from X to itself, then D_5 can be viewed as a subgroup of S_X.

An interesting point of view on this group is that it is an abstract algebraic structure, and it becomes concrete when we view it acting on the set of vertices of a pentagon. Note that the identity always fixes every vertex.

Example. The Rubik's cube group acts on the states of a Rubik's cube. For example, let U be the group element that corresponds to rotating the top face 90 degrees clockwise. Then given any state of the cube, U changes it to a new one by rotating the top face 90 degrees clockwise. With this in mind, it is not difficult to see that each element of the group is a bijection from the set of states of a cube to itself (or we can say it permutes the set of states of a cube). Notice again that the identity element in the group corresponds to the identity permutation.

Example. The group $GL_2(\mathbb{R})$ acts on vectors in $\mathbb{R}^2$ in the usual way from linear algebra. Given $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ and $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$, the matrix sends this vector to $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$.

Each element of $\mathrm{GL}_2(\mathbb{R})$ induces a permutation on $\mathbb{R}^2$. It is a permutation (or a bijection) because every matrix in $\mathrm{GL}_2(\mathbb{R})$ is invertible.

Lecture 25 - 04/07

Example. Let G be the group of rotational symmetries of a regular tetrahedron, defined in much the same way as the dihedral group is defined as the set of symmetries of a regular n-gon. Then it is not hard to see that every element of G permutes the 4 vertices. Furthermore the identity fixes every vertex, and it is the only element that does so. When the identity is the only element that fixes the set a group is acting on, we say the action is faithful.

G also acts on the three lines that join the midpoints of opposite edges. In this case, if we rotate the tetrahedron by π around one of these lines, all three of them are sent back to themselves! Here we have an example of an action that is not faithful, and it tells us that G is not a simple group (we will see why later).

Example. The group S_n acts on the set $\{1, \ldots, n\}$ in the obvious way. Each element is a bijection (and isn't simply associated to a bijection) from the set $\{1, \ldots, n\}$ to itself.

Example. Every group acts on itself. For example, consider $\mathbb{Z}_2 \times \mathbb{Z}_2$. For $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, consider $f_a : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ given by $f_a(g) = ag$. Since left multiplication is a bijection, each $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$ corresponds to a bijection from the set of elements to itself.

If we let X be the set of elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and S_X the group of permutations, then by sending a to f_a, we have a homomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_2$ to S_X. Furthermore, the homomorphism is injective since the only element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ that maps to the trivial permutation is e. Since $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, $S_X \cong S_4$. This argument shows us that there is a subgroup of S_4 isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Notice that nothing I said here was special to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and could just as well be applied to any other group.

All of the examples above have the following in common. They all allocate elements of a group to permutations of some set. In order to move forward, let's make some definitions.

Definition. Let X be a set and define S_X to be the group of permutations of X. That is, the elements are bijections from X to itself, and the operation is composition.

Exercise. Show that if $|X| = n$, then $S_X \cong S_n$.

Let's now define a group action.

Definition. Let G be a group and X a set. We say G **acts on** X, and write $G \curvearrowright X$, if there is a function

$$\cdot : G \times X \longrightarrow X$$

such that $e \cdot x = x$ for all $x \in X$ and $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$.

One way to think about a group action is to view each element of the group as a function from the set X to itself. In fact, we can define the function

$$\begin{aligned} \psi_g : X &\longrightarrow X \\ x &\longmapsto g \cdot x \end{aligned}$$

for each $g \in G$.

Exercise. Suppose $G \curvearrowright X$, and define $\psi_g : X \to X$ by $x \mapsto g \cdot x$. Prove that ψ_g is a bijection.

It is nice to have a formal definition of a group action, but it is even nicer to have two! Here is another way of thinking about a group action.

Lecture 26 - 07/07

Proposition 56. *Every group action of G on a set X induces a homomorphism $\phi : G \to S_X$. Conversely, every homomorphism $\phi : G \to S_X$ comes from a group action $G \curvearrowright X$.*

Proof. Suppose $G \curvearrowright X$ for some set X. Define a map

$$\begin{aligned} \phi : G &\longrightarrow S_X \\ g &\longmapsto \psi_g \end{aligned}$$

where $\psi_g(x) = g \cdot x$. We showed above that ψ_g is a permutation of X for all $g \in G$, so this map is well defined. To see it is a homomorphism, first note $\psi_g\psi_h(x) = g \cdot (h \cdot x) = (gh) \cdot x = \psi_{gh}(x)$, so $\psi_g\psi_h = \psi_{gh}$. We then have

$$\phi(gh) = \psi_{gh} = \psi_g\psi_h = \phi(g)\phi(h).$$

Conversely, suppose $\phi : G \to S_X$ is a homomorphism. Then define an action $G \curvearrowright X$ by $g \cdot x := \phi(g)(x)$. Notice $e \cdot x = \phi(e)(x) = \mathrm{id}_X(x) = x$ and $(gh) \cdot x = \phi(gh)(x) = \phi(g)\phi(h)(x) = g \cdot (h \cdot x)$ so $g \cdot x$ is a group action. ∎

Because of this proposition we can either think of a group action as a map $G \times X \to X$ or as a homomorphism $\phi : G \to S_X$. Either one works so whichever point of view is the most useful at the time should be the one you use.

Notice that this proposition really drives home the idea that a group action is simply an allocation of a permutation of X to each group element, in a way that the structure of the group is preserved.

Let's now use this idea to prove Cayley's theorem.

Theorem 57 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a symmetric group.*

Proof. Let G be a group and consider the set X to be the group G itself. Define a group action by left multiplication, that is $g \cdot x := gx$. Remember, elements of x are group elements so the product gx makes sense.

Note that $e \cdot x = x$ and $g \cdot (h \cdot x) = g \cdot (hx) = (gh)x = (gh) \cdot x$ so this is indeed a group action. Let $\phi : G \to S_X$ be the associated homomorphism.

Since $g \cdot x = x$ only when $g = e$, we see that $\ker(\phi) = \{e\}$ so ϕ is injective. If we consider ϕ as a homomorphism $\phi : G \to \mathrm{im}(\phi)$, then ϕ is injective and surjective so $G \cong \mathrm{im}(\phi)$. However, $\mathrm{im}(\phi)$ is a subgroup of S_X, completing the proof. ∎

Corollary 58. *If $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Proof. In the proof of Cayley's theorem, number the elements of X from 1 to n. Since $S_X \cong S_n$, the result follows. ∎

This theorem adds weight to everyone's favourite description of group theory as the study of symmetry. It also highlights the importance of the groups S_n, because they contain copies of every finite group.

14.1 The Orbit-Stabiliser Theorem

The orbit-stabiliser theorem pervades a surprisingly large proportion of mathematics. It is relatively simple to state once you have the language of group actions, and is extremely powerful. As we will see, Lagrange's theorem (which we will reprove as a quick corollary to the orbit-stabiliser theorem), Cauchy's theorem, and the class equation will all follow from this theorem. The theorem also gives us tools to count various things related to groups acting on sets.

This might make the orbit-stabiliser theorem seem like a deep and complicated theorem, but even though you don't know it, you already understand what this theorem says! Let's look at a nice example.

Let G be the group of rotational symmetries of the cube. Let's try to figure out what $|G|$ is. We will do this in a few different ways.

1. Pick a face on the cube. This face can end up at any of 6 faces. Once you have fixed which face it ends up at, you have 4 choices for where a face adjacent to it ends up at. Once these two choices have been fixed, we have determined an element of G. Therefore $|G| = 6 \times 4 = 24$.

2. Pick an edge. There are 12 edges it could get sent to, and 2 ways to rotate the cube so that the edge ends up at a selected edge. Therefore $|G| = 12 \times 2 = 24$.

3. Pick a corner. There are 8 corners this particular corner could get sent to, and 3 choices for an adjacent corner. Once you fixe two corners, you fix the entire cube. Therefore $|G| = 8 \times 3 = 24$.

4. Pick half an edge, the part joining the center of an edge to a vertex. There are 24 half edges that particular one can go to via a rotation of the cube. Once a destination has been chosen, the rotation of the cube has been determined. Therefore $|G| = 24$.

Each of these is a particular case of the orbit-stabiliser theorem applied to various actions of G. The first arises from G acting on the set of faces, the second from G acting on the set of edges, the third from G acting on the corners, and the fourth from G acting on the half-edges.

Each argument above went as follows. Pick an element from the set being acted on. Compute how many places it can get to (the size of its orbit). Compute how many elements of G keep it where it is (the size of its stabiliser). Multiply these two quantities together, and you get the size of the group. This is essentially the statement of the orbit-stabiliser theorem.

In order to state this theorem formally and harness its power, we must first make some formal definitions.

Definition. Let G act on a set X. For any $x \in X$, define the **orbit** of x by

$$G \cdot x := \{g \cdot x : g \in G\}.$$

Define the **stabiliser** of x by

$$G_x := \{g \in G : g \cdot x = x\}.$$

Intuitively, the orbit of an element x is the set of all the things in X that x can get to under the action. The stabiliser of an element is the set of all things in G that keep x where it is. It is important to remember that the orbit is a subset of X, and the stabiliser is a subset of G.

By now, it shouldn't be a surprise that the next proposition is coming.

Proposition 59. *Let G act on a set X. For any $x \in X$, the stabiliser G_x is a subgroup of G.*

Proof. This is an exercise. ■

Let's quickly illustrate these definitions with an example.

Example. Consider the group $G = S_4$ acting on the set $X = \{1, 2, 3, 4\}$ is the usual way. Consider $4 \in X$. Then $G \cdot 4 = \{1, 2, 3, 4\}$ since for any $a \in X$, the transposition $(4\,a)$ takes 4 to a, so $(4\,a) \cdot 4 = a$.

The stabiliser G_4 is the set of all permutations $\sigma \in S_4$ such that $\sigma(4) = 4$. As an exercise, prove that the stabiliser of 4 is isomorphic to the symmetric group on 3 letters, S_3.

Lecture 27 - 09/07

We are now ready to prove the orbit-stabiliser theorem.

Theorem 60 (Orbit-Stabiliser)**.** *Let G be a group acting on a set X. Let $x \in X$. Then $|G : G_x| = |G \cdot x|$. In particular, if G is finite, then $|G| = |G_x|\,|G \cdot x|$.*

Proof. Recall $|G : G_x|$ is the number of left cosets of G_x in G, so if we let $T = \{gG_x : g \in G\}$, then $|T| = |G : G_x|$. To show $|T| = |G| \cdot x$, we will construct a bijection between the two sets.

Define the function

$$\begin{aligned} \Phi : T &\longrightarrow G \cdot x \\ gG_x &\longmapsto g \cdot x. \end{aligned}$$

We will eventually show Φ is a bijection, but we must first show it is well defined. That is, if $gG_x = hG_x$, we must show $g \cdot x = h \cdot x$, so it doesn't matter which group element we use to define the coset in T.

If $gG_x = hG_x$, then $h^{-1}g \in G_x$ so $(h^{-1}g) \cdot x = x$. Both sides of this equation are elements of x, so we can act on both sides by h. Doing this we get

$$h \cdot x = h \cdot ((h^{-1}g) \cdot x) = (hh^{-1}g) \cdot x = g \cdot x$$

so Φ is well defined.

To show Φ is a bijection, we will construct an inverse to Φ. Define the function

$$\begin{aligned} \Psi : G \cdot x &\longrightarrow T \\ g \cdot x &\longmapsto gG_x. \end{aligned}$$

This looks like a great candidate for an inverse of Φ, but again, we must show it is well defined. We might have two different group elements $g, h \in G$ such that $g \cdot x = h \cdot x$. So, we need to show that if $g \cdot x = h \cdot x$, then $gG_x = hG_x$.

If $g \cdot x = h \cdot x$, then by acting on both sides by h^{-1} we get (after a bit of work) $(h^{-1}g) \cdot x = x$ so $h^{-1}g \in G_x$. Therefore $gG_x = hG_x$, so Ψ is well defined.

