Groups and Rings part I

Dr Jonathan Elmer, Middlesex University

2017/18

Chapter 1

Sets and binary operations

1.1 Introduction

In MSO1130 *Logic and Structures* you met various number systems:

$\mathbb{N}$ = The Natural Numbers = $\{1, 2, 3, 4, \ldots\}$;

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

$\mathbb{Q}$ = Rational Numbers = $\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$;

$\mathbb{R}$ = Real Numbers

$\mathbb{Z}_n$ = Integers modulo n = $\{[0], [1], [2], \ldots, [n-1]\}$ where $[k]$ represents the

set of numbers $\{\ldots, k-n, k, k+n, \ldots\}$

You also met various operations on them: for example, one can define addition on $\mathbb{N}$ such that $n+m \in \mathbb{N}$ if n and m are. One can define multiplication on $\mathbb{Z}_n$:

$$[a][b] = [a \times b];$$

we showed in logic and structures that this is "well-defined", in the sense that it doesn't matter what representative you take for $[a]$ and $[b]$.

These are examples of **binary operations** - informally, ways of taking two elements of a set, and combining them to make a third. Formally,

Definition 1.1

A binary operation on a set S is a function $f : S \times S \to S$.

We normally write $a \star b$ rather than $f(a, b)$.

Remark. *A note on these notes!* The definitions in these notes are in red boxes. I want them to stand out. This is because definitions have a special status in mathematics, especially in algebra. We need to know the precise definition of a binary operation in order to prove facts about binary operations in general.

You will be expected to learn definitions in this text by heart, and you will be tested on this and other definitions next week. You will also be expected to quote and use definitions in the test and exam later in the term.

1.2 Examples of binary operations

You already know lots of examples of binary operations.

Example 1.1. (Binary operations)

(a) Addition is a binary operation on $\mathbb{N}$.

(b) Multiplication is a binary operation on $\mathbb{N}$.

(c) Addition is a binary operation on $\mathbb{Z}$.

(d) Subtraction is a binary operation on $\mathbb{Z}$.

(e) Multiplication is a binary operation on $\mathbb{Z}$.

(f) Addition is a binary operation on $\mathbb{Q}$.

(g) Subtraction is a binary operation on $\mathbb{Q}$.

(h) Multiplication is a binary operation on $\mathbb{Q}$.

(i) Division is a binary operation on $\mathbb{Q}\backslash\{0\}$.

(j) Multiplication modulo n and addition modulo n are binary operations on $\mathbb{Z}_n$.

Note, however:

Example 1.2. (Not binary operations)

(a) Subtraction is not a binary operation on $\mathbb{N}$, since for example $1 - 2 \notin \mathbb{N}$.

(b) Division is not a binary operation on $\mathbb{Z}$, since for example $1 \div 2 \notin \mathbb{Z}$.

(c) Division is not a binary operation on $\mathbb{Q}$, since for example $1 \div 0 \notin \mathbb{Q}$.

Here are some less obvious ones:

Example 1.3. Let S be a set and let $\mathcal{F}$ be the set of all *functions* which map $S \to S$. Given a pair of functions $f, g : S \to S$ we can define a new function $f \star g$ by

$$f \star g(x) = f(g(x))$$

for all $x \in S$.

This is called **composition of functions**, and you met it in Logic and Structures.
Notice that $f \star g$ is another function from S to S. Therefore $\star$ is a binary operation on $\mathcal{F}$.

There's no rule that says binary operations have to be *useful*:

Example 1.4. Define $\star$ on $\mathbb{Z}$ by $a \star b = ab^2 - 17$. Then $\star$ is a binary operation on $\mathbb{Z}$.

Or we can go full-on abstract, as the next example shows:

Example 1.5. Let $S = \{a, b, c\}$ and define $\star$ as follows:

$$a \star b = c$$

$$b \star a = c$$

$$a \star c = b$$
$$c \star a = b$$
$$b \star c = a$$
$$c \star b = a$$
$$a \star a = a$$
$$b \star b = b$$
$$c \star c = c$$

Then $\star$ is a binary operation on S.

1.3 Properties of binary operations

The aim of this section is to develop some language to compare and contrast different binary operations. For example, notice that for some binary operations, order doesn't seem to matter:

Example 1.6. Let $a, b \in \mathbb{N}$. Then $a + b = b + a$ for all $a, b \in \mathbb{N}$.

Whereas for others it does:

Example 1.7. Consider $-$ on $\mathbb{Z}$. Notice that

$$-1 = 1 - 2 \neq 2 - 1 = 1.$$

Definition 1.2

Let S be a set. A binary operation $\star$ on S is said to be **commutative** if

$$a \star b = b \star a \text{ for all} a, b \in S.$$

Exercise 1.1

Decide which of the binary operations given in Examples 1.1, 1.4 and 1.5 are commutative.

Remark. *A reminder on proof:*

The condition of commutativity is a "for all" condition. Therefore, to prove a binary operation is commutative, you have to take general elements a and b and show that $a \star b = b \star a$. We proved that, for instance, $+$ on $\mathbb{N}$ is commutative in *Logic and Structures* and we won't do this again.

The negation of the definition of commutativity is

$$\text{There exist } a, b \in S \text{ such that } \; a \star b \neq b \star a.$$

So, to prove a binary operation is not commutative, it's enough to give just one example of a pair of elements which fail to commute. Like, for instance, 1 and 2 for $-$ on $\mathbb{Z}$.

The same discussion also applies to associativity below.

Definition 1.3

A binary operation $\star$ on S is called **associative** if

$$a \star (b \star c) = (a \star b) \star c$$

for all $a, b, c \in S$.

Example 1.8. Addition is associative on $\mathbb{Z}$. Subtraction is not, since for example

$$3 - (2 - 4) = 5 \neq -3 = (3 - 2) - 4$$

.

Exercise 1.2

Decide which of the binary operations given in Examples 1.1, 1.4 and 1.5 are associative.

Definition 1.4

Let S be a set and $\star$ a binary operation on S. An element $e \in S$ is called an **identity** for $\star$ if for all $s \in S$ we have

$$s \star e = e \star s = s.$$

Example 1.9.

(a) 0 is the unique identity for addition on $\mathbb{Z}$.

(b) 1 is the unique identity for multiplication on $\mathbb{Z}_n$ for any $n \in \mathbb{N}$.

(c) Subtraction on $\mathbb{Z}$ does not have an identity.

Exercise 1.3

Decide which of the binary operations given in Examples 1.1, 1.4 and 1.5 are have an identity.

You should notice that if a binary operation has an identity, then that identity is

unique. This is not a coincidence - we'll prove it next week.

There's one final property we need to consider.

Definition 1.5

Let S be a set, $\star$ a binary operation on S, $e \in S$ an identity, and $s \in S$. An element $t \in S$ is called an **inverse** for s under $\star$ if

$$s \star t = t \star s = e.$$

Example 1.10.

(a) Every element of $\mathbb{Z}$ has an inverse under addition.

(b) 7 is the inverse of 3 in $\mathbb{Z}_{10}$ under multiplication modulo 10, since $7 \times 3 = 21 = 1 \mod 10$.

(c) 2 does not have an inverse in $\mathbb{Z}_{10}$ under multiplication modulo 10.

Exercise 1.4

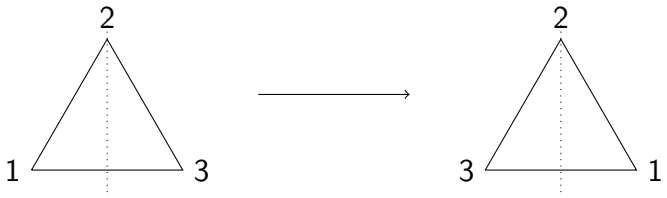
For which of the binary operations given in Examples 1.1, 1.4 and 1.5 which have an identity are also such that every element is invertible?

1.4 Extended tutorial: symmetries of a triangle

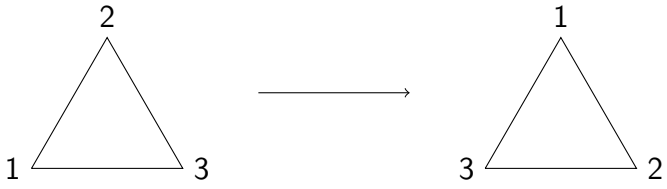
You probably learned about symmetry at school. For example, plane figures have two kinds of symmetry - rotational and reflectional. In this tutorial we will study the symmetry group[1] of a triangle.

[1] I know I haven't told you what a group is yet...

A **symmetry** of a plane figure is defined as a mapping from the shape to itself which preserves the underlying structure.For example, here are two different symmetries of a triangle.



x: the reflection in vertical axis

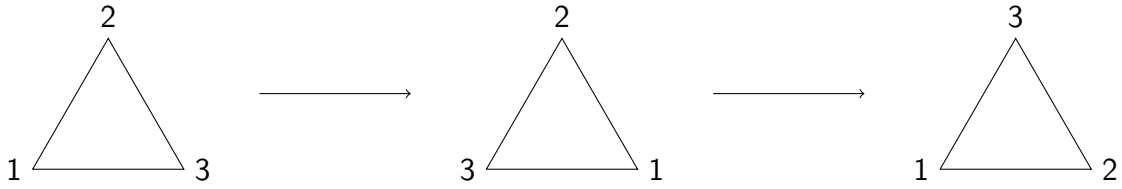


y: a 120 degree rotation clockwise

Exercise 1.5

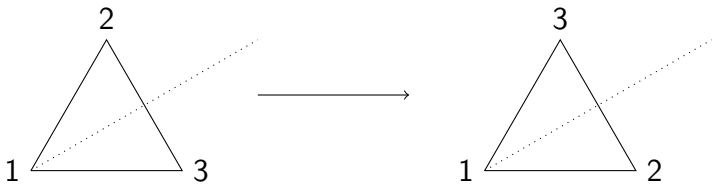
There are six symmetries of a triangle altogether. Describe them all in words.

