Algebra for Joint Honours

MATH1203

Last updated on April 16, 2013

These are the online notes for the course MATH1203 at UCL. They are typeset by Niko Laaksonen, but are heavily based on lecture notes from previous years. Please notice that not everything in these notes is examinable and, more precisely, these notes are not in 1–to–1 correspondence with what has been written in lectures. However, for the most part, these notes should be a good source for self-studying and complementing your own notes and understanding.

If you notice any typos or other mistakes (as I'm sure there will be aplenty) please drop me an email at n.laaksonen@ucl.ac.uk.

Contents

Chapter 1

Sets and Relations

1.1 Sets

We will begin by introducing basic (naive) set theory. It will be an underlying concept throughout the rest of the course. Naturally, in order to get started we need to have some notion of what a set actually is. The most common "definition" of a set is that it is a *collection of elements*. There are various problems with this approach. What exactly then is a *collection*? Brushing that under the carpet, let's suppose that anything that we could sensibly call a *collection* would be a set. Now, consider the set which contains all sets that are not members of themselves (this is to avoid so called "non-sets")[1]. It's a collection of "things" so surely it should be a well-defined set. There's a subtle problem here, though. If S is the set of all sets then is S a member of itself? If it's not then S cannot be the set of all sets as it does not contain the set S. However, if S is a member of itself then this contradicts the definition of S as a set of all sets that are not members of itself. Ouch! By the way, this is called Russell's paradox and historically led

[1]Consider, for example, the set of all weekdays. Of course this set is not a member of itself as it is not a weekday. However, if you take the set of non-weekdays (anything that is not a weekday) then the set is a member of itself as it is not a weekday. We wish to avoid this kind of funky sets.

into a more rigorous approach to logic and set theory. You can read more at `http://en.wikipedia.org/wiki/Russell's_paradox`.

After the initial headache it should be clear that we are treading on thin ice here. In order to make progress, however, we'll leave the details for another time and just take the notion of a set for granted. Generally we'll use capital letters like X, Y, S to denote sets and small letters x, y, s to denote **elements** (or **members**) of these sets. Furthermore, if x is an element of X, we write

$$x \in X.$$

Conversely, if y is not an element of X then we write

$$y \notin X.$$

There are various ways we can define any particular set S. The simplest one is just by listing all the elements of the set. Say, for example, that S is the set with elements 1, 2, 3 and k. Then we could write this as

$$S = \{1, 2, 3, k\},$$

whatever the value of k might be. Notice that repetition does not matter with sets (don't confuse this with ordered sets where repetition *does* matter). In other words, the set

$$\{1, 1, 2, 3, k, 3, k\}$$

would still be the same set as S. Alternatively, one can describe the elements of a set by a list of conditions. For example, the set of positive real numbers could be written as

$$\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\},$$

where the colon is read as "such that". The set of all even numbers could be written as

$$2\mathbb{Z} = \{n \in \mathbb{Z} : n = 2m \text{ for some } m \in \mathbb{Z}\}.$$

A particular set of importance is the set which does not have any elements. One could write $\{\}$ for this, but it would quickly get confusing (consider e.g. $\{\{\}, \{\{\}, \{\{\}, \{\}\}\}, \{\{\}\}\}$). Hence it makes sense to give this kind of a

set a special symbol. Thus we define the **empty set** to be the set with no elements (there is exactly 1 such set) and denote it by

$$\emptyset.$$

Most of mathematics is about establishing a common language so as to enable us to have meaningful conversations about abstract concepts that are independent of personal interpretation. In order to work with sets, we need ways for them to interact. In other words, we need to define operations on sets (like your usual operations of *addition*, *subtraction* etc. on integers).

Definition 1.1. Let A, B be two sets.

i) We say that B is a **subset** of A, denoted by $A \subseteq B$ (or $B \supseteq A$, or $B \subset A$ etc.), if every element of B is an element of A. Mathematically we would write

$$B \subseteq A \iff \forall x \in B, x \in A.$$

If we wish to insist that B is a subset of A, but not equal to A then we write[2] $B \subsetneq A$.

Note: Each nonempty set A has at least two subsets, $A \subseteq A$ and $\emptyset \subseteq A$.

ii) The **union** of A and B is the set of all elements which are members of A or B (or both). We denote this by $A \cup B$. So we could write that

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

iii) The **intersection** of A and B is the set whose elements belong to both A and B, and is denoted by $A \cap B$. Hence,

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

[2]Notice that some people might use $B \subset A$ for this meaning. We will not do that however as it leads to confusion easier. For us $\subset$ and $\subseteq$ are synonymous.

iv) The **difference** of A and B is the set whose elements belong to A, but not to B. We denote this by $A \setminus B$ (some people use the usual minus sign and write $A - B$). In other words,

$$A \setminus B = \{x : x \in A, x \notin B\}.$$

Note: $A \setminus B \neq B \setminus A$ in general.

v) Let Ω be the *universal set*[3]. The **complement** of A, $A \subseteq \Omega$, (in Ω) is defined as

$$A^{\mathsf{c}} = X \setminus A,$$

that is, everything in X that is not in A.

Note: By using the complement we can write that $A \setminus B = A \cap B^{\mathsf{c}}$.

vi) Finally, the **cartesian product** (or **cross product**) of A and B, $A \times B$, is the set of all ordered pairs[4] of elements where the first element is from A and the second from B. Thus,

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Let's look at some examples.

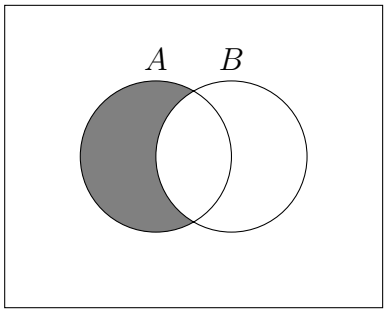
Example. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{4, 5, 6\}$. Then we have the following,

$$\begin{aligned}
&\{1, 2\} \subseteq A, && A \cup B = \{1, 2, 3, 4, 5, 6\},\\
&A \cap B = \{4, 5\}, && A \setminus B = \{1, 2, 3\},\\
&B \setminus A = \{6\}, && A \times B = \{(1, 4), (1, 5), (1, 6), (2, 4),\\
&B \subsetneq A, && \qquad (2, 5), \ldots, (5, 4), (5, 5), (5, 6)\}.
\end{aligned}$$

[3]We think of the universal set as a set inside which all of our sets live in. It varies from time to time, but is always clear from the context. For now we just take it to be some abstract set, but in practice (and in subsequent lectures) it will usually be $\mathbb{R}$.

[4]These are just sets where order matters and we use (and) instead of { and } for them. So for example $(1, 2)$ is a different than $(1, 1, 2)$ or $(2, 1)$.

We will now outline a few basic properties which are almost immediate from the definitions of the above properties. One useful tool for visualising sets and set operations is Venn diagrams. In a Venn diagram we draw a box to represent the universal set Ω and circles for sets contained in Ω. We usually highlight the part which is of interest to us. For example, $A \setminus B$ would look like



$A \setminus B$

Using these diagrams it is easy to verify the following properties.

Proposition 1.2. *Let A, B, C be sets.*

i) $A \cup \emptyset = A$ *and* $A \cap \emptyset = \emptyset$,

ii) $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$ *(commutativity)*

iii) $(A \cup B) \cup C = A \cup (B \cup C)$, *(associativity)*
$(A \cap B) \cap C = A \cap (B \cap C)$,

iv) $(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$, *(De Morgan's Laws)*
$(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$,

v) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, *(distributivity)*
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Definition 1.3. Let A be a set. The **power set** of A, denoted by $\mathcal{P}(A)$, is the set of all subsets of A.

Example. Let $A = \{1, 2, 3\}$. Then

$$\mathcal{P}(A) = \{\emptyset, A, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}.$$

Notice that $\emptyset \in \mathcal{P}(A)$ for any set A, this is because $\emptyset \subseteq A$ is true for any set A.

For our next definition we need to make a distinction between finite and infinite sets. All our sets A and B have been finite so far, whereas $\mathbb{R}$ or $\mathbb{Z}$ would be examples of infinite sets.

Definition 1.4. Let A be a finite set. The **order** (or **cardinality**) of A, denoted by $|A|$, is the number of elements of A.

So for the A in the previous example we would have $|A| = 3$ and $|\mathcal{P}(A)| = 8$. It is actually possible to define cardinality for infinite sets, which leads to infinities of different "size" (curiously, $\mathbb{N}$ and $\mathbb{Q}$ will have the same size). That is, however, beyond the scope of this course. At this point it's probably a good idea to clarify some of the notation used so far.

Note:

$\mathbb{N}$, the natural numbers, $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$,

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

$\mathbb{Q}$, the rational numbers[5], $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$,

$\mathbb{R}$, the real numbers, $\mathbb{R} = \{$ decimal expressions with possibly infinite digits $\}$,

$\mathbb{C}$, the complex numbers, $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$,

where $i = \sqrt{-1}$.

Notice that these were not given as a definition, because each of them can be constructed from the previous one by certain tools (some of which we will see

[5]Sometimes the natural numbers are taken without 0, I might do this sometimes as well as it should be clear from the context

in this course), and natural numbers can be constructed with help from e.g. set theory. We will not delve any deeper into this matter, however.

As you might know by now, mathematics is essentially about taking a few things for granted and proving logical consequences out of those premises (or *axioms* as we might call them). There are some tools to make our life a little easier though. Let's suppose you are trying to prove that some property is true for any natural number. Now, imagine an infinite line of dominoes each representing one of these natural numbers. If your property is true for one natural numbers, let's say that the corresponding domino piece will get knocked over. If you ever played with them as a kid you should know what to expect now! If one domino gets knocked over then it will cause a chain reaction leaving nothing but fallen dominoes in its wake! Thus our property would immediately be true for each of the dominoes (or natural numbers), supposing we started with the first one.

This is exactly the principle behind *mathematical induction*, a method of proof that we'll introduce next.

Definition 1.5 (Mathematical Induction)**.** Let $R(n)$ be a statement concerning the natural number n. Suppose also that:

i) $R(1)$ is true, and

ii) If $R(k)$ is true for some $k \in \mathbb{N}$, then $R(k+1)$ must be true as well.

Then $R(n)$ is true for all $n \in \mathbb{N}$.

Here the second condition is called the *inductive hypothesis* and it corresponds to the mechanic that falling dominoes have. Despite me giving this as a definition, it is actually something that can be proven with a little bit of set theory (which makes sense, since it is a method of *proof* after all!). We won't, however, concentrate on that.

Let's take a look at mathematical induction in action.

Theorem 1.6. *Let S be a set of order m. Then $|\mathcal{P}(S)| = 2^m$.*

Proof. Here the statement $R(m)$ is that 'if $|S| = m$ then $|\mathcal{P}(S)| = 2^m$'. We have to check the two conditions.

i) The base case is simple enough. $R(0)$ means that we are looking at a set with 0 elements, and we know there is only one such set, namely, the empty set $\emptyset$. But $\emptyset \subset \emptyset$ so $P(\emptyset) = \{\emptyset\}$ as we would expect. Hence, $|\mathcal{P}(S)| = 1 = 2^0$, so that $R(0)$ is true.

ii) For the inductive step we have to do a little more work. Suppose $R(k)$ is true, i.e.

$$|S| = k \implies |\mathcal{P}(S)| = 2^k.$$

We must prove $R(k+1)$. For this we take S to be any set with $k+1$ elements. In particular, as $k \geq 0$, S has at least one element, say, $c \in S$. Now, define a new set

$$S' = S \setminus \{c\}.$$

The set S' has k elements so by inductive hypothesis $|\mathcal{P}(S')| = 2^k$. The idea for the rest of the proof is that every subset of S (we are counting subsets after all...) either contains c or it doesn't.

So let's consider these two cases separately and try to count such subsets in each case. Let $A \subseteq S$. If $c \notin A$ then of course $A \subset S'$, because S' is just S without c. Hence there are exactly 2^k subsets of this type. If, however, $c \in A$ then we can define $A' = A \setminus \{c\}$. But then $A' \subseteq S'$ so we are back in the first case again! Thus there are 2^k subsets of this type as well. These are all the subsets that S can have, so adding up we have

$$|\mathcal{P}(S) = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1},$$

which is exactly what we wanted. Hence, by induction, $R(k)$ is true for any $k \in \mathbb{N}$.

□

Another common method of proof is "proof by contradiction". Suppose you are trying to prove that statement X implies statement Y (so you are assuming that X is true and trying to deduce that Y is true from that). Now, suppose that X is true and Y is false. If you can show that this leads to some absurd statement (a contradiction), then this leaves no other choice than for Y to be true. So, for example, let's suppose we're trying to prove that if n^2 for $n \in \mathbb{Z}$ is odd then n is odd as well. If we do this by contradiction, then we need to assume that n^2 is odd, but that n is even. Then we need to use this information to arrive at a logical contradiction. How do we do that? Well, if n is even then we can write it as $n = 2m$ for some $m \in \mathbb{Z}$. Squaring this last equation we get that $n^2 = 4m^2 = 2(2m^2)$, which implies that n^2 is even. But n^2 cannot be both even and odd at the same time, which is absurd! Hence our assumption that n is even must be false, i.e. we have shown that n must be odd. Reflect on this argument for a while before moving on to the next section.

1.2 Relations and Functions

We now move on to a different topic which will be fundamental for understanding the content of the rest of the course.

Definition 1.7. Let X, Y be sets. A **relation** R, from X to Y, is a subset of $X \times Y$.

> Note: If $T \subseteq X \times Y$ then we can identify a relation R with this subset. We write
>
> $$xRy \quad \text{if} \quad (x, y) \in T.$$

So what we are doing is establishing some kind of relationship between two arbitrary sets X and Y by pairing corresponding elements from both sets (hence the term "relation"). You already know many relations. One example would be your usual "less than or equal to", $\leq$, on, say, real numbers. But you can also have more concrete relations. Take, for example, the set X to

be the members of some family. Then we can define a relation R on $X \times X$ by requiring that if xRy then "x is a sibling of y". So, most likely, if x was the father and y the mother then x and y would not be related and we would write $x \not R y$, whereas if a and b are children in the family then most likely aRb.

There is an important subclass of relations, which you are already familiar with. These are functions.

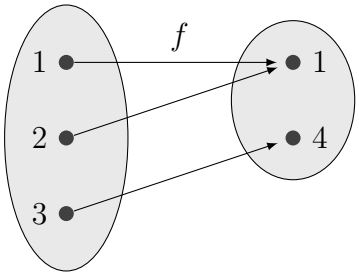
Definition 1.8. Let X, Y be sets. A **function** f from X to Y is a relatio, such that every element of X is mapped (related) to a unique element of Y.

- The most common way is to write $f : X \to Y$ and $x \mapsto y$. We call $y = f(x)$. This is more convenient notation than writing, for example, $f \subseteq X \times Y$, $(x, y) \in f$.
- X is called the **domain** of f, and
- Y is called the **co-domain** of f.
- If $y = f(x)$, then y is called the **image** of x and x is called the **preimage** of y.
- From the definition of f it follows that each $x \in X$ has precisely one image. On the other hand, it is not necessary for every $y \in Y$ to have exactly one preimage (it could have many or none at all).
- The **range** of f, denoted by $f(X)$ or $\mathrm{Im}(X)$, is the subset of Y composed of elements which have preimages in X. In other words,

$$f(X) = \{y \in Y : \exists x \in X \text{ such that } y = f(x)\}.$$

There are various ways to describe the rule for functions.

Example. i) Let $f : \{1, 2, 3\} \to \{1, 4\}$ then we can write out the rule as



ii) Alternatively, we can describe the rule with conditions. Let $\mathbb{Z} : 0, 1 \to$ and

$$f(x) = \begin{cases} 0, & \text{if } x \text{ is odd,} \\ 1, & \text{if } x \text{ is even.} \end{cases}$$

Recall that we gave no restrictions for how many preimages a $y \in Y$ can have (if any). It turns out to be useful to distinguish between the three cases.

Definition. [6] A function $f : X \to Y$ is called:

- **injective** (or 1-1) if every $y \in Y$ has at most one preimage, i.e.

$$f(x_1) = f(x_2) \implies x_1 = x_2;$$

- **surjective** (or onto) if every $y \in Y$ has at least one preimage, i.e.

$$\forall y \in Y, \exists x \in X \text{ s.t. } y = f(x);$$

- **bijective** if it is both injective and surjective, i.e.

$$\forall y \in Y, \exists! x \in X \text{ s.t. } y = f(x).$$

Example. Take $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. This is not injective as $f(1) = f(-1)$, but $1 \neq -1$. It is not surjective as -1 hs no preimage, that is, there is no $x \in \mathbb{R}$ with $x^2 = -1$. Hence it is not bijective either.

[6] Apparently in the lecture notes Definition 1.8 appeared twice so in order to be consistent with the numbering from lectures this definition will be without a number.

While you can add, subtract, multiply and divide functions exactly as you would expect, there is one more operation we can define that turns out to be extremely useful.

Definition 1.9. Let $f : Y \to Z$ and $g : X \to Y$ be two functions. The **composition** of f and g is the function $f \circ g : X \to Z$ such that

$$(f \circ g)(x) = f(g(x)), \quad \forall x \in X.$$

The following picture and example illustrate what's going on:

$$X \xrightarrow{g} Y \xrightarrow{f} Z, \qquad X \xrightarrow{f\circ g} Z$$

Example. Let $f, g : \mathbb{R} \to \mathbb{R}$ be functions such that $f(x) = x + 1$ and $g(x) = x^3$. Then, $g \circ f : \mathbb{R} \to \mathbb{R}$ is

$$(g \circ f)(x) = g(f(x)) = g(x + 1) = (x + 1)^3,$$

while $f \circ g : \mathbb{R} \to \mathbb{R}$ is

$$(f \circ g)(x) = f(g(x)) = f(x^3) = x^3 + 1.$$

Notice that, in general, $f \circ g \neq g \circ f$.

Just like for the other operations $(+, -, \cdot, \div)$ there is an identity element, we'd expect the composition of functions to have an identity as well. Also, having an identity element would allows us to define inverses under composition.

Definition 1.10. Let X,Y be sets.

i) The **identity function** of X is defined as $\mathrm{id}_X : X \to X$ such that

$$\mathrm{id}_X(x) = x, \quad \forall x \in X.$$

ii) A function $f : X \to Y$ is called **invertible** if there exists a function $f^{-1} : Y \to X$ such that

$$f \circ f^{-1} = \mathrm{id}_Y, \quad f^{-1} \circ f = \mathrm{id}_X .$$

There is a particularly nice characterisation of invertible functions, which is really useful for us.

Theorem 1.11. *A function $f : X \to Y$ is bijective if and only if it is invertible.*

Proof. This is an if and only if statement so we have to prove two directions.

$\underline{\Longrightarrow}$**:** Assume f is bijective. We need to prove that it is invertible. Since f is bijective we know that $\forall y \in Y$, $\exists! x \in X$ such that $y = f(x)$. We can then define $f^{-1} : Y \to X$ as $f^{-1}(y_0) = x_0$ if $y_0 = f(x_0)$. This is well-defined since f is surjective and the preimage of y_0 is unique. From this it follows that

$$\begin{aligned} x \mapsto f(x) \mapsto f^{-1}(f(x)) = x \\ y \mapsto f^{-1}(y) \mapsto f(f^{-1}(y)) = y, \end{aligned}$$

so $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$.

$\underline{\Longleftarrow}$**:** Assume f is invertible, we need to show that f is both injective and surjective. We do this by contradiction. Suppose that f is invertible but not bijective. There are two ways f can fail to be bijective: either it is not injective or it is not surjective (or both). We'll deal with the two cases separately.

First, suppose that f is not injective. This means that there exist x_1 and $x_2 \in X$ such that $x_1 \neq x_2$, but $f(x_1) = f(x_2)$. Applying f^{-1} to this last equation we get

$$\begin{aligned} f(x_1) &= f(x_2) \\ f^{-1}(f(x_1)) &= f^{-1}(f(x_2)) \\ x_1 &= x_2, \end{aligned}$$

but this is absurd as we assumed that $x_1 \neq x_2$! Hence f must be injective.

Now, suppose that f is not surjective. Then we can find a $y \in Y$ for which there is no $x \in X$ with $f(x) = y$. However, we know that f^{-1} exists and is a well-defined function, so by definition $f^{-1}(y)$ must map to some element in X. So suppose $f^{-1}(y) = \tilde{x}$ for some $\tilde{x} \in X$. Applying f to this equation gives that

$$y = f(f^{-1}(y)) = f(\tilde{x}),$$

which contradicts the fact that no such number should exist. Hence f must be surjective.

So we have shown that f is both injective and surjective so it must be bijective.

□

One question you might be tempted to ask is if you have a function $f : S \to T$ then how many different functions can there be? And how many of these are bijections? If you did, well, you're in luck as it is possible to give definite answers to these questions (at least when S and T are finite).

If f is as above then the definition of a function tells us that each element of S must map to precisely one element of T. So if the size of T is $|T| = k$, then for each $s \in S$ we have k different choices. That is, if $|S| = n$ then we have a total of k^n ways of making these choices (k options for n elements). In other words, the number of functions $f : S \to T$ is

$$|T|^{|S|}.$$

In order to deal with bijections we first need to decide when do they even exist. We already showed that f is a bijection if and only if it is invertible. Now, by similar reasoning as above if f is a function from S to T then each $s \in S$ has a unique $t \in T$ so $|S| \leq |T|$. On the other hand, f^{-1} is a function as well so by the same logic $|T| \leq |S|$. This means that $|S| = |T|$. So there

can only be a bijection if the sets have the same cardinality. This doesn't yet tell us whether there always is a bijection though. In order to do that we need a "constructive proof".

Theorem 1.12. *Let S, T be sets, with $|S| = |T|$ finite. Then, there is a bijection $f : S \to T$.*

Proof. Suppose $|S| = |T| = n$. Now pick some $s_1 \in S$ and $t_1 \in T$. We start defining a function $f : S \to T$ by letting $f(s_1) = t_1$. Now pick $s_2 \in S \setminus \{s_1\}$ and $t_2 \in T \setminus \{t_2\}$ and define $f(s_2) = t_2$. Notice that $|S \setminus \{s_1\}| = |T \setminus \{t_1\}| = n - 1$. So if we repeat this process n times then to each $s \in S$ we have assigned a unique $t \in T$. But S and T are of the same size so there are no elements left over in T. So we can define an inverse function f^{-1} by

$$f^{-1}(t_i) = s_i$$

for $i = 1, \ldots, n$. By the previous theorem f is bijective. □

Try to do the above proof with induction as well!

So, there can only be a bijection between S and T if they have the same cardinality. Even then, however, not every function $f : S \to T$ will be a bijection. So how many are there? Well, if I pick an $s_1 \in S$ then I can map it to anything in T (suppose $|S| = |T| = k$), i.e. I have k choices for s_1. Suppose $f(s_1) = t_1$ for some $t_1 \in T$. Now if I consider the next element of S then it can map to anything in T *except* t_1 because then our function would fail to be injective. In other words, I have $k - 1$ choices for the second element. Repeating this process shows that at step i I have $k - i$ choices for the next element. Hence the total number of choices is just the product of these numbers, i.e.

$$k(k-1)(k-2)\ldots 2 \cdot 1 = k!.$$

That is, there are $k!$ bijections $f : S \to T$ if $|S| = |T| = k$.

Another thing to notice is that a composition preserves bijection. What this means is that if I have functions

$$f : Y \to Z, \quad g : X \to Y,$$

which are both bijections, then

$$f \circ g : X \to Z$$

is a bijection as well. Let's prove this.

Proof. We need to prove that $f \circ g$ is both injective and surjective.

Injective: We need to prove that if $(f \circ g)(x_1) = (f \circ g)(x_2)$ then $x_1 = x_2$. Define $y_1 = g(x_1)$ and $y_2 = g(x_2)$. So we can write the above assumption as $f(y_1) = f(y_2)$. By injectivity of f this implies that $y_1 = y_2$, i.e. $g(x_1) = g(x_2)$. But now, since g is injective this immediately implies that $x_1 = x_2$. Hence, $f \circ g$ is injective.

Surjective: We need to prove that for all $z \in Z$ there is some $x \in X$ such that $(f \circ g)(x) = z$. Fix $z_0 \in Z$. Since f is surjective we know that there must exist some $y_0 \in Y$ such that $f(y_0) = z_0$. Again, since g is surjective, for this y_0 there must exist some $x_0 \in X$ such that $g(x_0) = y_0$. Substituting this into the previous equation gives

$$(f \circ g)(x_0) = f(g(x_0)) = z_0,$$

which proves that $f \circ g$ is surjective.

Hence $f \circ g$ is bijective. □

Before moving on we return to relations briefly to discuss particularly nice relations (remember that functions were relations after all).

Definition 1.13. Let R be a relation on $X \times X$.

i) R is called **reflexive** if xRx $\forall x \in R$ (i.e. $(x, x) \in R$),

ii) R is called **symmetric** if $xRy \implies yRx$ (i.e. $(x, y) \in R \implies (y, x) \in R$)

iii) R is called **transitive** if xRy and $yRz \implies xRz$ (i.e. $(x, y) \in R$ and $(y, z) \in R \implies (x, z) \in R$).

A relation which satisfies all three of these properties is so important that we give it a name of its own.

Definition 1.14. A relation R on a set X satisfying the above three properties (reflexive, symmetric, transitive) is called an **equivalence relation** on X. The **equivalence class** identified by the element $a \in X$ is the set

$$[a] = \{b \in X : aRb\}.$$

We say that a is a **representative** of this equivalence class.

The key idea behind equivalence relations is that equivalence classes end up partitioning your set X into disjoint subsets each of which can be represented by just one element under the equivalence relation. In other words, we can reduce the problem of studying really big sets into just studying a small number of equivalence classes and their representatives.

Exercise. Prove that an equivalence relation on X defines a partition of X, i.e. a decomposition of X into disjoint nonempty subsets such that each $x \in X$ belongs to exactly one subset (equivalence class). Prove also the converse that each partition of X gives rise to an equivalence relation on X.