To see Ψ is an inverse to Φ, notice that

$$\Phi\Psi(g \cdot x) = \Phi(gG_x) = g \cdot x \quad \text{and} \quad \Psi\Phi(gG_x) = \Psi(g \cdot x) = gG_x$$

for all $g \in G$. Therefore $\Phi\Psi = \mathrm{id}_{G \cdot x}$ and $\Psi\Phi = \mathrm{id}_T$ so Φ (and also Ψ) is a bijection. Therefore $|T| = |G \cdot x|$.

Finally, if G is finite we know $|G : G_x| = |G| \,/\, |G_x|$. Therefore $|G \cdot x| = |G| \,/\, |G_x|$ and rearranging gives us $|G| = |G_x|\,|G \cdot x|$. ∎

To get used to what this thoerem says, see if you can reformalise the four arguments above that compute the order of the rotational symmetry group of the cube in the language of orbits and stabilisers.

There are lots of problems and theorems which can be easily solved or proven by making a clever choice of an action of a group, and then applying the orbit-stabiliser theorem. Let's see some of these in action.

Example. Let's compute the size of $G = \mathrm{GL}_2(\mathbb{Z}_3)$. We know that this group acts on the set $\mathbb{Z}_3 \times \mathbb{Z}_3$ by matrix multiplication. Consider the vector $v = (1, 0) \in \mathbb{Z}_3 \times \mathbb{Z}_3$. Then we want

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

which happens when $a = 1$ and $b = 0$. So, to compute $|G_v|$ we must work out how many matrices in $\mathrm{GL}_2(\mathbb{Z}_3)$ are of the form $\begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix}$.

Recall from linear algebra that for a matrix to have non-zero determinant, the columns must be linearly indepedent. If the matrix is a 2×2 matrix, this is the same as saying that one of the columns cannot be a scalar multiple of the other. It turns out that when we're looking at $\mathbb{Z}_p$ for a prime p, the same thing holds, except the scalars we can multiply by are elements of $\mathbb{Z}_p$ (as opposed to $\mathbb{C}$ or $\mathbb{R}$ that we're used to).

So, for the second column, there are three possibilities for the pair (b, d) that would make this matrix not invertible and thus not in $\mathrm{GL}_2(\mathbb{Z}_3)$. They are the scalar multiples of $(1, 0)$, which are $(0, 0)$, $(1, 0)$, and $(2, 0)$. Any other pair of numbers from $\mathbb{Z}_3$ will be fine. This leaves us with $3x3 - 3 = 6$ possibilities. Therefore $|G_v| = 6$.

As for the orbit of v, for any vector $(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, we have

$$\begin{bmatrix} x & a \\ y & b \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}.$$

So, to work out which elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are in the orbit of $(1, 0)$, we must decide which matrices of the form above are in $\mathrm{GL}_2(\mathbb{Z}_3)$.

First notice that if $x = 0$ and $y = 0$, then the matrix is never invertible, so $(0, 0)$ is not in $G \cdot v$. However, for any other (x, y), if (x, y) is not a multiple of $(1, 0)$, then $\begin{bmatrix} x & 1 \\ y & 0 \end{bmatrix} \in GL_2(\mathbb{Z}_3)$ so $(x, y) \in G \cdot x$. If (x, y) is a multiple of $(1, 0)$ other than $(0, 0)$, then it is not a multiple of $(0, 1)$ and $\begin{bmatrix} x & 0 \\ y & 1 \end{bmatrix} \in GL_2(\mathbb{Z}_3)$.

Putting this together, we see that every element of $\mathbb{Z}_3 \times \mathbb{Z}_3$ other than $(0, 0)$ is in the orbit of $v = (1, 0)$. Therefore $|G \cdot v| = 3^2 - 1 = 8$.

Applying the orbit-stabiliser theorem, we see $|GL_2(\mathbb{Z}_3)| = |G_v|\,|G \cdot v| = 6 \times 8 = 48$.

In order to apply the orbit stabiliser to some other situations, we first need to work out how the set of orbits sits inside the set being acted on.

Let's take a look at some examples. In the example above with $\mathrm{GL}_2(\mathbb{Z}_3) \curvearrowright \mathbb{Z}_3 \times \mathbb{Z}_3$, there are two orbits. These orbits are $\{(0, 0)\}$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 \setminus \{(0, 0)\}$. It is an exercise to check this.

Let $\mathbb{Z}_2$ act on the set $\{1, 2, 3, 4, 5, 6\}$ where the action is given by the homomorphism $\phi : \mathbb{Z}_2 \to S_6$

where $\phi(1) = (12)(34)$. Then the orbits are

$$G \cdot x = \begin{cases} \{1,2\} & \text{if } x = 1,2 \\ \{3,4\} & \text{if } x = 3,4 \\ \{5\} & \text{if } x = 5 \\ \{6\} & \text{if } x = 6. \end{cases}$$

Notice that in both of these examples, all the orbits are disjoint and they cover the whole group. Another way of saying this is that the set of orbits partition the set X. This should be reminiscent of what happened with cosets of a subgroup partitioning the group. Let's prove that this happens in general.

In this proposition, we will be using the language of partitions and equivalence relations. For those who haven't seen this before, appendix III at the end of these notes deals with this.

Proposition 61. *Let G act on a set X. Then the set of subsets $\{G \cdot x : x \in X\}$ partitions the set X.*

Lecture 28 - 11/07

Proof. We will prove this by showing that being in the same orbit is an equivalence relation on X. The result will then follow since equivalence classes will correspond to orbits, and equivalence classes on a set partition the set (see Appendix C for an explanation of this).

Define the relation $\sim$ on X by $x \sim y$ if there exists $g \in G$ such that $g \cdot x = y$. We see $e \cdot x = x$ so $x \sim x$.

If $g \cdot x = y$ then $x = g^{-1} \cdot y$ so $x \sim y$ implies $y \sim x$.

Finally, if $g \cdot x = y$ and $h \cdot y = z$, then $(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z$. Therefore if $x \sim y$ and $y \sim z$ then $x \sim z$ and $\sim$ is an equivalence relation on X.

Observe that

$$[x] = \{y \in X : y \sim x\} = \{y \in X : y = g \cdot x \text{ for some } g \in G\} = G \cdot x.$$

Since equivalence classes partition a set the proof is complete. ■

The next theorem has one of the nicest and slickest proofs you are likely to see in your travels. It is the perfect demonstration of how a clever choice of group action can prove great things about a group. There is another standard proof of this theorem, but we will not talk about it here.

Theorem 62 (Cauchy's Theorem)**.** *Let G be a finite group and let p be a prime dividing the size of the group. Then there is an element $g \in G$ such that $|g| = p$.*

Proof. Consider the set $X = \{(g_1, g_2, \ldots, g_p) \in G \times \cdots \times G : g_1 g_2 \cdots g_p = e\}$. Note that each element in G is determined by its first $p-1$ entries, since $g_p = (g_1 \cdots g_{p-1})^{-1}$. Therefore $|X| = |G|^{p-1}$ and in particular, $p \mid |X|$.

Define an action of $\mathbb{Z}_p$ on X by $1 \cdot (g_1, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$. Notice that since $\mathbb{Z}_p = \langle 1 \rangle$, this determines the group action.

To see this is a group action, first note that if $g_1 g_2 \cdots g_p = e$, then

$$g_p g_1 g_2 \cdots g_{p-1} = g_p (g_1 g_2 \cdots g_p) g_p^{-1} = g_p e g_p^{-1} = e.$$

Therefore, if $(g_1, \ldots, g_p) \in X$, then $a \cdot (g_1, \ldots, g_p) \in X$ for any $a \in \mathbb{Z}_p$. As an exercise, show that this is a group action.

The orbit-stabiliser theorem implies that the orbit of any element divides the size of the group, so $|\mathbb{Z}_p \cdot x| = 1$ or p for any $x \in X$. Since the orbits partition X and p divides $|X|$, either all the orbits must have size p or there are a multiple of p orbits of size 1.

Observe that $(e, \cdots, e) \in X$ has an orbit of size 1, so there are $p-1$ other elements of X with orbit size 1. Also observe the only way that $(g_1, \ldots, g_p) \in X$ can have an orbit of size 1 is if $g_1 = g_2 = \cdots = g_p$.

Therefore there are $p-1$ tuples of the form $(g, \ldots, g) \in X$ where $g \neq e$. Therefore there are $p-1$ non-identity elements $g \in G$ such that $g^p = e$. We know that $g^p = e$ if and only if $|g| \mid p$, but since p is prime, $|g| = 1$ or p. Since $g \neq e$, $|g| = p$, completing the proof. ■

Corollary 63 (Assignment 1 bonus)**.** *Suppose G is an abelian group of order pq for distinct primes p and q. Then G is cyclic.*

Proof. Cauchy's theorem tells us there exist elements $g, h \in G$ such that $|g| = p$ and $|h| = q$. Since G is abelian, g and h commute. Since if g and h commute and $\gcd(|h|, |g|) = \gcd(p, q) = 1$, we have $|gh| = |g|\,|h| = pq$ (this is an exercise). This tells us $G = \langle gh \rangle$, completing the proof. ■

Lecture 29- 14/07

14.2 Groups acting on themselves

It should be starting to become apparent that we can learn lots about a group by studying its actions. By making a clever choice about the set it acts on, we can learn even more. One choice that can be made for the set being acted upon is the group itself, or subgroups of the group, or subsets, or something else that naturally comes from the group itself.

Here is an exercise to get your hands dirty with orbit-stabiliser and reprove Lagrange's theorem. Let G be a finite group, and let X be the set of all subsets of G with k elements. Let G act on X by left multiplication, which is an action since left multiplication is a bijection so subsets of size k must be taken to subsets of size k. Let $T \in X$, so T is a subset of G with $|T| = k$. Prove that if T is a subgroup, then $G_T = T$, and use orbit-stabiliser to conclude that if T is a subgroup, then $|T| \,\big|\, |G|$.

Here are some natural actions that a group can have on itself. These are by no means exhaustive, but are just here to give some examples.

Let G be a group, set $X = G$. Here are three actions $G \curvearrowright X$.

Left Multiplication. Define the action by $g \cdot x = gx$. We have seen this action in action a few times already, most notably in the proof of Cayley's theorem. Note that the corresponding homomorphism $\phi : G \to S_X$ is injective. Another way of saying this is that the only group element g such that $g \cdot x = x$ for all $x \in X$ is the identity. As an exercise, prove that this action is indeed a group action.

Right Multiplication. This is much the same, except we have to be careful with the actual definition. If we define $g \cdot x := xg$, then we run into trouble when trying to prove this is a group action. In particular we see $(gh) \cdot x = xgh$ whereas $g \cdot (h \cdot x) = xhg$. To overcome this, define $g \cdot x := xg^{-1}$, and as an exercise, prove that this is a group action. As with left multiplication above, this action also has the property that the corresponding homomorphism to S_X is injective.

Conjugation. Define $g \cdot x := gxg^{-1}$. This action is different in a couple of ways from the previous two. First, it is not always the case that the corresponding homomorphism $\phi : G \to S_X$ is injective. Second, this action doesn't forget that X is a group and it acts by automorphisms. What I mean when I say this is that every element of g doesn't just act as any old permutation on X, but by an automorphism. This turns out to be very useful.

Let's take a look at an example.

Example. Let $G = S_3$ and $X = S_3$. Consider the following situations where G acts on X.

Left Multiplication.
Notice that for any $\tau \in S_3$, $\tau \cdot (1) = \tau$ and therefore $\tau \in G \cdot (1)$. We can then conclude that $G \cdot (1) = X$. Since the orbits partition X, this is the only orbit so $G \cdot \sigma = X$ for all $\sigma \in X$. Furthermore, the orbit-stabiliser theorem tells us that $|G_\sigma| = 1$ for all $\sigma \in X$, so $G_\sigma = \{e\}$.

Let's contrast this with the action that comes from conjugation.

Conjugation.
Let's begin by investigating what $G \cdot (1\,2)$ and $G_{(1\,2)}$ are. We have

$$\begin{aligned}
(1) \cdot (12) &= (12) \\
(12) \cdot (12) &= (12)(12)(12)^{-1} = (12) \\
(13) \cdot (12) &= (13)(12)(13)^{-1} = (23) \\
(23) \cdot (12) &= (23)(12)(23)^{-1} = (13) \\
(123) \cdot (12) &= (123)(12)(123)^{-1} = (23) \\
(132) \cdot (12) &= (132)(12)(132)^{-1} = (13).
\end{aligned}$$

From this we can see that $G \cdot (1\,2) = \{(1\,2), (1\,3), (2\,3)\}$ and $G_{(1\,2)} = \{(1), (1\,2)\}$. Continuing in this way we get the following data.

