APSC 174
Lecture Notes

Abdol-Reza Mansouri

Department of Mathematics and Statistics
Queen's University

About These Notes

Dear APSC-174 student,

These notes are meant to be detailed and expanded versions of the classroom lectures you will be attending. Each section in these lecture notes will be covered in one or (often) more classroom lectures.

These lecture notes will be slightly and gradually updated and completed as the classroom lectures progress. Some parts of the lecture notes may even be updated and slightly modified after the corresponding classroom lectures have been delivered. It is therefore recommended that you always refer to the latest version of these lecture notes, which will be posted on the course website.

It is strongly recommended that you read these lecture notes carefully as a complement to the classroom lectures. Almost every section in these notes contains examples which have been worked out in detail. It is strongly recommended that you examine those in detail, and it is equally strongly recommended that you work out in detail the examples that have been left to the reader. Last but not least, it is strongly recommended that you attempt to solve the problems at the end of each section.

I hope you will find these notes useful, and I would appreciate your feedback. So please feel free to e-mail me at `mansouri@queensu.ca` . I look forward to hearing from you.

Abdol-Reza Mansouri
January 2018

Contents

Section 0

Study Topics

- A Review of Basic Notions

In this section, we shall review some of the basic mathematical notions that we will be using throughout the course.

Sets

One of the basic notions that we shall deal with throughout the course is that of **set**. By a set we mean nothing other than a collection of objects; these objects are then called the **elements** or **points** of the set. Some simple examples of sets are:

- the set of all integers greater than or equal to 0 and less than or equal to 5,
- the set of all letters in the Greek alphabet,
- the set of all words in a given book,
- the set of all common words in the English language,
- the set of all common words in the French language,
- the set of all integers greater than or equal to 0 (denoted by $\mathbb{N}$),
- the set of all integers (denoted by $\mathbb{Z}$),
- the set of all real numbers greater than or equal to 0 and less than or equal to 1,
- the set of all real numbers (denoted by $\mathbb{R}$),
- the set of all complex numbers (denoted by $\mathbb{C}$),
- ...

Note that in the list of examples given above, the first 5 sets in the list have a finite number of elements; the last 5, on the other hand, have infinitely many elements.

Let us now denote the first set in the list above by the capital letter A. By definition of the set A, the elements (or points) of A are all the integers greater than or equal to 0, and less than or equal to 5. We can therefore write the set A explicitely as:

$$A = \{0, 1, 2, 3, 4, 5\}.$$

The curly brace "{" to the left indicates the beginning of the set, and the curly brace "}" to the right indicates its end. The symbols enclosed by the curly braces and separated by commas "," are the elements of the set (namely the integers $0, 1, 2, 3, 4$ and 5).

As far as a set goes, the order in which its elements are written is of no consequence; hence, we can equivalently write the set A as:

$$A = \{2, 5, 0, 4, 3, 1\}$$

or as

$$A = \{0, 5, 2, 1, 3, 4\}$$

or any other permutation of the elements. On the other hand, when writing down the elements of the set, we shall not allow any repetition of any element; for example, we shall **never** write A as $\{0, 0, 1, 2, 3, 4, 5\}$ or as $\{0, 1, 2, 3, 4, 5, 4\}$, or in any other such manner: Each element of the set must appear only once.

Let now S be any set; if some entity, say x, is an element of the set S, then we write

$$x \in S$$

to denote this membership property. If x is not an element of S, then we write

$$x \notin S$$

to denote this. For example, for our set A above, we can write $0 \in A$, since the integer 0 is an element of A. On the other hand, the integer 8 is not an element of A, and therefore we write $8 \notin A$. Similarly, the integer 5 is an element of the set $\mathbb{N}$, and we can therefore write $5 \in \mathbb{N}$. On the other hand, the real number $\sqrt{2}$ is not an element of $\mathbb{N}$, and we write $\sqrt{2} \notin \mathbb{N}$.

There is a set containing no elements; it is called the **empty set**, and it is denoted by the symbol $\emptyset$ (it is also often denoted by $\{\}$).

Now that we have defined what we mean by a set and what we mean by an element of a set, we can define what we mean by two sets being equal:

Definition 1. Let A and B be two sets. A is said to be **equal to** B if A and B have exactly the same elements. We write this as $A = B$.

In other words, we have $A = B$ if and only if the following two conditions are met:

(i) Every element of A is also an element of B, and

(ii) every element of B is also an element of A.

For example, defining the set E as $E = \{0, 1, 2, 3\}$ and the set F as $F = \{2, 1, 3, 0\}$, we can write

$$E = F$$

since E and F have exactly the same elements, and hence, by our definition, are equal (recall again that, for a set, the order in which its elements are listed is of no importance). On the other hand, defining the set G as $G = \{3, 0, 2, 7, 1\}$, we can write

$$E \neq G,$$

since E and G do not have exactly the same elements; in particular, we can see that $7 \in G$ whereas $7 \notin E$, and this shows that the elements of E and G are not exactly the same.

Writing down the elements of a set explicitly is sometimes plainly impossible. Let B for example be the set of all integers greater than or equal to 5. How shall we describe B ? Certainly not by listing all its elements! Recalling that $\mathbb{N}$ denotes the set of all integers greater than or equal to 0, we can write:

$$B = \{x \in \mathbb{N} \ : \ x \geq 5\}.$$

The expression to the right of the equality sign should be read as "the set of all elements x in $\mathbb{N}$ such that $x \geq 5$"; in that expression, the colon ":" is to be read as "such that". It is worth noting that in some texts the vertical bar "|" is used in place of the colon ":", and hence the set B could also be written as

$$B = \{x \in \mathbb{N} \mid x \geq 5\},$$

with the vertical bar "|" to be read as "such that" just like we did with the semicolon. These are some of the standard ways of defining sets. Note that this way of defining sets is not restricted only to sets having infinitely many elements; for example, defining the set A as:

$$A = \{5, 2, 3, 4, 6\},$$

we could also write A as

$$A = \{x \in \mathbb{N} \ : \ x \geq 2 \text{ and } x \leq 6\};$$

indeed, it is immediate to verify that we have the equality of sets

$$\{5, 2, 3, 4, 6\} = \{x \in \mathbb{N} \ : \ x \geq 2 \text{ and } x \leq 6\},$$

since every element of the set to the left is also an element of the set to the right, and vice-versa. Similarly, we also have the equalities

$$A = \{x \in \mathbb{N} \ : \ x > 1 \text{ and } x < 7\},$$

and

$$A = \{x \in \mathbb{N} \ : \ x > 1 \text{ and } x \leq 6\},$$

and so on. These are all equivalent ways of defining the set A.

As another example, consider the set $[0,1]$ consisting of all real numbers greater than or equal to 0 and less than or equal to 1. We can write:

$$[0,1] = \{x \in \mathbb{R} \ : \ x \geq 0 \text{ and } x \leq 1\}.$$

We now define relations and operations between sets.

Definition 2. Let A and B be two sets. A is said to be a **subset** of B if every element of A is also an element of B; we write this as $A \subset B$.

For example, every element of $\mathbb{N}$ is also and element of $\mathbb{R}$, i.e. $\mathbb{N}$ is a subset of $\mathbb{R}$, and we can therefore write

$$\mathbb{N} \subset \mathbb{R},$$

On the other hand, it is not true that every element of $\mathbb{R}$ is also an element of $\mathbb{N}$, and hence $\mathbb{R}$ is not a subset of $\mathbb{N}$.
Using the "subset" relation, we can therefore state that two sets A and B are equal if and only if we have both $A \subset B$ and $B \subset A$; we can write this more formally as:

$$A = B \ \Leftrightarrow \ A \subset B \text{ and } B \subset A.$$

In the expression above, the symbol $\Leftrightarrow$ should be read as "if and only if" or "is equivalent to".

Given two sets S and T, we can construct a new set from them as follows:

Definition 3. Let S and T be sets. We denote by $S \cap T$ the set of all elements which are **both** in S **and** in T. We call $S \cap T$ the **intersection** of the sets S and T.

For example, if $A = \{0,1,2,3\}$, $B = \{2,3,4,5\}$, and $C = \{5,6,7\}$, then we can write:

$$\begin{aligned} A \cap B &= \{2,3\}, \\ B \cap C &= \{5\}, \\ A \cap C &= \emptyset. \end{aligned}$$

The following properties of set intersection are easy to verify (and strongly recommended to the reader):

Lemma 1. Let S, T, U be sets. We have:

$$\begin{aligned} S \cap T &= T \cap S, \\ S \cap (T \cap U) &= (S \cap T) \cap U. \end{aligned}$$

Given two sets S and T, we can construct a new set from them in yet another way:

Definition 4. Let S and T be sets. We denote by $S \cup T$ the set of all elements which are in either S or T or both. We call $S \cup T$ the **union** of the sets S and T.

For example, for the sets A, B, C defined just above, we have:

$$\begin{aligned} A \cup B &= \{0,1,2,3,4,5\}, \\ B \cup C &= \{2,3,4,5,6,7\}, \\ A \cup C &= \{0,1,2,3,5,6,7\}. \end{aligned}$$

The following properties of set union are easy to verify (and their verification is again strongly recommended to the reader):

Lemma 2. Let S, T, U be sets. We have:

$$\begin{aligned} S \cup T &= T \cup S, \\ S \cup (T \cup U) &= (S \cup T) \cup U. \end{aligned}$$

We shall construct new sets in yet another way:

Definition 5. Let S and T be sets. We denote by $S \setminus T$ the set of all elements of S which are not in T. We call $S \setminus T$ the **set difference** of the sets S and T (in that order).

For example, for the same sets A, B, C defined just above by $A = \{0,1,2,3\}$, $B = \{2,3,4,5\}$, and $C = \{5,6,7\}$, we have:

$$\begin{aligned} A \setminus B &= \{0,1\}, \\ B \setminus A &= \{4,5\}, \\ A \setminus C &= A, \\ C \setminus A &= C, \\ B \setminus C &= \{2,3,4\}, \\ C \setminus B &= \{6,7\}. \end{aligned}$$

It is easy to verify that for any set S, we have $S \setminus S = \emptyset$.
The following properties of set difference are again easy to verify (and their verification is again strongly recommended to the reader):

Lemma 3. Let S, T, U be sets. We have:

$$\begin{aligned} S \setminus (T \cap U) &= (S \setminus T) \cup (S \setminus U), \\ S \setminus (T \cup U) &= (S \setminus T) \cap (S \setminus U). \end{aligned}$$

We shall construct new sets in yet another way:

Definition 6. Let S and T be sets. We denote by $S \times T$ the set of all **pairs** of the form (s, t) where $s \in S$ and $t \in T$. We call $S \times T$ the **Cartesian product** of the sets S and T.

NOTE: It is important to recall that a pair (s, t) is an **ordered list** consisting (in that order) of s and t; in a pair of elements, order does matter. As a result, two pairs (a, b) and (c, d) are considered equal if and only if we have both $a = c$ and $b = d$. Hence, the pair (a, b) is not equal to the pair (b, a), unless we have $a = b$; if $a \neq b$, then the pairs (a, b) and (b, a) denote distinct pairs and are not equal. Hence, a pair of elements is **very different** from a set of elements, since, as we saw, in a set, order does not matter. So if $a \neq b$, the sets $\{a, b\}$ and $\{b, a\}$ will denote **identical sets**, whereas the pairs (a, b) and (b, a) will denote **distinct pairs**. One other key difference is that in a pair of elements, the two elements are allowed to be identical (i.e. repetitions are allowed), whereas this is not the case for a set. So, the pair of integers $(1, 1)$ is a valid pair, whereas the set $\{1, 1\}$ is not correctly written (since the element 1 is repeated) and should be instead written as $\{1\}$.

Let us consider some examples. If E and F are sets defined by $E = \{0, 1, 2\}$ and $F = \{4, 5\}$, then we have the following Cartesian products:

$$\begin{aligned}
E \times E &= \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}, \\
E \times F &= \{(0,4),(0,5),(1,4),(1,5),(2,4),(2,5)\}, \\
F \times E &= \{(4,0),(5,0),(4,1),(5,1),(4,2),(5,2)\}, \\
F \times F &= \{(4,4),(4,5),(5,4),(5,5)\}.
\end{aligned}$$

Note that if S and T are two sets, the set $S \times T$ is in general distinct from the set $T \times S$ (as you can see on the previous example). Note also that if either S or T is the empty set then $S \times T$ will also be the empty set.

We can use the Cartesian product operation to construct yet more sets from a given set S as follows: We can construct not just $S \times S$ (as we did above), but also $(S \times S) \times S$, and $((S \times S) \times S) \times S$, and ... We shall write these last ones simply as $S \times S \times S$, and $S \times S \times S \times S$, and ... (i.e. by removing the parentheses). So, just as we had $S \times S$ be the set of all pairs (s_1, s_2) with s_1 and s_2 elements of S, we will have:

- $S \times S \times S$ = set of all **triples** (s_1, s_2, s_3) with s_1, s_2, s_3 elements of S,
- $S \times S \times S \times S$ = set of all **quadruples** (s_1, s_2, s_3, s_4) with s_1, s_2, s_3, s_4 elements of S,
- $\cdots$
- $S \times S \times \cdots \times S$ (n times) is the set of all **n-tuples** $(s_1, s_2, \cdots, s_n)$ with $s_1, s_2, \cdots, s_n$ elements of S.

We shall denote the $n-$fold Cartesian product $S \times S \times \cdots \times S$ of S with itself by S^n, with the convention that $S^1 = S$. Generalizing what we saw for pairs, two $n-$tuples $(a_1, \cdots, a_n)$ and $(b_1, \cdots, b_n)$ in S^n are said to be equal if and only if we have $a_1 = b_1$, $a_2 = b_2$, $\cdots$, $a_n = b_n$.

We shall very soon encounter the following sets:

- $\mathbb{R}^2$, the set of all **pairs** of real numbers, i.e. the set of all pairs of the form (a, b) where $a, b \in \mathbb{R}$ (shorthand for "a and b are both elements of $\mathbb{R}$"),
- $\mathbb{R}^3$, the set of all **triples** of real numbers, i.e. the set of all triples of the form (a, b, c) where $a, b, c \in \mathbb{R}$,
- and more generally, $\mathbb{R}^n$, the set of all **n-tuples** of real numbers, i.e. the set of all $n-$tuples of the form $(a_1, a_2, \cdots, a_n)$ with $a_1, a_2, \cdots, a_n \in \mathbb{R}$.

Quantifiers

Let S be a set, and suppose **all** elements of S satisfy some property. We want to express this fact formally. To make this more concrete, consider the set $\mathbb{N}$ of all integers greater than or equal to 0; it is clear that every element x of $\mathbb{N}$ is such that $x + 1$ is also an element of $\mathbb{N}$. We can write this statement formally (and succintly) as:

$$\forall x \in \mathbb{N} : x + 1 \in \mathbb{N}.$$

The symbol $\forall$ in the expression above is to be read as "for any", or, equivalently, as "for all". The symbol $\forall$ is called the **universal quantifier**. The colon symbol ":" in the above expression should be read as "we have" or "the following holds".

Using the universal quantifier, many otherwise length statements can be written formally in a very succint way. For example, if S, T are two sets, we know that $S \subset T$ if and only if every element of S is also an element of T. We can write this formally as:

$$S \subset T \;\Leftrightarrow\; \forall x \in S : x \in T$$

where again the symbol of equivalence $\Leftrightarrow$ is meant to be read as "if and only if" or "is equivalent to".

Let now S be a set, and suppose there is **at least one** element in S which satisfies some property. We want to express this fact formally. Again, to make this more concrete, consider the set $\mathbb{N}$ of all integers greater than or equal to 0; it is clear that there are elements in $\mathbb{N}$ (namely all multiples of 2) which, after division by 2, yield again an integer in $\mathbb{N}$. Clearly, this is not true of all elements in $\mathbb{N}$ (consider any odd integer). We can write the statement "there exists at least one element in ℕ such that dividing it by 2 yields again an element of ℕ" as:

$$\exists x \in \mathbb{N} : \frac{x}{2} \in \mathbb{N}.$$

In the above expression, the symbol ∃ should be read as "there exists", and is called the **existential quantifier**. The colon symbol ":" in the above expression should be read as "such that".

Using the existential quantifier also allows writing expressions formally and succintly. For example, if S, T are two sets, then we know their intersection $S \cap T$ is non-empty if and only if (by definition of intersection), there is an element in S which is also an element in T. We can write this formally as:

$$S \cap T \neq \emptyset \;\Leftrightarrow\; \exists x \in S : x \in T$$

Mappings and Functions

The following definition is **fundamental**:

Definition 7. Let S and T be two sets. A **mapping** (also called **function**) **from** S **to** T is a **rule** which assigns **to each element** of S **one and only one element** of T.

To indicate that f is a function from S to T, we shall write:

$$\begin{aligned} f : S &\rightarrow T \\ x &\mapsto f(x) \end{aligned}$$

The above expression should be read as: "f is a mapping from the set S to the set T which assigns to every element x of S the element $f(x)$ of T".
In the expression above, S is called the **domain set** of the function f, T is called the **target set** of f. Each function is uniquely defined by specifying its domain set, its target set, and the rule by which it associates to each element of the domain set a unique element of the target set.

Let us immediately consider some examples:

1. The mapping

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{N} \\ x &\mapsto x^2 \end{aligned}$$

is the mapping with domain set $\mathbb{Z}$ and target set $\mathbb{N}$, defined by assigning to each integer x its squared value x^2.

2. The mapping

$$\begin{aligned} f:\mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sin(x) \end{aligned}$$

is the mapping with domain set and target set both equal to $\mathbb{R}$, defined by assigning to each real number x its sine $\sin(x)$.

3. The mapping

$$\begin{aligned} f:\mathbb{N}\times\mathbb{N} &\to \mathbb{R} \\ (x,y) &\mapsto \frac{x}{y^2+1} \end{aligned}$$

is the mapping with domain set the Cartesian product $\mathbb{N}\times\mathbb{N}$ (i.e. $\mathbb{N}^2$) and target set $\mathbb{R}$ which assigns to every pair (x,y) of integers the real number $\frac{x}{y^2+1}$.

4. The mapping

$$\begin{aligned} f \ : \ \mathbb{R}^3 &\to \mathbb{R}^2 \\ (x,y,z) &\mapsto (x+y, x-z) \end{aligned}$$

is the mapping with domain set $\mathbb{R}^3$ and target set $\mathbb{R}^2$ which assigns to every triple (x,y,z) of real numbers the pair $(x+y,x-z)$ of real numbers.

It is important to note that given two sets S and T, not every rule of assignement from S to T defines a function; the rule of assignment will define a function from S to T if to **every** element of S it associates a **unique** element of T. To make this clear, consider the set $\mathbb{N}$ for both the domain set and the target set. Suppose to each element x of $\mathbb{N}$ we assign an element y of $\mathbb{N}$ if x is a multiple of y (i.e. if y divides x). For example, we would assign to the element 2 of $\mathbb{N}$ both the element 1 of $\mathbb{N}$ (since 2 is a multiple of 1) and the element 2 of $\mathbb{N}$ (since 2 is a multiple of 2), and so on. Does this rule of assignment define a function from $\mathbb{N}$ to $\mathbb{N}$? NO! For the simple reason that some elements of the domain set (for example 2) are assigned to more than one element of the target set.
Consider now the rule of assignment defined by assigning to every element x of $\mathbb{N}$ the element y of $\mathbb{N}$ if the relation $y = x - 5$ is satisfied. Does this rule of assignment define a function from $\mathbb{N}$ to $\mathbb{N}$? NO! For the simple reason that some elements of the domain set (namely the integers $0,1,2,3,4$ are not assigned to any element at all of the target set.

It is important to point out that a mapping is defined by the data consisting of its domain set, its target set, and the law by which each element of the domain set is assigned a unique element of the target set. As a result, the two mappings f and g defined by

$$\begin{aligned} f:\mathbb{N} &\to \mathbb{N} \\ x &\mapsto x^3 \end{aligned}$$

and

$$\begin{aligned} g : \mathbb{N} &\to \mathbb{R} \\ x &\mapsto x^3 \end{aligned}$$

are considered to be **distinct mappings** (even though they both map each integer to its cube) since they do not have the same target set in their definition. In what follows, we shall assume that all the domain sets and target sets involved in the discussion are non-empty (since there would be not much to say if they were!).

It is important to a given mapping $f : S \to T$ from some set S to some set T is an entity in its own right; we can therefore talk about the set of all mappings from S to T. A given mapping from S to T will therefore be some element of that set.

Let now S, T be sets, and let $f : S \to T$ be a mapping from S to T. It may happen that distinct elements get mapped under f to distinct elements of T. This case is important enough to warrant a definition.

Definition 8. Let $f : S \to T$ be a mapping from S to T. f is said to be **injective** (or **one-to-one**) if $\forall x, y \in S$: $x \neq y \Rightarrow f(x) \neq f(y)$.

Equivalently, $f : S \to T$ is injective if $\forall x, y \in S : f(x) = f(y) \Rightarrow x = y$.

For example, the mapping

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3 \end{aligned}$$

is injective, whereas the mapping

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

is not.

If $f : S \to T$ is some mapping, it may also happen that each element of T is mapped to under f by some element of S (i.e. no element of T is left out). This case is also important enough to warrant a definition.

Definition 9. Let $f : S \to T$ be a mapping from S to T. f is said to be **surjective** (or **onto**) if $\forall x \in T$, $\exists y \in S : x = f(y)$, i.e. every element of T is the image under f of some element of S.

For example, the mapping

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto x + 1 \end{aligned}$$

is surjective, whereas the mapping

$$\begin{array}{rcl} g : \mathbb{N} & \to & \mathbb{N} \\ x & \mapsto & x+1 \end{array}$$

is not.

Let now S, T, U be three sets, and let $f : S \to T$ and $g : T \to U$ be two mappings. We can construct a new mapping from f and g as follows:

Definition 10. Let $f : S \to T$ and $g : T \to U$ be mappings. We define the **composition** $g \circ f$ of g and f to be the mapping with domain set S and target set U, and which assigns to every element x of S the element $g(f(x))$ of U.

In other words, the mapping $g \circ f$ is defined as:

$$\begin{array}{rcl} g \circ f : S & \to & U \\ x & \mapsto & g(f(x)) \end{array}$$

It is clear why $g \circ f$ is called the composition of g and f: an element x of S is first mapped to the element $f(x)$ of T, and g then maps the element $f(x)$ of T to the element $g(f(x))$ of U.
It is important to note from this definition that one cannot always compose any two arbitrary functions f and g; for the composition $g \circ f$ to make sense, the target set of f has to be equal to the domain set of g.

Let now S be any set; we denote by id_S the mapping

$$\begin{array}{rcl} id_S : S & \to & S \\ x & \mapsto & x \end{array}$$

i.e., the mapping which assigns to each element of S itself. id_S is called the **identity mapping** of S for the obvious reason that it maps each element of S to itself. It is easy to verify that for any set S, the identity mapping id_S of S is both injective and surjective.

Let now S, T be two sets, and let $f : S \to T$ be a mapping. The composition $f \circ id_S$ is defined, since the target set of id_S (namely S) is equal to the domain set of f, and the domain and target set of $f \circ id_S$ are exactly those of f. Furthermore, $\forall x \in S$:

$$f \circ id_S(x) = f(id_S(x)) = f(x),$$

and hence $f \circ id_S = f$, i.e. the two mappings $f \circ id_S$ and f are one and the same, since they have identical domain and target sets, and since they have the same exact rule of assignement. It is possible to verify in the same exact manner that the composition $id_T \circ f$ is defined, and that $id_T \circ f = f$.

Let now $f : S \to T$ be a mapping from S to T; an important special case happens when each element of the target set T is mapped to under f by exactly one element of the domain set S; clearly this implies that f is both injective and surjective. This case is also important enough to warrant a definition.

Definition 11. Let $f : S \to T$ be a mapping from S to T. f is said to be **bijective** if $\forall x \in T$, there exists one and only one element $y \in S$ such that $x = f(y)$.

Let now $f : S \to T$ be a mapping from S to T and assume f is **bijective**. The fact that f is bijective now allows us to define a mapping $g : T \to S$ (note that g has domain set T and target set S, i.e. the exact opposite of f) as follows: For each $x \in T$, we know there is exactly one element $y \in S$ which satisfies $f(y) = x$; we define $g(x)$ to be precisely that element y of S. In other words (and don't forget again that f is assumed bijective), for each $x \in T$ we define by $g(x)$ that unique element of S which satisfies $f(g(x)) = x$. It is easy to verify that, with this definition, g is a mapping from T to S, and that, furthermore, g itself is bijective. Note that the compositions $f \circ g : T \to T$ and $g \circ f : S \to S$ are both defined, and that $\forall x \in S$: $g \circ f(x) = x$, and $\forall x \in T$: $f \circ g(x) = x$. This shows that $f \circ g = id_T$ and $g \circ f = id_S$. For this reason, g is called the **inverse mapping** of f and is denoted by f^{-1} (not to be confused with "one over ..."!). Once again, the inverse mapping f^{-1} of f exists **only and only when f is bijective**.

Complex Numbers

We will be dealing with complex numbers only at the very end of this course (when eigenvalues and eigenvectors begin to appear), and since it is assumed here that you have learned or soon will learn complex numbers in different settings, we keep the treatment of complex numbers to the bare minimum. Formally, a complex number can be considered as a pair of real numbers, i.e. an element of $\mathbb{R}^2$, with addition of pairs and multiplication of pairs defined as follows:

$$\begin{aligned} \forall (a,b),(c,d) \in \mathbb{R}^2 &\quad : \quad (a,b)+(c,d) = (a+c, b+d), \\ \forall (a,b),(c,d) \in \mathbb{R}^2 &\quad : \quad (a,b)\times(c,d) = (ac-bd, ad+bc). \end{aligned}$$

It can be verified that two operations satisfy the usual properties of addition and multiplication that are satisfied for real numbers. The set of all complex numbers is denoted by $\mathbb{C}$.
Informally, you can think of a complex number as a number of the form $a + ib$, where a and b are real numbers, and where the symbol i satisfies $i^2 = -1$ (i.e. i is the square root of -1). Adding and multiplying complex numbers then proceeds just as with real numbers, with the proviso that $i^2 = -1$.

For example, adding the complex numbers $a+ib$ and $c+id$ (where again a, b, c, d are real numbers) yields (using the same grouping rules as for real numbers)

$$(a+ib)+(c+id) = (a+c)+i(b+d),$$

and multiplying them yields (using again the same grouping rules as for real numbers)

$$\begin{aligned}(a+ib)(c+id) &= a(c+id)+ib(c+id) = ac+a(id)+ibc+ib(id)\\ &= ac+iad+ibc+i^2bd = ac+iad+ibc-bd\\ &= (ac-bd)+i(ad+bc),\end{aligned}$$

where, in the second to last step, we have replaced i^2 by -1, as stipulated. As an exercise, try to relate the expressions obtained here to the ones above with the addition and multiplication of pairs!

For the complex number $z = a+ib$, where $a, b \in \mathbb{R}$, the real number a is called the **real part** of z, whereas the real number b is called the **imaginary part** of z. Note that the complex number i can be written as

$$i = 0 + i1,$$

which shows that i has real part 0 and imaginary part 1. On the other hand, if $a \in \mathbb{R}$ is any real number, we can write a as

$$a = a + i0,$$

which shows that the real number a has real part a (i.e. is equal to its own real part) and has imaginary part 0.

As a very simple example of manipulation of real numbers, we all know that for $a, b \in R$, we have the factorization:

$$a^2 - b^2 = (a-b)(a+b).$$

Using complex numbers, we can now factorize a^2+b^2 as follows:

$$a^2 + b^2 = (a-ib)(a+ib).$$

Assume now that we wish to find a complex number z which satisfies $z^2+1=0$. Since

$$z^2+1 = (z+i1)(z-i1) = (z+i)(z-i),$$

there are only two complex numbers which satisfy the equation $z^2+1=0$, namely the complex numbers i and $-i$. Similarly, if we wish to find a complex number z which satisfies $z^2+2=0$, we can write

$$z^2+2 = (z+i\sqrt{2})(z-i\sqrt{2}),$$

and hence the roots of the equation $z^2 + 2 = 0$ are given by $i\sqrt{2}$ and $-i\sqrt{2}$.

Let now $a, b \in R$, and consider the complex number $z = a + ib$. The **complex conjugate** of z is the complex number denoted by $\bar{z}$ and defined by $\bar{z} = a - ib$. Note that we have:

$$z\bar{z} = (a + ib)(a - ib) = a^2 + b^2.$$

Using the complex conjugate $\bar{z}$ of z, we can easily compute $\frac{1}{z}$ for $z \neq 0$. Note first that with $z = a + ib$ (with $a, b \in \mathbb{R}$), having $z \neq 0$ is equivalent to having $a = b = 0$, and hence $z \neq 0$ is equivalent to having a, b not both equal to 0. Let then $z = a + ib$ (again, with $a, b \in \mathbb{R}$) with $z \neq 0$. We can write:

$$\frac{1}{a + ib} = \frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2},$$

which shows that $\frac{1}{a+ib}$ has real part $\frac{a}{a^2+b^2}$ and imaginary part $-\frac{b}{a^2+b^2}$ (don't forget the minus sign!).

As an example, we can easily compute $\frac{1}{i}$, and we obtain:

$$\frac{1}{i} = \frac{1}{0 + i1} = -i,$$

whereas $\frac{1}{1+i}$ yields

$$\frac{1}{1 + i} = \frac{1}{1 + i1} = \frac{1}{2} - i\frac{1}{2}.$$

PROBLEMS:

1. (a) Let $A = \{0, 1, 2\}$, $B = \{2, 3, 4\}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (b) Let $A = \emptyset$, $B = \{1, 2\}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (c) Let $A = \{0, 1, 2\}$, $B = \emptyset$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (d) Let $A = \{0, 1, 2\}$, $B = \mathbb{N}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (e) Let $A = \{0, 1, 2\}$, $B = \mathbb{R}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (f) Let $A = \mathbb{N}$, $B = \mathbb{R}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (g) Let $A = \mathbb{N}$, $B = \mathbb{Z}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
   (h) Let $A = \mathbb{Z}$, $B = \mathbb{R}$. Compute $A \cap B$, $A \cup B$, $A \times B$, $B \times A$.
2. (a) Let A, B be sets; show that $A \cup B = B \cup A$.
   (b) Let A, B be sets; show that $A \cap B = B \cap A$.

(c) Let A, B be sets; show that $A \subset A \cup B$.

(d) Let A, B be sets; show that $A \cap B \subset A$.

(e) Let A, B, C be sets; show that $(A \cap B) \cap C = A \cap (B \cap C)$.

(f) Let A, B, C be sets; show that $(A \cup B) \cup C = A \cup (B \cup C)$.

(g) Let A, B, C be sets; show that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

(h) Let A, B, C be sets; show that $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

(i) Let A, B be sets; show that $A \subset B \ \Rightarrow A \cap B = A$.

(j) Let A, B be sets; show that $A \subset B \ \Rightarrow A \cup B = B$.

(k) Let A, B be sets; show that $A \cap B = A \cup B \ \Rightarrow A = B$.

3. For each of the cases below, determine whether the given rule of assignment defines a valid function with domain set and target set both equal to $\mathbb{N}$; in case it does, determine whether the function is injective, surjective, bijective.

   (a) To each $x \in \mathbb{N}$, we assign x.

   (b) To each $x \in \mathbb{N}$, we assign x^2.

   (c) To each $x \in \mathbb{N}$, we assign $x - 1$.

   (d) To each $x \in \mathbb{N}$, we assign x^3.

   (e) To each $x \in \mathbb{N}$, we assign $\frac{x}{3}$.

   (f) To each $x \in \mathbb{N}$, we assign $\sqrt{x}$.

   (g) To each $x \in \mathbb{N}$, we assign $\sin(x)$.

4. For each of the cases below, determine whether the given rule of assignment defines a valid function with domain set and target set both equal to $\mathbb{Z}$; in case it does, determine whether the function is injective, surjective, bijective.

   (a) To each $x \in \mathbb{Z}$, we assign x.

   (b) To each $x \in \mathbb{Z}$, we assign x^4.

   (c) To each $x \in \mathbb{Z}$, we assign $x - 1$.

   (d) To each $x \in \mathbb{Z}$, we assign x^5.

   (e) To each $x \in \mathbb{Z}$, we assign $\frac{x}{5}$.

   (f) To each $x \in \mathbb{Z}$, we assign $\sqrt{x+1}$.

   (g) To each $x \in \mathbb{Z}$, we assign $\cos(x)$.

5. For each of the cases below, determine whether the given rule of assignment defines a valid function with domain set equal to $\mathbb{N}^2$ and target set $\mathbb{N}$; in case it does, determine whether the function is injective, surjective, bijective.

   (a) To each pair $(x, y) \in \mathbb{N}^2$, we assign $x + y$.

(b) To each pair $(x, y) \in \mathbb{N}^2$, we assign $x - y$.

(c) To each pair $(x, y) \in \mathbb{N}^2$, we assign xy.

(d) To each pair $(x, y) \in \mathbb{N}^2$, we assign $\frac{x}{y}$.

(e) To each pair $(x, y) \in \mathbb{N}^2$, we assign $\frac{x}{y+1}$.

(f) To each pair $(x, y) \in \mathbb{N}^2$, we assign $\frac{x}{y^2+1}$.

6. For each of the cases below, determine whether the given rule of assignment defines a valid function with domain set equal to $\mathbb{N}^2$ and target set $\mathbb{R}$; in case it does, determine whether the function is injective, surjective, bijective.

   (a) To each pair $(x, y) \in \mathbb{N}^2$, we assign $x + y$.

   (b) To each pair $(x, y) \in \mathbb{N}^2$, we assign $x - y$.

   (c) To each pair $(x, y) \in \mathbb{N}^2$, we assign $-xy$.

   (d) To each pair $(x, y) \in \mathbb{N}^2$, we assign $\frac{x}{y}$.

   (e) To each pair $(x, y) \in \mathbb{N}^2$, we assign $\frac{x}{y+1}$.

   (f) To each pair $(x, y) \in \mathbb{N}^2$, we assign $\frac{x}{y^2+1}$.

7. For each of the following cases, determine whether the compositions $f \circ f$, $f \circ g$, $g \circ f$, and $g \circ g$ are defined; if so, explicit them.

   (a)

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto x + 1 \end{aligned}$$

   and

$$\begin{aligned} g : \mathbb{Z} &\to \mathbb{R} \\ x &\mapsto \frac{x^2 - 1}{x^2 + 1} \end{aligned}$$

   (b)

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto x^2 \end{aligned}$$

   and

$$\begin{aligned} g : \mathbb{N} &\to \mathbb{R} \\ x &\mapsto \frac{1}{x + 1} \end{aligned}$$

(c)

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

and

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \frac{1}{x^2+1} \end{aligned}$$

(d)

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{Z} \\ x &\mapsto x^2 \end{aligned}$$

and

$$\begin{aligned} g : \mathbb{Z} &\to \mathbb{N} \\ x &\mapsto x^3 \end{aligned}$$

(e)

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \frac{1}{x^2+4} \end{aligned}$$

and

$$\begin{aligned} g : \mathbb{Z} &\to \mathbb{R} \\ x &\mapsto \frac{1}{x^2+2} \end{aligned}$$

Section 1

Study Topics

- Systems of Linear Equations
- Number of Solutions to Systems of Linear Equations

Systems of Linear Equations

Linear algebra is ubiquitous in engineering, mathematics, physics, and economics. Indeed, many problems in those fields can be expressed as problems in linear algebra and solved accordingly. An important example of application of linear algebra which we will use as an illustration throughout these lectures, and as a motivation for the theory, is the problem of solving a system of linear equations. Systems of linear equations appear in all problems of engineering; for example, the problem of computing loop currents or node voltages in a passive electric circuit, as well as computing forces and torques in a mechanical system lead to systems of linear equations.

By a **system of linear equations** (with real coefficients), we mean a set of equations of the form:

$$(E)\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + \cdots a_{3n}x_n = b_3 \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots a_{mn}x_n = b_m \end{cases}$$

where the real numbers $a_{11}, a_{12}, \cdots, a_{1n}, a_{21}, a_{22}, \cdots, a_{2n}, \cdots, a_{m1}, a_{m2}, \cdots, a_{mn}$ and $b_1, b_2, \cdots, b_m$ are **given** real numbers, and we wish to solve for the real numbers $x_1, x_2, \cdots, x_n$; equivalently, we wish to solve for the $n-$tuple of real numbers $(x_1, x_2, \cdots, x_n)$. Each $n-$tuple $(x_1, x_2, \cdots, x_n)$ of real numbers satisfying the system (E) is called a **solution** of the system of linear equations (E). In this system, the integer m is called the **number of equations**, whereas the integer n is called the **number of unknowns**. Here are a few examples of systems of linear equations:

(a) Consider the system

$$\begin{cases} 2x = 3, \end{cases}$$

where we wish to solve for the real number x; this is a system of linear equations with one equation (i.e. $m = 1$) and one unknown (i.e. $n = 1$).

(b) Consider now the system

$$\begin{cases} 2x = 3, \\ 3x = 4, \end{cases}$$

where again we wish to solve for the real number x; this is a system of linear equations with two equations (i.e. $m = 2$) and one unknown (i.e. $n = 1$).

(c) Consider now the system

$$\begin{cases} 2x + y = 2, \\ x - y = 3, \end{cases}$$

where we now wish to solve for the real numbers x and y, or, equivalently, for the **pair** of real numbers (x, y); this is a system of linear equations with two equations (i.e. $m = 2$) and two unknowns (i.e. $n = 2$).

(d) Consider now the system

$$\begin{cases} x + y + z = 0, \\ y - z = 3, \end{cases}$$

where we now wish to solve for the real numbers x, y and z, or, equivalently, for the **triple** of real numbers (x, y, z); this is a system of linear equations with two equations (i.e. $m = 2$) and three unknowns (i.e. $n = 3$).

Number of Solutions of Systems of Linear Equations

Now that it is clear what we mean by a system of m linear equations in n unknowns, let us examine some examples. Let us begin with the simplest possible example, that is, a system of linear equations with one equation ($m = 1$) and one unknown ($n = 1$).

To start things off, consider the following system:

$$(A) \left\{ \; 2x = 3, \right.$$

where we wish to solve for the unknown real number x. Multiplying both sides of the equation $2x = 3$ by $\frac{1}{2}$, we obtain the equation:

$$\frac{1}{2}2x = \frac{1}{2}3,$$

which, upon simplification, yields:

$$x = \frac{3}{2}.$$

We conclude that the system of linear equations (A) has a **unique** solution, and it is given by the real number $x = \frac{3}{2}$.

Let us still deal with the simplest case of systems of linear equations with one equation and one unknown (i.e. $m = n = 1$), and consider now the system:

$$(B) \left\{ \; 0x = 0, \right.$$

where we again wish to solve for the real number x. It is clear that **any** real number x satisfies the equation $0x = 0$; we conclude therefore that the system (B) has **infinitely many** solutions.
Still remaining with the simplest case of systems of linear equations with one equation and one unknown (i.e. $m = n = 1$), consider now instead the system:

$$(C) \left\{ \; 0x = 2, \right.$$

where we again wish to solve for the real number x. It is clear that there is **no real number** x that satisfies the equation $0x = 2$; we conclude therefore that the system (C) has **no solution**.
We can recapitulate our findings for the three examples that we considered as follows:

- System (A) has **exactly one** solution.

- System (B) has **infinitely many** solutions.

- System (C) has **no** solution.

Let us now increase the complexity by one notch and examine systems of linear equations with 2 equations and 2 unknowns (i.e. $m = n = 2$). To begin with, let us consider the following system:

$$(A') \begin{cases} x + y = 2, \\ x - y = 1, \end{cases}$$

where we wish to solve for the **pair** (x, y) of real numbers. If the pair (x, y) is a solution of the system (A'), then we obtain from the first equation that $x = 2 - y$ and from the second equation that $x = 1 + y$. Hence, if the pair (x, y) is a solution of the system (A'), then we must have $x = 2 - y$ **and** $x = 1 + y$; this in turn implies that we must have $2 - y = 1 + y$, which then implies that $2y = 1$, from which we obtain that $y = \frac{1}{2}$. From the relation $x = 2 - y$, we then obtain that $x = 2 - \frac{1}{2} = \frac{3}{2}$. Note that we could have also used the relation $x = 1 + y$ instead, and we would still have obtained $x = \frac{3}{2}$. What we have therefore established is that if the pair (x, y) is a solution of the system (A'), then we must have $x = \frac{3}{2}$ and $y = \frac{1}{2}$, i.e., the pair (x, y) must be equal to the pair $(\frac{3}{2}, \frac{1}{2})$; conversely, it is easy to verify, by simply substituting in values, that the pair $(\frac{3}{2}, \frac{1}{2})$ is actually a solution to the system (A'); indeed, we have:

$$\begin{aligned} \frac{3}{2} + \frac{1}{2} &= \frac{4}{2} = 2, \\ \frac{3}{2} - \frac{1}{2} &= \frac{2}{2} = 1, \end{aligned}$$

as expected. We conclude therefore that the system (A') of linear equations has **exactly one** solution, and that this solution is given by the pair $(\frac{3}{2}, \frac{1}{2})$.

Consider now the following system of linear equations, again having 2 equations (i.e. $m = 2$) and 2 unknowns (i.e. $n = 2$):

$$(B') \begin{cases} x + y = 1, \\ 2x + 2y = 2, \end{cases}$$

where again we wish to solve for the **pair** (x, y) of real numbers. Applying the same "method" as previously, we obtain the relation $x = 1 - y$ from the first equation and the relation $2x = 2 - 2y$ from the second equation; multiplying both sides of this last relation by $\frac{1}{2}$ yields, upon simplification $x = 1 - y$. Proceeding as before, we use the two relations obtained, namely $x = 1 - y$ and $x = 1 - y$, obtaining as a result the equation $1 - y = 1 - y$, which then yields

$0y = 0$. Clearly, any real number y satisfies the relation $0y = 0$, and for each such y, the corresponding x is given by $x = 1 - y$. In other words, if the pair (x, y) is a solution of the system (B'), then we must have $x = 1-y$, i.e., we must have $(x, y) = (1 - y, y)$. Conversely, for **any** real number y, the pair $(1 - y, y)$ is a solution of the system (B'), as can be directly verified. Indeed,

$$\begin{aligned} (1-y)+y &= 1, \\ 2(1-y)+2y &= 2-2y+2y=2, \end{aligned}$$

as expected. We conclude from these manipulations that the system (B') of linear equations has **infinitely many** solutions, and they are all of the form $(1 - y, y)$ with y any real number.

Consider now the following system of linear equations, again having 2 equations (i.e. $m = 2$) and 2 unknowns (i.e. $n = 2$):

$$(C') \begin{cases} x+y=1, \\ 2x+2y=0, \end{cases}$$

where again we wish to solve for the **pair** (x, y) of real numbers. Applying the same "method" as previously, we obtain the relation $x = 1 - y$ from the first equation, and the relation $2x = -2y$ from the second equation; multiplying both sides of this last relation by $\frac{1}{2}$ yields, upon simplification, the relation $x = -y$. We have therefore that if the pair (x, y) is a solution of system (C'), then we must have $x = 1 - y$ **and** $x = -y$, and hence, we must also have as a result that $1 - y = -y$, which yields $0y = 1$. Since there exists no real number y such that $0y = 1$, we conclude that there exists no pair (x, y) of real numbers which would be a solution to system (C'). We conclude therefore that system (C') has **no** solution.

We recapitulate our findings concerning systems $(A'), (B')$ and (C') as follows:

- System (A') has **exactly one** solution.
- System (B') has **infinitely many** solutions.
- System (C') has **no** solution.

Note that these are **exactly** the cases that we encountered for the systems $(A), (B)$ and (C), which consisted of only one equation in one unknown.

Some **very natural** questions that come to mind at this point are:

- Can a system of linear equations, with whatever number of equations and whatever number of unknowns, have a number of solutions different from these, i.e. a number of solutions different from $0, 1$ and ∞ ?
- Can we come up with a system of linear equations that instead has exactly 2 solutions ? or exactly 17 solutions ? or 154 solutions ? ...

- Is there anything special with $0, 1, \infty$, or did we stumble on these by accident ?
- ... and many such questions!

We shall see in the next few lectures that these are the **only cases** that we can encounter with systems of linear equations; that is, a system of linear equations, with whatever number of equations and whatever number of unknowns, can have either **exactly one** solution, **infinitely many** solutions, or **no** solution at all; it is instructive to contrast this with the case of **polynomial equations of degree** 2 in one real variable, i.e. equations of the form $ax^2 + bx + c = 0$, with $a \neq 0$, which we know can **never** have **infinitely many** solutions (recall that they can have exactly 0, 1, or 2 solutions).

In order to get to a point where we can prove this **non-trivial** result, we shall first **develop the necessary tools**. This will be done in the next few lectures.

Later on, we will also see **how** to **quickly** and **systematically** solve systems of linear equations (as opposed to the ad hoc scheme we have been using) ...

Applications of Systems of Linear Equations

Systems of linear equations have numerous applications in engineering and applied sciences. We provide here a number of application examples of systems of linear equations. These by no means exhaust the rich diversity of contexts in which systems of linear equations naturally arise.

- **Chemical Balance Equations**: The fundamental law of conservation of mass implies that, in a chemical reaction, the number of atoms of each element involved in the reaction must be the same before and after the reaction. The mathematical expression of this principle is called a chemical balance equation, and arises as a system of linear equations. To give a simple example, hydrochloric acid (HCl) combines with sodium (Na) to yield salt ($NaCl$) and hydrogen gas (H_2); we can write the chemical reaction as follows:

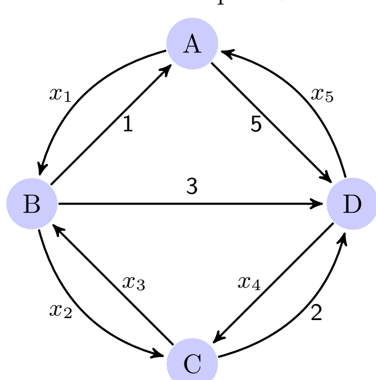
$$x_1 HCl + x_2 Na \ \rightarrow \ x_3 NaCl + x_4 H_2,$$

where x_1 and x_2 denote the number of molecules of hydrochloric acid and sodium, respectively, involved in the reaction, and x_3 and x_4 the number of molecules of salt and hydrogen, respectively, obtained from the reaction. The balance equations are obtained by stipulating that the number of atoms of each element must be conserved in the reaction, i.e., must be the same before and after the reaction. In this particular reaction, we have the elements H, Cl, Na. There are x_1 atoms of hydrogen (H) before the reaction, and $2x_4$ after the reaction; we must therefore have $x_1 = 2x_4$, i.e., $x_1 - 2x_4 = 0$. There are x_1 atoms of chlorine (Cl) before the reaction, and x_3 atoms after the reaction; we must therefore have $x_1 = x_3$, i.e.

$x_1 - x_3 = 0$. Finally, there are x_2 atoms of sodium (Na) before the reaction, and x_3 after; we must therefore have $x_2 = x_3$, i.e. $x_2 - x_3 = 0$. Hence, the balance equations for the given chemical reaction are given by the following system of linear equations:

$$\begin{aligned} x_1 - 2x_4 &= 0, \\ x_1 - x_3 &= 0, \\ x_2 - x_3 &= 0. \end{aligned}$$

- **Network Flow**: Many problems in engineering, economics, etc., can be abstracted as network flow problems: The basic data is a graph, consisting of vertices (also called nodes) and directed edges between pairs of vertices, as well as a numeric weight attached to each edge; in the context of electric circuits, this weight would denote the intensity of the electric current flowing from one node to another, while in the context of economics, and more specifically, transportation problems, it could denote the amount of goods that are conveyed from one city to another (both represented as vertices of the graph). Just as with chemical balance equations, we assume here a conservation law of the form: "What goes into a vertex must equal what comes out of a vertex" (in the context of electric circuits this conservation law is known as Kirchoff's current law). We illustrate this with an example: Consider then the graph:



consisting of four vertices (or nodes), labelled A,B,C,D, and edges connecting them. The numeric weight attached to each edge denotes the number of units flowing through that edge, and we write the so-called "node balance" equations by equating at each node the total weights of incoming and outgoing edges. If at a given node, there are no incoming (resp. outgoing) edges, then the total weight of incoming (resp. outgoing) edges for that node is 0. For the graph depicted above, x_1, x_2, x_3, x_4, x_5 are the unknown weights that have to be determined from the node balance equations. Here, we have a total of $1+x_5$ units flowing into node A, and a total of $5+x_1$ units flowing out of node A; equating these yields the equation $1+x_5 = 5+x_1$, or, equivalently, the equation $x_1 - x_5 = -4$. At node B, we have a total of x_1+x_3 flowing in, and a total of $1+3+x_2=4+x_2$ flowing out; equating these yields the equation $x_1-x_2+x_3=4$. At node C, we have a total of x_2+x_4 units flowing in, and a total of $2+x_3$ units flowing out; equating these yields the equation $x_2+x_3=2+x_4$, or, equivalently, $x_2+x_3-x_4=2$. At node D, we have a total of $5+3+2=10$ units flowing in, and x_4+x_5 units flowing out; equating these yields the equation $x_4+x_5=10$. Hence, we have obtained the following node balance equations:

$$\begin{aligned} x_1-x_5 &= -4, \\ x_1-x_2+x_3 &= 4, \\ x_2+x_3-x_4 &= 2, \\ x_4+x_5 &= 10, \end{aligned}$$

which form a system of linear equations.