Example. Let X be the set of all lines in $\mathbb{R}^3$. We can define an equivalence relation R on X by

$$\ell_1 R \ell_2 \iff \ell_1 \parallel \ell_2,$$

where $\ell_1 \parallel \ell_2$ means that the line ℓ_1 is parallel to the line ℓ_2. We need to check that R is reflexive, symmetric and transitive.

- We take it as part of the definition that that every line is parallel to itself. Hence,

  $$\ell_1 \parallel \ell_1,$$

  so R is reflexive.

- Symmetry is easy as well, if ℓ_1 is parallel to ℓ_2 then ℓ_2 must also be parallel to ℓ_2 according to the definition. Hence,

$$\ell_1 \parallel \ell_2 \implies \ell_2 \parallel \ell 1.$$

- Take three lines ℓ_1, ℓ_2 and ℓ_3 with $\ell_1 \parallel \ell_2$ and $\ell_2 \parallel \ell_3$. We need to show that $\ell_1 \parallel \ell_3$. Suppose this is not the case, that is, ℓ_1 is not parallel to ℓ_3. But ℓ_1 has the same direction as ℓ_2 so this would imply that ℓ_2 is not parallel to ℓ_3 either, which is a contradiction. Hence, $\ell_1 \parallel \ell_3$ and R is reflexive.

Thus we have shown that R is an equivalence relation on X.

Chapter 2

Group Theory

We now move on to group theory, which is a mathematical abstraction for the concept of symmetry. As symmetry is ubiquitous in nature it should be no surprise that group theory has found its way in to the theories of physicists and chemists. In this course we will cover most of the smaller finite groups giving foundation to more systematic study of finite and infinite groups.

2.1 Basic Properties

At the heart of group theory is the idea of a binary operation, which generally speaking is just a way of combining two objects to produce a new one. Say, if you give me yellow and blue paint then I can mix them to produce paint with new colour. We would say that "mixing paint" is a binary operation. If, however, I give you solid objects like a rock and a piece of wood and tell you to "mix" them you'd be left wondering what are you actually supposed to do. This highlights the point that binary operations are very dependent on the context. It is not just *what* you do to an object, but also *which* objects do you do it to. There are many abstract binary operations that you are also familiar with, such as taking two integers and adding them up to produce a

new integer. We can formalise this as follows.

Definition 2.1. Let S be a set. A **binary operation** $*$ on S is a function from $S \times S$ to S.

So in other words, $* : S \times S \to S$ and we write $(a, b) \mapsto a * b$, where $a, b, a * b \in S$. Another example of such an operation would be your usual multiplication on real numbers. The idea behind groups is to take particularly nice binary operations defined on interesting sets. It turns out that if we require our binary operation to have a few key properties then often we can construct the whole group from just knowing a little bit about it. We can now give a full definition.

Definition 2.2. A **group** is a pair $(G, *)$ where G is a set and $*$ is a binary operation on G such that:

G0 *(Closure)* For every $a, b \in G$, $a * b \in G$,

G1 *(Associativity)* For every $a, b, c \in G$

$$(a * b) * c = a * (b * c),$$

G2 *(Identity)* There exists an $e \in G$ such that

$$a * e = e * a = a \quad \forall a \in G,$$

G3 *(Inverse)* For every $a \in G$ there is an $a' \in G$ such that

$$a * a' = a' * a = e.$$

Often if a' is the inverse for $a \in G$, then we write $a^{-1} := a$ (don't confuse this with $\frac{1}{a}$ which has no meaning if a is not a nonzero number, e.g. what would "1 over green paint" mean?). Sometimes, in contexts which will be clear soon, we write $-a$ for the inverse. Notice also that strictly speaking the condition G0 is unnecessary, because our definition of a binary operation already implies closure. However, we've included it there to remind you that

it always needs to be checked that the binary operation is in fact closed[1] when investigating groups.Since the set and the binary operation in a group are so intricately tied together, usually if one is given the other is understood. Because of this we often just write G to mean the whole group and expect the reader to know which binary operation we are talking about.

Since groups capture such an essential concept of symmetry it should come as no surprise that you are already familiar with many examples.

Example. i) $(\mathbb{Z}, +)$ is a group. Let us check the group axioms.

G0 If I take two numbers $a, b \in \mathbb{Z}$ then naturally $a + b$ is another integer, and hence $+$ is closed.

G1 We also know that $(a+b)+c = a+(b+c)$ $\forall a, b, c \in \mathbb{Z}$ when adding up integers so we can ignore the brackets.

G2 For identity we need an $e \in \mathbb{Z}$ such that

$$e + a = a + e = a, \quad \forall a \in \mathbb{Z}.$$

Of course taking $e = 0 \in \mathbb{Z}$ does the trick.

G3 Finally we need to produce an inverse, but this is again easy. For $a \in \mathbb{Z}$ we need an $a' \in \mathbb{Z}$ such that

$$a' + a = a + a' = 0.$$

So if we take $a' = -a$ then we are done.[2]

This shows that $(\mathbb{Z}, +)$ satisfies the axioms G0–G3 and thus is a group. You should also show that $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are groups. Is $(\mathbb{N}, +)$ a group?

[1] Also, some texts take the binary operation to mean a function from $S \times S$ into some universal set in which case it is important to require closure.

[2] This brings up a curious point that you may not have paid attention to before. There is a small distinction between the minus signs in "-2" and "$2 - 5$". In the first case the minus sign is used to denote the inverse of 2 under addition whereas in the second example it is treated as a binary operation in its own right. Of course this distinction becomes nonexistent if we write "$2 + (-5)$", so for all intents and purposes they are the same thing and can just be treated as a notation shorthand.

ii) What about $(\mathbb{Z}, \cdot)$? That is, integers under multiplication. We can multiply any two integers together to obtain a new one and we also know that bracketing doesn't matter, i.e. $\cdot$ is associative. Moreover, we can multiply any number by 1 and still get back the same number so we have found an identity too. We know, of course, that it is impossible to multiply any integer (apart from 1 and -1) by another integer to arrive at the identity 1 since it would require the use of rational numbers. Hence $(\mathbb{Z}, \cdot)$ is not a group.

iii) The previous example would suggest that if we add rational numbers to the game then we have obtained a group. Is it so? Unfortunately the answer is no, there is still a problem with division (notice again that we have given a special name to the inverses under the operation of multiplication, just as we did with addition and subtraction). There is no rational number $r \in \mathbb{Q}$ such that

$$r \cdot 0 = 0 \cdot r = 1.$$

Hence $(\mathbb{Q}, \cdot)$ is not a group. However, we can fix this easily by removing 0 from consideration. So, as you can show yourself, $(\mathbb{Q} \setminus \{0\}, \cdot)$ is in fact a group. We often write a superscript $\times$ to denote the set of all invertible elements in a set when the binary operation is understood. So the above group could be written as $(\mathbb{Q}^\times, \cdot)$.

iv) Similarly you can show that $(\mathbb{R}^\times, \cdot)$ is a group.

v) We can also define more unusual binary operations. Consider $(\mathbb{Z}, *)$ where

$$a * b = a + b - 1.$$

Then clearly the group is closed under $*$ since addition and subtraction of integers is closed. But we'll have to prove that it is associative. Let $a, b, c \in \mathbb{Z}$ then

$$\begin{aligned} a * (b * c) &= a * (b + c - 1) \\ &= a + (b + c - 1) - 1 \\ &= (a + b - 1) + c - 1 \\ &= (a * b) + c - 1 \\ &= (a * b) * c. \end{aligned}$$

So $*$ is associative. What would the identity be? We have to solve $a * e = a$. This gives:

$$\begin{aligned} a + e - 1 &= a \\ e &= 1. \end{aligned}$$

After checking that $1 * a = a$ we conclude that the identity is 1. Now, in order to find the inverse we compute

$$\begin{aligned} a * a^{-1} &= 1 \\ a + a^{-1} - 1 &= 1 \\ a^{-1} &= 2 - a. \end{aligned}$$

Since $(2 - a) * a = 1$ as well, we can see that every element has an inverse. Naturally $2 - a \in \mathbb{Z}$ so $a^{-1} \in \mathbb{Z}$.[3]

Notice that in the examples above, and especially in the last one, it didn't really matter if we worked with $a * b$ or $b * a$ since $a + b - 1 = b + a - 1$. This is such an important property that we give it a name of its own.

Definition 2.3. A binary operation $*$ on a set S is **commutative** if $a * b = b * a$, $\forall a, b \in S$. A group $(G, *)$ with a commutative binary operation is called **abelian**.[4]

Of course, for example, all your usual operations, such as addition and multiplication, are commutative (what about subtraction and division?). We will now prove a few elementary, but powerful facts about groups.

Theorem 2.4. *Let $(G, *)$ be a group. Then*

i) *The identity e is unique.*

[3]It it always important to check that the inverse actually belongs to the group. Often it can exist only in some bigger superset of G.

[4]This is after the 19$^{\text{th}}$century Norwegian mathematician Niels Henrik Abel who died at the age of only 26 having already contributed more to the theory of groups than many would in their whole lifetime.

ii) *The inverse a' of an element $a \in G$ is unique.*

The crux of this is that the notation a^{-1} is justified for the inverse of a.

Proof. i) Suppose e' is also an identity, then by definition

$$e * e' = e' * e = e,$$
$$e * e' = e' * e = e'$$

since both e and e' are identities. But from these it immediately follows that $e = e'$.

ii) Fix $a \in G$. Suppose a has inverses a' and a''. Then, by definition,

$$a' * a = a * a' = e,$$
$$a'' * a = a * a'' = e.$$

Hence,

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

□

With groups we also have the following elementary property for solving equations.

Theorem 2.5 (Cancellation Laws)**.** *Let $(G, *)$ be a group. Then $\forall a, b, c \in G$*

i) *If $a * b = a * c$ then $b = c$.*

ii) *If $b * a = c * a$ then $b = c$.*

Proof. The proof is really simple.

i)

$$\begin{aligned} a * b &= a * c \\ a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c && \text{[G1]} \\ e * b &= e * c && \text{[G3]} \\ b &= c && \text{[G2].} \end{aligned}$$

ii) Similarly.

□

For the most part exponents work like with usual numbers, but you have to be a bit careful if G is not commutative.

Theorem 2.6. *Let $(G, *)$ be a group. Then,*

i) $\forall a, b \in G$

$$(a * b)^{-1} = b^{-1} * a^{-1},$$

ii) $\forall a, b \in G$ *let us define*

$$a^r := \underbrace{a * a * \ldots * a}_{r \text{ times}},$$

then

$$\begin{aligned} a^r * a^m &= a^{r+m} = a^m * a^r, \\ (a^r)^{-1} &= a^{-r} = (a^{-1})^r, \\ a^0 &= e. \end{aligned}$$

Proof. i) We just need to check that the definition of an inverse is satisfied:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e,$$

and similarly for the other direction. Hence

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

ii) The first property follows immediately from associativity. For the second property we notice that

$$(a * a)^{-1} = (a^{-1} * a^{-1}) = (a^{-1})^2,$$

by part i). Hence the result follows by induction, and letting $(a^n)^{-1} = a^{-n}$ is just notation as is $a^0 = e$.

□

Let us formulate the cancellation laws in terms of actual equations:

Theorem 2.7. *Let $(G, *)$ be a group. Then $\forall a, b \in G$ the equations*

i)

$$a * x = b$$

and

ii)

$$x * a = b$$

have a unique solution.

Proof. i) $a^{-1} * (a * x) = a^{-1} * b \implies e * x = a^{-1} * b \implies x = a^{-1} * b$. This proves the existence of a solution, let's now prove that it is unique. Let x_1 and x_2 be two solutions, then

$$a * x_1 = a * x_2 = b,$$

so by the cancellation laws we get that $x_1 = x_2$ and the solution is unique.

ii) Similarly.

□

2.2 Finite Groups

Major problem in group theory is to list all the *finite* groups of a certain size (meaning the cardinality of the set) at least up to some kind of equivalence (basically up to renaming the elements in the group). For example, the smallest group is the *trivial group* with only one element, which has to be the identity, i.e. $\{e\}$. Notice that it doesn't matter which binary operation we take since we already know how it works with the identity. Similarly if we take a group of size 2 then it is always of the form $\{e, g\}$ for any g (up to renaming). Again, we know how to compute all the products from definitions so it doesn't matter what the binary operation is. In the homework you will do this for groups of size 3 and 4. We will later see what happens for groups with particularly nice size.

Definition 2.8. Let $(G, *)$ be a finite group of order n (i.e. $|G| = n$). Write

$$G = \{a_1, a_2, \ldots, a_n\}.$$

Then a **group table** for G is a table that lists all the possible products of the elements of G:

$*$	a_1	a_2	a_3	$\ldots$	a_n
a_1	a_1^2	$a_1 * a_2$	$a_1 * a_3$	$\ldots$	$a_1 * a_n$
a_2	$a_2 * a_1$	a_2^2	$a_2 * a_3$		$a_2 * a_n$
$\vdots$	$\vdots$				$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$a_n * a_3$	$\ldots$	$a_n * a_n$

These group tables have a particularly nice property (which makes it easy to write them down). They look exactly like sudoku!

Definition 2.9. Let $n \in \mathbb{N}$. A **latin square** is a $n \times n$ array of n diffrerent numbers (or symbols) such that each row and each column contain each number exactly once.

Theorem 2.10. *Every group table is a latin square.*

Proof. Let $(G, *)$ be group, and $G = \{a_1, \ldots, a_n\}$, $|G| = n$. Pick a row, say, the first one, so the elements are of the form $a_1 * a_i$ for $i = 1, \ldots, n$. Suppose

$$a_1 * a_i = a_1 * a_j$$

for some i and j. Then from cancellation laws it follows that $a_i = a_j$ so $i = j$. So every entry in a given row is different. Similarly for columns. □

So, given this we can write down the group table for any group of size 2. Suppose $G = \{e, a\}$ then

$*$	e	a
e	e	a
a	a	$\textcircled{e}$

where the circled entry is forced by the fact that the table should be a latin square. In other words $a^{-1} = a$.

2.3 Modular Arithmetic

We will now have a brief interlude to introduce a certain class of concrete finite groups which have very rich properties. This will arise from something called *modular arithmetic* which is basically like counting on clock[5] So for example if we just think of the clock as being the numbers from 1 to 12 (or you can think of 12 as being 0). Then if the time is 9 and we go forward 4 hours we arrive at 1 so $9 + 4 = 1$ when counting on the clock. Similarly if the time is 3 and we go back 5 hours then we arrive at 10 so $3 - 5 = 10$. In modular arithmetic we just generalise this to situations where the maximum number might be something else than 12.

Definition 2.11. Fix $n \in \mathbb{N}$ where $n \neq 0$. Let $a, b \in \mathbb{Z}$, **congruent to** b **modulo** n, and write

$$a \equiv b \pmod{n}$$

[5]Hence it is sometimes called *clock arithmetic*.

if $b-a$ is a multiple of n (i.e. n divides $b-a$, $n|b-a$). This means that $\exists k \in \mathbb{Z}$ such that

$$b - a = kn.$$

Note: a and b have the same remainder when divided by n. Let $r \in [0, n-1]$ be the remainder. We call r the **residue** of a modulo n. Suppose $a \equiv b \pmod{n}$ but they have different residues, say, r_1 and r_2 respectively. Then

$$a = k_1 n + r_1, \quad b = k_2 n + r_2.$$

Hence,

$$a - b = (k_1 - k_2)n + (r_1 - r_2).$$

But n divides $a-b$ so $r_1 - r_2 = 0$. In particular the residues are the same.

There's a good reason for why we use a sign $\equiv$ which is similar to $=$. It turns out that $\equiv$ actually defines an equivalence relation on $\mathbb{Z}$! So this allows us to reduce the problem of considering all of $\mathbb{Z}$ into considering just a finite subset of $\mathbb{Z}$ consisting of the equivalence class representatives.

Theorem 2.12. *Fix $n \in \mathbb{N}$, $n \neq 0$. The relation on $\mathbb{Z}$*

$$aRb \iff a \equiv b \pmod{n}$$

is an equivalence relation. Its equivalence classes are $[0], [1], \ldots, [n-1]$, the residues up to $n-1$.

Proof. We need to prove the three properties of an equivalence relation.

- Take any $a \in \mathbb{Z}$ then

  $$aRa \iff a \equiv a \pmod{n}.$$

  But this is of course true since n divides $a - a = 0$. So R is reflexive.

- Let $a, b \in \mathbb{Z}$ then

$$a \equiv b \pmod{n} \implies b - a = k_1 n \implies a - b = (-k_1)n$$

for some $k_1 \in \mathbb{Z}$. But of course $-k_1 \in \mathbb{Z}$ as well so it follows that

$$b \equiv a \pmod{n},$$

i.e. $aRb \implies bRa$, which means that R is symmetric.

- Now, let $a, b, c \in \mathbb{Z}$ then

$$\left.\begin{array}{l} a \equiv b \pmod{n} \implies b - a = k_1 n \\ b \equiv c \pmod{n} \implies c - b = k_2 n \end{array}\right\} \implies c - a = (k_1 + k_2)n,$$

which means that

$$a \equiv c \pmod{n},$$

or $aRb, bRc \implies aRc$ so R is transitive.

We have shown that R is an equivalence relation. The equivalence classes are by definition

$$[a] = \{b \in \mathbb{Z} : \exists k \in \mathbb{Z}, b = a + kn\}.$$

Clearly there are only n distinct ones. □

We now start working towards introducing groups in to the picture.

Definition 2.13.

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

is the set of classes of residues modulo n. We can define the two operations:

$$[a] + [b] = [a + b],$$
$$[a] \cdot [b] = [a \cdot b],$$

the sum and product modulo n, respectively. We need to show that these operations are well-defined (i.e. that they do not depend on the choice of representative from the equivalence class).

Theorem 2.14. *Let $n \in \mathbb{N}$, $n \neq 0$. Then $(\mathbb{Z}_n, +)$ with addition modulo n is a group.*

Proof. We need to check the 4 properties of a group.

G0 $[a] + [b] = \{y \in \mathbb{Z} : (a + b) \equiv y \pmod{n}\}$ by definition. We need to show that the operation is well defined. Let $\tilde{a} \in [a]$ and $\tilde{b} \in [b]$ be some other representatives from the equivalence classes. We need to prove that

$$[\tilde{a} + \tilde{b}] = [a + b].$$

We know that $\tilde{a} = a + h_1 n$ and $\tilde{b} = b + h_2 n$. Hence

$$\tilde{a} + \tilde{b} = a + b + (h_1 + h_2)n,$$

but this means that $\tilde{a} + \tilde{b} \in [a + b]$, which is what we wanted to show.

Associativity follows from the associativity of natural numbers:

$$([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+([b]+[c]).$$

The obvious choice for the identity is

$$e = [0].$$

Similarly for the inverse we have an ovious choice

$$[a]^{-1} = [-a].$$

□

Note: We denote by $\mathbb{Z}_n^\times$ the set of invertible elements (under multiplication modulo n) in $\mathbb{Z}_n$ and $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]\}$.

We have constructed an additive group out of modular arithmetic. We'd now like to construct a multiplicative group as well. The problem here is that for arbitrary n there might not always be inverses. Consider e.g. $[2] \in \mathbb{Z}_4$ then there is no $b \in \mathbb{Z}$ such that $[2][b] = [1]$.

Theorem 2.15. *Let p be a prime number in $\mathbb{N}$. Then $(\mathbb{Z}_p^*)$ with multiplication modulo p is a group.*

Proof. The only problematic case will be with the inverse.

G0 We have that $[a] \cdot [b] = \{y \in \mathbb{Z} : ab \equiv y \pmod{p}\}$ by definition. Let us prove that this is independent of the choice of representative. Take $\tilde{a} \in [a]$ and $\tilde{[b]} \in [b]$, then $\tilde{a} = a + h_1 p$ and $\tilde{b} = b + h_2 p$ as before. Hence,

$$\tilde{a}\tilde{b} = ab + (ah_2 + bh_1 + h_1 h_2)p,$$

so $\tilde{a}\tilde{b} \in [ab]$ and the product is well defined. Note that $a, b \in [0]$ implies that $a \neq hp$ and $b \neq kp$ for any $h, k \in \mathbb{Z}$, so if we had $ab \in [0]$ then $ab = \tilde{k}p$ and as p is a prime this would mean that either $p|a$ or $p|b$ which is impossible. So the product is always nonzero and so defines a closed binary operation.

G1 This follows, similarly as before, from the associativity of multiplication of integers.

G2 Again, this is easy given $e = [1]$.

G3 For the inverse we need to do a bit of work. We need to prove that the inverse always exists for any $[a] \in \mathbb{Z}_p^*$. We do this by using a little trick[6]. Write all the elements of $\mathbb{Z}_p^*$ in a list and multiply each of them by a fixed element $[b] \in \mathbb{Z}_p^*$ then we still have a list which contains each element of the group exactly once (but in a different order, possibly). Let's first prove that this is actually true. So fix $[b] \in \mathbb{Z}_p^*$ and suppose $[c] \neq [d] \in \mathbb{Z}_p^*$. Without loss of generality (WLOG) we can choose $0 < b, c, d \leq p - 1$. We wish to prove that $[cb] \neq [db]$. Suppose this is not the case, so $[cb] = [db]$. Then $cb = db + kp$, i.e. $(c - d)b = kp$. Since

[6]This will actually be true for any finite group G, which we will prove later.

p is a prime this means that either $p|b$ or $p|c-d$. This cannot happen as $0 < b < p$ and $0 < |c-d| < p$. Hence $[cb] \neq [db]$.

So we have now written each element of the group in a list and multiplied them by $[b]$:

$$[b \cdot 1], [b \cdot 2], \ldots, [b \cdot (p-1)],$$

and we know that every element of the group appears in that list exactly once. Hence we can find an $0 < i \leq p-1$ such that

$$[b \cdot i] = [1].$$

Hence

$$[b]^{-1} = [i].$$

□

So we can see that $(\mathbb{Z}_p^*, \cdot)$ is the same as $(\mathbb{Z}_p^\times, \cdot)$. In particular you should notice that $(\mathbb{Z}_n, \cdot)$ is never a group and neither is $(\mathbb{Z}_p^\times, +)$. Hence there is no ambiguity in using just $\mathbb{Z}_n$ for the additive group or $\mathbb{Z}_p^*$ for the multiplicative group (or, indeed, $\mathbb{Z}_p^\times$). Notice also that while $(\mathbb{Z}_n^*, \cdot)$ is not in general a group, $(\mathbb{Z}_n^\times, \cdot)$ is since we are just picking the invertible elements from $\mathbb{Z}_n$.[7]

We can now use this information, and what we have proved about groups, to prove our main result for modular arithmetic.

Theorem 2.16 (Fermat's Little Theorem)**.** *Let p be a prime number and $a \in \mathbb{Z}$ fixed. Then,*

$$a^p \equiv a \pmod{p}.$$

Equivalently, if $[a] \neq [0]$ in $\mathbb{Z}_p$ (so $[a] \in \mathbb{Z}_p^\times$) then

$$a^{p-1} \equiv 1 \pmod{p}.$$

You could also formulate this in terms of the bracket notation by writing

$$[a]^{p-1} = [1].$$

[7] The invertible elements turn out to be the ones which are coprime to n.

Proof. We will prove the second version which is clearly equivalent to the first one. From the previous proof we know that the list

$$[a], [2a], \ldots, [(p-1)a],$$

contains each of the elements $[1]$, $[2], \ldots, [p-1]$ exactly once. Hence,

$$\begin{aligned}[a] \cdot [2a] \cdot \ldots \cdot [(p-1)a] &= [1] \cdot [2] \cdot \ldots \cdot [p-1] \\ [(p-1)!][a^{p-1}] &= [(p-1)!].\end{aligned}$$

But these are elements of a group so we can just apply the cancellation laws to deduce that

$$[a]^{p-1} = [1].$$

□

We will now state the fact that multiplying all elements of a group with one element still gives you the whole group as a theorem. We used it in the proof of Fermat's Little Theorem.

Theorem 2.17. i) *Let $n \in \mathbb{N}\{0\}$ and $a \in (\mathbb{Z}_n, +)$. Let S be the set*

$$\begin{aligned}S &= \{[h+a] : [h] \in \mathbb{Z}_n\} \\ &= \{[a], [1+a], [2+a], \ldots, [n-1+a]\}.\end{aligned}$$

Then $S = \mathbb{Z}_n$.

ii) *Let p be a prime number and $a \in \mathbb{Z}$ such that $[a] \in (\mathbb{Z}_p^{\times}, \cdot)$ (so $a \not\equiv 0 \pmod{p}$). Let S be the set*

$$\begin{aligned}S &= \{[ha] : [h] \in \mathbb{Z}_p^*\} \\ &= \{[a], [2a], \ldots, [(n-1)a]\}.\end{aligned}$$

Then $S = \mathbb{Z}_p^{\times}$.

Proof. We will prove the second part, first part is similar with the map $\phi : \mathbb{Z}_n \to S$, $\phi([s]) = [s+a]$.

Clearly $S \subseteq \mathbb{Z}_p^\times$. We must prove that $|S| = p-1$ as this would imply that $S = \mathbb{Z}_p^\times$. If we define the map $\psi : \mathbb{Z}_p^\times \to S$ then it suffices to prove that ψ is injective since then each $\psi([s])$ maps to a unique element in S. So suppose $\psi([s]) = \psi([r])$ then $[sa] = [ra]$ so $(s-r)a = kp$ for some $k \in \mathbb{Z}$. Since p is prime this means that either p divides a or p divides $s-r$. But this is a contradiction as $a \neq 0 \pmod{p}$ and $0 < |s-r| < p$. Hence $s - r = 0$ so $[s] = [r]$. Hence $S = \mathbb{Z}_p^\times$. □

That's all we want to do with modular arithmetic for now, so we'll move back to theory of groups.