$x \in X$	$G \cdot x$	G_x
(1)	$\{(1)\}$	S_3
(12)	$\{(12), (13), (23)\}$	$\{(1), (12)\}$
(13)	$\{(12), (13), (23)\}$	$\{(1), (13)\}$
(23)	$\{(12), (13), (23)\}$	$\{(1), (23)\}$
(123)	$\{(123), (132)\}$	$\{(1), (123), (132)\}$
(132)	$\{(123), (132)\}$	$\{(1), (123), (132)\}$.

Let's take a moment to observe that the orbits do indeed partition X into $G \cdot (1), G \cdot (12)$, and $G \cdot (123)$. Furthemore in each row, $|G \cdot x|\,|G_x| = |S_3| = 6$, verifying the orbit-stabiliser theorem. It is also worth pointing out that just because two elements have the same orbit, does not mean they have the same stabiliser.

As an exercise, repeat the example above for $\mathcal{Q}_8$, or any other non-abelian group (abelian groups are boring in this example. If you don't immediately see why, run through the example above with $\mathbb{Z}_2 \times \mathbb{Z}_2$).

Groups acting on themselves by conjugation are important enough that the orbits and stabilisers have their own names.

Definition. Let G act on itself by conjugation. For $g \in G$ define the **conjugacy class** of g, denoted $K(g)$, by the orbit $G \cdot g$. Define the **centraliser** of g, denoted $Z(g)$ by the stabiliser G_g.

Notice that I could have defined these two things without talking about group actions. They would be

$$K(g) := \{aga^{-1} : a \in G\}$$
$$Z(g) := \{a \in G : ag = ga\}.$$

Written this way, it's a little clearer as to why the conjugacy class and centraliser have these names. Intuitively, we think of the centraliser of an element as all the stuff that commutes with that particular element. Similarly we think of the conjugacy class of an element as the set of all conjugates of that element.

Exercise. Here are some exercises to legitimise the name "centraliser".

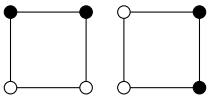
- Prove that $Z(G) = \bigcap_{g \in G} Z(g)$ (here $Z(G)$ is the center of the group G).
- Prove that $C(g)$ is the largest subgroup $H < G$ so that $g \in Z(H)$. That is, prove that if there is a subgroup $K < G$ such that $g \in Z(K)$, then $K < H$.

14.3 Counting Problems - The lemma that is not Burnside's

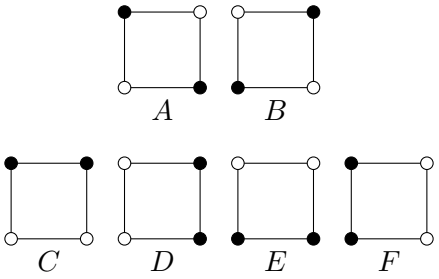
We now turn our attention to applying group actions to combinatorial problems which have a certain amount of symmetry.

Suppose we want to count how many different ways we can colour the vertices of a square, where two vertices have to be black and two have to be white. At first glance, the answer should be the same as the number of ways to pick two objects out of a collection of four, or $\binom{4}{2} = 6$. This is because we can choose two of the vertices and colour those black, and colour the other two white.

This is all well and good, but let's say we wanted to consider the next two colourings the same, because I can rotate one into the other.



We can now ask how many different ways there are to colour the vertices of a square, where two colourings are considered the same if we can rotate one to the other? If you play around for a little while, you will see the answer is two, and they are given by the two rows below. Here are all six possible colourings, grouped into rows which correspond to colourings which are obtained from one another by rotations of the square.



If you're observant, you will realise that this discussion has taken place in the chapter on group actions. The subgroup of rotations $H = \{e, r_1, r_2, r_3\} < D_4$ is acting on the set of all possible colourings, and we are interested in the number of orbits.

Lecture 30 - 16/07

This raises an interesting question: How can we count the number of orbits from a group action? If we can find a nice way to do this, then we can answer all sorts of combinatorial problems like the one above. Since we are doing combinatorics, we are typically counting things, so let's keep all groups and sets finite.

Say we have a finite group G acting on a finite set X, and we want to count the number of orbits N. Here is one way we could do it. We could overcount and then adjust.

To illustrate this, label the colourings of the vertices of the square above A, B, C, D, E, F as in the image above. Let the group be $H = \{e, r_1, r_2, r_3\}$ and $X = \{A, B, C, D, E, F\}$. Although there are 6 colourings, it feels like we should count A and B twice, because $r_2 \cdot A = A$ and $r_2 \cdot B = B$.

More precisely, we should keep track of the size of the stabiliser of each element of the set X. If we do that, then we can divide by the size of the group and get the number of orbits. Applying this to our example we get

$$N = \frac{|H_A| + |H_B| + |H_C| + |H_D| + |H_E| + |H_F|}{|H|} = \frac{2+2+1+1+1+1}{4} = 2.$$

Excellent, this gives us the correct anwer!

Although this is promising, it can get tedious and difficult to compute the stabilisers of each element of the set X. For example, if we were to count the number of ways to colour the vertices of an octagon with three colours and no restriciton on how many vertices had to be a certain colour, the set X we would be dealing with would have size $3^8 = 6561$. Far too many elements to compute the stabilisers of in any reasonable way.

All hope is not lost, there is another way to do it. In the situation just mentioned with the octagon, although the size of X is huge, the size of the group acting on X is eight (or sixteen if you want to allow flips as well as rotations). This is a much more reasonable number!

The idea is to run through each group element and count the number of elements that are fixed by each group element. Intuitively, if we add up all of these numbers we should get the same number as the sum of the sizes of the stabilisers. Let's make the following definition.

Definition. Let G act on a set X. For $g \in G$, define the **fixed set of** g as

$$X^g := \{x \in X : g \cdot x = x\}.$$

In our example with the square, the identity fixes everything so $X^e = \{A, B, C, D, E, F\}$. Nothing is fixed by r_1 and r_3, so $X^{r_1} = X^{r_3} = \emptyset$. Finally, $X^{r_2} = \{A, B\}$ since a rotation by 180 degrees takes A to A and B to B. Then

$$|X^e| + |X^{r_1}| + |X^{r_2}| + |X^{r_3}| = 4 + 0 + 2 + 0 = 8$$

which is the same as the sum of the sizes of the stabilisers of all the elements of X.

This strategy is exactly the statement of what is called *Burnside's lemma*, or *Burnside's theorem*, or *the lemma that is not Burnside's*. It is sometimes called the latter because it appears that Burnside was not the first one to state and prove it. It was stated and proved in a book by William Burnside in 1897, where he attributed it to Frobenius in 1887. However, it appears that Cauchy had already done it in 1845.

It is kind of strange (and unfortunate for Burnside) that this lemma in particular is known by such a name. There are undoubtedly many more cases of lemmas and theorems in mathematics being attributed to people who didn't prove them. However, Burnside has his fair share of lemmas and theorems, so I don't feel too guilty using this name.

Lecture 31 - 18/07

Lemma 64 (The Lemma that is not Burnside's)**.** *Let G be a finite group acting on a finite set X, and let N be the number of orbits. Then*

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g| .$$

Proof. Consider the set $T = \{(g, x) \in G \times X : g \cdot x = x\}$. We will count $|T|$ in two different ways.

First notice that if we fix a $g \in G$, then the number of pairs $(g, x) \in T$ is exactly $|X^g|$. Therefore $|T| = \sum_{g \in G} |X^g|$.

Second, notice that if we fix a $x \in X$, then the number of pairs $(g, x) \in T$ is exactly the stabiliser G_x and $|T| = \sum_{x \in X} |G_x|$.

The orbit-stabiliser theorem says $|G_x| = |G| / |G \cdot x|$, so we have

$$|T| = |G| \sum_{x \in X} \frac{1}{|G \cdot x|}.$$

It remains to show that $\sum_{x \in X} \frac{1}{|G \cdot x|}$ is precisely the number of orbits.

We know from an exercise that if $y \in G \cdot x$, then $G \cdot y = G \cdot x$. Therefore for a particular orbit $G \cdot y$ we have

$$\sum_{x \in G \cdot y} \frac{1}{|G \cdot x|} = \underbrace{\frac{1}{|G \cdot y|} + \cdots + \frac{1}{|G \cdot y|}}_{|G \cdot y| - \text{times}} = \frac{|G \cdot y|}{|G \cdot y|} = 1.$$

Call the N orbits $G \cdot y_1, \ldots, G \cdot y_N$. Since the orbits partition the set X we have

$$\sum_{x \in X} \frac{1}{|G \cdot x|} = \sum_{x \in G \cdot y_1} \frac{1}{|G \cdot x|} + \cdots + \sum_{x \in G \cdot y_N} \frac{1}{|G \cdot x|} = \underbrace{1 + \cdots + 1}_{N - \text{times}} = N.$$

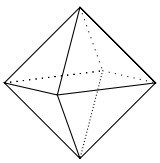
Putting all of this together we have

$$|T| = N\,|G| = \sum_{g \in G} |X^g|$$

and rearranging the second equality completes the proof. ∎

Let's now apply this to a bunch of counting problems.

Example. How many ways can we number an eight-sided die? In order to answer this, we will first assume that an eight-sided die is an octahedron with each face being numbered uniquely with a number from 1 to 8. An octahedron is one of the five platonic solids. It has eight faces (each is an equilateral triangle), twelve edges, and six vertices. Here is a picture of one.



There are 8! ways to number the faces from 1 to 8, however should consider two numberings to be the same if you can get one from the other by a rotation of the die.

Let G be the group of rotational symmetries of the octahedron. We know G acts on the set of vertices V. Pick a vertex $v \in V$. Since any vertex can be rotated to be any other vertex, $|G \cdot v| = 6$. If we want to fix a vertex, there are four rotations that are possible so $|G_v| = 4$. The orbit-stabiliser theorem then tells us that $|G| = 6 \times 4 = 24$.

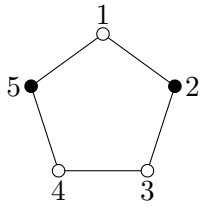
Let G act on the set X of 8! numberings. The number of numberings of an eight-sided die is exactly the number of orbits in this action.

The fixed set of the identity is everything, so $|X^e| = 8!$. For an element $g \neq e$ in G, at least one face is moved, and since each face is numbered distinctly, there are no elements in X^g. Applying Burnside's lemma we have

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{24} |X^e| = \frac{8!}{24} = 1680.$$

Therefore there are 1680 different ways to number an eight-sided die.

Example. How many necklaces can be made with five beads, using only black and white beads? If we abstract away the messy parts of jewelry making, we can assume that the string of a necklace is a pentagon, and the beads are the vertices. Here is a picture of one such necklace.



Since you can push beads around the string, and you can take a necklace off and put it back on from the other side, we will consider two necklaces to be the same if there is a rotation or flip of the pentagon that takes one to the other.

The question now becomes how many ways can you colour the vertices of a pentagon, if each vertex must be black or white, and we consider two colourings the same if there is an element of D_5 that takes one colouring to another. Let's use burnside where $G = D_5$ acts on the set of colourings of vertices of a pentagon.

The fixed set of the identity is the set of all possible colourings, and there are 2^5 such colourings (for each vertex we can choose if it is black or white, and there are 5 vertices). Therefore $|X^e| = 2^5$.