A **composition** of two symmetries is the result of performing first one symmetry then another immediately afterwards. For example, if we do x followed by y we get



x y

This is exactly the same as



xy: the reflection in given dotted line

which is another symmetry.

Exercise 1.6

Now for each ordered pair of symmetries in your list, work out the result of composing them. Find a way of recording your results.

Note that there 36 calculations to do here. Rather than doing all 36 by hand, try to find some rules which describe how your symmetries compose. One thing which might help is to try and write the 6 symmetries in terms of the two described in Exercise 1.5.

Exercise 1.7

Now try to write a set of rules which would enable someone to find the result of composing any two symmetries without needing to do any calculations. Try to be as efficient as possible, i.e. don't include rules which are not needed.

Exercise 1.8

If you have time, repeat the exercise with a square. What are the rules which are common to both situations?

1.5 Homework exercises

Exercise 1.9

For each of the following examples, say whether $\star$ is a binary operation on S.

(a) $S = \mathbb{Q}$, $a \star b = a + b$;

(b) $S = \mathbb{Q}$, $a \star b = a - b$;

(c) $S = \{-1, 1\}$, $a \star b = a + b$;

(d) $S = \{-1, 1\}$, $a \star b = ab$;

(e) $S = \mathbb{Z}$, $a \star b = a^b$;

(f) $S = \mathbb{N}$, $a \star b = a^b$;

(g) S the set of 2×2 matrices under matrix multiplication;

(h) $S = \mathbb{Z}$, $a \star b = a + b - 2$.

Exercise 1.10

Of the examples above which are binary operations, which are commutative? Which are associative? Explain your answers.

Exercise 1.11

Consider $\{0, 1, 2, 3, 4, 5\}$ with the binary operation $a \star b = ab \mod 6$. What is the identity for $\star$? Which elements have inverses?

Exercise 1.12

Consider $\mathbb{Q}$ with the binary operation $\star$ defined by

$$a \star b = a + b - ab.$$

(a) Show that $\star$ is commutative.

(b) Show that $\star$ is associative.

(c) Show that 0 is an identity for $\star$.

(d) Which elements of $\mathbb{Q}$ have an inverse? Explain your answer.

Chapter 2

Groups: definitions and examples

2.1 Introduction

Exercise 2.1: Definition Quiz

Let S be a set:

(a) What is meant by saying $\star$ is a **binary operation** on S?

(b) What is meant by saying $\star$ is **commutative**?

(c) What is meant by saying $\star$ is **associative**?

(d) What is meant by saying an element $e \in S$ is an **identity** for $\star$?

(e) What is meant by saying an element $g \in S$ has an **inverse** under $\star$?

In last week's lecture, we learned that many of features of arithmetic we already know and love are binary operations. We also learned some terminology to describe features of binary operations: commutative, associative, identity and inverses.

You probably noticed that the most natural looking operations tend to satisfy all four of these. For example:

Example 2.1.

(a) $+$ on $\mathbb{Z}$ is commutative and associative, has an identity (0) and every element in $\mathbb{Z}$ has an inverse under $+$.

(b) $\times$ on $\mathbb{Q} \setminus \{0\}$ is commutative and associative, has an identity (1) and every element in $\mathbb{Q} \setminus \{0\}$ has an inverse under $\times$.

There are many more besides. Here is the single most important definition of the course:

Definition 2.1

Let G be a set and $\star$ a binary operation on G. G is said to be a **group** under $\star$ if

1. $\star$ is associative;
2. G has an identity for $\star$;
3. Every element of G has an inverse under $\star$.

Notice that commutativity is not part of the definition. Commutative groups are special:

Definition 2.2

Let G be a group under $\star$. If $\star$ is commutative on G, G is said to be an **abelian group**.

2.2 Examples of groups

So we can rephrase Example 2.1 more efficiently: $\mathbb{Z}$ under addition and $\mathbb{Q} \setminus \{0\}$ under multiplication are abelian groups. Here are some more examples of abelian groups:

Example 2.2.

(a) $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ under addition;

(b) $\mathbb{R} \setminus \{0\}$ under multiplication;

(c) $\mathbb{Z}_n$ under addition modulo n, for any n.

(d) The set $S = \{-1, 1\}$ under multiplication.

In cases (a)-(c) we have already checked that the given operation is a binary operation on the given set, and that it is commutative, associative, has an identity and is such that every element has an inverse, during lecture 1.

(d) seems a bit surprising, so let's check that now. You can consider the following a model for checking whether something is a group:

- **Binary Operation (closure)** First we make sure we have a binary operation: we must ensure that $s_1 \star s_2 \in S$ for all pairs $s_1, s_2 \in S$. We can store the results of this calculation rather neatly in a table:

$\times$	-1	1
-1	1	-1
1	-1	1

- **Associativity** Next we make sure that $\star$ is associative on S. In this particular case there's nothing to check here; we know from *Logic and Structures* that multiplication is associative on $\mathbb{Q}$, and clearly it must remain so when restricted to S.

- **Identity** Now we make sure there's an identity in S. Unsurprisingly, we find that $1 \in S$ is an identity.

- **Inverses** Finally, make sure every element in S has an inverse. As the identity in S is 1, this means we need to show

$$(\forall s \in S)(\exists t \in S)(s \star t) = 1.$$

  A quick check of the multiplication table reveals that 1 is the inverse of 1 and -1 is the inverse of -1. So every element has an inverse under $\star$.

  At this point, we have already proved S is a group under $\star$. To prove it's an abelian group, we just need to check commutativity:

- **Commutativity** Again, there's nothing to do here. We know that multiplication is commutative on S because it is commutative on the larger set $\mathbb{Z}$.

All the examples you've seen this week have been abelian groups. But you saw an example of a non-abelian group last week - the set of symmetries of a triangle.

Exercise 2.2

Which of the following are examples of abelian groups?

(a) $\mathbb{Z}$ under multiplication;

(b) The set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ under multiplication modulo 10;

(c) The set $\{1, 3\}$ under multiplication modulo 4.

2.3 Properties of groups

Definition 2.1 is more than a definition. It is a set of **axioms** for the subject of group theory.

If you're not sure what that means, think back to the lecture on Number Systems 1 in *Logic and Structures*. In it, you met the axioms for the natural numbers. You used these axioms to define addition and multiplication on $\mathbb{N}$ and prove various properties, e.g. commutativity and associativity of multiplication.

The point of using an axiom system is that properties don't depend on the model you're using. Anything you've proved directly from the axioms remains true in any model satisfying the axioms.

The same is true in group theory. Anything we can prove using only the axioms of a group is *true for every single group.*

Here is an example of the kind of thing we might want to prove:

Proposition 2.1. *The identity element in a group G is unique.*

Proof. Now we already know that G has an identity - that's one of the axioms. So all we have to do is prove there's only one. The standard way to prove uniqueness is by contradiction; so, suppose G has *two* identities. Let's call them e and e'.

Now, for the sake of understanding, I'm going to introduce two new definitions.

Let's say that an element $x \in G$ is a **right identity** if

$$g \star x = g \text{ for all } g \in G.$$

And let's say $x \in G$ is a **left identity** if

$$x \star g = g \text{ for all } g \in G.$$

These are standard definitions, although we won't use them again in this course. Note that an identity in G is precisely both a right- and a left identity.

Now consider the element

$$e \star e'.$$

On the one hand, because e is a left identity, we have

$$e \star e' = e'.$$

On the other hand, because e' is a right identity, we have

$$e \star e' = e.$$

Putting these together we get

$$e = e'$$

which shows that the identity element in G is unique, as required.

□

Remark. As you know, the level of detail that needs to be included in a proof depends very much on the intended audience. I've written this proof for a group of students who only met the definition of a group today. A minimal proof of the previous proposition might look like this:

Proof. Suppose e and e' are identities. Then we have

$$e = e \star e' = e'$$

which shows that the identity in G is unique. □

This should make perfect sense to you by the end of the course but probably looks a bit baffling right now, hence the additional detail.

Exercise 2.3

Let G be a group and let $g \in G$. Prove that the inverse of g in G is unique.

Hint: Work by contradiction following the model of Proposition 2.1. Suppose h and k are both inverses of g and consider $(h \star g) \star k$. You may find it helpful to introduce the ideas of **left inverse** and **right inverse**.

2.4 A few words on notation

Up to now, we have used the symbol $\star$ for the binary operation in a group G. Usually, we use no symbol for the operation, rather like we do for multiplication. So:

Instead of $g \star h$ we write gh.

Thanks to associativity, there's never any need to use brackets either. So

Instead of $(g \star h) \star k$ or $g \star (h \star k)$ we can just write ghk.