2.4 Subgroups

Definition 2.18. Let $(G, *)$ be a group and let $H \subseteq G$. Then, H is called a **subgroup** of G if $(H, *)$ is a group. We denote it as $H \leq G$.

So essentially subgroups are groups sitting inside other groups. Subsets of groups inherit some properties from the group directly so it is not strictly necessary to require all the group axioms from H. We'll soon see some easier characterisations of subgroups, but let's first look at some examples.

Example. i) $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$,

ii) $(\mathbb{Q}^\times, \cdot) \leq (\mathbb{R}^\times, \cdot)$,

iii) $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$,

iv) If $(G, *)$ is a group then it always has at least two subgroups: the trivial subgroup $\{e\}$ and the group itself G, i.e. $\{e\} \leq G$ and $G \leq G$.

Proposition 2.19. *Let $(G, *)$ be a group. A subset H of G is a subgroup if and only if*

i) *$(H, *)$ satisfies [G0] (closure), i.e.*

$$h_1, h_2 \in H \implies h_1 * h_2 \in H,$$

ii) *the identity e of G is in H,*

iii) *for all $a \in H$, we have that $a^{-1} \in H$.*

This can be simplified to the following.

Corollary 2.20 (Criteria for subgroups)**.** *Let $(G, *)$ be a group and $H \subset G$. Then $H \leq G$ if and only if*

i) *$H \neq \emptyset$ and*

ii) *$a, b \in H \implies a * b^{-1} \in H$.*

Proof of the Corollary. $\implies$ is trivial. So suppose H satisfies the two properties. Then, by the first property we can choose $a \in H$ so by the second property $a * a^{-1} = e \in H$. Now, choose $a = e$ and $b = h$ then by the second property $h, e \in H \implies e * h^{-1} = h^{-1} \in H$ so inverses are in H. Finally, for closure pick $a = h_1$, $b = h_2$ then we know by above that $h_2^{-1} \in H$ so

$$h_1, h_2 \in H \implies h_1, h_2^{-1} \in H \implies h_1 * (h_2^{-1})^{-1} \in H \implies h_1 * h_2 \in H,$$

as required. □

Proof of the Proposition. Suppose $H \leq G$. Then by definition it satisfies the closure property. Suppose $e \in G$ is the identity and that $e' \in H$ is another identity. Then for all $h \in H$

$$e' * h = h = e * h \implies e'e = e$$

by the cancellation laws for G. Finally, for $h \in H$ if h^{-1} is the inverse of h in G and $h' \in H$ is another inverse then

$$h' * h = e = h^{-1} * h \implies h' = h^{-1},$$

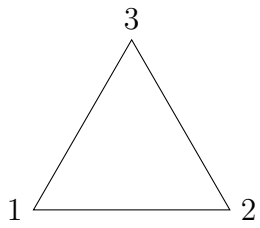
as before.

Suppose now that H satisfies the three properties, we need to prove that H is a subgroup. It suffices to prove that H is a group. By the first property we immediately obtain [G0] (closure). Associativity is inherited from G. Since the identity of G is in H and all elements of H are elements of G it follows that the identity for G works as the identity for H. Finally, we are given that the inverse of each $h \in H$ is in H so H is a group and $H \leq G$. □

We will next look at a couple of essential examples of finite groups.

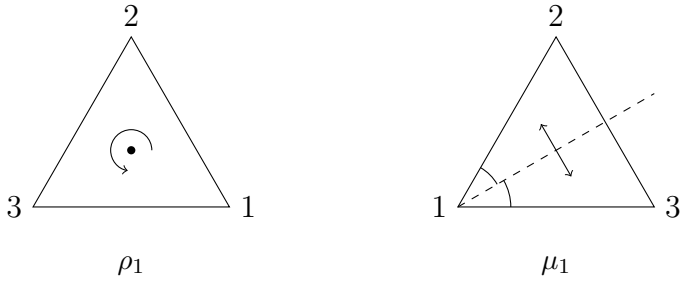
2.5 Dihedral group $\mathscr{D}_n$

Many interesting groups arise from something called *group actions*, which just means that we define a way in which our group transforms some other object[8]. Take for example an equilateral triangle and label its vertices 1, 2 and 3:



Let's now define rigid body transformations of this shape which leave it intact. These are called the *symmetries* of this triangle. So each of these will leave the actual shape of the triangle intact, but will cause the vertices to be in a different order. It turns out that each of these can be described by either a rotation about the centre of the triangle or a reflection through a bisector of any of the interior angles. Let us denote by ρ_1 the rotation by $\frac{2\pi}{3}$ and by μ_1 the reflection through the bisector of the south-west angle (no matter what the label is). So,

[8]These are sometimes called transformation groups.



ρ_1 μ_1

Let us also denote the trivial transformation (which does nothing) by ρ_0 (i.e. the identity map).

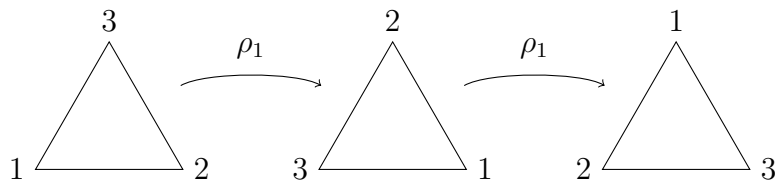
Recall from above that any symmetry just ends up permuting the vertices. Conversely, any permutation of the vertices will give us a symmetry (this is only true for triangles, you need to be more careful for general n-gons). So the full set of symmetries of the above triangle is

$$\{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\},$$

where ρ_2 is rotation by $\frac{4\pi}{3}$ and μ_2 and μ_3 are reflections corresponding to the remaining angles. The important point to notice is that these transformations form a group! (Check it yourself)

Definition 2.21. The group of symmetries of an equilaterla triangle is called the 3$^{\text{rd}}$**dihedral group** $\mathscr{D}_3$. In general the n^{th}dihedral group $\mathscr{D}_n$ is the group of symmetries of a regular n-gon with $|\mathscr{D}_n| = 2n$.

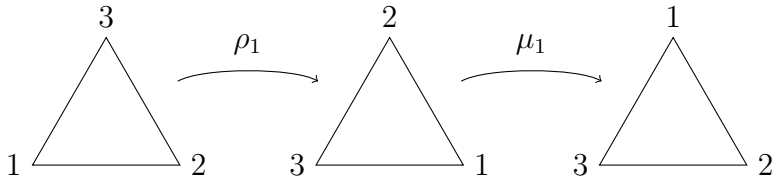
There are some interesting properties that these transformations have. For example,



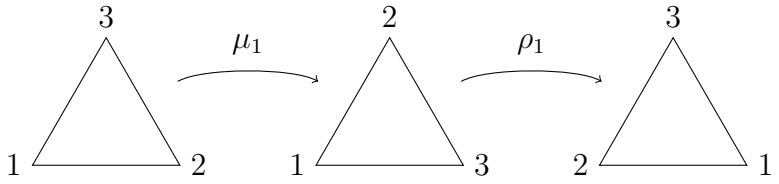
which shows that applying ρ_1 twice gives us the same result as applying ρ_2 once, i.e.

$$\rho_1^2 = \rho_2.$$

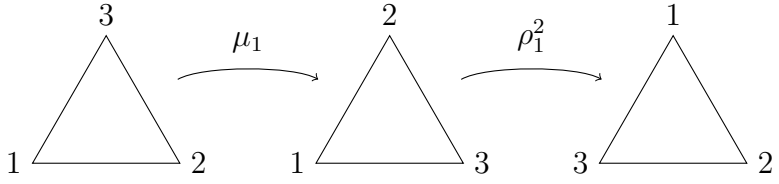
Similarly one can see that $\rho_1^3 = \rho_0$ and $\mu_1^2 = \rho_0$. Let us look at something more exciting.



This is $\rho_1\mu_1$. Let us compare it with $\mu_1\rho_1$.



We notice that the result is different! Hence $\mathscr{D}_3$ is not abelian. Instead,



gives the same result. So we have shown that

$$\mu\rho = \rho^2\mu.$$

It is possible then to show[9] that the third dihedral group then consists of the set

$$\mathscr{D}_3 = \{e, \rho, \rho^2, \mu, \rho\mu, \rho^2\mu\},$$

[9]But it won't be done rigorously in this course.

where we have written ρ instead of ρ_1 and μ instead of μ_1 and e instead of ρ_0. These satisfy,

$$e = \rho^3 = \mu^2 \quad \text{and} \quad \mu\rho = \rho^2\mu.$$

Usually we write this in a shorter form

$$\mathscr{D}_3 = \langle \rho, \mu | \rho^3 = \mu^2 = e, \mu\rho = \rho^2\mu \rangle.$$

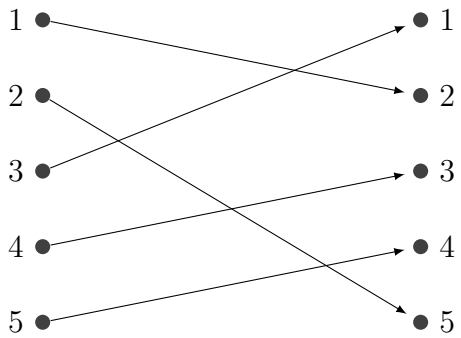
This is called the *presentation of the group*. A couple of things to notice here. There was nothing special about our choice of ρ and μ, we could've equally well have chosen $\rho = \rho_2$ and $\mu = \mu_3$ for example.

2.6 Permutations

The next important example of groups are permutations, which are somewhat related to the actions mentioned above (recall that each symmetry corresponded to a permutation of the vertices). Let us start by giving a precise definition.

Definition 2.22. A **permutation** of a countable[10] set $A \neq \emptyset$ is a bijection from A to A. We denote the set of all permutations on A by S_A. The set of permutations on the set $\{1, 2, \ldots, n\}$ is denoted simply by S_n.

Example. So take for example $n = 5$, then a permutation $\sigma \in S_5$ could be



[10] A being countable means that there is a bijection between A and some nonempty subset of $\mathbb{N}$. So, e.g. $\mathbb{N}$, $\{0, 1\}$, $\mathbb{Z}$ are all countable.

which we can see is a bijective function with $\sigma(1) = 2$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 3$ and $\sigma(5) = 4$.

Normally we denote permutations by small Greek letters like σ, τ, μ. Instead of having to draw arrows we can use the **functional notation** and write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

for arbitrary permutation σ. So for example the permutation above can also be written as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}.$$

We know want to define a binary operation which works on permutations. Since these are functions a natural choice would be the composition of functions.

Definition 2.23. Let $\sigma, \tau \in S_n$, then $\sigma\tau \in S_n$ is the **composition** of the permutations σ and τ (sometimes read as the "product of σ and τ", but not to be confused with multiplication) as functions.

Example. Take $\sigma, \tau \in S_5$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix},$$

while

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}.$$

So we can see that in general $\sigma\tau \neq \tau\sigma$ as composition of functions is not commutative.

Theorem 2.24. *Let $A \neq \emptyset$, then $(S_A, \circ)$ is a group with respect to composition of permutations. If $A = \{1, 2, \dots, n\}$, then $(S_n, \circ)$ is called the* ***symmetric group*** *on n letters and $|S_n| = n!$.*

Proof. We'll prove this for S_n. For any of the n elements of $\{1, \ldots, n\}$ we can map it to any element in $\{1, \ldots, n\}$, for the next element we can map it to any of the remaining $n-1$ elements and so on. So for the first element there are n choices, for the second $n-1$ etc. This process will yield all the bijections on $\{1, \ldots, n\}$, which means that

$$|S_n| = n(n-1)\ldots 2 \cdot 1 = n!.$$

You have proven that composition of bijections is associative in the homework. We have also shown that a composition of two bijections is a bijection. The obvious identity is id_A. If $\sigma \in S_n$,

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

then

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \ldots & \sigma(n) \\ 1 & 2 & \ldots & n \end{pmatrix},$$

up to rearrengement of columns. □

This proof also gives us a way of calculating inverse permutations. Let's see how this works in practice.

Example. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \in S_6,$$

then

$$\begin{aligned} \sigma^{-1} &= \begin{pmatrix} 3 & 1 & 4 & 5 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}. \end{aligned}$$

When working with the dihedral group we noticed that if we take high enough power of any element we will eventually arrive at the identity. Let us see what happens with permutations.

Consider the following relation on the set A. Fix a permutation $\sigma \in S_A$. Let $a, b \in A$, then

$$a \sim_\sigma b \iff \exists k \in \mathbb{Z} \text{ such that } b = \sigma^k(a).$$

So any powers of $\sigma(a)$ (or indeed $a = \sigma^0(a)$) are related. We will prove that this is in fact an equivalence relation.

Theorem 2.25. *Fix $\sigma \in S_A$. Then $\sim_\sigma$ is an equivalence relation on A.*

Proof. We have to show $\sim_\sigma$ is reflexive, symmetric and transitive.

- We need to show that $a \sim_\sigma a$ this is the same as having for some $k \in \mathbb{Z}$, $a = \sigma^k(a)$. But this is of course satisfied if we pick $k = 0$ so $\sim_\sigma$ is reflexive.
- Suppose $a \sim_\sigma b$, then for some $k_1 \in \mathbb{Z}$ we have $b = \sigma^{k_1}(a)$. Then

  $$a = (\sigma^{k_1})^{-1}(b) = \sigma^{-k_1}(b) = \sigma^{k_2}(b),$$

  where $k_2 = -k_1$. Thus $b \sim_\sigma a$ so $\sim_\sigma$ is symmetric.
- Now let $a \sim_\sigma b$ and $b \sim_\sigma c$. So $b = \sigma^{k_1}(a)$ and $c = \sigma^{k_2}(b)$, then

  $$c = \sigma^{k_2}(b) = \sigma^{k_2}(\sigma^{k_1}(a)) = \sigma^{k_1+k_2}(a),$$

  which means that $a \sim_\sigma c$.

Hence $\sim_\sigma$ is an equivalence relation. □

Recall that to any equivalence relation we can associate equivalence classes on the underlying set. We can repeat the above process for an arbitrary group G (with some additional information) and the equivalence classes turn out to be really important. We will now see how this works in the case of S_n.

Definition 2.26. Let $\sigma \in S_A$ be fixed. Then the equivalence classes of $\sim_\sigma$ are called **orbits** of σ. Let $a \in A$, then its orbit is

$$[a]_{\sim_\sigma} = \{b \in A : \exists k \in \mathbb{Z} \text{ s.t. } \sigma^k(a) = b\}.$$

In particular the number of distinct orbits for a fixed σ will somehow measure how close it is to being the identity. This is because a always belongs to its only orbit and if $\sigma(a) = a$ then a is the only element in its orbit. Of course if you consider the identity permutation then all orbits consist of one element so there are n distinct orbits. Let's look at an example.

Example. Let $\sigma \in S_8$ be

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 1 & 3 & 8 & 6 & 7 \end{pmatrix}.$$

Denote the orbits by B_i. The first orbit is then

$$B_1 = [1]_{\sim_\sigma} = \{1, 4\}$$

since σ maps 1 to 4 to 1. But by this reasoning of course this is the orbit of 4 as well as 4 maps to 1 maps to 4 by σ. So $[1]_{\sim_\sigma} = [4]_{\sim_\sigma} = B_1$. The next available element is 2:

$$B_2 = [2]_{\sim_\sigma} = \{2, 5, 3\}$$

As before we can tell that the orbits of 5 and 3 will be the same as the orbit of 2, i.e.

$$[3]_{\sim_\sigma} = [2]_{\sim_\sigma}, \quad [5]_{\sim_\sigma} = [2]_{\sim_\sigma}.$$

The next remaining number is 6, so we look at its orbit

$$B_3 = [6]_{\sim_\sigma} = \{6, 8, 7\}$$

and thus this is also the orbit of 8 and 7. There's no number remaining so we conclude that S_8 has 3 distinct orbits B_1, B_2 and B_3.

So previously we discussed the case when there are many orbits for a given σ. Now we'll look at the case when there aren't that many, and, in particular, when there is exactly one orbit. This is the same as saying that each number is in a single orbit.

Definition 2.27. Consider $A = \{1, 2, \ldots, n\}$. A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing k elements, with $k > 1$. k is called the **length** of the cycle. If σ is a cycle we write

$$\sigma = (a_1, a_2, a_3, \ldots, a_k),$$

where $a_{j+1} = \sigma(a_j)$ for $j = 1, \ldots, k-1$ and $a_1 = \sigma(a_k)$.

Example. i) Look at the permutation $\sigma \in S_5$ given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

There are 2 orbits:

$$\{1, 3, 5, 4\} \text{ and } \{2\}.$$

Hence there is only one orbit with more than 1 element so σ is a cycle. It has length 4 and we can write it as

$$\sigma = (1, 3, 5, 4).$$

Notice that it doesn't matter from which number we begin, so

$$\sigma = (3, 5, 4, 1) = (5, 4, 3, 1) = (4, 3, 1, 5)$$

are all equally valid as well.

ii) Take the $\sigma \in S_8$ from the previous example, where

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 1 & 3 & 8 & 6 & 7 \end{pmatrix}.$$

We saw that there are more than one orbits of length greater than 1, thus this σ is not a cycle. However we can write it as a product of cycles as

$$\sigma = (1, 4)(2, 5, 3)(6, 8, 7).$$

Notice that it doesn't matter in which order we write the cycles since they are disjoint, i.e. any number appears in only one cycle.

Let us give a precise definition for disjointness.

Definition 2.28. Consider k cycles in S_A. The cycles are said to be **disjoint** if no element appears in 2 different cycles.

Example. $(1, 6)$, $(7, 8, 9)$ and $(2, 3, 5)$ are disjoint cycles in S_9.

Remark. Product of disjoint cycles is commutative. For example,

$$(1, 4)(2, 5, 3)(6, 8, 7) = (2, 5, 3)(1, 4)(6, 8, 7) = (6, 8, 7)(2, 5, 3)(1, 4)$$

and so on.

The reason why cycles are important is that they function a little bit like primes in integers: we can build every permutation out of a unique product of cycles.

Theorem 2.29. *Every permutation σ of a finite set A is a product of disjoint cycles. This product is unique (up to reordering of the factors).*

Proof. Suppose $A = \{1, 2, \ldots, m\}$ (otherwise we can just relable the elements of the set A). Let $B_1, B_2, \ldots, B_r$ be the orbits of σ and define the cycles μ_j by

$$\mu_j : A \to A, \quad \mu_j(x) = \begin{cases} \sigma(x), & \text{for } x \in B_j \\ x, & \text{otherwise.} \end{cases}$$

So the cycle μ_j only touches elements in the j^{th}orbit. So for example, we have that

$$B_1 = \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^p(1)\}$$

for some p, and then

$$\mu_1(x) = \begin{cases} \sigma(x), & \text{for } x \in B_1 \\ x, & \text{otherwise.} \end{cases}$$

So we can write,

$$\mu_1(x) = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^r(1))$$

supposing that $\sigma^{r+1}(1) = 1$. Similarly, if

$$B_2 = \{\tilde{x}, \sigma(\tilde{x}), \ldots, \sigma^s(\tilde{x})\}$$

for some s and where $\tilde{x}$ is the next available number, then

$$\mu_2(x) = \begin{cases} \sigma(x), & \text{for } x \in B_2 \\ x, & \text{otherwise.} \end{cases}$$

So,

$$\mu_2 = (\tilde{x}, \sigma(\tilde{x}), \sigma^2(\tilde{x}), \ldots, \sigma^s(\tilde{x})),$$

if $\sigma^{s+1}(\tilde{x}) = \tilde{x}$.

Now we can write $\sigma = \mu_1 \mu_2 \ldots \mu_r$. Since the equivalence classes, i.e. the orbits of $\sim_\sigma$, are disjoint, then the cycles $\mu_1, \ldots, \mu_r$ are disjoint as well. $\square$

A particularly interesting special case of cycles are cycles of length two.

Definition 2.30. A **transposition** is a cycle of length 2.

Example. $\sigma = (1,3) \in S_5$ is a transposition, which we can also write as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

So transpositions just exchange the place of two elements.

Given any cycle $(a_1, a_2, \ldots, a_k)$ we can decompose it into a product of transpositions as

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2).$$

Check that this works! Beware though, this decomposition is not unique and we could equally well write for example

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_2, a_3) \ldots (a_{k-2}, a_{k-1})(a_{k-1}, a_k).$$

Putting together these observations gives us the following corollary.

Corollary 2.31. *Every permutation $\sigma \in S_n$ can be decomposed into a product of transpositions.*

Remember that this decomposition is not unique, unlike the decomposition into cycles. Moreover the transpositions will not be disjoint in general.

Proof. By the previous theorem, σ can be composed uniquely into a product of cycles, say,

$$\sigma = \mu_1 \ldots \mu_r.$$

By the observation above we can decompose each of the μ_i into a product of transpositions. □

There is something we can say about the decomposition into transpositions.

Theorem 2.32. *Let σ be a permutation of S_n. Then the number of factors in any decomposition of σ into a product of transpositions is either always an even number or always an odd number.*

The proof is omitted. We see that the decomposition is unique up to the parity of the number of transpositions. This allows us to classify permutations as follows.

Definition 2.33. A permutation $\sigma \in S_n$ is called **even** if it is the product of an even number of transpositions. Similarly, σ is called **odd** if it is the product of an odd number of transpositions.

The **signature** of σ is defined to be the number

$$\operatorname{sign}(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ is even,} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

Example. If $\sigma = (1,3,4,7)$ then we can write $\sigma = (1,7)(1,4)(1,3)$ as a product of odd number of transpositions, hence $\operatorname{sign}\sigma = -1$. In general you can notice that if you have a cycle of length k, say τ, then you can write it as a product of $k-1$ transpositions. Hence

$$\operatorname{sign}\tau = (-1)^{k-1}.$$

Moreover, in the homework you will prove that $\operatorname{sign}(\sigma\tau) = \operatorname{sign}\sigma \operatorname{sign}\tau$ which will give you a quick way of computing the sign of any permutation. Suppose, for example, that

$$\rho = (1,2,3,4)(5,6)(8,7,9).$$

Then in order to compute the sign of ρ we compute the sign of each cycle, write it underneath the cycle and multiply them together to get the sign of ρ:

$$\rho = \underset{-1}{(1,2,3,4)}\underset{-1}{(5,6)}\underset{+1}{(8,7,9)}_{=+1}$$

i.e. $\operatorname{sign}\rho = +1$.

2.7 Cyclic Groups

We will next formalise the concept that if you keep taking powers of an element in a group you eventually end up back at the identity. We've already seen how this works for $\mathscr{D}_3$ and S_n.

Definition 2.34. Let $(G, *)$ be a group and fix $a \in G$. Then the least integers $n \in \mathbb{N}$, $n > 0$, such that

$$a^n = e$$

is called the **order** of a, denoted by $o(a)$. If $a^n \neq e$ for every $n > 0$ then we write that $o(a) = \infty$.

So to phrase this in terms of S_n we have

Corollary 2.35. *Let $(S_n, \circ)$ be the symmetric group on n letters and let $\sigma \in S_n$ be a cycle of length k. Then*

$$o(\sigma) = k.$$

Proof. Omitted. □

Example. If $\sigma \in S_5$ is $\sigma = (1, 3, 5, 4)$ then $\sigma^4(i) = i$ for any $0 < i \leq 5$, and 4 is the smallest such integer. Hence, $o(\sigma) = 4 =$ length of σ.

We can say a couple of things about the order of any element $a \in G$.

Theorem 2.36. *Let $(G, *)$ be a group. Then*

i) *$o(e) = 1$ and e is the only element of order 1 in G,*

ii) *if $b \in G$ and $o(b) = r$, then $o(b^{-1}) = r$, and*

iii) *if $a \in G$ and $o(a) = m$, then $a^q = e \iff m|q$.*

Proof. i) $o(e) = 1$ by definition and it is the only element with order 1 since e is unique.

ii) $b^r = e$ means that $(b^{-1})^r = (b^r)^{-1} = e^{-1} = e$ by the rules for exponentiation that we have learnt before.

iii) This is an if and only if statement so we have to prove two directions:

$\underline{\Longleftarrow}$**:** Suppose m divides q so we can write $q = km$ for some $k \in \mathbb{Z}$. Then

$$a^q = a^{km} = (a^m)^k = e.$$

$\underline{\Longrightarrow}$**:** Now suppose that $a^q = e$ and, for contradiction, that m does not divide q. Then we can divide q by m with a remainder r to obtain

$$q = km + r$$

for some $0 < r \leq m - 1$. Then

$$a^r = a^{q-km} = a^q a^{-km} = a^q (a^m)^{-k} = e$$

by our assumptions. But $r < m = o(a)$, which is a contradiction. Thus $r = 0$ and so $m|q$.

□

So we've already seen how to find the order of any cycle by inspecting the length of the cycle. Now we'll see how to generalise this for any permutation in S_n. This hinges on the fact that any permutation can be decomposed into disjoint cycles which we've proved previously.

Corollary 2.37. *Let $\sigma \in S_n$. Write σ as a product of disjoint cycles $\sigma = \mu_1 \mu_2 \dots \mu_s$. Then the order $o(\sigma)$ is the least common multiple of the orders of the cycles μ_j, where $j = 1, \dots, s$.*

Proof. Consider $\sigma = \mu_1 \mu_2$ product of 2 disjoint cycles with $o(\mu_1) = p$, $o(\mu_2 = q$ and $o(\sigma) = r$. Then,

$$\sigma^r = e \implies \mu_1^r \mu_2^r = e$$

by associativity and commutativity of composition of disjoint cycles. By commutativity we also have that

$$\mu_2^r \mu_1^r = e.$$

So we have a product of two elements in a group being equal to the identity. Of course this means that either they both are equal to the identity, or one is the inverse of the other. In other words, we have the following two cases:

i) $\mu_1^r = e$ and $\mu_2^r = e$, or

ii) $\mu_2^r = (\mu_1^r)^{-1}$.