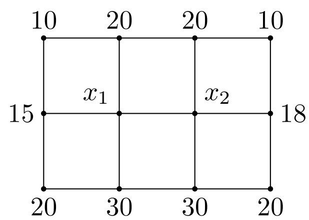
- **Polynomial Interpolation**: Suppose the position $x(t)$ of a particle at time t is given by the relation $x(t)=at^2+bt+c$, where the real coefficients a,b,c are unknown and have to be determined from experimental data. Suppose we observe the particle at times $t=0,1,2$, and suppose we determine experimentally that $x(0)=1, x(1)=2, x(2)=4$. Hence, equating $x(0)=a0^2+b0+c=c$ with $x(0)=1$ yields the equation $c=1$, equating $x(1)=a1^2+b1+c=a+b+c$ with $x(1)=2$ yields the equation $a+b+c=2$, and equating $x(2)=a2^2+b2+c=4a+2b+c$ with $x(2)=4$ yields the equation $4a+2b+c=4$. We have therefore obtained the following system of linear equations

$$\begin{aligned} c &= 1, \\ a+b+c &= 2, \\ 4a+2b+c &= 4, \end{aligned}$$

from which we can determine the unknowns a,b,c.

- **Steady-State Temperature Distribution**:

Consider a rectangular thin metal plate in which the temperature is at steady-state (i.e does not change as a function of time), and assume the temperature on the boundary is known; we wish to determine the temperature at points interior to the plate. We can consider the simpler problem of determining the temperature at regularly placed points on the plate. Consider then the following mesh, which represents points on the plate and on its boundary:



The temperature at each mesh point is indicated next to that mesh point. There are two points on this mesh which are in the interior of the plate (i.e. not on its boundary), with respective temperatures x_1 and x_2; we wish to determine these two temperatures. The fundamental laws of heat propagation imply that at steady-state, the temperature at each interior mesh point is the average of the temperatures of its neighboring mesh points. Applying this law to the two interior mesh points (with respective temperatures x_1 and x_2) yields:

$$\begin{aligned} x_1 &= \frac{1}{4}(15 + 20 + x_2 + 30), \\ x_2 &= \frac{1}{4}(x_1 + 20 + 18 + 30), \end{aligned}$$

which is equivalent to the system of linear equations:

$$\begin{aligned} 4x_1 - x_2 &= 65, \\ -x_1 + 4x_2 &= 68, \end{aligned}$$

from which x_1, x_2 can be obtained. Note that the temperatures obtained at the two interior points are merely approximations to the exact temperatures; however, the finer the mesh (i.e. the more grid points), the better the approximation.

PROBLEMS:

For each of the following systems of linear equations, identify the number of solutions using the same "procedure" as in the examples treated in this lecture (this should convince you that there can be only the three cases mentioned in this Lecture):

1.

$$\begin{cases} 2x = 3, \\ 4x = 5, \end{cases}$$

where we wish to solve for the real number x.

2.

$$\begin{cases} 2x = 3, \\ 4x = 6, \end{cases}$$

where we wish to solve for the real number x.

3.

$$\begin{cases} 2x + y = 1, \\ 4x + 2y = 3, \end{cases}$$

where we wish to solve for the pair (x, y) of real numbers.

4.

$$\begin{cases} 2x + y = 1, \\ 10x + 5y = 5, \\ 6x + 3y = 3, \\ 20x + 10y = 10, \end{cases}$$

where we wish to solve for the pair (x, y) of real numbers.

5.

$$\begin{cases} 2x + y = 1, \\ 10x + 5y = 5, \\ x - y = 1, \end{cases}$$

where we wish to solve for the pair (x, y) of real numbers.

6.

$$\begin{cases} 2x - y + z = 0, \\ x + y = 2, \\ x - y = 1, \\ y - z = 0, \end{cases}$$

where we wish to solve for the triple (x, y, z) of real numbers.

7.

$$\begin{cases} x + y - z = 0, \end{cases}$$

where we wish to solve for the triple (x, y, z) of real numbers.

8.

$$\begin{cases} x + y - z = 0, \\ x + y = 1, \\ y + z = 2, \end{cases}$$

where we wish to solve for the triple (x, y, z) of real numbers.

9.

$$\begin{cases} x + y - z - w = 0, \\ x + y = 2, \end{cases}$$

where we wish to solve for the quadruple (x, y, z, w) of real numbers.

10.

$$\begin{cases} x + y - z - w = 0, \\ -x - y = 2, \\ z + w = 3, \end{cases}$$

where we wish to solve for the quadruple (x, y, z, w) of real numbers.

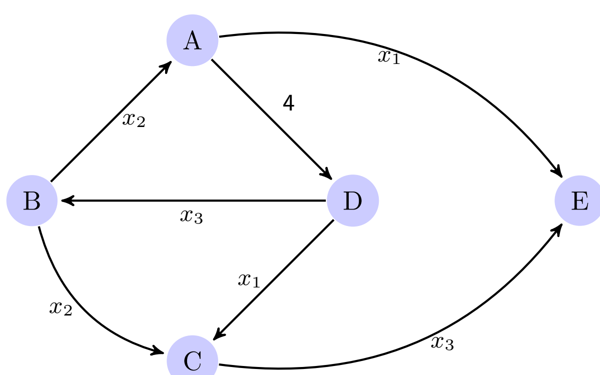
11. Methane (CH_4) combines with oxygen gas (O_2) to yield carbon dioxide (CO_2) and water (H_2O); write the chemical balance equations for this reaction as a system of linear equations.

12. Tin oxide (SnO_2) combines with hydrogen gas (H_2) to yield tin (Sn) and water (H_2O); write the chemical balance equations for this reaction as a system of linear equations.

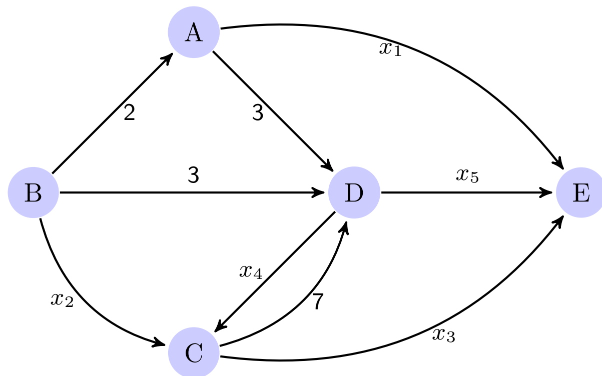
13. Iron (Fe) combines with sulfuric acid (H_2SO_4) to yield ferric sulfate ($Fe_2(SO_4)_3$) and hydrogen gas (H_2); write the chemical balance equations for this reaction as a system of linear equations.

14. Propane (C_3H_8) combines with oxygen gas (O_2) to produce water (H_2O) and carbon dioxide (CO_2); write the chemical balance equations for this reaction as a system of linear equations.

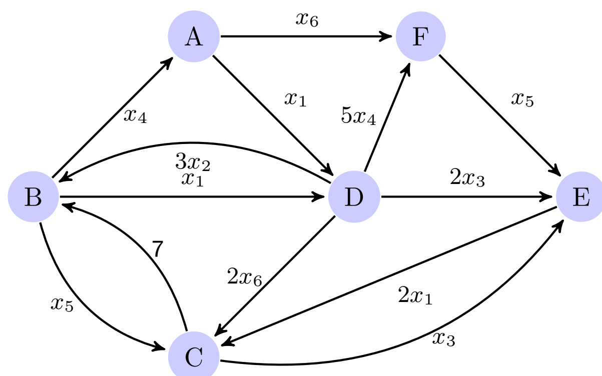
15. Write the node balance equations (as a system of linear equations in the unknowns x_1, x_2, x_3) for the following graph:



16. Write the node balance equations (as a system of linear equations in the unknowns x_1, x_2, x_3, x_4, x_5) for the following graph:



17. Write the node balance equations (as a system of linear equations in the unknowns $x_1, x_2, x_3, x_4, x_5, x_6$) for the following graph:

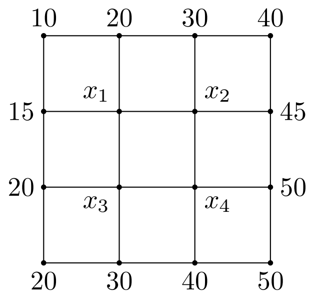


18. The voltage V at the output of an electric device is related to the input current I to the device by the polynomial function $V(I) = aI^3 + bI^2 + cI + d$, where the real coefficients a, b, c, d are unknown; we wish to determine a, b, c, d from experimental data. We experimentally measure the output voltage at the input current values $I = 0, 1, 2, 3$, and we determine from measurement that $V(0) = 0.2$, $V(1) = 2.1$, $V(2) = 5.7$, and $V(3) = 10.4$. Write the system of linear equations (in the unknowns a, b, c, d) corresponding to these measurements.

19. The elongation l of a metal bar is modelled as a function of temperature T by the polynomial function $l(T) = aT^4 + bT^3 + cT^2 + dT + e$, where the real coefficients a, b, c, d, e are unknown; we wish to determine a, b, c, d, e from experimental data. We experimentally measure the elongation of the bar at temperatures $T = 0, 1, 2, 3, 4$, and we determine from measurement that $l(0) = 0.11$, $l(1) = 2.21$, $l(2) = 4.35$, $l(3) = 7.26$, $l(4) = 9.77$. Write the system of linear equations (in the unknowns a, b, c, d, e) corresponding to these measurements.

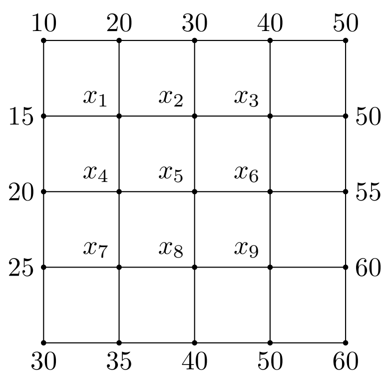
20. Consider a square thin metal plate with temperature at steady state and

with known boundary temperature; we represent this thin metal plate by the following square mesh:



The steady-state temperature at each mesh point is indicated next to that mesh point. The four mesh points interior to the plate have respective steady-state temperatures x_1, x_2, x_3, x_4; write the system of linear equations that governs the relation between these temperatures.

21. Consider a square thin metal plate with temperature at steady state and with known boundary temperature; we represent this thin metal plate by the following square mesh:



The steady-state temperature at each mesh point is indicated next to that mesh point. The nine mesh points interior to the plate have respective steady-state temperatures $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$; write the system of linear equations that governs the relation between these temperatures.

Section 2

Study Topics

- Real vector spaces
- Examples of real vector spaces

The basic notion in linear algebra is that of **vector space**. In this lecture, we give the basic definition and review a number of examples.

Definition 12. Let $\mathbf{V}$ be a **set**, with **two operations** defined on it:

(i) An operation denoted by "+" and called **addition**, defined formally as a mapping $+ : \mathbf{V} \times \mathbf{V} \to \mathbf{V}$ which maps a pair $(\mathbf{v}, \mathbf{w})$ in $\mathbf{V} \times \mathbf{V}$ to the element $\mathbf{v} + \mathbf{w}$ of $\mathbf{V}$;

(ii) An operation denoted by "·" and called **multiplication by a scalar**, defined formally as a mapping $\cdot : \mathbb{R} \times \mathbf{V} \to \mathbf{V}$ which maps a pair $(\alpha, \mathbf{v})$ in $\mathbb{R} \times \mathbf{V}$ (i.e. $\alpha \in \mathbb{R}$ and $\mathbf{v} \in \mathbf{V}$) to the element $\alpha \cdot \mathbf{v}$ of $\mathbf{V}$.

With these two operations in place, $\mathbf{V}$ is said to be a **real vector space** if the following properties are verified:

1. The operation + is **associative**, i.e. for any $\mathbf{x}, \mathbf{y}, \mathbf{z}$ in $\mathbf{V}$, we have:

$$\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$$

2. There exists an element in $\mathbf{V}$, called the **zero vector** of $\mathbf{V}$, and denoted by $\mathbf{0_V}$, such that for any $\mathbf{x}$ in $\mathbf{V}$, we have:

$$\mathbf{x} + \mathbf{0_V} = \mathbf{0_V} + \mathbf{x} = \mathbf{x}$$

3. For any $\mathbf{x}$ in $\mathbf{V}$, there exists an element in $\mathbf{V}$ denoted by $-\mathbf{x}$ (and usually called the **inverse** or **opposite** of $\mathbf{x}$) such that:

$$\mathbf{x} + (-\mathbf{x}) = (-\mathbf{x}) + \mathbf{x} = \mathbf{0_V}$$

4. The operation + is **commutative**, i.e. for any $\mathbf{x}, \mathbf{y}$ in $\mathbf{V}$, we have:

$$\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$$

5. For any α, β in $\mathbb{R}$ and any $\mathbf{x}$ in $\mathbf{V}$, we have:

$$\alpha \cdot (\beta \cdot \mathbf{x}) = (\alpha\beta) \cdot \mathbf{x}$$

6. For any α in $\mathbb{R}$ and any $\mathbf{x}, \mathbf{y}$ in $\mathbf{V}$, we have:

$$\alpha \cdot (\mathbf{x} + \mathbf{y}) = \alpha \cdot \mathbf{x} + \alpha \cdot \mathbf{y}$$

7. For any α, β in $\mathbb{R}$ and any $\mathbf{x}$ in $\mathbf{V}$, we have:

$$(\alpha + \beta) \cdot \mathbf{x} = \alpha \cdot \mathbf{x} + \beta \cdot \mathbf{x}$$

8. For any $\mathbf{x}$ in $\mathbf{V}$, we have:

$$1 \cdot \mathbf{x} = \mathbf{x}$$

We shall usually denote the vector space by $(\mathbf{V}, +, \cdot)$ and sometimes only by $\mathbf{V}$, when there is no risk of confusion about what the addition and multiplication by scalar operation are. Similarly, when there is no risk of confusion, we shall denote the zero vector of $\mathbf{V}$ by $\mathbf{0}$ instead of $\mathbf{0}_{\mathbf{V}}$. Each element of $\mathbf{V}$ is called a **vector**.

IMPORTANT NOTE: If given some set $\mathbf{V}$ and operations "+" and "·" defined in some way, one wants to verify whether or not $(\mathbf{V}, +, \cdot)$ is a real vector space, **before going through the axioms** one by one it is important to first **verify that the operations** "+" and "·" **are both well-defined**. To illustrate this point with an example, if we let $\mathbf{V} = \mathbb{N}^2$ and we define as the addition operation on $\mathbf{V}$ the operation "$\tilde{+}$" on $\mathbf{V}$ by stipulating that $\forall (x_1, y_1) \in \mathbb{N}^2$ and $\forall (x_2, y_2) \in \mathbb{N}^2$ we define $(x_1, y_1) \tilde{+} (x_2, y_2)$ to be the pair $(x_1 x_2, \sqrt{y_1 y_2})$, then this operation will not be well-defined since for some pairs $(x_1, y_1), (x_2, y_2)$ in $\mathbb{N}^2$ the pair $(x_1, y_1) \tilde{+} (x_2, y_2)$ will not be in $\mathbb{N}^2$; for example, if we take the pairs $(1, 1)$ and $(2, 2)$, we will have $(1, 1) \tilde{+} (2, 2) = (2, \sqrt{2})$ which is **not** an element of $\mathbb{N}^2$. Hence, we can stop right here and declare that since the operation $\tilde{+}$ is not well-defined, $(\mathbf{V}, \tilde{+}, \cdot)$ will not be a real vector space (no matter how we define the operation "·").

We now examine a number of examples in order to develop some familiarity with this concept.

(a) Consider the usual set $\mathbb{R}$ of real numbers, with the addition operation "+" being the usual addition of real numbers, and the multiplication by scalar operation "·" the usual multiplication operation of real numbers. It is easy to verify that, with these two operations, $\mathbb{R}$ satisfies all the axioms of a real vector space. We can write therefore that $(\mathbb{R}, +, \cdot)$ is a real vector space.

(b) Let $\mathbb{R}^2$ denote the set of all pairs (x, y) with x and y real numbers. We define an addition operation "+" on $\mathbb{R}^2$ as follows: If (x_1, y_1) and (x_2, y_2) are two elements of $\mathbb{R}^2$, we define:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

We also define a multiplication by scalar operation "·" on $\mathbb{R}^2$ as follows: For any α in $\mathbb{R}$ and any (x, y) in $\mathbb{R}^2$, we define:

$$\alpha \cdot (x, y) = (\alpha x, \alpha y).$$

It is easy to verify that endowed with these two operations, $\mathbb{R}^2$ satisfies all the axioms of a real vector space. We can write therefore that $(\mathbb{R}^2, +, \cdot)$ is a real vector space.

(c) Let $\mathcal{F}(\mathbb{R}; \mathbb{R})$ denote the set of all functions $f : \mathbb{R} \to \mathbb{R}$, i.e. the set of all real-valued functions of a real variable. We define the addition operation

"+" on $\mathcal{F}(\mathbb{R};\mathbb{R})$ as follows: If f,g are two elements of $\mathcal{F}(\mathbb{R};\mathbb{R})$, we define $(f+g):\mathbb{R}\to\mathbb{R}$ by:

$$(f+g)(t) = f(t) + g(t), \quad \text{for all } t \text{ in } \mathbb{R}.$$

We also define a multiplication by scalar operation "$\cdot$" on $\mathcal{F}(\mathbb{R};\mathbb{R})$ as follows: For any α in $\mathbb{R}$ and any f in $\mathcal{F}(\mathbb{R};\mathbb{R})$, we define the function $(\alpha\cdot f):\mathbb{R}\to\mathbb{R}$ by:

$$(\alpha\cdot f)(t) = \alpha f(t), \quad \text{for all } t \text{ in } \mathbb{R}.$$

It is easy to verify that endowed with these two operations, $\mathcal{F}(\mathbb{R};\mathbb{R})$ satisfies all the axioms of a real vector space. We can write therefore that $(\mathcal{F}(\mathbb{R};\mathbb{R}),+,\cdot)$ is a real vector space.

(d) Let now $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ denote the set of all functions $f:\mathbb{R}\to\mathbb{R}$ which satisfy $f(0)=0$, i.e. the set of all real valued functions of a real variable which vanish at 0. Formally, we write:

$$\mathcal{F}_0(\mathbb{R};\mathbb{R}) = \{f\in\mathcal{F}(\mathbb{R};\mathbb{R})|f(0)=0\}.$$

Note that $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ is a subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$. Note also that we can define the addition operation "+" on $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ the same way we defined it on $\mathcal{F}(\mathbb{R};\mathbb{R})$; indeed, if f,g are two elements of $\mathcal{F}_0(\mathbb{R};\mathbb{R})$, then the function $f+g$ satisfies $(f+g)(0)=f(0)+g(0)=0$ and hence $f+g$ is an element of $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ as well. Similarly, if we define the multiplication by scalar operation "$\cdot$" on $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ the same way we defined it on $\mathcal{F}(\mathbb{R};\mathbb{R})$, we have that if α is in $\mathbb{R}$ and f is in $\mathcal{F}_0(\mathbb{R};\mathbb{R})$, then the function $\alpha\cdot f$ satisfies $(\alpha\cdot f)(0)=\alpha f(0)=0$, and as a result, the function $\alpha\cdot f$ is an element of $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ as well. Just as easily as with $\mathcal{F}(\mathbb{R};\mathbb{R})$, it is immediate to verify that endowed with these two operations, $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ satisfies all the axioms of a real vector space. We can write therefore that $(\mathcal{F}_0(\mathbb{R};\mathbb{R}),+,\cdot)$ is a real vector space.

(e) Let $\mathbb{R}^n$ denote the set of all $n-$tuples $(x_1,x_2,\cdots,x_n)$ of real numbers (where n is any integer ≥ 1); $\mathbb{R}^n$ is defined as the n^{th} Cartesian product of $\mathbb{R}$ with itself, i.e. $\mathbb{R}^n=\mathbb{R}\times\mathbb{R}\times\cdots\times\mathbb{R}$ (n times). Note that we saw the special case of this construction for $n=1$ in Example (a) above, and for $n=2$ in Example (b) above. We define on $\mathbb{R}^n$ the addition operation "+" as follows: For any $n-$tuples $(x_1,x_2,\cdots,x_n)$ and $(y_1,y_2,\cdots,y_n)$ of real numbers, we define:

$$(x_1,x_2,\cdots,x_n)+(y_1,y_2,\cdots,y_n) = (x_1+y_1,x_2+y_2,\cdots,x_n+y_n).$$

We also define a multiplication by scalar operation "$\cdot$" on $\mathbb{R}^n$ as follows: For any α in $\mathbb{R}$ and any element $(x_1,x_2,\cdots,x_n)$ of $\mathbb{R}^n$, we define:

$$\alpha\cdot(x_1,x_2,\cdots,x_n) = (\alpha x_1,\alpha x_2,\cdots,\alpha x_n).$$

It is easy to verify that endowed with these two operations, $\mathbb{R}^n$ satisfies all the axioms of a real vector space. We can write therefore that $(\mathbb{R}^n, +, \cdot)$ is a real vector space.

(f) Let $(\mathbb{R}^n)_0$ denote the set of all $n-$tuples $(x_1, x_2, \cdots, x_n)$ of real numbers which satisfy $x_1 + x_2 + \cdots + x_n = 0$. Note that $(\mathbb{R}^n)_0$ is a subset of $\mathbb{R}^n$. Furthermore, we can define on $(\mathbb{R}^n)_0$ the addition operation "+" and the multiplication by scalar operation "·" in exactly the same way that we defined them on $\mathbb{R}^n$. Indeed, if $(x_1, x_2, \cdots, x_n)$ and $(y_1, y_2, \cdots, y_n)$ are two elements of $(\mathbb{R}^n)_0$, then the $n-$tuple $(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$ is also in $(\mathbb{R}^n)_0$ since

$$\begin{aligned}(x_1 + y_1) + \cdots + (x_n + y_n) &= (x_1 + \cdots + x_n) + (y_1 + \cdots + y_n) \\ &= 0 + 0 \\ &= 0.\end{aligned}$$

Similarly, if α is in $\mathbb{R}$ and $(x_1, x_2, \cdots, x_n)$ is an element of $(\mathbb{R}^n)_0$, then the $n-$tuple $\alpha \cdot (x_1, x2, \cdots, x_n)$ is also in $(\mathbb{R}^n)_0$, since

$$\begin{aligned}\alpha x_1 + \alpha x_2 + \cdots \alpha x_n &= \alpha(x_1 + x_2 + \cdots + x_n) \\ &= 0.\end{aligned}$$

It is easy to verify that endowed with these two operations, $(\mathbb{R}^n)_0$ satisfies all the axioms of a real vector space. We can write therefore that $((\mathbb{R}^n)_0, +, \cdot)$ is a real vector space.

Let us now consider examples of sets with operations on them which do **not** make them real vector spaces:

(g) On the set $\mathbb{R}^n$, which we have defined in Example (e) above, define an addition operation, which we denote by $\tilde{+}$ to distinguish it from the one defined in Example (e), as follows: For any $n-$tuples $(x_1, x_2, \cdots, x_n)$ and $(y_1, y_2, \cdots, y_n)$ of real numbers, define:

$$(x_1, x_2, \cdots, x_n)\tilde{+}(y_1, y_2, \cdots, y_n) = (x_1 + 2y_1, x_2 + 2y_2, \cdots, x_n + 2y_n).$$

Define the multiplication by scalar operation "·" as in Example (e). It is easy to verify that endowed with these two operations, $\mathbb{R}^n$ does **not** satisfy all the axioms of a real vector space. We can therefore write that $(\mathbb{R}^n, \tilde{+}, \cdot)$ is **not** a real vector space.

(h) On the set $\mathcal{F}(\mathbb{R};\mathbb{R})$, defined in Example (c) above, define the addition operation + exactly as in Example (c), but define the multiplication by scalar operation by $\tilde{\cdot}$ (to distinguish it from the one defined in Example (c)) as follows: For any α in $\mathbb{R}$ and f in $\mathcal{F}(\mathbb{R};\mathbb{R})$, define the element $\alpha\tilde{\cdot}f$ of $\mathcal{F}(\mathbb{R};\mathbb{R})$ as follows:

$$(\alpha\tilde{\cdot}f)(t) = \alpha(f(t))^2, \quad \text{for all } t \text{ in } \mathbb{R}.$$

> It is easy to verify that endowed with these two operations $\mathcal{F}(\mathbb{R};\mathbb{R})$ does **not** satisfy all the axioms of a real vector space. We can write therefore that $(\mathcal{F}(\mathbb{R};\mathbb{R}), +, \tilde{\cdot})$ is **not** a real vector space.

Now that the concept of real vector space is hopefully getting more concrete, let us prove the following simple (and very intuitive) results for general vector spaces:

Theorem 1. Let $(\mathbf{V}, +, \cdot)$ be a real vector space. Then:

- For any $\mathbf{v}$ in $\mathbf{V}$, we have $0 \cdot \mathbf{v} = \mathbf{0}$;
- For any α in $\mathbb{R}$, we have $\alpha \cdot \mathbf{0} = \mathbf{0}$.

Proof. Let us first prove the first statement. Since $0 = 0+0$, we have, of course:

$$0 \cdot \mathbf{v} = (0+0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v},$$

where we have used Property (7) of a vector space to get this last equality; now by property (3) of a vector space, there exists an element in $\mathbf{V}$, which we denote by $-0 \cdot \mathbf{v}$, such that $-0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} = \mathbf{0}$; adding $-0 \cdot \mathbf{v}$ to both sides of the above equality yields:

$$-0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} = -0 \cdot \mathbf{v} + (0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}),$$

which, by Property (1) of a vector space is equivalent to the equality:

$$-0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} = (-0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}) + 0 \cdot \mathbf{v},$$

which, by the fact that $-0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} = \mathbf{0}$ (Property (3)) is equivalent to the equality

$$\mathbf{0} = \mathbf{0} + 0 \cdot \mathbf{v},$$

which, by Property (2) of a vector space, is equivalent to

$$\mathbf{0} = 0 \cdot \mathbf{v},$$

i.e. $0 \cdot \mathbf{v} = \mathbf{0}$.
Let us now prove the second statement. Since $\mathbf{0} = \mathbf{0} + \mathbf{0}$ (Property (2)), we have:

$$\alpha \cdot \mathbf{0} = \alpha \cdot (\mathbf{0} + \mathbf{0}) = \alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0},$$

where we have used Property (6) to get this last equality; By property (3), there exists an element in $\mathbf{V}$, which we denote by $-\alpha \cdot \mathbf{0}$, such that $-\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = \mathbf{0}$; adding $-\alpha \cdot \mathbf{0}$ to both sides of the above equality yields:

$$-\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = -\alpha \cdot \mathbf{0} + (\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0}),$$

which, by Property (1) is equivalent to

$$-\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = (-\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0}) + \alpha \cdot \mathbf{0},$$

which by the fact that $-\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = \mathbf{0}$ (Property (3)) is equivalent to the equality

$$\mathbf{0} = \mathbf{0} + \alpha \cdot \mathbf{0},$$

which, by Property (2), is equivalent to

$$\mathbf{0} = \alpha \cdot \mathbf{0},$$

i.e., $\alpha \cdot \mathbf{0} = \mathbf{0}$. □

Recall that, by definition of a real vector space, if $(\mathbf{V}, +, \cdot)$ happens to be a real vector space, and if $\mathbf{v}$ is any element of $\mathbf{V}$, then there is an element in $\mathbf{V}$ which we denote by $-\mathbf{v}$ (and which we call the "inverse" or "opposite" of $\mathbf{v}$) and which satisfies:

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

(where $\mathbf{0}$ denotes the zero vector of $\mathbf{V}$). All we know is that such an element does exist in $\mathbf{V}$; we don't know yet whether for each choice of $\mathbf{v}$ in $\mathbf{V}$ such an element $-\mathbf{v}$ is unique or not, nor do we know how to compute it. The following theorem answers these two questions:

Theorem 2. Let $(\mathbf{V}, +, \cdot)$ be a real vector space. Then:

(a) For any $\mathbf{v}$ in $\mathbf{V}$, the element $-\mathbf{v}$ is uniquely defined.

(b) For any $\mathbf{v}$ in $\mathbf{V}$, we have: $-\mathbf{v} = (-1) \cdot \mathbf{v}$.

Proof. Let us prove (a) first. Let then $\mathbf{v} \in \mathbf{V}$ be any element of $\mathbf{V}$, and assume the element $\mathbf{w} \in \mathbf{V}$ satisfies the defining conditions for $-\mathbf{v}$, i.e. it satisfies:

$$\mathbf{w} + \mathbf{v} = \mathbf{v} + \mathbf{w} = \mathbf{0}.$$

We shall show that we necessarily have $\mathbf{w} = -\mathbf{v}$; this will prove that for any $\mathbf{v} \in \mathbf{V}$, the element $-\mathbf{v}$ is uniquely defined. Since

$$\mathbf{w} + \mathbf{v} = \mathbf{0},$$

we obtain (by adding $-\mathbf{v}$ to the right on both sides of the equality):

$$(\mathbf{w} + \mathbf{v}) + (-\mathbf{v}) = \mathbf{0} + (-\mathbf{v}),$$

and using axioms (1) and (2) of a real vector space, we obtain:

$$\mathbf{w} + (\mathbf{v} + (-\mathbf{v})) = -\mathbf{v},$$

and using axiom (3), we obtain:

$$\mathbf{w} + \mathbf{0} = -\mathbf{v},$$

and, finally, using axiom (2), we obtain:

$$\mathbf{w} = -\mathbf{v},$$

which is exactly what we wanted to prove. Hence this proves (a). We now prove (b). Let then $\mathbf{v} \in \mathbf{V}$ be any element of $\mathbf{V}$. Note that by axiom (8) of a real vector space we have $\mathbf{v} = 1 \cdot \mathbf{v}$, hence (using axiom (7) of a real vector space as well as the previous theorem):

$$(-1) \cdot \mathbf{v} + \mathbf{v} = (-1) \cdot \mathbf{v} + 1 \cdot \mathbf{v} = (-1+1) \cdot \mathbf{v} = 0 \cdot \mathbf{v} = \mathbf{0},$$

and, similarly,

$$\mathbf{v} + (-1) \cdot \mathbf{v} = 1 \cdot \mathbf{v} + (-1) \cdot \mathbf{v} = (1 + (-1)) \cdot \mathbf{v} = 0 \cdot \mathbf{v} = \mathbf{0},$$

Hence, we have shown that the element $(-1) \cdot \mathbf{v}$ of $\mathbf{V}$ satisfies:

$$\mathbf{v} + (-1) \cdot \mathbf{v} = (-1) \cdot \mathbf{v} + \mathbf{v} = \mathbf{0},$$

and by the result proved in part (a), this shows that

$$(-1) \cdot \mathbf{v} = -\mathbf{v},$$

which is exactly what we wanted to prove.

□

To recap the previous theorem: If you are given an element $\mathbf{v}$ in a real vector space $(\mathbf{V}, +, \cdot)$, you can compute its inverse $-\mathbf{v}$ simply by computing $(-1) \cdot \mathbf{v}$ (i.e. by "multiplying the vector $\mathbf{v}$ by the real number -1"); as simple as that!

Before closing this section, we consider an important example of a real vector space which we will deal with very frequently. We denote it by $\widehat{\mathbb{R}^n}$ (to distinguish it from $\mathbb{R}^n$) and call it the vector space of all **column** $n-$**vectors** with real entries. It is the set of all elements of the form

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

where $x_1, x_2, \cdots, x_n$ are real numbers. The addition operation "+" and multiplication by scalar operation "·" are defined on $\widehat{\mathbb{R}^n}$ as follows: For any α in $\mathbb{R}$

and any $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ and $\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$ in $\widehat{\mathbb{R}^n}$, we define:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

and

$$\alpha \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \alpha x_2 \\ \vdots \\ \alpha x_n \end{pmatrix}$$

It is easily verified (just as for $\mathbb{R}^n$ in Example (e) above) that endowed with these two operations, $\widehat{\mathbb{R}^n}$ is a real vector space.

A WORD ON NOTATION:

In the remainder of these notes, we will omit the multiplication by a scalar symbol "·" when multiplying a real number and a vector together, as this should cause no confusion. Hence, if α is a real number and $\mathbf{v}$ is an element of some vector space (i.e. a vector), we will write simply $\alpha\mathbf{v}$ instead of $\alpha\cdot\mathbf{v}$. For example, if (a, b) is an element of the vector space $\mathbb{R}^2$ (the set of all pairs of real numbers), we will write $\alpha(a, b)$ instead of $\alpha \cdot (a, b)$. Similarly, if $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ is an element of $\widehat{\mathbb{R}^3}$ (the set of all real column vectors with 3 entries), we will write simply $\alpha \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ instead of $\alpha \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix}$.

We will however continue to denote a vector space by a triple of the form $(\mathbf{V}, +, \cdot)$ (even though we will drop the "·" when actually writing the multiplication by a real number); occasionally, we will also denote a vector space only by $\mathbf{V}$ instead of $(\mathbf{V}, +, \cdot)$.

PROBLEMS:

1. Show that the set of all nonnegative integers $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$, with addition and multiplication defined as usual is **not** a real vector space, and explain precisely why.

2. Show that the set of all integers $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$, with addition and multiplication defined as usual is **not** a real vector space, and explain precisely why.

3. Show that the set of all non-negative real numbers $\mathbb{R}^+ = \{x \in \mathbb{R} | x \geq 0\}$ (with addition and multiplication defined as for $\mathbb{R}$) is **not** a real vector space, and explain precisely why.

4. Show that the set of all non-positive real numbers $\mathbb{R}^- = \{x \in \mathbb{R} | x \leq 0\}$ (with addition and multiplication defined as for $\mathbb{R}$) is **not** a real vector space, and explain precisely why.

5. Show that the subset of $\mathbb{R}$ defined by $S = \{x \in \mathbb{R} | -1 \leq x \leq 1\}$ (with addition and multiplication defined as for $\mathbb{R}$) is **not** a real vector space, and explain precisely why.

6. Let $\mathcal{F}_1(\mathbb{R}; \mathbb{R})$ be the set of all functions $f : \mathbb{R} \to \mathbb{R}$ which satisfy $f(0) = 1$. Show that with addition and multiplication defined as for $\mathcal{F}(\mathbb{R}; \mathbb{R})$ (see Example (c) of this Lecture), $\mathcal{F}_1(\mathbb{R}; \mathbb{R})$ is **not** a real vector space, and explain precisely why.

7. Let $\mathcal{F}_{[-1,1]}(\mathbb{R}; \mathbb{R})$ be the set of all functions $f : \mathbb{R} \to \mathbb{R}$ which satisfy $-1 \leq f(x) \leq 1$, for all $x \in \mathbb{R}$. Show that with addition and multiplication defined as for $\mathcal{F}(\mathbb{R}; \mathbb{R})$ (see Example (c) of this Lecture), $\mathcal{F}_{[-1,1]}(\mathbb{R}; \mathbb{R})$ is **not** a real vector space, and explain precisely why.

8. Consider the set $\mathbb{R}^2$ of all pairs (x, y) of real numbers. Define an "addition" operation, which we denote by "$\tilde{+}$", as follows: For any (x, y) and (u, v) in $\mathbb{R}^2$, we define $(x, y)\tilde{+}(u, v)$ to be the pair $(y + v, x + u)$. Define the multiplication operation $\cdot$ as in Example (b) (i.e. $\alpha \cdot (x, y) = (\alpha x, \alpha y)$). Is $(\mathbb{R}^2, \tilde{+}, \cdot)$ a real vector space ? Explain precisely why or why not.

9. Consider the set $\mathbb{R}^2$ of all pairs (x, y) of real numbers. Define an "addition" operation, which we again denote by "$\tilde{+}$", as follows: For any (x, y) and (u, v) in $\mathbb{R}^2$, we define $(x, y)\tilde{+}(u, v)$ to be the pair $(x+v, y+u)$. Define the multiplication operation $\cdot$ as in Example (b) (i.e. $\alpha \cdot (x, y) = (\alpha x, \alpha y)$). Is $(\mathbb{R}^2, \tilde{+}, \cdot)$ a real vector space ? Explain precisely why or why not.

10. Consider the subset V_1 of $\mathbb{R}^2$ consisting of all pairs (x, y) of real numbers such that $x+y = 1$. If we define the addition and multiplication operations on V_1 as we did for $\mathbb{R}^2$ in Example (b) of this Lecture, do we obtain a real vector space ? Explain precisely why or why not.

11. Consider the subset V_2 of $\mathbb{R}^2$ consisting of all pairs (x, y) of real numbers such that $x+y = 0$. If we define the addition and multiplication operations

on V_2 as we did for $\mathbb{R}^2$ in Example (b) of this Lecture, do we obtain a real vector space ? Explain precisely why or why not.

12. Consider now the subset V_3 of $\mathbb{R}^2$ consisting of all pairs (x, y) of real numbers such that $2x-3y = 1$. If we define the addition and multiplication operations on V_3 as we did for $\mathbb{R}^2$ in Example (b) of this Lecture, do we obtain a real vector space ? Explain precisely why or why not.

13. Consider now the subset V_3 of $\mathbb{R}^2$ consisting of all pairs (x, y) of real numbers such that $2x-3y = 0$. If we define the addition and multiplication operations on V_4 as we did for $\mathbb{R}^2$ in Example (b) of this Lecture, do we obtain a real vector space ? Explain precisely why or why not.

14. Let $a_1, a_2, \cdots, a_n$ be given real numbers, and consider the subset $\mathbf{V}$ of $\mathbb{R}^n$ (defined in Example (e) of this Lecture) consisting of all $n-$tuples $(x_1, x_2, \cdots, x_n)$ of real numbers which satisfy

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

With addition and multiplication operations defined as in Example (e) of this Lecture, is $\mathbf{V}$ a real vector space ? Explain precisely why or why not.

15. Let $a_1, a_2, \cdots, a_n$ be given real numbers, and consider the subset $\mathbf{V}$ of $\mathbb{R}^n$ (defined in Example (e) of this Lecture) consisting of all $n-$tuples $(x_1, x_2, \cdots, x_n)$ of real numbers which satisfy

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1.$$

With addition and multiplication operations defined as in Example (e) of this Lecture, is $\mathbf{V}$ a real vector space ? Explain precisely why or why not.

16. Let $a_1, a_2, \cdots, a_n$ be given real numbers, and consider the subset $\mathbf{W}$ of $\mathbb{R}^n$ (defined in Example (e) of this Lecture) consisting of all $n-$tuples $(x_1, x_2, \cdots, x_n)$ of real numbers which satisfy

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \geq 0.$$

With addition and multiplication operations defined as in Example (e) of this Lecture, is $\mathbf{W}$ a real vector space ? Explain precisely why or why not.

17. Let $S = \{\xi\}$ be a set consisting of a single element, denoted ξ. Define the addition operation "+" on S as follows: $\xi + \xi = \xi$, and define the multiplication (by a scalar) operation "$\cdot$" on S as follows: For any $\alpha \in \mathbb{R}$, $\alpha \cdot \xi = \xi$. Show that $(S, +, \cdot)$ is a real vector space.

18. Let $(\mathbf{V}, +, \cdot)$ be a real vector space. By the definition of a real vector space (see Property (2)), we know that there exists a "special" element in $\mathbf{V}$, which we denote by $\mathbf{0}$ and call the zero vector of $\mathbf{V}$, which has the property that for any $\mathbf{v}$ in $\mathbf{V}$, $\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}$. We wish to show that

this "special" element is actually **unique**. To do so, prove that if some (possibly other) element of $\mathbf{V}$, call it $\widehat{\mathbf{0}}$, satisfies Property (2) of a real vector space, then we **must** have $\widehat{\mathbf{0}} = \mathbf{0}$, i.e. there is no element in $\mathbf{V}$ other than the zero vector $\mathbf{0}$ itself, which satisfies Property (2).

19. Consider the set $\mathbb{R}^2$ of all pairs (x, y) of real numbers. Define an "addition" operation, which we denote by "$\tilde{+}$", as follows: For any (x, y) and (u, v) in $\mathbb{R}^2$, we define $(x, y)\tilde{+}(u, v)$ to be the pair $(x + u - 1, y + v - 2)$. Define the multiplication operation "$\tilde{\cdot}$" by $\alpha\tilde{\cdot}(x, y) = (\alpha x - \alpha + 1, \alpha y - 2\alpha + 2)$, for any $\alpha \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$. Show that $(\mathbb{R}^2, \tilde{+}, \tilde{\cdot})$ is a real vector space. What is the zero vector of $(\mathbb{R}^2, \tilde{+}, \tilde{\cdot})$?

Section 3

Study Topics

- Vector subspaces
- Examples and properties of vector subspaces

We now define another important notion, that of a **subspace** of a vector space.

Definition 13. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\mathbf{W}$ be a **subset** of $\mathbf{V}$ (i.e. $\mathbf{W} \subset \mathbf{V}$). $\mathbf{W}$ is said to be a **vector subspace** (or, for short, **subspace**) of $(\mathbf{V}, +, \cdot)$ (or, for short, of $\mathbf{V}$) if the following properties hold:

(i) The zero element $\mathbf{0}$ of $\mathbf{V}$ is in $\mathbf{W}$, that is, $\mathbf{0} \in \mathbf{W}$.

(ii) For any $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}$, we have $\mathbf{x} + \mathbf{y} \in \mathbf{W}$.

(iii) For any α in $\mathbb{R}$ and any $\mathbf{x}$ in $\mathbf{W}$, we have $\alpha\mathbf{x} \in \mathbf{W}$.

Before going further, we examine a number of examples:

(a) Recall the real vector space $(\mathbb{R}^n, +, \cdot)$ of all real $n-$tuples $(x_1, x_2, \cdots, x_n)$ which was defined in Lecture 2; recall also the subset $(\mathbb{R}^n)_0$ of $\mathbb{R}^n$ (defined in the same lecture), consisting of all $n-$tuples $(x_1, x_2, \cdots, x_n)$ in $\mathbb{R}^n$ for which $x_1 + x_2 + \cdots + x_n = 0$ (i.e. all entries add up to 0). Let us show that $(\mathbb{R}^n)_0$ is a vector subspace of the real vector space $(\mathbb{R}^n, +, \cdot)$: To do this, we have to show that properties (i),(ii), and (iii) of a vector subspace are verified. Let us begin with property (i); the zero element $\mathbf{0}$ of $\mathbb{R}^n$ is the $n-$tuple $(0, 0, \cdots, 0)$ (all zero entries); since $0 + 0 + \cdots + 0 = 0$, it is clear that the n-tuple $(0, 0, \cdots, 0)$ is in $(\mathbb{R}^n)_0$, i.e. $\mathbf{0} \in (\mathbb{R}^n)_0$; hence, property (i) of a vector subspace is verified. Let us now check Property (ii): Let $(x_1, x_2, \cdots, x_n)$ and $(y_1, y_2, \cdots, y_n)$ be two elements of $(\mathbb{R}^n)_0$; we have to show that the $n-$tuple $(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n)$, which is defined as the $n-$tuple $(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$, is in $(\mathbb{R}^n)_0$. Now, since

$$\begin{aligned} (x_1 + y_1) + \cdots + (x_n + y_n) &= (x_1 + \cdots + x_n) + (y_1 + \cdots + y_n) \\ &= 0 + 0 \\ &= 0, \end{aligned}$$

it follows that the $n-$tuple $(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$ is in $(\mathbb{R}^n)_0$, i.e. $(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n)$ is in $(\mathbb{R}^n)_0$. Hence Property (ii) is verified. Finally, let us check Property (iii); let then $\alpha \in \mathbb{R}$ be any real number and let $(x_1, x_2, \cdots, x_n)$ be any element of $(\mathbb{R}^n)_0$; we have to show that the $n-$tuple $\alpha(x_1, x_2, \cdots, x_n)$, which is defined as $(\alpha x_1, \alpha x_2, \cdots, \alpha x_n)$, is in $(\mathbb{R}^n)_0$. Now, since

$$\begin{aligned} \alpha x_1 + \alpha x_2 + \cdots \alpha x_n &= \alpha(x_1 + x_2 + \cdots + x_n) \\ &= \alpha(0) \\ &= 0, \end{aligned}$$

it follows that the $n-$tuple $(\alpha x_1, \alpha x_2, \cdots, \alpha x_n)$ is in $(\mathbb{R}^n)_0$, i.e. $\alpha(x_1, x_2, \cdots, x_n)$ is in $(\mathbb{R}^n)_0$. Hence, Property (iii) is verified as well. We conclude that $(\mathbb{R}^n)_0$ is a vector subspace of the real vector space $(\mathbb{R}^n, +, \cdot)$.

(b) Let $(\mathbf{V}, +, \cdot)$ be a real vector space. Then $\mathbf{V}$ is **itself** a vector subspace of $\mathbf{V}$.

(c) Let $(\mathbf{V}, +, \cdot)$ be a real vector space. Then the set $\{\mathbf{0}\}$ consisting of the zero element $\mathbf{0}$ of $\mathbf{V}$ alone is a vector subspace of $\mathbf{V}$.

(d) Recall the real vector space $(\mathcal{F}(\mathbb{R};\mathbb{R}), +, \cdot)$ of all real-valued functions of a real variable defined in Lecture 2, as well as the subset $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ of $\mathcal{F}(\mathbb{R};\mathbb{R})$ defined in the same lecture (recall $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ consists of all real-valued functions f of a real variable for which $f(0) = 0$). It is easy to verify that $\mathcal{F}_0(\mathbb{R};\mathbb{R})$ is a vector subspace of $\mathcal{F}(\mathbb{R};\mathbb{R})$.

For completeness, let us also consider examples of subsets which are **not** vector subspaces:

(e) Recall again the real vector space $(\mathbb{R}^n, +, \cdot)$ of all real $n-$tuples $(x_1, x_2, \cdots, x_n)$ which was defined in Lecture 2; let $(\mathbb{R}^n)_1$ denote the subset of $\mathbb{R}^n$ consisting of all $n-$tuples $(x_1, x_2, \cdots, x_n)$ of $\mathbb{R}^n$ for which $x_1 + x_2 + \cdots + x_n = 1$ (i.e. the entries add up to 1). It is easy to verify that $(\mathbb{R}^n)_1$ is **not** a vector subspace of $(\mathbb{R}^n, +, \cdot)$.

(f) Recall now again the real vector space $(\mathcal{F}(\mathbb{R};\mathbb{R}), +, \cdot)$ defined in Lecture 2, and let $\mathcal{F}_1(\mathbb{R};\mathbb{R})$ denote the subset of $(\mathcal{F}(\mathbb{R};\mathbb{R}), +, \cdot)$ consisting of all functions $f \in (\mathcal{F}(\mathbb{R};\mathbb{R}), +, \cdot)$ for which $f(0) = 1$. It is easy to verify that $\mathcal{F}_1(\mathbb{R};\mathbb{R})$ is **not** a vector subspace of $(\mathcal{F}(\mathbb{R};\mathbb{R}), +, \cdot)$.