Much of the notation we use in group theory looks like multiplication. So much so, that we even say "multiply" for an unspecified binary operation in a group.

Now it makes perfect sense to multiply an element by itself. And we can do this as many times as we like. We have a shorthand for this:

$$\underbrace{ggggg \cdots gggg}_{n \text{ times}} = g^n.$$

We showed in Proposition 2.1 that the identity in a group is unique. The identity in a group is usually denoted by e. Be warned though, some textbooks use the number 1 instead.

We also showed in Exercise 2.3 that inverses in a group are unique. If $g \in G$ then we write g^{-1} for the inverse of g.

Now if n is any positive integer we define

$$\underbrace{g^{-1}g^{-1}g^{-1} \cdots g^{-1}g^{-1}g^{-1}}_{n \text{ times}} = g^{-n}.$$

We also adopt the convention that

$$g^0 = e \text{ for all } g \in G.$$

With these conventions in place, we have

Proposition 2.2. *Let G be a group, $g \in G$, and $m, n \in \mathbb{Z}$. Then*

$$g^{m+n} = g^m g^n \quad \textit{and} \quad (g^m)^n = g^{mn}.$$

We'll finish this lecture with a very quick result which will be useful later. Remember, since we're proving it directly from the axioms, it applies to every single group.

Proposition 2.3 (Right cancellation law)**.** *Let G be a group. Let $a, b, c \in G$ and suppose $ac = bc$. Then $a = b$.*

Proof. Multiplying on the right by c^{-1} gives

$$(ac)c^{-1} = (bc)c^{-1}.$$

By the associative law,

$$a(cc^{-1}) = b(cc^{-1}).$$

Further, $cc^{-1} = e$ and so we get

$$ae = be$$

and so

$$a = b$$

as claimed. □

Proposition 2.4 (Left cancellation law)**.** *Let G be a group. Let $a, b, c \in G$ and suppose $ca = cb$. Then $a = b$.*

Proof. Similar to the right cancellation law. □

2.5 Exercises for week 2

In the lecture, we learned how to:

- Prove a set is a group under a given binary operation;
- Prove facts about all groups using the axioms.

In todays tutorial we'll practise doing both of these. Any questions left over can be considered homework.

Exercise 2.4

Let G be a group with identity $e \in G$. Prove that

(a) $e^{-1} = e$.

(b) For any $g \in G$ we have $(g^{-1})^{-1} = g$;

(c) For any $g, h \in G$ we have $(gh)^{-1} = h^{-1}g^{-1}$.

Hint: remember that inverses in a group are unique. So, if you are given an element $a \in G$, and you can show that $ba = ab = e$, then you know that $b = a^{-1}$.

Exercise 2.5

Let $G = \mathbb{Z}$ with binary operation $\star$ defined by $a \star b = a + b - 2$. Show that G is a group. Is G abelian?

Exercise 2.6

Let $G = \mathbb{Q}\backslash\{0\}$ with binary operation $\star$ defined by $a \star b = ab/5$. Show that G is a group. Is G abelian?

Exercise 2.7

Let G be the set of all $n \times n$ matrices of the form

$$\begin{pmatrix} x & -x \\ -x & x \end{pmatrix}$$

for some $x \in \mathbb{R}\backslash\{0\}$. Show that G is a group under matrix multiplication. Is G abelian?

Exercise 2.8

Let G be the subset of complex numbers $\{1, -1, i, -i\}$. Show that G is a group under multiplication. Is G abelian?

Chapter 3

Finite Groups and Cayley Tables

3.1 Introduction

Exercise 3.1: Definition Quiz

Let G be a set and $\star$ a binary operation on G. What does it mean to say that:

(a) G is a **group** under $\star$?

(b) G is an **abelian group** under $\star$?

Most of the groups we met in Lecture 2 were infinite:

Example 3.1. (a) $\mathbb{Z}$ under addition is an infinite group;

(b) $\mathbb{Q} \setminus \{0\}$ under multiplication is an infinite group.

But we also saw some examples of groups with a finite number of elements:

Example 3.2.

(a) The set $\{-1, 1\}$ under multiplication (see Example 2.2 (d));

(b) The set of complex numbers $\{1, i, -1, -i\}$ under multiplication (see Exercise 2.5;

(c) The symmetries of a triangle or square (see extended tutorial in Lecture 1);

(d) The set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under addition modulo n.

The next definition should not come as any kind of surprise:

Definition 3.1

A group with a finite number of elements is called a **finite group**. The number of elements in a finite group is called its **order**.

3.2 Cayley Tables

Finite groups are easy to handle, because all the information about the binary operation can be recorded in a table. Here, for example, is the table describing multiplication in the group $\{-1, 1\}$:

Example 3.3.

	-1	1
-1	1	-1
1	-1	1

The table describing the binary operation in a finite group G is sometimes called the **Cayley Table** of G.

Exercise 3.2

Write out the Cayley table for:

(a) $\{0, 1\}$ under addition modulo 2;

(b) $\{1, 3\}$ under multiplication modulo 4.

Do you notice anything interesting?

Here are some more Cayley tables:

Example 3.4. The Cayley table for the group $\{1, -1, i, -i\}$ under multiplication is

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	-1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

The Cayley table for the group $\{0, 1, 2, 3\}$ under addition modulo 4 is

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

3.3 Properties of Cayley Tables

You can tell a lot about a binary operation by looking at it's Cayley Table [1]

In particular, calculating a Cayley table is a good way to determine whether a finite set under a given binary operation is a group. Notice that the Cayley tables we've seen so far all have the following properties:

- *In the Cayley table of a finite group, there should be exactly one row and exactly one column which are the same as the outer row and column.*

  This is because every (finite) group has exactly one identity element. The row and column corresponding to the identity are the same as the outer row and column. For example, the red numbers in the Cayley table for $\{0, 1, 2, 3\}$ under addition modulo 4

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  which appear in a row and column indexed by 0 tell us that 0 is an identity.

[1] I shouldn't really call it a Cayley table unless I'm talking about the operation in a group, but you know what I mean...

- *In the Cayley table of a finite group, every row and column should contain the identity exactly once.*

  This is because every element has a unique inverse. The elements indexing the row and column where the identity is found are mutually inverse pairs. For example, in the table for $\{0, 1, 2, 3\}$ under addition modulo 4

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  the presence of a zero in the row and column index by 2 tells us that 2 is the inverse of 2.

- *In the Cayley table of a finite group, each row and column contains each group element exactly once.*

  This is a consequence of the cancellation laws (Proposition 2.4). Suppose g appears in the ith and jth position in row k. Let a, b, c be the elements labelling rows and columns i, j, k respectively. The table then looks something like this:

	a	$\ldots$	b
c	g	$\ldots$	g

  Then we have

$$ca = cb = g,$$

  so

$$a = b$$

  by the left cancellation law. This shows that $i = j$. Since there are the same number of columns as elements, all elements appear exactly once in each row. The proof for columns is similar.

Remark. So, you can use a Cayley table to check immediately whether a binary operation on a finite set has an identity and inverses. Determining whether it is associative is rather trickier. There is an example of this in the tutorial. But remember that a lot of familiar operations are associative anyway, so you rarely need to do this.

Exercise 3.3

Let $G = \{1, 2, 3, 4\}$ under multiplication modulo 5. Is this a group?

Flipping this on its head, if a binary operation on a finite set has a table which does not have one of these properties, the set is not a group.

Example 3.5. We calculate the multiplication table for $\{0, 1, 2, 3, 4, 5\}$ under multiplication modulo 6 (see also Exercise 1.5).

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Now the row and column indexed by 1 are identical to the outer row and column. Thus, 1 is an identity. But 1 does not appear on every row and column (e.g. it doesn't appear on the row indexed by 0) so $\{0, 1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6.

3.4 Isomorphism - an informal first look

Note that the Cayley table of a group is not unique - it depends on what order we write the group elements in. Sometimes, there's a natural order coming from

arithmetic, but often there isn't. For example, we could write the Cayley table for $\{1, i-1, -i\}$ under multiplication could also be written:

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

after swapping rows and columns labeled by i and -1.

Allowing for this, we often notice that Cayley tables are just relablings of one another. For instance, if we replace

$$\begin{aligned} 1 &\to 0 \\ i &\to 1 \\ -1 &\to 2 \\ -i &\to 3 \end{aligned}$$

in the table above we get

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

which is the Cayley table for $\{0, 1, 2, 3\}$ under addition modulo 3.

There's a fancy word for this phenomenon. We say two finite groups are **isomorphic**[2] if they have the same Cayley tables, possibly after relabling and reordering group elements. So we have just proved:

Proposition 3.1. *The groups* $\{1, i, -1, -i\}$ *under multiplication and* $\{0, 1, 2, 3\}$ *under addition modulo 4 are isomorphic.*

Exercise 3.4

Turn back to Exercise 3.2 and convince yourself that the two groups of order 2 you considered are also isomorphic.

This is not surprising. In fact we have:

Proposition 3.2. *Any two groups of order 2 are isomorphic.*

Proof. Let G be a group of order 2. Then G can be labelled as $\{e, a\}$ with e the identity and $a \neq e$. We have $ae = a = ea$ by definition. So after choosing an ordering we already know most of the Cayley table of G:

	e	a
e	e	a
a	a	?

.