Let's consider $r_1 \in D_5$, a rotation by $\frac{2\pi}{5}$ clockwise. If we number the vertices $1, 2, 3, 4, 5$ in as in the image above, then for a colouring to be in X^{r_1}, the colour of vertex 1 must be the same as the colour of vertex 2. This is because under r_1, vertex 1 gets sent to vertex 2. Similarly, vertex 2 must be the same colour as 3, which must be the same colour as 4, which must be the same colour as 5. There are only two such colourings, all vertices are white and all vertices are black. Therefore $|X^{r_1}| = 2$. You can make similar arguments for all the rotations and we find

$$|X^{r_1}| = |X^{r_2}| = |X^{r_3}| = |X^{r_4}| = 2.$$

Each flip in D_5 fixes a vertex. Let f_i be the flip that fixes vertex i and consider f_1. For a colouring to be in X^{f_1}, vertex 2 must be the same colour as vertex 5, and vertex 3 and 4 must be coloured the

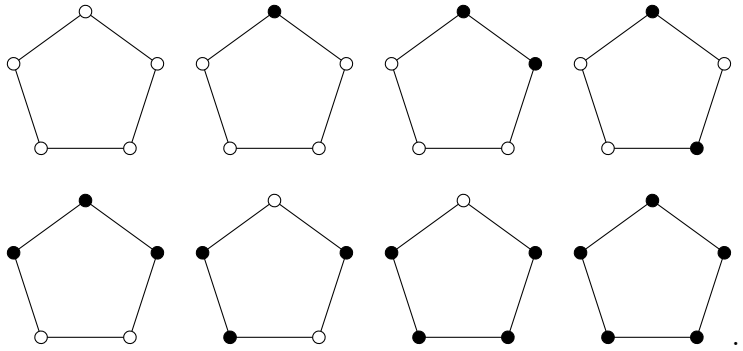
same. Therefore there are 2^3 colourings that stay fixed under f_1. We can make similar arguments for all the f_i and we get

$$\left|X^{f_1}\right| = \left|X^{f_2}\right| = \left|X^{f_3}\right| = \left|X^{f_4}\right| = \left|X^{f_5}\right| = 8.$$

Using Burnside's lemma we have

$$N = \frac{1}{|D_5|}\sum_{g\in D_5}|X^g| = \frac{1}{10}(2^5 + 4\times 2 + 5\times 8) = 8.$$

Therefore there are 8 possible necklaces to be made! If you're bored on a crafternoon, get yourself some black and white beads and make all 8 of them. Here is what the 8 necklaces will look like.



Lecture 32 - 12/07

15 Platonic Solids and Rotational Symmetries in Three-Dimensional Space

15.1 Platonic Solids

A platonic solid is a polyhedron whose faces are all the same regular polygon, and have the property that the same number of faces meet at each vertex. Curiously, there are only five platonic solids: The tetrahedron, cube, octahedron, dodecahedron, and icosahedron. These are illustrated in Figure 1 below.

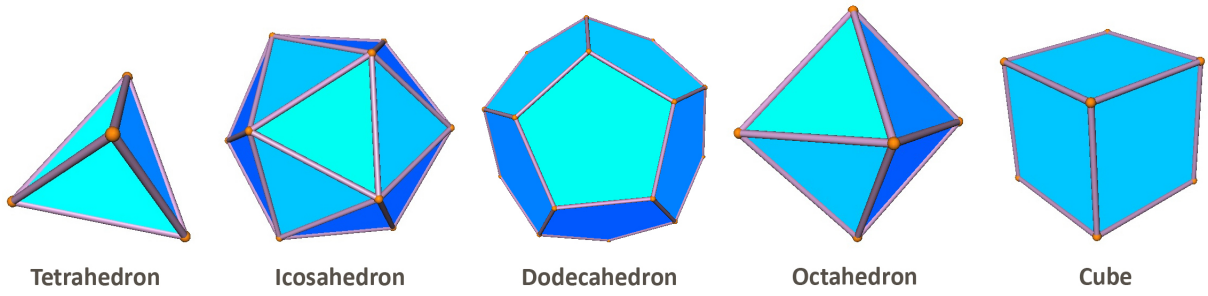


Figure 1: The Platonic solids, courtesy of www.ma.utexas.edu

For each platonic solid, let V be the number of vertices, E the number of edges and F the number of faces. The following table summarises this data for each of the platonic solids.

Platonic solid	Face	V	E	F
Tetrahedron	Triangle	4	6	4
Icosahedron	Triangle	12	30	20
Dodecahedron	Pentagon	20	30	12
Octahedron	Triangle	6	12	8
Cube	Square	8	12	6

The fact that there are only five is the source of a magnificent amount of psuedoscience today. Regardless, this fact is kind of strange. It relies on something that is hinted at in the table above. If you stare at it for long enough, you notice that $V - E + F = 2$ for all five of the solids. This is not a coincidence, and is true in a much more general setting than just platonic solids.

Fact 65. *For any polyhedron, let V be the number of vertices, E the number of edges and F the number of faces. Then $V - E + F = 2$.*

Notice that this fact says nothing about the faces of the polyhedron all being the same, or even all being regular polygons, so it is quite an amazing fact. If you're curious as to where it comes from, look up the *Euler characteristic of a sphere.* There is an exercise in the practice problems which leads you through the proof that the five platonic solids listed above are all of them, assuming the fact above.

Another thing to notice about the table above is that the icosahedron and dodecahoderon have the same number of edges, and each has the same number of vertices as the other has faces. The same goes for the octahedron and the cube. Again, this is not a coincidence.

Definition. Given a polyhedron, construct another polyhedron, which we call its **dual**, as follows. Create a vertex for each face of the original polyhedron, and join two vertices by an edge if they correspond to adjacent faces on the origina polyhedron.

A (fortunate) fact of life, is that the dual of a platonic solid is another platonic solid. As an exercise, verify the following table.

Platonic solid	Dual
Tetrahedron	Tetrahedron
Cube	Octahedron
Octahedron	Cube
Dodecahedron	Icosahedron
Icosahedron	Dodecahedron

Notice that the dual of a dual is the original polyhedron! Very convenient.

15.2 Rotational Symmetry Groups of Platonic Solids

The goal now is to study the rotational symmetry groups of the platonic solids. Given a platonic solid, its rotational symmetry group consists of rotational symmetries (rotations which are also symmetries), and the operation is composition.

To illustrate, let's take a look at the cube. Of course, there is the identity which does nothing. Another element of this group arises by taking a rotation of 90 degrees (in either direction) about an axis formed by joining the centres of opposite faces. Notice that such an element has order 4, and its inverse is a 90 degree rotation in the opposite direction.

Since these groups are all defined as symmetries of platonic solids, they come with a whole bunch of natural actions. Our strategy to learn about these groups will be to study their actions.

The first thing we can observe is that each of these groups acts on the set of faces of their corresponding polygon. For example, the rotational symmetry group of a cube acts on the 6 faces as follows. If g is a rotation and x a face, then $g \cdot x$ is the face that x ends up at after the rotation g has been performed. If we write the product gh to mean "perform rotation h and then rotation g" it is not hard to see that this is indeed an action.

This action allows us to use the orbit-stabiliser theorem to deduce the order of each of the groups. We have already seen this before, but in the case of a cube, let the group of rotational symmetries act on the faces, and let x be a face. The size of the orbit of x is 6 since any face can end up at any other face by rotating the cube. The size of the stabiliser of x is 4 since there are 4 rotations that fix a particular face. The orbit-stabiliser theorem then tells us that $|G| = 6 \times 4 = 24$ where G is the rotational symmetry group of the cube.

As an exercise, verify the rest of the following table.

Platonic Solid	$\lvert G\rvert$
Tetrahedron	12
Cube	24
Octahedron	24
Dodecahedron	60
Icosahedron	60

Our next goal is to see if any of these groups are familiar to us, and we will again do this by studying certain actions of these groups. It would be desirable for the action to give us an injective homomorphism into a symmetric group, as we could then look at the image of the homomorphism (which would be a group isomorphic to our original group) and see if we recognise it.

This leads us to the notion of a faithful action.

Definition. An action $G \curvearrowright X$ is called **faithful** if whenever $g \cdot x = x$ for all $x \in X$, $g = e$.

Definition. Let G act on a set X, and let $\phi : G \to S_X$ be the corresponding homomorphism. We say the action is **faithful** if ϕ is injective.

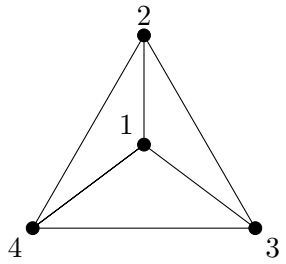
Exercise. Prove that the two definitions of faithful above are equivalent.

Intuitively, a faithful action is one with the property that the only thing that fixes everything in X is the identity.

The Tetrahedron

Let's focus our attention on the rotational symmetry group of the tetrahedron, which we will originally call G. This group has 12 elements, so we won't be able to find a faithful action on a set with 3 elements (since $|S_3| < 12$), but there is hope for a faithful action on a set with 4 elements!

Conveniently, a tetrahedron as 4 vertices, so let's see what we get out of the action of G on X where X is the set of vertices. For convenience, label these 4 vertices $1, 2, 3$, and 4 as in the image below. In this image, imagine vertex 1 is coming out of the page.



We know there are 12 elements in G, so let's try to identify them all and explicitly write down the homomorphism from G to S_4.

There is the identity, which is quite boring. Imagine now sticking a skewer through the tetrahedron, entering at a vertex and exiting through the middle of the opposite face. We can then rotate the tetrahedron 0, 120, or 240 degrees about that skewer in a clockwise direction if looking in the direction of the skewer (so looking at the vertex which is being rotated around). The 0 degree rotation is just the identity which we have already identified, so we ignore that one.

Suppose the skewer enters at vertex i. Then we will call the 120 degree rotation r_i and the 240 degree rotation r_i^2 (since it is obtained by doing r_i twice).

So, to illustrate, r_1 keeps vertex 1 where it is, sends 2 to 3, 3 to 4, and 4 to 2. The rotation r_1^2 sends 2 to 4, 4 to 3, and 3 to 2 while keeping vertex 1 fixed. The rotation r_4 (this requires a bit of imagination) fixes vertex 4 and sends 1 to 3, 3 to 2, and 2 to 1.

So far we have the 9 elements $\{e, r_1, r_1^2, r_2, r_2^2, r_3, r_3^2, r_4, r_4^2\}$, so there are three more.

To find these, consider a skewer that enters the tetrahedron at the midpoint of an edge, and exits it at the midpoint of the edge directly opposite. For example, one such skewer would enter at the midpoint of the edge joining vertices 1 and 2, and exit at the midpoint of the edge joining 3 and 4. In fact, there are 3 such skewers, and we can rotate 180 degrees around each of them, giving us our remaining three elements.

We can name these d_2, d_3, d_4, where d_i is a rotation about the skewer that passes through the edge joning vertices 1 and i. So d_2 sends vertex 1 to 2, 2 to 1, 3 to 4, and 4 to 3, for example.

So we have found all 12 elements of the rotational symmetry group of the tetrahedron, and we have

$$G = \{e, r_1, r_1^2, r_2, r_2^2, r_3, r_3^2, r_4, r_4^2, d_2, d_3, d_4\}.$$

Lecture 33 - 23/07 Now, let $\phi : G \to S_4$ be the homomorphism corresponding to the action of G

on the vertices of the tetrahedron, $\{1, 2, 3, 4\}$. From the discussion above we have

$$\begin{aligned}
\phi(e) &= (1) \\
\phi(r_1) &= (234) \\
\phi(r_1^2) &= (243) \\
\phi(r_2) &= (143) \\
\phi(r_2^2) &= (134) \\
\phi(r_3) &= (124) \\
\phi(r_3^2) &= (142) \\
\phi(r_4) &= (132) \\
\phi(r_4^2) &= (123) \\
\phi(d_2) &= (12)(34) \\
\phi(d_3) &= (13)(24) \\
\phi(d_4) &= (14)(23).
\end{aligned}$$

If you stare at this long enough, you see all the permutations are even and $|\text{im}(\phi)| = 12$ so $\text{im}(\phi) \cong A_4$. Even better, we see ϕ is injective so $G \cong A_4$. Excellent, this proves the following proposition.

Proposition 66. *The rotational symmetry group of a tetrahedron is isomorphic to A_4.*

Knowing that A_4 is isomorphic to the rotational symmetry group of the tetrahedron immediately opens up a world of actions of A_4, which can tell us important things about this group.