Vector subspaces of a given vector space have the following important property:

Theorem 3. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\mathbf{W}_1 \subset \mathbf{V}$ and $\mathbf{W}_2 \subset \mathbf{V}$ be two **vector subspaces** of $\mathbf{V}$; then their intersection $\mathbf{W}_1 \cap \mathbf{W}_2$ is also a vector subspace of $\mathbf{V}$.

Proof: To prove that $\mathbf{W}_1 \cap \mathbf{W}_2$ is a vector subspace of $\mathbf{V}$, we have to verify that $\mathbf{W}_1 \cap \mathbf{W}_2$ satisfies the three properties of a vector subspace.

(i) We begin by showing the first property, namely that the zero element $\mathbf{0}$ of $\mathbf{V}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$. Since $\mathbf{W}_1$ is by assumption a vector subspace of $\mathbf{V}$, the zero element $\mathbf{0}$ is in $\mathbf{W}_1$; similarly, since $\mathbf{W}_2$ is by assumption a vector subspace of $\mathbf{V}$, the zero element $\mathbf{0}$ is in $\mathbf{W}_2$. Hence, the zero element $\mathbf{0}$ is in $\mathbf{W}_1$ **and** in $\mathbf{W}_2$, that is, $\mathbf{0}$ is **in the intersection** $\mathbf{W}_1 \cap \mathbf{W}_2$ of $\mathbf{W}_1$ and $\mathbf{W}_2$.

(ii) Let us now prove the second property of a vector subspace, namely that for any $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_1 \cap \mathbf{W}_2$, $\mathbf{x} + \mathbf{y}$ is also in $\mathbf{W}_1 \cap \mathbf{W}_2$. For this, let us take $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_1 \cap \mathbf{W}_2$; we have to show that $\mathbf{x}+\mathbf{y}$ is also in $\mathbf{W}_1 \cap \mathbf{W}_2$. Since $\mathbf{x}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$, it is in $\mathbf{W}_1$; similarly, since $\mathbf{y}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$, it is also in $\mathbf{W}_1$. Since by assumption $\mathbf{W}_1$ is a vector subspace of $\mathbf{V}$, $\mathbf{x} + \mathbf{y}$ is also in $\mathbf{W}_1$. We now repeat this procedure for $\mathbf{W}_2$ instead of $\mathbf{W}_1$; since $\mathbf{x}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$, it is in $\mathbf{W}_2$; similarly, since $\mathbf{y}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$, it is also in $\mathbf{W}_2$. Since by assumption $\mathbf{W}_2$ is a vector subspace of $\mathbf{V}$, $\mathbf{x} + \mathbf{y}$ is also in $\mathbf{W}_2$. Hence, we have obtained that $\mathbf{x} + \mathbf{y}$ is in $\mathbf{W}_1$ **and** in $\mathbf{W}_2$; hence, $\mathbf{x} + \mathbf{y}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$.

(ii) Let us now prove the third and last property of a vector subspace, namely that for any α in $\mathbb{R}$ and any $\mathbf{x}$ in $\mathbf{W}_1 \cap \mathbf{W}_2$, then $\alpha\mathbf{x}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$. Since $\mathbf{x}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$, it is in $\mathbf{W}_1$; since by assumption $\mathbf{W}_1$ is a vector subspace of $\mathbf{V}$, $\alpha\mathbf{x}$ is also in $\mathbf{W}_1$. Similarly, since $\mathbf{x}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$, it is also in $\mathbf{W}_2$; since by assumption $\mathbf{W}_2$ is a vector subspace of $\mathbf{V}$, $\alpha\mathbf{x}$ is also in $\mathbf{W}_2$. We have therefore obtained that $\alpha\mathbf{x}$ is in $\mathbf{W}_1$ **and** in $\mathbf{W}_2$; hence, $\alpha\mathbf{x}$ is in $\mathbf{W}_1 \cap \mathbf{W}_2$.

We conclude that $\mathbf{W}_1 \cap \mathbf{W}_2$ satisfies the three properties of a vector subspace. This proves the theorem. □

Remark 1. It is important to note that if $(\mathbf{V}, +, \cdot)$ is a real vector space and $\mathbf{W}_1, \mathbf{W}_2$ two vector subspaces of $\mathbf{V}$, then their **union** $\mathbf{W}_1 \cup \mathbf{W}_2$ is in general **not** a vector subspace of $\mathbf{V}$.

PROBLEMS:

1. Consider the real vector space $(\mathbb{R}^2, +, \cdot)$ defined in Example (b) of Lecture 2. For each of the following subsets of $\mathbb{R}^2$, determine whether or not they are a **vector subspace** of $\mathbb{R}^2$:

   (a) S = set of all (x, y) in $\mathbb{R}^2$ such that $6x + 8y = 0$.

   (b) S = set of all (x, y) in $\mathbb{R}^2$ such that $6x + 8y = 1$.

   (c) S = set of all (x, y) in $\mathbb{R}^2$ such that $x = 0$.

   (d) S = set of all (x, y) in $\mathbb{R}^2$ such that $y = 0$.

   (e) S = set of all (x, y) in $\mathbb{R}^2$ such that $x = 3$.

   (f) S = set of all (x, y) in $\mathbb{R}^2$ such that $y = 5$.

   (g) S = set of all (x, y) in $\mathbb{R}^2$ such that $x^2 - y^2 = 0$.

   (h) S = set of all (x, y) in $\mathbb{R}^2$ such that $xy = 0$.

   (i) S = set of all (x, y) in $\mathbb{R}^2$ such that $xy = 1$.

2. Consider the real vector space $(\mathcal{F}(\mathbb{R}; \mathbb{R}), +, \cdot)$ defined in Example (c) of Lecture 2. For each of the following subsets of $\mathcal{F}(\mathbb{R}; \mathbb{R})$, determine whether or not they are a **vector subspace** of $\mathcal{F}(\mathbb{R}; \mathbb{R})$:

   (a) S = set of all f in $\mathcal{F}(\mathbb{R}; \mathbb{R})$ such that $f(1) = 0$.

   (b) S = set of all f in $\mathcal{F}(\mathbb{R}; \mathbb{R})$ such that $f(1) = 0$ and $f(2) = 0$.

   (c) S = set of all f in $\mathcal{F}(\mathbb{R}; \mathbb{R})$ such that $f(1) = f(2)$.

   (d) S = set of all f in $\mathcal{F}(\mathbb{R}; \mathbb{R})$ such that $f(1) = 1 + f(2)$.

   (e) S = set of all f in $\mathcal{F}(\mathbb{R}; \mathbb{R})$ such that $f(1) = f(2)$ and $f(2) = f(3)$.

   (f) S = set of all f in $\mathcal{F}(\mathbb{R}; \mathbb{R})$ such that $f(1) = f(2)$ and $f(4) = 0$.

(g) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) = 0$ for all $-1 \leq x \leq 1$.

(h) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) = 2$ for all $-1 \leq x \leq 1$.

(i) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) \geq 0$ for all $x \in \mathbb{R}$.

(j) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) > 0$ for all $x \in \mathbb{R}$.

(k) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) = f(-x)$ for all $x \in \mathbb{R}$.

(l) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) = -f(-x)$ for all $x \in \mathbb{R}$.

(m) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) + f(2x) = 0$ for all $x \in \mathbb{R}$.

(n) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) + (f(2x))^2 = 0$ for all $x \in \mathbb{R}$.

(o) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) + f(x^2 + 1) = 0$ for all $x \in \mathbb{R}$.

(p) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) + f(x^2 + 1) = 1$ for all $x \in \mathbb{R}$.

(q) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) - f(x + 1) = 0$ for all $x \in \mathbb{R}$.

(r) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) + f(x+1) + f(x+2) = 0$ for all $x \in \mathbb{R}$.

(s) S = set of all f in $\mathcal{F}(\mathbb{R};\mathbb{R})$ such that $f(x) + f(x+1) + f(x+2) = 1$ for all $x \in \mathbb{R}$.

3. For the real vector space $(\mathbb{R}^2, +, \cdot)$, defined in Example (b) of Lecture 2, give an example of two **vector subspaces** $\mathbf{V}_1$ and $\mathbf{V}_2$ such that their union $\mathbf{V}_1 \cup \mathbf{V}_2$ is **not** a vector subspace of $\mathbb{R}^2$ (See Remark 1 in this Lecture).

4. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let the subset $\mathbf{W}$ of $\mathbf{V}$ be a vector subspace of $\mathbf{V}$. Show that with the same addition operation "+" and multiplication (by a scalar) operation "·" as in $\mathbf{V}$, $\mathbf{W}$ satisfies all the properties of a real vector space, and hence, is itself (with those two operations) a real vector space.

Section 4

Study Topics

- Linear combinations of vectors
- Linear span of a finite set of vectors

We know that in a real vector space, we can **add** two vectors and **multiply a vector by a real number** (aka **scalar**). A natural question that comes to mind is: if we have a real vector space $\mathbf{V}$ and we take, say, two vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ of $\mathbf{V}$, what can we get by doing **all these possible operations** on **these two vectors**, i.e. by taking the set of **all** vectors of the form $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2$ (with α and β being real numbers) ?
We shall examine this question in this lecture, and we shall see at the end of this lecture how it relates to our original problem, that of **understanding systems of linear equations**.

Definition 14. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\mathbf{v}_1, \cdots, \mathbf{v}_p$ be a **finite** number of elements of $\mathbf{V}$ (with $p \geq 1$). The expression

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_p\mathbf{v}_p,$$

with $\alpha_1, \alpha_2, \cdots, \alpha_p$ real numbers, is called a **linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; we also sometimes call it "the linear combination of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ with respective coefficients $\alpha_1, \alpha_2, \cdots, \alpha_p$".
If an element $\mathbf{v}$ of $\mathbf{V}$ can be written as

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_p\mathbf{v}_p,$$

with $\alpha_1, \alpha_2, \cdots, \alpha_p$ real numbers, then we say that $\mathbf{v}$ is a **linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ (with respective coefficients $\alpha_1, \cdots, \alpha_p$). We denote by $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ the **set of all linear combinations of** the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, that is:

$$\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)} = \{\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_p\mathbf{v}_p | \alpha_1, \alpha_2, \cdots, \alpha_p \in \mathbb{R}\}.$$

It is clear that $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ is a **subset** of $\mathbf{V}$; indeed, since $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ are in V, multiplying them by real numbers and adding them up gives us something still in $\mathbf{V}$, since $\mathbf{V}$ is a vector space. So we can write:

$$\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)} \subset \mathbf{V}.$$

But **there is more**! Indeed, the following result shows that $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ is not just any old subset of $\mathbf{V}$; rather, it is a **vector subspace** of $\mathbf{V}$:

Proposition 1. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\mathbf{v}_1, \cdots, \mathbf{v}_p$ be a **finite** number of elements of $\mathbf{V}$ (where $p \geq 1$). The subset $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ of $\mathbf{V}$ consisting of **all linear combinations** of the vectors $\mathbf{v}_1, \cdots, \mathbf{v}_p$ is a **vector subspace** of $\mathbf{V}$.

Proof. To prove this result, we have to show that $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ satisfies the **three properties** that a vector subspace of $\mathbf{V}$ should satisfy. We verify these properties one by one:

(i) We have to show that the zero vector $\mathbf{0}$ of $\mathbf{V}$ is also an element of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$; to do this, we have to show that the zero vector $\mathbf{0}$ can be written as a **linear combination** $\alpha_1\mathbf{v}_1+\alpha_2\mathbf{v}_2+\cdots+\alpha_p\mathbf{v}_p$ of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ for **some choice** of the scalars $\alpha_1, \alpha_2, \cdots, \alpha_p$. It is clear that choosing $\alpha_1, \alpha_2, \cdots, \alpha_p$ to be all zero yields the desired linear combination; indeed, we can write:

$$\mathbf{0} = 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_p,$$

and this shows that the zero vector **0 can indeed** be expressed as a **linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; hence the zero vector $\mathbf{0}$ is an element of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$, i.e. $\mathbf{0} \in \mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$.

(ii) Let $\mathbf{x}$ and $\mathbf{y}$ be two elements of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$; we have to show that the vector $\mathbf{x}+\mathbf{y}$ is also in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$. But since by assumption $\mathbf{x}$ is in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$, it must be that

$$\mathbf{x} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p$$

for some real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$, by definition of the set $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ itself. Similarly, since by assumption $\mathbf{y}$ is in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$, it must be that

$$\mathbf{y} = \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2 + \cdots \beta_p\mathbf{v}_p$$

for some real numbers $\beta_1, \beta_2, \cdots, \beta_p$, by definition of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$. Hence, the sum $\mathbf{x}+\mathbf{y}$ of $\mathbf{x}$ and $\mathbf{y}$ can be written as:

$$\begin{aligned} \mathbf{x}+\mathbf{y} &= (\alpha_1\mathbf{v}_1 + \cdots \alpha_p\mathbf{v}_p) + (\beta_1\mathbf{v}_1 + \cdots \beta_p\mathbf{v}_p) \\ &= (\alpha_1+\beta_1)\mathbf{v}_1 + \cdots (\alpha_p+\beta_p)\mathbf{v}_p, \end{aligned}$$

which shows that $\mathbf{x}+\mathbf{y}$ **itself is a linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; hence $\mathbf{x}+\mathbf{y}$ is an element of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$, i.e. $\mathbf{x}+\mathbf{y} \in \mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$.

(iii) Let now $\mathbf{x}$ be an element of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ and γ be a real number; we have to show that the vector $\gamma\mathbf{x}$ is also in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$. Since, by assumption, $\mathbf{x}$ is in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$, it must be that

$$\mathbf{x} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p$$

for some real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$, by definition of the set $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ itself. Hence, we can write:

$$\begin{aligned} \gamma\mathbf{x} &= \gamma(\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p) \\ &= (\gamma\alpha_1)\mathbf{v}_1 + \cdots (\gamma\alpha_p)\mathbf{v}_p, \end{aligned}$$

which shows that $\gamma\mathbf{x}$ **itself is a linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; hence $\gamma\mathbf{x}$ is in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$, i.e. $\gamma\mathbf{x} \in \mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$.

We conclude that $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ satisfies all three properties of a vector subspace of $\mathbf{V}$; hence $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ is a **vector subspace** of $\mathbf{V}$. □

Before going any further, we give a name to $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$:

Definition 15. The vector subspace $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ of $\mathbf{V}$ is called the **subspace of $\mathbf{V}$ generated by the vectors $\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p$**; it is also called the **linear span of the vectors $\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p$**.

Now that $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_p)}$ has an honest name (actually two!), we examine a number of examples:

(a) Let $(\mathbf{V},+,\cdot)$ be a real vector space, and let $\mathbf{v}_1 = \mathbf{0}$ be the **zero vector** of $\mathbf{V}$. The vector subspace of $\mathbf{V}$ generated by $\mathbf{v}_1$ is clearly seen to be the **zero subspace** $\{\mathbf{0}\}$ of $\mathbf{V}$.

(b) Consider the real vector space $(\mathbb{R}^2,+,\cdot)$ defined previously, and let $\mathbf{v}_1 = (1,0)$ and $\mathbf{v}_2 = (0,1)$; it is easy to verify that the subspace of $(\mathbb{R}^2,+,\cdot)$ generated by $\mathbf{v}_1,\mathbf{v}_2$ is **$\mathbf{V}$ itself**.

(c) Consider the real vector space $(\mathbb{R}^3,+,\cdot)$ defined previously, and consider the two elements $\mathbf{v}_1 = (1,-1,0)$ and $\mathbf{v}_2 = (0,1,-1)$ of $\mathbb{R}^3$. Let us show that the vector subspace $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)}$ of $\mathbb{R}^3$ spanned by $\mathbf{v}_1$ and $\mathbf{v}_2$ is the set of all (a,b,c) in $\mathbb{R}^3$ such that $a+b+c=0$, that is, we wish to show that

$$\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)} = \{(a,b,c)\in\mathbb{R}^3 | a+b+c=0\}.$$

To show this equality, we will show first that we have the inclusion

$$\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)} \subset \{(a,b,c)\in\mathbb{R}^3 | a+b+c=0\},$$

following which we will show that we have the inclusion

$$\{(a,b,c)\in\mathbb{R}^3 | a+b+c=0\} \subset \mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)};$$

these two inclusions will, together, show the desired equality. Let us then begin by showing the first inclusion. For this, let us take an arbitrary element $\mathbf{x}$ in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)}$, and show that it is also in the set $\{(a,b,c)\in\mathbb{R}^3 | a+b+c=0\}$. By definition of $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)}$, $\mathbf{x}$ can be written as:

$$\mathbf{x} = \alpha\mathbf{v}_1 + \beta\mathbf{v}_2,$$

for some real numbers α and β. Hence, we have:

$$\begin{aligned} \mathbf{x} &= \alpha\mathbf{v}_1 + \beta\mathbf{v}_2 \\ &= \alpha(1,-1,0) + \beta(0,1,-1) \\ &= (\alpha,-\alpha,0) + (0,\beta,-\beta) \\ &= (\alpha,-\alpha+\beta,-\beta); \end{aligned}$$

clearly, since $\alpha + (-\alpha+\beta) + (-\beta) = 0$, we have that $\mathbf{x}$ is in the set $\{(a,b,c)\in\mathbb{R}^3 | a+b+c=0\}$. This proves the first inclusion.

To prove the second inclusion, let us take an arbitrary element $\mathbf{y}$ in the set $\{(a,b,c) \in \mathbb{R}^3 | a+b+c=0\}$, and show that it is also in the linear span $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)}$ of $\mathbf{v}_1$ and $\mathbf{v}_2$. Let then $\mathbf{y} = (\alpha, \beta, \gamma) \in \{(a,b,c) \in \mathbb{R}^3 | a+b+c=0\}$; since $\alpha+\beta+\gamma=0$, we deduce that $\beta = -(\alpha+\gamma)$, and hence, we can write $\mathbf{y}$ as:

$$\begin{aligned}
\mathbf{y} &= (\alpha, -(\alpha+\gamma), \gamma) \\
&= (\alpha, -\alpha-\gamma, \gamma) \\
&= (\alpha, -\alpha, 0) + (0, -\gamma, \gamma) \\
&= \alpha(1,-1,0) + (-\gamma)(0,1,-1) \\
&= \alpha\mathbf{v}_1 + (-\gamma)\mathbf{v}_2,
\end{aligned}$$

that is, $\mathbf{y}$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$ (with coefficients α and $-\gamma$, respectively) and hence is in $\mathcal{S}_{(\mathbf{v}_1,\mathbf{v}_2)}$. This proves the second inclusion, and hence, together with the first inclusion, we obtain the desired result.

We now have enough tools at our disposal to revisit our original "experiments" with systems of linear equations and to have some basic understanding of what it is that happens when a system of linear equations has a solution or has no solution. In order to make things concrete, let us consider two examples:

1. Let us begin with the following system of 3 linear equation in 2 unknowns:

$$(A)\begin{cases} x_1 - x_2 = 1, \\ 2x_1 + x_2 = 0, \\ x_1 - 2x_2 = 2, \end{cases}$$

where we wish to solve for the pair (x_1, x_2) of real numbers. Let us now recall the **real vector space** $(\widehat{\mathbb{R}^3}, +, \cdot)$ of all **column vectors** of the form $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ where a, b, c are real numbers. Consider the elements $\mathbf{v}_1, \mathbf{v}_2, \mathbf{w}$ of $\widehat{\mathbb{R}^3}$ defined as follows:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix} -1 \\ 1 \\ -2 \end{pmatrix}, \mathbf{w} = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix},$$

Let now x_1, x_2 be real numbers. We have, by definition of the operations "+" and "$\cdot$" in $\widehat{\mathbb{R}^3}$:

$$\begin{aligned}
x_1 \cdot \mathbf{v}_1 + x_2 \cdot \mathbf{v}_2 &= x_1 \cdot \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -1 \\ 1 \\ -2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ 2x_1 \\ x_1 \end{pmatrix} + \begin{pmatrix} -x_2 \\ x_2 \\ -2x_2 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 \\ 2x_1 + x_2 \\ x_1 - 2x_2 \end{pmatrix}.
\end{aligned}$$

Hence, the pair (x_1, x_2) of real numbers satisfies the system (A) of linear equations above **if and only if** we have:

$$x_1 \cdot \mathbf{v}_1 + x_2 \cdot \mathbf{v}_2 = \mathbf{w};$$

It follows immediately from this that:

- If $\mathbf{w}$ is **not** in the linear span of $\mathbf{v}_1$ and $\mathbf{v}_2$, then system (A) has **no solution**,
- if $\mathbf{w}$ **is** in the linear span of $\mathbf{v}_1$ and $\mathbf{v}_2$, then system (A) has **at least one solution** (but we can't yet tell how many!).

2. Consider now the following system of 2 linear equations in 2 unknowns:

$$(B)\left\{\begin{array}{r} x_1 - x_2 = 1, \\ -x_1 + x_2 = 1, \end{array}\right.$$

where we wish to solve for the pair (x_1, x_2) of real numbers. In order to understand whether this system has a solution or not, consider the following vectors in $\widehat{\mathbb{R}^2}$:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \mathbf{w} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Let now (x_1, x_2) be a pair of real numbers; we clearly have:

$$x_1 \cdot \mathbf{v}_1 + x_2 \cdot \mathbf{v}_2 = x_1 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 \\ -x_1 + x_2 \end{pmatrix}.$$

It follows that the pair (x_1, x_2) is a solution of system (B) **if and only if** we have:

$$x_1 \cdot \mathbf{v}_1 + x_2 \cdot \mathbf{v}_2 = \mathbf{w};$$

Hence, we again have:

- If $\mathbf{w}$ is **not** in the linear span of $\mathbf{v}_1$ and $\mathbf{v}_2$, then system (B) has **no solution**,
- if $\mathbf{w}$ **is** in the linear span of $\mathbf{v}_1$ and $\mathbf{v}_2$, then system (B) has **at least one solution** (again we can't yet tell how many!).

So we now have some basic "picture" of what it means for a system of linear equations to have, or not to have, a solution: If some given vector happens to lie in some given subspace, then the system has a solution (at least one); otherwise, it has no solution.
In order to get to a point where we can explain why that number of solutions is always 0,1, or ∞, we have to further sharpen our tools. This is what we will do in the following sections.

PROBLEMS:

1. Consider the (by now familiar) real vector space $\mathbb{R}^2$, consisting of all pairs (x, y) of real numbers, with the usual addition and scalar multiplication operations. Consider the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5$ in $\mathbb{R}^2$ defined as follows:

$$\mathbf{v}_1 = (0,0),\ \mathbf{v}_2 = (1,0),\ \mathbf{v}_3 = (-1,0),\ \mathbf{v}_4 = (0,3),\ \mathbf{v}_5 = (2,1).$$

   (a) Is $\mathbf{v}_1$ in the linear span of $\{\mathbf{v}_2\}$?
   (b) Is $\mathbf{v}_1$ in the linear span of $\{\mathbf{v}_3, \mathbf{v}_4\}$?
   (c) Is $\mathbf{v}_2$ in the linear span of $\{\mathbf{v}_1, \mathbf{v}_4\}$?
   (d) Is $\mathbf{v}_2$ in the linear span of $\{\mathbf{v}_1\}$?
   (e) Is $\mathbf{v}_2$ in the linear span of $\{\mathbf{v}_2, \mathbf{v}_4\}$?
   (f) Is $\mathbf{v}_3$ in the linear span of $\{\mathbf{v}_2\}$?
   (g) Is $\mathbf{v}_3$ in the linear span of $\{\mathbf{v}_4\}$?
   (h) Is $\mathbf{v}_4$ in the linear span of $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$?
   (i) Is $\mathbf{v}_5$ in the linear span of $\{\mathbf{v}_2\}$?
   (j) Is $\mathbf{v}_5$ in the linear span of $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$?
   (k) Is $\mathbf{v}_5$ in the linear span of $\{\mathbf{v}_2, \mathbf{v}_4\}$?
   (l) Is $\mathbf{v}_5$ in the linear span of $\{\mathbf{v}_3, \mathbf{v}_4\}$?

2. Consider the real vector space $\widehat{\mathbb{R}^4}$ (see Lecture 2) consisting of all column vectors of the form $\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$ with x, y, z, w real, with the usual addition and scalar multiplication operations. Define the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4$ in $\widehat{\mathbb{R}^4}$ as follows:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ \mathbf{v}_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ \mathbf{v}_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix},\ \mathbf{v}_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

   For each of these four vectors, determine whether they are in the linear span of the other three.

3. Consider the (familiar) real vector space $\mathbb{R}^3$ consisting of all triples of the form (x, y, z) with x, y, z real numbers, with the usual addition and scalar multiplication operations. For each of the following list of vectors in $\mathbb{R}^3$, determine whether the first vector is in the linear span of the last two:

   (a) $(1,1,1),\ (1,2,1),\ (1,3,1)$
   (b) $(0,0,0),\ (1,2,1),\ (1,3,1)$

(c) $(1,2,1),\ (1,1,1),\ (1,3,1)$

(d) $(0,1,0),\ (1,2,1),\ (1,3,1)$

(e) $(1,1,1),\ (2,5,0),\ (3,2,0)$

(f) $(1,0,1),\ (0,2,0),\ (0,3,0)$

(g) $(1,1,1),\ (0,0,0),\ (2,2,2)$

(h) $(1,1,0),\ (1,0,1),\ (0,1,1)$

(i) $(3,2,1),\ (3,2,2),\ (1,1,1)$

(j) $(0,0,0),\ (3,2,1),\ (4,3,1)$

(k) $(1,2,1),\ (2,2,1),\ (1,3,1)$

4. Consider the real vector space $\mathcal{F}(\mathbb{R};\mathbb{R})$ of all real-valued functions of a real variable (defined in Lecture 2), with the usual addition and scalar multiplication operations. Consider the elements f_1, f_2, f_3, f_4 in $\mathcal{F}(\mathbb{R};\mathbb{R})$, defined as follows:

$$\begin{aligned} f_1(t) &= \begin{cases} 0, & t < 0 \\ t, & t \geq 0 \end{cases} \\ f_2(t) &= \begin{cases} 0, & t < 0 \\ 3t+1, & t \geq 0 \end{cases} \\ f_3(t) &= \begin{cases} 0, & t < 0 \\ t^2, & t \geq 0 \end{cases} \\ f_4(t) &= \begin{cases} 0, & t < 0 \\ 3t^2+2t+1, & t \geq 0 \end{cases} \end{aligned}$$

For each of these four elements (i.e. vectors) in $\mathcal{F}(\mathbb{R};\mathbb{R})$, verify whether or not they are in the linear span of the other three.

Section 5

Study Topics

- Linear dependence of a set of vectors
- Linear independence of a set of vectors

Consider the vector space $\mathbb{R}^2$ of all pairs (x, y) of real numbers, which we have defined previously and used numerous times. Consider the following subsets of $\mathbb{R}^2$:

$$S_1 = \{(3,2),(12,8)\}, \quad S_2 = \{(3,2),(0,1)\}.$$

What are the similarities and differences between S_1 and S_2 ? Well, they both contain two vectors each; in that, they are similar; another similarity is that they both contain the vector $(3,2)$. What about differences ? Notice that the second vector in S_1, namely $(12,8)$, is a **scalar multiple** of $(3,2)$, i.e. $(12,8)$ can be obtained by multiplying $(3,2)$ by some real number (in this case, the real number 4); indeed, we have:

$$4(3,2) = (4 \times 3, 4 \times 2) = (12,8).$$

We can also obviously claim that $(3,2)$ is a scalar multiple of $(12,8)$ (this time with a factor of $\frac{1}{4}$), since we can write:

$$\frac{1}{4}(12,8) = (\frac{1}{4} \times 12, \frac{1}{4} \times 8) = (3,2).$$

On the other hand, no such thing is happening with S_2; indeed, $(0,1)$ is **not** a scalar multiple of $(3,2)$, since mutiplying $(3,2)$ by a real number can **never** yield $(0,1)$ (prove it!). Similary, multiplying $(0,1)$ by a real number can **never** yield $(3,2)$ (prove it also!).
So we have identified a fundamental difference between S_1 and S_2: Whereas the two elements of S_1 are **related**, in the sense that they are scalar multiples of one another, those of S_2 are **completely unrelated** (in the sense that they are not scalar multiples of each other).
Before going further, we generalize this observation into a definition:

Definition 16. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a **finite** subset of $\mathbf{V}$.

(i) The subset S is said to be **linearly independent** if for any $\alpha_1, \cdots, \alpha_p \in \mathbb{R}$, the relation

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0}$$

implies that $\alpha_1 = \alpha_2 = \cdots = \alpha_p = 0$.

(ii) The subset S is said to be **linearly dependent** if it is **not linearly independent**.

Equivalent ways to re-state these definitions are as follows:

(i) The subset S is **linearly independent** if the **only** real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$ which yield

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0}$$

are given by $\alpha_1 = \alpha_2 = \cdots = \alpha_p = 0$.

(ii) The subset S is **linearly independent** if **whenever** the linear combination $\alpha_1\mathbf{v}_1 + \cdots + \alpha_p\mathbf{v}_p$ is equal to $\mathbf{0}$, it **must be** that $\alpha_1, \cdots, \alpha_p$ are **all** 0.

(iii) The subset S is **linearly dependent** if there exist real numbers $\alpha_1, \cdots, \alpha_p$ **not all** 0, but for which the linear combination $\alpha_1\mathbf{v}_1 + \cdots + \alpha_p\mathbf{v}_p$ is nevertheless equal to $\mathbf{0}$.

Before going any further, let us show that the set S_1 above is a **linearly dependent** subset of $\mathbb{R}^2$, and that the set S_2 above is a **linearly independent** subset of $\mathbb{R}^2$. Let us begin with S_1: Let $\alpha_1 = -4$ and $\alpha_2 = 1$; we have:

$$\begin{aligned}\alpha_1(3,2) + \alpha_2(12,8) &= -4(3,2) + 1(12,8)\\ &= (-12,-8) + (12,8)\\ &= (0,0)\\ &= \mathbf{0}\end{aligned}$$

(recall that the zero element $\mathbf{0}$ of $\mathbb{R}^2$ is the pair $(0,0)$). Hence we have found real numbers α_1, α_2 which are not both zero but such that the linear combination $\alpha_1(3,2) + \alpha_2(12,8)$ is the zero vector $\mathbf{0} = (0,0)$ of $\mathbb{R}^2$. This proves that S_1 is a **linearly dependent** subset of $\mathbb{R}^2$.
Let us now show that the set S_2 above is a **linearly independent** subset of $\mathbb{R}^2$. To do this, we have to show that if for some real numbers α_1, α_2 we have

$$\alpha_1(3,2) + \alpha_2(0,1) = (0,0),$$

then, necessarily, we must have $\alpha_1 = 0$ and $\alpha_2 = 0$. Note that:

$$\begin{aligned}\alpha_1(3,2) + \alpha_2(0,1) &= (3\alpha_1, 2\alpha_1) + (0, \alpha_2)\\ &= (3\alpha_1, 2\alpha_1 + \alpha_2).\end{aligned}$$

Hence, if the linear combination $\alpha_1(3,2) + \alpha_2(0,1)$ is to be equal to the zero vector $(0,0)$ of $\mathbb{R}^2$, we must have $(3\alpha_1, 2\alpha_1 + \alpha_2) = (0,0)$, or, equivalently, we must have $3\alpha_1 = 0$ **and** $2\alpha_1 + \alpha_2 = 0$; the relation $3\alpha_1 = 0$ implies $\alpha_1 = 0$, and substituting this value of α_1 in the second relation yields $\alpha_2 = 0$. Hence, we have shown that if the linear combination $\alpha_1(3,2)+\alpha_2(0,1)$ is to be equal to the zero vector $(0,0)$ for some real numbers α_1 and α_2, then we **must** have $\alpha_1 = 0$ and $\alpha_2 = 0$. This proves that the subset S_2 of $\mathbb{R}^2$ is **linearly independent**.
At this point, we may wonder how these notions of linear dependence and independence tie in with our initial observations about the subsets S_1 and S_2 of $\mathbb{R}^2$, namely, that in S_1 one of the elements can be written as a scalar multiple of the other element, whereas we cannot do the same thing with the two elements of S_2; how does this relate to linear dependence and independence of the subsets ? The answer is given in the theorem below:

Theorem 4. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a **finite** subset of V. Then:

(i) If S is a **linearly dependent** subset of $\mathbf{V}$, then at least one of the elements of S can be written as a **linear combination** of the **other elements** of S;

(ii) conversely, if at least one of the elements of S can be written as a **linear combination** of the **other elements** of S, then S is a **linearly dependent** subset of $\mathbf{V}$.

Proof. Let us first prove (i): Since S is assumed **linearly dependent**, there do exist real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$ **not all** 0, such that:

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0}.$$

Since $\alpha_1, \alpha_2, \cdots, \alpha_p$ are not all equal to 0, **at least one of them** must be non-zero; Assume first that α_1 is non-zero, i.e. $\alpha_1 \neq 0$. From the above equality, we deduce:

$$\alpha_1 \mathbf{v}_1 = -\alpha_2 \mathbf{v}_2 - \alpha_3 \mathbf{v}_3 - \cdots - \alpha_p \mathbf{v}_p,$$

and multiplying both sides of this last equality by $\frac{1}{\alpha_1}$ (which we can do since $\alpha_1 \neq 0$), we obtain:

$$\mathbf{v}_1 = -\frac{\alpha_2}{\alpha_1} \mathbf{v}_2 - \frac{\alpha_3}{\alpha_1} \mathbf{v}_3 - \cdots - \frac{\alpha_p}{\alpha_1} \mathbf{v}_p,$$

which shows that $\mathbf{v}_1$ is a linear combination of $\mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_p$. Now if it is α_2 which happens to be non-zero, and not α_1, we repeat the same procedure, but with α_2 and $\mathbf{v}_2$ instead, and we obtain that $\mathbf{v}_2$ is a linear combination of $\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_4, \cdots, \mathbf{v}_p$. If instead, it is α_3 which is non-zero, then we repeat the same procedure with α_3 and $\mathbf{v}_3$; and so on. Since one of the $\alpha_1, \alpha_2, \cdots, \alpha_p$ is non-zero, we will be able to write one of the $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ as a linear combination of the others.

Let us now prove (ii): Assume then, that one of the $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ can be written as a linear combination of the others. Again, for simplicity, assume it is $\mathbf{v}_1$ which can be written as a linear combination of the other vectors, namely $\mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_p$ (if it is another vector instead of $\mathbf{v}_1$, we do the same thing for that vector); hence, there exist real numbers $\alpha_2, \alpha_3, \cdots, \alpha_p$ such that:

$$\mathbf{v}_1 = \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 + \cdots + \alpha_p \mathbf{v}_p.$$

We can write the above equality equivalently as:

$$-\mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0},$$

and, equivalently, as:

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0},$$

where $\alpha_1 = -1$; but this shows that the above linear combination is the zero vector $\mathbf{0}$, and yet not all of $\alpha_1, \alpha_2, \cdots, \alpha_p$ are 0 (for the good reason that $\alpha_1 = -1$). This shows that the subset $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ of $\mathbf{V}$ is linearly dependent.

□

We now examine a number of examples.

(a) Recall the real vector space $\widehat{\mathbb{R}^3}$ consisting of all column vectors (with 3 real entries) of the form $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$, where a, b, c are real numbers. Consider the subset S of $\widehat{\mathbb{R}^3}$ given by:

$$S = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \}.$$

Let us show that S is a **linearly independent** subset of $\widehat{\mathbb{R}^3}$: Let then $\alpha_1, \alpha_2, \alpha_3$ be three real numbers such that

$$\alpha_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix};$$

we have to show that this implies that $\alpha_1 = \alpha_2 = \alpha_3 = 0$. We have:

$$\alpha_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix},$$

and the equality

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

does imply that $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Hence, S is a linearly independent subset of $\widehat{\mathbb{R}^3}$.

(b) Recall the real vector space $\mathcal{F}(\mathbb{R};\mathbb{R})$ of all real-valued functions on $\mathbb{R}$; consider the two elements f_1, f_2 in $\mathcal{F}(\mathbb{R};\mathbb{R})$, defined as follows:

$$f_1(t) = \begin{cases} 1, & t < 0, \\ 0, & t \geq 0, \end{cases} \qquad f_2(t) = \begin{cases} 0, & t < 0, \\ 1, & t \geq 0. \end{cases}$$

We wish to show that $\{f_1, f_2\}$ is a **linearly independent** subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$. Let then α_1, α_2 be two real numbers such that

$$\alpha_1 f_1 + \alpha_2 f_2 = \mathbf{0};$$

(recall that the zero element $\mathbf{0}$ of $\mathcal{F}(\mathbb{R};\mathbb{R})$ is defined to be the constant 0 function). Hence, we must have

$$\alpha_1 f_1(t) + \alpha_2 f_2(t) = 0,$$

for all t in $\mathbb{R}$; in particular, this relation should hold for $t = 1$ and $t = -1$. But for $t = 1$, we have:

$$\alpha_1 f_1(1) + \alpha_2 f_2(1) = \alpha_2,$$

and for $t = -1$, we get:

$$\alpha_1 f_1(-1) + \alpha_2 f_2(-1) = \alpha_1.$$

Hence we must have $\alpha_2 = 0$ and $\alpha_1 = 0$, which shows that $\{f_1, f_2\}$ is a linearly independent subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$.

(c) Let $(\mathbf{V}, +, \cdot)$ be any real vector space, and let $S = \{\mathbf{0}\}$ be the subset of $\mathbf{V}$ consisting of the zero element alone. Let us show that S is a **linearly dependent** subset of $\mathbf{V}$: For this, consider the linear combination $1 \cdot \mathbf{0}$; we evidently have $1 \cdot \mathbf{0} = \mathbf{0}$; on the other hand, the (unique) coefficient of this linear combination (namely the real number 1) is non-zero. This shows that $\{\mathbf{0}\}$ is a **linearly dependent** subset of $\mathbf{V}$.

Consider now a real vector space $(\mathbf{V}, +, \cdot)$, and let S and T be two finite subsets of $\mathbf{V}$ such that $S \subset T$ (i.e. S is itself a subset of T); suppose we know that S is a **linearly dependent** subset of $\mathbf{V}$; what can we then say about T ? The following lemma does answer this question.

Lemma 4. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and S, T two **finite** subsets of $\mathbf{V}$ such that $S \subset T$. If S is linearly dependent, then T is **also** linearly dependent.

Proof. Assume S has p elements and T has q elements (necessarily, we have $q \geq p$ since S is a subset of T). Let us then write:

$$\begin{aligned} S &= \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}, \\ T &= \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p, \mathbf{v}_{p+1}, \mathbf{v}_{p+2}, \cdots, \mathbf{v}_q\}. \end{aligned}$$

Since S is by assumption a **linearly dependent** subset of $\mathbf{V}$, there do exist real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$ **not all zero**, such that the linear combination

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p$$

is equal to the zero vector $\mathbf{0}$ of $\mathbf{V}$, i.e.,

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0}.$$

But then, the linear combination

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p + 0\mathbf{v}_{p+1} + \cdots + 0\mathbf{v}_q$$

is also equal to $\mathbf{0}$, and yet, **not all** of the coefficients in the above linear combination are zero (since not all of the $\alpha_1, \alpha_2, \cdots, \alpha_p$ are zero); this proves that T is a **linearly dependent** subset of $\mathbf{V}$. □

Remark 2. Let $(\mathbf{V}, +, \cdot)$ be a real vector space. We have seen in Example (c) above that the subset $\{\mathbf{0}\}$ of $\mathbf{V}$ consisting of the zero vector alone is linearly dependent; it follows from the previous lemma that if S is any finite subset of $\mathbf{V}$ such that $\mathbf{0} \in S$, then S is linearly dependent.

Remark 3. The previous lemma also implies the following: If a finite subset S of a vector space $\mathbf{V}$ is linearly independent, then **any** subset of S is linearly independent as well.

Remark 4. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. We will sometimes write "$\mathbf{v}_1, \cdots, \mathbf{v}_p$ are linearly independent (resp. dependent) elements of $\mathbf{V}$" instead of "$\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is a linearly independent (resp. dependent) subset of $\mathbf{V}$"; the two statements in quotes are meant to say exactly the same thing. One reason we will occasionally prefer to express linear dependence or independence of $\mathbf{v}_1, \cdots, \mathbf{v}_p$ by writing a statement such as "$\mathbf{v}_1, \cdots, \mathbf{v}_p$ are linearly independent (resp. dependent)" is because this does not require $\mathbf{v}_1, \cdots, \mathbf{v}_p$ to be all distinct; if, however, we were to write "the subset $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is linearly independent (resp. dependent)", this would assume that $\mathbf{v}_1, \cdots, \mathbf{v}_p$ are all distinct. To give a concrete example, let $\mathbf{v}_1 \in \mathbf{V}$ be any element of $\mathbf{V}$. Then we can say that the vectors $\mathbf{v}_1$ and $\mathbf{v}_1$ are linearly dependent (since, for example, $(1)\cdot\mathbf{v}_1 + (-1)\cdot\mathbf{v}_1 = \mathbf{0}_V$, i.e. there is a linear combination of the vectors $\mathbf{v}_1$ and $\mathbf{v}_1$ that gives the zero vector of $\mathbf{V}$ but in which at least one coefficient is non-zero); on the other hand, the subset of $\mathbf{V}$ consisting of the vectors $\mathbf{v}_1$ and $\mathbf{v}_1$ is the subset $\{\mathbf{v}_1\}$ (not $\{\mathbf{v}_1, \mathbf{v}_1\}$ Remember that repetitions are not allowed when writing sets by listing their elements), so we would have no way of discussing the linear dependence or independence of the vectors $\mathbf{v}_1$ and $\mathbf{v}_1$ by constructing a subset of $\mathbf{V}$ from them.

Remark 5. Continuing the previous remark, it should be pointed out that when we write a statement such as "$\mathbf{v}_1, \cdots, \mathbf{v}_p$ are linearly independent (resp. dependent) elements of $\mathbf{V}$" we mean that the "collection" or "family" consisting of the vectors $\mathbf{v}_1, \cdots, \mathbf{v}_p$ is linearly independent (resp. dependent), and not that each of $\mathbf{v}_1, \cdots, \mathbf{v}_p$ is separately linearly independent (resp. dependent). In other words, the usage of the plural here is not meant in the usual sense it is commonly employed. This is because linear dependence/independence is a collective property of all the vectors involved. To give an example, a statement such as "the numbers $2, 4, 6$ are even" means that 2 is even, 4 is even, and 6 is even, whereas a statement such as "$\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly independent" means that the collection or family consisting of the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ is linearly independent, i.e. for any $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ such that $\alpha_1 \cdot \mathbf{v}_1 + \alpha_2 \cdot \mathbf{v}_2 + \alpha_3 \cdot \mathbf{v}_3 = \mathbf{0}_V$ it necessarily follows that $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

PROBLEMS:

1. Consider the following vectors in the real vector space $\mathbb{R}^2$:

$$\mathbf{v}_1 = (1, 0),\ \mathbf{v}_2 = (3, 0),\ \mathbf{v}_3 = (0, 0), \mathbf{v}_4 = (1, 1), \mathbf{v}_5 = (2, 1).$$

For each of the following finite subsets of $\mathbb{R}^2$, specify whether they are linearly dependent or linearly independent:

(a) $\{\mathbf{v}_1\}$
(b) $\{\mathbf{v}_1, \mathbf{v}_2\}$
(c) $\{\mathbf{v}_2\}$
(d) $\{\mathbf{v}_3\}$
(e) $\{\mathbf{v}_1, \mathbf{v}_4\}$
(f) $\{\mathbf{v}_2, \mathbf{v}_4\}$
(g) $\{\mathbf{v}_3, \mathbf{v}_4\}$
(h) $\{\mathbf{v}_4, \mathbf{v}_5\}$
(j) $\{\mathbf{v}_1, \mathbf{v}_4, \mathbf{v}_5\}$
(k) $\{\mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_5\}$
(l) $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_5\}$
(m) $\{\mathbf{v}_1, \mathbf{v}_5\}$

2. Consider the following vectors in the real vector space $\widehat{\mathbb{R}^4}$:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ \mathbf{v}_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ \mathbf{v}_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \ \mathbf{v}_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \ \mathbf{v}_5 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

For each of the following finite subsets of $\mathbb{R}^2$, specify whether they are linearly dependent or linearly independent:

(a) $\{\mathbf{v}_1\}$
(b) $\{\mathbf{v}_1, \mathbf{v}_2\}$
(c) $\{\mathbf{v}_2\}$
(d) $\{\mathbf{v}_3\}$
(e) $\{\mathbf{v}_1, \mathbf{v}_4\}$
(f) $\{\mathbf{v}_2, \mathbf{v}_4\}$
(g) $\{\mathbf{v}_3, \mathbf{v}_4\}$
(h) $\{\mathbf{v}_4, \mathbf{v}_5\}$
(j) $\{\mathbf{v}_1, \mathbf{v}_4, \mathbf{v}_5\}$
(k) $\{\mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_5\}$
(l) $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_5\}$
(m) $\{\mathbf{v}_1, \mathbf{v}_5\}$
(n) $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$
(o) $\{\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$

(p) $\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$

3. Consider the real vector space $(\mathcal{F}(\mathbb{R};\mathbb{R}), +, \cdot)$ defined in Lecture 2, and consider the elements f_1, f_2, f_3, f_4 in $\mathcal{F}(\mathbb{R};\mathbb{R})$, defined as follows:

$$\begin{aligned} f_1(t) &= 1, \ \forall t \in \mathbb{R}, \\ f_2(t) &= t, \ \forall t \in \mathbb{R}, \\ f_3(t) &= (t+1)^2, \ \forall t \in \mathbb{R}, \\ f_4(t) &= t^2 + 5, \ \forall t \in \mathbb{R}, \\ f_5(t) &= t^3, \ \forall t \in \mathbb{R}, \\ f_6(t) &= t^3 + 2t^2, \ \forall t \in \mathbb{R}, \end{aligned}$$

For each of the following finite subsets of $\mathcal{F}(\mathbb{R};\mathbb{R})$, specify whether they are linearly dependent or linearly independent:

(a) $\{f_1\}$

(b) $\{f_1, f_2\}$

(c) $\{f_1, f_2, f_3\}$

(d) $\{f_1, f_2, f_3, f_4\}$

(e) $\{f_2, f_3, f_4\}$

(f) $\{f_4, f_5, f_6\}$

(g) $\{f_3 f_4, f_5, f_6\}$

(h) $\{f_2, f_3, f_4, f_5, f_6\}$

(j) $\{f_1, f_2, f_3, f_4, f_5, f_6\}$

4. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\{\mathbf{v}_1, \mathbf{v}_2\}$ be a linearly independent subset of $\mathbf{V}$. Let $\mathbf{w}_1, \mathbf{w}_2 \in \mathbf{V}$ be defined by $\mathbf{w}_1 = \mathbf{v}_1 + \mathbf{v}_2$, $\mathbf{w}_2 = \mathbf{v}_1 - \mathbf{v}_2$. Show that $\{\mathbf{w}_1, \mathbf{w}_2\}$ is a linearly independent subset of $\mathbf{V}$.

5. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let S be a finite subset of $\mathbf{V}$. Show directly (without using Lemma 1 or Remark 2 of these lectures) that if $\mathbf{0}$ is in S then S is a linearly dependent subset of V.