We have to decide whether $a^2 = e$ or $a^2 = a$. Suppose the latter. This can be written

$$aa = ae.$$

Then by right cancellation (Proposition 2.3) we get

$$a = e$$

a contradiction. So we must have $a^2 = e$ and Cayley table

[2]This definition is not in a red box, because it's not the official definition of isomorphism. That comes later.

	e	a
e	e	a
a	a	e

.

□

3.5 Tutorial: Calculating Cayley Tables

In today's lecture, you calculated the Cayley tables of some (rather small) groups. In this tutorial we'll have a look at the Cayley tables of some larger groups, and also look more deeply at the structure of finite groups.

Exercise 3.5

Consider the following four matrices:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \quad D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Show that they form a group under matrix multiplication and write down its Cayley table. Is it isomorphic to either of the groups in Example 3.4 in todays lecture?

Exercise 3.6

The following is part of a Cayley table for a finite group of order 5. Complete the table.

Hint: use the properties of Cayley tables found in section 3.3

	a	b	c	d	e
a					
b					
c					
d		e		a	
e		b			

.

Exercise 3.7

Consider the following four matrices:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

where $i \in \mathbb{C}$ is such that $i^2 = -1$. Show that the set of 8 matrices $\{\pm E, \pm I, \pm J, \pm K\}$ form a group under matrix multiplication. Is it abelian?

Exercise 3.8

Let $G = \{2, 4, 6, 8\}$ with binary operation multiplication modulo 10. Show that G is a group and write down its Cayley table. Is G isomorphic to any of the other groups of order 4 you've seen?

Exercise 3.9

Prove that any pair of groups of order 3 are isomorphic.

Hint: try to fill in the Cayley table step by step.

Chapter 4

More Examples of Groups

4.1 Introduction

Today we will look in more detail at two large classes of examples of groups - groups of units and groups of matrices. While we're seeing these objects in a new context, much of today's lecture will be revision from either MSO1130 *Logic and Structures* or MSO1110 *Vectors and Matrices*.

4.2 Groups of units and modular arithmetic

Modular arithmetic provides us with a good supply of finite groups to study. For example, the set

$$\mathbb{Z}_n = \{0, 1, 2, 3, 4, 5 \ldots, n-1\}$$

is always a group under addition modulo n. Thus, there exists a finite group of

order n for every positive integer n.

$\mathbb{Z}_n$ is never a group under multiplication modulo n, because 0 is never invertible modulo n. However, if we remove 0, we sometimes do get a group.

Example 4.1.

- Recall from Exercise 3.3, that $\{1, 2, 3, 4\}$ is a group under multiplication modulo 5.

- Deduce from Exercise 1.5 that $\{1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6, because this is not a binary operation on this set. For example,
$$2 \times 3 = 6 = 0 \mod 6.$$

Exercise 4.1

Write out the multiplication tables for:

- $\{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7;
- $\{1, 2, 3, 4, 5, 6, 7\}$ under multiplication modulo 8;
- $\{1, 2, 3, 4, 5, 6, 7, 8\}$ under multiplication modulo 9.

Which of these are groups? For which values of n in general do you think that $\mathbb{Z}_n \setminus \{0\}$ is a group under multiplication modulo n?

You should have discovered that:

- $\{1, 2, 3, 4, 5, 6\}$ is a group under multiplication modulo 7;
- $\{1, 2, 3, 4, 5, 6, 7\}$ is not a group under multiplication modulo 8, because for instance $2 \times 4 = 8 = 0 \mod 8$.
- $\{1, 2, 3, 4, 5, 6, 7, 8\}$ is not a group under multiplication modulo 9, because for instance $3 \times 3 = 9 = 0 \mod 9$.

Now let's look more carefully at the multiplication table for $\{1, 2, 3, 4, 5, 6, 7\}$ modulo 8:

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Now, which elements are preventing multiplication modulo 8 from being a binary operation on the set? The ones that have a zero in the row or column they label. That's the elements $2, 4$ and 6. And what do these have in common? They all share a *common divisor* (2) with 8. We can generalize this quite easily to any value of n.

Proposition 4.1. *Let a and n share a common divisor $d > 1$. Then there exists $b < n$ such that $ab = 0 \mod n$.*

Proof. Suppose a and n are divisible by $d > 1$. Set $b = n/d$; this is an integer. Then

$$ab = a\frac{n}{d} = n\frac{a}{d} = 0 \mod n$$

because a/d is an integer. □

Now look what happens if we remove these elements:

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

We get a group!

This always happens. It's a very important example of a group, called the **group of units modulo** n. We denote it by $\mathbb{Z}_n^\times$.

We will prove that $\mathbb{Z}_n^\times$ is indeed a group for any value of n. We will need to recall some results from *Logic and Structures*, which we'll quote without proof.

Definition 4.1

Let a and b be natural numbers. The **greatest common divisor** of a and b is is the largest natural number c such that $c|a$ and $c|b$. We write $c = \gcd(a, b)$ or just $c = (a, b)$. We say a and b are **coprime** if $(a, b) = 1$.

So, the elements of $\mathbb{Z}_n^\times$ are precisely the numbers which are less than n and coprime to n. Now we need:

Proposition 4.2 (Bézout)**.** *Suppose $a, b, c \in \mathbb{N}$ and write $d = (a, b)$. Then there exist $k, l \in \mathbb{Z}$ such that $ak + bl = c$ if and only if $d|c$.*

You saw two proofs of this result last year. There is an algorithm, called the **Extended Euclid Algorithm** which we can use to find k and l. You have used this recently in MSO2130 *Discrete Mathematics and Geometry*. We also need:

Proposition 4.3 (Euclid)**.** *Let p be a prime number. Let a and b be natural numbers and suppose that $p|ab$. Then $p|a$ or $p|b$.*

Theorem 4.1

$\mathbb{Z}_n^\times$ is an abelian group under multiplication modulo n.

Proof. We check that multiplication modulo n is a binary operation on $\mathbb{Z}_n^\times$ satisfying the group axioms.

- **Binary operation:** Suppose $a, b \in \mathbb{Z}_n^\times$. Then $(a, n) = (b, n) = 1$. We have to show that $(ab, n) = 1$.

  Suppose p is a common prime factor of (ab) and n.

  Then $p|n$, and $p|a$ or $p|b$ by Proposition 4.3.

  Then $p < (a, n)$ or $p < (b, n)$ by definition.

  Since $(a, n) = 1$ and $(b, n) = 1$ we must conclude ab and n have no common prime factors, and hence $(ab, n) = 1$.

  It follows that multiplication modulo n is a binary operation on $\mathbb{Z}_n^\times$.

- **Associativity:** Multiplication modulo n is associative.

- **Identity:** $(1, n) = 1$ and therefore $1 \in \mathbb{Z}_n^\times$. This is an identity for multiplication modulo n.

- **Inverses:** Let $a \in \mathbb{Z}_n^\times$. Then $(a, n) = 1$. By Proposition 4.2 there exist $k, l \in \mathbb{Z}$ such that
$$ak + nl = 1.$$
This implies that
$$ak = 1 \mod n.$$
In other words k is an inverse for a modulo n. Moreover, $(k, n) = 1$ by the "only if" part of Proposition 4.2

The above shows that $\mathbb{Z}_n^\times$ is a group under multiplication modulo n. It is an abelian group because multiplication modulo n is commutative. □

For the sake of emphasis, a definition (in red!)

Definition 4.2

Let n be a natural number. Then $\mathbb{Z}_n^\times$ denotes the set of natural numbers which are smaller than n and coprime to n. It is an abelian group under multiplication modulo n. It is called the **group of units modulo** n.

Remark. The order of $\mathbb{Z}_n^\times$ is not n. If n is prime then $\mathbb{Z}_n^\times$ has order $n - 1$, otherwise it has order smaller than this.

Remark. Don't confuse $\mathbb{Z}_n^\times$ with $\mathbb{Z}_n$, which denotes the set of all numbers less than n and is a group under *addition* modulo n. This group does indeed have order n.

Exercise 4.2

List the elements of $\mathbb{Z}_{10}^\times$.

4.3 Infinite Groups

In MSO1130 *Logic and Structures* you learned two ways to describe infinite sets:

- As a list following some obvious pattern:

$$S = \{\ldots -4, -2, 0, 2, 4, 6, 8, \ldots\}$$

- As a set of elements satisfying some property:

$$S = \{n \in \mathbb{Z} | (\exists m \in \mathbb{Z})(n = 2m)\}.$$

When dealing with infinite groups, we usually need to use the latter.

Example 4.2. We prove that the set of all even integers forms a group under addition. Let S be the set of all even integers.

- **Binary Operation:** We proved in *Logic and Structures* that the sum of two even integers is even. So addition is a binary operation on the set of even integers.
- **Associativity:** Addition is associative on $\mathbb{Z}$, and hence so on S.
- **Identity:** 0 is an even integer. Since 0 is an identity on $\mathbb{Z}$, it is an identity on S.
- **Inverses:** Let n be an even integer. Then $-n$ is its inverse in $\mathbb{Z}$ under addition. We claim that $-n$ is even.

To see this, let $n = 2m$. Then

$$-n = -2m = 2 \times (-m) \in S.$$

So every element of S has an inverse in S.

4.4 Matrix Groups

A group whose elements are matrices and whose binary operation is matrix multiplication is called a **Matrix Group.**

Matrix groups can be finite or infinite. We looked at some finite ones in the last tutorial. As always with finite groups, the best way to deal with them is to make a Cayley Table.