For example, we can use this to give a slick proof that A_4 is not simple. Remember that a group is simple if it contains no proper normal subgroups.

Consider the action of A_4 on the set of three lines that join the midpoint of opposite edges of the tetrahedron. We construct the action by first viewing an element of A_4 as a rotational symmetry of a tetrahedron using the isomorphism ϕ. Then the element of A_4 acts on the set of lines in the usual way, by checking where each line gets sent under the corresponding rotation.

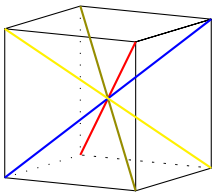
This action gives us a homomorphism $\varphi : A_4 \to S_3$, but it is not faithful. As an exercise, prove that $\ker(\varphi) = \{(1), (12)(34), (13)(24), (14)(23)\}$, and we can conclude that $\ker(\varphi)$ is a proper normal subgroup of A_4. This is nice and slick, and would have made a previous assignment question much easier!

The Cube

Let's shift our focus now to the cube, and let G be the group of rotational symmetries of the cube. We know $|G| = 24$ and our strategy to learn more about it will be to find a faithful action of G on some set X and look at the image of the corresponding homomorphism $\phi : G \to S_X$.

Since G has 24 elements, we cannot have a faithful action on a set of 3 things (because then G would be isomorphic to a subgroup of S_3, which only has 6 things). Ideally, we would find a faithful action on a set with 4 elements. This would give us an injective homomorphism $\phi : G \to S_4$, and since $|G| = 24$ we would be able to conclude $G \cong S_4$. This seems a little hopeful, but let's try anyway.

Let's try to find a set of 4 things that G acts on. One candidate is the set of 4 lines that connects opposite vertices. These lines are denoted below in red, olive, blue and yellow below, and we will denote this set of 4 lines by X.



Any rotation of the cube certainly permutes these 4 lines, so we do have an action of G on X. Let's see whether or not it is faithful.

In order to do this, we must first identify all of the 24 elements of G.

1. There is the identity. This fixes all the elements of X.

2. We can rotate 0, 90, 180, and 270 degrees about an axes that goes through the center of two opposite faces. There are 3 such axes so there are 9 non-identity rotations of this form. No elements of X are fixed by any of these rotations.

3. We can rotate 0, 120, and 240 degrees about each of the lines in X itself. Since there are 4 such lines we can choose, these give us another 8 elements. Each of these rotations fixes the element of X that is the rotation axes, but doesn't fix any of the other three elements.

4. Finally, we can rotate 0 and 180 degrees about an axes that goes through the center of two opposite edges. There are 6 such axes, and each contributes 1 non-identity element. Each of these rotations switches the two elements of X that share a vertex with the edges that are fixed under the rotation, and fixes the other two elements.

These rotations give us 1 identity, 9 rotations fixing opposite vaces, 8 rotations fixing opposite vertices and 6 rotations fixing opposite edges, giving us our 24 elements.

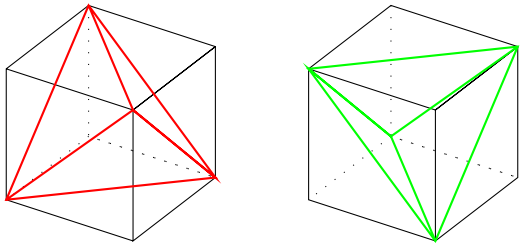
More importantly, the only element $g \in G$ such that $g \cdot x = x$ for all $x \in X$ is $g = e$. Therefore this action is faithful and gives us an injective homomorphism $\phi : G \to S_4$. Since $|G| = |S_4|$, ϕ is infact an isomorphism and we have the following proposition.

Proposition 67. *The rotational symmetry group of a cube is isomorphic to S_4.*

As an exercise, label the elements of X by $\{1, 2, 3, 4\}$, give all 24 elements of G names, and explicitly write down the isomorphism ϕ. Notice that the rotations in item 2 above map to elements of the form $(abcd)$ and $(ab)(cd)$, the rotations in item 3 above map to elements of the form (abc) and the rotations in item 4 map to elements of the form (ab).

So, we now know that the rotational symmetry group of a tetrahedron is isomorphic to A_4, and the rotational symmetry group of a cube is isomorphic to S_4. We know that A_4 is most naturally viewed as a subgroup of S_4, so one might ask if there is a way to view the rotational symmetry group of a tetrahedron as a subgroup of the rotational symmetry group of a cube. There certainly is!

Observe that hidden inside the cube are two tetrahdra as indicated in the picture below.



If we let Y be the set consisting of these two tetrahedra, then G acts on Y, giving us a homomorphism $\phi : G \to S_2$. It turns out that $\ker(\phi) \cong A_4$. So every element of G that fixes both tetrahedra is an even permutation in S_4 (and thus is in A_4 and induces a rotational symmetry of the tetrahedron), and every element of G that switches the two tetrahedra is an odd permutation.

An interesting connection between the cube and $\mathrm{Aut}(\mathcal{Q}_8)$

Before we move on to the next platonic solid, there is an interesting way to view elements of $\mathrm{Aut}(\mathcal{Q}_8)$ that comes from the rotational symmetries of a cube.

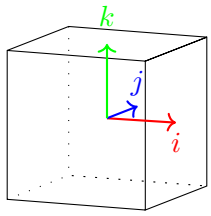
First note that any automorphism $\varphi \in \mathrm{Aut}(\mathcal{Q}_8)$ must have the property that $\varphi(1) = 1$ and $\varphi(-1) = -1$. This is because 1 is the identity and -1 is the only element of order 2. So, in order to define an automorphism of $\mathcal{Q}_8$, it is enough to know what $\varphi(i)$, $\varphi(j)$, and $\varphi(k)$ are. This is because $\varphi(-i) = \varphi(i)^{-1}$ and similarly for j and k.

If you think about what an automorphism can do to i, j, and k, you can convince yourself that $|\mathrm{Aut}(\mathcal{Q}_8)| = 24$. In fact, the following turns out to be true.

Fact 68. $\mathrm{Aut}(\mathcal{Q}_8) \cong S_4$.

If you ever hear on the streets that two groups are isomorphic, your first question should be, "what is the isomorphism?" Here is an excellent way to view the isomorphism, even though we will not prove that it's an isomorphism.

Construct a cube in $\mathbb{R}^3$ with side length 2 and its center at the origin. Orient it so that the coordinate axes pass through the centers of the 6 faces. Let i, j, and k be the vectors $i = (1, 0, 0)$, $j = (0, 1, 0)$, and $k = (0, 0, 1)$.



Any rotation of the cube sends these three coordinate unit vectors to three of $\{i, -i, j, -j, k, -k\}$, and the image of these vectors uniquely determines an element of $\mathrm{Aut}(\mathcal{Q}_8)$. For example, a rotation by 180 degrees about the x-axis fixes i, sends j to $-j$ and k to $-k$. This gives us the automorphism $\varphi \in \mathcal{Q}_8$ given by $\varphi(i) = i$, $\varphi(j) = -j$ and $\varphi(k) = -k$. In this particular example, φ is the inner automorphism given by conjugation by i.

It turns out that this gives us the isomorphism between S_4 and $\mathrm{Aut}(\mathcal{Q}_8)$. Pretty neat hey?

Aside: Generating Sets and the Alternating Group

Our next Platonic solid to look at is the dodecahedron. One of the results we will need in the investigation will be that A_n is the unique index-2 subgroup of S_n. In order to prove this, we will need the notion of a generating set for a group or subgroup. We have already seen this with subgroups generated by single elements, and this notion is a natural generalisation of that.

For example, the set $S = \{(1, 0), (0, 1)\}$ generates the group $\mathbb{Z}_9 \times \mathbb{Z}_9$, because every element $(a, b) \in \mathbb{Z}_9 \times \mathbb{Z}_9$ can be written as

$$(a, b) = \underbrace{(1, 0) \cdots (1, 0)}_{a-\text{times}} \underbrace{(0, 1) \cdots (0, 1)}_{b-\text{times}}.$$

Lecture 34 - 25/07

Definition. Let G be a group and H a subgroup. A **generating set** for H is a subset $S \subset H$ with the property that if any subgroup $K < G$ contains S, then $H < K$. We also say that H is generated by S.

Intuitively a set S generates a group G if once you add everything you need to S to make it a group, you end up with G. Here are some examples of generating sets for groups.

- $\mathbb{Z}$ is generated by $\{1\}$, as well as $\{-1\}$. It is also generated by $\{2, 3\}$.
- S_n is generated by transpositions, since every permutation is a product of transpositions.
- S_n is generated by $\{(12), (1 \cdots n)\}$. This is an exercise.
- D_n is generated by $\{r_1, f\}$ where r_1 is a rotation about $360/n$ degrees and f is any flip.
- $\mathcal{Q}_8$ is generated by $\{i, j\}$. This is also an exercise.
- $\mathbb{Z}_n \times \mathbb{Z}_m$ is generated by $\{(1, 0), (0, 1)\}$.

With this in mind, let's continue with our goal of proving that A_n is the unique index-2 subgroup of S_n.

Lemma 69. *The alternating group A_n is generated by the set of all 3-cycles.*

Proof. Let S be the set of all 3-cycles in S_n, and suppose we have a subgroup $H < S_n$ that contains S. We will show $A_n < H$.

We first prove that every product of two transpositions can be written as a product of 3-cycles. Suppose we have two transpositions that share an entry in common, $(a\,b)$ and $(a\,c)$. Then

$$(a\,b)(a\,c) = (a\,b\,c).$$

Suppose we have two transpositions that do not share an entry in common. Then

$$(a\,b)(c\,d) = (d\,a\,c)(a\,b\,d).$$

Now suppose that we have an element $\sigma \in A_n$. Then since σ is an even permutation,

$$\sigma = (a_1\,b_1)(c_1\,d_1)\cdots(a_k\,b_k)(c_k\,d_k)$$

for $a_i, b_i, c_i, d_i \in \{1, \ldots, n\}$. Then each pair of transpositions $(a_i\,b_i)(c_i\,d_i)$ can be written as a product of 3-cycles, so σ is a product of 3-cycles. Since H is a subgroup, $\sigma \in H$ and $A_n < H$, completing the proof. ■

Lemma 70. *Every index 2 subgroup of S_n contains all the 3-cycles.*

Proof. Let $H < S_n$ be such that $|S_n : H| = 2$, so H is normal.

Since H is normal, $\sigma^{|S_n:H|} = \sigma^2 \in H$ for all $\sigma \in S_n$. For any 3-cycles $(a\,b\,c) \in S_n$, $(a\,b\,c) = (a\,c\,b)^2$ so $(a\,b\,c) \in H$. Thereofore H contains every 3-cycle in S_n, completing the proof. ■

Theorem 71. *The alternating group A_n is the unique index-2 subgroup of S_n.*

Proof. Suppose $H < S_n$ is such that $|S_n : H| = 2$. Then H contains all the 3-cycles in S_n. Since the set of all 3-cycles generates A_n, $A_n < H$. However, $|A_n| = |H| = \frac{1}{2}n!$ so $A_n = H$, completing the proof. ■

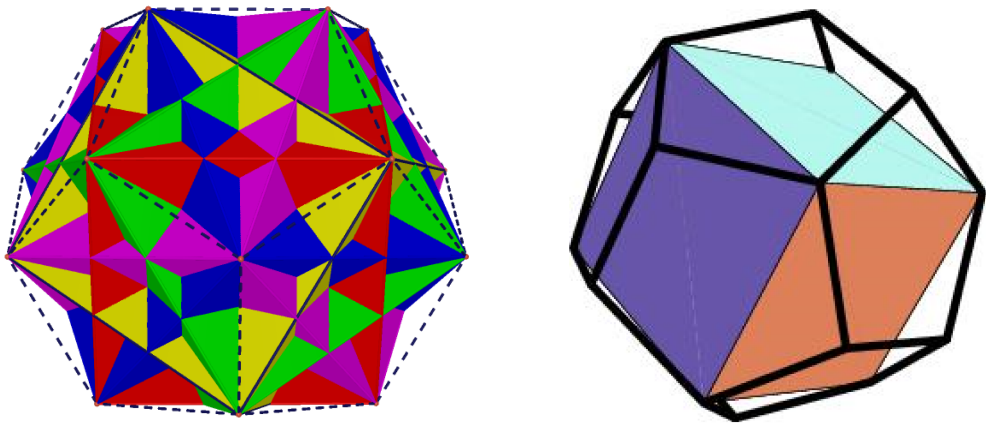


Figure 2: 5 cubes inscribed in a dodecahedron

The Dodecahedron

Let's take the same approach with the dodecahedron. Let G be the group of rotational symmetries of the dodecahedron, and recall that $|G| = 60$. In order for us to have an injective homomorphism $\phi : G \to S_n$, we must have $n \geq 5$. Once again, let's shoot for the best case scenario and find a set X with $|X| = 5$ on which G acts faithfully.