Section 6

Study Topics

- Linear dependence/independence and linear combinations
- Application to systems of linear equations (or, **we now have the complete answer to our initial question!**)

Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. We know that **if** the element $\mathbf{v}$ of $\mathbf{V}$ is in the **linear span** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, then $\mathbf{v}$ can be written as **some** linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, that is, we can find real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$ such that

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p = \mathbf{v};$$

A very natural question at this point is: **In how many different ways** can this same $\mathbf{v}$ be expressed as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$? Does there exist **another** $p-$tuple of real numbers, say $(\gamma_1, \gamma_2, \cdots, \gamma_p)$, **distinct** from the $p-$tuple $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ such that we also have

$$\gamma_1\mathbf{v}_1 + \gamma_2\mathbf{v}_2 + \cdots \gamma_p\mathbf{v}_p = \mathbf{v} \ ?$$

The complete answer to this question is given in the following theorems:

Theorem 5. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. Let $\mathbf{v} \in \mathbf{V}$ be in the **linear span** of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$. If S is a **linearly independent** subset of $\mathbf{V}$, then $\mathbf{v}$ can be expressed only in a **unique** way as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; i.e., there is a **unique** $p-$tuple $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ of real numbers such that:

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p = \mathbf{v};$$

Proof. To prove this result, we have to show that if $\mathbf{v}$ (which is assumed to be in the linear span of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$) can be expressed as two linear combinations of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, then those two linear combinations must be one and the same. Assume then that we have two $p-$tuples of real numbers $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ and $(\gamma_1, \gamma_2, \cdots, \gamma_p)$ such that

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p = \mathbf{v}$$

and

$$\gamma_1\mathbf{v}_1 + \gamma_2\mathbf{v}_2 + \cdots \gamma_p\mathbf{v}_p = \mathbf{v}.$$

We have to show that the $p-$tuples $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ and $(\gamma_1, \gamma_2, \cdots, \gamma_p)$ are equal, i.e. that $\alpha_1 = \gamma_1$, $\alpha_2 = \gamma_2$, $\cdots$, $\alpha_p = \gamma_p$. This will show (obviously!) that those two linear combinations are exactly the same. Now these last two equalities imply:

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p = \gamma_1\mathbf{v}_1 + \gamma_2\mathbf{v}_2 + \cdots \gamma_p\mathbf{v}_p,$$

which then implies (by putting everything on the left-hand side of the "=" sign):

$$(\alpha_1 - \gamma_1)\mathbf{v}_1 + (\alpha_2 - \gamma_2)\mathbf{v}_2 + \cdots (\alpha_p - \gamma_p)\mathbf{v}_p = \mathbf{0};$$

but by **linear independence** of $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$, we **must** have:

$$(\alpha_1 - \gamma_1) = (\alpha_2 - \gamma_2) = \cdots = (\alpha_p - \gamma_p) = 0,$$

which, equivalently, means:

$$\begin{aligned}\alpha_1 &= \gamma_1,\\ \alpha_2 &= \gamma_2,\\ &\cdots\\ \alpha_p &= \gamma_p,\end{aligned}$$

i.e. the two linear combinations

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p = \mathbf{v}$$

and

$$\gamma_1\mathbf{v}_1 + \gamma_2\mathbf{v}_2 + \cdots \gamma_p\mathbf{v}_p = \mathbf{v}.$$

are **one and the same**. □

Conversely, we have the following:

Theorem 6. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. Assume that any $\mathbf{v} \in \mathbf{V}$ that is in the **linear span** of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ can be expressed **only in a unique way** as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; i.e., for any $\mathbf{v} \in \mathcal{S}_{(\mathbf{v}_1, \cdots, \mathbf{v}_p)}$ there is a **unique** $p-$tuple $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ of real numbers such that:

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p = \mathbf{v};$$

Then, S is a **linearly independent** subset of $\mathbf{V}$.

Proof. Consider the zero vector $\mathbf{0}$ of $\mathbf{V}$, and Let $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{R}$ be such that

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_p\mathbf{v}_p = \mathbf{0};$$

to show that S is linearly independent, we have to show that this last equality implies that $\alpha_1, \alpha_2, \cdots, \alpha_p$ are all zero. Note first that $\mathbf{0}$ is in the linear span of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; indeed, we can write:

$$\mathbf{0} = 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_p.$$

Since we have assumed that any element in the linear span of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ can be written only in a unique way as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, and since we have written $\mathbf{0}$ as the following linear combinations of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$:

$$\begin{aligned}\mathbf{0} &= \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_p\mathbf{v}_p,\\ \mathbf{0} &= 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_p,\end{aligned}$$

it follows that these two linear combinations must be one and the same, i.e. their respective coefficients must be equal, i.e., we must have:

$$\begin{aligned} \alpha_1 &= 0, \\ \alpha_2 &= 0, \\ &\cdots \\ \alpha_p &= 0. \end{aligned}$$

Hence, to summarize the previous steps, we have shown that

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{0}$$

implies $\alpha_1 = \alpha_2 = \cdots = \alpha_p = 0$. This proves that S is a **linearly independent** subset of $\mathbf{V}$. □

Now that we know the full story for the case when S is a linearly independent subset of $\mathbf{V}$, let us examine the case when S is a **linearly dependent** subset of $\mathbf{V}$:

Theorem 7. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. Let $\mathbf{v} \in \mathbf{V}$ be in the **linear span** of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$. If S is a **linearly dependent** subset of $\mathbf{V}$, then $\mathbf{v}$ can be expressed in **infinitely many** distinct ways as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; i.e., there exist **infinitely many** distinct $p-$tuples $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ of real numbers such that:

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots \alpha_p \mathbf{v}_p = \mathbf{v};$$

Proof. Let us assume then that the finite subset $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ of $\mathbf{V}$ is **linearly dependent**, and let $\mathbf{v}$ be any element in the linear span of S. We have to "produce" or "manufacture" **infinitely many** distinct $p-$tuples of real numbers $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ for which we have:

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots \alpha_p \mathbf{v}_p = \mathbf{v}.$$

Since $\mathbf{v}$ is assumed to be in the linear span of S, we know that there is **at least one** such $p-$tuple. Let that $p-$tuple be $(\lambda_1, \cdots, \lambda_p)$ (to change symbols a bit!), i.e. assume we have

$$\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \cdots \lambda_p \mathbf{v}_p = \mathbf{v}.$$

Since $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ is assumed to be a **linearly dependent** subset of $\mathbf{V}$, we know (**by definition** of linear dependence) that there exist real numbers $\beta_1, \beta_2, \cdots, \beta_p$ **not all** 0, such that:

$$\beta_1 \mathbf{v}_1 + \beta_2 \mathbf{v}_2 + \cdots + \beta_p \mathbf{v}_p = \mathbf{0}.$$

Consider now **for each real number** μ the $p-$tuple of real numbers given by:

$$(\lambda_1 + \mu\beta_1, \lambda_2 + \mu\beta_2, \cdots, \lambda_p + \mu\beta_p);$$

since at least one of $\beta_1, \beta_2, \cdots, \beta_p$ is non-zero, we obtain **infinitely many** distinct $p-$tuples of real numbers in this way, one for each $\mu \in \mathbb{R}$. To see this, note that the entry in the $p-$tuple

$$(\lambda_1 + \mu\beta_1, \lambda_2 + \mu\beta_2, \cdots, \lambda_p + \mu\beta_p)$$

corresponding to that particular β_i which is non-zero will vary as μ varies, and will never have the same value for two different values of μ.
Finally, note that for each μ in $\mathbb{R}$, the $p-$tuple of real numbers

$$(\lambda_1 + \mu\beta_1, \lambda_2 + \mu\beta_2, \cdots, \lambda_p + \mu\beta_p)$$

yields:

$$\begin{aligned}(\lambda_1 + \mu\beta_1)\mathbf{v}_1 + \cdots + (\lambda_p + \mu\beta_p)\mathbf{v}_p &= (\lambda_1\mathbf{v}_1 + \cdots + \lambda_p\mathbf{v}_p) \\ &+ \mu(\beta_1\mathbf{v}_1 + \cdots + \beta_p\mathbf{v}_p) \\ &= \mathbf{v} + \mu\mathbf{0} \\ &= \mathbf{v}.\end{aligned}$$

This last calculation shows that the linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ with coefficients given by the entries of the $p-$tuple $(\lambda_1 + \mu\beta_1, \cdots, \lambda_p + \mu\beta_p)$ yields the vector $\mathbf{v}$; since we have shown that there are **infinitely many distinct** $p-$tuples $(\lambda_1 + \mu\beta_1, \cdots, \lambda_p + \mu\beta_p)$ (one for each μ in $\mathbb{R}$), this shows that $\mathbf{v}$ can be written as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ in **infinitely many** distinct ways. □

Conversely, we have the following:

Theorem 8. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. Assume that there exists a vector $\mathbf{v} \in \mathbf{V}$ which is in the **linear span** of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ and such that it can be expressed as **two distinct linear combinations** of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, i.e. there exist two **distinct** $p-$tuples $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ and $(\beta_1, \beta_2, \cdots, \beta_p)$ of real numbers such that:

$$\begin{aligned}\mathbf{v} &= \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots \alpha_p\mathbf{v}_p, \\ \mathbf{v} &= \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2 + \cdots \beta_p\mathbf{v}_p;\end{aligned}$$

Then, S is a **linearly dependent** subset of $\mathbf{V}$.

Proof. Subtracting the second linear combination from the first yields:

$$\mathbf{0} = \mathbf{v} - \mathbf{v} = (\alpha_1 - \beta_1)\mathbf{v}_1 + (\alpha_2 - \beta_2)\mathbf{v}_2 + \cdots (\alpha_p - \beta_p)\mathbf{v}_p,$$

and since the two $n-$tuples $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ and $(\beta_1, \beta_2, \cdots, \beta_p)$ are assumed distinct, there should be some integer i in $\{1, 2, \cdots, p\}$ such that $\alpha_i \neq \beta_i$, i.e. such that $(\alpha_i - \beta_i) \neq 0$; but this implies that the above linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ is equal to the zero vector $\mathbf{0}$ but does not have all its coefficients zero; as a result, S is **linearly dependent**. □

APPLICATIONS TO SYSTEMS OF LINEAR EQUATIONS

We can now give a **complete answer** to our initial question:

- **why** is it that a system of linear equations can have **only** 0,1, or infinitely many solutions ?

Consider then the system of linear equations

$$(E)\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + \cdots a_{3n}x_n = b_3 \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots a_{mn}x_n = b_m \end{cases}$$

where the a_{ij} and the b_k are given real numbers. We would like to know how many distinct $n-$tuples $(x_1, x_2, \cdots, x_n)$ of real numbers are a solution to that system of equations (i.e. satisfy all the equalities above).
In order to answer this question using the tools we have developed, consider the real vector space $(\widehat{\mathbb{R}^m}, +, \cdot)$ which we are by now familiar with, and consider the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ in $\widehat{\mathbb{R}^m}$ defined as follows:

$$\mathbf{v}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \cdots \\ a_{m1} \end{pmatrix}, \ \mathbf{v}_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \\ \cdots \\ a_{m2} \end{pmatrix}, \ \cdots, \ \mathbf{v}_n = \begin{pmatrix} a_{1n} \\ a_{2n} \\ a_{3n} \\ \cdots \\ a_{mn} \end{pmatrix},$$

as well as the vector $\mathbf{w}$ in $\widehat{\mathbb{R}^m}$ defined as:

$$\mathbf{w} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \cdots \\ b_m \end{pmatrix}.$$

It is clear that the $n-$tuple of real numbers $(x_1, x_2, \cdots, x_n)$ is a **solution** to the system (E) of linear equations above **if and only if** it satisfies:

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n = \mathbf{w}.$$

We can therefore state:

- **If w** is **not** in the linear span of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, then there is **no** $n-$tuple of real numbers $(x_1, x_2, \cdots, x_n)$ satisfying the equality $x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n = \mathbf{w}$; in this case therefore, the system of linear equations (E) has **NO SOLUTION**;

- **If** now **w is** in the linear span of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, then there are 2 subcases:
  - If the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ are **linearly independent**, then there is a **unique** $n-$tuple of real numbers $(x_1, x_2, \cdots, x_n)$ satisfying the equality $x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n = \mathbf{w}$; in this case therefore, the system of linear equations (E) has a **UNIQUE SOLUTION**;
  - If on the other hand the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ are **linearly dependent**, then there are **infinitely many** $n-$tuples of real numbers $(x_1, x_2, \cdots, x_n)$ satisfying the equality $x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n = \mathbf{w}$; in this case therefore, the system of linear equations (E) has **INFINITELY MANY SOLUTIONS**;

PROBLEMS:

1. For each of the following systems of linear equations, study the number of solutions by formulating and analyzing the corresponding linear algebra problem, as done in the last section of this Lecture under the heading "Application to Systems of Linear Equations".

   (a)
   $$\begin{cases} 2x = 4, \\ 4x = 5, \end{cases}$$

   (b)
   $$\begin{cases} 2x = 4, \\ 4x = 8, \end{cases}$$

   (c)
   $$\left\{ \; 0x = 1, \right.$$

   (d)
   $$\left\{ \; 0x = 0, \right.$$

   (e)
   $$\begin{cases} 2x + y = 1, \\ 10x + 5y = 5, \\ x - y = 1, \end{cases}$$

   (f)
   $$\begin{cases} x + y - z = 0, \\ x + y = 1, \\ y + z = 2, \end{cases}$$

(g)

$$\begin{cases} x+y-z-w=0, \\ x+y=2, \end{cases}$$

(h)

$$\begin{cases} x+y-z-w=0, \\ -x-y=2, \\ z+w=3, \end{cases}$$

(i)

$$\begin{cases} 2x+y=1, \\ 4x+2y=2, \end{cases}$$

(j)

$$\begin{cases} 2x+y=1, \\ 4x+2y=3, \end{cases}$$

(k)

$$\begin{cases} 2x+y=1, \\ x=1, \end{cases}$$

(l)

$$\begin{cases} 2x+y=1, \\ y=0, \end{cases}$$

(m)

$$\{ \; x+y+z=1,$$

(n)

$$\begin{cases} x+y+z=1, \\ x=0 \end{cases}$$

(o)

$$\begin{cases} x+y+z=1, \\ x=0 \\ y=0 \\ z=0 \end{cases}$$

(p)

$$\begin{cases} x+y+z=1, \\ x=0 \\ y=0 \end{cases}$$

(q)

$$\begin{cases} x+y+z=1, \\ 2x+2y+2z=2 \\ y=0 \end{cases}$$

(r)

$$\begin{cases} x+y+z=1, \\ 2x+2y+2z=2 \\ x=0 \\ y=0 \end{cases}$$

(s)

$$\begin{cases} x+y+z=1, \\ 2x+2y+2z=2 \\ x=0 \\ y=0 \\ z=0 \end{cases}$$

Section 7

Study Topics

- Systems of linear equations in upper triangular form
- Solution by back-substitution
- Gaussian Elimination to put systems of linear equations in upper triangular form
- Augmented matrix of a system of linear equations
- Elementary Row operations

We now take a little pause from theory and examine a **quick and efficient** approach to **solving systems of linear equations**. Recall that in Section 1, we solved systems of linear equations using the ad hoc (and quite primitive!) procedure of isolating one variable from one of the equations, substituting its expression in terms of the other variables in all other equations, and repeating the procedure. Such a scheme could be suitable for small systems of linear equations (i.e. having few equations and few unknowns), but quickly becomes unwieldy for larger systems of linear equations. In this section, we will learn a systematic approach to solving such systems. The approach we will learn is often called "Gaussian Elimination and Substitution". To motivate the approach, we begin with a few examples.
Consider first the system of linear equations given by

$$\begin{aligned} x_1 + 3x_2 - 4x_3 + 2x_4 &= 5, \\ x_2 + 3x_3 - 2x_4 &= 1, \\ x_3 + 4x_4 &= 2, \\ 2x_4 &= 6. \end{aligned}$$

Such a system is said to be in **upper-triangular form** or **row-echelon form** since (beyond the obvious fact of its appearance) it has the property that the coefficient of the first variable (namely x_1) is zero on row 2 and beyond, the coefficient of the second variable (namely x_2) is zero on row 3 and beyond, the coefficient of the third variable (namely x_3) is zero on row 4 and beyond, ... (and this is precisely what gives it its "triangular" appearance!).
Solving a system of linear equations which is in upper-triangular (aka row-echelon) form is extremely easy, and is accomplished through a process known as **back-substitution**. To illustrate this process, we return to our example above. We **begin with the last row** and **gradually make our way up** (this is precisely where the "back" in "back-substitution" comes from). The equation on the last row is given by

$$2x_4 = 6,$$

from which we immediately obtain that $x_4 = 3$. We now **substitute** this value of x_4 that we just obtained in all other equations, and we obtain:

$$\begin{aligned} x_1 + 3x_2 - 4x_3 + 6 &= 5, \\ x_2 + 3x_3 - 6 &= 1, \\ x_3 + 12 &= 2, \end{aligned}$$

which, after rearranging, yields the system of linear equations:

$$\begin{aligned} x_1 + 3x_2 - 4x_3 &= -1, \\ x_2 + 3x_3 &= 7, \\ x_3 &= -10. \end{aligned}$$

Note that this system of linear equations now involves only the variables x_1, x_2, x_3 (since we already solved for x_4), and is also in upper-triangular (aka row-echelon) form. We begin again with the last row. The equation on the last row is given by

$$x_3 = -10,$$

which yields directly that $x_3 = -10$. We now **substitute** this value of x_3 that we just obtained in all other equations, and we obtain:

$$\begin{aligned} x_1 + 3x_2 + 40 &= -1, \\ x_2 - 30 &= 7, \end{aligned}$$

which, after rearranging, yields the system of linear equations:

$$\begin{aligned} x_1 + 3x_2 &= -41, \\ x_2 &= 37. \end{aligned}$$

Note that this system of linear equations now involves only the variables x_1, x_2 (since we already solved for x_3 and x_4), and is also in upper-triangular form. We begin again with the last row. The equation on the last row is given by

$$x_2 = 37,$$

which yields directly that $x_2 = 37$. We now **substitute** this value of x_2 that we just obtained into the first equation (since it is the only equation left!), and we obtain:

$$x_1 + 111 = -41,$$

which, after rearranging, yields the system of linear equations

$$x_1 = -152.$$

We have therefore solved our original system, and we have found that the **unique solution** to our system is given by $(x_1, x_2, x_3, x_4) = (-152, 37, -10, 3)$. The important thing to note is how systematic and painless the whole procedure was.

We now examine yet another example. Consider the system of linear equations given by:

$$\begin{aligned} 2x_1 + 4x_2 - x_3 + 3x_4 &= 8, \\ x_3 - x_4 &= 6. \end{aligned}$$

This is again a system of linear equations in upper-triangular (aka row-echelon) form; indeed, the coefficient of the first variable (namely x_1) is zero in the second equation. Solving for x_3 in the second equation yields

$$x_3 = x_4 + 6,$$

and **substituting** this value of x_3 into the first equation yields

$$2x_1 + 4x_2 - (x_4 + 6) + 3x_4 = 8,$$

i.e., after rearranging,

$$2x_1 + 4x_2 + 2x_4 - 6 = 8,$$

and solving for x_1 in this equation yields

$$x_1 = -2x_2 - x_4 + 7.$$

We have thus obtained that **for any** real numbers x_2 and x_4, the 4−tuple of real numbers given by

$$(-2x_2 - x_4 + 7, x_2, x_4 + 6, x_4)$$

is a solution to our system of linear equations. Note that this system has **infinitely many solutions** (we sometimes say that we have parametrized our solutions by x_2 and x_4).
Let us examine one last example; consider the system of linear equations given by

$$\begin{aligned} 2x_1 + x_2 - x_3 &= 5, \\ 0x_3 &= 2. \end{aligned}$$

This is again a system of linear equations in upper-triangular form; indeed, the coefficient of the first variable (namely x_1) is zero in the second equation. Solving for x_3 in the second equation yields **no solution**; indeed there is no real number x_3 that satisfies $0x_3 = 2$. We conclude therefore that this system of linear equations has **no solution**.
It is now quite clear from the few examples we have seen that systems of linear equations in upper-triangular form are very easy to solve thanks to the back-substitution scheme, and that the fact that the system happens to have a unique solution, infinitely many solutions, or no solution at all, appears clearly during the back-substitution process.
Now that we have seen the benefit of systems of linear equations in upper-triangular form, a natural question we can ask ourselves is whether given a system of linear equations, we can somehow "transform it into upper-triangular form" in such a way that the solutions remain exactly the same as for the original system; can such a transformation always be done ? The answer is a deafening "YES", and before introducing the systematic scheme for transforming any system of linear equations in upper triangular form, we motivate it on a simple example.
Consider therefore the system of linear equations given by

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ 4x_1 + x_2 + 3x_3 &= 2, \\ 6x_1 + x_2 + 4x_3 &= 0. \end{aligned}$$

Let us multiply the first row by -2 and add the result to the second row; denoting row 1 by $R1$, row 2 by $R2$, and row 3 by $R3$, the operation we are describing consists of replacing $R2$ by $-2R1+R2$. We shall denote this operation as follows:

$$-2R1 + R2 \to R2.$$

After this operation, our system becomes:

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ 0x_1 - x_2 + x_3 &= -8, \\ 6x_1 + x_2 + 4x_3 &= 0. \end{aligned}$$

To see that this system has exactly the same solution (or solutions) as our original system, note that we can go back to our original system from this system by replacing the second row with 2 times row 1 + row 2. Whenever two systems of linear equations have exactly the same solutions, we say that they are **equivalent**. By the row operation described by

$$-2R1 + R2 \to R2,$$

we have therefore gone from our original system of linear equations to an equivalent system. Consider now the (equivalent) system we have obtained:

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ 0x_1 - x_2 + x_3 &= -8, \\ 6x_1 + x_2 + 4x_3 &= 0. \end{aligned}$$

Let us multiply the first row by -3 and add the result to the third row; the operation we are describing consists of replacing $R3$ by $-3R1 + R3$, and can be denoted as follows:

$$-3R1 + R3 \to R3.$$

After this operation, our system becomes:

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ 0x_1 - x_2 + x_3 &= -8, \\ 0x_1 - 2x_2 + x_3 &= -15, \end{aligned}$$

which we can also rewrite (by eliminating the terms having coefficient 0) as:

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ -x_2 + x_3 &= -8, \\ -2x_2 + x_3 &= -15. \end{aligned}$$

Note again that this system is equivalent to the previous one, and therefore, to our original system. The solutions to this last system are exactly those of our original system, and vice-versa. Note also that this system is **not** upper-triangular, but we're **almost there**! To get there, let us now multiply the second row by -2 and add the result to the third row; the operation we are describing consists of replacing $R3$ by $-2R2 + R3$, and we shall denote it as follows:

$$-2R2 + R3 \to R3.$$

After this operation, our system becomes:

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ -x_2 + x_3 &= -8, \\ -x_3 &= 1. \end{aligned}$$

Note again that this system is equivalent to the previous one, and therefore to our original system, and that this last system is now indeed in upper-triangular form; we can now easily solve this system by back-substitution, and we obtain that the unique solution of this system, and hence of our original system, is given by the triple $(x_1, x_2, x_3) = (-1/2, 7, -1)$.
Let us now describe a **systematic approach** that captures what we have done; this process is known as **Gaussian Elimination**. Before we get there however, we need some more terminology.

Definition 17. Consider the system of linear equations in m equations and n unknowns given by

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots a_{1,n}x_n &= b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots a_{2,n}x_n &= b_2, \\ &\cdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots a_{m,n}x_n &= b_m. \end{aligned}$$

The **augmented matrix** of this system is the table of real numbers with m rows and $n+1$ columns given by

$$\begin{pmatrix} a_{1.1} & a_{1,2} & \cdots & a_{1,n} & | & b_1 \\ a_{2.1} & a_{2,2} & \cdots & a_{2,n} & | & b_2 \\ & & \cdots & & & \\ a_{m.1} & a_{m,2} & \cdots & a_{m,n} & | & b_m \end{pmatrix}.$$

(Note: The vertical bars "|" in this table are meant to visually separate the coefficients that multiply the unknowns from those that appear on the right-hand side of the equation).

For example, the augmented matrix corresponding to the system of linear equations

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 5, \\ 4x_1 + x_2 + 3x_3 &= 2, \\ 6x_1 + x_2 + 4x_3 &= 0. \end{aligned}$$

is given by the table (with 3 rows and 4 columns):

$$\begin{pmatrix} 2 & 1 & 1 & | & 5 \\ 4 & 1 & 3 & | & 2 \\ 6 & 1 & 4 & | & 0 \end{pmatrix}.$$

It is important to note that, conversely, an $m \times (n+1)$ table of real numbers of the form

$$\begin{pmatrix} a_{1.1} & a_{1,2} & \cdots & a_{1,n} & | & b_1 \\ a_{2.1} & a_{2,2} & \cdots & a_{2,n} & | & b_2 \\ & & \cdots & & & \\ a_{m.1} & a_{m,2} & \cdots & a_{m,n} & | & b_m \end{pmatrix}.$$

uniquely defines a system of m linear equations in n unknowns, namely the system:

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots a_{1,n}x_n = & \quad b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots a_{2,n}x_n = & \quad b_2, \\ & \quad \cdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots a_{m,n}x_n = & \quad b_m. \end{aligned}$$

Hence, we can represent any system of linear equations by its augmented matrix, and vice-versa.
We now define what it means for a system of linear equations – or, equivalently, its augmented matrix, to be in upper-triangular, aka row-echelon form:

Definition 18. The augmented matrix

$$\begin{pmatrix} a_{1.1} & a_{1,2} & \cdots & a_{1,n} & | & b_1 \\ a_{2.1} & a_{2,2} & \cdots & a_{2,n} & | & b_2 \\ & & \cdots & & & \\ a_{m.1} & a_{m,2} & \cdots & a_{m,n} & | & b_m \end{pmatrix}.$$

is said to be in **row-echelon form** if the following two conditions are met:

1. Each row with all entries equal to 0 is below every row having at least one nonzero entry,

2. the leftmost non-zero entry on each row is to the right of the leftmost non-zero entry of the preceding row.

For example, the augmented matrices

$$\begin{pmatrix} 2 & 1 & 1 & | & 5 \\ 0 & 1 & 3 & | & 2 \\ 0 & 0 & 3 & | & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 1 & | & 5 \\ 0 & 0 & 0 & | & 2 \\ 0 & 0 & 0 & | & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 1 & 3 & | & 5 \\ 0 & 0 & 3 & 2 & | & 2 \\ 0 & 0 & 0 & 3 & | & 0 \end{pmatrix}$$

are in row-echelon form, whereas the augmented matrices

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

are not.
We now formalize the operations we performed on the system of linear equations that we began with in order to put it in upper-triangular form. We define some more terminology.

Definition 19. Let

$$\left(\begin{array}{cccc|c} a_{1.1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2.1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ & & \cdots & & \\ a_{m.1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{array}\right).$$

be the augmented matrix of a system of linear equations. An **elementary row operation** on this table consists of one of the following operations:

1. Multiplying a given row by a **non-zero** scalar;
2. Exchanging **any two** rows;
3. Adding to a given row a scalar multiple of any **other** row.

The key results (which we shall prove later, when dealing with matrices) are the following:

Theorem 9. let T be the augmented matrix corresponding to a system of linear equations, and let T' be the augmented matrix obtained from T by a **sequence of elementary row operations**. The system of linear equations corresponding to T' is **equivalent** to the system of linear equations corresponding to T (i.e. they have exactly the same solutions).

Theorem 10. let T be the augmented matrix corresponding to a system of linear equations; then **there does exist a sequence of elementary row operations** (by no means unique) such that the augmented matrix T' obtained from T by that sequence of elementary row operations is in **row-echelon form**.

In light of these two theorems, the **Gaussian elimination/substitution** procedure for systematically solving systems of linear equations can be described as follows:

Step 1: **Write down the augmented matrix** of the system of linear equations;

Step 2: **Transform the augmented matrix in row-echelon form** through a **sequence of elementary row operations**;

Step 3: **Solve the system corresponding to the row-echelon augmented matrix** obtained in Step 2 by **back-substitution**.

We now illustrate this approach on a number of examples:

1. Consider the system of linear equations given by:

$$\begin{aligned} x_2 + x_3 &= 1, \\ 2x_1 + x_2 - x_3 &= 0, \\ 4x_1 + x_2 + 2x_3 &= 5. \end{aligned}$$

Step 1: The augmented matrix of this system is the 3×4 table given by:

$$\left(\begin{array}{cccc} 0 & 1 & 1 & | & 1 \\ 2 & 1 & -1 & | & 0 \\ 4 & 1 & 2 & | & 5 \end{array} \right).$$

Step 2: We put this augmented matrix in row-echelon form through a sequence of elementary row operations. Exchanging rows 1 and 2 (we denote this by $R1 \leftrightarrow R2$) yields the augmented matrix

$$\left(\begin{array}{cccc} 2 & 1 & -1 & | & 0 \\ 0 & 1 & 1 & | & 1 \\ 4 & 1 & 2 & | & 5 \end{array} \right).$$

Let us now multiply row 1 by -2 and add the result to row 3 (we denote this by $-2R1 + R3 \to R3$); we obtain the augmented matrix

$$\left(\begin{array}{cccc} 2 & 1 & -1 & | & 0 \\ 0 & 1 & 1 & | & 1 \\ 0 & -1 & 4 & | & 5 \end{array} \right).$$

Let us now add row 2 to row 3 (we denote this by $R2 + R3 \to R3$); we obtain the augmented matrix

$$\left(\begin{array}{cccc} 2 & 1 & -1 & | & 0 \\ 0 & 1 & 1 & | & 1 \\ 0 & 0 & 5 & | & 6 \end{array} \right).$$

This augmented matrix is now in row-echelon form, and it corresponds to the following system of linear equations:

$$\begin{aligned} 2x_1 + x_2 - x_3 &= 0, \\ x_2 + x_3 &= 1, \\ 5x_3 &= 6. \end{aligned}$$

Step 3: Solving this last system by back-substitution yields $x_3 = \frac{6}{5}$, $x_2 = -\frac{1}{5}$, $x_1 = \frac{7}{10}$. Hence, we can state that the unique solution of our original system of linear equations is given by $(x_1, x_2, x_3) = (\frac{7}{10}, -\frac{1}{5}, \frac{6}{5})$.

2. Consider now the system of linear equations given by:

$$\begin{aligned} x_2 + x_3 &= 2, \\ 2x_2 + 2x_3 &= 2, \\ x_1 + x_3 &= 1. \end{aligned}$$

Step 1: The augmented matrix of this system is the 3×4 table given by:

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

Step 2: We put this augmented matrix in row-echelon form through a sequence of elementary row operations. Exchanging rows 1 and 3 (we denote this by $R1 \leftrightarrow R3$) yields the augmented matrix

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

Let us now multiply row 2 by $-1/2$ and add the result to row 3 (we denote this by $-\frac{1}{2}R2 + R3 \to R3$); we obtain the augmented matrix

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

This augmented matrix is now in row-echelon form, and it corresponds to the following system of linear equations:

$$\begin{aligned} x_1 + x_3 &= 1, \\ 2x_2 + 2x_3 &= 2, \\ 0x_3 &= 1. \end{aligned}$$

Step 3: Solving this last system by back-substitution involves first solving for x_3 from the equation $0x_3 = 1$. Clearly there is no real number that satisfies this equation. We conclude that our original system of linear equations has no solution.

3. Consider now the system of linear equations given by:

$$\begin{aligned} x_1 + x_3 - x_4 &= 2, \\ 2x_1 + 2x_4 &= 0, \\ x_1 + x_2 - x_4 &= 1. \end{aligned}$$

Step 1: The augmented matrix of this system is the 3×5 table given by:

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & -1 & 2 \\ 2 & 0 & 0 & 2 & 0 \\ 1 & 1 & 0 & -1 & 1 \end{array}\right).$$

Step 2: We put this augmented matrix in row-echelon form through a sequence of elementary row operations. Let us multiply row 1 by -2 and add the result to row 2 (we denote this by $-2R1 + R2 \to R2$); we obtain the augmented matrix

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & -2 & 4 & -4 \\ 1 & 0 & 0 & -1 & 1 \end{array}\right).$$

This augmented matrix is not in row-echelon form yet; let us now multiply row 1 by -1 and add the result to row 3 (we denote this by $-R1 + R3 \to R3$); we obtain the augmented matrix

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & -2 & 4 & -4 \\ 0 & 0 & -1 & 0 & -1 \end{array}\right).$$

This augmented matrix is still not in row-echelon form yet; let us now multiply row 2 by $-1/2$ and add the result to row 3 (we denote this by $-\frac{1}{2}R2 + R3 \to R3$); we obtain the augmented matrix

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & -2 & 4 & -4 \\ 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

and this augmented matrix is now indeed in row-echelon form, and it corresponds to the linear system of equations

$$\begin{aligned} x_1 + x_3 - x_4 &= 2, \\ -2x_3 + 4x_4 &= -4, \\ -2x_4 &= 1. \end{aligned}$$

Step 3: Solving this last system by back-substitution involves first solving for x_4 from the last equation, namely $-2x_4 = 1$. This yields $x_4 = -\frac{1}{2}$. Substituting this value of x_4 in the remaining equations yields the system

$$\begin{aligned} x_1 + x_3 + \frac{1}{2} &= 2, \\ -2x_3 - 2 &= -4, \end{aligned}$$

which, after rearranging, yields:

$$\begin{aligned} x_1 + x_3 &= \frac{3}{2}, \\ -2x_3 &= -2, \end{aligned}$$

Solving for x_3 from the last equation yields $x_3 = 1$, and substituting this value of x_3 in the first equation yields

$$x_1 + 1 = \frac{3}{2},$$

i.e.

$$x_1 = \frac{1}{2}.$$

We have completed the back-substitution process, and we have found that $x_1 = \frac{1}{2}$, x_2 is any real number, $x_3 = 1$, and $x_4 = -\frac{1}{2}$. We conclude that our original system of equations has infinitely many solutions, and each $4-$tuple of the form $(\frac{1}{2}, x_2.1, -\frac{1}{2})$, with x_2 any real number, is a solution to our original system.

Remark 6. An augmented matrix is said to be in **reduced row-echelon** form if:

- It is in row echelon form, and
- the first non-zero entry in each row is 1, and
- the first non-zero entry in each row is the only non-zero entry in its column.

Any augmented matrix can be put in reduced row-echelon form using a sequence of elementary row operations; such a sequence of operations is then called **Gauss-Jordan elimination**.

PROBLEMS:

1. Determine the set of solutions for each of the following systems of linear equations using the Gaussian Elimination and Back-Substitution method described in this Section, i.e. for each system:

   (i) Write the augmented matrix,

   (ii) convert the augmented matrix in row-echelon form using elementary row operations,

   (iii) solve the resulting system by back-substitution.

   (a)

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ 2x_1 + x_3 &= 1, \\ x_1 - 3x_3 &= 2. \end{aligned}$$

(b)

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1 + x_3 &= 1, \\ x_1 - 3x_3 &= 2, \\ x_1 + 2x_3 &= 1. \end{aligned}$$

(c)

$$\begin{aligned} x_1 + 3x_2 + x_3 &= 3, \\ 2x_1 + x_3 &= 1, \\ 2x_1 + 3x_2 &= 5. \end{aligned}$$

(d)

$$\begin{aligned} x_1 - x_2 + 2x_3 + x_4 &= 0, \\ 2x_1 + 2x_2 + 3x_3 - x_4 &= -1, \\ x_1 + 3x_2 + x_3 - 2x_4 &= 2. \end{aligned}$$

(e)

$$\begin{aligned} x_1 + x_2 + 2x_3 &= 1, \\ 3x_1 + 2x_2 + 3x_3 &= 3, \\ 2x_1 + x_2 + x_3 &= 2. \end{aligned}$$

(f)

$$\begin{aligned} x_1 + x_2 + x_4 &= 0, \\ x_1 + x_3 &= 1, \\ x_1 - x_4 &= 2, \\ x_1 + x_2 &= 1. \end{aligned}$$

(g)

$$\begin{aligned} 2x_3 + x_4 &= 2, \\ x_1 + x_2 &= 0, \\ x_1 - x_3 &= 1, \\ x_3 + x_4 &= 0. \end{aligned}$$

(h)

$$\begin{aligned} 2x_3 + x_4 &= 2, \\ x_1 + x_2 &= 0, \\ x_1 - x_3 &= 1, \\ x_3 + x_4 &= 0, \\ x_1 + x_2 + x_3 + x_4 &= 1. \end{aligned}$$

(i)

$$\begin{aligned} x_2 + x_3 &= 1, \\ x_1 - x_4 &= 1, \end{aligned}$$

2. Consider the system of equations given by

$$\begin{aligned} x_1 + x_2 + x_3 &= 1 + a, \\ 2x_1 + 2x_2 + 4x_3 &= 2, \\ 3x_1 + 3x_2 + 2x_3 &= a, \end{aligned}$$

where a is a real number. By putting this system in row-echelon form, determine for which values of a it has no solution.

3. Consider the system of equations given by

$$\begin{aligned} x_1 + x_2 + x_3 &= a, \\ x_1 + x_3 &= 2a, \\ 4x_1 + 4x_3 &= a, \end{aligned}$$

where a is a real number. By putting this system in row-echelon form, determine for which values of a it has no solution.

4. Consider the system of equations given by

$$\begin{aligned} x_1 + x_2 + 2x_3 + 2x_4 &= a, \\ x_1 + x_2 + 2x_4 &= a, \\ 2x_1 + 4x_4 &= 1, \\ -x_1 + x_2 - 2x_4 &= 2. \end{aligned}$$

where a is a real number. By putting this system in row-echelon form, determine for which values of a it has no solution.

5. For each of the following chemical reactions, solve the corresponding chemical balance equations using Gaussian elimination and back-substitution:

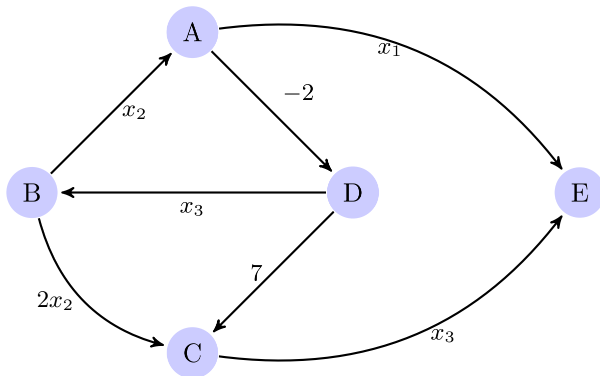
   (a) $CH_4 + O_2 \rightsquigarrow CO_2 + H_2O$

   (b) $SnO_2 + H_2 \rightsquigarrow Sn + H_2O$

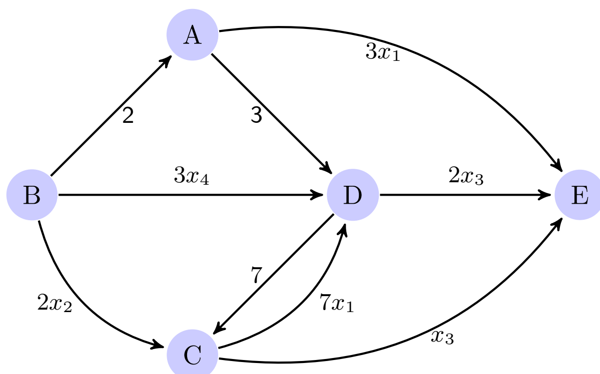
   (c) $Fe + H_2SO_4 \rightsquigarrow Fe_2(SO_4)_3 + H_2$

   (d) $C_3H_8 + O_2 \rightsquigarrow H_2O + CO_2$

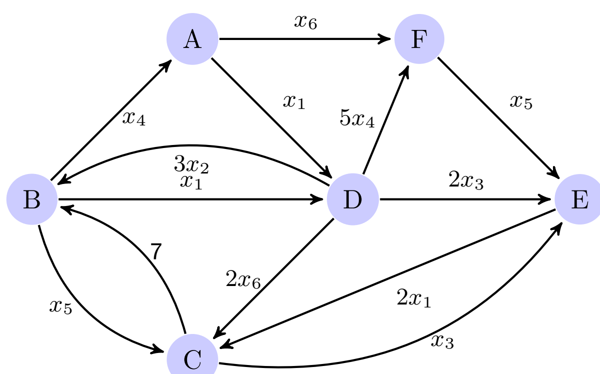
6. Solve the node balance equations (as a system of linear equations in the unknowns x_1, x_2, x_3) for the following graph:



7. Solve the node balance equations (as a system of linear equations in the unknowns x_1, x_2, x_3, x_4) for the following graph:



8. Solve the node balance equations (as a system of linear equations in the unknowns $x_1, x_2, x_3, x_4, x_5, x_6$) for the following graph:

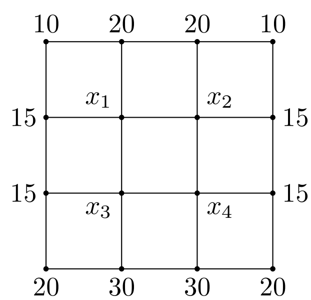


9. The voltage V at the output of an electric device is related to the input current I to the device by the polynomial function $V(I) = aI^2 + bI + c$, where the real coefficients a, b, c are unknown; we wish to determine a, b, c

from experimental data. We experimentally measure the output voltage at the input current values $I = 0, 1, 2$, and we determine from measurement that $V(0) = -5$, $V(1) = 5$, $V(2) = 21$. Solve the system of linear equations (in the unknowns a, b, c) corresponding to these measurements.

10. The velocity v of a particle is modelled as a function of time t by the polynomial function $v(t) = at^3 + bt^2 + ct + d$, where the real coefficients a, b, c, d are unknown; we wish to determine a, b, c, d from experimental data. We experimentally measure the velocity of the particle at times $t = 0, 1, 3, 5$, and we determine from measurement that $v(0) = 5$, $v(1) = 2$, $v(3) = 2$, $v(5) = 50$. Solve the system of linear equations (in the unknowns a, b, c, d) corresponding to these measurements.

11. Consider a square thin metal plate with temperature at steady state and with known boundary temperature; we represent this thin metal plate by the following square mesh:



The steady-state temperature at each mesh point is indicated next to that mesh point. The four mesh points interior to the plate have respective steady-state temperatures x_1, x_2, x_3, x_4; solve the system of linear equations (in the unknowns x_1, x_2, x_3, x_4) that governs the relations between these temperatures.

Section 8

Study Topics

- Generating set for a vector space
- Basis of a vector space
- Coordinates of a vector with respect to a basis

Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ be a finite number of vectors in $\mathbf{V}$. We are by now (hopefully) familiar with the notion of **linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$: A vector $\mathbf{v}$ in $\mathbf{V}$ is said to be a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ if it is equal to the vector

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p$$

for **some** choice of real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$. We have seen in previous lectures that the set of all linear combinations of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$, which we have denoted by $\mathcal{S}_{(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)}$, is a vector subspace of $\mathbf{V}$.
The case where $\mathcal{S}_{(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)}$ is $\mathbf{V}$ itself is of particular interest, since it means that **any** vector $\mathbf{v}$ in $\mathbf{V}$ is some linear combination of just $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$. Due to the importance of this special case, we make it into a definition:

Definition 20. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$. S is said to be a **generating set** for the vector space $\mathbf{V}$ if **any** vector $\mathbf{v}$ in $\mathbf{V}$ can be written as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$; that is, for any $\mathbf{v}$ in $\mathbf{V}$, we can find real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$ such that:

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p.$$

Let us examine a few examples:

(a) in the (by now familiar) real vector space $\widehat{\mathbb{R}^3}$, consider the three vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ defined as follows:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix};$$

It is easy to verify that **none** of the sets $\{\mathbf{v}_1, \mathbf{v}_2\}$, $\{\mathbf{v}_2, \mathbf{v}_3\}$, and $\{\mathbf{v}_1, \mathbf{v}_3\}$ is a generating set for $\widehat{\mathbb{R}^3}$, but that the set $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ **is** a generating set for $\widehat{\mathbb{R}^3}$. To be sure, let us do some of these verifications. Let us first prove that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\widehat{\mathbb{R}^3}$: To do this we have to show that **any** element of $\widehat{\mathbb{R}^3}$ can be written as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. Let then $\mathbf{v}$ be **any** element in $\widehat{\mathbb{R}^3}$; by definition of $\widehat{\mathbb{R}^3}$, $\mathbf{v}$ is a real column vector, with three entries, i.e. is of the form

$$\mathbf{v} = \begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

for some real numbers a, b and c; but then, it is clear that we have the equality

$$\mathbf{v} = a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3,$$

since, writing it out in detail, we have:

$$\begin{aligned} a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3 &= a\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + c\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ b \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ c \end{pmatrix} \\ &= \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \end{aligned}$$

which is none other than $\mathbf{v}$. This proves our assertion that any element in $\widehat{\mathbb{R}^3}$ can be written as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$, and hence shows that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is indeed a generating set for $\widehat{\mathbb{R}^3}$.

Let us now show that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is **not** a generating set for $\widehat{\mathbb{R}^3}$; for this it is **enough** to find **one** vector in $\widehat{\mathbb{R}^3}$ which **cannot** be written as a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$; consider then the vector $\mathbf{v}$ in $\widehat{\mathbb{R}^3}$ defined by:

$$\mathbf{v} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Let us show there is **no linear combination** of $\mathbf{v}_1$ and $\mathbf{v}_2$ that equals $\mathbf{v}$. How can we show this ? Well, we can assume that there does exist such a linear combination, and show that we are then led to a contradiction. Let us then assume that there do exist real numbers α_1, α_2 such that

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2,$$

or, equivalently,

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \alpha_1\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

that is,

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \alpha_2 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ 0 \end{pmatrix};$$

But we have a **contradiction** since the two column vectors $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ 0 \end{pmatrix}$ can **never** be equal, no matter what α_1 and α_2 are (since their equality would imply that $1 = 0$). This shows that there is no linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$ that equals $\mathbf{v}$; hence, $\{\mathbf{v}_1, \mathbf{v}_2\}$ is **not** a generating set for $\widehat{\mathbb{R}^3}$.

(b) Consider now the (equally familiar) real vector space $\widehat{\mathbb{R}^2}$ of all real column vectors with two entries. Consider the subset $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ of $\widehat{\mathbb{R}^2}$, where the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ in $\widehat{\mathbb{R}^2}$ are defined as:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} -1 \\ 0 \end{pmatrix}.$$

Let us show that $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\widehat{\mathbb{R}^2}$. To do this, we have to show that any element in $\widehat{\mathbb{R}^2}$ can be written as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. Let then $\begin{pmatrix} a \\ b \end{pmatrix}$ (with a, b real numbers) be **any** element of $\widehat{\mathbb{R}^2}$; it is clear that we can write:

$$\begin{pmatrix} a \\ b \end{pmatrix} = a\mathbf{v}_1 + b\mathbf{v}_2 + 0\mathbf{v}_3,$$

that is, any element $\begin{pmatrix} a \\ b \end{pmatrix}$ of $\widehat{\mathbb{R}^2}$ can be written as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. This shows that S is indeed a generating set for $\widehat{\mathbb{R}^2}$.

Let us note now that $\begin{pmatrix} a \\ b \end{pmatrix}$ can **also** be expressed as the following linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$:

$$\begin{pmatrix} a \\ b \end{pmatrix} = 0\mathbf{v}_1 + b\mathbf{v}_2 - a\mathbf{v}_3,$$

and **even** as the following linear combination:

$$\begin{pmatrix} a \\ b \end{pmatrix} = 2a\mathbf{v}_1 + b\mathbf{v}_2 + a\mathbf{v}_3,$$

and **even** as:

$$\begin{pmatrix} a \\ b \end{pmatrix} = 3a\mathbf{v}_1 + b\mathbf{v}_2 + 2a\mathbf{v}_3,$$

and so on ... (you get the idea). This shows that any element in $\widehat{\mathbb{R}^2}$ can be written as **many distinct linear combinations** of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$.

The case where a given generating set of a vector space is such that any vector in that vector space can be expressed as a linear combination of vectors in the generating set in a **unique** way is of particular interest, since then there is no ambiguity as to how the vector should be written as a linear combination of the elements of the generating set. Note that this was the case with Example (a) above (prove it!), but not with Example (b).

A very natural question at this point is therefore the following: Suppose we have a vector space $\mathbf{V}$, and we are given a finite subset S of $\mathbf{V}$ which is also a **generating set** for $\mathbf{V}$. We then know of course that any element of $\mathbf{V}$ can be written as **some** linear combination of the elements of S; how then, can we determine whether that is the **only possible** linear combination that yields the desired element ? We already have the answer to that question from Theorem 4 of Lecture 6; we can therefore state:

Theorem 11. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $S = \{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$ such that:

(i) S is a **generating set** for $\mathbf{V}$, and

(ii) S is a **linearly independent** of $\mathbf{V}$;

Then, any element of $\mathbf{V}$ can be expressed in a **unique** way as a linear combination of elements of S.

Finite subsets of $\mathbf{V}$ which happen to be both **generating** and **linearly independent** are of particular importance, as we will see later; we shall therefore give them a special name. However, for a reason that will become clear soon, **we will care about the order**, i.e. we will consider not just subsets of $\mathbf{V}$, but rather **ordered subsets**, or equivalently $p-$tuples of vectors. We therefore define:

Definition 21. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, and let $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p \in \mathbf{V}$. The $p-$tuple $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)$ is said to be a **basis** of $\mathbf{V}$ if

(i) $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ is a **generating set** for $\mathbf{V}$, and

(ii) the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ are **linearly independent**.