With infinite matrix groups we have to work with properties of the elements. We will look at the most important matrix group, namely the group of all invertible $n \times n$ matrices with real entries. This is called the **General Linear Group** and denoted by $\mathrm{GL}_n(\mathbb{R})$ We'll need to recall a few results from MSO1110 *Vectors and Matrices.*

Properties of Matrices

(a) The set of $n \times n$ matrices over $\mathbb{R}$ contains a special matrix I_n which is

an identity for multiplication:

$$XI_n = I_nX = X$$

for any $n \times n$ matrix X. I_n has ones on the diagonal and zeros everywhere else, for example

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(b) An $n \times n$ matrix A is said to be **invertible** if there exists an $n \times n$ matrix B such that

$$AB = BA = I_n.$$

(c) There is a real-valued function $\det$ which associates every $n \times n$ matrix A with its **determinant** $\det(A)$. A matrix A is invertible if and only if

$$\det(A) \neq 0.$$

(c) The determinant is a multiplicative function; this means that for all $n \times n$ matrices A and B we have

$$\det(AB) = \det(A)\det(B).$$

Property (c) above allows us to make the following definition:

Definition 4.3

The **general linear group** $\mathrm{GL}_n(\mathbb{R})$ is the set of real $n \times n$ matrices with nonzero determinant.

Theorem 4.2

The general linear group $\mathrm{GL}_n(\mathbb{R})$ is a group under matrix multiplication.

Proof. First, we must show that matrix multiplication is a binary operation on $\mathrm{GL}_n(\mathbb{R})$. In other words, the product of two invertible $n \times n$ matrices is an invertible $n \times n$ matrix.

Let A and B be invertible $n \times n$ matrices. Then AB is an $n \times n$ matrix. We have

$$\det(A) \neq 0 \text{ and } \det(B) \neq 0.$$

So

$$\det(AB) = \det(A)\det(B) \neq 0$$

which shows that AB is invertible.

Now we check the axioms:

- **Associativity:** Matrix multiplication is associative.
- **Identity:** We have
$$\det(I_n) = 1 \neq 0.$$
So $I_n \in \mathrm{GL}_n(\mathbb{R})$. As I_n is an identity for the set of all $n \times n$ matrices, it is an identity in $GL_n(\mathbb{R})$.
- **Inverses:** Every element of $\mathrm{GL}_n(\mathbb{R})$ has an inverse by property (c) above. Let $A \in \mathrm{GL}_n(\mathbb{R})$ and denote its inverse by A^{-1}. Then
$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1})$$
which shows that $\det(A^{-1}) \neq 0$. In particular, $A^{-1} \in \mathrm{GL}_n(\mathbb{R})$.

□

Remark. In general, if a matrix group contains I_n then this is the identity in the group. Not every matrix group contains I_n, though. See Exercise **??** for an example.

4.5 Tutorial - investigating groups of units

In today's lecture, we introduced the groups $\mathbb{Z}_n^\times$ for various values of n. In the tutorial we will take closer look at these groups. The purpose of this is two-fold: firstly to practise modular arithmetic, and second to improve your research skills.

First a quick reminder: the elements of $\mathbb{Z}_n^\times$ are the numbers which are less than n and coprime to n. So for example

$$\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$$

and

$$\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$$

Now a new idea: an element $x \in \mathbb{Z}_n^\times$ is called a **generator** if every element of $\mathbb{Z}_n^\times$ can be written as a power of x. So for example

- 3 is a generator of $\mathbb{Z}_{10}^\times$, because

$$\begin{aligned} 3^0 &= 1 \mod 10 \\ 3^1 &= 3 \mod 10 \\ 3^2 &= 9 \mod 10 \\ 3^3 = 27 &= 7 \mod 10. \end{aligned}$$

- $\mathbb{Z}_{12}^\times$ has no generator, because

$$\begin{aligned} 5^0 &= 1 \mod 12 \\ 5^1 &= 5 \mod 12 \\ 5^2 = 25 &= 1 \mod 12 \ldots \end{aligned}$$

$$\begin{aligned} 7^0 &= 1 \mod 12 \\ 7^1 &= 7 \mod 12 \\ 7^2 = 49 &= 1 \mod 12 \ldots \end{aligned}$$

$$\begin{aligned} 11^0 &= 1 \mod 12 \\ 11^1 &= 11 \mod 12 \\ 11^2 = 121 &= 1 \mod 12 \ldots \end{aligned}$$

Exercise 4.3

(a) For a range of values of n (say, 3-20) write down all the elements of $\mathbb{Z}_n^\times$. Make a note of how many there are for each n. Can you spot any general patterns?

(b) For which values of n in your range does $\mathbb{Z}_n^\times$ have a generator? For which larger values of n would you expect $\mathbb{Z}_n^\times$ to have a generator?

(c) Make a note of anything else interesting you discover.

Remark. This exercise is deliberately left open-ended, and it's up to you where you go with it. However, it's worth considering the *prime decomposition* of n in your investigations - what happens if n is prime? or a power of a prime? or a product of two distinct primes?

4.6 Homework Exercises

This week's homework focuses on the second part of the lecture - infinite groups. When proving something is a group, I suggest you stick to the model suggested in Section 4.3. Your proofs should contain enough detail to be understood by a student from another university who recently started studying group theory.

Exercise 4.4

Prove that the set of all integers divisible by 3 is a group under addition.

Exercise 4.5

Let G be the set of $n \times n$ real matrices with determinant 1. G is called the **special linear group**, or $\mathrm{SL}_n(\mathbb{R})$ for short.

Prove that G is a group under matrix multiplication. You may quote any result on matrices you need provided you state it clearly.

Exercise 4.6

In Exercise 2.7 you proved that the set G of all $n \times n$ matrices of the form

$$\begin{pmatrix} x & -x \\ -x & x \end{pmatrix}$$

where $x \in \mathbb{R}\backslash\{0\}$ is a group under matrix multiplication.

Now let I be the 2×2 identity matrix. The set $\{I\} \cup G$ is closed under matrix multiplication. Why is it *not* a group?

Chapter 5

Cyclic Groups

5.1 Introduction

Exercise 5.1: Definition Quiz

(a) For any n, $\mathbb{Z}_n^\times$ is a group. What are the elements and what is the binary operation?

(b) For any n, $\mathrm{GL}_n(\mathbb{R})$ is a group. What are the elements and what is the binary operation?

In yesterdays tutorial we saw that some groups of units are generated by a single element, e.g.

- 2 is a generator of $\mathbb{Z}_5^\times$, because

$$\begin{aligned} 2^0 &= 1 \mod 5 \\ 2^1 &= 2 \mod 5 \\ 2^2 &= 4 \mod 5 \\ 2^3 = 8 &= 3 \mod 5. \end{aligned}$$

  and $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$.

- $\mathbb{Z}_8^\times$ has no generator, because $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ and

$$\begin{aligned} 3^0 &= 1 \mod 8 \\ 3^1 &= 3 \mod 8 \\ 3^2 = 9 &= 1 \mod 8 \ldots \end{aligned}$$

$$\begin{aligned} 5^0 &= 1 \mod 8 \\ 5^1 &= 5 \mod 8 \\ 5^2 = 25 &= 1 \mod 8 \ldots \end{aligned}$$

$$\begin{aligned} 7^0 &= 1 \mod 8 \\ 7^1 &= 1 \mod 8 \\ 7^2 = 49 &= 1 \mod 8 \ldots \end{aligned}$$

We can extend this idea to other groups too:

Example 5.1.

- The group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition modulo 4 is generated by a single element 1, because

$$\begin{aligned} 0 &= && 0 \times 1 \mod 4 \\ 1 &= 1 = && 1 \times 1 \mod 4 \\ 2 &= 1 + 1 = && 2 \times 1 \mod 4 \\ 3 &= 1 + 1 + 1 = && 3 \times 1 \mod 4 \end{aligned}$$

- The group $\{1, -1, i, -i\}$ under multiplication is generated by a single element i, because

$$\begin{aligned} i^0 &= 1 \\ i^1 &= i \\ i^2 &= -1 \\ i^3 &= -i \end{aligned}$$

We have a name for groups like this:

Definition 5.1

Let G be a group. We say G is **cyclic** if there exists $g \in G$ with the following property:

For all $h \in G$ there exists $k \in \mathbb{Z}$ such that $h = g^k$.

We say g **generates** G.

5.2 Examples of cyclic groups

We've shown in today's lecture that $\mathbb{Z}_5^\times$, $\mathbb{Z}_4$ under addition modulo 4, and $\{1, -1, i, -i\}$ under multiplication are examples of cyclic groups. Note that these are all finite groups. There is one very important example of an infinite cyclic group:

Example 5.2. $\mathbb{Z}$ is a cyclic group under addition, generated by 1.

This is because every element of $\mathbb{Z}$ can be written as

$$n = 1 \times n = \underbrace{1+1+1+1+\ldots+1}_{n \text{ times}}$$

or

$$-n = 1 \times (-n) = \underbrace{(-1)+(-1)+(-1)+(-1)+\ldots+(-1)}_{n \text{ times}}.$$

Both parts of Example 5.1 can be generalised:

Example 5.3. The group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under addition modulo n is cyclic, generated by 1.