The second case is impossible since μ_1 and μ_2 are disjoint which means the LHS only acts on different elements than the RHS. Hence we are in the first case. This means that $p|r$ and $q|r$ by the previous theorem. So r is a multiple of both p and q, the orders of μ_1 and μ_2. Suppose $r \neq \text{lcm}(p,q)$ and let $\tilde{r} = \text{lcm}(p,q)$ (so $r \neq \tilde{r}$). Hence we can write $\tilde{r}$ as $\tilde{r} = ap$ and $\tilde{r} = bq$ for some $a, b \in \mathbb{Z}$. Thus,

$$\sigma^{\tilde{r}} = \mu_1^{\tilde{r}} \mu_2^{\tilde{r}} = \mu_1^{ap} \mu_2^{bp} = (\mu_1^p)^a (\mu_2^q)^b,$$

where we have used different expressions for $\tilde{r}$ depending on whether we deal with μ_1 and μ_2. But now we are raising both of them to the power of their order so we get that

$$\sigma^{\tilde{r}} = e \cdot e = e.$$

But remember that we showed that r is a common multiple of p and q and we assumed it is not the least one. This means that $\tilde{r} < r$ since $\tilde{r}$ is the least common multiple of p and q. This is a contradiction as $\tilde{r} < r = o(\sigma)$, but $\sigma^{\tilde{r}} = e$. Hence $r = \tilde{r} = \text{lcm}(p,q)$. We can now generalise this argument by induction to any finite number of disjoint cycles. □

Let's see how this works in practice.

Example. Take $\sigma \in S_8$ to be

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 2 & 1 & 3 & 8 & 6 & 7 \end{pmatrix}.$$

We can decompose σ as

$$\sigma = (1,4)(2,5,3)(6,8,7) = \mu_1\mu_2\mu_3,$$

say. We know how to compute the order of a cycle, so $o(\mu_1) = 2$, $o(\mu_2) = 3$, $o(\mu_3) = 3$. The previous corollary implies that $o(\sigma) = \text{lcm}(2,3,3) = 6$. Hence

$$\sigma^6 = e.$$

Now that we know how the order of an element of a group works, we can characterize the nicest groups that you could think of—the cyclic groups.

Definition 2.38. A group $(G, *)$ is called **cyclic** if its elements are powers of a common element $a \in G$, i.e. we can write that

$$G = \{a^n : n \in \mathbb{Z}\}.$$

We say that a is a **generator** of G and we write $G = \langle a \rangle$.

We can explain the above definition in terms of orders of the group and its elements:

Theorem 2.39. *Let $(G, *)$ be a group and $a \in G$. Then,*

i) *$H = \{a^n : n \in \mathbb{Z}\}$ is an abelian subgroup of G of order $o(a)$, that is, the powers of a form a subgroup;*

ii) *if $|G| = m$ (m is finite), then G is cyclic if and only if $\exists b \in G$ such that $o(b) = m$. This is the same as saying that $H = G$ where H corresponds to powers of the element b.*

For the proof we will use the criteria for subgroups.

Proof. i) By choosing $n = 1$ we can see that $a \in H$, so in particular $H \neq \emptyset$. If $b, c \in H$ then we need to prove that $b * c^{-1} \in H$. By definition H is

the set of powers of a so we can write b and c as $b = a^p$ and $c = a^q$ for some $p, q \in \mathbb{Z}$. Hence[11],

$$b * c^{-1} = a^p * (a^q)^{-1} = a^p a^{-q} = a^{p-q} \in H$$

because we have expressed $b * c^{-1}$ as a power of a. To prove that H is abelian we show that b and c commute:

$$b * c = a^p * a^q = a^{p+q} = a^{q+p} = a^q * a^p = c * b.$$

So H is abelian and in particular $|H| =$ number of distinct powers of a $= o(a)$, by definition.

ii) It is enough to consider G of the form $G = \{e, b, b^2, \ldots, b^{s-1}\}$ for some $s = |G|$ with $o(b) = s$.

$\underline{\Longrightarrow}$**:** Suppose G is cyclic, we want to find an element of order m from G. Since $G = \langle b \rangle$ (as it is cyclic) we can suspect that one element of order m should be b. Let's prove this. From the previous part we know that if we look at the subset $H = \langle b \rangle$ of G then not only is H a subgroup of G, but it satisfies $|H| = o(b)$. But we assumed that G is cyclic with $G = \langle b \rangle = H$ then $|G| = o(b) = |G|$, as required.

$\underline{\Longleftarrow}$**:** Suppose we have an element of order $m = |G|$ in G. Call it b. Look, again, at $H = \langle b \rangle$. Then by part (a) this is a subgroup of G. But by assumption the order of H, which is the order of b, is equal to the order of G, i.e. $|H| = o(b) = m = |G|$. So we have a subgroup of G with the same order as G itself which means that the subgroup must be the whole group, i.e. $H = G$. This means that $G = \langle b \rangle$, so G is cyclic and of course abelian (by part (a), again).

□

[11]Notice that I tend to drop the notation $*$ for the group operation and just write products of elements as standard multiplication. This makes it easier to read and causes no confusion since the group operation is always clear from the context (and remains unchanged).

Since cyclic groups are so common we wish to give them a special notation. If $G = \langle a \rangle$ is a cyclic group and $o(a) = n$ then G is called the **cyclic group of order** n denoted C_n. Hence

$$C_n = \{e, a, a^2, \ldots, a^{n-1}\}.$$

If, on the other hand, $o(a) = \infty$, then G is called the **infinite cyclic group**, denoted by C_∞, so

$$C_\infty = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}.$$

So for example $(\mathbb{Z}, +)$ is generated by 1, which has an infinite order so $\mathbb{Z}$ is in fact C_∞, while $(\mathbb{Z}_m, +)$ is C_m. We'll make this identification more precise later when we talk about isomorphisms. Then we'll make it precise that both $\mathbb{Z}$ and $3\mathbb{Z}$ are actually the same group (same meaning same in the sense of isomorphism).

2.8 Cosets and Lagrange's Theorem

In this section we will prove our most important theorem about groups known as Lagrange's Theorem. In order to do this we have to look at something called *cosets* which can be understood in terms of partitions of an equivalence relation, which we've met before.

Definition 2.40. Let H be a subgroup of a group $(G, *)$. The subset

$$aH = \{a * h : h \in H\}$$

is called the **left coset** of H containing a, while

$$Ha = \{h * a : h \in H\}$$

is called the **right coset** of H containing a.

Remark. If G is abelian then $aH = Ha$, i.e. all the left and righ cosets coincide.

Let's do an example of computing cosets.

Example. Let $G = (\mathbb{Z}_6, +)$. This is an abelian group. Consider the subgroup $H = \{[0], [3]\}$ of G. Notice first that $[0]H = H$. Now, let $a = [1]$, then

$$aH = \{a + h : h \in H\} = \{[1], [4]\} = [1]H.$$

If $a = [2]$ then

$$aH = \{[2], [5]\} = [2]H$$

. If $a = [3]$ then we see that $aH = H$ and this pattern repeats for $[4]$ and $[5]$. Hence we can decompose G as

$$\mathbb{Z}_6 = H \cup [1]H \cup [2]H = H \cup \{[1], [4]\} \cup \{[2], [5]\}.$$

We'll prove Lagrange's Theorem by using two lemmas. We'll work with left cosets here, but everything would work exactly the same if we chose to use right cosets instead.

Lemma A. Every coset (left or right) of a subgroup H of a group G has the same number of elements as H, i.e.

$$|H| = |aH|.$$

Proof. Consider $a \in H$ and aH the corresponding left coset. In order to prove that these two sets have the same size we need to find a bijection between them. Define a map $\phi : H \to aH$ by $h \mapsto ah$. This is a surjection since if $b \in aH$ then we can write $b = ah_1$ for some $h_1 \in H$ ($h_1 = a^{-1}b$). It follows that $b = \phi(h_1)$ so it is surjective.

Let's now prove that ϕ is injective. Suppose $\phi(h_1) = \phi(h_2)$, then by definition $ah_1 = ah_2$. By the cancellation laws we get that $h_1 = h_2$. Hence ϕ is injective and thus bijective. This implies that $|H| = |aH|$. Notice that this proof is valid even if H is not finite. □

Lemma B. Let H be a subgroup of G. The relation

$$a \sim b \iff a^{-1}b \in H \iff b \in aH$$

for $a, b \in G$, is an equivalence relation on G. It defines a partition of G having as equivalence classes the left cosets

$$aH = \{b \in G : b = ah \text{ for some } h \in H\}.$$

Proof. We need to prove that $\sim$ is reflexive, symmetric and transitive. Reflexive means that $a^{-1}a \in H$, but $a^{-1}a = e \in H$ since H is a subgroup so it has to contain the identity. Hence $a \sim a$.

Now, look at $a \sim b$. So, $a^{-1}b \in H$. Since H is a subgroup it is closed under inverses so $(a^{-1}b)^{-1} \in H$, i.e. $b^{-1}a \in H$. This means by definition that $b \sim a$ so $\sim$ is symmetric.

Finally, suppose that $a \sim b$ and $b \sim c$. Then $a^{-1}b, b^{-1}c \in H$, but their product must lie in H too. Hence $a^{-1}c = a^1bb^{-1}c \in H$. Thus $a \sim c$ and so $\sim$ is an equivalence relation. □

Hence G is partitioned into the left cosets of H. This implies, in particular, that all cosets are either equal or disjoint. So each $g \in G$ belongs to exactly one coset.

Lagrange's Theorem. Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof. Let $|G| = n < \infty$, and $|H| = m \leq n$. By Lemma A every coset of H has m elements, too. By Lemma G is the disjoint union of its left or right cosets. Hence $n = rm$ where r is the number of left cosets and m is the number of elements in each left coset. Thus m is a divisor of n. □

Definition 2.41. The **index of H in G** is the number $|G|/|H|$, i.e. the number of left (right) cosets of H. We denote the index by $[G : H]$.

So in some sense the index of a subgroup is a measure of how close it is to being the whole group G. For example if the index is 2 then H contains half of the elements of G.

Corollary 2.42. *Let $|G| = n$. Then the order $o(a)$ of any element $a \in G$ is a divisor of n.*

Proof. Consider $H = \langle a \rangle$, the cyclic subgroup generated by a. We know $|H| = o(a)$, hence by Lagrange's Theorem $o(a)$ divides the order of G. □

Let's just verify Lagrange's Theorem in some simple cases.

Example. i) Look at $(\mathscr{D}_6, \circ)$, the 6th dihedral group. Let $H = \langle \rho \rangle$ be the cyclic subgroup generated by the rotation by $2\pi/6$. By Lagrange's Theorem $|H|$ divides 12, which is indeed the case as $|H| = o(\rho) = 6$ and $|\mathscr{D}_6| = 12$.

ii) You can also use Lagrange's Theorem to say things about arbitrary groups. For example, if $|G| = 10$ then G cannot have a subgroup of order 6. In fact, if H is a subgroup with more than 5 elements then it is automatically all of G as any subgroup is of order 1, 2, 5 or 10.

We'll conclude our discussion of cyclic groups by an important consequence of Lagrange's Theorem. This will allow us to easily characterise (and find) subgroups of any cyclic group.

Theorem 2.43. *Every subgroup of a cyclic group G is also cyclic.*

Proof. Let $G = \langle g \rangle$ be generated by g. Let $H \leq G$ be a subgroup of G. Then any $h \in H$ is of the form $h = g^m$ for some $m \in \mathbb{Z}$. We claim that $H = \langle \tilde{h} \rangle = \langle g^{\tilde{m}} \rangle$ where $\tilde{h}$ is the element in H with the smallest power $\tilde{m}$ in its representation as a power of g. Let $h \in H$, then $h = g^s$ for some $s \geq \tilde{m} \geq 0$. By the remainder theorem we can write $s = q\tilde{m} + r$ for some $0 \leq r \leq \tilde{m} - 1$, and so

$$g^r = g^{s - q\tilde{m}} = g^s g^{-q\tilde{m}} = g^s (g^{\tilde{m}})^{-q} = h\tilde{h}^{-q} \in H.$$

So $g^r \in H$ with $r < \tilde{m}$. This implies that $r = 0$ since $\tilde{m}$ was chosen to be minimal. Hence $h = g^s = (g^{\tilde{m}})^q = \tilde{h}^q$. □

2.9 Isomorphisms of Groups

A huge problem in group theory is to determine how many different possible groups there are of a given size n. For example, there can be only one group of size 1 since every group must contain the identity. Same goes for groups of size 2 since it has to contain an identity which leaves over one element which has to be its own inverse as there are no more elements left. This is called *classification of finite groups*. Of course, as stated, there's some ambiguity involved. What is the group operation in our group of size 1 or 2? And what exactly are the elements? They could be numbers from $\mathbb{Z}$ or just some arbitrary elements. The key insight here is that the choice of elements or the group operation doesn't matter to a certain extent since a lot of the structure of the group is forced by the group axiom (the definition of a group). Also, we saw earlier that, for example, $\mathbb{Z}$ and $3\mathbb{Z}$ form the same kind of infinite cyclic group. We will say that 2 groups are isomorphic if they have the same structure (same number of elements, same interactions between each element etc.). In order to define isomorphisms we start with the notion of a group homomorphism, which is just a structure preserving mapping between groups.

Definition 2.44. Let $(G_1, *)$ and $(G_2, \bullet)$ be two groups. A mapping $\phi : G_1 \to G_2$ is called a **homomorphism** if it preserves the group product, i.e. if for all $a, b \in G_1$ we have

$$\phi(a * b) = \phi(a) \bullet \phi(b).$$

Theorem 2.45. *Let G_1, G_2 and ϕ be as before. Then,*

i) *If e_1 is the identity of G_1, then $\phi(e_1)$ is the identity of G_2,*

ii) *if $a \in G_1$, then $\phi(a^{-1}) = \phi(a)^{-1}$,*

iii) *if $H \leq G_1$ then $\phi(H) \leq G_2$,*

iv) *if $K \leq G_2$ then $\phi^{-1}(K) \leq G_1$, where $\phi^{-1}(K)$ is the set of preimages of K.*

Essentially what the theorem says is that homomorphisms map identities to identities, inverses to inverses and preserve subgroups.

Proof. i) $\forall a \in G_1$ we have that $a = a * e_1$, thus

$$\begin{aligned}\phi(a) &= \phi(a * e_1) \\ &= \phi(a) \bullet \phi(e_1).\end{aligned}$$

Now from cancellation laws it follows that $\phi(e_1) = e_2$, the identity of G_2.

ii) By previous part we have

$$\begin{aligned}e_2 &= \phi(e_1) \\ &= \phi(a * a^{-1}) \\ &= \phi(a) \bullet \phi(a^{-1}).\end{aligned}$$

Multiplying both sides by $\phi(a)^{-1}$ yields $\phi(a^{-1}) = \phi(a)^{-1}$.

iii) See Fraleigh for the remaining proofs.

□

An isomorphism is simply a bijective homomorphism.

Definition 2.46. An **isomorphism** $\phi : G_1 \to G_2$ between the groups G_1 and G_2 is a bijective homomorphism. We denote this by writing $G_1 \cong G_2$.

It is easy to see that the inverse mapping ϕ^{-1} is also an isomorphism. Let's look at some examples of isomorphisms.

Example. i) Let $(G_1, *) = (\mathbb{R}, +)$ and $(G_2, \bullet) = (\mathbb{R}^+, \cdot)$. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ by $x \mapsto e^x = \phi(x)$. Here $\mathbb{R}^+ = \{a \in \mathbb{R} : a > 0\}$. We'll show that this is an isomorphism. It is easy to see that this is a bijection as the inverse map is given by the natural logarithm. To see that it is a homomorphism we look at

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x) \cdot \phi(y).$$

Hence $\mathbb{R} \cong \mathbb{R}^+$. Prove that ϕ^{-1} is an isomorphism as an exercise.

ii) We mentioned this example before: let $(G_1, *) = (\mathbb{Z}, +)$ and $(G_2, \bullet) = (2\mathbb{Z}, +)$. Here the isomorphism is given by $\phi : G_1 \to G_2$, $x \mapsto 2x = \phi(x)$. Obviously this is a bijection. For homomorphism we check

$$\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y).$$

Hence $\mathbb{Z} \cong 2\mathbb{Z}$.

iii) Consider $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ given by $\phi(x) = x^5$. This is again clearly an isomorphism (the inverse is given by taking the fifth root). It is, however, not a homomorphism.

$$\phi(x + y) = (x + y)^5 \neq x^5 + y^5 = \phi(x) + \phi(y).$$

Try to prove as an exercise that if $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ are isomorphisms then $\psi \circ \phi : G_1 \to G_3$ is also an isomorphism. There are many more properties which are preserved by isomorphism. We'll list a few (without proof). Suppose $G_1 \cong G_2$, then

i) $|G_1| = |G_2|$,

ii) G_1 is cyclic $\iff$ G_2 is cyclic,

iii) G_1 is abelian $\iff$ G_2 is abelian,

iv) $o(a) = p \iff o(\phi(a)) = p$,

v) both groups have exactly the same subgroup structure.

This concludes the theoretical part of groups that we'll cover. It is not the last we've heard of groups, however, as they are ubiquitous in mathematics. Then we can but this theory we've learnt into more practical use and hopefully it will highlight the importance of covering some abstract theory.

Chapter 3

Linear Algebra

For the remainder of the course we'll concentrate on a fairly simple but important problem, that is, solving systems of linear equations. Rather than attempting to solve these systems by inefficiently substituting variables as you might be used to doing from school, we'll develop an algorithm which always guarantees us a procedure which will either produce a solution or tell us that there are none. This will be done by expressing the system in terms of matrices. Having done this enables us to apply the knowledge to the world of vector spaces which culminates in diagonalisation of matrices. This is essentially the process of finding the nicest possible form for a matrix which still shares properties with the original matrix. It has uses in many physical and computational problems in the real world.

Let's state the problem more precisely. We can do it in three different ways:

A) We start with the system of linear equations, e.g.

$$\begin{cases} x_1 & +2x_2 & -3x_3 & = 0 \\ 2x_1 & -2x_2 & -x_3 & = -1 \\ -3x_1 & +5x_2 & +x_3 & = 3, \end{cases} \tag{3.1}$$

which is a system of 3 equations in 3 unknowns x_1, x_2 and x_3. We ask the following questions:

- How to solve this equation?
- What can we say about a system of n equations with m unknowns?

As said above we wish to come up with a systematic way of coming up with the solution to this system.

B) We will now rephrase these questions in terms of matrices. Let A be the following 3×3 matrix:

$$A = \begin{pmatrix} 1 & 2 & -3 \\ 2 & -2 & -1 \\ -3 & 5 & 1 \end{pmatrix}.$$

This is called the matrix of coefficients. We can rewrite (3.1) as

$$A\mathbf{x} = \mathbf{b}, \tag{3.2}$$

where $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ is the vector of unknowns and $\mathbf{b} = \begin{pmatrix} 0 \\ -1 \\ 3 \end{pmatrix}$ is the vector of constants. In order to study the previous questions from this perspective we need to determine how various operations on A affect the set of solutions of our system of equations. Moreover, we will investigate what various properties of A tell us about the original system of equations.

C) Finally, we move to study vector spaces and linear transformations. For our purposes this will essentially reduce to studying maps of the form $T : \mathbb{R}^3 \to \mathbb{R}^3$ with $\mathbf{x} \mapsto A\mathbf{x}$, where $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$. Here, $\mathbb{R}^3$ is something called a "vector space" and T a "linear transformation". It is not surprising that studying the mapping T we get information about the matrix A which ultimately provides us information about the possible solutions of (3.1). Of course we can state this problem in terms of linear maps as well: we wish to find all $\mathbf{x}$ such that

$$T(\mathbf{x}) = \mathbf{b}. \tag{3.3}$$

In other words we wish to find all preimages of $\mathbf{b}$ under the linear map T.

Linear algebra is the study of these three different worlds and their interconnections. In this course we'll start with matrices and then see how they apply to systems of linear equations and vector spaces.

3.1 Matrices

We'll first cover some basics of matrices which should be familiar to most.

Definition 3.1. A (real) $m \times n$ **matrix** A is an array of real numbers $a_{ij} \in \mathbb{R}$, where $1 \leq i \leq m$ and $1 \leq j \leq n$, arranged in m rows and n columns as follows:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

We can write this matrix as $A = (a_{ij})$ or sometimes $A = (a_{ij})_{m \times n}$ if we wish to emphasise the size of the matrix. a_{ij} is called the ij**-th element** (entry) of A. We can also denote the ij-th entry of A by A_{ij}.

So for example

$$A = \begin{pmatrix} 1 & -5 & 0 \\ 10 & \frac{1}{2} & \sqrt{2} \end{pmatrix}$$

is an example of a 2×3 matrix with $a_{11} = 1$, $a_{12} = -5$, $a_{13} = 0$, $a_{21} = 10$ and so on. A different matrix would be

$$B = \begin{pmatrix} 1 & -5 \\ 0 & 10 \\ \frac{1}{2} & \sqrt{2} \end{pmatrix},$$

which is a 3×2 matrix ith $b_{11} = 1$, $b_{12} = -5$, $b_{21} = 0$ and so on. There are some terms which we use with particular matrices.

i) If $m = n$, then A is called a **square matrix**.

ii) If $m = 1$, then A is called a **row vector**.

iii) If $n = 1$, then A is called a **column vector**.

iv) A square matrix $A = (a_{ij})_{n\times n}$ is called a **diagonal matrix** if $a_{ij} = 0$ for $i \neq j$, i.e.

$$A = \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & a_{22} & 0 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}.$$

v) The $n \times n$ **identity matrix** $I_n = (a_{ij})_{n\times n}$ is defined as the diagonal matrix with

$$a_{ij} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases},$$

so

$$I_n = \begin{pmatrix} 1 & 0 & \dots & & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & & 0 & 1 \end{pmatrix}.$$

It's worth knowing that sometimes we write this matrix as $I_n = (\delta_{ij})$ where δ_{ij} is the *Kronecker delta* function

$$\delta_{ij} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

vi) Finally, the $m \times n$ **zero matrix** is the matrix $\mathbf{0}_{m\times n} = (a_{ij})_{m\times n}$ with $a_{ij} = 0$ for all $i = 1, \dots, m$ and $j = 1, \dots, n$. So

$$\mathbf{0}_{m\times n} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Often the size of the zero matrix is understood and we simply write $\mathbf{0}$.

Definition 3.2. Two matrices $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{r\times s}$ are said to be **equal** if $m = r$ and $n = s$, and $a_{ij} = b_{ij}$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

Example. i) $A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \end{pmatrix}$ then $A \neq B$,

ii) $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ then $A \neq B$,

iii) $A = \begin{pmatrix} 1 & 2 & 6 \\ 3 & 4 & 6 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 4 & 6 \end{pmatrix}$ then $A = B$.

So two matrices are equal only if they have the same size and identical entries. We'll next define some basic operations on matrices.

Definition 3.3. Let $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{m\times n}$ be two $m \times n$ matrices. Then the **sum** of A and B is defined as the $m \times n$ matrix

$$A + B = (a_{ij} + b_{ij})_{m\times n}.$$

Similarly we can define the **difference** of A and B as

$$A - B = (a_{ij} - b_{ij})_{m\times n}.$$

Example. i) $A = \begin{pmatrix} 1 & -1 \\ 2 & 6 \\ -3 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ 1 & -2 \\ 3 & 0 \end{pmatrix}$, then

$$A + B = \begin{pmatrix} 1+2 & -1+1 \\ 2+1 & 6-2 \\ -3+3 & 1+0 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 3 & 4 \\ 0 & 1 \end{pmatrix},$$

ii) $A = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 1 & 0 \\ 4 & 1 & 0 \end{pmatrix}$, then $A + B$ is not defined!

iii)

$$\begin{pmatrix} 1 & -1 \end{pmatrix} - \begin{pmatrix} 0 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 & -8 \end{pmatrix}.$$

Before we define the multiplication between two matrices we define a simpler kind of a product.

Definition 3.4. Let $\alpha \in \mathbb{R}$ and $A = (a_{ij})_{m\times n}$. Then the **scalar product** of α and A is the $m \times n$ matrix

$$\alpha A = (\alpha a_{ij})_{m\times n}.$$

Example. $\alpha = -2$ and $A = \begin{pmatrix} 1 & 3 & 0 \\ 0 & -1 & 1 \end{pmatrix}$ then

$$\alpha A = \begin{pmatrix} -2 & -6 & 0 \\ 0 & 2 & -2 \end{pmatrix}.$$

We'll next state some elementary properties of addition and scalar product. We give proofs for some of them, and you can do the rest as exercises as the proofs are fairly easy.

Proposition 3.5. *Let $\alpha, \beta, \gamma \in \mathbb{R}$ and A, B, C be $m \times n$ matrices. Then:*

V1

$$(A + B) + C = A + (B + C)$$

V2

$$A + \mathbf{0} = \mathbf{0} + A = A$$

V3

$$A + (-A) = (-A) + A = \mathbf{0}$$

V4

$$A + B = B + A$$

V5

$$\alpha(A + B) = \alpha A + \alpha B$$

V6

$$(\alpha + \beta)A = \alpha A + \beta B$$

V7

$$(\alpha\beta)A = \alpha(\beta A)$$

V8

$$1A = A$$

V9

$$0A = \mathbf{0}$$

Proof. **V1** Let $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$ and $C = (c_{ij})_{m\times n}$. Then,

$$(A + B) + C = (a_{ij} + b_{ij})_{m\times n} + (c_{ij})_{m\times n} = ((a_{ij} + b_{ij}) + c_{ij})_{m\times n},$$

$$A + (B + C) = (a_{ij})_{m\times n} + (b_{ij} + c_{ij})_{m\times n} = (a_{ij} + (b_{ij} + c_{ij}))_{m\times n}.$$

These are queal since associativity holds in $(\mathbb{R}, +)$.

V2-V9 These are left as exercises.

□

The product of 2 matrices is slightly more complicated.