It is **important** to note again that in a $p-$tuple **order is important**, and that is what distinguishes it from a set; for example, the $2-$tuples of vectors $(\mathbf{v}_1, \mathbf{v}_2)$ and $(\mathbf{v}_2, \mathbf{v}_1)$ are distinct unless $\mathbf{v}_1 = \mathbf{v}_2$. Similarly, the $3-$tuples $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ and $(\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_1)$ are distinct unless $\mathbf{v}_1 = \mathbf{v}_3$, and so on.

Before going further, let us consider two familiar examples:

1. Consider the real vector space $(\mathbb{R}^2, +, \cdot)$, and consider the elements $(0, 1)$,$(1, 1)$,$(2, 2)$,$(1, 0)$ of $\mathbb{R}^2$. Consider the following few tuples of vectors made from these 4 vec-

tors:

$$
\begin{aligned}
\mathcal{B}_1 &= ((0,1)), \quad \mathcal{B}_2 = ((0,1),(1,0)),\\
\mathcal{B}_3 &= ((1,0),(0,1)), \quad \mathcal{B}_4 = ((0,1),(1,1)),\\
\mathcal{B}_5 &= ((0,1),(2,2)), \quad \mathcal{B}_6 = ((1,1),(2,2)),\\
\mathcal{B}_7 &= ((1,1),(1,0),(2,2)), \quad \mathcal{B}_8 = ((1,1),(1,0)),\\
\mathcal{B}_9 &= ((1,1),(0,1)), \quad \mathcal{B}_{10} = ((1,1),(1,0),(2,2)),\\
\mathcal{B}_{11} &= ((2,2),(1,0)), \quad \mathcal{B}_{12} = ((1,0),(2,2)),\\
\mathcal{B}_{13} &= ((0,1),(2,2)), \quad \mathcal{B}_{14} = ((0,1),(2,2),(1,1)),\\
\mathcal{B}_{15} &= ((2,2),(0,1)), \quad \mathcal{B}_{16} = ((2,2)),\\
\mathcal{B}_{17} &= ((2,2),(1,1)), \quad \mathcal{B}_{18} = ((2,2),(0,1),(1,1),(0,1)),\\
\mathcal{B}_{19} &= ((2,2),(2,2),(2,2),(2,2)), \quad \mathcal{B}_{20} = ((0,1),(2,2),(2,2),(2,2));
\end{aligned}
$$

It is easy to verify that among these 20 tuples, only $\mathcal{B}_2$, $\mathcal{B}_3$, $\mathcal{B}_4$, $\mathcal{B}_5$, $\mathcal{B}_8$, $\mathcal{B}_9$, $\mathcal{B}_{11}$, $\mathcal{B}_{12}$, $\mathcal{B}_{13}$, $\mathcal{B}_{15}$, are a basis of the real vector space $\mathbb{R}^2$. Again **it is important to remember** that the two tuples $\mathcal{B}_2$ and $\mathcal{B}_3$ are **not the same** since, although their constituent elements are the same (namely the two vectors $(1,0)$ and $(0,1)$), their order in $\mathcal{B}_2$ and $\mathcal{B}_3$ is not the same; similarly, the two tuples $\mathcal{B}_4$ and $\mathcal{B}_9$ are **not the same**, the two tuples $\mathcal{B}_5$ and $\mathcal{B}_{15}$ are **not the same**, ...

2. Consider the real vector space $(\widehat{\mathbb{R}^3},+,\cdot)$, and consider the vectors

$$
\mathbf{v}_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, \mathbf{v}_3 = \begin{pmatrix}0\\0\\1\end{pmatrix},
$$

$$
\mathbf{v}_4 = \begin{pmatrix}1\\1\\0\end{pmatrix}, \mathbf{v}_5 = \begin{pmatrix}1\\1\\1\end{pmatrix}, \mathbf{v}_6 = \begin{pmatrix}0\\1\\1\end{pmatrix},
$$

of $\widehat{\mathbb{R}^3}$. Here again, it is easy to verify that each of the $3-$tuples $(\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3)$,$(\mathbf{v}_2,\mathbf{v}_1,\mathbf{v}_3)$,$(\mathbf{v}_3,\mathbf{v}_1,\mathbf{v}_2)$,$(\mathbf{v}$ (and still many more!) are distinct bases of the real vector space $\widehat{\mathbb{R}^3}$; on the other hand, the tuples $(\mathbf{v}_1)$, $(\mathbf{v}_1,\mathbf{v}_2)$, $(\mathbf{v}_3)$, $(\mathbf{v}_1,\mathbf{v}_1,\mathbf{v}_1)$, $(\mathbf{v}_5,\mathbf{v}_6)$ (to give only a few examples) do **not** form a basis of $\widehat{\mathbb{R}^3}$.

The attentive reader may have noticed that in the case of the real vector space $\mathbb{R}^2$ given above, all the tuples which did form a basis of $\mathbb{R}^2$ happened to have exactly the same number of vectors (namely 2); similarly, in the case of the real vector space $\widehat{\mathbb{R}^3}$, all the tuples which did form a basis of $\widehat{\mathbb{R}^3}$ happened to have exactly the same number of vectors (namely 3). We will see in the next lecture that this is not accidental, and that in a vector space, all bases have the same number of elements.

Now that we have defined the notion of **basis** for a real vector space, we define another important notion, that of **components of a vector with respect to a basis**:

Definition 22. Let $(\mathbf{V}, +, \cdot)$ be a real vector space, let $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)$ be a **basis** of $\mathbf{V}$, and let $\mathbf{v} \in \mathbf{V}$. The $p-$tuple $(\alpha_1, \alpha_2, \cdots, \alpha_p)$ of real numbers is called the **component vector** or **coordinate vector** of $\mathbf{v}$ with respect to the basis $\mathcal{B}$ if we have:

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p = \mathbf{v}.$$

The real number α_1 is called the first component (or first coordinate) of $\mathbf{v}$ with respect to the basis $\mathcal{B}$, the real number α_2 is called the second component (or second coordinate) of $\mathbf{v}$ with respect to the basis $\mathcal{B}$, ... and so on.

It is **absolutely essential to note the following point:**

- If $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)$ is a basis of $\mathbf{V}$ and $\mathbf{v}$ is an element of $\mathbf{V}$, then $\mathbf{v}$ has **at least one** component vector with respect to $\mathcal{B}$ (since $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ is a **generating set** for $\mathbf{V}$); furthermore, since the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p$ are **linearly independent**, there is only a **unique** $p-$tuple $(\alpha_1, \cdots, \alpha_p)$ of real numbers for which $\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p$ is equal to $\mathbf{v}$; i.e. to each $\mathbf{v}$ in $\mathbf{V}$ there corresponds only a **unique** component vector. This is why in the previous definition, we wrote "**the** component vector of $\mathbf{v}$ with respect to $\mathcal{B}$" and not "**a** component vector of $\mathbf{v}$ with respect to $\mathcal{B}$".

It is also important to make note of the following point:

- If $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)$ is a basis of $\mathbf{V}$ and $\mathbf{v}$ is an element of $\mathbf{V}$, we have defined the component vector of $\mathbf{v}$ with respect to $\mathcal{B}$ to be some $p-$tuple of real numbers, i.e. some element of $\mathbb{R}^p$; we will find it occasionally convenient to denote the component vector of $\mathbf{v}$ by an element of $\widehat{\mathbb{R}^p}$ instead, i.e. by a column vector with p real entries.

We close this section with three examples:

(a) Consider the real vector space $(\mathbb{R}^2 +, \cdot)$, and let $\mathbf{W}$ denote the subset of $\mathbb{R}^2$ consisting of all pairs (x, y) of real numbers such that $x = y$. It is easy to verify that $\mathbf{W}$ is a vector subspace of $\mathbb{R}^2$, and hence, by Problem 4 of Lecture 3, $\mathbf{W}$ (with the operations of addition and scalar multiplication it receives from $\mathbb{R}^2$) is itself a real vector space. Consider the vector $\mathbf{v}_1 = (1, 1)$ of $\mathbb{R}^2$; clearly, $\mathbf{v}_1$ is an element of $\mathbf{W}$, since $\mathbf{W}$ is the subset of $\mathbb{R}^2$ consisting of all pairs (x, y) with $x = y$, and the pair $(1, 1)$ satisfies this condition. Consider the "$1-$tuple" $\mathcal{B} = (\mathbf{v}_1)$; let us show that $\mathcal{B}$ is a basis of $\mathbf{W}$. To do this, we have to show two things:

  (i) That $\{\mathbf{v}_1\}$ is a **generating set** for $\mathbf{W}$, and

  (ii) that $\{\mathbf{v}_1\}$ is a **linearly independent** subset of $\mathbf{W}$.

  To show (i), namely that $\{\mathbf{v}_1\}$ is a generating set for $\mathbf{W}$, we have to show that **any** $\mathbf{v} \in \mathbf{W}$ can be written as some linear combination of $\mathbf{v}_1$; let then $\mathbf{v} = (x, y)$ be an element of $\mathbf{W}$; since (x, y) is in $\mathbf{W}$, we have (by definition of $\mathbf{W}$) $x = y$. Hence, $\mathbf{v} = (x, x) = x(1, 1) = x\mathbf{v}_1$, which shows that $\mathbf{v}$ is a linear combination of $\mathbf{v}_1$. To recapitulate, we have shown that **any** element of $\mathbf{W}$ is a linear combination of $\mathbf{v}_1$; this proves that $\{\mathbf{v}_1\}$ is a generating set for $\mathbf{W}$. Let us now show (ii), i.e. that $\{\mathbf{v}_1\}$ is a linearly independent set. Let then α be any real number such that $\alpha\mathbf{v}_1 = \mathbf{0}$; we have to show that we must then have $\alpha = 0$. Now, $\alpha\mathbf{v}_1 = \mathbf{0}$ is equivalent to $\alpha(1,1) = (0,0)$, which is equivalent to $(\alpha,\alpha) = (0,0)$, which implies $\alpha = 0$. Hence, we have shown that $\alpha\mathbf{v}_1 = \mathbf{0}$ implies $\alpha = 0$, and this proves that $\{\mathbf{v}_1\}$ is a linearly independent subset of $\mathbf{W}$. We have thus shown (i) and (ii), and hence, we have shown that $\mathcal{B}$ is a **basis of W**.

Any element of $\mathbf{W}$ is a pair of the form (a,a) for some $a \in \mathbb{R}$; Let us compute the **component vector** of (a,a) with respect to the basis $\mathcal{B}$. We have:

$$(a,a) = a(1,1) = a\mathbf{v}_1,$$

which shows that the component vector of the vector (a,a) of $\mathbf{W}$ with respect to the basis $\mathcal{B}$ is the $1-$tuple (a). (Note: It may sound a bit akward to talk about $1-$tuples, but think of them as a list with only one entry!).

(b) Consider the real vector space $(\mathbb{R}^3,+,\cdot)$, and let $\mathbf{v}_1 = (1,0,0)$, $\mathbf{v}_2 = (0,1,0)$, $\mathbf{v}_3 = (0,0,1)$, $\mathbf{v}_4 = (1,1,0)$, $\mathbf{v}_5 = (1,1,1)$. It is easy to verify that each of the $3-$tuples of vectors $\mathcal{B}_1 = (\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3)$, $\mathcal{B}_2 = (\mathbf{v}_2,\mathbf{v}_3,\mathbf{v}_1)$, and $\mathcal{B}_3 = (\mathbf{v}_1,\mathbf{v}_4,\mathbf{v}_5)$ is a basis of $\mathbb{R}^3$. Let now $\mathbf{v} = (a,b,c)$ be an element of $\mathbb{R}^3$. It is easy to verify that the component vector of $\mathbf{v}$ with respect to $\mathcal{B}_1$ is (a,b,c) (i.e. $\mathbf{v}$ itself!), whereas its component vector with respect to the basis $\mathcal{B}_2$ is (b,c,a), and its component vector with respect to the basis $\mathcal{B}_3$ is $(a-b, b-c, c)$.

(c) Consider again the real vector space $(\mathbb{R}^3,+,\cdot)$, and let $\mathbf{W}$ be the subset of $\mathbb{R}^3$ consisting of all triples (x,y,z) with $x+y+z=0$. It is easy to verify that $\mathbf{W}$ is a vector subspace of $\mathbb{R}^3$. By Problem 4 of Lecture 3, we know that $\mathbf{W}$ (with the operations of addition and scalar multiplication it receives from $\mathbb{R}^3$) is itself a real vector space. Consider the elements $\mathbf{v}_1, \mathbf{v}_2$ of $\mathbf{W}$ defined by:

$$\begin{aligned}\mathbf{v}_1 &= (1,0,-1),\\ \mathbf{v}_2 &= (0,1,-1).\end{aligned}$$

Define $\mathcal{B}$ to be the $2-$tuple $\mathcal{B} = (\mathbf{v}_1,\mathbf{v}_2)$. Let us show that $\mathcal{B}$ is indeed a basis for the real vector space $\mathbf{W}$. Once again, to show this, we must show two things:

(i) That $\{\mathbf{v}_1,\mathbf{v}_2\}$ is a **generating set** for $\mathbf{W}$, and

(ii) that $\{\mathbf{v}_1,\mathbf{v}_2\}$ is a **linearly independent** subset of $\mathbf{W}$.

Let us first show (i): We have to show that **any** element of $\mathbf{W}$ is some linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. Let then $\mathbf{v} = (x,y,z)$ be any element in

$\mathbf{W}$. Since $\mathbf{v}$ is in $\mathbf{W}$, we must have (by definition of $\mathbf{W}$) $x + y + z = 0$, i.e. $z = -x - y$. Hence, $\mathbf{v} = (x, y, -x - y)$. Now note that we can write:

$$\begin{aligned} \mathbf{v} &= (x, y, -x - y) \\ &= (x, 0, -x) + (0, y, -y) \\ &= x(1, 0, -1) + y(0, 1, -1) \\ &= x\mathbf{v}_1 + y\mathbf{v}_2, \end{aligned}$$

which shows that $\mathbf{v}$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. We have thus shown that **any** element of $\mathbf{W}$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$, and this shows that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is a **generating set** for $\mathbf{W}$.

Let us now show (ii). Let then α, β be real numbers such that $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 = \mathbf{0}$; we must show that this necessarily implies that $\alpha = \beta = 0$. Now, $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 = \mathbf{0}$ is equivalent to

$$\alpha(1, 0, -1) + \beta(0, 1, -1) = (0, 0, 0),$$

which is equivalent to

$$(\alpha, 0, -\alpha) + (0, \beta, -\beta) = (0, 0, 0),$$

which is equivalent to

$$(\alpha, \beta, -\alpha - \beta) = (0, 0, 0),$$

which implies $\alpha = \beta = 0$. Hence, we have shown that if α, β are real numbers such that $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 = \mathbf{0}$ then it must follow that $\alpha = \beta = 0$. This proves (ii), i.e. that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is a **linearly independent** subset of $\mathbf{W}$. We have therefore shown (i) and (ii), i.e., we have shown that $\mathcal{B}$ is a basis of $\mathbf{W}$.

Let now (a, b, c) be any element of $\mathbf{W}$; let us compute the **component vector** of (a, b, c) with respect to the basis $\mathcal{B}$. Since (a, b, c) is in $\mathbf{W}$, we must have (by definition of $\mathbf{W}$) $a + b + c = 0$; it follows that $c = -a - b$, i.e.

$$(a, b, c) = (a, b, -a - b) = a(1, 0, -1) + b(0, 1, -1) = a\mathbf{v}_1 + b\mathbf{v}_2,$$

which shows that the component vector of the element (a, b, c) of $\mathbf{W}$ with respect to the basis $\mathcal{B}$ is the pair (a, b).

PROBLEMS:

1. Consider the real vector space $(\mathbb{R}^3, +, \cdot)$, and consider the following vectors in $\mathbb{R}^3$:

$$\mathbf{v}_1 = (1, 0, 0), \quad \mathbf{v}_2 = (1, 1, 0), \quad \mathbf{v}_3 = (1, 2, 1), \quad \mathbf{v}_4 = (0, 0, 3),$$

(a) Show that $\{\mathbf{v}_1\}$ is not a generating set for $\mathbb{R}^3$.
(b) Show that $\{\mathbf{v}_2\}$ is not a generating set for $\mathbb{R}^3$.
(c) Show that $\{\mathbf{v}_3\}$ is not a generating set for $\mathbb{R}^3$.
(d) Show that $\{\mathbf{v}_4\}$ is not a generating set for $\mathbb{R}^3$.
(e) Show that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is not a generating set for $\mathbb{R}^3$.
(f) Show that $\{\mathbf{v}_1, \mathbf{v}_3\}$ is not a generating set for $\mathbb{R}^3$.
(g) Show that $\{\mathbf{v}_2, \mathbf{v}_3\}$ is not a generating set for $\mathbb{R}^3$.
(h) Show that $\{\mathbf{v}_1, \mathbf{v}_4\}$ is not a generating set for $\mathbb{R}^3$.
(i) Show that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\mathbb{R}^3$.
(j) Show that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4\}$ is a generating set for $\mathbb{R}^3$.
(k) Show that $\{\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_4\}$ is a generating set for $\mathbb{R}^3$.
(l) Show that $\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ is a generating set for $\mathbb{R}^3$.
(m) Show that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ is a generating set for $\mathbb{R}^3$.

2. Consider the real vector space $(\widehat{\mathbb{R}^3}, +, \cdot)$, and let $\mathbf{W}$ be the subset of $\widehat{\mathbb{R}^3}$ consisting of all elements $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ of $\widehat{\mathbb{R}^3}$ for which $x + y - z = 0$. It is easy to verify that $\mathbf{W}$ is a vector subspace of $\widehat{\mathbb{R}^3}$, and hence, is itself a real vector space.

Consider now the following vectors in $\mathbf{W}$:

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad \mathbf{v}_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

(a) Show that $\{\mathbf{v}_1\}$ is not a generating set for $\mathbf{W}$.
(b) Show that $\{\mathbf{v}_2\}$ is not a generating set for $\mathbf{W}$.
(c) Show that $\{\mathbf{v}_3\}$ is not a generating set for $\mathbf{W}$.
(d) Show that $\{\mathbf{v}_4\}$ is not a generating set for $\mathbf{W}$.
(e) Show that $\{\mathbf{v}_1, \mathbf{v}_4\}$ is not a generating set for $\mathbf{W}$.
(f) Show that $\{\mathbf{v}_2, \mathbf{v}_4\}$ is not a generating set for $\mathbf{W}$.
(g) Show that $\{\mathbf{v}_3, \mathbf{v}_4\}$ is not a generating set for $\mathbf{W}$.
(h) Show that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is a generating set for $\mathbf{W}$.
(i) Show that $\{\mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\mathbf{W}$.
(j) Show that $\{\mathbf{v}_1, \mathbf{v}_3\}$ is a generating set for $\mathbf{W}$.
(k) Show that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\mathbf{W}$.
(l) Show that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ is a generating set for $\mathbf{W}$.

3. Consider the real vector space $(\mathbb{R}^4, +, \cdot)$, and let $\mathbf{W}$ be the subset of $\mathbb{R}^4$ consisting of all $4-$tuples (x, y, z, w) of real numbers for which $3x+y-w = 0$ **and** $z - 2w = 0$. It is easy to verify that $\mathbf{W}$ is a vector subspace of $\mathbf{W}$, and hence, is itself a real vector space. Consider the following vectors in $\mathbf{W}$:

$$\mathbf{v}_1 = (1, 0, 6, 3), \quad \mathbf{v}_2 = (0, 1, 2, 1), \quad \mathbf{v}_3 = (1, 1, 8, 4)$$

   (a) Show that $\{\mathbf{v}_1\}$ is not a generating set for $\mathbf{W}$.
   (b) Show that $\{\mathbf{v}_2\}$ is not a generating set for $\mathbf{W}$.
   (c) Show that $\{\mathbf{v}_3\}$ is not a generating set for $\mathbf{W}$.
   (d) Show that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is a generating set for $\mathbf{W}$.
   (e) Show that $\{\mathbf{v}_1, \mathbf{v}_3\}$ is a generating set for $\mathbf{W}$.
   (f) Show that $\{\mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\mathbf{W}$.
   (g) Show that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a generating set for $\mathbf{W}$.

4. Consider the real vector space $(\mathbb{R}^2, +, \cdot)$, and consider the following vectors in $\mathbb{R}^2$:

$$\mathbf{v}_1 = (1, 1), \quad \mathbf{v}_2 = (-1, 1), \quad \mathbf{v}_3 = (0, 1), \quad \mathbf{v}_4 = (1, 2)$$

   (a) Show that $(\mathbf{v}_1)$ is not a basis of $\mathbb{R}^2$.
   (b) Show that $(\mathbf{v}_2)$ is not a basis of $\mathbb{R}^2$.
   (c) Show that $(\mathbf{v}_3)$ is not a basis of $\mathbb{R}^2$.
   (d) Show that $(\mathbf{v}_4)$ is not a basis of $\mathbb{R}^2$.
   (e) Show that $\mathcal{B}_1 = (\mathbf{v}_1, \mathbf{v}_2)$ is a basis of $\mathbb{R}^2$.
   (f) Show that $\mathcal{B}_2 = (\mathbf{v}_1, \mathbf{v}_3)$ is a basis of $\mathbb{R}^2$.
   (g) Show that $\mathcal{B}_3 = (\mathbf{v}_1, \mathbf{v}_4)$ is a basis of $\mathbb{R}^2$.
   (h) Show that $\mathcal{B}_4 = (\mathbf{v}_2, \mathbf{v}_3)$ is a basis of $\mathbb{R}^2$.
   (i) Show that $\mathcal{B}_5 = (\mathbf{v}_3, \mathbf{v}_2)$ is a basis of $\mathbb{R}^2$.
   (j) Show that $\mathcal{B}_6 = (\mathbf{v}_3, \mathbf{v}_4)$ is a basis of $\mathbb{R}^2$.
   (k) Show that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is not a basis of $\mathbb{R}^2$.
   (l) Show that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4)$ is not a basis of $\mathbb{R}^2$.
   (m) Show that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4)$ is not a basis of $\mathbb{R}^2$.
   (n) Compute the component vectors of $\mathbf{v}_1$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_6$.
   (o) Compute the component vectors of $\mathbf{v}_2$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_6$.
   (p) Compute the component vectors of $\mathbf{v}_3$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_6$.

(q) Compute the component vectors of $\mathbf{v}_4$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_6$.

5. Consider the real vector space $(\mathbb{R}^4, +, \cdot)$, and let $\mathbf{W}$ be the subset of $\mathbb{R}^4$ consisting of all 4−tuples (x, y, z, w) of real numbers for which $x+y+z-w=0$ **and** $y-z=0$. It is easy to verify that $\mathbf{W}$ is a vector subspace of $\mathbb{R}^4$, and hence, is itself a real vector space. Consider the following vectors in $\mathbf{W}$:

$$\mathbf{v}_1 = (1,0,0,1), \quad \mathbf{v}_2 = (0,1,1,2), \quad \mathbf{v}_3 = (1,1,1,3), \quad \mathbf{v}_4 = (1,-1,-1,-1).$$

(a) Show that $(\mathbf{v}_1)$ is not a basis of $\mathbf{W}$.

(b) Show that $(\mathbf{v}_2)$ is not a basis of $\mathbf{W}$.

(c) Show that $(\mathbf{v}_3)$ is not a basis of $\mathbf{W}$.

(d) Show that $(\mathbf{v}_4)$ is not a basis of $\mathbf{W}$.

(e) Show that $\mathcal{B}_1 = (\mathbf{v}_1, \mathbf{v}_2)$ is a basis of $\mathbf{W}$.

(f) Show that $\mathcal{B}_2 = (\mathbf{v}_1, \mathbf{v}_3)$ is a basis of $\mathbf{W}$.

(g) Show that $\mathcal{B}_3 = (\mathbf{v}_3, \mathbf{v}_1)$ is a basis of $\mathbf{W}$.

(h) Show that $\mathcal{B}_4 = (\mathbf{v}_1, \mathbf{v}_4)$ is a basis of $\mathbf{W}$.

(k) Show that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is not a basis of $\mathbf{W}$.

(l) Show that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4)$ is not a basis of $\mathbf{W}$.

(m) Show that $(\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_4)$ is not a basis of $\mathbf{W}$.

(n) Compute the component vectors of $\mathbf{v}_1$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_4$.

(o) Compute the component vectors of $\mathbf{v}_2$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_4$.

(p) Compute the component vectors of $\mathbf{v}_3$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_4$.

(q) Compute the component vectors of $\mathbf{v}_4$ with respect to each of the bases $\mathcal{B}_1, \cdots, \mathcal{B}_4$.

Section 9

Study Topics

- Finite-dimensional vector spaces
- Dimension of a real vector space

We know from elementary geometry that we can represent real numbers (i.e. elements of the real vector space $\mathbb{R}$) by points on a line, pairs of real numbers (i.e. elements of the real vector space $\mathbb{R}^2$) by points in a plane, triples of real numbers (i.e. elements of the real vector space $\mathbb{R}^3$) by points in space, ... The question we may ask at this point is how the difference between, say, a line and a plane, manifests itself in a difference between the vector spaces $\mathbb{R}$ and $\mathbb{R}^2$. Or how the difference between a plane and space manifests itself in a difference between the vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$. In other words, how is the "line-like" feature of the real vector space $\mathbb{R}$ captured in the vector space structure of $\mathbb{R}$, how is the "plane-like" feature of the real vector space $\mathbb{R}^2$ captured in the vector space structure of $\mathbb{R}^2$, how is the "space-like" feature of the real vector space $\mathbb{R}^3$ captured in the vector space structure of $\mathbb{R}^3$, ... In one word: How do these "geometric" concepts get expressed in terms of linear algebra ? We shall soon see that one point of contact between linear algebra and geometry is given by the notion of **dimension**.

Definition 23. Let $(\mathbf{V}, +, \cdot)$ be a real vector space.

- $\mathbf{V}$ is said to be **finite-dimensional** if there exists an integer $N \geq 0$ such that **any** subset of $\mathbf{V}$ containing $N+1$ elements is **linearly dependent**. The **smallest** integer N for which this holds is then called the **dimension of $\mathbf{V}$** (equivalently, $\mathbf{V}$ is said to have dimension N).
- $\mathbf{V}$ is said to be **infinite-dimensional** if it is not finite-dimensional.

It is important to note the following points:

- By the above definition, if $\mathbf{V}$ has dimension N, then any subset of $\mathbf{V}$ containing $N+1$ elements is linearly dependent, and as a result, any subset of $\mathbf{V}$ containing $N+2$ or more elements is **also** linearly dependent.
- By the above definition, if $\mathbf{V}$ has dimension N, then any subset of $\mathbf{V}$ containing $N+1$ elements is linearly dependent, but there exists **at least one linearly independent** subset of $\mathbf{V}$ containing **exactly** N **elements**, since otherwise the dimension of $\mathbf{V}$ would be strictly less than N.
- $\mathbf{V}$ is **infinite-dimensional** if **for any** positive integer N, no matter how large, there exists a **linearly independent** subset of $\mathbf{V}$ containing **exactly** N elements.

Let's recapitulate:

- $\mathbf{V}$ is said to have dimension N if and only if the following two conditions are met:
  - (i) There exists a **linearly independent** subset of $\mathbf{V}$ containing **exactly** N **elements**,
  - (ii) **Any subset** of $\mathbf{V}$ containing $N+1$ elements is **linearly dependent**.

Let us now examine some simple examples:

1. Recall the real vector space $(\mathcal{F}(\mathbb{R};\mathbb{R}),+,\cdot)$ consisting of all functions $f:\mathbb{R}\to\mathbb{R}$ (i.e. all real-valued functions of a real variable). Let us show that $\mathcal{F}(\mathbb{R};\mathbb{R})$ is an **infinite-dimensional** vector space. To do this, we have to show that for **any** integer $N \geq 0$ (no matter how large), there exists a **linearly independent** subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$ containing exactly N elements.

   Let then N be **any** integer ≥ 0. Consider the following elements $f_1, f_2, \cdots, f_N$ in $\mathcal{F}(\mathbb{R};\mathbb{R})$ defined as follows:

$$
\begin{array}{cccc}
f_1(t)=0 \text{ for } & t\neq 1 & \text{and} & f_1(1)=1,\\
f_2(t)=0 \text{ for } & t\neq 2 & \text{and} & f_2(2)=1,\\
f_3(t)=0 \text{ for } & t\neq 3 & \text{and} & f_3(3)=1,\\
 & \cdots & & \\
f_N(t)=0 \text{ for } & t\neq N & \text{and} & f_N(N)=1.
\end{array}
$$

   (You may want to draw the graphs of these functions just to see what they look like). In other words, if k is an integer in the range $1 \leq k \leq N$, f_k is the function from $\mathbb{R}$ to $\mathbb{R}$ defined to be 0 everywhere except at k (where it takes the value 1). Let us show that $\{f_1, f_2, \cdots, f_N\}$ is a **linearly independent** subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$. Let then $\alpha_1, \alpha_2, \cdots, \alpha_N$ be real numbers such that

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_N f_n = \mathbf{0}.$$

   (Recall that the zero vector $\mathbf{0}$ of the vector space $\mathcal{F}(\mathbb{R};\mathbb{R})$ is the function from $\mathbb{R}$ to $\mathbb{R}$ which maps every real number to zero). We have to show that α_1,α_2,$\cdots$,α_N must all be zero. Now, the equality

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_N f_n = \mathbf{0}.$$

   is equivalent to

$$\alpha_1 f_1(t) + \alpha_2 f_2(t) + \cdots + \alpha_N f_n(t) = 0, \quad \forall t \in \mathbb{R},$$

   and in particular, this last equality must hold for particular choices of t, such as $t=1$, $t=2$, $\cdots$, $t=N$. But since $f_1(1)=1$ and $f_2(1)=f_3(1)=\cdots=f_N(1)=0$, the above equality, for the particular choice of $t=1$ becomes:

$$\alpha_1 = 0.$$

   Similarly, since $f_2(2)=1$ and $f_1(2)=f_3(2)=\cdots=f_N(2)=0$, that same equality, for the particular choice of $t=2$ becomes:

$$\alpha_2 = 0.$$

Continuing in this way with, successively, $t = 3$, $t = 4$, $\cdots$, $t = N$, we obtain successively that $\alpha_3 = 0$, $\alpha_4 = 0$, $\cdots$, $\alpha_N = 0$. Hence, we have shown that if $\alpha_1, \alpha_2, \cdots, \alpha_N$ are real numbers such that

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_N f_n = \mathbf{0},$$

then it follows that $\alpha_1 = \alpha_2 = \cdots = \alpha_N = 0$. This proves that $\{f_1, f_2, \cdots, f_N\}$ is a **linearly independent** subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$.

Let us recapitulate: **For any integer** $N \geq 0$, we have constructed a **linearly independent** subset of $\mathcal{F}(\mathbb{R};\mathbb{R})$ **containing exactly** N **elements**; this proves that $\mathcal{F}(\mathbb{R};\mathbb{R})$ is an **infinite-dimensional** real vector space.

2. Let $\mathbf{V}$ be a set containing only one element, which we denote by ξ (the zero vector), that is, $\mathbf{V} = \{\xi\}$; define addition and scalar multiplication on $\mathbf{V}$ as follows:

$$\begin{aligned} \xi + \xi &= \xi \\ \alpha \cdot \xi &= \xi, \quad \forall \alpha \in \mathbb{R}. \end{aligned}$$

It is easy to verify that $(\mathbf{V}, +, \cdot)$ is a real vector space and that ξ itself is the zero vector of this vector space. Let us show that $\mathbf{V}$ has dimension 0. Let $N = 0$; there is only one possible subset of $\mathbf{V}$ containing $N + 1 = 1$ elements, namely $\{\xi\}$, which is $\mathbf{V}$ itself, and since that subset contains the zero vector (since ξ itself is the zero vector), that subset is linearly dependent. It follows from the definition of dimension that $\mathbf{V}$ is $0-$dimensional.

3. Let now $\mathbf{V} = \mathbb{R}$, with the usual addition and multiplication operations (we have already seen that with these operations, $\mathbb{R}$ is a real vector space). Let us show that $\mathbf{V}$ has dimension 1. For this, we have to show that we can find a linearly independent subset of $\mathbb{R}$ containing exactly one element, but that any subset of $\mathbb{R}$ containing two elements is linearly dependent. Consider then the subset of $\mathbb{R}$ given by $\{1\}$ (i.e. the subset containing only the vector 1 of $\mathbb{R}$). Let $\alpha \in \mathbb{R}$, and assume $\alpha \cdot 1 = 0$; since $\alpha \cdot 1 = \alpha$, this implies $\alpha = 0$, which shows that $\{1\}$ is a linearly independent subset of $\mathbb{R}$. Let us now show that any subset of $\mathbb{R}$ containing two elements is linearly dependent. Let then $\{\mathbf{v}_1, \mathbf{v}_2\}$ be any subset of $\mathbb{R}$; we have to show that there exists a linear combination $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2$ of $\mathbf{v}_1, \mathbf{v}_2$ that is equal to 0 but such that α, β are not both zero. Consider the following three cases:

   (i) If $\mathbf{v}_1 = 0$, then with $\alpha = 1, \beta = 0$, we obtain $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 = 0$, and since α, β are not both zero (since $\alpha = 1$), this proves linear dependence of $\{\mathbf{v}_1, \mathbf{v}_2\}$ in this case.

   (ii) If $\mathbf{v}_2 = 0$, then with $\alpha = 0, \beta = 1$, we obtain $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 = 0$, and since α, β are not both zero (since $\beta = 1$), this proves linear dependence of $\{\mathbf{v}_1, \mathbf{v}_2\}$.

(iii) If $\mathbf{v}_1 \neq 0$ and $\mathbf{v}_2 \neq 0$, then, with $\alpha = 1, \beta = -\frac{\mathbf{v}_1}{\mathbf{v}_2}$ (remember that since $\mathbf{V} = \mathbb{R}$ in this example, our vectors are real numbers so we can divide by them if they are non-zero), we have $\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 = 0$, and since α, β are not both zero, this proves linear dependence of $\{\mathbf{v}_1, \mathbf{v}_2\}$.

Hence, we have linear dependence of $\{\mathbf{v}_1, \mathbf{v}_2\}$ in all cases. To recapitulate, we have shown that:

- There exists a linearly independent subset of $\mathbb{R}$ containing exactly one element,
- Any subset of $\mathbb{R}$ containing two elements is linearly dependent.

This proves that $\mathbb{R}$ has dimension 1.

The reader may feel at this point that the dimension of a real vector space may not be such an easy thing to compute: After all, it took us quite a few lines above to compute the dimension of a simple vector space such as $\mathbb{R}$. Recall again that to prove that a real vector space has dimension N, we have to do two things:

- Find N linearly independent vectors in that vector space,
- Show that any subset containing $N+1$ vectors is linearly dependent.

The first item is usually easy to accomplish; it is enough to find one linearly independent subset containing exactly N elements. The difficulty comes from the second item: How does one prove that **any** subset containing $N+1$ elements is necessarily linearly dependent ?
The following theorems will yield an **extremely simple** way to compute the dimension of a finite-dimensional real vector space.

Theorem 12. Let $(\mathbf{V}, +, \cdot)$ be a **finite-dimensional** real vector space of dimension N. Let $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$ containing p vectors. If $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is a **linearly independent** subset of $\mathbf{V}$ then $p \leq N$.

Proof. The proof follows directly from the definition of dimension. If we had $p > N$, then that would mean that $p \geq N+1$; since $\mathbf{V}$ is assumed to have dimension N, we know (by definition of dimension) that **any** subset of $\mathbf{V}$ containing $N+1$ or more elements has to be linearly dependent; hence, if $p > N$, i.e. equivalently $p \geq N+1$, the subset $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ has $N+1$ or more elements, and hence is **linearly dependent**. Hence, if we assume that $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is **linearly independent**, then we must have $p \leq N$. □

Theorem 13. Let $(\mathbf{V}, +, \cdot)$ be a **finite-dimensional** real vector space of dimension N. Let $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ be a finite subset of $\mathbf{V}$ containing p vectors. If $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is a **generating set** for $\mathbf{V}$ of $\mathbf{V}$ then $p \geq N$.

Proof. We will show that, under the assumption that $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is a generating set for $\mathbf{V}$, we cannot have $p < N$. So let us begin by assuming that $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is a generating set for $\mathbf{V}$, and that $p < N$; we will show that this leads to a contradiction.
Since $\mathbf{V}$ is assumed to have dimension N, there does exist (by definition of dimension) a **linearly independent** subset of $\mathbf{V}$ containing **exactly** N **elements**; let $\{\mathbf{e}_1, \cdots, \mathbf{e}_N\}$ denote that subset. Since $\{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$ is a generating set for $\mathbf{V}$, each of $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_N$ can be expressed as a linear combination of $\mathbf{v}_1, \cdots, \mathbf{v}_p$. Let us start with $\mathbf{e}_1$; we can write:

$$\mathbf{e}_1 = \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_p \mathbf{v}_p,$$

for some real numbers $\alpha_1, \alpha_2, \cdots, \alpha_p$. Since the subset $\{\mathbf{e}_1, \cdots, \mathbf{e}_N\}$ is **linearly independent**, **none** of $\mathbf{e}_1, \cdots, \mathbf{e}_N$ is the **zero vector**; in particular, $\mathbf{e}_1 \neq \mathbf{0}$, and hence, **at least one** of $\alpha_1, \alpha_2, \cdots, \alpha_p$ must be non-zero (since if all of $\alpha_1, \alpha_2, \cdots, \alpha_p$ were zero, we would obtain $\mathbf{e}_1 = \mathbf{0}$ from the linear combination above). Assume with no loss of generality (relabel the vectors if necessary) that it is α_1 which is non-zero, i.e. $\alpha_1 \neq 0$. We can then write:

$$\mathbf{v}_1 = \frac{1}{\alpha_1}\mathbf{e}_1 - \frac{\alpha_2}{\alpha_1}\mathbf{v}_2 - \cdots - \frac{\alpha_p}{\alpha_1}\mathbf{v}_p,$$

and this shows that $\{\mathbf{e}_1, \mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_p\}$ is a **generating set** for $\mathbf{V}$ (since $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ itself is assumed to be a generating set for $\mathbf{V}$). Hence $\mathbf{e}_2$ can be written as some linear combination of $\mathbf{e}_1, \mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_p$, i.e.

$$\mathbf{e}_2 = \lambda_1 \mathbf{e}_1 + \lambda_2 \mathbf{v}_2 + \lambda_3 \mathbf{v}_3 + \cdots + \lambda_p \mathbf{v}_p,$$

for some real numbers $\lambda_1, \cdots, \lambda_p$. Note that **at least one** of $\lambda_2, \lambda_3, \cdots, \lambda_p$ is non-zero, since if all of $\lambda_2, \lambda_3, \cdots, \lambda_p$ were zero, we would obtain $\mathbf{e}_2 = \lambda_1 \mathbf{e}_1$, contradicting the linear independence of $\{\mathbf{e}_1, \cdots, \mathbf{e}_N\}$. Assume with no loss of generality (relabel the vectors if necessary) that it is λ_2 which is non-zero, i.e. $\lambda_2 \neq 0$. This then yields:

$$\mathbf{v}_2 = -\frac{\lambda_1}{\lambda_2}\mathbf{e}_1 + \frac{1}{\lambda_2}\mathbf{e}_2 - \frac{\lambda_3}{\lambda_2}\mathbf{v}_3 - \cdots - \frac{\lambda_p}{\lambda_2}\mathbf{v}_p,$$

This last equality, together with the equality

$$\mathbf{v}_1 = \frac{1}{\alpha_1}\mathbf{e}_1 - \frac{\alpha_2}{\alpha_1}\mathbf{v}_2 - \cdots - \frac{\alpha_p}{\alpha_1}\mathbf{v}_p,$$

and the assumption that $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ is a generating set for $\mathbf{V}$, implies that $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{v}_3, \mathbf{v}_4 \cdots, \mathbf{v}_p\}$ is a **generating set** for $\mathbf{V}$. Continuining in this way, we obtain successively that $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{v}_4 \cdots, \mathbf{v}_p\}$ is a generating set for $\mathbf{V}$, that $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{v}_5 \cdots, \mathbf{v}_p\}$ is a generating set for $\mathbf{V}$, ..., and finally, that $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_p\}$ is a generating set for $\mathbf{V}$, in other words, that the linear span of $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_p\}$ is the whole vector space $\mathbf{V}$. Note that we have assumed $p < N$; hence, the number of elements of $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_p\}$ is strictly smaller than the number of elements of $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_p, \mathbf{e}_{p+1}, \cdots, \mathbf{e}_N\}$. In particular, $\mathbf{e}_N$ is in the linear span of $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_p\}$, and this **contradicts** the assumed linear independence of $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_p, \mathbf{e}_{p+1}, \cdots, \mathbf{e}_N\}$. Hence, we cannot have $p < N$; in other words, we must have $p \geq N$. □

We can now combine the previous two theorems in the following theorem:

Theorem 14. Let $(\mathbf{V}, +, \cdot)$ be a finite-dimensional real vector space of **dimension** N. Let $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)$ be a **basis** for $\mathbf{V}$. Then, we must have $p = N$.

Proof. Since $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p)$ is assumed to be a basis for $\mathbf{V}$, $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_p\}$ is **both** a **generating subset** for $\mathbf{V}$ and a **linearly independent** subset of $\mathbf{V}$; the first property implies $p \geq N$, and the second property implies $p \leq N$. Together, they imply $p = N$. □

We can establish the following **two very important corollaries** of the previous theorem:

(i) In a finite-dimensional real vector space, **all bases have the same number of elements** (and that number is the dimension of the vector space);

(ii) **To compute the dimension** of a finite-dimensional real vector space, it is enough to **find a basis** for it; the **dimension** of the vector space is then equal to the **number of elements of the basis**.

Let us illustrate the application of these results on some examples:

1. Consider the (by now extremely familiar) real vector space $(\mathbb{R}^2, +, \cdot)$. Let us compute the dimension of $\mathbb{R}^2$. As we have seen above, all we need to do is find a basis for $\mathbb{R}^2$; the dimension of $\mathbb{R}^2$ will then be equal to the number of elements of that basis. Consider then the following vectors in $\mathbb{R}^2$:

$$\mathbf{v}_1 = (1, 0), \quad \mathbf{v}_2 = (0, 1).$$

   We have already seen that $(\mathbf{v}_1, \mathbf{v}_2)$ is a basis of $\mathbb{R}^2$; since it has 2 elements, we conclude that $\mathbb{R}^2$ is a real vector space of dimension 2.

2. Consider the (equally familiar) real vector space $(\mathbb{R}^3, +, \cdot)$. Let us compute the dimension of $\mathbb{R}^3$. As we have seen above, all we need to do is find a basis for $\mathbb{R}^3$; the dimension of $\mathbb{R}^3$ will then be equal to the number of elements of that basis. Consider the following vectors in $\mathbb{R}^3$:

$$\mathbf{v}_1 = (1, 0, 0), \quad \mathbf{v}_2 = (0, 1, 0), \quad \mathbf{v}_3 = (0, 0, 1).$$

   We have already seen that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is a basis of $\mathbb{R}^3$; since it has 3 elements, we conclude that $\mathbb{R}^3$ is a real vector space of dimension 3.

3. More generally, let n be an integer ≥ 1 and consider the real vector space $(\mathbb{R}^n, +, \cdot)$. Let us compute the dimension of $\mathbb{R}^n$. Proceeding as before, let us construct a basis for $\mathbb{R}^n$; the dimension of $\mathbb{R}^n$ will then be given by the number of elements in that basis. For this, consider the following elements of $\mathbb{R}^n$:

$$\begin{aligned} \mathbf{v}_1 &= (1, 0, 0, 0, \cdots, 0), \\ \mathbf{v}_2 &= (0, 1, 0, 0, \cdots, 0), \\ \mathbf{v}_3 &= (0, 0, 1, 0, \cdots, 0), \\ &\cdots \\ \mathbf{v}_n &= (0, 0, 0, 0, \cdots, 1). \end{aligned}$$

(i.e. $\mathbf{v}_k$ is the $n-$tuple with the k^{th} entry equal to 1 and all other entries equal to 0). It is easy to verify that $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_n)$ is a basis of $\mathbb{R}^n$. Since it has exactly n elements, this shows that $\mathbb{R}^n$ has dimension n.

4. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^2$ defined as the set of all (x, y) in R^2 with $x = y$. Consider the vector $\mathbf{v}_1 = (1, 1)$ in $\mathbf{W}$. We have already seen (in the previous lecture) that $(\mathbf{v}_1)$ is a basis of $\mathbf{W}$. Since it has one element, we deduce that $\mathbf{W}$ is a real vector space of dimension 1.

5. Consider now the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all (x, y, z) in $\mathbb{R}^3$ with $x + y + z = 0$. Consider the vectors $\mathbf{v}_1 = (1, 0, -1)$ and $\mathbf{v}_2 = (0, 1, -1)$ of $\mathbf{W}$. We have already seen (in the previous lecture) that $(\mathbf{v}_1, \mathbf{v}_2)$ is a basis of $\mathbf{W}$. Since it has 2 elements, we conclude that $\mathbf{W}$ is a real vector space of dimension 2.

Let us restate once more the following important point:

- To **compute the dimension** of a real vector space, it is enough to **find a basis for that vector space**. The **dimension** of the vector space is then **equal to** the **number of elements of that basis**.

PROBLEMS:

1. Let $\mathcal{C}(\mathbb{R}; \mathbb{R})$ be the real vector space of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ (with addition and scalar multiplication defined as in $\mathcal{F}(\mathbb{R}; \mathbb{R})$). Show that $\mathcal{C}(\mathbb{R}; \mathbb{R})$ is an infinite-dimensional vector space.

2. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^2$ defined as the set of all $(x, y) \in \mathbb{R}^2$ such that $x + y = 0$. Show that $\mathbf{W}$ has dimension 1.

3. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^2$ defined as the set of all $(x, y) \in \mathbb{R}^2$ such that $2x + 3y = 0$. Show that $\mathbf{W}$ has dimension 1.

4. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^2$ defined as the set of all $(x, y) \in \mathbb{R}^2$ such that $5x - 7y = 0$. Show that $\mathbf{W}$ has dimension 1.

5. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^2$ defined as the set of all $(x, y) \in \mathbb{R}^2$ such that $x = 0$. Show that $\mathbf{W}$ has dimension 1.

6. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^2$ defined as the set of all $(x, y) \in \mathbb{R}^2$ such that $y = 0$. Show that $\mathbf{W}$ has dimension 1.

7. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $x - y = 0$. Show that $\mathbf{W}$ has dimension 2.

8. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $2x + y + z = 0$. Show that $\mathbf{W}$ has dimension 2.

9. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $x = 0$. Show that $\mathbf{W}$ has dimension 2.

10. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $y = 0$. Show that $\mathbf{W}$ has dimension 2.

11. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $z = 0$. Show that $\mathbf{W}$ has dimension 2.

12. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $x + y = 0$ **and** $z = 0$. Show that $\mathbf{W}$ has dimension 1.

13. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^3$ defined as the set of all $(x, y, z) \in \mathbb{R}^3$ such that $x - z = 0$ **and** $x + y + z = 0$. Show that $\mathbf{W}$ has dimension 1.

14. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x + y + z + w = 0$. Show that $\mathbf{W}$ has dimension 3.

15. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x + w = 0$. Show that $\mathbf{W}$ has dimension 3.

16. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x - y = 0$. Show that $\mathbf{W}$ has dimension 3.

17. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x = 0$. Show that $\mathbf{W}$ has dimension 3.

18. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $w = 0$. Show that $\mathbf{W}$ has dimension 3.

19. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x + y = 0$ **and** $z + w = 0$. Show that $\mathbf{W}$ has dimension 2.

20. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x+y+z+w = 0$ **and** $z-w = 0$. Show that $\mathbf{W}$ has dimension 2.

21. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x + 2w = 0$ **and** $2z + w = 0$. Show that $\mathbf{W}$ has dimension 2.

22. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x - y = 0$ **and** $z + w = 0$ **and** $y + w = 0$. Show that $\mathbf{W}$ has dimension 1.

23. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x + 2y + z = 0$ **and** $z = 0$ **and** $2y + w = 0$. Show that $\mathbf{W}$ has dimension 1.

24. Consider the vector subspace $\mathbf{W}$ of $\mathbb{R}^4$ defined as the set of all $(x, y, z, w) \in \mathbb{R}^4$ such that $x + 2y + z + w = 0$ **and** $x + y = 0$ **and** $y - z = 0$. Show that $\mathbf{W}$ has dimension 1.

Section 10

Study Topics

- Linear Transformations
- Range and Kernel of a Linear Transformation

In the previous lectures, we have studied vector spaces by themselves; for example, we have started from a real vector space, and we have found subspaces of that vector space, generating sets for that vector space, linearly dependent or independent subsets for that vector space, bases for that vector space, ... and so on. We now consider **functions between vector spaces**, i.e. functions from one vector space to another. Among these functions, there are some which have a desirable property (called linearity) which we will precisely define shortly; these functions are called linear, and are the main object of study of this and the next few lectures.

A WORD ON TERMINOLOGY: We will often use the words **mapping** and **transformation** instead of **function** – They will all mean the **same thing**.

Definition 24. Let $\mathbf{V}$ and $\mathbf{W}$ be two **real vector spaces**, and let $L : \mathbf{V} \to \mathbf{W}$ be a mapping from $\mathbf{V}$ to $\mathbf{W}$. L is said to be a **linear mapping** (also called a **linear transformation** or a **linear function**) if the following two properties are verified:

1. For any $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$, $L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2)$;
2. For any $\alpha \in \mathbb{R}$ and any $\mathbf{v} \in \mathbf{V}$, $L(\alpha\mathbf{v}) = \alpha L(\mathbf{v})$.

Before going further, let us give some examples of linear mappings:

1. Let $\mathbf{V}$ be a real vector space, and let $L : \mathbf{V} \to \mathbf{V}$ be the **identity mapping** of $\mathbf{V}$, defined by $L(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in \mathbf{V}$; it is easy to verify that L is a **linear mapping**.

2. Let $\mathbf{V}$ be a real vector space, let $\alpha \in \mathbb{R}$ be any real number, and let $L : \mathbf{V} \to \mathbf{V}$ be the mapping defined by $L(\mathbf{v}) = \alpha\mathbf{v}$ for all $\mathbf{v} \in \mathbf{V}$; it is easy to verify that L is a **linear mapping**.

3. Let $\mathbf{V}$ and $\mathbf{W}$ be real vector spaces, and let $\mathbf{0}_W$ denote the zero vector of $\mathbf{W}$. Let $L : \mathbf{V} \to \mathbf{W}$ denote the **zero mapping** from $\mathbf{V}$ to $\mathbf{W}$, defined by $L(\mathbf{v}) = \mathbf{0}_W$ for all $\mathbf{v} \in \mathbf{V}$ (i.e. everything in $\mathbf{V}$ is mapped to the zero vector of $\mathbf{W}$); here again, it is easy to verify that L is a **linear mapping**.

4. Consider the familiar vector spaces $\mathbb{R}^2$ and $\mathbb{R}$, and let $L : \mathbb{R}^2 \to \mathbb{R}$ be the mapping defined by $L((x, y)) = 2x + 3y$ for all $(x, y) \in \mathbb{R}^2$. Let us show that L is a **linear mapping**:

   (i) Let $\mathbf{v}_1 = (x_1, y_1) \in \mathbb{R}^2$ and $\mathbf{v}_2 = (x_2, y_2) \in \mathbb{R}^2$. We have to show that $L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2)$. We have:

$$\begin{aligned}
L(\mathbf{v}_1 + \mathbf{v}_2) &= L((x_1, y_1) + (x_2, y_2)) \\
&= L((x_1 + x_2, y_1 + y_2)) \\
&= 2(x_1 + x_2) + 3(y_1 + y_2) \\
&= (2x_1 + 3y_1) + (2x_2 + 3y_2) \\
&= L((x_1, y_1)) + L((x_2, y_2)) \\
&= L(\mathbf{v}_1) + L(\mathbf{v}_2),
\end{aligned}$$

which shows that the first property of a linear mapping is verified.

(ii) Let $\mathbf{v} = (x, y) \in \mathbb{R}^2$ and $\alpha \in \mathbb{R}$. We have to show that $L(\alpha\mathbf{v}) = \alpha L(\mathbf{v})$. We have:

$$\begin{aligned} L(\alpha\mathbf{v}) &= L(\alpha(x, y)) \\ &= L((\alpha x, \alpha y)) \\ &= 2(\alpha x) + 3(\alpha y) \\ &= \alpha(2x + 3y) \\ &= \alpha L((x, y)) \\ &= \alpha L(\mathbf{v}), \end{aligned}$$

which shows that the second property of a linear mapping is verified.

Both defining properties of a linear mapping are verified; we have therefore shown that the mapping L of this example is a **linear mapping**.

5. Consider the familiar real vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$, and let $L : \mathbb{R}^2 \to \mathbb{R}^3$ be the mapping defined by $L((x, y)) = (x-y, x+y, 2x+5y)$ for all $(x, y) \in \mathbb{R}^2$. It is easy to verify that L is a **linear mapping**.

6. Consider again the familiar real vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$, and let $L : \mathbb{R}^2 \to \mathbb{R}^3$ be the mapping defined by $L((x, y)) = (x, y, 0)$ for all $(x, y) \in \mathbb{R}^2$. It is easy to verify that L is a **linear mapping**.

7. Consider once more the familiar real vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$, and let $L : \mathbb{R}^3 \to \mathbb{R}^2$ be the mapping defined by $L((x, y, z)) = (x, y)$ for all $(x, y, z) \in \mathbb{R}^3$. It is easy to verify that L is a **linear mapping**.

8. Consider now the familiar real vector spaces $\mathbb{R}^3$ and $\mathbb{R}$, and let $L : \mathbb{R}^3 \to \mathbb{R}$ be the mapping defined by $L((x, y, z)) = x + y + z$ for all $(x, y, z) \in \mathbb{R}^3$. It is easy to verify that L is a **linear mapping**.

9. Consider now the real vector spaces $\mathcal{F}(\mathbb{R}; \mathbb{R})$ and $\mathbb{R}$ (recall $\mathcal{F}(\mathbb{R}; \mathbb{R})$ is the real vector space of all functions from $\mathbb{R}$ to $\mathbb{R}$), and let $L : \mathcal{F}(\mathbb{R}; \mathbb{R}) \to \mathbb{R}$ be the mapping defined by $L(f) = f(0)$ for all $f \in \mathcal{F}(\mathbb{R}; \mathbb{R})$. Let us prove that L is a linear mapping:

(i) We have to show that $\forall f_1, f_2 \in \mathcal{F}(\mathbb{R}; \mathbb{R})$, we have $L(f_1 + f_2) = L(f_1) + L(f_2)$. We have:

$$\begin{aligned} L(f_1 + f_2) &= (f_1 + f_2)(0) \\ &= f_1(0) + f_2(0) \\ &= L(f_1) + L(f_2), \end{aligned}$$

which shows that the first property of a linear mapping is verified.

(ii) Let now $f \in \mathcal{F}(\mathbb{R};\mathbb{R})$ and $\alpha \in \mathbb{R}$; we have to show that $L(\alpha f) = \alpha L(f)$. We have:

$$\begin{aligned} L(\alpha f) &= (\alpha f)(0) \\ &= \alpha f(0) \\ &= \alpha L(f), \end{aligned}$$

which shows that the second property of a linear mapping is verified.

Both defining properties of a linear mapping are verified; we have therefore shown that the mapping L of this example is a **linear mapping**.

10. Consider again the real vector spaces $\mathcal{F}(\mathbb{R};\mathbb{R})$ and $\mathbb{R}$, and let $L : \mathcal{F}(\mathbb{R};\mathbb{R}) \to \mathbb{R}$ be the mapping defined by $L(f) = 5f(1) + 7f(2)$ for all $f \in \mathcal{F}(\mathbb{R};\mathbb{R})$. It is easy to verify that L is indeed a **linear mapping**.

11. Consider now the real vector spaces $C([0,1];\mathbb{R})$ and $\mathbb{R}$, where $C([0,1];\mathbb{R})$ denotes the set of all **continuous** functions from $[0,1]$ to $\mathbb{R}$ (with addition and scalar multiplication defined as for $\mathcal{F}(\mathbb{R};\mathbb{R})$; $C([0,1];\mathbb{R})$ is actually a vector subspace of $\mathcal{F}(\mathbb{R};\mathbb{R})$ (prove it as an exercise!)). Define the mapping $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ by $L(f) = \int_0^1 f(t)dt$, for all $f \in C([0,1];\mathbb{R})$. Let us prove that L is a linear mapping:

    (i) We have to show that $\forall f_1, f_2 \in C([0,1];\mathbb{R})$, we have $L(f_1 + f_2) = L(f_1) + L(f_2)$. We have:

    $$\begin{aligned} L(f_1 + f_2) &= \int_0^1 (f_1 + f_2)(t)dt \\ &= \int_0^1 (f_1(t) + f_2(t))dt \\ &= \int_0^1 f_1(t)dt + \int_0^1 f_2(t)dt \\ &= L(f_1) + L(f_2), \end{aligned}$$

    which shows that the first property of a linear mapping is verified.

    (ii) Let now $f \in C([0,1];\mathbb{R})$ and $\alpha \in \mathbb{R}$; we have to show that $L(\alpha f) = \alpha L(f)$. We have:

    $$\begin{aligned} L(\alpha f) &= \int_0^1 (\alpha f)(t)dt \\ &= \int_0^1 (\alpha f(t))dt \\ &= \alpha \int_0^1 f(t)dt \\ &= \alpha L(f), \end{aligned}$$

    which shows that the second property of a linear mapping is verified.

Both defining properties of a linear mapping are verified; we have therefore shown that the mapping L of this example is a **linear mapping**.

Before going further and giving examples of mappings between vector spaces which are **not** linear, we prove the following useful and simple theorem:

Theorem 15. Let $\mathbf{V}$ and $\mathbf{W}$ be real vector spaces; let $\mathbf{0}_V$ denote the zero vector of $\mathbf{V}$, and let $\mathbf{0}_W$ denote the zero vector of $\mathbf{W}$. let $L : \mathbf{V} \to \mathbf{W}$ be a **linear mapping**. Then, we have:

$$L(\mathbf{0}_V) = \mathbf{0}_W.$$

What the above theorem says, in other words, is the following: **if** $L : \mathbf{V} \to \mathbf{W}$ is **linear**, then it **must** map the zero vector of $\mathbf{V}$ to the zero vector of $\mathbf{W}$. Where can we use this theorem ? Well, if we ever stumble upon a mapping $L : \mathbf{V} \to \mathbf{W}$ which maps the zero vector of $\mathbf{V}$ to **something other** than the zero vector of $\mathbf{W}$, then we can be sure that L is **not** a linear mapping. Before going further, we prove the theorem:

Proof. Let $\alpha = 0$ (i.e. α is the real number zero); we have $\alpha\mathbf{0}_V = \mathbf{0}_V$ (we have already shown that any real number times the zero vector is equal to the zero vector, and in particular if that real number happens to be zero), and therefore, we can write:

$$\begin{aligned} L(\mathbf{0}_V) &= L(\alpha\mathbf{0}_V) \\ &= \alpha L(\mathbf{0}_V) \\ &= 0L(\mathbf{0}_V) \\ &= \mathbf{0}_W \end{aligned}$$

since, as we have already shown, the real number 0 times any vector of a vector space is equal to the zero vector of that vector space. □

Let us now examine mappings between vector spaces, which are **not** linear.

1. Let $\mathbf{V}$ and $\mathbf{W}$ be real vector spaces, and let $\mathbf{w} \in \mathbf{W}$ be a given vector in $\mathbf{W}$ such that $\mathbf{w} \neq \mathbf{0}_W$ (i.e. $\mathbf{w}$ is **not** the zero vector of $\mathbf{W}$). Define the mapping $L : \mathbf{V} \to \mathbf{W}$ by $L(\mathbf{v}) = \mathbf{w}$, for all $\mathbf{v} \in \mathbf{V}$. We have:

$$L(\mathbf{0}_V) = \mathbf{w} \neq \mathbf{0}_W,$$

   i.e. L maps the zero vector of $\mathbf{V}$ to something other than the zero vector of $\mathbf{W}$; it follows therefore from the previous theorem that the mapping L is **not linear**.

2. Let $\mathbf{V}$ be a real vector space, let $\lambda \in \mathbb{R}$ be a real number, and let $\mathbf{v}_1$ be a vector in $\mathbf{V}$ such that $\mathbf{v}_1 \neq \mathbf{0}_V$ (i.e. $\mathbf{v}_1$ is distinct from the zero vector of

$\mathbf{V}$). Let $L : \mathbf{V} \to \mathbf{V}$ be the mapping defined by $L(\mathbf{v}) = \lambda\mathbf{v} + \mathbf{v}_1$, for all $\mathbf{v} \in \mathbf{V}$. We have:

$$\begin{aligned} L(\mathbf{0}_V) &= \lambda\mathbf{0}_V + \mathbf{v}_1 \\ &= \mathbf{0}_V + \mathbf{v}_1 \\ &= \mathbf{v}_1 \neq \mathbf{0}_V, \end{aligned}$$

and since L maps the zero vector of $\mathbf{V}$ to something other than the zero vector of $\mathbf{V}$, it follows from the previous theorem that the mapping L is **not linear**.

3. Consider the real vector spaces $\mathbb{R}^2$ and $\mathbb{R}$, and let $L : \mathbb{R}^2 \to \mathbb{R}$ be the mapping defined by $L((x,y)) = x^2 + y^2$ for all $(x,y) \in \mathbb{R}^2$. Let us show that the mapping L is not linear. The previous theorem is not of much help here, since L does indeed map the zero vector of $\mathbb{R}^2$ (namely the pair $(0,0)$) to the zero vector of $\mathbb{R}$ (namely the real number 0); indeed, we have:

$$L((0,0)) = 0^2 + 0^2 = 0 + 0 = 0;$$

so we cannot use the previous theorem to show that L is not linear, unlike what we did in the previous examples.

So how do we proceed ? Well, we have to go back to the definition. From there, it is clear that it is enough to find two vectors $\mathbf{v}_1, \mathbf{v}_2$ in $\mathbb{R}^2$ for which $L(\mathbf{v}_1 + \mathbf{v}_2)$ is not equal to $L(\mathbf{v}_1) + L(\mathbf{v}_2)$, or a real number α and a vector $\mathbf{v}$ in $\mathbb{R}^2$ such that $L(\alpha\mathbf{v})$ is not equal to $\alpha L(\mathbf{v})$, in order to conclude that L is not a linear mapping.

Let us choose for example $\alpha = 2$ and $\mathbf{v} = (1,1)$. For these choices of α and $\mathbf{v}$, we have:

$$\begin{aligned} L(\alpha\mathbf{v}) &= L(2(1,1)) = L(2,2) = 2^2 + 2^2 = 4 + 4 = 8, \\ \alpha L(\mathbf{v}) &= 2L((1,1)) = 2(1^2 + 1^2) = 2(1+1) = 4. \end{aligned}$$

Hence, we have found some real number α (namely $\alpha = 2$) and some vector $\mathbf{v}$ in $\mathbb{R}^2$ (namely $\mathbf{v} = (1,1)$) for which $L(\alpha\mathbf{v})$ is **not** equal to $\alpha L(\mathbf{v})$. This shows that the second property in the definition of a linear mapping does **not** hold for our mapping L, and we conclude from this that the mapping L is **not linear**.

4. Consider the real vector space $\mathbb{R}^2$, and let $L : \mathbb{R}^2 \to \mathbb{R}^2$ be the mapping defined by $L((x,y)) = (x^3 + y, x - y)$ for all $(x,y) \in \mathbb{R}^2$. It is easy to verify here as well that the mapping L defined here is **not linear**.

5. Consider the real vector space $C([0,1];\mathbb{R})$ of all continuous functions from $[0,1]$ to $\mathbb{R}$, and define the mapping $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ from the real vector space $C([0,1];\mathbb{R})$ to the real vector space $\mathbb{R}$ as follows: $L(f) = \int_0^1 (f(t))^2 dt$ for all $f \in C([0,1];\mathbb{R})$. Let us show that L is not a linear

mapping. For this, let us show that the second property in the definition of a linear mapping fails in this case. Let then $\alpha = 2$, and define the vector $f \in C([0,1];\mathbb{R})$ as follows (recall that in the real vector space $C([0,1];\mathbb{R})$, a vector is nothing other than a continuous function from $[0,1]$ to $\mathbb{R}$): $f(t) = 1$, for all $t \in \mathbb{R}$ (in other words, f is defined to be the constant function on $[0,1]$ which maps every $t \in [0,1]$ to the real number 1). Clearly, f is continuous on $[0,1]$ with values in $\mathbb{R}$, and hence is an honest element of $C([0,1];\mathbb{R})$. With these choices of $\alpha \in \mathbb{R}$ and $f \in C([0,1];\mathbb{R})$, let us compute $L(\alpha f)$ and $\alpha L(f)$. We have:

$$
\begin{aligned}
L(\alpha f) &= \int_0^1 ((\alpha f)(t))^2 dt \\
&= \int_0^1 (\alpha f(t))^2 dt \\
&= \int_0^1 \alpha^2 (f(t))^2 dt \\
&= \alpha^2 \int_0^1 (f(t))^2 dt \\
&= 2^2 \int_0^1 (1)^2 dt \\
&= 4 \int_0^1 dt \\
&= 4,
\end{aligned}
$$

whereas

$$
\begin{aligned}
\alpha L(f) &= \alpha \int_0^1 (f(t))^2 dt \\
&= 2 \int_0^1 (1)^2 dt \\
&= 2 \int_0^1 dt \\
&= 2,
\end{aligned}
$$

which shows that for these choices of $\alpha \in \mathbb{R}$ and $f \in C([0,1];\mathbb{R})$, $L(\alpha f)$ is **not** equal to $\alpha L(f)$, and this shows that the second property in the definition of a linear mapping does **not** hold for our mapping L, and we conclude from this that the mapping L is **not linear**.

Now that we have seen examples of linear (and non-linear) mappings between vector spaces, let us examine an interesting property of linear mappings: Consider three real vector spaces $\mathbf{V}$, $\mathbf{W}$, and $\mathbf{Z}$, let $L_1 : \mathbf{V} \to \mathbf{W}$ be a mapping from the real vector space $\mathbf{V}$ to the real vector space $\mathbf{W}$, and $L_2 : \mathbf{W} \to \mathbf{Z}$ a a mapping from the real vector space $\mathbf{W}$ to the real vector space $\mathbf{Z}$. We know we can then define a mapping from $\mathbf{V}$ to $\mathbf{Z}$, which we denote by $L_2 \circ L_1$ (pay attention to the order!) as follows:

- $L_2 \circ L_1 : \mathbf{V} \to \mathbf{Z}$ is defined to be the mapping from $\mathbf{V}$ to $\mathbf{Z}$ which maps every element $\mathbf{v} \in \mathbf{V}$ to the element $L_2(L_1(\mathbf{v}))$ of $\mathbf{Z}$.

$L_2 \circ L_1$ is called the **composition** of the two mappings L_1 and L_2; its definition is very intuitive: If we are given $\mathbf{v}$ in $\mathbf{V}$ and we want to compute $L_2 \circ L_1(\mathbf{v})$, we first "apply" L_1 to $\mathbf{v}$, obtaining the element $L_1(\mathbf{v})$ of $\mathbf{W}$. Since $L_1(\mathbf{v})$ is **in** $\mathbf{W}$ and since the mapping L_2 maps **from** $\mathbf{W}$ (to wherever), it makes sense to "apply" L_2 to $L_1(\mathbf{v})$. We then "apply" L_2 to $L_1(\mathbf{v})$, obtaining the element of $L_2(L_1(\mathbf{v}))$ of $\mathbf{Z}$, and it is this last element that we denote by $L_2 \circ L_1(\mathbf{v})$.
Let us now again consider three real vector spaces $\mathbf{V}$, $\mathbf{W}$, and $\mathbf{Z}$, let $L_1 : \mathbf{V} \to \mathbf{W}$ be a mapping from the real vector space $\mathbf{V}$ to the real vector space $\mathbf{W}$, and $L_2 : \mathbf{W} \to \mathbf{Z}$ a a mapping from the real vector space $\mathbf{W}$ to the real vector space $\mathbf{Z}$; assume now that L_1 and L_2 are both **linear** mappings. What can we say then about the mapping $L_2 \circ L_1$? The answer is given by the following theorem:

Theorem 16. Let $\mathbf{V}$, $\mathbf{W}$, and $\mathbf{Z}$ be real vector spaces, and let $L_1 : \mathbf{V} \to \mathbf{W}$ and $L_2 : \mathbf{W} \to \mathbf{Z}$ be **linear** mappings. Then, the mapping $L_2 \circ L_1 : \mathbf{V} \to \mathbf{Z}$ is also **linear**.

Proof. We have to show that for any $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$, $L_2 \circ L_1(\mathbf{v}_1 + \mathbf{v}_2)$ is equal to $L_2 \circ L_1(\mathbf{v}_1) + L_2 \circ L_1(\mathbf{v}_2)$, and that for any $\alpha \in \mathbb{R}$ and any $\mathbf{v} \in \mathbf{V}$, $L_2 \circ L_1(\alpha\mathbf{v})$ is equal to $\alpha(L_2 \circ L_1(\mathbf{v}))$. Let us then prove these properties in turn:

(i) Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$; we have, using the linearity of L_1 and L_2:

$$\begin{aligned} L_2 \circ L_1(\mathbf{v}_1 + \mathbf{v}_2) &= L_2(L_1(\mathbf{v}_1 + \mathbf{v}_2)) \\ &= L_2(L_1(\mathbf{v}_1) + L_1(\mathbf{v}_2)) \\ &= L_2(L_1(\mathbf{v}_1)) + L_2(L_1(\mathbf{v}_2)) \\ &= L_2 \circ L_1(\mathbf{v}_1) + L_2 \circ L_1(\mathbf{v}_2), \end{aligned}$$

which proves the first property in the definition of a linear mapping.

(ii) Let now $\alpha \in \mathbb{R}$ and $\mathbf{v} \in \mathbf{V}$; we have, using the linearity of L_1 and L_2:

$$\begin{aligned} L_2 \circ L_1(\alpha\mathbf{v}) &= L_2(L_1(\alpha\mathbf{v})) \\ &= L_2(\alpha L_1(\mathbf{v})) \\ &= \alpha L_2(L_1(\mathbf{v})) \\ &= \alpha(L_2 \circ L_1(\mathbf{v})), \end{aligned}$$

which proves the second property in the definition of a linear mapping.

We have shown that $L_2 \circ L_1$ satisfies both properties of the definition of a linear mapping; it follows that $L_2 \circ L_1$ is a **linear** mapping. □

Let us now consider two real vector spaces $\mathbf{V}$ and $\mathbf{W}$ and a **linear** mapping $L : \mathbf{V} \to \mathbf{W}$. Consider the set of all $\mathbf{v}$ in $\mathbf{V}$ which are mapped to the zero vector $\mathbf{0}_W$ of $\mathbf{W}$ by L, i.e. the set of all $\mathbf{v} \in \mathbf{V}$ for which $L(\mathbf{v}) = \mathbf{0}_W$. Let us give a name to the set of all such elements of $\mathbf{V}$; we denote by $\ker(L)$ (and we call this "**Kernel of** L or **Null Space of** L") the set of all $\mathbf{v} \in \mathbf{V}$ for which $L(\mathbf{v}) = \mathbf{0}_W$; we can write this statement more formally as:

$$\ker(L) = \{\mathbf{v} \in \mathbf{V} | L(\mathbf{v}) = \mathbf{0}_W\}.$$

What do we know about $\ker(L)$? Well, the first thing we know about $\ker(L)$, which follows straight from its definition, is that it is a **subset** of $\mathbf{V}$. But as the following theorem will show, $\ker(L)$ is not just any old subset of $\mathbf{V}$; rather, it is a **vector subspace** of $\mathbf{V}$.

Theorem 17. Let $\mathbf{V}$ and $\mathbf{W}$ be real vector spaces, and let $L : \mathbf{V} \to \mathbf{W}$ be a **linear** mapping. Then, the kernel $\ker(L)$ of L is a **vector subspace** of $\mathbf{V}$.

Proof. To show that $\ker(L)$ is a vector subspace of the real vector space $\mathbf{V}$, we have to show that:

(i) The zero vector $\mathbf{0}_V$ of $\mathbf{V}$ is in $\ker(L)$,

(ii) for any $\mathbf{v}_1$ and $\mathbf{v}_2$ in $\ker(L)$, $\mathbf{v}_1 + \mathbf{v}_2$ is also in $\ker(L)$,

(iii) for any $\mathbf{v}$ in $\ker(L)$ and any α in $\mathbb{R}$, $\alpha\mathbf{v}$ is also in $\ker(L)$.

- We know from the first theorem we proved in this lecture that (by linearity of L) $L(\mathbf{0}_V) = \mathbf{0}_W$, from which we obtain that $\mathbf{0}_V$ is indeed in $\ker(L)$ (by definition of $\ker(L)$); i.e. we have shown property (i), namely that $\mathbf{0}_V \in \ker(L)$.

- Let us now prove property (ii). Let then then $\mathbf{v}_1, \mathbf{v}_2 \in \ker(L)$; we have to show that $\mathbf{v}_1 + \mathbf{v}_2$ is also in $\ker(L)$, i.e. that $L(\mathbf{v}_1 + \mathbf{v}_2) = \mathbf{0}_W$. But, by linearity of L and the fact that $\mathbf{v}_1$ and $\mathbf{v}_2$ are assumed to be in $\ker(L)$ (and therefore $L(\mathbf{v}_1) = \mathbf{0}_W$ and $L(\mathbf{v}_2) = \mathbf{0}_W$):

$$\begin{aligned} L(\mathbf{v}_1 + \mathbf{v}_2) &= L(\mathbf{v}_1) + L(\mathbf{v}_2) \\ &= \mathbf{0}_W + \mathbf{0}_W \\ &= \mathbf{0}_W, \end{aligned}$$

  which proves that $\mathbf{v}_1 + \mathbf{v}_2$ is also in $\ker(L)$. This proves property (ii).

- Let us now prove property (iii). Let then then $\mathbf{v} \in \ker(L)$ and $\alpha \in \mathbb{R}$; we have to show that $\alpha\mathbf{v}$ is also in $\ker(L)$, i.e. that $L(\alpha\mathbf{v}) = \mathbf{0}_W$. But, by linearity of L and the fact that $\mathbf{v}$ is assumed to be in $\ker(L)$ (and therefore $L(\mathbf{v}) = \mathbf{0}_W$):

$$\begin{aligned} L(\alpha\mathbf{v}) &= \alpha L(\mathbf{v}) \\ &= \alpha\mathbf{0}_W \\ &= \mathbf{0}_W, \end{aligned}$$

  which proves that $\alpha\mathbf{v}$ is also in $\ker(L)$. This proves property (iii).

We have shown that $\ker(L)$ satisfies all three properties of a vector subspace; this shows that $\ker(L)$ is a **vector subspace** of $\mathbf{V}$. □

Recall that a mapping $L : \mathbf{V} \to \mathbf{W}$ is said to be **injective** or **one-to-one** if for any two elements $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ with $\mathbf{v}_1 \neq \mathbf{v}_2$ it must follow that $L(\mathbf{v}_1) \neq L(\mathbf{v}_2)$; equivalently, L is injective if for any $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$, the equality $L(\mathbf{v}_1) = L(\mathbf{v}_2)$ implies $\mathbf{v}_1 = \mathbf{v}_2$ (i.e two distinct elements in $\mathbf{V}$ cannot map to the same value under L). The following theorem relates the property of L being injective to the kernel $\ker(L)$ of L.

Theorem 18. Let $L : \mathbf{V} \to \mathbf{W}$ be a **linear** mapping from the real vector space $\mathbf{V}$ to the real vector space $\mathbf{W}$. We have:

- L is **injective** if and only if the kernel $\ker(L)$ of L is equal to $\{\mathbf{0}_V\}$, i.e. $\ker(L) = \{\mathbf{0}_V\}$.

Proof. (i) Assume first that L is injective; we have to show then that if $\mathbf{v} \in \ker(L)$, then $\mathbf{v} = \mathbf{0}_V$ (i.e. the only element of $\ker(L)$ is the zero vector of $\mathbf{V}$). Let then $\mathbf{v} \in \ker(L)$. Then, $L(\mathbf{v}) = \mathbf{0}_W$ (by definition of $\mathbf{v}$ being an element of the kernel $\ker(L)$ of L). On the other hand, we also know that $L(\mathbf{0}_V) = \mathbf{0}_W$. We therefore have:

$$L(\mathbf{v}) = L(\mathbf{0}_V).$$

Since L is assumed injective, it must follow that $\mathbf{v} = \mathbf{0}_V$. Hence, we have shown that if $\mathbf{v}$ is any element in $\ker(L)$, then it must follow that $\mathbf{v} = \mathbf{0}_V$; this shows that $\ker(L) = \{\mathbf{0}_V\}$.

(ii) Let us now assume that $\ker(L) = \{\mathbf{0}_V\}$; we have to show then that for any $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$, the equality $L(\mathbf{v}_1) = L(\mathbf{v}_2)$ implies that $\mathbf{v}_1 = \mathbf{v}_2$. Let then $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ and assume that $L(\mathbf{v}_1) = L(\mathbf{v}_2)$. Hence, by linearity of L:

$$\begin{aligned} L(\mathbf{v}_1 - \mathbf{v}_2) &= L(\mathbf{v}_1 + (-1)\mathbf{v}_2) \\ &= L(\mathbf{v}_1) + L((-1)\mathbf{v}_2) \\ &= L(\mathbf{v}_1) + (-1)L(\mathbf{v}_2) \\ &= L(\mathbf{v}_1) - L(\mathbf{v}_2) \\ &= \mathbf{0}_W, \end{aligned}$$

which shows that $\mathbf{v}_1 - \mathbf{v}_2 \in \ker(L)$ (since $L(\mathbf{v}_1 - \mathbf{v}_2) = \mathbf{0}_W$). Since we have assumed that $\ker(L) = \{\mathbf{0}_V\}$, it must follow that $\mathbf{v}_1 - \mathbf{v}_2 = \mathbf{0}_V$, i.e. that $\mathbf{v}_1 = \mathbf{v}_2$. This is what we wanted to show, and this establishes injectivity of L.

□

Let us now consider again a linear mapping $L : \mathbf{V} \to \mathbf{W}$ from a real vector space $\mathbf{V}$ to a real vector space $\mathbf{W}$. Consider now the subset $\mathrm{Im}(L)$ of $\mathbf{W}$ (Note:

subset of $\mathbf{W}$, not of $\mathbf{V}$ like last time!) defined formally by:

$$\mathrm{Im}(L) = \{L(\mathbf{v}) \in \mathbf{W} | \mathbf{v} \in \mathbf{V}\};$$

Here are, in plain English, two equivalent definitions for $\mathrm{Im}(L)$:

- $\mathrm{Im}(L)$ is the set of all values in $\mathbf{W}$ that L can take.
- $\mathbf{w}$ is in $\mathrm{Im}(L)$ if and only if there exists a $\mathbf{v}$ in $\mathbf{V}$ such that $\mathbf{w} = L(\mathbf{v})$.

$\mathrm{Im}(L)$ is called the **Range of** L or **Image of** L.
What do we know about $\mathrm{Im}(L)$? Well, by its very definition, it is a subset of $\mathbf{W}$; but as the following result will show, $\mathrm{Im}(L)$ is not just any old subset of $\mathbf{W}$, rather, it is a **vector subspace** of $\mathbf{W}$.

Theorem 19. Let $\mathbf{V}$ and $\mathbf{W}$ be real vector spaces, and let $L : \mathbf{V} \to \mathbf{W}$ be a **linear mapping**. Then, the range $\mathrm{Im}(L)$ of L is a **vector subspace** of $\mathbf{W}$.

Proof. We have to prove that $\mathrm{Im}(L)$ satisfies the three properties that a vector subspace of $\mathbf{W}$ should satisfy, namely, we have to show that:

(i) The zero vector $\mathbf{0}_W$ of $\mathbf{W}$ is in $\mathrm{Im}(L)$,

(ii) for any $\mathbf{v}_1$ and $\mathbf{v}_2$ in $\mathrm{Im}(L)$, $\mathbf{v}_1 + \mathbf{v}_2$ is also in $\mathrm{Im}(L)$,

(iii) for any $\mathbf{v}$ in $\mathrm{Im}(L)$ and any α in $\mathbb{R}$, $\alpha\mathbf{v}$ is also in $\mathrm{Im}(L)$.

- We know from the first theorem we proved in this lecture that (by linearity of L) $L(\mathbf{0}_V) = \mathbf{0}_W$, from which we obtain that there exists an element in $\mathbf{V}$ (namely the zero vector of $\mathbf{V}$) which is mapped by L to the zero vector $\mathbf{0}_W$ of $\mathbf{W}$; this shows that $\mathbf{0}_W$ is in the range of L, i.e. $\mathbf{0}_W \in \mathrm{Im}(L)$. Hence, we have shown property (i).

- Let us now prove property (ii). Let then then $\mathbf{w}_1, \mathbf{w}_2 \in \mathrm{Im}(L)$; we have to show that $\mathbf{w}_1 + \mathbf{w}_2$ is also in $\mathrm{Im}(L)$, i.e. we have to show that $\mathbf{w}_1 + \mathbf{w}_2$ is L of something in $\mathbf{V}$. Since we have $\mathbf{w}_1 \in \mathrm{Im}(L)$, by definition of $\mathrm{Im}(L)$, there must exist a vector in $\mathbf{V}$, call it $\mathbf{v}_1$, such that $L(\mathbf{v}_1) = \mathbf{w}_1$. Similarly, since we have $\mathbf{w}_2 \in \mathrm{Im}(L)$, by definition of $\mathrm{Im}(L)$, there must exist a vector in $\mathbf{V}$, call it $\mathbf{v}_2$, such that $L(\mathbf{v}_2) = \mathbf{w}_2$. Consider now the vector $\mathbf{v}$ in $\mathbf{V}$ defined by $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$ (i.e. $\mathbf{v}$ is defined to be the sum of the two vectors $\mathbf{v}_1$ and $\mathbf{v}_2$). We have:

$$\begin{aligned} L(\mathbf{v}) &= L(\mathbf{v}_1 + \mathbf{v}_2) \\ &= L(\mathbf{v}_1) + L(\mathbf{v}_2) \\ &= \mathbf{w}_1 + \mathbf{w}_2, \end{aligned}$$

  which proves that $\mathbf{w}_1 + \mathbf{w}_2$ is in the range of L, i.e. $\mathbf{w}_1 + \mathbf{w}_2 \in \mathrm{Im}(L)$ (since we have been able to write $\mathbf{w}_1 + \mathbf{w}_2$ as L of something in $\mathbf{V}$). This proves property (ii).

- Let us now prove property (iii). Let then then $\mathbf{w} \in \mathrm{Im}(L)$ and $\alpha \in \mathbb{R}$; we have to show that $\alpha\mathbf{w}$ is also in $\mathrm{Im}(L)$, i.e. we have to show that $\alpha\mathbf{w}$ is L of something in $\mathbf{V}$. We have:

$$\begin{aligned} L(\alpha\mathbf{v}) &= \alpha L(\mathbf{v}) \\ &= \alpha\mathbf{w}, \end{aligned}$$

  which proves that $\alpha\mathbf{w}$ is in $\mathrm{Im}(L)$ (since we have written $\alpha\mathbf{w}$ as L of something in $\mathbf{V}$). This proves property (iii).

We have shown that $\mathrm{Im}(L)$ satisfies all three properties of a vector subspace; this shows that $\mathrm{Im}(L)$ is a **vector subspace** of $\mathbf{W}$. □

We close this section with some important terminology and an important theorem which we shall merely state and not prove:

Definition 25. Let $\mathbf{V}, \mathbf{W}$ be real vector spaces, assume $\mathbf{V}$ is **finite-dimensional**, and let $L : \mathbf{V} \to \mathbf{W}$ be a **linear mapping**.

(i) The **rank of** L is defined to be the **dimension of** $\mathrm{Im}(L)$, and is denoted by $\mathrm{rank}(L)$.

(ii) The **nullity of** L is defined to be the **dimension of** $\ker(L)$, and is denoted by $\mathrm{nullity}(L)$.

The following **important theorem** is known as the **Rank-Nullity theorem**:

Theorem 20. Let $\mathbf{V}, \mathbf{W}$ be real vector spaces, and let $L : \mathbf{V} \to \mathbf{W}$ be a **linear mapping**. Assume $\mathbf{V}$ is **finite-dimensional**, and let N denote the dimension of $\mathbf{V}$. Then:

$$\mathrm{rank}(L) + \mathrm{nullity}(L) = N.$$

PROBLEMS:

Show which of the following mappings between real vector spaces are linear and which are not linear:

1. $L : \mathbb{R} \to \mathbb{R}$, defined by $L(x) = 2x + 1$.
2. $L : \mathbb{R} \to \mathbb{R}$, defined by $L(x) = x^2 + x$.
3. $L : \mathbb{R} \to \mathbb{R}^2$, defined by $L(x) = (x, 3x)$.
4. $L : \mathbb{R} \to \mathbb{R}^2$, defined by $L(x) = (x + 5, 3x)$.
5. $L : \mathbb{R} \to \mathbb{R}^2$, defined by $L(x) = (x + x^2, 2x)$.

6. $L : \mathbb{R} \to \mathbb{R}^2$, defined by $L(x) = (3x, 2x - 1)$.
7. $L : \mathbb{R}^2 \to \mathbb{R}^2$, defined by $L((x, y)) = (x + y, x - y)$.
8. $L : \mathbb{R}^2 \to \mathbb{R}^2$, defined by $L((x, y)) = (x^2 + y, x - y^2)$.
9. $L : \mathbb{R}^2 \to \mathbb{R}^2$, defined by $L((x, y)) = (x^2 + y^2, x^2 - y^2)$.
10. $L : \mathbb{R}^2 \to \mathbb{R}^3$, defined by $L((x, y)) = (x + y, x - y, xy)$.
11. $L : \mathbb{R}^2 \to \mathbb{R}^3$, defined by $L((x, y)) = (x + y, x - y, x)$.
12. $L : \mathbb{R}^2 \to \mathbb{R}^3$, defined by $L((x, y)) = (x + y, x - y, 3y)$.
13. $L : \mathbb{R}^2 \to \mathbb{R}^3$, defined by $L((x, y)) = (x + y + 1, x - y, 3y)$.
14. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (x + z, x - y, 3z)$.
15. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (z, x, y)$.
16. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (z, y, x)$.
17. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (z, x, z)$.
18. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (x, x, x)$.
19. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (x, x, x + 1)$.
20. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (x, x^2, x^3)$.
21. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (zx, xy, yz)$.
22. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (2x + y, y - 3z, x + y + z)$.
23. $L : \mathbb{R}^3 \to \mathbb{R}^3$, defined by $L((x, y, z)) = (x^2, y^2, z^2)$.
24. $L : \mathbb{R}^3 \to \mathbb{R}^2$, defined by $L((x, y, z)) = (x, y)$.
25. $L : \mathbb{R}^3 \to \mathbb{R}^2$, defined by $L((x, y, z)) = (x, z)$.
26. $L : \mathbb{R}^3 \to \mathbb{R}^2$, defined by $L((x, y, z)) = (y, z)$.
27. $L : \mathbb{R}^3 \to \mathbb{R}^2$, defined by $L((x, y, z)) = (y, x)$.
28. $L : \mathbb{R}^3 \to \mathbb{R}$, defined by $L((x, y, z)) = x + y + z$.
29. $L : \mathbb{R}^3 \to \mathbb{R}$, defined by $L((x, y, z)) = x + y + z + 2$.
30. $L : \mathbb{R}^3 \to \mathbb{R}$, defined by $L((x, y, z)) = x^2 + y^2 + z^2$.
31. $L : \mathbb{R}^3 \to \mathbb{R}$, defined by $L((x, y, z)) = x^3 + y^3 + z^3$.
32. $L : \mathbb{R}^3 \to \mathbb{R}$, defined by $L((x, y, z)) = xyz$.
33. $L : \mathcal{F}(\mathbb{R}; \mathbb{R}) \to \mathbb{R}$ defined by $L(f) = 2f(-1) + 5f(1)$.

34. $L : \mathcal{F}(\mathbb{R};\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = f(0)f(1)$.

35. $L : \mathcal{F}(\mathbb{R};\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = f(-2) + (f(1))^2$.

36. $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = \int_{1/2}^{1} f(t)dt$.

37. $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = \int_0^{1/2} f(t)dt - \int_{1/2}^{1} f(t)dt$.

38. $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = \int_0^{1/2} f(t)dt - \int_{1/2}^{1}(f(t))^2 dt$.

39. $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = 1 + \int_0^{1/2} f(t)dt - \int_{1/2}^{1} f(t)dt$.

40. $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = f(3/4) - \int_0^{1/2} f(t)dt - \int_{1/2}^{1} f(t)dt$.

41. $L : C([0,1];\mathbb{R}) \to \mathbb{R}$ defined by $L(f) = (f(3/4))^2 - \int_0^{1/2} f(t)dt - \int_{1/2}^{1} f(t)dt$.

42. Let $(\mathbf{V}, +, \cdot)$ and $(\mathbf{W}, +, \cdot)$ real vector spaces, and let $L : \mathbf{V} \to \mathbf{W}$ linear. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$. Show that if $L(\mathbf{v}_1), L(\mathbf{v}_2)$ are linearly independent, then $\mathbf{v}_1, \mathbf{v}_2$ are linearly independent.

43. Let $(\mathbf{V}, +, \cdot)$ and $(\mathbf{W}, +, \cdot)$ real vector spaces, and let $L : \mathbf{V} \to \mathbf{W}$ linear. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$. Show that if $\mathbf{v}_1, \mathbf{v}_2$ are linearly independent and $\text{Ker}(L) = \{\mathbf{0}_\mathbf{V}\}$, then $L(\mathbf{v}_1), L(\mathbf{v}_2)$ are linearly independent.

Section 11

Study Topics

- Real Matrices
- Linear Transformations Defined by Matrices
- Range and Kernel of a Matrix

In the previous lecture, we have studied a special class of functions from one real vector space to another, namely those that were linear, and we called them **linear functions**, or, equivalently, **linear mappings**, or equivalently, **linear transformations**. In this lecture, we introduce the notion of a real "matrix". What is a real matrix ? Think of it as a table, with, say m rows and n columns, of real numbers. That's it! So what's the relation between a matrix and a linear transformation ? As we will see in this lecture, a real matrix with m rows and n columns will allow us to define a **linear transformation** from $\widehat{\mathbb{R}^n}$ to $\widehat{\mathbb{R}^m}$.

Definition 26. Let m and n be integers ≥ 1. A **real matrix with m rows and n columns** (also called a **real $m \times n$ matrix**) is a table (or array) of the form:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

where all the entries (i.e. $a_{1,1}, a_{1,2}, a_{1,3}, \cdots$) are **real numbers**.
$a_{i,j}$ is called the entry of the matrix on row i and column j.

Let us look immediately at some examples:

1. The matrix $\begin{pmatrix} \sqrt{2} \\ -\pi \end{pmatrix}$ is a real 2×1 real matrix (2 rows, 1 column).
2. The matrix $\begin{pmatrix} 2 & 0 \\ -1 & 1/\sqrt{3} \end{pmatrix}$ is a 2×2 real matrix (2 rows, 2 columns).
3. The matrix $\begin{pmatrix} 1 & 0 \\ -1 & 1 \\ 2 & 3 \end{pmatrix}$ is a 3×2 real matrix (3 rows, 2 columns).
4. The matrix $\begin{pmatrix} 1 & 0 & -2 & 1 \\ -1 & 1 & 2 & 3 \end{pmatrix}$ is a 2×4 real matrix (2 rows, 4 columns).
5. The matrix $\begin{pmatrix} 1 & 3 & 2 & 1 & 5 \end{pmatrix}$ is a 1×5 real matrix (1 row, 5 columns).
6. The matrix (-7) is a 1×1 real matrix (1 row, 1 column).

It is important to point out that the place of the elements in a matrix matters; exchanging the place of two elements in the matrix will change the matrix if those two elements are not equal. For example, the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are **not** equal. More generally, if A is defined to be the $m \times n$ real matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

and B is defined to be the $m \times n$ real matrix

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ b_{m,1} & b_{m,2} & \cdots & b_{m,n} \end{pmatrix},$$

then we have $A = B$ if and only if $a_{i,j} = b_{i,j}$ for all $1 \leq i \leq m$ and all $1 \leq j \leq n$, i.e. the corresponding entries of A and B must be equal.

Definition 27. Let

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

be a real $m \times n$ matrix. Let $j \in \{1, 2, \cdots, n\}$. The j^{th} **column vector** of A, denoted by $A_{;j}$ is defined to be the element of $\widehat{\mathbb{R}^m}$ given by:

$$A_{;j} = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ a_{3,j} \\ \vdots \\ a_{m,j} \end{pmatrix}.$$

Similarly, letting $i \in \{1, 2, \cdots, m\}$, the i^{th} **row vector** of A, denoted by $A_{i;}$ is defined to be the element of $\mathbb{R}^n$ given by:

$$A_{i;} = (a_{i,1}, a_{i,2}, a_{i,3}, \cdots, a_{i,n}).$$

We shall **very often** write the row vector $A_{i;}$ **without the separating commas**, i.e., as:

$$A_{i;} = \begin{pmatrix} a_{i,1} & a_{i,2} & a_{i,3} & \cdots & a_{i,n} \end{pmatrix};$$

despite the lack of the separating commas, $A_{i;}$ will still be understood as an $n-$tuple of real numbers, i.e. as an element of $\mathbb{R}^n$.

Let us look at an example: Consider the 3×2 real matrix $\begin{pmatrix} 3 & 2 \\ -1 & 0 \\ 0 & 1 \end{pmatrix}$; its first column vector is the element of $\widehat{\mathbb{R}^3}$ given by $\begin{pmatrix} 3 \\ -1 \\ 0 \end{pmatrix}$, and its second column vector is the element of $\widehat{\mathbb{R}^3}$ given by $\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$. Its first row vector is the element of $\mathbb{R}^2$ given by $(3,2)$, its second row vector is the element of $\mathbb{R}^2$ given by $(-1,0)$, and finally, its third row vector is the element of $\mathbb{R}^2$ given by $(0,1)$. As was mentionned above, we shall often omit the separating commas when writing row vectors of matrices; for example, we shall write the first row vector of this matrix as $\begin{pmatrix} 3 & 2 \end{pmatrix}$ instead, and its second and third row vectors as $\begin{pmatrix} -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \end{pmatrix}$, respectively, and we shall still consider them as elements of $\mathbb{R}^2$ (i.e. pairs of real numbers), despite the absence of the separating commas.

Definition 28. Let m, n be integers ≥ 1. We denote the **set of all** $m \times n$ **real matrices** by $\mathcal{M}_{m,n}(\mathbb{R})$.