Our candidate set will be 5 inscribed cubes in a dodecahedron, as illustrated in image 2.

Let X be the set of 5 cubes, and let's take a look at the action of G on X. Here are the elements of G and the permutations they induce on X.

1. The identity, e, which fixes every element of X.

2. Consider a skewer passing through the middle of opposite faces. There are 4 non-identity rotations about this skewer, by angles of 72, 144, 216, and 288 degrees. There are 6 pairs of opposite faces, so there are 24 rotations like this. Each rotation doesn't fix any elements of X.

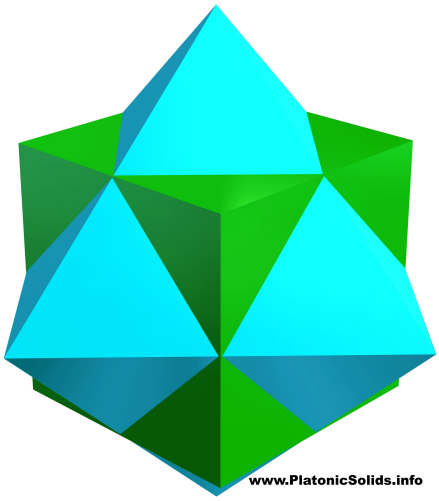
3. Consider a skewer passing through the middle of opposite edges. For each pair of edges, there is 1 non-identity rotation by 180 degrees about the skewer. There are 15 opposite pairs of edges, giving us 15 more elements of G. Each rotation like this fixes exactly one of the elements of X.

4. Finally, consider a skewer passing throught opposite vertices. For each such skewer, there are 2 non-identity rotations by 120 and 240 degrees. There are 10 such pairs of vertices, giving us 20 elements of G. Each of these rotations fixes exactly two elements of X.

These are all 60 elements of G, and we see that the action $G \curvearrowright X$ is faithful. This gives us the following proposition.

Proposition 72. *The rotational symmetry group of the dodecahedron is isomorphic to A_5.*

Proof. There is an injective homomorphism $\phi : G \to S_5$, and since $|G| = 60$, $|\text{im}(\phi)| = 60$. Since $|S_5| = 120$, $|S_5 : \text{im}(\phi)| = 2$. Since A_5 is the only index 2 subgroup of S_5, we must have $\text{im}(\phi) = A_5$ and thus $G \cong A_5$. ■



The Octahedron and Icosahedron

Recall that the octahedron is the dual of the cube, and the icosahedron is the dual of the dodecahedron. Intuitively, any symmetry of the cube (for example) should translate to a symmetry of the octahedron and vice versa, especially if you visualise the octahedron and cube being connected as in the following image. As an exercise, use the fact that the octahedron is the dual of the cube to find a set X with $|X| = 4$ such that the rotational symmetry group of the octahedron acts faithfully on X. Do the same for the icosahedron (except this time $|X| = 5$) and prove the following two propositions.

Proposition 73. *The rotational symmetry group of the octahedron is isomorphic to S_4.*

Proposition 74. *The rotational symmetry group of the icosahedron is isomorphic to A_5.*

Here is a table to summarise what we've found.

Platonic solid	Rotational symmetry group
Tetrahedron	A_4
Cube	S_4
Octahedron	S_4
Dodecahedron	A_5
Icosahedron	A_5

Lecture 35 - 28/07

15.3 Rotational Symmetries in $\mathbb{R}^3$

Now that we have seem some examples of rotational symmetry groups, it might be natural to ask the following question: Which groups arise as rotational symmetry groups of objects in 3-dimensional space?

We have already seen that A_4, S_4, and A_5 can arise, but what about others? For example, what about a circle? Well, we can rotate it x degrees clockwise for any real number x, and we can flip

it around any axes passing through its center. This group is infinite and complicated, so to keep things under control we as the following question.

Which finite groups arise as rotational symmetry groups of objects in 3-dimensional space? Let's formalise this question a little.

Definition. Define the **orthogonal group** and the **special orthogonal group** as the subgroups of $\mathrm{GL}_3(\mathbb{R})$ given by

$$\mathrm{O}(3) = \{A \in \mathrm{GL}_3(\mathbb{R}) : AA^T = I\} \quad \text{and} \quad \mathrm{SO}(3) = \{A \in O(3) : \det(A) = 1\}.$$

Exercise. What is the index of SO(3) in O(3)?

Recall from your first year linear algebra days that if a 3×3 matrix is orthogonal, then it preserves the dot product in $\mathbb{R}^3$. Since the dot product gives a notion of length and angle on $\mathbb{R}^3$, orthogonal matrices are rigid rotations or reflections (or compositions of such things) in $\mathbb{R}^3$. It turns out that every element of SO(3) is a rotation of $\mathbb{R}^3$ about some axis passing through the origin. Because of this, SO(3) can be thought of as the group of rigid rotations of $\mathbb{R}^3$, or even better, the group of rotational symmetries of a sphere.

So, our question now becomes which groups are isomorphic to finite subgroups of SO(3)?

Besides the ones we have already found, we can also see that D_n and $\mathbb{Z}_n$ appear for all $n \geq 2$ as rotational symmetry groups of objects in $\mathbb{R}^3$. For example, D_5 and $\mathbb{Z}_5$ are the rotational symmetry groups of the following two objects respectively.

It is worth noting that D_2 is the rotational symmetry group of a bigon or the following object, for example.

This group has 4 elements: the identity, a rotation about 180 degrees, a vertical flip and a horizontal flip, denoted $D_2 = \{e, r_1, f_1, f_2\}$. As an exercise, prove $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The amazing thing about all of this is that this is it! These are all the finite groups that appear.

Fact 75. *Any finite subgroup of* SO(3) *is isomorphic to one of* $A_4, S_4, A_5, \mathbb{Z}_n$, *or* D_n *for* $n \geq 2$.

So, for example, if an object has a rotational symmetry group of order 45, we know that rotational symmetry group must be isomorphic to $\mathbb{Z}_{45}$.

It is worth noting here that since all cyclic groups of order n are isomorphic, sometimes $\mathbb{Z}_n$ is denoted C_n.

16 Finite Abelian Groups

So far we have seen a bunch of examples of finite abelian groups, but they all seem to have something to do with $\mathbb{Z}$ or $\mathbb{Z}_n$.

For example, it appears that all the abelian groups of order 4 that we've come across so far are isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$. Conversely, we know if G and H are abelian groups, then $G \times H$ is also abelian.

We have already seen some evidence. For example, we know that if p and q are distinct primes, then any abelian group G such that $|G| = pq$ is isomorphic to $\mathbb{Z}_{pq}$.

We also know that some abelian groups can be represented in different ways as direct products of different groups. For example, we know from an assignment question that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$ if and only if $\gcd(n, m) = 1$.

We would like a nice classification of finite abelian groups, and in order to get there, we must first work out when an abelian group G can be written as a direct product $H \times K$ of subgroups.

16.1 Direct Product Decomposition

Let's take a look at a direct product $G \times H$ for some groups G and H. Any direct product like this comes with two proper subgroups (as long as G and H are not the trivial group) for free. These are

$$\overline{G} := \{(g, h) \in G \times H : h = e\} \quad \text{and} \quad \overline{H} := \{(g, h) \in G \times H : g = e\}.$$

In an assignment you showed that $\overline{G}$ and $\overline{H}$ are normal, and it is not difficult to see that $\overline{G} \cap \overline{H} = \{e\}$. It is natural to ask if the converse is true, that is if you have two normal subgroups $H_1, H_2 \triangleleft G$ such that $H_1 \cap H_2 = \{e\}$, is it the case that $G \cong H_1 \times H_2$? The answer is almost, and here is what is true.

Proposition 76. *Let G be a finite group and $H_1, H_2 \triangleleft G$ be normal subgroups. If $H_1 \cap H_2 = \{e\}$ and $|H_1|\,|H_2| = |G|$, then $G \cong H_1 \times H_2$.*

Proof. This is an exercise. ■

We wish to extend this to more than 2 subgroups. In order to do this we must introduce the notation $\langle H_1, \ldots, H_k \rangle$. This indicates the subgroup generated by the subset $H_1 \cup \cdots \cup H_k$. Another way to think of this is as the smallest subgroup of G that contains each of $H_1, \ldots, H_k$. Using the previous proposition and a little bit of trickery (some people call it induction), we have the following result.

Corollary 77. *Let G be a finite group and let $H_1, \ldots, H_k$ be a collection of normal subgroups of G. If $H_i \cap \langle H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_k \rangle = \{e\}$ for all i and $|H_1|\,|H_2| \cdots |H_k| = |G|$, then $G \cong H_1 \times \cdots \times H_k$.*

Proof. This is an exercise. ■

16.2 The Classification

We are now ready to state the classification of finite abelian groups.

Theorem 78 (Classification of Finite Abelian Groups)**.** *Let G be a finite abelian group. Then*

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

for some primes $p_1, \ldots, p_k$ and positive integers $n_1, \ldots, n_k$. Furthermore, such a presentation is unique up to permuting the factors. That is,

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} \cong \mathbb{Z}_{q_1^{m_1}} \times \cdots \times \mathbb{Z}_{q_l^{m_l}}$$

if and only if $k = l$ and there is some permutation $\sigma \in S_k$ such that $p_i = q_{\sigma(i)}$ and $n_i = m_{\sigma(i)}$ for all $i \in \{1, \ldots, n\}$.

Proofish. Here is a sketch of the proof. The details are worked through in the exercises.

1. Suppose $|G| = p_1^{a_1} \cdots p_k^{a_k}$ where each p_i is a prime and $p_i \neq p_j$ for all $i \neq j$. For each p_i, define
$$H_i := \{g \in G : g^{(p_i^{a_i})} = e\}.$$
Then H_i is a subgroup of G and $|H_i| = p_i^{a_i}$.

2. Since all the p_i are distinct, $H_i \cap \langle H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_k \rangle = \{e\}$ for all i. Furthermore, $|H_1| \cdots |H_k| = |G|$. Therefore
$$G \cong H_1 \times \cdots \times H_k.$$

3. Note that $|H_i| = p_i^{a_i}$, so it is a power of a prime (we call such a group a p_i**-group**). Let $h \in H_i$ be an element with the maximum possible order and let $C = \langle h \rangle$. We prove that $H_i \cong C \times K_i$ for some subgroup $K_i < H_i$. Note that by Cauchy's theorem $|h| \geq p$, so $|K_i| < |H_i|$. Furthermore K_i is also a p_i-group.

4. Use induction to conclude that $H_i \cong C_1 \times C_2 \times \cdots \times C_l$ for cyclic groups $C_j < H_i$. Note that $|C_j| = p_i^j$ for some positive integer j.

5. Apply this to each H_i to get that G is isomorphic to a direct product of cyclic groups of order $p_i^{n_i}$ for some primes p_i and positive integers n_i.

6. Prove such a direct product is unique up to permuting the factors. ■

It is very rare in mathematics that you have such a nice classification of anything, so when something like this comes along you should keep it very near and dear to your heart. Let's see how useful this is in practice.