Example 5.4. Recall from MSO1110 *Vectors and Matrices* that an n**th root of unity** is a complex number z which satisfies the equation

$$z^n = 1.$$

The set of nth roots of unity is, in complex exponential form

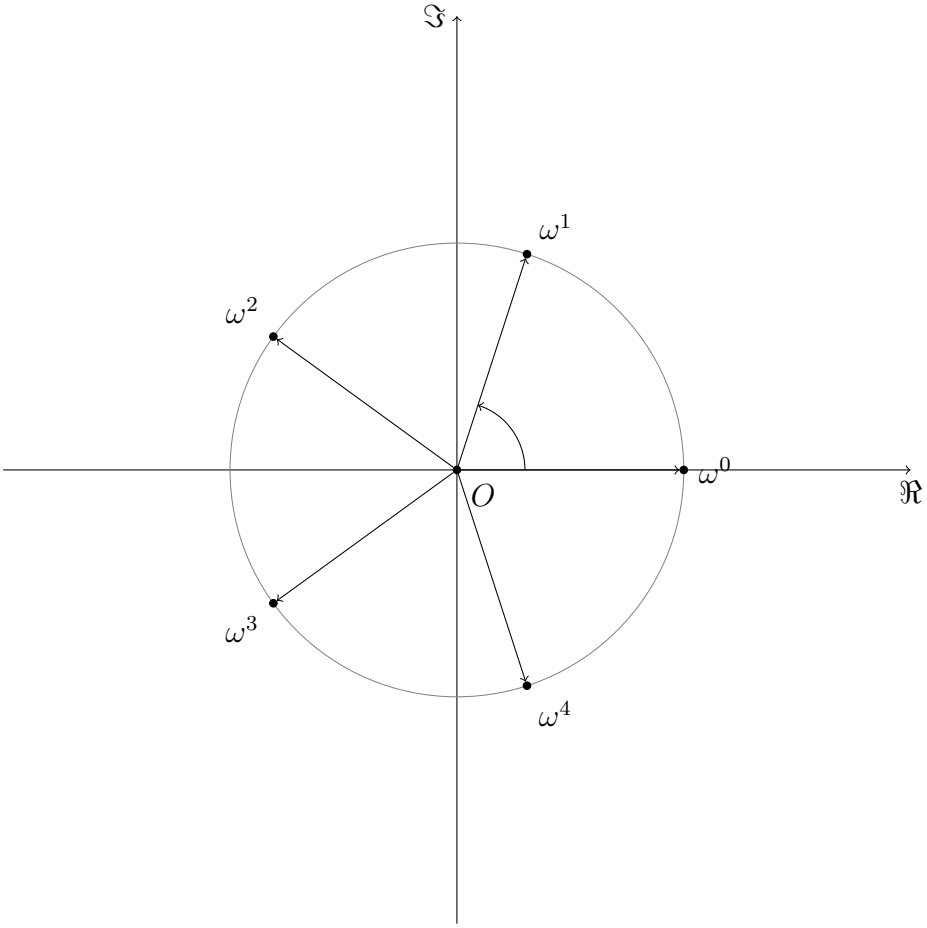
$$\{e^{\frac{2\pi ik}{n}} : k = 0, 1, \ldots, n-1\}.$$

These form a group U_n under multiplication. It is a cyclic group, generated by $\omega = e^{\frac{2\pi i}{n}}$, because for each $k = 0, 1, \ldots, n-1$ we have

$$e^{\frac{2\pi ik}{n}} = (e^{\frac{2\pi i}{n}})^k = \omega^k.$$

The group $\{1, -1, i, -i\}$ is of course U_4.

Here is a picture of U_5.



5.3 Properties of cyclic groups

In this section we will use the definition of a cyclic group, and the group axioms, to investigate cyclic groups. Remember, because we're proving directly from definitions and axioms, whatever we prove in this section is true for every single cyclic group.

The first thing we will prove is

Proposition 5.1. *Every cyclic group is abelian.*

Proof. Let G be a cyclic group generated by g. Let $a, b \in G$. We have to show that

$$ab = ba.$$

Now because G is cyclic, there exists an integer k and an integer l such that

$$g^k = a \quad \text{and } g^l = b.$$

Therefore

$$\begin{aligned} ab &= g^k g^l \\ &= g^{k+l} && \text{by Proposition 2.2} \\ &= g^{l+k} \\ &= g^l g^k && \text{by Proposition 2.2 again} \\ &= ba. \end{aligned}$$

This shows that G is abelian as required. □

Note that the converse of this result is not true, i.e. not every abelian group is cyclic. A counterexample is provided by $\mathbb{Z}_8^\times$ (see introduction to this lecture) amongst many others.

Finite cyclic groups

Let G be a finite cyclic group with generator g. Then as every element of G can be written as a power of g, we can write

$$G = \{e = g^0, g^{k_1}, g^{k_2}, \ldots\}.$$

In all the examples we've looked at so far, we were able to take the powers k_i to be positive numbers less than $|G|$. For example, in $\mathbb{Z}_{10}^\times$ we had

$$G = \{1 = 3^0, 3 = 3^1, 9 = 3^2, 7 = 3^3\}.$$

We will now show that this always happens:

Exercise 5.2

Let G be a cyclic group with generator g. Suppose $g^{k_1} = g^{k_2}$ with $k_1 > k_2$. Show that

$$g^{k_1 - k_2} = e.$$

Hint: use left or right cancellation (Proposition 2.4).

Now suppose G is a *finite* cyclic group. Then the elements

$$\{e, g, g^2, g^3, \ldots\}$$

can't all be *different*, otherwise there would be an infinite number of elements. Consequently, there are a pair of powers (say k_1 and k_2) such that $g^{k_1} = g^{k_2}$. The proposition above now implies there exists an integer k with the following property:

$$k > 0 \text{ is the smallest positive integer such that } g^k = e.$$

k may be equal to $k_1 - k_2$, or it may be smaller. k is called the **order** of g.

Proposition 5.2.

Let G be a finite cyclic group with generator g of order k. Then every element of G can be written as g^r where

$$0 \leq r \leq k - 1.$$

Proof. Let $h \in G$. Since G is cyclic with generator G, h can be written as g^t for some $t \in Z$. By division with remainder (note that this also works for *negative* values of t), we can write

$$t = qk + r \qquad \text{for some } q, r \in \mathbb{Z}, 0 \leq r \leq k - 1.$$

Now we have

$$\begin{aligned} h &= g^t \\ &= g^{qk+r} \\ &= (g^k)^q g^r \text{ by Proposition 2.2} \\ &= e^q g^r \\ &= g^r. \end{aligned}$$

As $0 \leq r \leq k - 1$ we have proved our result.

□

Now the elements $\{e, g, g^2, \ldots, g^{n-1}\}$ must all be different, otherwise there is a value of $k < n$ such that $g^k = e$ by the result of Exercise 5.3. So we have shown

Theorem 5.1

Let G be a cyclic group with generator g of order n. Then

$$G = \{e, g, g^2, \ldots, g^{n-1}\}.$$

In particular, the order of G is n.

One consequence is the following. Let G and H be cyclic groups of the same order. Take g to be a generator of G and h to be a generator of H. Then

$$G = \{e, g, g^2, \ldots, g^{n-1}\} \text{ and } H = \{e, h, h^2, \ldots, h^{n-1}\}.$$

It's easy to see now that if we write the elements of G and H in this order, they will have the same Cayley table, except that the elements will be labelled by g^i or h^i respectively. In particular we have shown

Theorem 5.2

Any pair of cyclic groups of the same order are isomorphic. Any cyclic group of order n is isomorphic to the group $\mathbb{Z}_n$ of integers modulo n under addition.

5.4 Order of Elements

We defined the **order** of a generator of a cyclic group in the last section. But this idea can be extended to any element of any group:

Definition 5.2

Let G be a group and $g \in G$. Then the **order** of G is the smallest positive integer $k > 0$ such that $g^k = e$.

The order of g in G is sometimes denoted by $|g|$.

Remark. Try not to confuse the *order of an element* $|g|$ with the *order of the group* $|G|$, which is the number of different elements in G. There is a reason we use the same word for both, but they're not generally the same.

Example 5.5. We consider once more the group $\{1, -1, i, -i\}$ under multiplication. This is cyclic of order 4. We find the order of each element:

- 1 is the identity, which has order 1.
- -1 has order 2, since $(-1)^1 = -1 \neq 1$, $(-1)^2 = 1$.
- i has order 4, since $i^1 = i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$, $i^4 = 1$.
- $-i$ has order 4, since $(-i)^1 = -i \neq 1$, $(-i)^2 = -1 \neq 1$, $i^3 = -i \neq 1$, $i^4 = 1$.

Exercise 5.3

Find the order of each element of the following groups:

(a) The group $\mathbb{Z}_9$ of integers under addition modulo 9;

(b) The group $\mathbb{Z}_{14}^{\times}$ of integers coprime to 14 under multiplication modulo 14 (refer back to Exercise 4.5 if you need to).

What do you notice about the orders which appear?

5.5 Tutorial: More About Isomorphisms

Recall that a pair of finite groups G and H are said to be **isomorphic** if they have the same Cayley Table, possibly after reordering rows and columns and relabling rows.

You should think of isomorphic groups as having the same structure, even if they arise in different contexts.