In other words, an element of $\mathcal{M}_{m,n}(\mathbb{R})$ is nothing other than a real $m \times n$ matrix, and any real $m \times n$ matrix is an element of $\mathcal{M}_{m,n}(\mathbb{R})$.
We now define **two operations** on $\mathcal{M}_{m,n}(\mathbb{R})$, namely **addition of real matrices** and **multiplication of a real matrix by a real number**. Let us define the addition operation first. Let then

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

and

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ b_{m,1} & b_{m,2} & \cdots & b_{m,n} \end{pmatrix},$$

be two real $m \times n$ matrices. We define the **sum** of A and B, and we denote by $A + B$, the real $m \times n$ matrix given by:

$$A + B = \begin{pmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} & \cdots & a_{1,n} + b_{1,n} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} & \cdots & a_{2,n} + b_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m,1} + b_{m,1} & a_{m,2} + b_{m,2} & \cdots & a_{m,n} + b_{m,n} \end{pmatrix};$$

in other words, $A + B$ is the real $m \times n$ matrix obtained by adding together the corresponding entries of the matrices A and B.
Let now α be a real number; we define the **product** of the matrix A and the real number α, and we denote by $\alpha \cdot A$ (the "$\cdot$", denoting the scalar multiplication operation – as with vectors, we shall drop the "$\cdot$" in the notation very soon ...), the real $m \times n$ matrix given by:

$$\alpha \cdot A = \begin{pmatrix} \alpha a_{1,1} & \alpha a_{1,2} & \cdots & \alpha a_{1,n} \\ \alpha a_{2,1} & \alpha a_{2,2} & \cdots & \alpha a_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha a_{m,1} & \alpha a_{m,2} & \cdots & \alpha a_{m,n} \end{pmatrix};$$

in other words, $\alpha \cdot A$ is the real $m \times n$ matrix obtained by scaling by α each entry of A.
We have now defined an **addition operation** (denoted by the usual "+" symbol), as well as a **scalar multiplication** operation (denoted by the usual "·" symbol), on the set $\mathcal{M}_{m,n}(\mathbb{R})$ of all real $m \times n$ matrices. What do we gain from this ? The answer is given by the next theorem:

Theorem 21. $(\mathcal{M}_{m,n}(\mathbb{R}), +, \cdot)$ is a **real vector space**. The **zero vector 0** of this vector space is the real $m \times n$ matrix with **all entries equal to** 0, i.e.,

$$\mathbf{0} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix};$$

The proof of this theorem is immediate and is left to the reader. The bottom line is that we can think of real $m \times n$ matrices themselves as vectors (in the real vector space $\mathcal{M}_{m,n}(\mathbb{R})$) ...
Let now again m, n be integers ≥ 1 and let $A \in \mathcal{M}_{m,n}(\mathbb{R})$ be the matrix defined by:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

where the $a_{i,j}$ are some given real numbers. Consider the function L_A from $\widehat{\mathbb{R}^n}$ to $\widehat{\mathbb{R}^m}$, i.e. the function $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$ defined as follows: Let

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

be any element of $\widehat{\mathbb{R}^n}$; $L_A(\mathbf{v})$ is defined to be the element of $\widehat{\mathbb{R}^m}$ given by:

$$L_A(\mathbf{v}) = \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n \end{pmatrix}.$$

NOTE: We shall **very often** denote $L_A(\mathbf{v})$ by $A\mathbf{v}$.
Let us examine some examples before going further:

1. Consider the real 1×4 matrix A given by $A = \begin{pmatrix} -1 & 1 & 0 & 3 \end{pmatrix}$; The mapping L_A defined by A is the mapping $L_A : \widehat{\mathbb{R}^4} \to \mathbb{R}$ (we consider $\widehat{\mathbb{R}^1}$ to be just $\mathbb{R}$ itself!) given by the following rule: Let

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

be any element of $\widehat{\mathbb{R}^4}$; $L_A(\mathbf{v})$ is defined to be the element of $\mathbb{R}$ given by:

$$\begin{aligned} L_A(\mathbf{v}) &= (-1)x_1 + (1)x_2 + (0)x_3 + (3)x_4 \\ &= -x_1 + x_2 + 3x_4. \end{aligned}$$

Again, as indicated above, we shall often write simply $A\mathbf{v}$ instead of $L_A(\mathbf{v})$, and in this case, we will write therefore

$$A\mathbf{v} = -x_1 + x_2 + 3x_4.$$

2. Consider now the real 3×2 matrix A given by $A = \begin{pmatrix} -1 & 2 \\ 3 & 0 \\ 4 & 5 \end{pmatrix}$; The mapping L_A defined by A is the mapping $L_A : \widehat{\mathbb{R}^2} \to \widehat{\mathbb{R}^3}$ given by the following rule: Let

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

be any element of $\widehat{\mathbb{R}^2}$; $L_A(\mathbf{v})$ is defined to be the element of $\widehat{\mathbb{R}^3}$ given by:

$$L_A(\mathbf{v}) = \begin{pmatrix} -x_1 + 2x_2 \\ 3x_1 + 0x_2 \\ 4x_1 + 5x_2 \end{pmatrix} = \begin{pmatrix} -x_1 + 2x_2 \\ 3x_1 \\ 4x_1 + 5x_2 \end{pmatrix}$$

and again, we shall often simply write $A\mathbf{v}$ instead of $L_A(\mathbf{v})$, i.e., we shall write

$$A\mathbf{v} = \begin{pmatrix} -x_1 + 2x_2 \\ 3x_1 \\ 4x_1 + 5x_2 \end{pmatrix}.$$

3. Let n be an integer ≥ 1 and let A be the real $n \times n$ matrix given by:

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

i.e. the matrix A has 1's on the diagonal, and 0's everywhere else. As we have seen, A defines therefore a function $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^n}$ as follows: Let

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

be any element of $\widehat{\mathbb{R}^n}$; $L_A(\mathbf{v})$ is defined to be the element of $\widehat{\mathbb{R}^n}$ given by:

$$L_A(\mathbf{v}) = \begin{pmatrix} 1x_1 + 0x_2 + \cdots + 0x_n \\ 0x_1 + 1x_2 + \cdots + 0x_n \\ \vdots \\ 0x_1 + 0x_2 + \cdots + 1x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{v},$$

i.e., for any $\mathbf{v} \in \widehat{\mathbb{R}^n}$, we have: $L_A(\mathbf{v}) = \mathbf{v}$. This shows that L_A is nothing other than the **identity mapping** of $\widehat{\mathbb{R}^n}$ (i.e. the function which maps every vector in $\widehat{\mathbb{R}^n}$ to itself); for this reason, the matrix A in this example is usually called the $n \times n$ **identity matrix**. Hence, with A being the $n \times n$ **identity matrix**, we can write (in keeping with our simplified notation): $A\mathbf{v} = \mathbf{v}$ for every $\mathbf{v} \in \widehat{\mathbb{R}^n}$.

Let now A be a real $m \times n$ matrix (i.e. an element of $\mathcal{M}_{m,n}(\mathbb{R})$; what can we say about the function $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$? Does it have any special property ? The answer is given by the following theorem:

Theorem 22. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$; the mapping $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$ defined by A is **linear**.

Proof. Let

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

be any element in $\mathcal{M}_{m,n}(\mathbb{R})$, and consider the mapping $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$. To show that L_A is linear, we have to show the following two properties:

(i) $\forall \mathbf{v}_1, \mathbf{v}_2 \in \widehat{\mathbb{R}^n}$, we have $L_A(\mathbf{v}_1 + \mathbf{v}_2) = L_A(\mathbf{v}_1) + L_A(\mathbf{v}_2)$, and

(ii) $\forall \mathbf{v} \in \widehat{\mathbb{R}^n}$, $\forall \alpha \in \mathbb{R}$, we have $L_A(\alpha\mathbf{v}) = \alpha L_A(\mathbf{v})$.

Let us begin by showing the first property. For this, let

$$\mathbf{v}_1 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_n \end{pmatrix},$$

be any two elements in $\widehat{\mathbb{R}^n}$; we have to show that $L_A(\mathbf{v}_1+\mathbf{v}_2) = L_A(\mathbf{v}_1)+L_A(\mathbf{v}_2)$. Let us first calculate $L_A(\mathbf{v}_1 + \mathbf{v}_2)$, and before we do this, let us first calculate $\mathbf{v}_1 + \mathbf{v}_2$. We have:

$$\mathbf{v}_1 + \mathbf{v}_2 = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \\ \vdots \\ x_n + y_n \end{pmatrix},$$

and therefore, by definition of L_A,

$$L_A(\mathbf{v}_1 + \mathbf{v}_2) = \begin{pmatrix} a_{1,1}(x_1 + y_1) + a_{1,2}(x_2 + y_2) + \cdots + a_{1,n}(x_n + y_n) \\ a_{2,1}(x_1 + y_1) + a_{2,2}(x_2 + y_2) + \cdots + a_{2,n}(x_n + y_n) \\ \vdots \\ a_{m,1}(x_1 + y_1) + a_{m,2}(x_2 + y_2) + \cdots + a_{m,n}(x_n + y_n) \end{pmatrix}.$$

Separating the x_i's from the y_j's in the expression obtained, we can write:

$$\begin{aligned} L_A(\mathbf{v}_1 + \mathbf{v}_2) &= \begin{pmatrix} (a_{1,1}x_1 + \cdots + a_{1,n}x_n) + (a_{1,1}y_1 + \cdots + a_{1,n}y_n) \\ (a_{2,1}x_1 + \cdots + a_{2,n}x_n) + (a_{2,1}y_1 + \cdots + a_{2,n}y_n) \\ \vdots \\ (a_{m,1}x_1 + \cdots + a_{m,n}x_n) + (a_{m,1}y_1 + \cdots + a_{m,n}y_n) \end{pmatrix} \\ &= \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{pmatrix} + \begin{pmatrix} a_{1,1}y_1 + \cdots + a_{1,n}y_n \\ a_{2,1}y_1 + \cdots + a_{2,n}y_n \\ \vdots \\ a_{m,1}y_1 + \cdots + a_{m,n}y_n \end{pmatrix} \\ &= L_A(\mathbf{v}_1) + L_A(\mathbf{v}_2). \end{aligned}$$

This shows that property (i) holds, namely, that $\forall \mathbf{v}_1, \mathbf{v}_2 \in \widehat{\mathbb{R}^n}$, we have $L_A(\mathbf{v}_1 + \mathbf{v}_2) = L_A(\mathbf{v}_1) + L_A(\mathbf{v}_2)$.
Let us now prove property (ii); for this, let $\alpha \in \mathbb{R}$ be any real number, and let

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

be any element in $\widehat{\mathbb{R}^n}$; we have to show that $L_A(\alpha\mathbf{v}) = \alpha L_A(\mathbf{v})$. Let us first compute $\alpha\mathbf{v}$; we have:

$$\alpha\mathbf{v} = \alpha \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \alpha x_2 \\ \alpha x_3 \\ \vdots \\ \alpha x_n \end{pmatrix},$$

and therefore,

$$\begin{aligned} L_A(\alpha\mathbf{v}) &= \begin{pmatrix} a_{1,1}(\alpha x_1) + a_{1,2}(\alpha x_2) + \cdots + a_{1,n}(\alpha x_n) \\ a_{2,1}(\alpha x_1) + a_{2,2}(\alpha x_2) + \cdots + a_{2,n}(\alpha x_n) \\ \vdots \\ a_{m,1}(\alpha x_1) + a_{m,2}(\alpha x_2) + \cdots + a_{m,n}(\alpha x_n) \end{pmatrix} \\ &= \begin{pmatrix} \alpha(a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n) \\ \alpha(a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n) \\ \vdots \\ \alpha(a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n) \end{pmatrix} \\ &= \alpha \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n \end{pmatrix} \\ &= \alpha L_A(\mathbf{v}). \end{aligned}$$

This proves property (ii), namely that $\forall \mathbf{v} \in \widehat{\mathbb{R}^n}$ and $\forall \alpha \in \mathbb{R}$, we have $L_A(\alpha\mathbf{v}) = \alpha L_A(\mathbf{v})$.
Hence, L_A satisfies properties (i) and (ii) and is therefore a **linear** mapping. ☐

We now show the converse to the previous result, i.e. we show that if $L : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$ is a **linear** mapping, then there exists a real $m \times n$ matrix C such that $L = L_C$; in other words, **any linear** mapping from $\widehat{\mathbb{R}^n}$ to $\widehat{\mathbb{R}^m}$ is actually defined by a real $m \times n$ matrix.

Theorem 23. Let $L : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$ be a **linear** mapping. Then, there exists $C \in \mathcal{M}_{m,n}(\mathbb{R})$ such that $L = L_C$.

Proof. Let $L : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$ be a **linear** mapping.
Define the vectors $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n \in \widehat{\mathbb{R}^n}$ as follows:

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \cdots \ \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

i.e. for $i \in \{1, \cdots, n\}$, $\mathbf{e}_i$ has entry 1 on row i and entry 0 everywhere else. Note that $(\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n)$ is a basis of $\widehat{\mathbb{R}^n}$, and it is called the **canonical basis** of $\widehat{\mathbb{R}^n}$. Note also that any element $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \in \widehat{\mathbb{R}^n}$ can be written as

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = x_1 \cdot \mathbf{e}_1 + x_2 \cdot \mathbf{e}_2 + \cdots + x_n \cdot \mathbf{e}_n.$$

Hence, we have, by linearity of L:

$$\begin{aligned} L(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}) &= L(x_1 \cdot \mathbf{e}_1 + x_2 \cdot \mathbf{e}_2 + \cdots + x_n \cdot \mathbf{e}_n) \\ &= x_1 \cdot L(\mathbf{e}_1) + x_2 \cdot L(\mathbf{e}_2) + \cdots + x_n \cdot L(\mathbf{e}_n). \end{aligned}$$

$L(\mathbf{e}_1), L(\mathbf{e}_2), \cdots, L(\mathbf{e}_n)$ are all elements of $\widehat{\mathbb{R}^m}$, i.e. are column vectors with m real entries; denote their entries as follows:

$$L(\mathbf{e}_1) = \begin{pmatrix} c_{1,1} \\ c_{2,1} \\ c_{3,1} \\ \vdots \\ c_{m,1} \end{pmatrix}, \ L(\mathbf{e}_2) = \begin{pmatrix} c_{1,2} \\ c_{2,2} \\ c_{3,2} \\ \vdots \\ c_{m,2} \end{pmatrix}, \ \cdots \ L(\mathbf{e}_n) = \begin{pmatrix} c_{1,n} \\ c_{2,n} \\ c_{3,n} \\ \vdots \\ c_{m,n} \end{pmatrix};$$

Let now $C \in \mathcal{M}_{m,n}(\mathbb{R})$ be the real $m \times n$ matrix constructed from the entries of $L(\mathbf{e}_1), L(\mathbf{e}_2), \cdots, L(\mathbf{e}_n)$ as follows:

$$C = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,n} \end{pmatrix}.$$

Note that the first column vector of C is nothing other than $L(\mathbf{e}_1)$, the second column vector of C is nothing other than $L(\mathbf{e}_2)$, and so on.

We have, for any element $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \in \widehat{\mathbb{R}^n}$:

$$\begin{aligned}
L_C(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}) &= \begin{pmatrix} c_{1,1}x_1 + c_{1,2}x_2 + \cdots + c_{1,n}x_n \\ c_{2,1}x_1 + c_{2,2}x_2 + \cdots + c_{2,n}x_n \\ \vdots \\ c_{m,1}x_1 + c_{m,2}x_2 + \cdots + c_{m,n}x_n \end{pmatrix} \\
&= x_1 \cdot \begin{pmatrix} c_{1,1} \\ c_{2,1} \\ c_{3,1} \\ \vdots \\ c_{m,1} \end{pmatrix} + x_2 \cdot \begin{pmatrix} c_{1,2} \\ c_{2,2} \\ c_{3,2} \\ \vdots \\ c_{m,2} \end{pmatrix} + \cdots + x_n \cdot \begin{pmatrix} c_{1,n} \\ c_{2,n} \\ c_{3,n} \\ \vdots \\ c_{m,n} \end{pmatrix} \\
&= x_1 \cdot L(\mathbf{e}_1) + x_2 \cdot L(\mathbf{e}_2) + \cdots + x_n \cdot L(\mathbf{e}_n) \\
&= L(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}).
\end{aligned}$$

Hence, $L_C = L$.

□

Now that we have shown that for any real $m \times n$ matrix A the mapping $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$ is **linear** (and the converse result), we can ask some further questions; in particular, we can try (in the spirit of the previous lecture) to identify the **kernel** and **range** of L_A ...
Before we go any further, a few words on **notation** and **terminology**:

- As has been stated a number of times already, we shall often write $A\mathbf{v}$ instead of $L_A(\mathbf{v})$; in that notation, the linearity of L_A that we have just established means that $A(\mathbf{v}_1 + \mathbf{v}_2) = A\mathbf{v}_1 + A\mathbf{v}_2$ and $A(\alpha\mathbf{v}) = \alpha A\mathbf{v}$.

- We shall denote the kernel of L_A by $\ker(A)$ instead of the more cumbersome (but correct!) notation $\ker(L_A)$, and we shall often just say "**kernel of the matrix** A" instead of the more cumbersome "kernel of the linear mapping L_A defined by the matrix A".

- Similarly, we shall denote the range of L_A by $\text{Im}(A)$ instead of the more cumbersome (but correct!) notation $\text{Im}(L_A)$, and we shall often just say "**range (or image) of the matrix** A" instead of the more cumbersome "range (or image) of the linear mapping L_A defined by the matrix A".

Let then

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

be a real $m \times n$ matrix (i.e. an element of $\mathcal{M}_{m,n}(\mathbb{R})$), and let us first try to identify the **range of** A, i.e. **the range of the linear mapping** $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$. Recall that the range of L_A, **which we shall simply write as** $\mathrm{Im}(A)$, is the set of all $L_A(\mathbf{v})$ in $\widehat{\mathbb{R}^m}$ with $\mathbf{v}$ in $\widehat{\mathbb{R}^n}$; i.e., writing this formally, we have:

$$\mathrm{Im}(A) = \{L_A(\mathbf{v}) | \mathbf{v} \in \widehat{\mathbb{R}^n}\}.$$

Let now

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

be any element in $\widehat{\mathbb{R}^n}$; we can write:

$$\begin{aligned} L_A(\mathbf{v}) &= \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n \end{pmatrix} \\ &= x_1 \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{m,1} \end{pmatrix} + x_2 \begin{pmatrix} a_{1,2} \\ a_{2,2} \\ \vdots \\ a_{m,2} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ a_{m,n} \end{pmatrix} \\ &= x_1 A_{;1} + x_2 A_{;2} + \cdots x_n A_{;n}, \end{aligned}$$

where, as we have already seen, $A_{;1}$ denotes the first column vector of A, $A_{;2}$ denotes the first column vector of A, ..., and so on. Recall that the column vectors of A, namely $A_{;1}, A_{;2}, \cdots, A_{;n}$ are all elements of the real vector space $\widehat{\mathbb{R}^m}$ (since A is $m \times n$, i.e. has m rows!).
So what have we shown ? Well, we have shown that if we take a vector

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

in $\widehat{\mathbb{R}^n}$, then $L_A(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix})$ is nothing other than the **linear combination**

$$x_1 A_{;1} + x_2 A_{;2} + \cdots x_n A_{;n}$$

of the **column vectors of** A, with the coefficients of this linear combination (namely the real numbers $x_1, x_2, \cdots, x_n$) given by the entries of the vector $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$. This shows that **any element in** $\mathrm{Im}(A)$ **is a linear combination of the column vectors of** A, i.e. a linear combination of $A_{;1}, A_{;2}, \cdots, A_{;n}$. **Conversely**, we shall show that **any linear combination of the column vectors of** A **is in** $\mathrm{Im}(A)$; indeed, let the vector $\mathbf{w} \in \widehat{\mathbb{R}^m}$ be a linear combination of $A_{;1}, A_{;2}, \cdots, A_{;n}$, i.e. assume there exist real numbers $\alpha_1, \alpha_2, \cdots, \alpha_n$ such that:

$$\mathbf{w} = \alpha_1 A_{;1} + \alpha_2 A_{;2} + \cdots \alpha_n A_{;n}.$$

We therefore have:

$$\begin{aligned} \mathbf{w} &= \alpha_1 \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{m,1} \end{pmatrix} + \alpha_2 \begin{pmatrix} a_{1,2} \\ a_{2,2} \\ \vdots \\ a_{m,2} \end{pmatrix} + \cdots + \alpha_n \begin{pmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ a_{m,n} \end{pmatrix} \\ &= \begin{pmatrix} a_{1,1}\alpha_1 + a_{1,2}\alpha_2 + \cdots + a_{1,n}\alpha_n \\ a_{2,1}\alpha_1 + a_{2,2}\alpha_2 + \cdots + a_{2,n}\alpha_n \\ \vdots \\ a_{m,1}\alpha_1 + a_{m,2}\alpha_2 + \cdots + a_{m,n}\alpha_n \end{pmatrix} \\ &= L_A(\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}), \end{aligned}$$

which shows that $\mathbf{w}$ is in $\mathrm{Im}(A)$ (since it is L_A of something in $\widehat{\mathbb{R}^n}$!).
Let us recapitulate what we have shown: We have shown that if A is a real $m \times n$ matrix, then $\mathrm{Im}(A)$ (i.e. the range of the linear mapping $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$) is **the set of all linear combinations of the column vectors of** A; but we already have a name for this! The set of all linear combinations of the column

vectors of A is nothing other than the vector subspace of $\widehat{\mathbb{R}^m}$ generated by the column vectors of A, i.e. the **linear span** of the column vectors of A. We have therefore proved the following theorem:

Theorem 24. Let A be a real $m \times n$ matrix; the **range** $\mathrm{Im}(A)$ **of the matrix** A (i.e. the range of the linear mapping $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m}$) is the **linear span of the column vectors** $A_{;1}, A_{;2}, \cdots, A_{;n}$ **of** A.

Let us consider some examples:

1. Let A be the real 2×3 matrix given by $A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 3 & 5 \end{pmatrix}$; then, $\mathrm{Im}(A)$ is the **vector subspace** of $\widehat{\mathbb{R}^2}$ **generated by** the subset $\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}\}$ of $\widehat{\mathbb{R}^2}$; in other words, $\mathrm{Im}(A)$ is the **linear span** of $\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}\}$.
   It is easy to show that the linear span of this set is $\widehat{\mathbb{R}^2}$ itself (for example, one can easily show that any vector in $\widehat{\mathbb{R}^2}$ can be written as a linear combination of the first two vectors, i.e. $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 3 \end{pmatrix}$), and hence $\mathrm{Im}(A) = \widehat{\mathbb{R}^2}$.

2. Let now A be the real 4×2 matrix given by $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \\ -2 & 3 \\ 1 & -3 \end{pmatrix}$; then, $\mathrm{Im}(A)$ is the **vector subspace** of $\widehat{\mathbb{R}^4}$ **generated by** the subset $\{\begin{pmatrix} -1 \\ 0 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \\ -3 \end{pmatrix}\}$ of $\widehat{\mathbb{R}^4}$; in other words, $\mathrm{Im}(A)$ is the **linear span** of $\{\begin{pmatrix} -1 \\ 0 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \\ -3 \end{pmatrix}\}$.
   Could it be the case here that $\mathrm{Im}(A)$ is $\widehat{\mathbb{R}^4}$ itself ? Well, we know from Lecture 8 that $\widehat{\mathbb{R}^4}$ has **dimension** 4; we also know from **Theorem 10** of Lecture 8 that if a subset S of an $N-$dimensional real vector space $\mathbf{V}$ is a generating set for $\mathbf{V}$, then the number of elements of S must be $\geq N$. In our case, $S = \{\begin{pmatrix} -1 \\ 0 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \\ -3 \end{pmatrix}\}$, and therefore has only 2 elements (and 2 is not ≥ 4); we conclude that $\mathrm{Im}(A) \neq \widehat{\mathbb{R}^4}$.

The observations made in these two examples can be packaged into a theorem:

Theorem 25. Let A be a real $m \times n$ matrix (i.e. with m rows and n columns). We have:

- If $\mathrm{Im}(A) = \widehat{\mathbb{R}^m}$, then we must have $n \geq m$. Hence, if $n < m$, then $\mathrm{Im}(A)$ cannot be equal to $\widehat{\mathbb{R}^m}$.

Proof. We know that $\mathrm{Im}(A)$ is equal to the linear span of the n column vectors $A_{;1}, A_{;2}, \cdots, A_{;n}$ of A. Recall that each of $A_{;1}, A_{;2}, \cdots, A_{;n}$ is a vector in $\widehat{\mathbb{R}^m}$. If $\mathrm{Im}(A) = \widehat{\mathbb{R}^m}$, then the subset $\{A_{;1}, A_{;2}, \cdots, A_{;n}\}$ is a **generating set** for $\widehat{\mathbb{R}^m}$; that generating subset has n **elements** and $\widehat{\mathbb{R}^m}$ has **dimension** m (we have seen this in Lecture 8), and it follows therefore from Theorem 10 of Lecture 8 that **if** $\mathrm{Im}(A) = \widehat{\mathbb{R}^m}$ **then** we must have $n \geq m$. $\square$

Now that we have investigated the range $\mathrm{Im}(A)$ of a real matrix A, let us examine its kernel $\ker(A)$ (again, by $\ker(A)$ we mean the kernel of the linear map L_A defined by A, i.e. $\ker(L_A)$). Let then

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

be a real $m \times n$ matrix, and let us try to get some information about the kernel $\ker(A)$ of A. By definition of $\ker(A)$, a vector $\mathbf{v}$ of $\widehat{\mathbb{R}^n}$ is in $\ker(A)$ if and only if $L_A(\mathbf{v}) = \mathbf{0}_{\widehat{\mathbb{R}^m}}$ (where $\mathbf{0}_{\widehat{\mathbb{R}^m}} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ denotes the zero vector of $\widehat{\mathbb{R}^m}$); let us be more precise. Let then

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

be any element in $\widehat{\mathbb{R}^n}$; We have seen already that

$$L_A(\mathbf{v}) = x_1 A_{;1} + x_2 A_{;2} + \cdots x_n A_{;n},$$

where $A_{;1}, A_{;2}, \cdots, A_{;n}$ are the column vectors of A.
Assume now that $A_{;1}, A_{;2}, \cdots, A_{;n}$ are **linearly independent**. Then, the equality

$$L_A(\mathbf{v}) = \mathbf{0}_{\widehat{\mathbb{R}^m}}$$

(where $\mathbf{0}_{\widehat{\mathbb{R}^m}} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ denotes the zero vector of $\widehat{\mathbb{R}^m}$) is equivalent to the equality

$$x_1 A_{;1} + x_2 A_{;2} + \cdots x_n A_{;n} = \mathbf{0}_{\widehat{\mathbb{R}^m}},$$

which, by linear independence of $A_{;1}, A_{;2}, \cdots, A_{;n}$, implies $x_1 = x_2 = \cdots = x_n = 0$, i.e. $\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}}$, i.e. $\mathbf{v}$ is the zero vector of $\widehat{\mathbb{R}^n}$. In other words, we have shown that if the column vectors of A are **linearly independent**, then the kernel of L_A (which we denote by $\ker(A)$) is just $\{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$, i.e. $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$.
Let us now prove the converse. Assume therefore that $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$; we would like to show that the column vectors of A are then linearly independent. Let then $\alpha_1, \alpha_2, \cdots, \alpha_n$ be real numbers such that

$$\alpha_1 A_{;1} + \alpha_2 A_{;2} + \cdots + \alpha_n A_{;n} = \mathbf{0}_{\widehat{\mathbb{R}^m}};$$

we want to show that $\alpha_1, \alpha_2, \cdots, \alpha_n$ must then all be zero. Now let $\mathbf{v} \in \widehat{\mathbb{R}^n}$ be given by:

$$\mathbf{v} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

The equality

$$\alpha_1 A_{;1} + \alpha_2 A_{;2} + \cdots + \alpha_n A_{;n} = \mathbf{0}_{\widehat{\mathbb{R}^m}};$$

can be written

$$L_A(\mathbf{v}) = \mathbf{0}_{\widehat{\mathbb{R}^m}}$$

which implies $\mathbf{v} \in \ker(A)$ (by definition of $\ker(A)$), and since we have assumed that $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$, it follows that $\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}}$, i.e.

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

which implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, as desired. This proves that the column vectors $A_{;1}, A_{;2}, \cdots, A_{;n}$ of A are **linearly independent**.
In summary, we have proved the following theorem:

Theorem 26. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$ (i.e. A is a real $m \times n$ matrix). We have $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$ **if and only if** the column vectors of A are **linearly independent**.

We close this section with some important terminology and an important theorem which is a direct adaptation of the **Rank-Nullity Theorem** of Lecture 9:

Definition 29. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$, i.e. A is a real $m \times n$ matrix.

(i) The **rank of** A is defined to be the **dimension of** $\mathrm{Im}(A)$, and is denoted by $\mathrm{rank}(A)$.

(ii) The **nullity of** A is defined to be the **dimension of** $\ker(A)$, and is denoted by $\mathrm{nullity}(A)$.

Theorem 27. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$; then:

$$\mathrm{rank}(A) + \mathrm{nullity}(A) = n,$$

i.e. $\mathrm{rank}(A) + \mathrm{nullity}(A)$ is equal to the **number of columns of** A.

Proof. The result follows directly from the **Rank-Nullity Theorem** of Lecture 9, taking into account the fact that:

- $\mathrm{rank}(A)$ is **by definition** the dimension of $\mathrm{Im}(L_A)$ (which we have denoted $\mathrm{Im}(A)$),
- $\mathrm{nullity}(A)$ is **by definition** the dimension of $\ker(L_A)$ (which we have denoted $\ker(A)$),
- L_A is a **linear mapping from** the real vector space $\widehat{\mathbb{R}^n}$ **to** the real vector space $\widehat{\mathbb{R}^m}$,
- $\widehat{\mathbb{R}^n}$ is a real vector space of **dimension** n.

□

PROBLEMS:

1. For each of the following choices for the matrix A, do the following:
   - Specify the linear transformation L_A that it defines (for example, if $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, then L_A is the mapping $L_A : \widehat{\mathbb{R}^2} \to \widehat{\mathbb{R}^2}$ defined by $L_A(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}) = \begin{pmatrix} x_1 \\ 2x_1 + x_2 \end{pmatrix}$, for every $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \widehat{\mathbb{R}^2}$,
   - specify its range $\mathrm{Im}(A)$ as well as the dimension of $\mathrm{Im}(A)$,

- specify its kernel $\ker(A)$ as well as the dimension of $\ker(A)$;
- verify the Rank-Nullity theorem for A (i.e. verify that $\dim(\mathrm{Im}(A)) + \dim(\ker(A)) =$ number of columns of A).

(a) $A = \begin{pmatrix} -1 & 2 \end{pmatrix}$.

(b) $A = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$.

(c) $A = \begin{pmatrix} 1 & 0 & 3 \end{pmatrix}$.

(d) $A = \begin{pmatrix} 3 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

(e) $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(f) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(g) $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

(h) $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(i) $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ -1 & 3 \end{pmatrix}$.

(j) $A = \begin{pmatrix} 1 & 0 \\ 1 & -1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$.

(k) $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 2 \\ 1 & 0 & -1 \end{pmatrix}$.

(l) $A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

(m) $A = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \end{pmatrix}$.

(n) $A = \begin{pmatrix} 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \end{pmatrix}$.

(o) $A = \begin{pmatrix} 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$.

(p) $A = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$.

(q) $A = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \end{pmatrix}$.

(r) $A = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

(s) $A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 4 \\ -2 & 0 & -4 \\ -1 & 1 & 1 \end{pmatrix}$.

(t) $A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 4 \\ -2 & 0 & -4 \\ -1 & 1 & -2 \end{pmatrix}$.

(u) $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 4 & 4 \\ -2 & -4 & -4 \\ -1 & -2 & -2 \end{pmatrix}$.

(v) $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 4 & 4 \\ -2 & -4 & -4 \\ -1 & 2 & -2 \end{pmatrix}$.

(x) $A = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 3 & 0 & 6 & -3 \\ -2 & 0 & -4 & 2 \end{pmatrix}$.

(y) $A = \begin{pmatrix} 1 & 1 & 2 & -1 \\ 3 & 0 & 6 & -3 \\ -2 & 0 & -4 & 2 \end{pmatrix}$.

(z) $A = \begin{pmatrix} 1 & 1 & 2 & -1 \\ 3 & 0 & 6 & 3 \\ -2 & 0 & -4 & 2 \end{pmatrix}$.

Section 12

Study Topics

- Systems of Linear Transformations Revisited
- Solving Systems of Linear Equations

Consider the system of linear equations in m equations and n unknowns given by:

$$(E)\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 + \cdots a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 + \cdots a_{2,n}x_n = b_2 \\ a_{3,1}x_1 + a_{3,2}x_2 + a_{3,3}x_3 + \cdots a_{3,n}x_n = b_3 \\ a_{m,1}x_1 + a_{m,2}x_2 + a_{m,3}x_3 + \cdots a_{m,n}x_n = b_m \end{cases}$$

where the real numbers $a_{1,1}, a_{1,2}, \cdots, a_{m,n}$ and $b_1, b_2, \cdots, b_m$ are **given** real numbers, and we wish to solve for the real numbers $x_1, x_2, \cdots, x_n$.
Can we write this system in terms of matrices and vectors ? Before answering this question, you may ask what the point of writing such a system in terms of matrices and vectors would be. The answer to this last question is quite simple: If we are able to write that system of equations in terms of matrices and vectors, then with the linear algebra knowledge we have accumulated so far, we may be able to say something interesting about that system of equations: For example, whether or not it has a solution, how many solutions it does have, and so on, and even beyond this, in case it does have a solution, **how** to go about finding that solution. So let us not waste any time and let us try to express that system of linear equations using matrices and vectors.
Let then $A \in \mathcal{M}_{m,n}(\mathbb{R})$ be the real $m \times n$ matrix defined by

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

and let $\mathbf{b} \in \widehat{\mathbb{R}^m}$ be the real vector defined by

$$\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

It is easy to verify that the real numbers $x_1, x_2, \cdots, x_n$ satisfy the above system of linear equations **if and only if** the vector $\mathbf{v} \in \widehat{\mathbb{R}^n}$ defined by

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

satisfies the **vector equation** (so called because the unknown is now a vector in $\widehat{\mathbb{R}^n}$):

$$L_A(\mathbf{v}) = \mathbf{b}.$$

Note that in keeping with our simplified notation (i.e. writing $A\mathbf{v}$ instead of $L_A(\mathbf{v})$), we can write this last equation simply as

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

Before going further, let us now see how easily we can prove that our original system of linear equations (E) can have only $0, 1$ or infinitely many solutions. We already proved this in Lecture 6, but let us prove it again here.
From the discussion above, we need only show therefore that the equation $L_A(\mathbf{v}) = \mathbf{b}$, where $A \in \mathcal{M}_{m,n}(\mathbb{R})$ and $\mathbf{b} \in \widehat{\mathbb{R}^m}$ are given, and where we wish to solve for the unknown vector $\mathbf{v} \in \widehat{\mathbb{R}^n}$, can have only $0, 1$ or infinitely many solutions. We have the following cases:

(Case 1) $\mathbf{b} \notin \mathrm{Im}(A)$. In this case, there is no $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$ (since otherwise $\mathbf{b}$ would be in $\mathrm{Im}(A)$), i.e. there is **no solution**.

(Case 2) $\mathbf{b} \in \mathrm{Im}(A)$. In this case, there is at least one vector in $\widehat{\mathbb{R}^n}$ which satisfies the equation $L_A(\mathbf{v}) = \mathbf{b}$; let $\mathbf{v}_1$ be one such vector (i.e. $L_A(\mathbf{v}_1) = \mathbf{b}$). To find out how many other vectors satisfy that equation, we consider the following two subcases:

(Case 2a) $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$. In this subcase L_A is **one-to-one** and hence there is a **unique** $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$, namely $\mathbf{v}_1$.

(Case 2b) $\ker(A) \neq \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$. In this subcase, there is a **non-zero** vector $\mathbf{w} \in \ker(A)$, i.e $\mathbf{w} \neq \mathbf{0}_{\widehat{\mathbb{R}^n}}$. Since $\ker(A)$ is a vector subspace of $\widehat{\mathbb{R}^n}$, we have $\alpha\mathbf{w} \in \ker(A)$, $\forall \alpha \in \mathbb{R}$. Then, $\forall \alpha \in \mathbb{R}$:

$$L_A(\mathbf{v}_1 + \alpha\mathbf{w}) = L_A(\mathbf{v}_1) + L_A(\alpha\mathbf{w}) = \mathbf{b} + \alpha L_A(\mathbf{w}) = \mathbf{b} + \mathbf{0}_{\widehat{\mathbb{R}^m}} = \mathbf{b},$$

which shows that $\mathbf{v}_1 + \alpha\mathbf{w}$ is **also** a solution to the vector equation $L_A(\mathbf{v}) = \mathbf{b}$. There are infinitely many distinct vectors of the form $\mathbf{v}_1 + \alpha\mathbf{w}$ (one for each choice of the real number α), and hence in this subcase, there are **infinitely many** solutions to the vector equation $L_A(\mathbf{v}) = \mathbf{b}$.

And this completes the proof!
There are **two important points** to take away from this:

1. The ease with which that non-trivial result is proved,

2. The **key role** played by the **range** $\mathrm{Im}(A)$ and the **kernel** $\ker(A)$ in determining the number of solutions to the equation $L_A(\mathbf{v}) = \mathbf{b}$.

Now that we have seen that a system of linear equations can be written very compactly using matrices and vectors in the form of a vector equation $L_A(\mathbf{v}) = \mathbf{b}$ (with $A, \mathbf{b}$ given, and $\mathbf{v}$ the unknown), let us try to use this connection to further our understanding of systems of linear equations. In particular, let us examine the following question:

- Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$; **under what conditions on** A does there exist, **for each** choice of $\mathbf{b} \in \widehat{\mathbb{R}^m}$, a **unique** solution to the equation $L_A(\mathbf{v}) = \mathbf{b}$?

The answer to this important question is given in the next theorem:

Theorem 28. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$. We have the following:

(a) If, **for each** $\mathbf{b} \in \widehat{\mathbb{R}^m}$, there exists a **unique** $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$, then $m = n$ **and** the column vectors of A are **linearly independent**.

(b) Conversely, if $m = n$ **and** the column vectors of A are **linearly independent**, then **for each** $\mathbf{b} \in \widehat{\mathbb{R}^m}$, there exists a **unique** $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$.

Proof. (a) Assume that for each $\mathbf{b} \in \widehat{\mathbb{R}^m}$ there exists a unique $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$; since **for each** $\mathbf{b} \in \widehat{\mathbb{R}^m}$ the equation $L_A(\mathbf{v}) = \mathbf{b}$ has a solution, it follows that $\text{Im}(A) = \widehat{\mathbb{R}^m}$, which implies that $m \leq n$; furthermore, since that solution is unique, it follows that $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$, which implies that $m \geq n$. Since we have both $m \leq n$ and $m \geq n$, it follows that $m = n$.

(b) Assume now that $m = n$ and that the column vectors of A are linearly independent. Since the n column vectors $A_{;1}, A_{;2}, \cdots, A_{;n}$ of A are elements of $\widehat{\mathbb{R}^n}$ (since $m = n$), since they are assumed to be linearly independent, and since $\widehat{\mathbb{R}^n}$ has dimension n, it follows (from Lecture 8) that $\{A_{;1}, A_{;2}, \cdots, A_{;n}\}$ is also a **generating set** for $\widehat{\mathbb{R}^n}$, i.e. that $\text{Im}(A) = \widehat{\mathbb{R}^n}$. Hence, for each $\mathbf{b} \in \widehat{\mathbb{R}^m}$, there is at least one vector $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$. Furthermore, since the column vectors of A are assumed to be linearly independent, it follows (from Lecture 10) that $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$, and therefore (again from lecture 10), for each $\mathbf{b} \in \widehat{\mathbb{R}^m}$, there is a **unique** $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies $L_A(\mathbf{v}) = \mathbf{b}$.

□

Now that, thanks to this last theorem, we have the answer to the question we posed earlier, let us examine **how** we could go about solving an equation of the form $L_A(\mathbf{v}) = \mathbf{b}$, with A a **square** $n \times n$ real matrix.

NOTE: For simplicity, we will denote the set of all **square** $n \times n$ real matrices simply by $\mathcal{M}_n(\mathbb{R})$.

Let then $A \in \mathcal{M}_n(\mathbb{R})$, and let $\mathbf{b} \in \widehat{\mathbb{R}^n}$. We wish to find $\mathbf{v} \in \widehat{\mathbb{R}^n}$ which satisfies

$$L_A(\mathbf{v}) = \mathbf{b}.$$

Assume that there exist some matrix $B \in \mathcal{M}_n(\mathbb{R})$ such that $L_B(L_A(\mathbf{v})) = \mathbf{v}$ for all $\mathbf{v} \in \widehat{\mathbb{R}^n}$, i.e., such that $L_B \circ L_A(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in \widehat{\mathbb{R}^n}$; **how** can the knowledge of this matrix B help us solve our equation ? Well, **if** some vector of $\widehat{\mathbb{R}^n}$, say $\mathbf{w}$, satisfies the equation

$$L_A(\mathbf{w}) = \mathbf{b},$$

then, applying L_B to both sides, it must also satisfy the equation

$$L_B(L_A(\mathbf{w})) = L_B(\mathbf{b}),$$

and since we assumed B was such that $L_B(L_A(\mathbf{v})) = \mathbf{v}$ for all $\mathbf{v} \in \widehat{\mathbb{R}^n}$, it follows that $\mathbf{w}$ must also satisfy

$$\mathbf{w} = L_B(\mathbf{b}),$$

i.e. $\mathbf{w}$ must be equal to $L_B(\mathbf{b})$, i.e. the solution to the equation $L_A(\mathbf{v}) = \mathbf{b}$ is given by $\mathbf{v} = L_B(\mathbf{b})$; in other words, **we have solved the equation**!
Let us examine this idea on an example before going further:

- Let $A \in \mathcal{M}_2(\mathbb{R})$ be the square 2×2 matrix defined by $A = \begin{pmatrix} 4 & 1 \\ 3 & 1 \end{pmatrix}$, and let $\mathbf{b} \in \widehat{\mathbb{R}^2}$ be the vector defined by $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$. We wish to find $\mathbf{v} \in \widehat{\mathbb{R}^2}$ such that $L_A(\mathbf{v}) = \mathbf{b}$. Note that since the column vectors of A are linearly independent (as can be easily verified), it follows that for any $\mathbf{b} \in \widehat{\mathbb{R}^2}$, the equation $L_A(\mathbf{v}) = \mathbf{b}$ has a **unique** solution. Let now $B \in \mathcal{M}_2(\mathbb{R})$ be the square 2×2 matrix defined by $B = \begin{pmatrix} 1 & -1 \\ -3 & 4 \end{pmatrix}$. Let now $\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ be any vector in $\widehat{\mathbb{R}^2}$. We have:

$$\begin{aligned} L_B \circ L_A(\mathbf{v}) &= L_B(L_A(\mathbf{v})) \\ &= L_B(\begin{pmatrix} 4x_1 + x_2 \\ 3x_1 + x_2 \end{pmatrix}) \\ &= \begin{pmatrix} (4x_1 + x_2) - (3x_1 + x_2) \\ -3(4x_1 + x_2) + 4(3x_1 + x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= \mathbf{v}, \end{aligned}$$

We have shown therefore that $\forall \mathbf{v} \in \widehat{\mathbb{R}^2}$, $L_B \circ L_A(\mathbf{v}) = \mathbf{v}$. Thanks to this, and in line with our previous discussion, we can solve the vector equation $L_A(\mathbf{v}) = \mathbf{b}$; indeed, let $\mathbf{v} \in \widehat{\mathbb{R}^2}$ satisfy $L_A(\mathbf{v}) = \mathbf{b}$. Then, applying L_B to both sides yields the equality:

$$L_B \circ L_A(\mathbf{v}) = L_B(\mathbf{b}),$$

i.e., equivalently,

$$\mathbf{v} = L_B(\mathbf{b}) = L_B(\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}) = \begin{pmatrix} b_1 - b_2 \\ -3b_1 + 4b_2 \end{pmatrix}.$$

Hence, thanks to the fact that we got our hands on that special matrix B, we were able to solve our vector equation.

The natural questions one may ask at this point are:

- **How** did this matrix B show up ?
- How does one find such a matrix B in a **systematic** way ?

We will have the complete answer to these questions in the next few lectures.

Section 13

Study Topics

- Matrix Multiplication

Let m, n, p be given integers ≥ 1, let $A \in \mathcal{M}_{m,n}(\mathbb{R})$ be the real $m \times n$ matrix defined by

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \dots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix},$$

and let $B \in \mathcal{M}_{n,p}(\mathbb{R})$ be the real $n \times p$ matrix defined by

$$B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,p} \\ \vdots & \dots & \vdots \\ b_{n,1} & \cdots & b_{n,p} \end{pmatrix}.$$

Before going further, let us pay attention to the fact that A **has** m **rows and** n **columns** whereas B **has** n **rows and** p **columns**; in particular **the number of columns of** A **is equal to the number of rows of** B.
We know that A defines the **linear** mapping

$$L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^m},$$

and similarly, B defines the **linear** mapping

$$L_B : \widehat{\mathbb{R}^p} \to \widehat{\mathbb{R}^n}.$$

Note that since L_A maps **from** $\widehat{\mathbb{R}^n}$ and since L_B maps **to** $\widehat{\mathbb{R}^n}$, we can compose these two mappings and obtain the mapping $L_A \circ L_B : \widehat{\mathbb{R}^p} \to \widehat{\mathbb{R}^m}$, which is defined by:

$$L_A \circ L_B(\mathbf{v}) = L_A(L_B(\mathbf{v})), \quad \forall \mathbf{v} \in \widehat{\mathbb{R}^p}.$$

What do we know about $L_A \circ L_B$? Well, it is the **composition of two linear mappings** (namely L_A and L_B) hence it is also **linear**. **But there is more!** We will soon see that $L_A \circ L_B$ is actually equal to L_C where C is a real $m \times p$ matrix obtained from A and B ...
Let us begin by computing $L_A \circ L_B(\mathbf{v})$. Let then $\mathbf{v} \in \widehat{\mathbb{R}^p}$ be given by

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix};$$

then, we obtain:

$$L_B(\mathbf{v}) = \begin{pmatrix} b_{1,1}x_1 + \cdots + b_{1,p}x_p \\ \vdots \\ b_{n,1}x_1 + \cdots + b_{n,p}x_p \end{pmatrix},$$

and hence

$$
\begin{aligned}
L_A \circ L_B(\mathbf{v}) &= \begin{pmatrix} a_{1,1}(b_{1,1}x_1 + \cdots + b_{1,p}x_p) + \cdots + a_{1,n}(b_{n,1}x_1 + \cdots + b_{n,p}x_p) \\ \vdots \\ a_{m,1}(b_{1,1}x_1 + \cdots + b_{1,p}x_p) + \cdots + a_{m,n}(b_{n,1}x_1 + \cdots + b_{n,p}x_p) \end{pmatrix} \\
&= \begin{pmatrix} (a_{1,1}b_{1,1} + \cdots + a_{1,n}b_{n,1})x_1 + \cdots + (a_{1,1}b_{1,p} + \cdots a_{1,n}b_{n,p})x_p \\ \vdots \\ (a_{m,1}b_{1,1} + \cdots + a_{m,n}b_{n,1})x_1 + \cdots + (a_{m,1}b_{1,p} + \cdots a_{m,n}b_{n,p})x_p \end{pmatrix} \\
&= L_C(\mathbf{v}),
\end{aligned}
$$

where $C \in \mathcal{M}_{m,p}(\mathbb{R})$ is the real $m \times p$ matrix given by

$$
C = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,p} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,p} \\ \vdots & \vdots & \cdots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,p} \end{pmatrix}
$$

with $c_{i,j}$ given by

$$
\begin{aligned}
c_{i,j} &= a_{i,1}b_{1,j} + a_{i,2}b_{2,j} + a_{i,3}b_{3,j} + \cdots + a_{i,n}b_{n,j} \\
&= \sum_{k=1}^{n} a_{i,k}b_{k,j}
\end{aligned}
$$

for every $1 \leq i \leq m$ and $1 \leq j \leq p$. We call C the **product of A and B** and we write $C = AB$. **NOTE:** C has the same number of rows as A, and the same number of columns as B.
Let us consider a few examples:

1. Let A be the 2×3 matrix given by $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 5 & 1 \end{pmatrix}$, and let B be the 2×2 matrix given by $B = \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix}$; we wish to compute the product AB of A and B. But **this is not possible**, since the number of columns of A is **not** equal to the number of rows of B. Hence, the product AB does not make any sense! On the other hand, the number of columns of B is indeed equal to the number of rows of A, so it **does make sense** to compute the product BA, and we obtain the 2×3 real matrix (with the "·" denoting ordinary multiplication):

$$
\begin{aligned}
BA &= \begin{pmatrix} 1 \cdot 1 + 0 \cdot 3 & 1 \cdot 2 + 0 \cdot 5 & 1 \cdot 0 + 0 \cdot 1 \\ 3 \cdot 1 + 5 \cdot 3 & 3 \cdot 2 + 5 \cdot 5 & 3 \cdot 0 + 5 \cdot 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 0 \\ 18 & 31 & 5 \end{pmatrix}
\end{aligned}
$$

2. Let A be the real $m \times n$ matrix given by

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \cdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix},$$

and let $\mathbf{v}$ be the real $n \times 1$ matrix (i.e. the column vector) given by:

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix};$$

Since the number of columns of A (namely n) is equal to the number of rows of $\mathbf{v}$, it makes sense to consider the product $A\mathbf{v}$ of these two matrices, and we obtain the $m \times 1$ real matrix:

$$A\mathbf{v} = \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{pmatrix}$$

which is **nothing other than** $L_A(\mathbf{v})$!!!! This is why we shall often simply write $A\mathbf{v}$ instead of $L_A(\mathbf{v})$ ...