Example. Let's find all the abelian groups of order 40. We know $40 = 2^3 5$ so our possibilities are

$$\begin{aligned} &\mathbb{Z}_{2^3} \times \mathbb{Z}_5, \\ &\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_5, \quad \text{and} \\ &\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5. \end{aligned}$$

Example. Suppose we want to write $\mathbb{Z}_{40} \times \mathbb{Z}_{15}$ as a product of cyclic groups of prime power order. Recall that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$. Using this we have

$$\mathbb{Z}_{40} \times \mathbb{Z}_{15} \cong \mathbb{Z}_{2^3 5} \times \mathbb{Z}_{3 \cdot 5} \cong \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3.$$

Example. Suppose I have a finite abelian group G such that $|G| = 27$ and for all $g \in G$, $g^3 = 0$. With this information we can completely determine up to isomorphism which group G is.

The classification tells us G is isomorphic to one of

$$\begin{aligned}&\mathbb{Z}_{27},\\&\mathbb{Z}_9 \times \mathbb{Z}_3, \quad \text{or}\\&\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3.\end{aligned}$$

We know $\mathbb{Z}_{27}$ has an element of order 27, and in $\mathbb{Z}_9 \times \mathbb{Z}_3$, $|(1,0)| = 9$ which rules out these two groups. Therefore $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Here is something interesting about finite abelian groups. We know that in general, if two groups G and H do not have the same number of elements of order k for some positive integer k, then they cannot be isomorphic. However, the converse does not hold in general. That is, if G and H are finite groups such that they have the same number of elements of order k for every positive integer k, then it does not necessarily follow that $G \cong H$.

For example, $\mathcal{Q}_8 \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times \mathbb{Z}_4$ have 1 element of order 1, 3 elements of order 2 and 12 elements of order 4, but they are not isomorphic.

Here is an interesting family of counterexamples. Let p be an odd prime and define the **Heisenberg group modulo** p as the group

$$H_p := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{Z}_p) : a, b, c \in \mathbb{Z}_p \right\}$$

which is a subgroup of $\mathrm{GL}_3(\mathbb{Z}_p)$. As an exercise, you can check that every non-identity element has order p, and $|H_p| = p^3$. As another exercise, it is not too difficult to show that H_p is non-abelian.

On the other hand, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ is a group of order p^3 and every non-identity element has order p. However $H_p \ncong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

This example shows that if G and H are finite groups such that they both have the same number of elements of every order, then they are not necessarily isomorphic. However, we can prove this converse in the case where G and H are abelian, and it follows from the classification.

Corollary 79. *Let G and H be finite abelian groups. $G \cong H$ if and only if G and H have the same number of elements of order k for all integers $k \geq 1$.*

Proof. This is an exercise. ■

17 That's All Folks

This is the end of this introduction to group theory course. Although it seems like we have covered a lot of material, we have barely scratched the surface into the wonderful world of group theory. Groups make appearances in just about every corner of mathematics, both in small, non-speaking cameo roles and as the star of the show!

In my opinion, group theory really is a subject that is incredibly aesthetically pleasing. Hopefully during this course you have caught glimpses of the pure unadulterated beauty that resides within this corner of pure mathematics. If you have, I promise that you will find more beauty if you go on to learn more pure mathematics.

As a great man once said, "There is no life I know that compares with pure ~~mathematics~~ imagination."

A Modular Arithmetic

We are all familiar with number systems (whatever they are), say for example, the real numbers $\mathbb{R}$, or the rational numbers $\mathbb{Q}$, or the integers $\mathbb{Z}$. What all of these things have in common is not only that we're quite familiar with them, but that if you take any two things in one of these and multiply or add them together, you get another member of the number system. We might ask ourselves, what else could we consider?

Well that's simple, a clock of course!

Consider a clock with seven numbers, 0 through 6, with the 0 at the top. What we're going to do now, is to try to imitate arithmetic operations on this clock. We will call this clock *the integers modulo 7*. We denote it $\mathbb{Z}_7$ and it consists of the seven elements

$$\mathbb{Z}_7 := \{0, 1, 2, 3, 4, 5, 6\}.$$

But how do we do math in $\mathbb{Z}_7$? Well, kind of as you would expect to do math on a clock. For example,

$$\begin{aligned} 3 + 4 &= 0 \mod 7 \\ 1 + 2 &= 3 \mod 7 \\ 5 + 6 &= 4 \mod 7. \end{aligned}$$

So addition is just what you would do on a clock! So what is $-3 \mod 7$? Well -3 does not live in $\mathbb{Z}_7$ (since it's not one of 0,1,2,3,4,5 or 6), so which element is it? Whatever it is, call it Bob, it better have the property that $\text{Bob} + 3 = 0 \mod 7$. Therefore we have

$$-3 = 4 \mod 7.$$

Alternatively, we could just count backwards around the clock, either way will work and no harm will come to you! Let's do some more examples. What about 22 + 11? Well we have

$$22 + 11 = 33 = 5 \mod 7 \quad \text{OR} \quad 22 + 11 = 1 + 4 = 5 \mod 7.$$

Look at that, it doesn't seem to matter if we convert 22 and 11 to mod 7 before or after doing the addition. It turns out that this is always the case. It doesn't matter when you reduce things to live inside $\mathbb{Z}_7$, no harm will come to you.

Ok, so we've dealt with addition and subtraction (since subtraction doesn't really exist, it's just adding by negative numbers), but what about multiplication and division? Well multiplication will work as we expect. Given two numbers, multiply them together and then keep subtracting (or adding) multiples of 7 until you end up in $\mathbb{Z}_7$. Piece of cake! For example

$$\begin{aligned} 3 \cdot 4 &= 5 \mod 7 \\ 5 \cdot 3 &= 1 \mod 7 \\ 2 \cdot 3 &= 6 \mod 7. \end{aligned}$$

So, what about division or inverses? What is $3^{-1} \mod 7$? Well, let's think about it for a moment. The element that equals 3^{-1}, whatever it is, call it Jenny, had better have the property that $(\text{Jenny}) \cdot 3 = 1 \mod 7$. Well, since $3 \cdot 5 = 1 \mod 7$, and $2 \cdot 4 = 1 \mod 7$, we see

$$3^{-1} = 5 \mod 7 \quad \text{and} \quad 2^{-1} = 4 \mod 7.$$

Let's draw up a table of inverses for $\mathbb{Z}_7$.

x	0	1	2	3	4	5	6
x^{-1}	$*$	1	4	5	2	3	6

Notice here that every non-zero element appears exactly once in both rows, and since nothing multiplies by 0 to be 1, we leave that entry out.

Let's shift our attention now to $\mathbb{Z}_4$. So this is the clock with only $\{0, 1, 2, 3\}$, with 0 at the top. Using the same idea as above we see $1 + 2 = 3 \mod 4$, $2 \cdot 3 = 2 \mod 4$ and $-1 = 3 \mod 4$. Let's draw up a table of inverses for $\mathbb{Z}_4$.

x	0	1	2	3
x^{-1}	$*$	1	$*$	3

This is interesting, it appears that 2^{-1} does not exist, that is 2 does not have an inverse. You might ask how we know this. Well, if 2 has an inverse, it better be one of $\{0, 1, 2, 3\}$, so let's just check them.

$$2 \cdot 0 = 0 \mod 4, \quad 2 \cdot 1 = 2 \mod 4, \quad 2 \cdot 2 = 0 \mod 4, \quad \text{and} \quad 2 \cdot 3 = 2 \mod 4.$$

Since none of these were $1 \mod 4$, we see that 2 does not have an inverse. Interesting. We must now make the following definition.

Definition. A number x in $\mathbb{Z}_n$ is called a **unit** in $\mathbb{Z}_n$ if x^{-1} exists. The set of all units in $\mathbb{Z}_n$ will be denoted by $\mathbb{Z}_n^*$.

So, for example, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, and $\mathbb{Z}_4^* = \{1, 3\}$. The following fact can be proven using the Euclidean algorithm and the application of the Euclidean algorithm to solving diophantine equations. See your Math 135 notes, or the internet, if you're curious as to why it is true.

Fact 80. *An element $a \in \mathbb{Z}_n$ is a unit if and only if* $\gcd(a, n) = 1$.

B Some Set Theory

The goal of this appendix is to go over some facts about functions between sets, and what we can say about sizes of sets by looking at functions between sets. It is often the case that what is coming up is taken for granted. For example, at various points in the notes above we prove that a function is a bijection by finding an inverse. In this appendix we will show that these kinds of techniques actually work!

B.1 Injections, Surjections, and Bijections

Intuitively we know the definitions of an injection, surjection and bijection. An injection from S to T is a function that doesn't send any two elements of S to the same element of T. A surjection from S to T is a function that sends something to everything in T, or a function that hits everything in T. A bijection is a perfect matching, kind of like a dictionary, between elements of S and elements of T. That is, every element of S has an element of T associated to it, and vice versa. This is the same as saying that f is both surjective and injective. Let's make these intuitions formal.

Definition. Let $f : S \to T$ be a function.

- We say f is **injective** (or f is an **injection**) if whenever $f(s_1) = f(s_2)$, we have $s_1 = s_2$.

- We say f is **surjective** (or f is a **surjection**) if for all $t \in T$, there exists an $s \in S$ such that $f(s) = t$.
- We say f is **bijective** (or f is a **bijection**) if f is both injective and surjective.

This definition is all well and good, but there is another way to think about injections, surjections, and bijections. The idea is as follows.

If $f : S \to T$ is an injection, then every element in T that gets hit has a unique preimage (a unique element $s \in S$ such that $f(s) = t$) so we can define a $g : T \to S$ such that if we do f first and then g, we can return every element in S to itself.

If $f : S \to T$ is a surjection, then every $t \in T$ has at least one preimage, so we can define $g : T \to S$ to be a function that sends t to one of its preimages. Since every t has a preimage, this function has the property that if we do g first and then f, every element of t ends up back where it started.

If $f : S \to T$ is a bijection, then we can do what we did for the injections and surjections in a unique way to get a $g : T \to S$ such that $fg(t) = t$ for all $t \in T$ and $gf(s) = s$ for all $s \in S$.

These ideas are formalised in the following proposition. Here is a bit of notation we will use for the proposition and throughout the notes above. Let S be a set and define the identity function $\mathrm{id}_S : S \to S$ by $\mathrm{id}_S(s) = s$ for all $s \in S$.

Proposition 81. *Let $f : S \to T$ be a function between sets.*

- *f is an injection if and only if there exists a function $g : T \to S$ such that $gf = id_S$.*
- *f is a surjection if and only if there exists a function $g : T \to S$ such that $fg = id_T$.*
- *f is a bijection if and only if there exists a function $g : T \to S$ such that $fg = id_T$ and $gf = id_S$. Furthermore, such a g is unique and we denote it $g = f^{-1}$.*

Proof. Suppose f is an injection. Pick an $x \in S$ and for every $t \in f(S)$, let $s_t \in S$ be the unique element of S such that $f(s_t) = t$. Recall $f(S) := \{t \in T : \text{there exists } s \in S \text{ such that } f(s) = t\}$. Define $g : T \to S$ by

$$g(t) = \begin{cases} s_t & \text{if } t \in f(S) \\ x & \text{otherwise.} \end{cases}$$

Since every $s \in S$ is of the form s_t for some $t \in T$, we see $gf(s_t) = g(t) = s_t$ for all $s_t \in S$ so $gf = \mathrm{id}_S$.

Conversely suppose $f(a) = f(b) = t_0$ where $a \neq b$ in S. Suppose $g : T \to S$ is such that $gf = \mathrm{id}_S$. If $g(t_0) \neq a$, then $gf(a) \neq a$, so we must have $g(t_0) = a$. Then we have $gf(b) = a \neq b$, so such a g cannot exist.

Suppose f is a surjection. Define $g : T \to S$ by $g(t) = s_t$ where $f(s_t) = t$. Note that since f is surjective, we can always do this. Then $fg(t) = f(s_t) = t$ for all $t \in T$, so $fg = \mathrm{id}_T$.

Conversely, if f is anot a surjection there is some $t_0 \in T$ such that there is no $s \in S$ such that $f(s) = t_0$. Let $g : T \to S$ be a candidate function such that $fg = \mathrm{id}_T$. Then $fg(t_0) \neq t_0$ since there is no element in S such that $f(s) = t_0$. Therefore there is no function $g : T \to S$ such that $fg = \mathrm{id}_T$.