It can be hard to determine whether a pair of given groups are isomorphic. However, if two groups are isomorphic, they have to share most of the characteristics we've studied in this course. Obviously we have

If G and H are isomorphic groups, then G and H have the same order.

The converse statement is not true. Let H be the set $\{1, -1, i, -i\}$ under multiplication and let G be the set of matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \quad D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

You should in Exercise 3.5 that these groups are not isomorphic.

More generally suppose G and H have the same order. Then we have

If G and H are isomorphic groups and G is cyclic, then H is cylic.

The converse is of course Theorem 5.3.

We also have

If G and H are isomorphic groups and G is abelian, then H is abelian.

Again the converse is not true. The non-isomorphic groups of order 4 above are both abelian.

More generally still we have

If G and H are isomorphic groups, then they have the same number of elements of every given order.

This is probably the best way to show that a pair of groups are not isomorphic.

Example 5.6.

We show that the groups G and H on the last page are not isomorphic.

The orders of elements in H were found in Example 5.5. The list of orders was

$$\{1, 2, 4, 4\}.$$

On the other hand the orders occuring in G are

$$\{1, 2, 2, 2\}$$

because $B^2 = C^2 = D^2 = A$ and A is the identity. So G and H are not isomorphic.

Exercise 5.4

Consider the set of 8 matrices $G = \{\pm E, \pm I, \pm J, \pm K\}$ where

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

You showed in Exercise 3.5 that they form a non-abelian group of order 8 under matrix multiplication.

Now let H be the group of symmetries of a square. This is also a non-abelian group of order 8.

(a) List the elements of H and their orders.

(b) List the order of each element of G, and hence deduce that G and H are not isomorphic.

Remark. Even if two groups have the same number of elements of each order, and are both abelian/both non-abelian, it still doesn't mean they are isomorphic. There are two non-abelian groups of order 27, with the same number of elements of each order in each, which are not isomorphic.

Homework Exercises

The first two exercises are a good way to check if you understand the definitions of **cyclic group** and **order**. As usual, aim to put enough detail in your proofs that a student at another university could understand your argument.

Exercise 5.5

Let G be a group with identity e and let $g \in G$. Suppose $g^n = e$. Prove that n is divisible by the order of g.

Hint: use division with remainder.

Exercise 5.6

Prove that the set of matrices of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ where $n \in \mathbb{Z}$ is a group under matrix multiplication. Is it a cyclic group?

Exercise 5.7

Let G be a group in which $x^2 = e$ for all $x \in G$. Prove that G is abelian.

Hint: let $a, b \in G$ and consider $abab$.

Fact: the order of every element of a finite group divides the order of the group. You will prove this next term.

Exercise 5.8

Using the previous exercise and the fact above:

(a) Deduce that every group of order 4 is abelian;

(b) Prove that every group of order 4 is either cyclic or isomorphic to the matrix group

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Chapter 6

Subgroups and generating sets

6.1 Introduction

Exercise 6.1: Definition Quiz

(a) Let G be a group. What does it mean to say that G is **cyclic**?

(b) Let $g \in G$. What is meant by the **order** of g?

The prefix *sub* means "under". It is used in many places in mathematics.

- In MSO1130 *Logic and Structures* you learned that a **subset** of a set S is a set T such that every element of T is contained in S. We write $T \subseteq S$ for "T is a subset of S."

- in MSO1110 *Vectors and Matrices* you learned that a **subspace** of a vector space V is a subset W of V which is also a vector space, under the same notions of addition and scalar multiplication.

In view of this, the next definition should not be surprising:

Definition 6.1

Let G be a group under a binary operation $\star$. We say H is a **subgroup** of G if:

1. H is a subset of G;

   and

2. H is a group under $\star$.

So, a subgroup of a group is a subset which is also a group under the same binary operation.

We sometimes write $H \leq G$ for "H is a subgroup of G".

You have already seen lots of examples of subgroups:

Example 6.1.

You saw in Example 5.1 and many times since that the set

$$G = \{1, -1, i, -i\}$$

is a group under multiplication.

You also saw in Example 2.2 that $H = \{-1, 1\}$ is a group under multiplication.

As H is clearly a subset of G, we conclude that H is a subgroup of G.

Example 6.2.

You proved in Theorem 4.2 that

$$\mathrm{GL}_n(\mathbb{R}) = \{n \times n \text{ matrices } A : \det(A) \neq 0\}$$

is a group under multiplication.

You also saw in Exercise 4.5 that

$$\mathrm{SL}_n(\mathbb{R}) = \{n \times n \text{ matrices } A : \det(A) = 1\}$$

is a group under multiplication.

As H is clearly a subset of G, we conclude that H is a subgroup of G.

Example 6.3.

You saw in Example 2.1 and many times since that $\mathbb{Z}$ is a group under addition

You also saw in Example 4.2 that the set of even integers is a group under addition.

As this is clearly a subset of $\mathbb{Z}$, we conclude that the set of even integers is a subgroup of $\mathbb{Z}$ under addition.

Note that in Example 6.1, H is not the only subgroup. In addition:

- G is a subgroup of itself;
- The set $\{1\}$ (with just one element, the identity) is a subgroup of G.

A group is always a subgroup of itself, because a set is always a subset of itself.

Recall that a set T is said to be a **proper subset** of S if $T \subseteq S$ and $T \neq S$. Accordingly, we say H is a **proper subgroup** of G if $H \leq G$ and $H \neq G$.

We sometimes write $H < G$ for "H is a proper subgroup of G".

In addition, if $e \in G$ is the identity, then $\{e\}$ is a subgroup of G. This is called the **trivial subgroup** of G.

Usually we're most interested in the the other subgroups of a given group - i.e. the **proper nontrivial** subgroups.

Exercise 6.2

You know that the following four matrices form a group G under multiplication:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Find all the subgroups of G.

6.2 The subgroup test

In order to *prove* that a given set H is a subgroup of a group G, it is necessary to prove that H is a subset of G, and H is itself a group under the same binary operation as in G.

The first of these is usually easy. Once we know that H is a subset of G, we can take some shortcuts to proving H is a group. These are summed up neatly in

Theorem 6.1: The Subgroup Test

Let G be a group with identity e, and suppose H is a subset of G. Suppose the following conditions all hold:

1. H is **closed**: that is, $ab \in H$ for all $a, b \in H$;
2. $e \in H$;
3. H is **closed under taking inverses:** that is, for all $h \in H$ we also have $h^{-1} \in H$, where h^{-1} denotes the inverse of h in G.

Then H is a subgroup of G.

Proof. We already know $H \subseteq G$, so it remains to show H is a group. We use the axioms as usual.

- **Binary Operation:** Condition (1) is equivalent to the binary operation on G also being a binary operation on H.
- **Associative:** The binary operation on G is associative, so remains so on H.
- **Identity:** Condition (2) ensures H contains an identity.
- **Inverses:** Condition (3) ensures that every element of H has an inverse.

□

Remark. There's really not much to this proof. The subgroup test isn't anything profound, it's just a formal way of recognising that if we already know $H \subseteq G$, we don't need to bother checking associativity and it's enough that H contains the identity and inverses we already know exist in G.

Example 6.4. We revisit the proof that $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. This is basically the same as Exercise 4.5, but the proof is a little shorter.

Proof. We use the subgroup test. Clearly $\mathrm{SL}_n(\mathbb{R}) \subseteq \mathrm{GL}_n(\mathbb{R})$.

- **Closure:** Let $A, B \in \mathrm{SL}_n(\mathbb{R})$. Then

  $$\det(A) = 1 \text{ and } \det(B) = 1.$$

  So

  $$\det(AB) = \det(A)\det(B) = 1 \times 1 = 1$$

  so $AB \in \mathrm{SL}_n(\mathbb{R})$ as required.

- **Identity:** I_n is the identity in $\mathrm{GL}_n(\mathbb{R})$. We have $\det(I_n) = 1$, so $I_n \in \mathrm{SL}_n(\mathbb{R})$.
- **Closed under taking inverses:** Let $A \in \mathrm{SL}_n(\mathbb{R})$ and denote its inverse in $\mathrm{GL}_n(\mathbb{R})$ by A^{-1}. Then

  $$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = 1 \times \det(A^{-1}) = \det(A^{-1})$$

  which shows that $\det(A^{-1}) = 1$. Therefore, $A^{-1} \in \mathrm{SL}_n(\mathbb{R})$.

Therefore $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$. □

6.3 Generating Sets

Let G be a group and let $g \in G$. Consider the following set:

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\}.$$

i.e. the set of all elements in G which are powers of g.

It's easy to show that $\langle g \rangle$ is a subgroup of G. In fact, a *cyclic* subgroup of G, generated by g.

Notice that G is generated by g if and only if

$$\langle g \rangle = G,$$

and, in that case, G is a cyclic group.

This gives us an easier way to describe some subgroups: for example, in Exercise 6.2, the 5 subgroups of the matrix group $\{A, B, C, D\}$ were

$$\{A\}, \langle B\rangle, \langle C\rangle, \langle D\rangle, \text{ and the whole group.}$$

We can take this idea further. Let G be a group and let S be a *subset* of G. Then we define $\langle S\rangle$ to be the set of "words" in the "alphabet" consisting of the elements of S and their inverses.