Definition 3.6. Let $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{r\times p}$. Then the **product** of A and B is defined if $n = r$ (so the number of columns of A is same as the number of rows of B) and is the $m \times p$ matrix

$$AB = (c_{ij})_{m\times p}$$

with

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

So it is the matrix where the ij-th entry is the sum of the products of corresponding entries from the i-th column of A with the j-th column of B.

Example. i) $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$ then AB is defined as A is 2×3 and B is 3×1. The product will thus be $2 \times \not{3} \not{\times} \not{3} \times 1$ matrix:

$$\begin{pmatrix} c_{11} \\ c_{21} \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 3 \\ -1 \cdot 0 + 0 \cdot 1 + 1 \cdot 3 \end{pmatrix} = \begin{pmatrix} 11 \\ 3 \end{pmatrix},$$

where

$$c_{11} = \sum_{k=1}^{3} a_{1k} b_{k1} = a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31},$$

and

$$c_{21} = \sum_{k=1}^{3} a_{2k} b_{k1} = a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31}.$$

Of course BA is not defined.

ii) $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 2 \\ 3 & 0 \end{pmatrix}$ Since A is 2×3 and B is 3×2 both AB and BA are defined. For example,

$$AB = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} 11 & 5 \\ 3 & -1 \end{pmatrix}.$$

We'll now state some properties of matrix multiplication and again leave the proofs as exercises.

Proposition 3.7. *Let A, B, C be $m \times p$, $p \times r$, $r \times n$ matrices respectively and let $\alpha \in \mathbb{R}$. Then,*

M1

$$(AB)C = A(BC)$$

M2 *If $p = r$ and $r = n$ then*

$$A(B + C) = AB + AC$$

M3 *If $m = p$ and $p = r$ then*

$$(A + B)C = AC + BC$$

M4

$$\alpha(AB) = (\alpha A)B = A(\alpha B)$$

M5

$$AI_p = I_m A = A$$

M6

$$\mathbf{0}_{n\times m}A = \mathbf{0}_{n\times p}$$

and

$$A\mathbf{0}_{p\times q} = \mathbf{0}_{m\times q}$$

Remark. Notice that $AB \neq BA$ in general! This is not true even if both A and B are square matrices. For example, try it with

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

3.2 Systems of Linear Equations

We are now ready to start working towards answering the questions asked in the beginning of this chapter. Consider n unknowns x_1, x_2, ..., x_n and the system of linear equations:

$$\begin{cases} a_{11}x_1 & +a_{12}x_2 & +\ldots & +a_{1n}x_n & = b_1 \\ a_{21}x_1 & +a_{22}x_2 & +\ldots & +a_{2n}x_n & = b_2 \\ \quad\ldots & & & & \\ a_{m1}x_1 & +a_{m2}x_2 & +\ldots & +a_{mn}xn & = b_m \end{cases}$$

where $a_{ij} \in \mathbb{R}$ are the coefficients and $b_j \in \mathbb{R}$ the constants. The problem is to find the set of solutions to this system. There are three possible cases:

- A solution exists and is unique,

- a solution exists and is not unique (infinitely many solutions),
- there are no solutions.

In the first two cases when our system has at least one solution we say that the system is **consistent**. If there are no solutions we say that the system is **inconsistent**.

The idea we will use to solve this system is to express it in terms of matrices and then reduce to a simpler system of equations which still has the same solution set. Such a system is called an **equivalent system** of equations. Given a system, the way to obtain an equivalent system is to perform elementary operations which we define next.

There are three types of elementary operations:

Type 1 Multiply one equation with a nonzero number $\alpha \in \mathbb{R} \setminus \{0\}$.

Type 2 Addition of a multiple of one equation to another equation.

Type 3 Interchanging the position of two equations.

It will be easier to understand these in terms of the matrix corresponding to the system of equations as can be seen from the following example.

Example. Look at

$$\begin{cases} x_1 + 2x_2 - 3x_3 = 0 \\ 2x_1 - 2x_2 - x_3 = -1 \\ -3x_1 + 5x_2 + x_3 = 3 \end{cases}$$

We can rewrite this by using matrices as

$$\begin{pmatrix} 1 & 2 & -3 \\ 2 & -2 & -1 \\ -3 & 5 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 3 \end{pmatrix}$$

or in short

$$A\mathbf{x} = \mathbf{b}.$$

We form the **augmented matrix** corresponding to this system

$$\left(\begin{array}{ccc|c} 1 & 2 & -3 & 0 \\ 2 & -2 & -1 & -1 \\ -3 & 5 & 1 & 3 \end{array}\right)$$

where the last column corresponds to the constants on the right-hand side of the system of equations. Denote the first, second and third rows of this matrix by R_1, R_2 and R_3, respectively. We can perform the elementary operations on this matrix if we just think of it representing the equation with the variables omitted. So to get this matrix into a simpler form we might do the following:

$$\xrightarrow[R_3+3R_1]{R_2-2R_1} \left(\begin{array}{ccc|c} 1 & 2 & -3 & 0 \\ 0 & -6 & 5 & -1 \\ 0 & 11 & -8 & 3 \end{array}\right)$$

$$\xrightarrow{R_3+\frac{11}{6}R_2} \left(\begin{array}{ccc|c} 1 & 2 & -3 & 0 \\ 0 & -6 & 5 & -1 \\ 0 & 0 & \frac{7}{6} & \frac{7}{6} \end{array}\right).$$

Hence we get the equivalent system

$$\begin{cases} x_1 + & 2x_2 - & 3x_3 & = 0 \\ - & 6x_2 + & 5x_3 & = -1 \\ & & \frac{7}{6}x_3 & = \frac{7}{6} \end{cases}$$

This gives us that

$$\begin{cases} x_1 = 1 \\ -6x_2 = -1 - 5 \\ x_3 = 1 \end{cases}.$$

Hence there is a unique solution $(x_1, x_2, x_3) = (1, 1, 1)$.

So we see that each of the elementary operations corresponds to an operation in the associated augmented matrix. These are called **elementary row operations** for matrices, and they are

Type 1 Multiply a row by a non-zero scalar.

Type 2 Add a multiple of a row to another row.

Type 3 Swap the position of two rows.

Using these operations we aim to bring the matrix first into a **row echelon form** (REF) in which each row starts with a strictly longer string of zeros than the previous one (unless both rows consist of only zeros). So for example

$$\begin{pmatrix} 1 & 2 & 0 & 3 & 0 & 5 \\ 0 & 2 & 5 & -2 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in REF. After this it's easy to reduce the matrix to the simplest possible form the **reduced row echelon form** (RREF) in which the following conditions hold

E1 All zero rows are at the bottom of the matrix.

E2 The first non-zero entry in each row is 1 (called the leading 1).

E3 Every other element in the column of every leading 1 is zero.

E4 Every leading 1 is strictly to the right of the one in the previous row.

The RREF of the previous matrix would be

$$\begin{pmatrix} 1 & 0 & -5 & 5 & 0 & 11 \\ 0 & 1 & \frac{5}{2} & -1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & -7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let's do another example where we illustrate the general procedure of finding the RREF of a matrix.

Example. Start with

$$\begin{pmatrix} 0 & 2 & 4 & 2 & 14 & -6 \\ 0 & 1 & 2 & 0 & 3 & 6 \\ 0 & 2 & 4 & 1 & 10 & 4 \end{pmatrix}.$$

Since the first row is divisible by two it makes sense to do that and then subtract it from the second and third rows to get the column for the first leading one (if the first row wasn't divisible by two it would make more sense to swap rows 1 and 2). This gives

$$\xrightarrow{\frac{1}{2}R_1} \begin{pmatrix} 0 & 1 & 2 & 1 & 7 & -3 \\ 0 & 1 & 2 & 0 & 3 & 6 \\ 0 & 2 & 4 & 1 & 10 & 4 \end{pmatrix} \xrightarrow[R_3-2R_1]{R_2-R_1} \begin{pmatrix} 0 & 1 & 2 & 1 & 7 & -3 \\ 0 & 0 & 0 & -1 & -4 & 9 \\ 0 & 0 & 0 & -1 & -4 & 10 \end{pmatrix}.$$

Now the first leading one is sorted. We then look at the second row and notice we need to multiply it by -1 to get a leading one after which we use it to remove the other entries in that column:

$$\xrightarrow{-1\cdot R_2} \begin{pmatrix} 0 & 1 & 2 & 1 & 7 & -3 \\ 0 & 0 & 0 & 1 & 4 & -9 \\ 0 & 0 & 0 & -1 & -4 & 10 \end{pmatrix} \xrightarrow[R_3+R_2]{R_1-R_2} \begin{pmatrix} 0 & 1 & 2 & 0 & 3 & 6 \\ 0 & 0 & 0 & 1 & 4 & -9 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The last row already has a leading one so it remains to use it to remove the nonzero numbers from the other entries in its column:

$$\xrightarrow[R_2+9R_3]{R_1-6R_3} \begin{pmatrix} 0 & 1 & 2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

This is now in reduced row echelon form.

Let's do another example which illustrates how to find the **general solution** to a system of linear equations. This is done by reducing the augmented matrix to RREF and then noting the dependent and independent variables. Of course it could happen that in the RREF we get something absurd like $1 = 0$ which would imply that the system is inconsistent.

Example. Look at the system of equations

$$\begin{cases} 2x_1 & +x_2 & +8x_3 & = 7 \\ & 2x_2 & +4x_3 & = -2 \\ x_1 & +x_2 & +5x_3 & = 3 \end{cases}.$$

This system has the augmented matrix

$$\left(\begin{array}{ccc|c} 2 & 1 & 8 & 7 \\ 0 & 2 & 4 & -2 \\ 1 & 1 & 5 & 3 \end{array}\right).$$

We reduce it to RREF with the following elementary row operations:

$$\xrightarrow{\frac{1}{2}R_2} \left(\begin{array}{ccc|c} 2 & 1 & 8 & 7 \\ 0 & 1 & 2 & -1 \\ 1 & 1 & 5 & 3 \end{array}\right) \xrightarrow[R_3-R_2]{R_1-R_2} \left(\begin{array}{ccc|c} 2 & 0 & 6 & 8 \\ 0 & 1 & 2 & -1 \\ 1 & 0 & 3 & 4 \end{array}\right)$$

$$\xrightarrow{\frac{1}{2}R_1} \left(\begin{array}{ccc|c} 1 & 0 & 3 & 4 \\ 0 & 1 & 2 & -1 \\ 1 & 0 & 3 & 4 \end{array}\right) \xrightarrow{R_3-R_1} \left(\begin{array}{ccc|c} 1 & 0 & 3 & 4 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

which is in RREF. Notice that while this is probably the most optimal way of reducing the matrix it might not be the most obvious way. You can of course arrive at the same result by reducing in many other ways. They key point about RREF that we'll soon see is that no matter what you do the RREF is always unique for a specific matrix. Nevertheless we can now write down the general solution by using the RREF.

First we write down the variables underneath the columns and circle the ones which are under a column with a leading one:

$$\left(\begin{array}{ccc|c} 1 & 0 & 3 & 4 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$
$$\textcircled{x_1}\ \textcircled{x_2}\ x_3$$

Our **independent** (or *free*) variables are then given by the uncircled ones, x_3 in this case and the **dependent** variables by the circled ones, that is,

x_1 and x_2. We then write the general solution as a vector in terms of the independent variables:

$$\begin{pmatrix} 4-3x_3 \\ -1-2x_3 \\ x_3 \end{pmatrix}$$

Alternatively if we set $x_3 = \alpha$ for arbitrary $\alpha \in \mathbb{R}$ then the general solution is given by

$$\begin{cases} x_1 = 4-3\alpha \\ x_2 = -1-2\alpha \\ x_3 = \alpha \end{cases}$$

i.e.

$$\begin{pmatrix} 4-3\alpha \\ -1-2\alpha \\ \alpha \end{pmatrix}.$$

The key thing, that was pointed out in the preceding examples already, is that it is always possible to reduce a matrix to RREF and, moreover, it is unique for every matrix. So no matter what sequence of elementary row operations you use you will always arrive at the same RREF.

Theorem 3.8. *Each $m \times n$ matrix is row-equivalent to an $m \times n$ matrix in RREF. The RREF is unique.*

Proof. Suppose $A \neq \mathbf{0}_{m\times n}$, otherwise A is already in RREF. Let c_{k_1} be the first column containing a nonzero element in any row, such a column must exist as $A \neq \mathbf{0}$. By row interchange we can assume that $a_{ik_1} \neq 0$. Then we change it to a leading 1 by performing $R_1 \longrightarrow \frac{1}{a_{1k_1}} R_1$. Next we make all the other entries in this column 0, that is, if for any $j \neq 1$ we have that $a_{jk_1} \neq 0$ then we perform $R_j \longrightarrow R_j - a_{jk_1} R_1$. The column for the first leading one is now done.

Next we look for the next column which contains a nonzero element in any row below the first one. If such a column exists call it c_{k_2}. Again by row interchange we can assume that $\tilde{a}_{2k_2} \neq 0$. Repeating as before we can change

this into a leading one and make all other entries in that column 0. Repeat for the remaining columns.

We'll leave the proof of uniqueness for later. □

3.3 Matrices (Continuation)

To make more progress in characterising the solutions of systems of linear equations we need to develop a little more theory for matrices.

Definition 3.9. Let $A = (a_{ij})_{m\times n}$ be an $m \times n$ matrix. The **transpose** of A, denoted by $A^\intercal$, is the $n \times m$ matrix obtained by interchanging the rows and columns of A, i.e.

$$A^\intercal = (a_{ji})_{n\times m}.$$

So for example if

$$A = \begin{pmatrix} 2 & 1 \\ 0 & -1 \\ 1 & 0 \end{pmatrix},$$

then

$$A^\intercal = \begin{pmatrix} 2 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

The transpose has some obvious properties. Try proving these yourself.

Proposition 3.10. *Let $\alpha \in \mathbb{R}$, A, B matrices. Then (for appropriately sized A and B)*

T1

$$(A + B)^\intercal = A^\intercal + B^\intercal$$

T2

$$(\alpha A)^\intercal = \alpha A^\intercal$$

T3

$$(AB)^\intercal = B^\intercal A^\intercal$$

T4

$$(A^\intercal)^\intercal = A$$

Definition 3.11. A square matrix $A = (a_{ij})_{n\times n}$ for which $A = A^\intercal$ is called **symmetric**. If $A^\intercal = -A$ then A is **antisymmetric**.

Notice that if A is antisymmetric then $a_{ij} = -a_{ji}$ for all i and j. This implies that if $i = j$ then $a_{ii} = 0$ for all i. In other words the main diagonal of an antisymmetric matrix is all zeros.

We've now covered addition, subtraction and multiplication of matrices. Drawing from the analogy of operations from real numbers we'd like some kind of "division" or rather an inverse operation for matrix multiplication. Unfortunately this cannot always be done (which makes matrix operations even more complicated compared to working with regular numbers).

Definition 3.12. A square matrix $A = (a_{ij})_{n\times n}$ is called **invertible** if there is a matrix $B = (b_{ij})_{n\times n}$ such that

$$AB = BA = I_n.$$

Then B is called the **inverse** of A and denoted by

$$A^{-1} := B.$$

Theorem 3.13. *If a square matrix A is invertible, then the inverse is unique.*

This justifies the notation A^{-1} for the inverse.

Proof. This will follow immediately as a consequence of the group structure of $(GL(n, \mathbb{R}), \cdot)$, which is done in the homework. □

Again, we list some obvious properties for the matrix inversion.

Proposition 3.14. *Let A, B be $n \times n$ invertible matrices and $\alpha \in \mathbb{R} \setminus \{0\}$ then*

I1 *αA is invertible and $(\alpha A)^{-1} = \frac{1}{\alpha} A^{-1}$.*

I2 *AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$.*

I3 *A^{-1} is invertible and $(A^{-1})^{-1} = A$.*

I4 *$A^\intercal$ is invertible and $(A^\intercal)^{-1} = (A^{-1})^\intercal$.*

The second property can be generalised to a finite product of matrices. That is,

$$(A_1 A_2 \dots A_n)^{-1} = A_n^{-1} A_{n-1}^{-1} \dots A_2^{-1} A_1^{-1}.$$

Similarly we find that

$$\begin{aligned} A^{-n} = (A^{-1})^n &= \overbrace{A^{-1}A^{-1}\dots A^{-1}}^{\text{n times}} \\ A^m A^n &= A^n A^m = A^{m+n} \\ (A^m)^n &= (A^n)^m = A^{mn}. \end{aligned}$$

We wish to develop a method of computing the inverse of a matrix, but we also wish to understand when the inverse of A exist as we pointed out before that it's not always the case. Luckily computing inverse is fairly easy and doable with the tools we already have. In order to justify why it works and to understand when the inverse exists we need to learn a couple of more things.

First we need the notion of elementary matrices which are simply matrices obtained from I_n by applying elementary row operations.

Definition 3.15. The result of applying an elementary row operation (ERO) to an identity matrix I_n is called an **elementary matrix** of size n. There are 3 types of elementary matrices:

Type 1

$$E_r(\alpha) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \alpha & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

where the α entry appears in row r, column r position. This elementary matrix corresponds to the row operation $R_r \longrightarrow \alpha R_r$.

Type 2 The second elementary matrix corresponds to $R_r \longrightarrow R_r + \alpha R_s$:

$$E_{rs}(\alpha) = \begin{pmatrix} 1 & 0 & \dots & & & & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & \dots & 1 & \dots & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & & & & & 1 \end{pmatrix},$$

where the α entry is in the row r, column s position.

Type 3 Finally, the third type of elementary matrix corresponds to just swapping two of the rows so

$$E_{rs} = \begin{pmatrix} 1 & 0 & \dots & & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & 1 & & \vdots \\ 0 & \dots & & & 1 \end{pmatrix}$$

where we have just interchanged rows r and s. This of course is given by the row operation $R_r \leftrightarrow R_s$.

Let's see what happens if we multiply square matrices from the left by an elementary matrix.

Example. Let

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Then,

$$E_2(-1)A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ -4 & -5 & -6 \\ 7 & 8 & 9 \end{pmatrix},$$

where the resulting matrix is just the row operation $-1 \cdot R_2$ applied to A. Similarly,

$$E_{31}(1)A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 8 & 10 & 12 \end{pmatrix}.$$

Again we see that the result is just applying the corresponding row operation $R_3 \to R_3 + R_1$ to A. Verify that this is true for the matrix E_{13} as well.

From this example we see that multiplying from left by elementary matrices is the same as performing the corresponding elementary row operations on a square matrix A. A simple theorem with powerful consequences is the fact that all these matrices are invertible (which is why elementary row operations are chosen to be what they are).

Theorem 3.16. *Elementary matrices are invertible and their inverses are also elementary matrices of the same type.*

Proof. As a proof you can just do a verification that the following inverses work:

$$\begin{aligned} E_r(\alpha)^{-1} &= E_r(\alpha^{-1}) \\ E_{rs}(\alpha)^{-1} &= E_{rs}(-\alpha) \\ E_{rs}^{-1} &= E_{rs}. \end{aligned}$$

□

This allows us to prove the following theorem.

Theorem 3.17. *If B is row-equivalent to A (i.e. B results from applying EROs to A), then there is P invertible matrix such that $B = PA$.*

Proof. Let $E_1, \ldots, E_k$ be the elementary matrices corresponding to the EROs performed on A to obtain B. Then

$$B = E_k E_{k-1} \ldots E_1 A.$$

Denote $P = E_k \ldots E_1$. Then by previous theorem all of the E_j's are invertible and thus by properties of matrix inversion P is invertible with inverse

$$P^{-1} = E_1^{-1} \ldots E_k^{-1}.$$

□

We are now in position to state the algorithm for finding the inverse of A, if it exists.

Theorem 3.18. *If the $n \times n$ square matrix A can be row-reduced to the identity matrix I_n by a sequence of EROs, then A is invertible and the inverse is given by applying the same sequence of EROs to I_n.*

Proof. By assumption

$$E_r E_{r-1} \ldots E_1 A = I_n.$$

Then,

$$A = E_1^{-1} E_2^{-1} \ldots E_r^{-1} I_n = E_1^{-1} \ldots E_r^{-1}.$$

The right-hand side is of course invertible so it follows that A is invertible. Hence the inverse is given by

$$A^{-1} = E_r E_{r-1} \ldots E_1 I_n.$$

□

So in practice what we do is we form the augmented matrix $(A|I_n)$ and reduce A to the identity matrix and then the inverse can be found from $(I_n|A^{-1})$. Let's do an example.

Example. Let

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

We form $(A|I_3)$ and reduce it to RREF:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \end{array}\right) \xrightarrow[-R_3]{R_2-R_1} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{array}\right)$$

$$\xrightarrow[-R_2, R_2+2R_3]{R_1+R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 & -1 & -2 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{array}\right).$$

Hence,

$$A^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}.$$

3.4 Determinants

Next we'll try to answer when is the process of inverting actually doable. Of course this corresponds to precisely to determining whether the RREF of A is I_n or not. Luckily, however, it is easier to determine *a priori* whether A is invertible or not. For this we need to introduce determinants.

Definition 3.19. If $A = (a_{ij})_{n\times n}$ is a $n \times n$ square matrix, then the **determinant** of A, denoted by $\det A$, is given by

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)},$$

where the sum is taken over all $n!$ permutations $\sigma \in S_n$.

While this definition might seem a bit complicated, luckily in practice one does not have to rely on it that much. We'll soon come up with extremely efficient ways of computing determinants of square matrices. Let's still do a few examples by using the definition.

Example. i) Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

To compute the determinant we need to sum over $S_2 = \{\sigma_1 = \mathrm{id}, \sigma_2 = (1,2)\}$. Then

$$\det A = \operatorname{sign}(\sigma_1 a_{1\sigma_1(1)} a_{2\sigma_1(2)} + \operatorname{sign}(\sigma_2) a_{1\sigma_2(1)} a_{2\sigma_2(2)} = a_{11}a_{22} - a_{12}a_{21}.$$

ii) We can do the same for 3×3 matrices by summing over S_3. This will lead to

$$\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$
$$-a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

An easy way to remember this is called Sarrus' Rule[1] Use this to verify that the determinant of the following matrix is 12:

$$A = \begin{pmatrix} 1 & 2 & -1 & \\ -2 & 1 & 1\,3 & -2 \quad 1 \end{pmatrix}.$$

It is useful to know how the determinant of A and the determinant of the RREF of A are related. In order to do that we of course should determine how each elementary row operation affects the determinant.

Theorem 3.20. *Let $A = (a_{ij})_{n\times n}$ be an $n \times n$ square matrix. Then,*

D1

$$\det A = \sum_{\tau \in S_n} (\operatorname{sign} \tau) a_{\tau(1)1} a_{\tau(2)2} \dots a_{\tau(n)n}.$$

D2 *If every element of a row (or column) of A is multiplied by a real number λ then* $\det A$ *is multiplied by λ.*

D3 *Interchanging two rows (or columns) of A changes the sign of* $\det A$.

[1]Read more at `http://en.wikipedia.org/wiki/Rule_of_Sarrus`.

D4 *Let*

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_{i1} + c_{i1} & \dots & b_{in} + c_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_{i1} & \dots & b_{in}+ \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}, C = \begin{pmatrix} a_{11} \\ \vdots \\ c_{i1} \\ \vdots \\ a_{n1} \end{pmatrix}$$

Then

$$\det A = \det B + \det C.$$

This theorem will allow us to prove the following proposition.

Proposition 3.21. *Let $A = (a_{ij})_{n\times n}$ be a $n \times n$ square matrix, $\lambda \in \mathbb{R}$. Then*

D5

$$\det A = \det A^{\intercal}$$

D6

$$\det(\lambda A) = \lambda^n \det A$$

D7 *If A contains a row or a column of only zeros then* $\det A = 0$.

D8 *If two rows (or columns) are identical, then* $\det A = 0$.

D9 *Adding λ times row s to row r ($r \neq s$) leaves* $\det A$ *unchanged. Similarly for columns.*

D10 *Let A be in a triangular form (upper or lower). Then*

$$\det A = \prod_{i=1}^{n} a_{ii} = a_{11}a_{22}\dots a_{nn}.$$

Proof of Theorem. **D1** Call σ^{-1} the inverse permutation of $\sigma \in S_n$. Then for $\sigma(r) = s$ we have $r = \sigma^{-1}(s)$ and thus $a_{r\sigma(r)} = a_{\sigma^{-1}(s)s}$. Hence,

$$\begin{aligned}
\det A &= \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} \\
&= \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{\sigma^{-1}(1)1} \dots a_{\sigma^{-1}(n)n} && (\text{since } a_{r\sigma(r)} = a_{\sigma^{-1}(s)s}) \\
&= \sum_{\sigma \in S_n} (\operatorname{sign} \sigma^{-1}) a_{\sigma^{-1}(1)1} \dots a_{\sigma^{-1}(n)n} && (\text{since } \operatorname{sign} \sigma = \operatorname{sign} \sigma^{-1}) \\
&= \sum_{\tau \in S_n} \operatorname{sign} \tau a_{\tau(1)1} \dots a_{\tau(n)n} && (\text{by renaming } \sigma^{-1} \mapsto \tau)
\end{aligned}$$

D2 Suppose row r is multiplied by λ to give matrix $B = (b_{ij})_{n \times n}$ with

$$b_{ij} = \begin{cases} a_{ij}, & i \neq r \\ \lambda a_{ij}, & i = r. \end{cases}$$

Then,

$$\begin{aligned}
\det B &= \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) b_{1\sigma(1)} \dots \underbrace{b_{r\sigma(r)}}_{=\lambda a_{r\sigma(r)}} \dots b_{n\sigma(n)} \\
&= \lambda \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} \\
&= \lambda \det A.
\end{aligned}$$

D3 Similarly as D2 with

$$b_{ij} = \begin{cases} a_{rj} & \text{if} i = s \\ a_{sj} & \text{if} i = r \\ a_{ij} & \text{otherwise.} \end{cases}$$

D4 Similarly as before:

$$\begin{aligned}
\det A &= \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{1\sigma(1)} \dots (b_{i\sigma(i)} + c_{i\sigma(i)}) \dots a_{n\sigma(n)} \\
&= \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{1\sigma(1)} \dots b_{i\sigma(i)} \dots a_{n\sigma(n)} + \sum_{\sigma \in S_n} (\operatorname{sign} \sigma) a_{1\sigma(1)} \dots c_{i\sigma(i)} \dots a_{n\sigma(n)} \\
&= \det B + \det C.
\end{aligned}$$

□

Proof of Proposition. **D5** This follows immediately from D1 as $A^{\intercal}_{i\sigma(i)} = A_{\sigma(i)i}$.