Finally, if f is a bijection, then define $g : T \to S$ to be $g(t) = s_t$ where $s_t \in S$ is the unique element such that $f(s_t) = t$. Note that every element in S is of the form s_t for some t. Then

$$gf(s_t) = g(t) = s_t \quad \text{and} \quad fg(t) = f(s_t) = t$$

for all $s_t \in S$ and $t \in T$, so $gf = \mathrm{id}_S$ and $fg = \mathrm{id}_T$. Conversely, if f is not injective or surjective, the same arguments above show that there cannot exist a $g : T \to S$ such that $fg = \mathrm{id}_S$ or $gf = \mathrm{id}_T$ respectively.

It remains to show that in the case when f is a bijection, the inverse g is unique. Suppose there is another map $h : T \to S$ such that $fh = \mathrm{id}_S$. Then $f(h(t)) = t = f(g(t))$ fur all $t \in T$. Since f is injective, we must have $h(t) = g(t)$ for all $t \in T$, completing the proof. ■

As is discussed several times in the notes above, whenever you have a sutuation like this, you can use either property as the definition in your head. For example, we can now think of an injection has a map with a left inverse, or as a map which sends different elements to different elements. Whichever definition is easier or more helpful in a particular situation should be the one you use.

It is worth noting here that the above proof relies on the axiom of choice, but that is a discussion for another time and course.

As an application of these ideas, let's show that left-multiplication by a group element is a bijection on a group. This is something you proved in Assignment 1.

Proposition 82. *Let G be a group and $a \in G$. Then $f_a : G \to G$ given by $f_a(g) = ag$ is a bijection.*

Proof. We will show that f_a has an inverse. Consider the map $f_{a^{-1}}$. Then

$$f_a f_a^{-1}(g) = f_a(a^{-1}g) = aa^{-1}g = g \quad \text{and} \quad f_{a^{-1}} f_a(g) = a^{-1}ag = g$$

for all $g \in G$. Therefore $f_a f_{a^{-1}} = \mathrm{id}_G$ and $f_{a^{-1}} f_a = \mathrm{id}_G$, so f_a is a bijection. ■

B.2 Comparing the Sizes of Sets

There are lots of times you might want to show that two sets have the same size, or that one is bigger than the other. Here is a formal way to compare the size of two sets. Here, let $|S|$ be the size of a group.

Definition. Let S and T be sets.

- If there exists an injection $f : S \to T$, then $|S| \leq |T|$.
- If there exists a surjection $f : S \to T$, then $|S| \geq |T|$.
- If there exists a bijection $f : S \to T$, then $|S| = |T|$.

If $|S|$ and $|T|$ are finite, it is easy to see that this agrees with our intuition about what it means for a set to be bigger (or smaller) than another set. The advantage of this definition really becomes apparent when comparing infinite sets, because it gives us a formal way to say whether or not an infinite set is bigger or smaller than another infinite set.

When infinite sets get involved though, there are a few things that we need to check to make sure our notation using $\leq$ and $\geq$ actually makes sense. It turns out that these definitions work because of the following facts, which are far from obvious. They will be stated in terms of the existence of functions, and then in terms of what that means with regards to the relation $\leq$ defined above.

Fact 83. *Let S and T be sets.*

1. *There exists a surjection from S to T or from T to S (or both). Equivalently, $|S| \geq |T|$ or $|T| \geq |S|$ (or both).*

2. *There exists an injection $f : S \to T$ if and only if there exists a surjection $g : T \to S$. Equivalently $|S| \leq |T|$ if and only if $|T| \geq |S|$.*

3. *If there exists an injection $f_1 : S \to T$ and a surjection $f_2 : S \to T$, then there exists a bijection $f : S \to T$. Equivalently, if $|S| \geq |T|$ and $|S| \leq |T|$, then $|S| = |T|$.*

Facts 1 and 2 both rely on the axiom of choice, and fact 3 is called the Schröder-Bernstein theorem.

With these definitions we can formally prove that $|\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$. However, we have $|\mathbb{Z}| \lneq |\mathbb{R}|$, and we can prove that although there is an injection from $\mathbb{Z}$ to $\mathbb{R}$ (which is the regular inclusion map), we cannot find a bijection. If you're curious about this, look up Cantor's diagonalisation argument. It's one of the neatest lines of reasoning you'll see!

C Equivalence Relations and Partitions

Equivalence classes and partitions pop up in just about every area of mathematics, and we will see that both equivalence classes and partitions are two sides of the same coin. It is a common occurrence for us to have a set, and then to consider certain subsets of that set to represent a single element, or to make all the elements in a subset the same.

There are lots of natural examples of equivalence relations.

Example. One that you have seen before (or in appendix 1) is an equivalence relation on the integers $\mathbb{Z}$. Consider the set of numbers that have the same remainder when divided by 7, or the numbers which are the same when reduced modulo 7. Then we can say that two integers $a, b \in \mathbb{Z}$ are equivalent if $a - b$ is a multiple of 7. Then this is an equivalence relation, and it splits the integers up into 7 disjoint sets, one corresponding to each element of the integers modulo 7. In this scenario, we view all the integers which have the same remainder when divided by 7 as the same. Alternatively, we can view this as identifying all of these elements with each other.

Notice that the set of subsets consisting of elements of $\mathbb{Z}$ that are equivalent (which we will soon call equivalence classes) cover all of $\mathbb{Z}$, and no element belongs to two of these subsets. Another way of saying this is that the subsets partition $\mathbb{Z}$.

Example. Consider the set $X = \{1, 2, 3, 4, 5, 6\}$ and identify 1 and 2 together, and identify 3, 4, and 6 as the same element. In this case, the equivalence relation identifies each of the subsets $\{1, 2\}, \{3, 4, 6\}, \{5\}$. The idea is that we may as well just consider 1 to be equal to 2, and 3 to be equal to 4 to be equal to 6.

Notice that the subsets that define which elements are equal partition the set X. If we denote equality in this example by $\sim$ we also notice that for all $x, y, z \in X$, $x \sim x$, if $x \sim y$ then $y \sim x$, and if $x \sim y$ and $y \sim z$, then $x \sim z$.

This last example hints at what we would formally want an equivalence relation to be, and we would like it to imitate what we understand "=" to mean. Intuitively in any context, $x = x$ always, if $x = y$ then $y = x$, and if $x = y$ and $y = z$, then $x = z$. Furthermore, if we group equal things together in a set, we should get a partition of that set into subsets consisting of things that are equal!

Let's formalise these ideas. In the next definition, think of a relation as something like $=$ or $\leq$. So something that takes in two elements of a set and gives back that it is either true or false.

Definition. Let X be a set. An **equivalence relation** on X is a relation $\sim$ that satisfies the following properties.

1. $x \sim x$ for all $x \in X$. We say $\sim$ is **reflexive**.

2. If $x \sim y$ then $y \sim x$. We say $\sim$ is **symmetric**.

3. If $x \sim y$ and $y \sim z$, then $x \sim z$. We say $\sim$ is **transitive**.

Definition. Let X be a set and $\sim$ an equivalence relation on X. For $x \in X$, define the **equivalence class of** x by

$$[x] := \{y \in X : y \sim x\}.$$

The set of equivalence classes is denoted by

$$X/\sim := \{[x] : x \in X\}.$$

This last bit of notation should remind you of the notation for a quotient group, and this is not a coincidence! For a subgroup H of a group G, we will see below that $g_1 \sim g_2$ if they are in the same left coset of H is an equivalence relation on G. Furthermore, the equivalence classes are exactly the left cosets of H in G. With this in mind, the notation G/H for the quotient group makes sense.

Definition. Let X be a set. A **partition of** X is a collection of subsets $\{Y_i\}$ such that $Y_i \cap Y_j = \emptyset$ if $i \neq j$, and $\bigcup_i Y_i = X$.

Intuitively a partition is a way to split up your set into a collection of subsets in such a way that every element of X belongs to exactly one of the subsets.

As we have seen above, we can interchange the idea of an equivalence relation on a set with the notion of a partition. Intuitively they come hand in hand, and this is what the next proposition shows.

Proposition 84. *Let X be a set. If $\sim$ is an equivalence relation on X, then the set of equivalence classes of elements in X partition X. Conversely, if we have a partition of X, it arises as the set of equivalnce classes from an equivalence relation on X.*

Proof. Suppose $\sim$ is an equivalence relation on X. Since $x \in [x]$, every element is in an equivalence class. It remains to show that two equivalence classes are disjoint or equal. Suppose $y \in [x_1] \cap [x_2]$, we want to show that $[x_1] = [x_2]$. Let $z \in [x_1]$. Then since $y \in [x_1]$, $z \sim y$ and since $y \in [x_2]$, $y \sim x_2$. By transitivity of $\sim$, $z \sim x_2$ so $z \in [x_2]$. Conversely, if $z \in [x_2]$, $z \sim y$ and $y \sim x_1$ so $z \sim x_1$ and $z \in [x_1]$. Therefore $[x_1] = [x_2]$.

For each equivalence class $\mathcal{T} \in X/\sim$, pick an element $x \in \mathcal{T}$ and define the subset $Y_x \subset X$ by $Y_x = [x]$. Then by the discussion in the previous paragraph, $\bigcup Y_x = X$ and $Y_x \cap Y_y = \emptyset$ if $x \neq y$. Therefore the set of equivalence classes partitions the set X.

Conversely, suppose $\{Y_i\}$ is a partition of X. Then define a relation on X by $x \sim y$ if and only if $x \in Y_i$ and $y \in Y_i$ for the same subset Y_i. Alternatively, the relation is defined by $x \sim y$ if they both belong to the same subset Y_i. Since if $x \in Y_i$, then $x \in Y_i$, we have $x \sim x$. If x and y are both in Y_i for some i, then y and x both belong to the same subset, so $x \sim y$ implies $y \sim x$. Finally, if $x \sim y$ and $y \sim z$ we must have that $x, y \in Y_i$ and $y, z \in Y_j$ for some i, j. Then $y \in Y_i \cap Y_j$, and since $\{Y_i\}$ is a partition, $Y_i = Y_j$. Therefore $x, z \in Y_i$ and $x \sim z$. This shows $\sim$ is an equivalence relation.

It remains to show the subsets Y_i are exactly the equivalence classes of $\sim$. Let $x \in X$, then $x \in Y_i$ for some i. Then $[x] = \{y \in X : y \sim x\} = \{y \in X : y \in Y_i\} = Y_i$, completing the proof. ■

The important take home message from this proposition is that we can think of equivalence relations and partitions as two sides of the same coin. This theme occurs lots of times in this course, and it's always useful to have multiple ways of thinking about the same thing.

The partition business should remind you of how we proved Lagrange's theorem. An important part of this was showing that the cosets of a subgroup $H < G$ partition the group G.

Example. Let G be a group and H a subgroup. We will show provide a proof different to that given in the notes in Lagrange's theorem that the set of cosets of H partition G.

Following the idea in the proposition above, we would like to show that $a \sim b$ if and only if $aH = bH$, that is they are equivalent if they belong to the same coset. If we can show $\sim$ is an equivalence relation, then the result follows from the proposition above. Notice that $a \sim b$ if and only if $b^{-1}a \in H$.

Since $a^{-1}a = e \in H$ for any $a \in G$, $a \sim a$ for any $a \in G$. Suppose $a \sim b$, so $b^{-1}a \in H$. Then $a^{-1}b = (b^{-1}a)^{-1} \in H$ so $b \sim a$. Finally, suppose $a \sim b$ and $b \sim c$. Then $b^{-1}a \in H$ and $c^{-1}b \in H$. Then $c^{-1}a = c^{-1}bb^{-1}a \in H$ so $a \sim c$. Therefore $\sim$ is an equivalence relation.

Finally, note that for any $a \in G$,

$$\begin{aligned}
[a] &= \{b \in G : b^{-1}a \in H\} \\
&= \{b \in G : a = bh \text{ for some } h \in H\} \\
&= \{ah^{-1} \in G : h \in H\} \\
&= \{ah : h \in H\} \\
&= aH.
\end{aligned}$$

Since the equivalence classes of $\sim$ are the left cosets of H in G, the left cosets of H in G partition G. Once you have this fact, you just need to prove that left cosets have the same size and Bob's your uncle - you've proved Lagrange's theorem.