For example, if $S = \{a, b\}$ then the elements of $\langle S\rangle$ are things like

$$abbba^{-1}ba^{-1}a^{-1}b^{-1}babb$$

which would usually be simplified to

$$ab^3a^{-1}ba^{-2}ab^{-2}.$$

Remark. If G is abelian then

$$\langle a, b\rangle = \{a^ib^j : i, j \in \mathbb{Z}\};$$

Or with 3 elements

$$\langle a, b, c\rangle = \{a^ib^jc^k : i, j, k \in \mathbb{Z}\};$$

and so on.

If G is also finite, then the exponents can be taken to be non-negative.

For any subset $S \subseteq G$, $\langle S \rangle$ is a subgroup of G. In fact, it is the smallest subgroup of G containing S.

If $\langle S \rangle = G$ we say G **is generated by** S. We also say that S **is a generating set for** G.

6.4 Non-cyclic groups

A group G is cyclic if and only if it has a generating set consisting of just one element. Many non-cyclic groups have generating sets consisting of only a small number of elements.

Example 6.5.

Consider

$$\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$$

under multiplication modulo 8. We showed in chapter 5 that this is not a cyclic group, because

$$\begin{aligned} 3^0 &= 1 \mod 8 \\ 3^1 &= 3 \mod 8 \\ 3^2 = 9 &= 1 \mod 8 \ldots \end{aligned}$$

$$\begin{aligned} 5^0 &= 1 \mod 8 \\ 5^1 &= 5 \mod 8 \\ 5^2 = 25 &= 1 \mod 8 \ldots \end{aligned}$$

$$\begin{aligned} 7^0 &= 1 \mod 8 \\ 7^1 &= 1 \mod 8 \\ 7^2 = 49 &= 1 \mod 8 \ldots \end{aligned}$$

i.e. no element of $\mathbb{Z}_8^\times$ generates the group on its own.

Notice, however, that

$$7 = 3 \times 5 \mod 8.$$

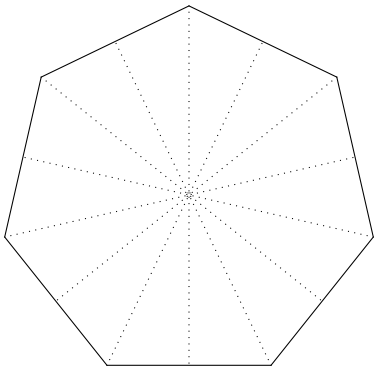
So 7 lies in the subgroup generated by 3 and 5. As this also contains 1 by definition, we have

$$\mathbb{Z}_8^\times = \langle 3, 5 \rangle$$

i.e. $\{3, 5\}$ is a generating set for $\mathbb{Z}_8^\times$.

Example 6.6.

Let $n \geq 3$ and consider a regular n-gon (the picture below is a 7-gon or heptagon):



The regular n-gon has n lines of symmetry, one through each vertex and the centre as shown in the diagram. The reflection in any one of these lines is a symmetry of the n-gon.

There are also $n-1$ different rotations which are symmetries of the n-gon. A rotation about the center of an angle $2\pi k/n$ radians is a symmetry for any value of $k = 1, 2, \ldots, n-1$. For example, the rotation of $2\pi/n$ radians anticlockwise moves each edge onto the next edge in an anticlockwise direction.

Finally, the identity is a symmetry (we could consider this a rotation of 0 radians). This gives $2n$ symmetries in total.

The symmetries of an n-gon form a group G under composition. It is not a cyclic group, because the order of any rotation is at most n and the order of any reflection is 2. So there is no element of order $2n$.

Now let τ be an anticlockwise rotation of $2\pi/n$ radians about the origin. And let σ be any of the n reflections through lines of symmetry.

Then the n reflections are

$$\sigma, \sigma\tau, \sigma\tau^2, \ldots, \sigma\tau^{n-1}$$

and the $n-1$ rotations are

$$\tau, \tau^2, \tau^3, \ldots, \tau^{n-1}.$$

Thus,

$$\langle \tau, \sigma \rangle = G$$

i.e. G is generated by the 2 element set $\{\sigma, \tau\}$.

The group G is called the **dihedral group** of order $2n$. It is not an abelian group, because

$$\sigma\tau = \tau^{n-1}\sigma \neq \tau\sigma.$$

6.5 Tutorial: subgroups and Hasse diagrams

In this lecture we learned about subgroups. We saw the complete list of subgroups of a cyclic group of order 4 (Example 6.1) and of another group of order 4 (Exercise 6.2).

We didn't say much about how to find subgroups. This is because there isn't really a well-defined method, beyond checking subsets of a given group. However, the following two facts (which we've yet to prove) are very useful:

Fact one: every subgroup of a cyclic group is cyclic.

Fact two (Lagrange's Theorem): the order of every subgroup of a group G divides the order of G.

Let's look yet again at the group $G = \{A, B, C, D\}$ where

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

A is the identity in this group, so $\{A\}$ is a (trivial) subgroup of G. G is a subgroup of itself. Are there any more?

Well, every subgroup of G must contain A. And Lagrange's theorem tells us G

has no subgroups of order 3, because this is not a factor of 4. So the only possible subgroups are $\{A, B\}$, $\{A, C\}$ and $\{A, D\}$. We check (using the subgroup test) that these are indeed subgroups.

Exercise 6.3

Find all subgroups of the following additive groups (which are cyclic):

(a) $\mathbb{Z}_8$;

(b) $\mathbb{Z}_9$.

Exercise 6.4

For the following groups of units, find a generating set and hence find all subgroups of the given group:

(a) $\mathbb{Z}_9^\times$;

(b) $\mathbb{Z}_{12}^\times$.

(c) $\mathbb{Z}_{15}^\times$.

Exercise 6.5

Find all subgroups of:
(a) The group of symmetries of a triangle.
(b) The group of symmetries of a square.

Note that you've done calculations with all these groups before. You might find it helpful to have those calculations in front of you.

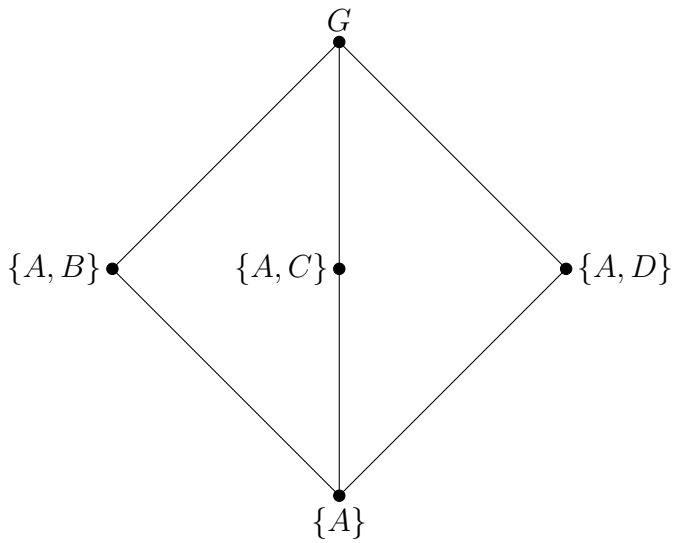
6.5.1 Hasse diagrams

If G is a finite group and H a subgroup of G, then it's possible that H has subgroups of its own. These in turn, are also subgroups of G.

The set of all subgroups of a finite group G, and the data about which ones are subgroups of which other ones, is called the **subgroup lattice** of G.

This information can be recorded in a picture called a **Hasse diagram**. This is a graph with a node labeled by each subgroup of G, and two subgroups joined by an edge if one contains the other. Usually we put the group G at the top, and the larger the order of a subgroup, the higher in the picture it goes.

Here, for example, is the Hasse diagram for the group $\{A, B, C, D\}$ we considered earlier:



Exercise 6.6

Draw the Hasse diagram for the subgroup lattice of each of the groups in Exercises 6.3 - 6.5.

Homework Exercises

The rest of the questions are homework. They mainly focus on using the definition of subgroup to prove theorems.

Exercise 6.7

In section 6.1 we claimed that, for any group G, the set $\{e\}$ is a subgroup of G.
Prove this assertion using the subgroup test.

Hint: this question is easy. But somehow, it's so easy that it passes through the vortex of easy and becomes confusing again...

The key is writing down what the three parts of the subgroup test actually mean when applied to the subset $\{e\}$. Once you've done that, the three statements you need to prove are either vacuous or proved elsewhere in this text. You can quote references if you'd rather not prove them again.

Exercise 6.8

Prove that the *converse* of the subgroup test (Theorem 6.1) is also true. That is, prove that if $H \leq G$ then the three conditions

1. **Closure:** $ab \in H$ for all $a, b \in H$,
2. **Identity:** $e \in H$, where e is the identity in G,
3. **Inverses:** If $h \in H$ then $h^{-1} \in H$, where h^{-1} is the inverse of h in G,

must all hold.

Exercise 6.9

Prove that every subgroup of a cyclic group is cyclic.

Hint: let G be a cyclic group generated by g and let H be a subgroup of G. Then every element of H can be written as a positive power of g. Thus

$$H = \{e, g^{k_1}, g^{k_2}, g^{k_3}, \dots, \}$$

with $k_1, k_2, k_3, \dots$ integers. What element of H do you think is a generator for H? Can you prove it?

Exercise 6.10

Let G be a group and let K and H be subgroups of G. Show that $H \cap K$ is a subgroup of G.

Is the same true of $H \cup K$?