D6 Apply D2 to each row.

D7 Apply D2 with $\lambda = 0$.

D8 Apply D3, we get $\det A = -\det A$ so $\det A = 0$.

D9 Follows from D4 and D2.

D10 Suppose A is upper triangular (proof is the same for lower triangular), that is, $a_{ij} = 0$ for $i > j$. Then in the general term of the sum in determinan $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ we can always find a term with $i > j$ unless $i = j$ for each of them, which corresponds to the identity permutation. Hence the determinant is the product of the diagonal entries.

□

We can now characterise the invertible matrices in terms of their determinant.

Proposition 3.22. *Let $A = (a_{ij})_{n\times n}$ be a square matrix and B its RREF. Then,*

i) *$B = I_n$ or else B contains at least one row of zeros.*

ii) *(a) $B = I_n \iff A$ is invertible.*
(b) B contains a row of zeros $\iff A$ is non-invertible (singular).

Proof. i) Follows immediately from the definition of the RREF.

ii) (a) We know that $B = E_r \dots E_1 A$ for some elementary matrices E_i. If $B = I_n$ then $A^{-1} = E_r \dots E_1$. If $B \neq I_n$ then it has a row of zeros, notice then that for any square matrix C we have that $BC \neq I_n$ as BC must still contain a zero row. Hence for any square A' we have

$$AA' = (E_1^{-1} \dots E_r^{-1} B)A \neq I_n$$

since by the above remark $E_1^{-1} \dots E_r^{-1} B$ is not invertible and thus the whole product is not invertible.

(b) This is equivalent to the previous part.

□

Theorem 3.23. *The $n \times n$ matrix A is invertible if and only if* $\det A \neq 0$.

Proof. Write $B = E_r \dots E_1 A$ be the RREF of A. Then

$$\det B = \det(E_r \dots E_1 A).$$

But by a direct check (which you should do yourself)

$$\det(EA) = \det E \det A$$

for any elementary matrix E. By induction you can also show that

$$\det(E_r \dots E_1 A) = \det E_r \dots \det E_1 \det A.$$

Again, by a direct check you can show that $\det E_i \neq 0$ so it follows that

$$\det A \neq 0 \iff \det B \neq 0 \iff B = I_n \iff A \text{ invertible.}$$

□

An important fact we used in the previous proof was that $\det(EA) = \det E \det A$. This is actually true not just for elementary E but for any square matrices. This is called Binet's Theorem which we will not prove in this course.

Theorem 3.24 (Binet's Theorem)**.** *Let $A = (a_{ij})_{n\times n}$ and $B = (b_{ij})_{n\times n}$ be two square matrcies. Then,*

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

Corollary 3.25. *If A is invertible, then* $\det A^{-1} = \frac{1}{\det A}$.

Rather than using only row operations we have one more trick to compute determinants. For this we need one more definition.

Definition 3.26. Let $A = (a_{ij})_{n\times n}$ be a $n \times n$ matrix. The **(r, s)-minor of A**, denoted by Δ_{rs}, is the determinant of the $(n-1) \times (n-1)$ matrix obtained from A by omitting row r and column s.

The **(r, s)-cofactor of A** is then defined to be

$$A_{rs} = (-1)^{r+s}\Delta_{rs}.$$

We can now use these cofactors to "expand the matrix along a row (column)" to reduce the computation of the determinant to one involving a smaller matrix (and repeat this until the computation becomes easy.

Theorem 3.27 (Laplace's Theorem (Expanding Along Rows))**.** *Let $A = (a_{ij})_{n\times n}$ be a $n \times n$ matrix. Then, for a fixed $r \in \{1, \ldots, n\}$,*

$$\det A = \sum_{s=1}^{n} a_{rs}A_{rs} \quad \textit{(expanding along row } r\textit{)}$$

and

$$\det A = \sum_{s=1}^{n} a_{sr}A_{sr} \quad \textit{(expanding along column } r\textit{).}$$

An example should make this process clear.

Example. Consider

$$A = \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 0 & 2 & 0 \\ 2 & 1 & 4 & -5 \\ 11 & 0 & 2 & 1 \end{pmatrix}.$$

Then we can expand along row 2 since most of the entries are 0 to get

$$\begin{aligned} \det A &= a_{21}A_{21} + a_{22}A_{22} + a_{23}A_{23} + a_{24}A_{24} \\ &= a_{23}A_{23}. \end{aligned}$$

So we only need to compute A_{23}. This is

$$A_{23} = (-1)^{2+3} \det \begin{pmatrix} 1 & 0 & 4 \\ 2 & 1 & -5 \\ 11 & 0 & 1 \end{pmatrix}.$$

To compute this determinant we expand along the second column to get

$$\det A = -2(-1)^{2+2} \det \begin{pmatrix} 1 & 4 \\ 11 & 1 \end{pmatrix} = -2(1 - 44) = 86.$$

All this work actually allows us to compute A^{-1} fully without having to do much row reduction.

Definition 3.28. Let $A = (a_{ij})_{n\times n}$ and $B = (A_{ij})_{n\times n}$ where A_{ij} is the (i, j)-cofactor of A. The matrix $B^\intercal$ is called the **adjugate** of A and denoted by $\operatorname{adj} A$.

Theorem 3.29. i)

$$A(\operatorname{adj} A) = (\operatorname{adj} A)A = (\det A)I_n.$$

ii) *If A is invertible, then*

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A.$$

Example. Let

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

By a quick computation we find that $\det A = 1$ which implies that A is invertible. We first form the matrix of minors which is

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ -1 & 2 & -1 \end{pmatrix}.$$

This allows us to compute A^{-1} as

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ -1 & -2 & -1 \end{pmatrix}^\intercal = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}.$$

3.5 Systems of Homogeneous Equations

We briefly mention an important special case of systems of linear equations which occurs when all the constants are 0. We're looking at

$$A\mathbf{x} = \mathbf{b}, \tag{3.4}$$

where A is a $n \times n$ matrix.

Theorem 3.30. *Let* $A = (a_{ij})n \times n$ *and* $\mathbf{b} = \mathbf{0}_{n\times 1} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. *Then* (3.4) *has a unique solution* $\mathbf{x} = \mathbf{0}_{n\times 1} \iff \det A \neq 0$. *Similarly, the system* (3.4) *has a non-trivial solution* $\iff \det A = 0$.

Proof. The RREF of $(A|\mathbf{0})$ is $B = (I_n|\mathbf{0})$ if $\det A \neq 0$. This implies immediately that $A\mathbf{x} = \mathbf{0}$ has a unique solution $\mathbf{x} = \mathbf{0}$.

Now, if $B \neq I_n$ then there is at least one row of zeros. By induction we can construct a nonzero solution $\mathbf{x}$ to (3.4) (See Theorem 4.71 in Towers for details). □

In general, $A\mathbf{x} = \mathbf{b}$ has a unique solution if and only if $\det A \neq 0$.

This concludes the theory of matrices for now. We'll next take a brief interlude to the more abstract theory of vector spaces before putting everything we've done together by looking at eigenvalues of matrices.

Chapter 4

Vector Spaces

Before jumping into the definition of a vector space we will need to look at something called *fields*. A field is simply an abstraction of all the nice properties that $\mathbb{R}$ or $\mathbb{Q}$ have (which are both examples of fields). You can simply think of it as a set which has two group structures embedded in it (like addition and multiplication in real numbers).

Definition 4.1. A **field** is a triple $(\mathbb{F}, +, \cdot)$ where $\mathbb{F}$ is a set and $+, \cdot$ are binary operations such that

i) $(\mathbb{F}, +)$ is an abelian group,

ii) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group,

iii) The distributive law holds:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

for any $x, y, z \in \mathbb{F}$.

Notice that the 0 that appears in the definition is the additive identity from $(\mathbb{F}, +)$. As said before $(\mathbb{R}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are fields as is $(\mathbb{C}, +, \cdot)$. We can now give the (rather lengthy) definition of a vector space.

Definition 4.2. A **vector space** V over the field $\mathbb{F}$ is a set with two operations such that

I) $(V, +)$ is an abelian group,

V1

$$(a + b) + c = a + (b + c)$$

$\forall a, b, c \in V$.

V2 There is an additive identity $\mathbf{0} \in V$ (called null vector) such that for any $a \in V$

$$a + \mathbf{0} = \mathbf{0} + a = a$$

V3 $\forall a \in V$ there is the inverse $-a \in V$ such that

$$a + (-a) = -a + a = \mathbf{0}$$

V4

$$a + b = b + a$$

$\forall a, b \in V$

II) The scalar product $\mathbb{F} \times V \longrightarrow V$ such that $(\lambda, v) \mapsto \lambda v$ satisfies

V5

$$\alpha(a + b) = \alpha a + \alpha b$$

$\forall \alpha \in \mathbb{F}$, $\forall a, b \in V$

V6

$$(\alpha + \beta)a = \alpha a + \beta a$$

$\forall \alpha, \beta \in \mathbb{F}$, $\forall a \in V$

V7

$$(\alpha\beta)a = \alpha(\beta a)$$

$\forall \alpha, \beta \in \mathbb{F}$, $\forall a \in B$

V8

$$1 \cdot a = a,$$

where $1 \in \mathbb{F}$ is the multiplicative identity

We call $\mathbb{F}$ the **field of scalars** and any particular $\lambda \in \mathbb{F}$ is called a **scalar**. Let's look at some (familiar) examples of vector spaces.

Example. i) Let $V = \mathbb{R}^n$. This is a vector space over $\mathbb{F} = \mathbb{R}$, where the sum for

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

is defined as

$$a + b = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}.$$

The scalar product is defined as

$$\lambda a = \begin{pmatrix} \lambda a_1 \\ \lambda a_2 \\ \lambda a_3 \end{pmatrix},$$

for any $\lambda \in \mathbb{R}$. It is easy to see that $(\mathbb{R}^n, +)$ is an abelian group and that V5-V8 are satisfied for the scalar product.

ii) Let $V = M(n, m, \mathbb{R}) = \{A : A \text{ is a } n \times m \text{ matrix}\}$. We know that $(M(n, m, \mathbb{R}), +)$ is an abelian group from our definition of matrix addition. Consider $\mathbb{F} = \mathbb{R}$, then we have already defined the scalar product λA for any $\lambda \in \mathbb{R}$ and $A \in V$; and it is not hard to see that it satisfies V5-V8.

iii) Let $V = \{f | f : \mathbb{R} \to \mathbb{R} \text{ is a function}\}$ and $\mathbb{F} = \mathbb{R}$. We can then define the sum of $f, g \in V$ as the function $f + g \in V$ such that

$$(f + g)(x) = f(x) + g(x).$$

Similarly, we can define the scalar product of $\lambda \in \mathbb{R}$ and $f \in V$ as λf given by

$$(\lambda f)(x) = \lambda f(x).$$

With these operations V is a vector space over $\mathbb{R}$.

Proposition 4.3. i)

$$0v = \mathbf{0},$$

for any $v \in V$.

ii)
$$\lambda \mathbf{0} = \mathbf{0},$$
for any $\lambda \in \mathbb{F}$.

iii)
$$\lambda v = \mathbf{0} \implies \lambda = 0 \text{ or } v = \mathbf{0}$$

iv)
$$(-\lambda)v = \lambda(-v) = -(\lambda v),$$
for any $\lambda \in \mathbb{F}$ *and* $v \in V$.

Proof. i) In any field we have that $0 = 0 + 0$, this gives us that for any $v \in V$
$$\begin{aligned} 0v &= (0+0)v \\ &= 0v + 0v. \end{aligned}$$
By cancellation laws of $(V, +)$ we have that
$$\mathbf{0} = 0v.$$

ii) Let $v \in V$ then for any $\lambda \in \mathbb{F}$ we have that
$$\lambda v + \mathbf{0} = \lambda v = \lambda(v + \mathbf{0}) = \lambda v + \lambda \mathbf{0},$$
which implies that
$$\mathbf{0} = \lambda \mathbf{0}.$$

iii) We already dealt with the case $\lambda = 0$ so suppose $\lambda \neq 0$, this means that λ has an inverse $\lambda^{-1} \in \mathbb{F}$, then
$$\lambda v = \mathbf{0} \implies \lambda^{-1}\lambda v = \lambda^{-1}\mathbf{0} \implies v = \lambda^{-1}\mathbf{0} = \mathbf{0}.$$

iv) We know that
$$\mathbf{0} = 0v = (\lambda + (-\lambda))v = \lambda v + (-\lambda)v.$$
Hence,
$$(-\lambda v)v = -(\lambda v).$$

In particular, $(-1)v = -v$. Furthermore,

$$\mathbf{0} = \lambda\mathbf{0} = \lambda(v - v) = \lambda v + \lambda(-v) \implies \lambda(-v) = -(\lambda v).$$

□

Just as with subgroups we can have vector spaces sitting inside bigger vector spaces.

Definition 4.4. Let V be a vector space over $\mathbb{F}$. A non-empty susbset W of V is called a (linear) **subspace** of V if it forms a vector space over $\mathbb{F}$ with the same operations of sum and scalar product.

Theorem 4.5. *Let V be a vector space over $\mathbb{F}$ and $W \subset V$. Then W is a subspace of V if and only if the following conditions hold*

S1

$$\mathbf{0} \in W$$

S2

$$a, b \in W \implies a + b \in W$$

S3

$$\lambda \in \mathbb{F}, a \in W \implies \lambda a \in W.$$

Proof is left as an exercise.

Example. i) V and $\{\mathbf{0}\}$ are always subspaces of V.

ii) Let $u \in V$ and $u \neq \mathbf{0}$. Then,

$$W = \{w = \lambda u : \lambda \in \mathbb{F}\}$$

is a subspace for V. Indeed, $\mathbf{0} = 0u$ so $\mathbf{0} \in W$ satisfying S1. For S2 we look at $a = \lambda_1 u$ and $b = \lambda_2 u$, then

$$a + b = (\lambda_1 + \lambda_2)u \in W.$$

And for S3 we take $a = \lambda_1 u$ so

$$\lambda a = (\lambda\lambda_1)u \in W.$$

We can also express the previous conditions more concisely, as with subgroups.

Theorem 4.6 (Criteria for Subspaces)**.** *Let $W \subset V$, where V is a vector space over $\mathbb{F}$. Then W is a subspace of V if the following conditions hold:*

$\tilde{\text{S}}$1

$$\mathbf{0} \in W$$

$\tilde{\text{S}}$2

$$a, b \in W, \lambda, \mu \in \mathbb{F} \implies \underbrace{\lambda a + \mu b}_{\textit{linear combination}} \in W.$$

Theorem 4.7. *Let U, W be subspaces of the vector space V. Then*

i) *$U \cap W$ is a subspace of V, and*

ii) *$U + W = \{u + w : u \in U, w \in W\}$ is a subspace of V.*

Proof. i) In homework.

ii) First, $\mathbf{0} \in U, W$ so $\mathbf{0} = \mathbf{0} + \mathbf{0} \in U + W$, so S1 is satisfied. Let a, $b \in U + W$ then $a = u_1 + w_1$ and $b = u_2 + w_2$ for some $u_i \in U$ and $w_i \in W$. Then,

$$a + b = (u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2) \in U + W.$$

This means that S2 is satisfied. For S3 we have

$$\lambda a = \lambda(u_1 + w_1) = \lambda u_1 + \lambda u_w \in U + W.$$

Hence $U + W$ is a subspace of V.

□

These properties of course immediately generalise to any number of finite subspaces. So if $U_1, \ldots, U_m$ are subspaces of V then

$$\cap_{j=1}^{m} U_j$$

and

$$\sum_{j=1}^{m} U_j$$

are subspaces of V.

We previously already introduced the concept of a linear combination. Let's make it precise.

Definition 4.8. Let $v_1, \ldots, v_m$ belong to the vector space V. Then the vector

$$v = \sum_{j=1}^{m} \lambda_j v_j = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_m v_m,$$

for any $\lambda_j \in \mathbb{F}$, is called a **linear combination** of the vectors $v_1, \ldots, v_m$.

The name *linear subspace* comes from the fact that a linear subspace is the smallest vector space containing all the possible linear combinations of the generating vectors. This kind of subspace is also called the span of the generating vectors.

Theorem 4.9. *Let $\{v_1, \ldots, v_m\}$ be vectors in V, then the **span** of $v_1, \ldots, v_m$, denoted by*

$$\langle v_1, \ldots, v_m \rangle = \text{span}\{v_1, \ldots, v_m\} = \left\{ \sum_{j=1}^{m} \lambda_j v_j : \lambda_j \in \mathbb{F} \right\},$$

the set of all linear combinations of $v_1, \ldots, v_m$, is a subspace of V.

Proof. Of course $\mathbf{0} = 0v_1 + \ldots + 0v_m$ so $\mathbf{0}$ is in the span, then for $u = \sum_{j=1}^{m} \mu_j v_j$ and $w = \sum_{j=1}^{m} \nu_j v_j$ we have that

$$\lambda u + \rho w = \sum_{j=1} (\lambda \mu_j + \rho \nu_j) v_j \in \langle v_1, \ldots, v_m \rangle.$$

Hence the span is a subspace of V. □

Remark. i) If $U \cap W = \emptyset$, then we write

$$U \oplus W$$

instead of $U + W$ and call it a **direct sum**.

ii) We say that the vectors $v_1, \ldots, v_m$ **span** W if

$$W = \langle v_1, \ldots, v_m \rangle.$$

4.1 Linear Independence and Bases

Having introduced linear combinations it makes sense to ask which vectors in a vector space can be expressed as a linear combination of some other vectors. We'll introduce some terminology in order to answer this question.

Definition 4.10. Let V be a vector space over $\mathbb{F}$.

- The collection of vectors $v_1, \ldots, v_m$ of V is called **linearly dependent** if there exists a nontrivial dependency relation between them, i.e. if we can find $\lambda_1, \ldots, \lambda_m \in \mathbb{F}$, not all zero, such that

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = \mathbf{0}.$$

- Conversely, the collection of vectors $v_1, \ldots, v_m$ of V is called **linearly independent** if there is no such nontrivial dependency relation, i.e. if

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = \mathbf{0}$$

implies that $\lambda_1 = \ldots = \lambda_m = 0$.

Example. The vectors

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

in $\mathbb{R}^3$ are linearly dependent since

$$v_1 = v_2 + v_3,$$

i.e. we can write

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \mathbf{0}$$

with $\lambda_1 = 1$, $\lambda_2 = -1$, $\lambda_3 = -1$.

In our investigation of which sets are linearly independent and which sets span the whole vector space, we start with the following simple observations.

Proposition 4.11. *Let V be a vector space and $\{v_1, \ldots, v_m\}$ a collection of its vectors.*

i) *If $\mathbf{0} \in \{v_1, \ldots, v_m\}$ then $v_1, \ldots, v_m$ are linearly dependent.*

ii) *If $m > 1$ and $\{v_1, \ldots, v_m\}$ are linearly dependent, then at least one vector of the set can be written as a linear combination of the others.*

iii) *If the set $\{v_1, \ldots, v_m\}$ is linearly dependent, then each superset[1] of $\{v_1, \ldots, v_m\}$ is also linearly dependent.*

iv) *A single vector $v \neq \mathbf{0}$ is linearly independent.*

v) *Each subset of a collection of linearly independent vectors is also linearly independent.*

Proof. i) Suppose WLOG[2] $v_1 = \mathbf{0}$, then pick some $\lambda_1 \neq 0$ and let $\lambda_2 = \ldots = \lambda_m = 0$. Then

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = \mathbf{0},$$

but not all coefficients are 0. Hence this is a nontrivial dependence relation and so $\{\mathbf{0}, v_2, \ldots, v_m\}$ is linearly dependent.

[1] A superset B of A is any set such that A is contained in B, i.e. $A \subseteq B$.
[2] Without loss of generality

ii) Suppose

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = \mathbf{0}.$$

Then we can pick at least one λ_i to be nonzero. WLOG suppose that $\lambda_1 \neq 0$. Hence $\exists \lambda^{-1} \in \mathbb{F}$, so

$$v_1 + \lambda_1^{-1}\lambda_2 v_2 + \ldots + \lambda_1^{-1}\lambda_m v_m = \mathbf{0}$$

and

$$v_1 = (-\lambda_1^{-1}\lambda_2)v_2 + \ldots + (-\lambda_1^{-1}\lambda_m)v_m.$$

iii) Suppose

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = \mathbf{0}$$

for some scalars $\lambda_i \in \mathbb{F}$, not all zero. Then take any set of vectors $\{v_{m+1}, \ldots, v_s\}$ in V and look at the union $\{v_1, \ldots, v_s\}$. To see that these are linearly dependent write

$$\lambda_1 v_1 + \ldots + \lambda_m v_m + \lambda_{m+1} v_{m+1} + \ldots + \lambda_s v_s = \mathbf{0}.$$

Then, we can take $\lambda_{m+1} = \ldots = \lambda_s = 0$ and $\lambda_1, \ldots, \lambda_m$ to be the same as before, giving us a nontrivial dependency relation. Hence $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_s\}$ is linearly dependent.

iv) $\lambda_1 v = \mathbf{0}$ implies that $\lambda_1 = 0$ or $v = \mathbf{0}$. Since $v \neq 0$ we must have that $\lambda_1 = 0$.

v) Suppose

$$\lambda_1 v_1 + \ldots + \lambda_m v_m + \lambda_{m+1} v_{m+1} + \ldots + \lambda_s v_s = \mathbf{0}$$

if and only if $\lambda_1 = \ldots = \lambda_s = 0$ so that these vectors are linearly independent. Then if you take any subset of these vectors, say, $\{v_1, \ldots, v_m$, by seting $\lambda_{m+1} = \ldots = \lambda_s = 0$ and looking at

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = \mathbf{0}$$

gives that $\lambda_1 = \ldots = \lambda_m = 0$ as otherwise we could get a nontrivial dependence relation for $\{v_1, \ldots, v_s\}$.

□

Definition 4.12. The vectors $\{v_1, \ldots, v_m\}$ are called **generators** of the vector space V if they span V, i.e. if every vector of V can be written as linear combination of them. So,

$$V = \langle v_1, \ldots, v_m \rangle,$$

i.e.

$$\forall v \in V \exists \lambda_j \in \mathbb{F} \text{ s.t. } v = \sum_{j=1}^{m} \lambda_j v_j.$$

Try doing the following exercise:

Example. Do the following vectors span $\mathbb{R}^3$?

$$\{u_1, u_2, u_3, u_4\} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix} \right\}.$$

You need to see if for any $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ you can find $\lambda_1, \ldots, \lambda_4$ such that

$$\lambda_1 u_1 + \ldots + \lambda_4 u_4 = v.$$

This is a linear system with 4 unknowns $\lambda_1, \ldots, \lambda_4$ and constants from v on the right hand side.

An important case of a set of vectors is when they are both linearly independent and span the whole vector space.

Definition 4.13. Let $B = \{v_1, \ldots, v_n\}$ be a set of vectors in the vector space V. B is called a **basis** for V if the following two conditions hold:

i) B is linearly independent, and

ii) B spans V.

Example. Let

$$B = \left\{ e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \in \mathbb{R}^2.$$

To see that these are linearly independent we need to look at

$$\lambda_1 \begin{pmatrix} 1 // 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbf{0}.$$

This simplifies to

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

so $\lambda_1 = \lambda_2 = 0$. Hence B is linearly independent.

To see that they span $\mathbb{R}^2$ we need to express $v = \begin{pmatrix} x \\ y \end{pmatrix}$ in terms of e_1 and e_2. Clearly,

$$v = xe_1 + ye_2.$$

Hence B spans $\mathbb{R}^2$ and thus is a basis.

Note: In general

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}$$

is a basis for $\mathbb{R}^n$, called the **standard basis**. We normally denote it by

$$\{e_1, \ldots, e_n\}.$$

Theorem 4.14. *The set $\{v_1, \ldots, v_n\}$ of vectors in V is a basis for V if and only if every element of V can be written as a unique linear combination of $v_1, \ldots, v_n$.*

Proof. $\underline{\Longrightarrow:}$ Let $\{v_1, \ldots, v_n\}$ be a basis for V. Suppose, for contradiction, that for some $v \in V$, the linear combination is not unique. Then we have

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$
$$v = \mu_1 v_1 + \ldots + \mu_n v_n.$$

where the linear combinations are different. But then,

$$\mathbf{0} = (\lambda_1 - \mu_1)v_1 + \ldots + (\lambda_n - \mu_n)v_n,$$

which by linear independence implies that $\lambda_i - \mu_i = 0$, i.e. $\lambda_1 = \mu_1, \ldots, \lambda_n = \mu_n$, contradiction. Hence the linear combination is unique.

$\underline{\Longleftarrow:}$ Assume that every v can be expressed as a unique linear combination of $v_1, \ldots, v_n$. We need to show that these vectors form a basis. Spanning is immediate from the assumption, so let us prove the linear independence. Consider,

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = \mathbf{0}.$$

Then, $\lambda_1 = \ldots = \lambda_n = 0$ is one possible solution. But by assumption the solution is unique so the above is the only solution. Hence these vectors are linearly independent and form a basis for V.

□

So clearly bases are a useful thing to have a vector space because they give us a nice representation for any vector in the vector space. The natural question to ask is whether vector spaces always have a basis, and if they do, then what do different bases have in common? First we differentiate an important class of vector spaces.

Definition 4.15. The vector space V is called **finitely generated** if there is a finite set of vectors $\{v_1, \ldots, v_m\}$ $(m < \infty)$ spanning V.

Definition 4.16. Let V be a finitely generated vector space. Then every finite set of vectors which spans V contains a subsequence which is a basis for V.

Proof. Let $e_1, \ldots, e_m$ span V. If $e_1 = \mathbf{0}$, discard e_1; otherwise keep it. If e_2 can be written as linear combination of e_1 then discard e_2, otherwise keep e_2. In general, if e_j belongs to

$$\langle e_1, \ldots, e_{j-1} \rangle,$$

then discard e_j, otherwise keep it. This produces a subsequence $e_{k_1}, \ldots, e_{k_r}$, where $k_1 < k_2 < \ldots < k_r$ in which no vector is linearly independent of the predecessors. We claim that this is a basis for V. Let's prove this.

spanning: Since each $v \in V$ can be written as

$$v = \sum_{j=1}^{m} \alpha_j e_j$$

and since each e_j can be written as

$$e_j = \sum_{i=1}^{r} \beta_i e_{k_i},$$

then

$$v = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{r} \beta_i e_{k_i}$$

which rearranges to

$$v = \sum_{i=1}^{r} \left(\sum_{j=1}^{m} \alpha_j \beta_i \right) e_{k_i}.$$

Hence any vector can be expressed as a linear combination of e_{k_i}, i.e.

$$V = \langle e_{k_1}, \ldots, e_{k_r} \rangle.$$

linear independence: By contradiction, suppose $\{e_{k_1}, \ldots, e_{k_r}\}$ is linearly dependent, so that

$$\lambda_1 e_{k_1} + \ldots + \lambda_r e_{k_r} = \mathbf{0},$$

with some $\lambda_j \neq 0$. Let λ_s be the last nonzero scalar in the sequence of scalars $\lambda_1, \ldots, \lambda_r$. Then

$$\lambda_1 e_{k_1} + \ldots + \lambda_s e_{k_s} = \mathbf{0}.$$

Hence

$$e_{k_s} = (-\lambda_s^{-1}\lambda_1)e_{k_1} + \ldots + (-\lambda_s^{-1}\lambda_{s-1})e_{k_{s-1}}.$$

This is a contradiction since by construction the e_{k_i}'s are linearly independent of the predecessing ones. Hence $e_{k_1}, \ldots, e_{k_r}$ are linearly independent and so form a basis for V.

□

So we have shown that any spanning set can be reduced to a basis. Similar theorem holds for extending a linearly independent set to a basis for finitely generated vector spaces.

Theorem 4.17 (Extension Theorem)**.** *Let V be a finitely generated vector space and let $B = \{e_1, \ldots, e_n\}$ be a basis for V. Then,*

i) *If $\{v_1, \ldots, v_p\}$ is a sequence of linearly independent vectors $(p \leq n)$ of V then the sequence can be extended to a basis $\{v_1, \ldots, v_p, e_{k_{p+1}}, \ldots, e_{k_n}\}$ of n vectors by adding $n - p$ elements of B.*

ii) *If $\{f_1, \ldots, f_r\}$ is another basis for V, then $r = n$.*

Proof. i) Since V is a finitely generated, then V has a basis by the previous theorem. Then

$$V = \langle e_1, \ldots, e_n \rangle.$$

We can add v_1 and still have spanning:

$$V = \langle v_1, e_1, \ldots, e_n \rangle$$

with $v_1 \neq 0$. Moreover v_1 can be expressed as a unique linear combination of the e_i, say,

$$v_1 = \lambda_1 e_1 + \ldots + \lambda_n e_n, \tag{4.1}$$

where some $\lambda_j \neq 0$. Without loss of generality (WLOG) we can assume that $\lambda_1 \neq 0$, then,

$$e_1 = \lambda_1^{-1} v_1 + (-\lambda_1^{-1}\lambda_2)e_2 + \ldots + (-\lambda_1^{-1}\lambda_n)e_n.$$

Hence e_1 can be expressed in terms of $v_1, e_2, \ldots, e_n$, so

$$V = \langle v_1, e_2, \ldots, e_n \rangle.$$

Let's prove that $v_1, e_2, \ldots, e_n$ are also linearly independent. Suppose:

$$\mu_1 v_1 + \mu_2 e_2 + \ldots + \mu_n e_n = \mathbf{0}.$$

Then, either

- $\mu_1 \neq 0$ in which case

  $$v_1 = (-\mu_1^{-1}\mu_2)e_2 + \ldots + (-\mu_1^{-1}\mu_n)e_n.$$

  This is different from the decomposition (4.1) where the coefficient of e_1 was nonzero (above it is 0). This is a contradiction so this case cannot occur.

- $\mu_1 = 0$, then

  $$\mu_2 e_2 + \ldots + \mu_n e_n = \mathbf{0},$$

  which gives $\mu_2 = \ldots = \mu_n = 0$ since these vectors are linearly independent. Hence $\{v_1, e_2, \ldots, e_n\}$ is a basis for V.

Let us now use an induction argument to extend this to all of $\{v_1, \ldots, v_p\}$. By the above argument the property holds for $p = 1$. Now suppose it's true for $v_1, \ldots, v_{p-1}$. That is, $\{v_1, \ldots, v_{p-1}, e_p, \ldots, e_n\}$ (up to relabeling the e_is) is a basis for V. We need to prove it for p vectors.

Consider $v_1, \ldots, v_p$ and write

$$v_p = \eta_1 v_1 + \ldots + \eta_{p-1} v_{p-1} + \eta_{p+1} e_{p+1} + \ldots + \eta_n e_n.$$

Since $v_1, \ldots, v_p$ are linearly independent, then at least one of the scalars $\eta_{p+1}, \ldots, \eta_n$ is not zero. WLOG suppose that $\eta_p \neq 0$. Then by a similar argument as before the vectors $\{v_1, v_2, \ldots, v_p, e_{p+1}, \ldots, e_n\}$ are a basis for V (up to relabeling of the e_i's). Hence the first part is proved for $p \leq n$.

ii) If $r > n$ then consider $\{f_1, \ldots, f_n\}$ which is still a linearly independent set. By the previous part (with $p = 0$) this is also a basis for V. Hence we can express f_r in terms of $\{f_1, \ldots, f_n\}$. This contradicts the fact

that $\{f_1, \ldots, f_r\}$ is a linearly independent set of vectors. Hence $r \leq n$. Similarly $n \leq r$. Hence $r = n$.

□

So we have proven that every basis of a given vector space has the same number of elements. It makes sense to give this number a name.

Definition 4.18. Let V be a finitely generated vector space. Then every basis for V contains the same number of vectors. We call this number the **dimension** of V, denoted by $\dim V$.

Example. i) $\dim \mathbb{R}^2 = 2$,

ii) $\dim \mathbb{R}^n = n$,

iii) $\dim M(n, m, \mathbb{R}) = nm$,

iv) $\dim\{\mathbf{0}\} = 0$ as it has no basis.

So let's summarize what we've found out so far. If $\dim V = n$ then,

- any basis B for V has n vectors,
- if $\{v_1, \ldots, v_p\}$ span V, then $p \geq n$,
- if $\{v_1, \ldots, v_m\}$ are linearly independent then $m \leq n$.

Proposition 4.19. *Let U be a subspace of V. Then*

i) $\dim U \leq \dim V$. *If* $\dim U = \dim V$ *then* $U = V$.

ii) *There is a subspace M such that*

$$U \oplus M = V,$$

that is $U + M = V$ and $U \cap M = \{\mathbf{0}\}$.

iii) *(Grassmann's equality) Let W be a second subspace of V, then*

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W).$$

Proof. The first part is clear by definition. For the second part let $\{u_1, \ldots, u_r\}$ be a basis for U. Then, given $n = \dim V$, we can extend this to a basis for V by the extension theorem, say, $\{u_1, \ldots, u_r, e_{r+1}, \ldots, e_n\}$. Let's define

$$M = \langle e_{r+1}, \ldots, e_n \rangle.$$

Then clearly $M \cap U = \{\mathbf{0}\}$ as otherwise we would get a nontrivial dependence relation for our basis. Also $M + U = V$ since the above set spans V. The last part of the proposition is proved in the exercises. □

Example. Let $V = \mathbb{R}^3$ and suppose $U = \{(x_1, x_2, 0) | x_1, x_2 \in \mathbb{R}\}$, $W = \{(0, y_1, y_2) | y_1, y_2 \in \mathbb{R}\}$. Then U and W are subspaces of V (prove it!). A basis for U is given by

$$B_1 = \{e_1 = (1, 0, 0), e_2 = (0, 1, 0)\}.$$

To see this we need to prove that B_1 spans V and is L.I. For spanning let $x = (x_1, x_2, 0) \in U$, then

$$x = x_1 e_1 + x_2 e_2,$$

so B_1 spans U. For linear independence suppose that

$$\lambda_1 e_1 + \lambda_2 e_2 = (\lambda_1, \lambda_2, 0) = \mathbf{0},$$

which immediately implies that $\lambda_1 = \lambda_2 = 0$. So B_1 is a basis for U.

Similarly you can prove that $B_2 = \{e_2 = (0, 1, 0), e_3 = (0, 0, 1)\}$ is a basis for W. Now let's verify Grassman's equality. We know that $\dim U = \dim W = 2 \leq 3$. Clearly

$$U + W = V = \langle e_1, e_2, e_3 \rangle$$

and

$$U \cap W = \langle e_2 \rangle \neq \{\mathbf{0}\}.$$

Thus,

$$\dim(U+W) = 3 = 2 + 2 - 1 = \dim U + \dim W - \dim(U \cap W).$$

4.2 Linear Transformations

Linear transformations (or linear maps) are special kind of mappings between vector spaces which are group homomorphisms in two different ways.

Definition 4.20. Let V, W be two vector spaces over the same field $\mathbb{F}$. A mapping $T : V \to W$ is called a **linear transformation** or **linear map** if it satisfies

T1

$$T(a+b) = T(a) + T(b), \quad \forall a, b \in V$$

T2

$$T(\alpha a) = \alpha T(a), \quad \forall a \in V, \forall \alpha \in \mathbb{F}.$$

Corollary 4.21. *$T : (V, +) \to (W, +)$ is a homomorphism of groups, hence*

i)
$$T(\mathbf{0}_V) = \mathbf{0}_W,$$

ii)
$$T(-a) = -T(a), \forall a \in V.$$

Proof. The first property follows from the fact that group homomorphism maps identities to identities. The second from mapping inverses to inverses. □

Example. Let $T : V \to W$ with $V = \mathbb{R}^3$ and $W = \mathbb{R}^2$ be defined by

$$T(x_1, x_2, x_3) = (x_1 + x_2, x_3).$$

We'll prove that T is a linear map.

T1 Let $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$, then

$$a + b = (a_1 + b_1, a_2 + b_2, a_3 + b_3),$$

and so

$$T(a+b) = (a_1 + b_1 + a_2 + b_2, a_3 + b_3)$$

while

$$T(a) + T(b) = (a_1 + a_2, a_3) + (b_1 + b_2, b_3) = T(a+b).$$

T2 Let $\alpha a = (\alpha a_1, \alpha a_2, \alpha a_3)$, then

$$T(\alpha a) = (\alpha a_1 + \alpha a_2, \alpha a_3)$$

while

$$\alpha T(a) = \alpha(a_1 + a_2, a_3) = T(\alpha a).$$

Hence T is a linear map.

There are two subspaces associated to each linear map, which are related to injectivity and surjectivity.

Definition 4.22. Let $T : V \to W$ be a linear map between the vector spaces V, W over $\mathbb{F}$. The **kernel** of T is the subset of V given by

$$\ker T = \{v \in V : T(v) = \mathbf{0}\}.$$

The **image** of T is the subset of W given by

$$\operatorname{Im} T = \{w \in W : w = T(v) \text{ for some } v \in V\}.$$

Let us prove that these actually form subspaces.

Theorem 4.23. *Let T, V, W be as before. Then*

i) $\ker T$ *is a subspace of* V,

ii) $\operatorname{Im} T$ *is a subspace of* W.

Proof. i) From the previous corollary, $T(\mathbf{0}_V) = \mathbf{0}_W$. Hence $\mathbf{0} \in \ker T$. Let $a, b \in \ker T$ and $\lambda, \mu \in \mathbb{F}$,then

$$T(\lambda a + \mu b) = T(\lambda a) + T(\mu b) = \lambda T(a) + \mu T(b) = \lambda \mathbf{0} + \mu \mathbf{0} = \mathbf{0}.$$

Hence $\ker T$ is a subspace of V.

ii) Again by the same argument $\mathbf{0} \in \operatorname{Im} T$. Let $c, d \in \operatorname{Im} T$ then there are $a, b \in V$ such that $T(a) = c$ and $T(b) = d$. Hence, for $\lambda, \mu \in \mathbb{F}$,

$$\lambda c + \mu d = \lambda T(a) + \mu T(b) = T(\lambda a) + T(\mu b) = T(\lambda a + \mu b).$$

As $\lambda a + \mu b \in V$, it follows that $\lambda a + \mu d \in \operatorname{Im} T$. Hence $\operatorname{Im} T$ is a subspace of W.

□

Theorem 4.24. *Let $T : V \to W$ be a linear transformation, then*

i) *T is surjective* $\iff \operatorname{Im} T = W \iff \dim \operatorname{Im} T = \dim W$.

ii) *T is injective* $\iff \ker T = \{\mathbf{0}_V\} \iff \dim \ker T = 0 \iff \dim \operatorname{Im} T = \dim V$.

Proof. i) This is by definition.

ii) $\underline{\Longrightarrow}$**:** Suppose T is injective. Let $a \in \ker T$. We already know that $T(\mathbf{0}) = \mathbf{0}$, but by assumption $T(a) = \mathbf{0}$. Hence by injectivity $a = \mathbf{0}$, so $\ker T = \{\mathbf{0}\}$.

$\underline{\Longleftarrow}$**:** Suppose $\ker T = \{\mathbf{0}\}$, and that $T(a) = T(b)$. Then by linearity $T(a - b) = \mathbf{0}$. By assumption $a - b = \mathbf{0}$ so $a = b$, which proves injectivity. The last equivalency will follow from the Rank-Nullity theorem that we'll prove later.

□

Example. Let $T : \mathbb{R}^3 \to \mathbb{R}^2$ and $T(x_1, x_2, x_3) = (x_1 + x_2, x_3)$ as before. We wish to find the kernel and image of T.

- Suppose $a \in \ker T$. Then $T(a) = \mathbf{0}_{\mathbb{R}^2} = (0, 0)$. Hence,

$$T(a) = (a_1 + a_2, a_3) = (0, 0)$$

so we deduce that

$$\begin{cases} a_1 + a_2 = 0 \\ a_3 = 0 \end{cases}.$$

Hence $a = (a_1, -a_1, 0)$ so

$$\ker T = \{a \in \mathbb{R}^3 : a = (a_1, -a_1, 0) \text{ for any } a_1 \in \mathbb{R}\}.$$

To find a basis for $\ker T$ we write the general element as

$$(a_1, -a_1, 0) = a_1(1, -1, 0).$$

So if we let $e = (1, -1, 0)$ then

$$\ker T = \langle e \rangle,$$

so $\dim \ker T = 1$.

- Suppose $c \in \operatorname{Im} T$. Then there exists an $a \in V$ with $c = T(a)$. This means that

  $$c = (c_1, c_2) = (a_1 + a_2, a_3) = T(a).$$

  So any such c must satisfy

  $$\begin{cases} c_1 = a_1 + a_2 \\ c_2 = a_3 \end{cases}$$

  for some $a_i \in \mathbb{R}$. Since we are free to choose a_i freely we can let e.g. $a_2 = 0$ to get that $c_1 = a_1$, $c_2 = a_3$, i.e. $\operatorname{Im} T = \mathbb{R}^2$. Thus a basis for the image is

  $$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

  Therefore $\dim \operatorname{Im} T = 2$.

Even though the kernel and the image are subspaces of a different vector space, they are still intimately related. We will now prove the most important theorem about the dimension of these spaces. It is called the Rank-Nullity Theorem (or sometimes the Kernel-Rank Theorem or the Dimension Theorem).

Theorem 4.25 (Rank-Nullity Theorem)**.** *Let V, W be finite-dimensional vector spaces over the same field $\mathbb{F}$. Let $T : V \to W$ be a linear transformation. Then*

$$\dim \operatorname{Im} T + \dim \ker T = \dim V.$$

Proof. Let $\{v_1, \ldots, v_s\}$ be a basis for $\ker T$, i.e. $\dim \ker T = s$. Then, by the extension theorem, we can extend this into a basis for V:

$$\{v_1, \ldots, v_s, v_{s+1}, \ldots, v_n\}$$

where $n = \dim V$ and $s \leq n$. If $n = s$ then $\ker T = V$ and $\operatorname{Im} T = \{\mathbf{0}\}$ so the result is clear. Suppose $n > s$. We'll show that $\{T(v_{s+1}), \ldots, T(V_n)\}$ is a basis for $\operatorname{Im} T$. This is enough as then

$$\dim \operatorname{Im} T = n - s = \dim V - \dim \ker T.$$

- For linear independence let

$$\begin{aligned} \mathbf{0} &= \lambda_{s+1} T(v_{s+1}) + \ldots + \lambda_n T(v_n) \\ &= T(\lambda_{s+1} v_{s+1} + \ldots \lambda v_n \end{aligned}$$

  as T is a linear transformation. This implies that $\lambda_{s+1} v_{s+1} + \ldots + \lambda_n v_n \in \ker T$. Hence we can express this as a linear combination of the basis of $\ker T$. So there are some $\lambda_1, \ldots, \lambda_s \in \mathbb{F}$ such that

$$\lambda_{s+1} v_{s+1} + \ldots + \lambda_n v_n = \lambda_1 v_1 + \ldots + \lambda_s v_s$$

$$\implies \lambda_1 v_1 + \ldots + \lambda_s v_s - \lambda_{s+1} v_{s+1} - \ldots - \lambda_n v_n = \mathbf{0}.$$

  These vectors are linearly independent so $\lambda_1 = \ldots = \lambda_n = 0$. In particular, $\lambda_{s+1} = \ldots = \lambda_n = 0$. Hence $\{T(v_{s+1}), \ldots, T(v_n)\}$ is linearly independent.

- For spannign let $w \in \operatorname{Im} T$. Then $w = T(v)$ for some $v \in V$. Write

$$v = \mu_1 v_1 + \ldots + \mu_n v_n$$

  for some $\mu_i \in \mathbb{F}$. We have

$$w = T(v) = T(\mu_1 v_1 + \ldots + \mu_n v_n) = \mu_1 T(v_1) + \ldots + \mu_n T(v_n).$$

But $T(v_1) = \ldots = T(v_s) = \mathbf{0}$ since $\{v_1, \ldots, v_s\} \subset \ker T$. It follows that

$$w = \mu_{s+1}T(v_{s+1}) + \ldots + \mu_n T(v_n).$$

Hence $w \in \langle T(v_{s+1}), \ldots, T(v_n)\rangle$. We conclude that $\{T(v_{s+1}), \ldots, T(v_n)\}$ is a basis for $\operatorname{Im} T$.

□

Corollary 4.26. *Let $T : V \to W$ be a linear transformation and let $\{e_1, \ldots, e_n\}$ be a basis for V. Then $T(e_1), \ldots, T(e_n)$ span $\operatorname{Im} T$.*

Proof. See the "spanning" part of the previous proof. We do not get linear independence as some of the e_i's might belong to the kernel, for example. □

Another way to compute a basis for image is by using this corollary. We take a basis for the domain and extract a basis from the image of the basis elements.

Example. We work in the same setting as in the previous example. Take a basis for $\mathbb{R}^3$, e.g.

$$B = \{(1,0,0), (0,1,0), (0,0,1)\}.$$

Compute its image:

$$\begin{aligned} T(1,0,0) &= (1,0) \\ T(0,1,0) &= (1,0) \\ T(0,0,1) &= (0,1). \end{aligned}$$

The corollary says that the image is spanned by these vectors, i.e.

$$\operatorname{Im} T = \langle (1,0), (1,0), (0,1)\rangle.$$

Obviously they are not linearly independent, but we can extract a linearly independent set. An obvious choice is $\{(1,0), (0,1)\}$. Thus this is a basis for $\operatorname{Im} T$ and we get that

$$\dim \mathbb{R}^3 - \dim \operatorname{Im} T = 3 - 2 = 1 = \dim \ker T.$$

Example. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be given by

$$T(x, y, z) = (x + y - z, 3x - y - z, 5x + y - 3z).$$

Prove that T is a linear transformation. To find a basis for $\ker T$ we need to look at

$$T(x, y, z) = (0, 0, 0),$$

which gives us the system

$$\begin{cases} x & +y & -z & = 0 \\ 3x & -y & -z & = 0 \\ 5x & +y & -3z & = 0 \end{cases}$$

To solve this we use row reduction on the augmented matrix to get

$$\left(\begin{array}{ccc|c} 1 & 0 & \frac{-1}{2} & 0 \\ 0 & 1 & \frac{-1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence, if we let $z = 2\alpha$, then $x = \alpha$, $y = \alpha$. So,

$$\ker T = \{(x, y, z) = (\alpha, \alpha, 2\alpha) = \alpha(1, 1, 2)\}.$$

Thus,

$$\ker T = \langle (1, 1, 2) \rangle,$$

and $\dim \ker T = 1$.

To find a basis for the iamge we look at the images of the basis vectors of $\mathbb{R}^3$ under T:

$$\begin{aligned} T(e_1) &= T(1, 0, 0) = (1, 3, 5), \\ T(e_2) &= T(0, 1, 0) = (1, -1, 1), \\ T(e_3) &= T(0, 0, 1) = (-1, -1, -3). \end{aligned}$$

Hence the image is spanned by these vectors, so,

$$\operatorname{Im} T = \langle (1, 3, 5), (1, -1, 1), (-1, -1, -3) \rangle.$$

These vectors are not, however, linearly independent and thus do not form a basis for $\operatorname{Im} T$. We have that

$$(1, 3, 5) = -(1, -1, 1) - 2(-1, -1, 3).$$

The 2 vectors on the right hand side are linearly independent so by removing $(1, 3, 5)$ we get a basis for $\operatorname{Im} T$ to be $\{(1, -1, 1), (-1, -1, 3)\}$ and $\dim \operatorname{Im} T = 2$.

Theorem 4.27. *Let V, W be vector spaces over the same field $\mathbb{F}$. Let $\{e_1, \ldots, e_n\}$ be a basis for V and let $\{f_1, \ldots, f_n\}$ be n vectors of W. Then there is a unique mapping T such that*

$$T(e_j) = f_j$$

for $j = 1, \ldots, n$. T is a linear transformation. If, furthermore, $f_1, \ldots, f_n$ is a basis for W then T is invertible.

Proof. Let $a = \sum_{j=1}^{n} \mu_j e_j$ and let $b = \sum_{j=1}^{n} \nu_j e_j$ be vectors of V expressed as a linear combination with respect to the basis $\{e_1, \ldots, e_n\}$. Then we define T by letting

$$T\left(\sum_{j=1}^{n} \mu_j e_j\right) = \sum_{j=1}^{n} \mu_j f_j.$$

We check that T is linear:

T1

$$\begin{aligned} T(a + b) &= T\left(\sum_{j=1}^{n} (\mu_j \nu_j) e_j\right) \\ &= \sum_{j=1}^{n} (\mu_j + \nu_j) f_j \\ &= \sum_{j=1}^{n} \mu_j f_j + \sum_{j=1}^{n} \nu_j f_j \\ &= T(a) + T(b). \end{aligned}$$

T2

$$\begin{aligned} T(\lambda a) &= T\left(\sum_{j=1}^{n}(\lambda\mu_j)e_j\right) \\ &= \sum_{j=1}^{n}(\lambda\mu_j)f_j \\ &= \lambda\sum_{j=1}^{n}\mu_j f_j \\ &= \lambda T(a). \end{aligned}$$

Hence T is linear. Now suppose that $f_1, \ldots, f_n$ forms a basis for W. Then

$$\dim W = \dim \operatorname{Im} T = \dim V.$$

This implies that T is surjective and by rank-nullity theorem it is then injective. Hence T is bijective.

To see that T is unique suppose that $\tilde{T} : V \to W$ be such that $\tilde{T}(e_j) = f_j$ for all j. Then $\tilde{T}(a) = \sum_{j=1}^{n}\mu_j f_j = T(a)$ which means that $T = \tilde{T}$. □

This allows us to give a convenient presentation to vector spaces. Take $W = \mathbb{F}^n$. Then $\dim V = \dim \mathbb{F}^n = n$. Suppose $\{e_1, \ldots, e_n\}$ is a basis for V and $\{f_1, \ldots, f_n\}$ a basis for $\mathbb{F}^n$. Then by above there is an invertible linear map between V and W. So we say that $V \cong \mathbb{F}^n$, that is the two spaces are isomorphic as vector spaces. So we can always represent vector spaces in the form $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ where the x_i belong to some field $\mathbb{F}$.

Proposition 4.28. *Let V, W, U be vector spaces over the same field $\mathbb{F}$.*

i) *If $T_1 : V \to W$ and $T_2 : W \to U$ are linear maps then $T_2 \circ T_1 : V \to U$ is also a linear map.*

ii) *If $T : V \to W$ is bijective linear map then the inverse map $T^{-1} : W \to V$ is also linear.*

iii) *If $T_1, T_2 : V \to W$ are linear maps then for $\lambda \in \mathbb{F}$:*

- *$T_1 + T_2 : V \to W$, given by*

$$(T_1 + T_2)(v) = T_1(v) + T_2(v),$$

and

- *$\lambda T_1 : V \to W$, given by*

$$(\lambda T_1)(v) = \lambda T_1(v)$$

are linear transformations.

4.3 The Matrix of a Linear Transformation

Let us now show how matrices and linear transformations are related. Let $T : V \to W$ be a linear map, and let $B_V = \{e_1, \ldots, e_n\}$, $B_W = \{b_1, \ldots, b_m\}$ be bases for V and W, respectively. Hence $\dim V = n$ and $\dim W = m$. Then, given a vector $v \in V$, say,

$$v = \mu_1 e_1 + \ldots + \mu_n e_n,$$

we get

$$T(v) = T\left(\sum_{j=1}^{n} \mu_j e_j\right) = \sum_{j=1}^{n} \mu_j T(e_j).$$

Hence, T is *completely determined by its action on the basis* for V. Since $T(e_j) \in W$, $1 \leq j \leq n$, we can write them as unique linear combinations of the basis B_W:

$$\begin{aligned} T(e_1) &= \alpha_{11} b_1 + \ldots + \alpha_{m1} b_m \\ T(e_2) &= \alpha_{12} b_1 + \ldots + \alpha_{m2} b_m \\ &\vdots \\ T(e_n) &= \alpha_{1n} b_1 + \ldots + \alpha_{mn} b_m, \end{aligned}$$

where $\alpha_{ij} \in \mathbb{F}$. We associate with T the matrix

$$A = (\alpha_{ij})_{m\times n} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \vdots & & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}.$$

Notice that the columns of A correspond to the rows in the above system of equations, i.e. the coefficients of $T(e_1)$ give the first *column* of the matrix A and so on. A is of course uniquely determined by T along with the chosen bases for V and W. An A of this form is called the **matrix associated with the linear map** T with respect to the bases B_V and B_W. So, this allows us to write (at least if V and W are of the form $\mathbb{F}^n$ and $\mathbb{F}^m$)) T as

$$T : V \to W, v \mapsto Av.$$

There's a subtle point we haven't emphasised so far. We saw that any vector space is isomorphic to a vector space of the form $\mathbb{F}^n$. However, this representation sneakily hides the fact that each element of the vector space is a multiple of some vector whereas when we write e.g. $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ we are only specifying *coordinates*. These coordinates need to be with respect to some basis. So for example, most commonly the above coordinates would correspond to the vector $1 \cdot e_1 + 0 \cdot e_2$ in the standard basis of $\mathbb{R}^2$, but equally well we could consider another basis, say,

$$F = \left\{ f_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, f_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

(In here these coordinates are with respect to the standard basis so $f_1 = e_1 - e_2$ and $f_2 = e_2$) Then the vector with coordinates $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ with respect to this basis would correspond to the vector $1 \cdot f_1 + 0 \cdot f_2$, in standard basis this corresponds to the vector $e_1 - e_2$ as seen before. To avoid this confusion we sometimes write the name of the basis as a subscript when it's important. If we are using the standard basis then we normally write the coordinates without a subscript. So the two vectors

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 \\ 0 \end{pmatrix}_F$$

actually represent two different vectors in the same vector space (e_1 and $e_1 - e_2$). Let's do an example of this.

Example. Let $T : \mathbb{R}^3 \to \mathbb{R}^2$ be given by

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + y \\ x - y \end{pmatrix}.$$

Verify that T is linear. Choose,

$$B_V = \left\{ e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$
$$B_W = \left\{ b_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, b_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

to be the standard bases for $\mathbb{R}^3$ and $\mathbb{R}^2$, respectively. Then,

$$T(e_1) = T\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2b_1 + b_2$$
$$T(e_2) = T\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = b_1 - b_2$$
$$T(e_3) = T\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0 \cdot b_1 + 0 \cdot b_2.$$

So the matrix associated to T with respect to the bases B_V and B_W is

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix}.$$

Let's now change the basis[3] for W, so that we get a new matrix. Keep B_V as it is and consider

$$\tilde{B}_W = \left\{ a_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, a_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}.$$

[3]There's more to say about changing bases but we won't focus on that in this course. If you want to find out more look, for example, at Towers sections 7.1 and 7.2.

Then

$$\begin{aligned} T(e_1) &= 1 \cdot a_1 + 1 \cdot a_2 \\ T(e_2) &= -1 \cdot a_1 + 2a_2 \\ T(e_3) &= 0 \cdot a_1 + 0 \cdot a_2. \end{aligned}$$

So the matrix associated to A with respect to these bases is

$$\tilde{A} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 0 \end{pmatrix}.$$

Let's see now what happens with the action of T expressed in the form Av. Take $v = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}_{B_V} \in V$. That is,

$$\begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}_{B_V} = 4e_1 + 1cdote_2 + 2e_3.$$

Then

$$T(v) = T \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}_{B_V} = \begin{pmatrix} 9 \\ 3 \end{pmatrix}_{B_W} \in \mathbb{R}^2.$$

This is equal to

$$A \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 9 \\ 3 \end{pmatrix}.$$

Now consider $T(v)$ expressed in the new basis $\tilde{B}_W$, so

$$T(v) = \tilde{A}v = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix}_{\tilde{B}_W} = 3a_1 + 6a_2.$$

So now,

$$3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 6 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 9 \\ 3 \end{pmatrix}_{B_V} \neq \begin{pmatrix} 3 \\ 6 \end{pmatrix}_{\tilde{B}_V}.$$

$$\begin{array}{ccc} (V, B_V^1) & \xrightarrow{\quad T_A \quad} & (W, B_W^1) \\ J_V \uparrow & & J_W \uparrow \\ (V, B_V^2) & \xrightarrow{\quad T_B \quad} & (W, B_W^2) \end{array}$$

But this is fine since the coordinates on the left hand side are with respect to the standard basis while on the right-hand side the coordinates are with respect to $\tilde{B}_W$.

In general, if we take $\dim V = n$ and $\dim W = m$ and $T : V \to W$ a linear map, and let B_V^1, B_V^2 be bases for V and B_W^1, B_W^2 be bases for W then the following hold:

Here T_A, T_B have the corresponding matrices A and B with respect to the indicated bases. Also, J_V and J_B are the isomorphisms which map one of the bases to the other (remember we showed that such maps are invertible!) with corresponding matrices P and C respectively. Then we can rewrite T_B as

$$T_B = J_W^{-1} \circ T_A \circ J_V,$$

or in terms of the corresponding matrices

$$B = C^{-1}AP.$$

We are interested in the particular case $V = W$ in which case $C = P$ so the above becomes

$$B = P^{-1}AP.$$

So we see that any two matrices for a given linear map, with respect to different bases, are related by conjugation by an invertible matrix. We wish to find properties of T that remain invariant under this conjugation. This will be the focus of the following sections.

4.4 Rank of a Matrix

Let $A = (\alpha_{ij})_{m\times n}$ be an $m \times n$ matrix with $\alpha_{ij} \in \mathbb{F}$. Let $S_n = \{e_1, \ldots, e_n\}$ and $S_m = \{f_1, \ldots, f_m\}$ be the standard bases for $\mathbb{F}^n$ and $\mathbb{F}^m$, respectively. Define $T : \mathbb{F}^n \to \mathbb{F}^m$ to be the linear transformation corresponding to A with respect to S_n and S_m. So,

$$T(e_i) = \sum_{j=1}^{m} \alpha_{ji} f_j.$$

Definition 4.29. The **rank** of A is defined as

$$\operatorname{rank} A = \dim \operatorname{Im} T (= \operatorname{rank} T).$$

The **row rank** of A is the dimension of the subspace of $\mathbb{F}^m$ spanned by the rows of A. The **column rank** of A is the dimension of the subspace of $\mathbb{F}^n$ spanned by the columns of A.

Example. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ with

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + y \\ x - y \end{pmatrix}.$$

The matrix associated with T with respect to the standard basis is

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix}.$$

So,

$$\begin{aligned} \text{column rank of } A &= \dim\langle \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \rangle \\ &= 2 \\ &= \dim\langle T(e_1), T(e_2), T(e_3) \rangle \\ &= \dim \operatorname{Im} T = \operatorname{rank} A. \end{aligned}$$

Theorem 4.30.

$$\operatorname{rank} A = \textit{column rank of } A = \textit{row rank of } A.$$

Proposition 4.31. *Let $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{p\times r}$ be matrices over $\mathbb{F}$. Then,*

i) *If $m = p$ and $n = r$,*

$$\operatorname{rank}(A + B) \leq \operatorname{rank} A + \operatorname{rank} B.$$

ii)
$$\operatorname{rank} A^{\intercal} = \operatorname{rank} A$$

iii) *If $n = p$,*
$$\operatorname{rank}(AB) \leq \min(\operatorname{rank} A, \operatorname{rank} B).$$

iv)
$$\operatorname{rank} A = \operatorname{rank} B$$

if A and B are row-equivalent. In particular, if B is the RREF of A, then $\operatorname{rank} A = \operatorname{rank} B =$ *number of nonzero rows of B.*

4.5 Systems of Linear Equations and Rank

Consider the system of equations

$$\begin{aligned} a_{11}x_1 &+ \ldots &+ a_{1n}x_n &= b_1 \\ &\vdots & & \\ a_{m1}x_1 &+ \ldots &+ a_{mn}x_n &= b_m, \end{aligned} \tag{4.2}$$

and let

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{F}^n, b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{F}^m, A = (a_{ij})_{m\times n}.$$

Then we see that (4.2) is equivalent to

$$Ax = b. \tag{4.3}$$

Consider $T : \mathbb{F}^n \to \mathbb{F}^m$ given by $x \mapsto Ax$, i.e. the linear map associated to A with respect to the standard bases on both sides. Then (4.3) becomes

$$T(x) = b. \tag{4.4}$$

Let's reformulate our findings in terms of the rank of A.

Theorem 4.32. *The following conditions are equivalent:*

i) $Ax = b$ *is consistent (has solutions)*

ii) $b \in \operatorname{Im} T$

iii) $b \in$ *column space of* A

iv) $\operatorname{rank} A = \operatorname{rank}(A|b)$.

Theorem 4.33. *Let* $\mathbf{0}_m$ *be the null vectors of* $\mathbb{F}^m$. *Then*

i)
$$Ax = \mathbf{0}_m \iff x \in \ker T,$$
so
$$\dim \textit{(space of solutions)} = \dim \ker T = n - \operatorname{rank} A.$$

ii)
$$Ax = b \iff x = x_0 + x_1,$$
where $x_0 \in \ker T$ *and* x_1 *is any particular solution of* $Ax_1 = b$.

So now we can give a final summary of our findings for nonhomogeneous systems:

Theorem 4.34. *Let* $A = (a_{ij})_{n\times n}$ *be* $n \times n$ *matrix and* b *a fixed column vector. Then the following are equivalent:*

i) $Ax = b$ *has a unique solution.*

ii)

$$\operatorname{rank} A = n.$$

iii)

$$\det A \neq 0.$$

Moreover, if the solution exists it equals

$$x = A^{-1}b.$$

Chapter 5

Eigenvalues and Diagonalisation

We now turn to the final chapter of this course. First we introduce one more invariant for matrices and then we put everything together in order to find particularly nice forms of matrices by diagonalisation.

5.1 Eigenvalues and Eigenvectors

Let $T : V \to V$ be a linear map from an n-dimensional vector space V into itself.

Definition 5.1. An **eigenvector** for T is a nonzero vector $v \in V$ for which there is a $\lambda \in \mathbb{F}$ such that

$$T(v) = \lambda v.$$

λ is called an **eigenvalue** of T corresponding to the eigenvector v. The set of all eigenvalues of T is called the **spectrum** of T, denoted by $\operatorname{spec} T$.

Moreover, if $\lambda \in \operatorname{spec} T$, we denote by $E(\lambda)$ the set of eigenvectors

corresponding to λ together with $\mathbf{0}$, i.e.

$$E(\lambda) = \{v \in V : T(v) = \lambda v\}.$$

$E(\lambda)$ is called the **eigenspace** of λ.

Example. Let $T : \mathbb{R}^2 \to \mathbb{R}^3$ be given by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}.$$

You can see easily that geometrically this is reflection about the x-axis. When looking for eigenvalues we need to solve

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}.$$

Which is the same as the following system of equations:

$$\begin{cases} \lambda x = x \\ \lambda y = -y. \end{cases}.$$

It is easily seen that there are two possible solutions: if $x \neq 0$ then $\lambda = 1$ and $y = 0$; or if $y \neq 0$ then $\lambda = -1$ and $x = 0$. Hence there are two eigenvalues with associated eigenspaces:

$$E(1) = \{\begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R}^3\}$$
$$E(-1) = \{\begin{pmatrix} 0 \\ y \end{pmatrix} : y \in \mathbb{R}^3\}.$$

The matrix associated to T w.r.t. the standard basis is

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

Notice that this is a diagonal matrix with the eigenvalues on the diagonal. Moreover, this matrix satisfies the same eigenvalue properties as T, so

$$A\begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}, \quad A\begin{pmatrix} 0 \\ y \end{pmatrix} = -\begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Theorem 5.2. *Let λ be an eigenvalue for a linear map $T : V \to V$ then $E(\lambda)$ is a subspace of V.*

Proof. **S1** $Tv = \lambda v$ is satisfied by $\mathbf{0}$ so hence $\mathbf{0} \in E(\lambda)$.

S2 Suppose $a, b \in E(\lambda)$ then $T(a) = \lambda a$ and $T(b) = \lambda b$. So

$$T(a + b) = T(a) + T(b) = \lambda a + \lambda b = \lambda(a + b).$$

This implies that $a + b \in E(\lambda)$.

S3 Let $a \in E(\lambda)$ then

$$T(\mu a) = \mu T(a) = \mu\lambda a = \lambda(\mu a),$$

so $\lambda a \in E(\lambda)$.

Hence, $E(\lambda)$ is a subspace of V. □

Not all linear transformations have eigenvalues:

Example. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ such that

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y \\ -x + y \end{pmatrix}.$$

Look for eigenvalues:

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \lambda\begin{pmatrix} x \\ y \end{pmatrix} \iff \begin{cases} x + y = \lambda x \\ -x + y = \lambda y \end{cases} \iff \begin{cases} (\lambda - 1)x = y \\ (\lambda - 1)y = -x. \end{cases}$$

This means that we must have

$$(\lambda - 1)^2 x = -x.$$

Here we have either that $(\lambda - 1)^2 = -1$, which is impossible as the square of a number is always positive, or $x = 0$ in which case $y = 0$ which is not an eigenvector. Hence there can be no eigenvectors.

So the natural question to ask is which T have eigenvalues and how to compute them efficiently.

Let A be a matrix associated with T w.r.t. some basis for V. Then

$$T(v) = \lambda v \iff Av = \lambda v \iff (A - \lambda I_n)v = \mathbf{0}.$$

This system of equations has a nontrivial solution if and only if

$$\det(A - \lambda I_n) = 0.$$

That is, if $A - \lambda I_n$ is noninvertible. This is called the **characteristic equation** of A (or T).

Definition 5.3. The characteristic polynomial of T (or A) is defined as

$$\mathrm{ch}_A(x) = \det(A - \lambda I_n).$$

This is a polynomial of order n. The roots of this polynomial are by definition the eigenvalues of A.

Example. Let

$$A = \begin{pmatrix} 9 & 2 \\ 2 & 6 \end{pmatrix}.$$

We wish to compute the eigenvalues and the corresponding eigenspaces.

First, we factorize the characteristic polynomial:

$$\begin{aligned} \det(A - \lambda I_2) &= \begin{vmatrix} 9-\lambda & 2 \\ 2 & 6-\lambda \end{vmatrix} \\ &= (9-\lambda)(6-\lambda) - 4 \\ &= 54 - 9\lambda - 6\lambda + \lambda^2 - 4 \\ &= \lambda^2 - 15\lambda + 50 \\ &= (\lambda - 5)(\lambda - 10). \end{aligned}$$

So there are two eigenvalues $\lambda_1 = 5$ and $\lambda_2 = 10$.

- $\lambda_1 = 5$ is a simple root. The corresponding eigenvectors satisfy

$$(A - 5I_2)v = \mathbf{0}.$$

So

$$\begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

This gives us the system

$$\begin{cases} 4x + 2y = 0 \\ 2x + y = 0. \end{cases}$$

Hence if $x = \alpha$ then $y = -2\alpha$ so the eigenspace is

$$E(5) = \{ \begin{pmatrix} \alpha \\ -2\alpha \end{pmatrix}, \alpha \in \mathbb{R} \}.$$

A basis for this eigenspace is $\{ \begin{pmatrix} 1 \\ -2 \end{pmatrix} \}$ so it has $\dim E(5) = 1$.

- $\lambda_2 = 10$ is a simple root and the corresponding eigenvectors are such that

$$(A - 10I_2)v = \mathbf{0}.$$

Hence,

$$\begin{pmatrix} -1 & 2 \\ 2 & -4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

This gives us the system

$$\begin{cases} -x + 2y = 0 \\ 2x - 4y = 0 \end{cases}.$$

So if we let $y = \alpha$ then $x = 2\alpha$ and the eigenspace is

$$E(10) = \{ \begin{pmatrix} 2\alpha \\ \alpha \end{pmatrix}, \alpha \in \mathbb{R} \}.$$

Hence a basis is $\{ \begin{pmatrix} 2 \\ 1 \end{pmatrix}. \}$ and the dimension is $\dim E(10) = 1$.

Theorem 5.4. *Let $T : V \to V$ be a linear transformation and B_V^1 and B_V^2 two bases for V. Let A and B be the matrices associated with T w.r.t. B_V^1 and B_V^2 respectively. Then A and B have the same eigenvalues, i.e.*

$$\det(A - \lambda I_n) = 0 \text{ and}$$

$$\det(B - \lambda I_n) = 0$$

have the same roots.

Proof. We call P the matrix of the isomorphism $J : V \to V$, $J(e_j) = c_j$ for $j = 1, \ldots, n$, where $B_V^2 = \{e_1, \ldots, e_n\}$ and $B_V^1 = \{c_1, \ldots, c_n\}$. Then, as seen, $B = P^{-1}AP$ where P is the matrix of J. Consequently,

$$B - \lambda I_n = P^{-1}AP - P^{-1}(\lambda I_n)P = P^{-1}(A - \lambda I_n)P$$

and

$$\begin{aligned} \det(B - \lambda I_n) &= \det P^{-1} \det(A - \lambda I_n) \det P \\ &= \det(A - \lambda I_n). \end{aligned}$$

and the polynomials $\det(B - \lambda I_n)$ and $\det(A - \lambda I_n)$ have the same roots. □

Theorem 5.5. *Eigenspaces corresponding to different eigenvalues are disjoint, i.e. if $\lambda_1 \neq \lambda_2$ then*

$$E(\lambda_1) \cap E(\lambda_2) = \{\mathbf{0}\}.$$

In general, if $\lambda_1 \neq \lambda_2 \neq \ldots \neq \lambda_m$ then

$$E(\lambda_1) \cap \ldots \cap E(\lambda_m) = \{\mathbf{0}\}.$$

Proof. Suppose $\lambda_1 \neq \lambda_2$ and consider $v \in E(\lambda_1) \cap E(\lambda_2)$. Then $T(v) = \lambda_1 v$ and $T(v) = \lambda_2 v$, so

$$(\lambda_1 - \lambda_2)v = \mathbf{0}.$$

Since $\lambda_1 - \lambda_2 \neq 0$ this implies that $v = \mathbf{0}$, i.e.

$$E(\lambda_1) \cap E(\lambda_2) = \{vec0\}.$$

□

Corollary 5.6. *Let $\lambda_1 \neq \ldots \neq \lambda_m$ be distinct eigenvalues of T, then the sum*

$$E(\lambda_1) + \ldots + E(\lambda_m)$$

is direct.

5.2 Diagonalisable Matrices

Definition 5.7. A linear map $T : V \to V$ is called **diagonalisable** if there exists a basis for V such that the matrix D of T associated with this basis on both sides is a diagonal matrix.

A $n \times n$ matrix A is **diagonalisable** if there exists a $P \in GL(n, \mathbb{F})$ such that $P^{-1}AP$ is a diagonal matrix.

Theorem 5.8 (1st Criterion of Diagonalisation)**.** *A linear map $T : V \to V$ is diagonalisable $\iff$ there exists a basis for V composed by eigenvectors of T.*

Proof. $\underline{\Longleftarrow}$**:** If $\{e_1, \ldots, e_n\}$ then $T(e_j) = \lambda_j e_j$. So the matrix associated to T w.r.t. B is the diagonal matrix

$$D = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

so T is diagonalisable.

$\underline{\Longrightarrow}$**:** If D is the matrix of T w.r.t. B, then $T(e_j) = De_j = \lambda_j e_j$ so e_j are eigenvectors.

□

Theorem 5.9 (2nd Criterion of Diagonalisation)**.** *A linear map $T : V \to V$ is diagonalisable $\iff$ given $\lambda_1, \ldots, \lambda_k$ the distinct eigenvalues of T then the sum*

$$E(\lambda_1) \oplus \ldots \oplus E(\lambda_k)$$

is equal to V.

Theorem 5.10 (3rd Criterion of Diagonalisation)**.** *A linear map $T : V \to V$ is diagonalisable $\iff$ the following 2 conditions hold:*

- *characteristic polynomial has n roots in $\mathbb{F}$ (counting with multiplicity),*
- *for each eigenvalue λ_j with algebraic multiplicity f_j we have*

$$\dim E(\lambda_j) = f_j.$$

The dimension $\dim E(\lambda_j)$ is called the **geometric multiplicity** of λ_j and denoted by g_j.

Corollary 5.11. *If the linear transformation $T : V \to V$ on V has n distinct eigenvalues ($\dim V = n$) then T is diagonalisable.*

Theorem 5.12. *Let $T : V \to V$ be a linear transformation and let A be the associated matrix with respect to the basis $B = \{e_1, \ldots, e_n\}$ of V ($\dim V = n$). Let D be the diagonal matrix of its eigenvalues*

$$D = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ 0 & \ddots & 0 \\ 0 & \ldots & \lambda_n \end{pmatrix}$$

and let $\{a_1, \ldots, a_n\}$ be the set of linearly independent eigenvectors related to them. Then call U the matrix having along the columns the components of the vectors $a_1, \ldots, a_n$ w.r.t. the basis B. Then

$$D = U^{-1}AU.$$

Proof. By construction $\{a_1, \ldots, a_n\}$ is the basis for V of eigenvectors of T obtained as union of the bases for $E(\lambda_1), \ldots, E(\lambda_k)$. So U is the invertible matrix of the change of basis $J : V \to V$, $a_i \mapsto a_i = \sum_{j=1}^{n} u_{ji} e_j$, where $U = (u_{ji})_{n \times n}$. Let T_D be the linear map corresponding to D, then we can write it as

$$T_D = J^{-1} \circ T_A \circ J,$$

which, as seen before, gives us

$$D = U^{-1}AU.$$

□

Example. Find the parameter $a \in \mathbb{R}$ such that the matrix

$$A = \begin{pmatrix} 1 & a & a \\ -1 & 1 & -1 \\ 1 & 0 & 2 \end{pmatrix}$$

is diagonalisable.

We first find the roots of the characteristic polynomial:

$$\begin{aligned} \det(A - \lambda I_3) &= \det \begin{vmatrix} 1-\lambda & a & a \\ -1 & 1-\lambda & -1 \\ 1 & 0 & 2-\lambda \end{vmatrix} \\ &= (2-\lambda)(1-\lambda)^2 - a - a(1-\lambda) + (2-\lambda)a \\ &= (2-\lambda)(1-\lambda)^2 \\ &= (2-\lambda)(1-\lambda)^2. \end{aligned}$$

So the eigenvalues are $\lambda_1 = 1$ and $\lambda_2 = 2$ with algebraic multiplicities $f_1 = 2$ and $f_2 = 1$, respectively.

The third criterion says that A is diagonalisable if and only if

$$\dim E(\lambda_1) = f_1 = 2$$

and

$$\dim E(\lambda_2) = f_2 = 1.$$

The second condition is automatically satisfied as any eigenspace is non-trivial, so we need to check the dimension of the first.

All eigenvectors associated to $\lambda_1 = 1$ must solve the system

$$(A - \lambda_1 I_3)v = \mathbf{0}.$$

Hence,

$$\begin{pmatrix} 0 & a & a \\ -1 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This gives us the system

$$\begin{cases} ay + az = 0 \\ -x - z = 0 \\ x + z = 0, \end{cases}$$

which simplifies to

$$\begin{cases} a(y + z) = 0 \\ x + z = 0 \end{cases}.$$

There are two possibilities: either $a = 0$ and y and z are free variables, or $a \neq 0$ and then $y = -z$. In any case $x = -z$.

Let's look at these two cases separately. If $a \neq 0$, then all vectors of the eigenspace are of the form

$$\begin{pmatrix} -z \\ -z \\ z \end{pmatrix} = z \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix},$$

where $z \neq 0$. Hence the eigenspace would have a basis $\{\begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}\}$ and thus a dimension of 1 which is different from the algebraic multiplicity. Hence this case cannot occur.

So we must have $a = 0$, then all eigenvectors are of the form

$$\begin{pmatrix} -z \\ y \\ z \end{pmatrix} = y \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}.$$

So a basis for the eigenspace is $\{\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}\}$, which gives us dimension 2 as required. Hence A is diagonalisable if and only if $a = 0$.

Let's find the eigenspace for $\lambda_2 = 2$ in order to diagonalise A. We need to solve

$$(A - \lambda_2 I_3)v = \mathbf{0}.$$

This gives

$$\begin{pmatrix} -1 & 0 & 0 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

So,

$$\begin{cases} -x = 0 \\ -x - y - z = 0 \\ x = 0 \end{cases}$$

becomes

$$\begin{cases} x = 0 \\ y = -z \end{cases}.$$

So $\begin{pmatrix} 0 \\ -z \\ z \end{pmatrix} = z \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$ is the general eigenvector for λ_2. Then,

$$E(2) = \{\alpha \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \alpha \in \mathbb{R}\}.$$

Thus $\dim E(2) = 1$.

Hence, by the previous theorem the diagonalisation is done with

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

where we have the eigenvalues on the diagonal, and the corresponding matrix of eigenvectors is

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

Notice that the order of eigenvalues on the diagonal doesn't matter: it simply permutes the order of columns of U. So hence,

$$A = UDU^{-1}.$$

You can also compute U^{-1} to be

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