3. Let now $A \in \mathcal{M}_n(\mathbb{R})$ be the real $n \times n$ (**square**) matrix given by

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

(i.e. 1's on the diagonal, and 0's everywhere else), and let $B \in \mathcal{M}_{n,p}(\mathbb{R})$ be a real $n \times p$ matrix. Since the number of columns of A (namely n) is equal to the number of rows of B, it makes sense to consider the matrix product AB. AB has n rows and p columns, just like B. Furthermore, a simple computation shows that $AB = B$ for any $B \in \mathcal{M}_{n,p}(\mathbb{R})$. For this reason, (as we have seen before), this particular matrix A is called the $n \times n$ **identity matrix**.

4. Let now $A \in \mathcal{M}_{3,2}(\mathbb{R})$ be the real 3×2 matrix given by

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

and $B \in \mathcal{M}_{2,3}(\mathbb{R})$ be the real 2×3 matrix given by

$$B = \begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix};$$

since the number of columns of A (namely 2) is equal to the number of rows of B, it makes sense to consider the matrix product AB, and we obtain after a simple computation that AB is the 3×3 real matrix given by:

$$AB = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 2 & 2 \\ 1 & -2 & 1 \end{pmatrix}.$$

Note that since in this particular case the number of columns of B (namely 3) is equal to the number of rows of A, it **also** makes sense to compute the matrix product BA, and we obtain after a simple computation that BA is the 2×2 real matrix given by:

$$BA = \begin{pmatrix} 1 & 7 \\ 1 & 5 \end{pmatrix}.$$

Note that in this particular example where both AB and BA made sense, AB and BA ended up being of different types: AB is 3×3 whereas BA is 2×2. The next example shows that **even when** AB and BA are of the **same** type, they are not necessarily equal ...

5. Let now A and B both be real 2×2 matrices (so both matrix products AB and BA make sense in this case) given by:

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

We obtain for AB:

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

whereas

$$BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

which shows that AB is **not equal** to BA. So keep in mind that **matrix multiplication is NOT like ordinary multiplication of real numbers!** (Another way to put this is that matrix multiplication is **not commutative**).

6. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$ be a real $m \times n$ matrix, and let $B \in \mathcal{M}_{n,p}(\mathbb{R})$ be a real $n \times p$ matrix. Denote the p column vectors of B by (in order)

$B_{;1}, B_{;2}, \cdots, B_{;p}$, i.e. we can write $B = (B_{;1}\ B_{;2}\ \cdots\ B_{;p})$. It is easy to verify that the matrix product AB has columns vectors given (in order) by $AB_{;1}, AB_{;2}, \cdots, AB_{;p}$, i.e., we can write $AB = (AB_{;1}\ AB_{;2}\ \cdots\ AB_{;p})$. This is often useful in proofs ...

Now that we have seen the "mechanics" of matrix multiplication, let us examine some of its properties:

Theorem 29. Matrix multiplication satisfies the following properties:

(i) Let m, n, p, q be integers ≥ 1. $\forall A \in \mathcal{M}_{m,n}(\mathbb{R})$, $\forall B \in \mathcal{M}_{n,p}(\mathbb{R})$, and $\forall C \in \mathcal{M}_{p,q}(\mathbb{R})$, we have:

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

i.e. matrix multiplication is **associative**.

(ii) Let m, n, p be integers ≥ 1. $\forall A \in \mathcal{M}_{m,n}(\mathbb{R})$, $\forall B, C \in \mathcal{M}_{n,p}(\mathbb{R})$, we have:

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

(iii) Let m, n, p be integers ≥ 1. $\forall A, B \in \mathcal{M}_{m,n}(\mathbb{R})$, $\forall C \in \mathcal{M}_{n,p}(\mathbb{R})$, we have:

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

(iv) Let m, n, p be integers ≥ 1. $\forall A \in \mathcal{M}_{m,n}(\mathbb{R})$, $\forall B \in \mathcal{M}_{n,p}(\mathbb{R})$, $\forall \lambda \in \mathbb{R}$, we have:

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

NOTE: What statement (i) of the theorem says is that we can first multiply A and B to obtain AB, and then multiply this with C to obtain $(AB)C$; we can also first multiply B and C to obtain BC and then multiply A with BC to obtain $A(BC)$. Both give the same result. Hence, we can remove the parentheses and simply write ABC instead of either $(AB)C$ or $A(BC)$.

We shall only prove (i); Properties (ii),(iii),(iv) can be directly verified by computation and are left as an exercise to the reader.

Proof. Recall that the matrix product AB is defined by $L_{AB} = L_A \circ L_B$; similarly, the matrix product $(AB)C$ is defined by $L_{(AB)C} = L_{AB} \circ L_C$. Hence, $L_{(AB)C} = (L_A \circ L_B) \circ L_C$, and since **composition of functions is associative**, we have

$$L_{(AB)C} = (L_A \circ L_B) \circ L_C = L_A \circ (L_B \circ L_C) = L_A \circ L_{BC} = L_{A(BC)},$$

which implies $(AB)C = A(BC)$, and this proves (i). □

Let us now see on some simple examples **how we can apply matrix operations** to the **solution of systems of linear equations**:

1. Consider the system of linear equations given by

$$\begin{aligned} 2x + 3y &= 5 \\ 3x + y &= 7, \end{aligned}$$

where we wish to solve for the pair (x, y) of real numbers which satisfies that system, if such a pair does exist. We can write this equation in matrix form as:

$$\begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix},$$

and since the column vectors of the 2×2 matrix $\begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}$ are **linearly independent** we know that this system has a **unique** solution. Consider now the 2×2 matrix given by $\begin{pmatrix} -\frac{1}{7} & \frac{3}{7} \\ \frac{3}{7} & -\frac{2}{7} \end{pmatrix}$. It is easy to verify that

$$\begin{pmatrix} -\frac{1}{7} & \frac{3}{7} \\ \frac{3}{7} & -\frac{2}{7} \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which is nothing other than the 2×2 identity matrix. Hence, multiplying both sides of the equation

$$\begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix},$$

by the matrix $\begin{pmatrix} -\frac{1}{7} & \frac{3}{7} \\ \frac{3}{7} & -\frac{2}{7} \end{pmatrix}$, we obtain

$$\begin{pmatrix} -\frac{1}{7} & \frac{3}{7} \\ \frac{3}{7} & -\frac{2}{7} \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -\frac{1}{7} & \frac{3}{7} \\ \frac{3}{7} & -\frac{2}{7} \end{pmatrix} \begin{pmatrix} 5 \\ 7 \end{pmatrix},$$

i.e., equivalently,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{16}{7} \\ \frac{1}{7} \end{pmatrix},$$

and since

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix},$$

we finally obtain the solution to our system of equations as

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{16}{7} \\ \frac{1}{7} \end{pmatrix}.$$

2. More generally, consider the system of linear equations (in n equations and n unknowns) given by

$$\begin{aligned} a_{1,1}x_1 + \cdots a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + \cdots a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{n,1}x_1 + \cdots a_{n,n}x_n &= b_n \end{aligned}$$

where we wish to solve for the $n-$tuples $(x_1, x_2, \cdots, x_n)$ of real numbers. We can write this system in matrix form as:

$$A\mathbf{v} = \mathbf{b},$$

where $A \in \mathcal{M}_n(\mathbb{R})$ is the square $n \times n$ matrix given by

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix},$$

$\mathbf{b} \in \mathcal{M}_{n,1}(\mathbb{R})$ is the $n \times 1$ matrix (i.e. column vector) given by

$$\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix},$$

and, finally,

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

is the $n \times 1$ matrix (i.e. column vector) we wish to solve for. **Assume** there exists a matrix $B \in \mathcal{M}_n(\mathbb{R})$ such that the matrix product of B and A, i.e. BA, is equal to the $n \times n$ **identity matrix**. Then, multiplying (to the left) both sides of the equality

$$A\mathbf{v} = \mathbf{b},$$

by B yields

$$BA\mathbf{v} = B\mathbf{b},$$

and since BA is the $n \times n$ identity matrix, we obtain

$$\mathbf{v} = B\mathbf{b},$$

i.e. we have the solution to our original system of equations. In the next lectures, we will see **when** such a matrix B does exist and **how** to compute it.

Applications of Matrix Multiplication

The notion of matrix multiplication (together with other linear algebraic notions we have studied so far) can lead to interesting engineering applications. We present two of these in what follows.

- **Message Scrambling**

  Suppose we wish to communicate a message to another party, but in such a way that it could not be easily decoded by a third party. Assume also that the message is to be sent as a string of integers greater than or equal to 0 (in some large enough range, say 0 to 1000), arranged in matrix form. The simplest way to proceed would be, say, to assign the integer 1 to the letter "a", the integer 2 to the letter "b", and so on, until the integer 26, assigned to the letter "z" (assume for simplicity that we care only about lower case letters, and no other symbols other than the space symbol and the period – it is of course easy to see how these ideas can be generalized). Assume also that the integer 0 would be assigned to the space symbol, and the integer 27 to the period ".". We could then transmit the sentence "hello world." as the 1×12 matrix

$$\begin{pmatrix} 8 & 5 & 12 & 12 & 15 & 0 & 23 & 15 & 18 & 12 & 4 & 27 \end{pmatrix},$$

  and we could similarly transmit longer messages (the corresponding matrix will of course have the same number of columns as there are characters in the message to be sent). What is the problem with this approach ? The main problem is that the code can be easily broken. Indeed, the statistics regarding the frequency of occurence of individual letters in the English alphabet are well known (e.g. the letter "e" occurs the most often), and from these statistics it would be possible (assuming the message is long enough) to find out which integer was assigned to which letter. Note that even a slightly less straightforward scheme, such as asssigning 100 to "a", 22 to "b", 33 to "c", and so on, would still suffer from the same problem: The correspondence between the integers and the letters (i.e. the "code") could be recovered by examining the frequency of occurence of the individual integers.

  Is there any way around this ? Well, consider the matrices $A = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$, and $B = \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$. Note that all the entries of A are integers greater than or equal to 0. Note also that the product AB is the 2×2 identity matrix. These properties will be essential in what follows. Consider now the following more involved way of transmitting the above message, i.e. the matrix

$$\begin{pmatrix} 8 & 5 & 12 & 12 & 15 & 0 & 23 & 15 & 18 & 12 & 4 & 27 \end{pmatrix};$$

We first chop it up in blocks of length 2, and then multiply by matrix A on the right; this is of course possible since A has two rows. The first block of length 2 is the 1×2 submatrix $\begin{pmatrix} 8 & 5 \end{pmatrix}$; multiplying it by A yields the 1×2 matrix $\begin{pmatrix} 37 & 29 \end{pmatrix}$. The next block of length 2 in our message above is the submatrix $\begin{pmatrix} 12 & 12 \end{pmatrix}$; multiplying it by A yields the 1×2 matrix $\begin{pmatrix} 60 & 48 \end{pmatrix}$. The next block of length 2 is the submatrix $\begin{pmatrix} 15 & 0 \end{pmatrix}$; multiplying it by A yields the 1×2 matrix $\begin{pmatrix} 60 & 45 \end{pmatrix}$. The next block of length 2 is the submatrix $\begin{pmatrix} 23 & 15 \end{pmatrix}$; multiplying it by A yields the 1×2 matrix $\begin{pmatrix} 107 & 84 \end{pmatrix}$. The next block of length 2 is the submatrix $\begin{pmatrix} 18 & 12 \end{pmatrix}$; multiplying it by A yields the 1×2 matrix $\begin{pmatrix} 84 & 66 \end{pmatrix}$. The final block of length 2 is the submatrix $\begin{pmatrix} 4 & 27 \end{pmatrix}$; multiplying it by A yields the 1×2 matrix $\begin{pmatrix} 43 & 39 \end{pmatrix}$. After all this, we would put together the blocks of length 2 we have obtained as a result of multiplication by A, and we would send our message as the following 1×12 matrix:

$$\begin{pmatrix} 37 & 29 & 60 & 48 & 60 & 45 & 107 & 84 & 84 & 66 & 43 & 39 \end{pmatrix}.$$

What we have done is "scramble" the original message; the code cannot be easily recovered from the occurence statistics of the integers. But how do we recover our original message ? Well, the party we are sending our message to is aware that they need matrix B to recover the message. All they need to do is break down the message they have received (i.e. the 1×12 matrix above) into blocks of length 2, and multiply each block on the right by B. Since AB is the 2×2 identity matrix, the original message can be recovered. For example, multiplying the first block of length 2 of the received message, i.e. $\begin{pmatrix} 37 & 29 \end{pmatrix}$ by matrix B on the right yields the 1×2 matrix $\begin{pmatrix} 8 & 5 \end{pmatrix}$. Continuing this procedure for all subsequent 1×2 blocks yields the original message.

There are more sophisticated variations of this approach; we could for example scramble the message even more by arranging the original message as the following 2×6 matrix:

$$\begin{pmatrix} 8 & 5 & 12 & 12 & 15 & 0 \\ 23 & 15 & 18 & 12 & 4 & 27 \end{pmatrix};$$

We would then take the first 2×2 block, i.e. the submatrix $\begin{pmatrix} 8 & 5 \\ 23 & 15 \end{pmatrix}$, multiply it on the right by A, obtaining $\begin{pmatrix} 37 & 29 \\ 107 & 84 \end{pmatrix}$. We would then do the same with the next 2×2 block, and so on. We would then arrange all the 2×2 blocks thus obtained as a 2×6 matrix which we would send to the other party; the receiving party would then take the consecutive 2×2 blocks of this 2×6 matrix, multiply them on the right by B, thereby recovering the original 2×6 matrix containing the message. Compared to our original approach, this would scramble the original message even more, making it even harder to recover the correspondence between the letters and the integers.

Note that we could also scramble the original message more by taking A and B to be 3×3 (or even larger) square matrices; the key properties of A and B are that A should have integer entries (greater than or equal to 0) and that the product AB should be equal to the identity matrix. The requirement that A have integer entries greater than or equal to 0 will ensure that if the original unscrambled message is encoded using integers greater than or equal to 0, so will the scrambled message. The requirement that the product AB be equal to the identity matrix ensures that the original message can be recovered from the scrambled message.

- **Process Control**

  Consider two reservoirs containing a certain liquid, and assume the level of the liquid in the reservoirs at time n ($n = 0, 1, 2, \ldots$) is represented by the vector $\mathbf{x}_n = \begin{pmatrix} y_n \\ z_n \end{pmatrix} \in \hat{\mathbb{R}}^2$, with y_n representing the level in the first reservoir at time n, and z_n representing the level in the second reservoir at time n. Assume also that from time n to time $n+1$, a certain fraction of the liquid in both reservoirs is lost due to evaporation. We also assume that a certain fraction of the liquid in the first reservoir is transferred to the second reservoir through some channel in going from time n to time $n+1$. Finally, we assume that a certain amount of liquid is injected in the first reservoir at times $n = 0, 1, 2, \ldots$. This process can be modelled mathematically as follows:

$$\mathbf{x}_{n+1} = A\mathbf{x}_n + Bu_n,$$

  where A is a real 2×2 matrix representing the evaporation of the liquids and the transfer from the first to the second reservoir, $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and u_n represents the amount of liquid injected in the first reservoir at time n (a negative value would represent an amount of liquid taken from the first reservoir). For example, if in going from time n to time $n+1$, 25 percent of the liquid in the first reservoir and 10 percent of the liquid in the second reservoir are lost due to evaporation, and 20 percent of the liquid in the first reservoir is transferred to the second reservoir, matrix A would be equal to the matrix $\begin{pmatrix} .75 & 0 \\ .2 & .9 \end{pmatrix}$, and the level of the liquid in the reservoirs at times $n = 0, 1, 2, \ldots$ would be governed by the equation:

$$\begin{pmatrix} y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} .75 & 0 \\ .2 & .9 \end{pmatrix} \begin{pmatrix} y_n \\ z_n \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} u_n, \quad n = 0, 1, 2, \ldots$$

The vector $\begin{pmatrix} y_0 \\ z_0 \end{pmatrix}$ represents the level of the liquid in the reservoirs at the initial time $n = 0$; assuming at time $n = 0$ the amount u_0 of liquid is injected into the first reservoir, the above equation gives us the vector $\begin{pmatrix} y_1 \\ z_1 \end{pmatrix}$, which represents the level of the liquid in the reservoirs at time $n = 1$. With u_1 denoting the amount of liquid injected in the first reservoir at time $n = 1$, we then obtain from the above equation the vector $\begin{pmatrix} y_2 \\ z_2 \end{pmatrix}$, which represents the level of the liquid in the reservoirs at time $n = 2$. Continuing in this way we obtain the vector $\begin{pmatrix} y_n \\ z_n \end{pmatrix}$ for all $n = 0, 1, 2, \ldots$.

A natural question at this point is whether we can make the reservoirs have a desired level of liquid at a given time by suitably choosing $u_0, u_1, u_2, \ldots$. For example, assume that the reservoirs are initially empty, i.e. $\begin{pmatrix} y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$; by suitably choosing u_0, u_1, u_2, can we make the level of liquid in the reservoirs at time $n = 3$ be equal to $\begin{pmatrix} 10 \\ 20 \end{pmatrix}$? In other words, by suitably choosing u_0, u_1, u_2, can we make the vector $\mathbf{x}_3 = \begin{pmatrix} y_3 \\ z_3 \end{pmatrix}$ be equal to the vector $\begin{pmatrix} 10 \\ 20 \end{pmatrix}$? To answer this question, we return to the governing equation for $\mathbf{x}_n$, i.e.

$$\mathbf{x}_{n+1} = A\mathbf{x}_n + Bu_n, \quad n = 0, 1, 2, \ldots$$

We have:

$$\mathbf{x}_1 = A\mathbf{x}_0 + Bu_0,$$

and hence

$$\mathbf{x}_2 = A\mathbf{x}_1 + Bu_1 = A(A\mathbf{x}_0 + Bu_0) + Bu_1 = A^2\mathbf{x}_0 + ABu_0 + Bu_1,$$

and finally

$$\begin{aligned} \mathbf{x}_3 &= A\mathbf{x}_2 + Bu_2 = A(A^2\mathbf{x}_0 + ABu_0 + Bu_1) + Bu_2 \\ &= A^3\mathbf{x}_0 + A^2Bu_0 + ABu_1 + Bu_2. \end{aligned}$$

Since we have assumed that the reservoirs are initially empty, i.e. $\mathbf{x}_0$ is the zero vector, we actually have:

$$\mathbf{x}_3 = A^2 B u_0 + AB u_1 + B u_2.$$

The question is now: Can we choose u_0, u_1, u_2 such that $\mathbf{x}_3$ be equal to the vector $\begin{pmatrix} 10 \\ 20 \end{pmatrix}$? A simple calculation shows that the vectors B, AB, A^2B span $\hat{\mathbb{R}}^2$; hence not only can we choose u_0, u_1, u_2 to ensure that $\mathbf{x}_3$ is equal to the vector $\begin{pmatrix} 10 \\ 20 \end{pmatrix}$ – for example choosing $u_0 = 0$, $u_1 = 100$ and $u_2 = -65$ yields the desired outcome – we can actually, by a proper choice of u_0, u_1, u_2, make sure that $\mathbf{x}_3$ is *any* desired vector of $\hat{\mathbb{R}}^2$. In the language of process control, the vector $\mathbf{x}_n$ is called the **state** of the system at time n, whereas u_n is called the **control** at time n.

PROBLEMS:

1. For each of the following choices for the matrices A and B, do the following:

   - Specify whether it makes sense to consider the matrix product AB (and indicate why or why not), and if
     the product AB makes sense, do compute it.
   - Specify whether it makes sense to consider the matrix product BA (and indicate why or why not), and if
     the product BA makes sense, do compute it.

   (a) $A = \begin{pmatrix} -1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$.

   (b) $A = \begin{pmatrix} -1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

   (c) $A = \begin{pmatrix} -1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

   (d) $A = \begin{pmatrix} -1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \end{pmatrix}$.

   (e) $A = \begin{pmatrix} -1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 2 & 2 \end{pmatrix}$.

   (g) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -3 \\ 5 & 1 \end{pmatrix}$.

   (h) $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 2 & -3 \\ 0 & 0 \end{pmatrix}$.

(i) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$

(j) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$

(k) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$

(l) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$

(m) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$

(n) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & -3 \\ -2 & 0 & 1 \end{pmatrix}.$

(o) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$

(p) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 5 & 7 \\ 0 & 0 & 1 \end{pmatrix}.$

(q) $A = \begin{pmatrix} -1 & 2 & 5 \\ 3 & -2 & 5 \\ 7 & 0 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$

(r) $A = \begin{pmatrix} -1 & 2 & 5 \\ 3 & -2 & 5 \\ 7 & 0 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$

(s) $A = \begin{pmatrix} -1 & 2 & 5 \\ 3 & -2 & 5 \\ 7 & 0 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$

(t) $A = \begin{pmatrix} -1 & 2 & 5 \\ 3 & -2 & 5 \\ 7 & 0 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$

(u) $A = \begin{pmatrix} -2 & 1 \\ 1 & 2 \\ 3 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 5 \end{pmatrix}.$

(v) $A = \begin{pmatrix} -2 & 1 \\ 1 & 0 \\ 3 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$

(w) $A = \begin{pmatrix} -1 & 3 \\ 0 & 0 \\ 1 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(x) $A = \begin{pmatrix} -3 & 3 \\ 2 & 7 \\ -2 & -5 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

(y) $A = \begin{pmatrix} -1 & 2 \\ 3 & 5 \\ 7 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$.

(z) $A = \begin{pmatrix} -5 & -2 \\ -3 & 1 \\ -2 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 3 & 0 & 1 \end{pmatrix}$.

2. We wish to transmit a message, encoded as the following 2×6 matrix in a secure way (in that matrix, as in the example in the text, the integer 1 to the letter "a", the integer 2 to the letter "b", and so on, and the integer 0 is assigned to the

space symbol, and the integer 27 to the period "." (the first half of the message is on the first row, and the second half on the second row):

$$\text{M} = \begin{pmatrix} 16 & 12 & 5 & 1 & 19 & 5 \\ 0 & 3 & 1 & 12 & 12 & 27 \end{pmatrix}.$$

We wish to do so by scrambling the message before sending it, and have the receiving party unscramble the received message. We will do the scrambling using the 2×2 matrix $A = \begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix}$; the receiving party will unscramble the received message

and recover the original message M using matrix $B = \begin{pmatrix} 1 & -4 \\ -1 & 5 \end{pmatrix}$. The scrambling will be done by taking consecutive 2×2 blocks from M (note that there are 3 such blocks in M) and multiplying them on the right by matrix A. The result of these

multiplications will form the scrambled message. At the receiving it, the receiving party will take the received (scrambled) 2×6 matrix, break it into consecutive 2×2 blocks and multiply each on the right by B, thereby recovering the original message M.

(a) Verify directly that AB is the 2×2 identity matrix.

(b) Compute the scrambled message using A (according to the scrambling procedure above).

(c) Recover the original message by directly unscrambling the scrambled message using matrix B (using the unscrambling procedure detailed above).

3. We wish to transmit the same message as above message, encoded now as the following 1×12 matrix, in a secure way:

$$\mathrm{M} = \begin{pmatrix} 16 & 12 & 5 & 1 & 19 & 5 & 0 & 3 & 1 & 12 & 12 & 27 \end{pmatrix}.$$

We wish to do so by scrambling the message before sending it, and have the receiving party unscramble the received message. We will do the scrambling using the 3×3 matrix $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 1 & 1 \end{pmatrix}$; the receiving party will unscramble the received message

and recover the original message M using matrix $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & -1 & 3 \end{pmatrix}$.

The scrambling will be done by taking consecutive 1×3 blocks from M (note that there are 4 such blocks in M) and multiplying

them on the right by matrix A. The result of these

multiplications will form the scrambled message. At the receiving it, the receiving party will take the received (scrambled) 1×12 matrix, break it into consecutive 1×3 blocks and multiply each on the right by B, thereby recovering the original message M.

(a) Verify directly that AB is the 3×3 identity matrix.

(b) Compute the scrambled message using A (according to the scrambling procedure above).

(c) Recover the original message by directly unscrambling the scrambled message using matrix B (using the unscrambling procedure detailed above).

4. Two reservoirs containing a certain liquid are involved in a chemical process. With the vector $\mathbf{x}_n = \begin{pmatrix} y_n \\ z_n \end{pmatrix}$ representing the level of the liquids

in the reservoirs at time $n = 0, 1, 2, \ldots$ (with y_n being the level in the first reservoir, and

z_n in the second), we assume that due to various physical processes (evaporation, leaks from one reservoir to the other, external injection of liquid in the reservoirs) the equation governing the level of fluids in the reservoirs is given by

$$\mathbf{x}_{n+1} = \begin{pmatrix} .5 & .1 \\ .2 & .7 \end{pmatrix} \mathbf{x}_n + \begin{pmatrix} 0 \\ 1 \end{pmatrix} u_n, \quad n = 0, 1, 2, \cdots$$

where u_n denotes the amount of liquid injected in the second reservoir at time n.

(a) Assuming that the reservoirs are empty at time $n = 0$, i.e. assuming $\mathbf{x}_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, can we suitably choose u_0 to ensure that $\mathbf{x}_1$ will be equal to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$?

(b) Assuming that the reservoirs are empty at time $n = 0$, i.e. assuming $\mathbf{x}_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, can we suitably choose u_0, u_1 to ensure that $\mathbf{x}_2$ will be equal to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$?

(c) Assuming that the initial fluid levels are given by $\mathbf{x}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, can we suitably choose u_0 to ensure that $\mathbf{x}_1$ will be equal to $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$?

(d) Assuming that the initial fluid levels are given by $\mathbf{x}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, can we suitably choose u_0, u_1 to ensure that $\mathbf{x}_2$ will be equal to $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$?

5. Three reservoirs containing a certain liquid are involved in a chemical process. With the vector $\mathbf{x}_n = \begin{pmatrix} y_n \\ z_n \\ w_n \end{pmatrix}$ representing the level of the liquids in the reservoirs at time $n = 0, 1, 2, \ldots$ (with y_n being the level in the first reservoir,

z_n in the second, and w_n in the third), we assume that due to various physical processes (evaporation, leaks from one reservoir to the other, external injection of liquid in the reservoirs) the equation governing the level of fluids in the reservoirs is given by

$$\mathbf{x}_{n+1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mathbf{x}_n + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} u_n, \quad n = 0, 1, 2, \cdots$$

where u_n denotes the amount of liquid injected in the first reservoir at time n.

(a) Assuming that the reservoirs are empty at time $n = 0$, i.e. assuming $\mathbf{x}_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, can we suitably choose u_0 to ensure that $\mathbf{x}_1$ will be equal to
$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$?

(b) Assuming that the reservoirs are empty at time $n = 0$, i.e. assuming $\mathbf{x}_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, can we suitably choose u_0, u_1 to ensure that $\mathbf{x}_2$ will be equal to
$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$?

(c) Assuming that the reservoirs are empty at time $n = 0$, i.e. assuming $\mathbf{x}_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, can we suitably choose u_0, u_1, u_2 to ensure that $\mathbf{x}_3$ will be equal to
$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$?

Section 14

Study Topics

- Invertible Square Matrices
- Determinant of a Square Matrix

Consider the system of linear equations (with m equations and n unknowns) given by

$$\begin{array}{rcl} a_{1,1}x_1 + a_{1,2}x_2 + \cdots a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots a_{2,n}x_n & = & b_2 \\ & \cdots & \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots a_{m,n}x_n & = & b_m \end{array}$$

where we wish to solve for $x_1, x_2, \cdots, x_n$. Defining the matrix Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$ by

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \cdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix},$$

defining $\mathbf{v} \in \widehat{\mathbb{R}^n}$ and $\mathbf{w} \in \widehat{\mathbb{R}^m}$ by

$$\mathbf{v} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

we have seen that the above system of linear equations can be written equivalently (using the operation of matrix multiplication we have introduced) as the one matrix/vector equation

$$A\mathbf{v} = \mathbf{w}.$$

Assume now there exists a real $n \times m$ matrix $B \in \mathcal{M}_{n,m}(\mathbb{R})$ such that $BA = I_n$. Multiplying both sides of the above equation by matrix B on the left yields

$$B(A\mathbf{v}) = B\mathbf{w},$$

and, using the associativity of matrix multiplication, we obtain:

$$(BA)\mathbf{v} = B\mathbf{w},$$

and since $BA = I_n$ by assumption, we finally obtain

$$I_n\mathbf{v} = B\mathbf{w},$$

i.e.

$$\mathbf{v} = B\mathbf{w}.$$

In other words, we have shown that, **assuming there exists** $B \in \mathcal{M}_{n,m}(\mathbb{R})$ such that $BA = I_n$, if $\mathbf{v}$ satisfies the equation $A\mathbf{v} = \mathbf{w}$ then, necessarily, $\mathbf{v} = B\mathbf{w}$. Does it follow from this that if now $\mathbf{v}$ is given by $\mathbf{v} = B\mathbf{w}$ then necessarily $A\mathbf{v} = \mathbf{w}$? Not at all! To see this, consider the very simple system of linear equations in 2 equations and 1 unknown given by

$$\begin{aligned} 2x &= 0 \\ 2x &= 4, \end{aligned}$$

which we can write as the matrix equation $A\mathbf{v} = \mathbf{w}$ with $A = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$, $\mathbf{v} = (x)$, and $\mathbf{w} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. It is clear that this system has no solution, and hence, no $\mathbf{v}$ satisfies the equation $A\mathbf{v} = \mathbf{w}$ for this particular choice of matrix A and vector $\mathbf{w}$. However, note that there does exist a 1×2 matrix B such that $BA = 1$ (the 1×1 identity matrix!), namely the matrix given by $B = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \end{pmatrix}$, and $B\mathbf{w}$ is equal to the 1×1 matrix (i.e. real number) 1. However, the latter is not a solution to the original equation $A\mathbf{v} = \mathbf{w}$.
So the question now becomes: Under what condition on matrix A does it follow that $\mathbf{v} = B\mathbf{w}$ implies $A\mathbf{v} = \mathbf{w}$? For this, let **assume that we also have** $AB = I_m$. Then, multiplying both sides of the equation $\mathbf{v} = B\mathbf{w}$ on the left by A yields:

$$A\mathbf{v} = A(B\mathbf{w}),$$

and, again using the associativity of matrix multiplication, we obtain:

$$A\mathbf{v} = (AB)\mathbf{w},$$

and since we have assumed $AB = I_m$, we obtain:

$$A\mathbf{v} = I_m\mathbf{w} = \mathbf{w}.$$

Hence, to recapitulate, we have shown that **if there exists** $B \in \mathcal{M}_{n,m}(\mathbb{R})$ such that $BA = I_n$ **and** $AB = I_m$, then the equation

$$A\mathbf{v} = \mathbf{w}$$

is **equivalent to** the equation

$$\mathbf{v} = B\mathbf{w},$$

i.e. we have solved our original equation.
We can now ask ourselves the question: Given an arbitrary real matrix $A \in \mathcal{M}_{m,n}(\mathbb{R})$, does there always exist a real matrix $B \in \mathcal{M}_{n,m}(\mathbb{R})$ satisfying $AB = I_m$ and $BA = I_n$? The answer is clearly no! (to see this, let A be the matrix with all entries 0). As the theorem below shows, there are severe restrictions on real matrices A which admit such a B. Indeed, as we now prove. if, for a given real $m \times n$ matrix A, there exists a real $n \times m$ matrix B such that $AB = I_m$ and $BA = I_n$, then, necessarily $m = n$, i.e. A must be a **square** matrix.

Theorem 30. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$, and assume there exists $B \in \mathcal{M}_{n,m}(\mathbb{R})$ satisfying $AB = I_m$ and $BA = I_n$; then $m = n$, i.e., A is a **square** matrix.

Proof. Let $A \in \mathcal{M}_{m,n}(\mathbb{R})$, and assume there exists $B \in \mathcal{M}_{n,m}(\mathbb{R})$ satisfying $AB = I_m$ and $BA = I_n$. Let now $\mathbf{v} \in \text{Ker}(A)$ be any element in the kernel of A. By definition of the kernel, we have $A\mathbf{v} = \mathbf{0}$, and multiplying both sides of this equation on the left by B yields $B(A\mathbf{v}) = B\mathbf{0} = \mathbf{0}$, i.e. (by associativity of matrix multiplication) $(AB)\mathbf{v} = I_n\mathbf{v} = \mathbf{v} = \mathbf{0}$; this shows $\text{Ker}(A) = \{\mathbf{0}\}$. It follows then (from what we have seen in previous lectures) that the column vectors of A are linearly independent, and since the n column vectors of A are elements of the $m-$dimensional vector space $\widehat{\mathbb{R}^m}$, it follows that $m \geq n$. Let now $\mathbf{w} \in \widehat{\mathbb{R}^m}$ be any element of $\widehat{\mathbb{R}^m}$, and let $\mathbf{v} = B\mathbf{w}$. Multiplying both sides of this equation on the left by A yields $A\mathbf{v} = A(B\mathbf{w}) = (AB)\mathbf{w} = I_m\mathbf{w} = \mathbf{w}$, which shows that $\mathbf{w}$ is in the image of A. Since $\mathbf{w}$ was an arbitrary element of $\widehat{\mathbb{R}^m}$, this shows that $\text{Im}(A) = \widehat{\mathbb{R}^m}$. Hence, from what we have seen in previous lectures, it follows that the column vectors of A form a generating family for $\widehat{\mathbb{R}^m}$, and since there are n of them (and the dimension of $\widehat{\mathbb{R}^m}$ is m), it follows that $m \leq n$. □

We have therefore shown $m \geq n$ and $m \leq n$; hence $m = n$, i.e. A is a **square** matrix.
We are then very naturally led to the following definition:

Definition 30. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. A is said to be **invertible** if there exists a real $n \times n$ matrix B such that $AB = BA = I$, where I is the $n \times n$ identity matrix.

Remark 7. It is easy to show (but we won't do it here) that if A, B are **square** matrices, the relation $AB = I$ actually implies $BA = I$, and vice-versa. This follows from the **rank-nullity theorem** (and the fact that A, B are assumed to be **square** matrices.

Let now $A \in \mathcal{M}_n(\mathbb{R})$ and **assume** A **invertible**; by definition of invertibility, this means that there exists $B \in \mathcal{M}_n(\mathbb{R})$ such that $AB = BA = I$ (I denoting again the $n \times n$ identity matrix). A natural question at this point is: Is there **only one** matrix B which satisfies this, or **are there many** ? The answer is given in the following theorem.

Theorem 31. Let $A \in \mathcal{M}_n(\mathbb{R})$. If A is **invertible**, then there exists a **unique** $B \in \mathcal{M}_n(\mathbb{R})$ such that $AB = BA = I$ (I denoting again the $n \times n$ identity matrix).

Proof. Assume there exist $n \times n$ matrices $B, C \in \mathcal{M}_n(\mathbb{R})$ such that $AB = BA = I$ and $AC = CA = I$; we have to show that B must then be equal to C. We have:

$$B = BI = B(AC) = (BA)C = IC = C,$$

which is exactly what we wished to prove. □

This leads naturally to the following definition:

Definition 31. Let $A \in \mathcal{M}_n(\mathbb{R})$ and assume A is invertible. The **unique** matrix $B \in \mathcal{M}_n(\mathbb{R})$ which satisfies $AB = BA = I$ is called **the inverse of** A and is denoted A^{-1}.

Before going further, let us **highlight a few key points**:

(i) The definition of **invertible** matrices applies **only** to **square matrices**.

(ii) it does not make **any sense** to talk about invertibility of an $m \times n$ matrix with $m \neq n$.

Let us now consider a few simple examples:

1. Consider the $n \times n$ **identity matrix** I; it is easy to see that the inverse of I is I itself since we have $II = I$. In particular, I is invertible.

2. Let A be the $n \times n$ **zero matrix** (i.e. the $n \times n$ matrix with all entries equal to zero); since for any $B \in \mathcal{M}_n(\mathbb{R})$ the matrix products BA and AB are equal to the zero matrix, it follows that there is no $B \in \mathcal{M}_n(\mathbb{R})$ for which the matrix products BA and AB be equal to the $n \times n$ identity matrix; hence the $n \times n$ zero matrix is **not invertible**.

3. Let A be the 2×2 matrix given by $A = \begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix}$; it is easy to verify that the 2×2 matrix given by $B = \begin{pmatrix} 1 & -1 \\ -4 & 5 \end{pmatrix}$ satisfies $AB = BA = I$ (I being the 2×2 identity matrix); hence A is invertible and B is its inverse.

The following questions arise naturally at this point: Consider an $n \times n$ real matrix A;

- **How do we find out whether or not A is invertible** ?
- In case A is invertible, **how do we compute the inverse of** A ?

The following important theorem addresses the first question:

Theorem 32. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. We have:

- A is **invertible if and only if** the column vectors of A are **linearly independent**.

Equivalently, A is **invertible if and only if** A has **rank** n.

Proof. (i) Assume first that A is invertible, and let $B \in \mathcal{M}_n(\mathbb{R})$ be its inverse (i.e. $AB = BA = I$, where I is the $n \times n$ identity matrix). We wish to show that this implies that the column vectors of A are linearly independent. From what we have seen in Lecture 10, showing that the column vectors of A are linearly independent is equivalent to showing that $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$

(i.e. the kernel of A contains only the zero vector of $\widehat{\mathbb{R}^n}$); equivalently, we need to show that if $\mathbf{v} \in \ker(A)$, then we must have $\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}}$. Let then $\mathbf{v} \in \ker(A)$; then, by definition of $\ker(A)$, we have:

$$A\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}},$$

and multiplying both sides of the above equation by the matrix B (the inverse of A), we obtain:

$$B(A\mathbf{v}) = B\mathbf{0}_{\widehat{\mathbb{R}^n}} = \mathbf{0}_{\widehat{\mathbb{R}^n}},$$

i.e., equivalently (by associativity of matrix multiplication),

$$(BA)\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}},$$

i.e.

$$\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}},$$

since $BA = I$ and $I\mathbf{v} = \mathbf{v}$. Hence, we have shown that $\mathbf{v} \in \ker(A)$ **implies** $\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}}$. This proves that $\ker(A) = \{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$, which (by Lecture 10) implies that the column vectors of A are linearly independent, as desired.

(ii) Assume now that the column vectors of A are linearly independent; we need to show that A is then invertible. Since the column vectors of A are assumed linearly independent, it follows that the linear map $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^n}$ defined by matrix A is **one-to-one** (i.e. injective); furthermore, it follows from the rank-nullity theorem that the range (i.e. image) $\text{Im}(A)$ of matrix A is all of $\widehat{\mathbb{R}^n}$, i.e. that the linear map L_A is **onto** (i.e. surjective). It follows that there exists a real $n \times n$ matrix B such that:

$$L_B \circ L_A(\mathbf{v}) = L_A \circ L_B(\mathbf{v}) = \mathbf{v}, \quad \forall \mathbf{v} \in \widehat{\mathbb{R}^n},$$

i.e.

$$BA = AB = I,$$

where I is the $n \times n$ identity matrix. Hence, A is invertible.

□

Before going further, let us **summarize how we can apply** this last **extremely important** theorem: Suppose you are given a real $n \times n$ matrix A; then,

- **If the column vectors of** A form a **linearly independent** family of $\widehat{\mathbb{R}^n}$, then A **is** invertible;
- **If the column vectors of** A form a **linearly dependent** family of $\widehat{\mathbb{R}^n}$, then A is **not** invertible.

Let us now look at a few examples before going further:

1. Let $I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ be the $n \times n$ identity matrix; we have already seen that I is invertible (and it's inverse is I itself). Now we know **why** I is invertible: It's n column vectors are **linearly independent**, as can be easily verified (and as we have seen many times earlier!).

2. Consider the 3×3 real matrix $A = \begin{pmatrix} 1 & 1 & 2 \\ -1 & 1 & 0 \\ 2 & 3 & 5 \end{pmatrix}$; Is A invertible ? Well, by the previous theorem, we have to see whether or not the column vectors of A are linearly independent. Let $A_{;1}, A_{;2}, A_{;3}$ denote the three column vectors of A; it is easy to see that

$$A_{;1} + A_{;2} - A_{;3} = \mathbf{0}_{\widehat{\mathbb{R}^3}},$$

which shows that the column vectors of A are **not** linearly independent; hence, by the previous theorem, A is **not** invertible.

3. Consider the 3×3 real matrix $A = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 2 & 3 & 5 \end{pmatrix}$; Is A invertible ? Again, by the previous theorem, we have to see whether or not the column vectors of A are linearly independent. Let $A_{;1}, A_{;2}, A_{;3}$ denote the three column vectors of A; it is easy to verify that $\{A_{;1}, A_{;2}, A_{;3}\}$ is a **linearly independent** subset of $\widehat{\mathbb{R}^3}$; hence, it follows from the previous theorem that A **is invertible**.

We now introduce an **extremely important** function of matrices, the **determinant**. Before, however, we need to introduce some notation:

Definition 32. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a square $n \times n$ matrix. Let i, j be integers ≥ 1 and $\leq n$. We denote by $[A]_{i,j}$ the $(n-1) \times (n-1)$ matrix obtained from A by **deleting row i and column j**.

Let us see consider a few examples:

1. Consider the real 2×2 matrix $A = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$; we have:

$$[A]_{1,1} = (4), \quad [A]_{1,2} = (3), \quad [A]_{2,1} = (1), \quad [A]_{2,2} = (2).$$

2. Consider the real 3×3 matrix $A = \begin{pmatrix} 5 & 1 & 0 \\ -1 & 2 & 3 \\ 7 & 4 & 1 \end{pmatrix}$; we have:

$$[A]_{1,1} = \begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix}, \quad [A]_{1,2} = \begin{pmatrix} -1 & 3 \\ 7 & 1 \end{pmatrix}, \quad [A]_{1,3} = \begin{pmatrix} -1 & 2 \\ 7 & 4 \end{pmatrix},$$

$$[A]_{2,1} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \quad [A]_{2,2} = \begin{pmatrix} 5 & 0 \\ 7 & 1 \end{pmatrix}, \quad [A]_{2,3} = \begin{pmatrix} 5 & 1 \\ 7 & 4 \end{pmatrix},$$

$$[A]_{3,1} = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}, \quad [A]_{3,2} = \begin{pmatrix} 5 & 0 \\ -1 & 3 \end{pmatrix}, \quad [A]_{3,3} = \begin{pmatrix} 5 & 1 \\ -1 & 2 \end{pmatrix}.$$

We are now ready to define the **determinant of a square matrix:**

Definition 33. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a **square** $n \times n$ real matrix. The **determinant** $\det(A)$ of A is the **real number** defined as follows:

(i) If $n = 1$, i.e. $A = (a)$ for some real number a, then $\det(A) = a$;

(ii) If $n > 1$, then $\det(A)$ is recursively defined as follows:

$$\det(A) = \sum_{j=1}^{n} (-1)^{1+j} a_{1,j} \det([A]_{1,j}).$$

Let us again consider some examples:

1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a real 2×2 matrix. We have:

$$\begin{aligned} \det(A) &= (-1)^{1+1} a \det([A]_{1,1}) + (-1)^{1+2} b \det([A]_{1,2}) \\ &= (-1)^2 a \det([A]_{1,1}) + (-1)^3 b \det([A]_{1,2}) \\ &= a \det((d)) - b \det((c)) \\ &= ad - bc. \end{aligned}$$

   You should **learn this identity by heart:**

$$\det(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc.$$

2. Let now $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ be a real 3×3 matrix. We have:

$$\begin{aligned} \det(A) &= (-1)^{1+1} a \det([A]_{1,1}) + (-1)^{1+2} b \det([A]_{1,2}) + (-1)^{1+3} c \det([A]_{1,3}) \\ &= a \det([A]_{1,1}) - b \det([A]_{1,2}) + c \det([A]_{1,3}) \\ &= a \det(\begin{pmatrix} e & f \\ h & i \end{pmatrix}) - b \det(\begin{pmatrix} d & f \\ g & i \end{pmatrix}) + c \det(\begin{pmatrix} d & e \\ g & h \end{pmatrix}) \\ &= a(ei - fh) - b(di - fg) + c(dh - eg). \end{aligned}$$

   (You should definitely **not** try to memorize this last identity!).

We state without proof the following **extremely important** result:

Theorem 33. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. We have:

- A is **invertible** if and only if $\det(A) \neq 0$.

Let us recapitulate: We now have **two distinct ways** to establish whether or not a given $n \times n$ matrix A is invertible:

1. Consider the **column vectors** $A_{;1}, A_{;2}, \cdots, A_{;n}$ of A: If they are **linearly independent** then A is **invertible**; if they are linearly dependent, then A is not invertible.
2. Compute $\det(A)$: If $\det(A) \neq 0$, then A is **invertible**; if $\det(A) = 0$, then A is not invertible.

The reader may wonder: Why not always use the first scheme to verify invertibility of a given $n \times n$ matrix ? Or why not always use the second scheme for that purpose ? What is the use of having these two schemes (which at the end give the same result) ? Well, in some cases, the first scheme may be easier to apply, and in other cases, the second. Let us illustrate this on two examples:

1. Let $A = \begin{pmatrix} -1 & 2 & 1 & -4 \\ 0 & 3 & 3 & 7 \\ 2 & 3 & 5 & -3 \\ 1 & 1 & 2 & 3 \end{pmatrix}$; The question is: **is A invertible ?** To see whether or not A is invertible, we could either:

   - Check whether or not the **column vectors** of A are linearly independent, **or**
   - compute the **determinant** $\det(A)$ of A and check whether or not it is distinct from zero.

   Well, we can immediately see that the **third column vector** of A is the **sum of the first two**; this shows that the column vectors of A are **linearly dependent**, and hence A is **not** invertible. We could have also computed $\det(A)$ and found it to be zero, but this would have been mildly tedious.

2. Let now $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$; The question is: **is A invertible ?** Here again, to answer this question, we could either check linear dependence/independence of the column vectors of A or we could compute the determinant $\det(A)$ of A. It happens that in this example computing $\det(A)$ is extremely easy, due to so many entries of A being zero. Applying the definition of the determinant, we obtain:

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

   and hence $\det(A) \neq 0$, which shows that A **is** invertible.

Now that we have seen how to use the determinant function to verify whether or not a given real $n \times n$ matrix A is invertible, let us see how we can **compute the inverse** A^{-1} of A. Before going further, we need an important definition:

Definition 34. Let $M \in \mathcal{M}_{m,n}(\mathbb{R})$ be a real $m \times n$ matrix. The **transpose** of M, denoted M^T, is the $n \times m$ real matrix defined by: $(M^T)_{i,j} = (M)_{j,i}$, for all $1 \leq i \leq n$ and $1 \leq j \leq m$, where by the notation $(C)_{a,b}$ we mean the entry of matrix C on row a and column b.

In other words, the entry of M^T on row i and column j is exactly the entry of M on row j and column i. A very simple way to remember how to construct the transpose A^T of A is as follows: The first row of A becomes the first column of A^T, the second row of A becomes the second column of A^T, ..., the last row of A becomes the last column of A^T.
Let us illustrate this on a few examples:

1. Let $A = \begin{pmatrix} 1 & 2 & -3 & 7 \\ -1 & 4 & 5 & 0 \end{pmatrix}$ be a real 2×4 matrix; its transpose A^T is the real 4×2 matrix given by
$$A^T = \begin{pmatrix} 1 & -1 \\ 2 & 4 \\ -3 & 5 \\ 7 & 0 \end{pmatrix}.$$
2. Let $A = \begin{pmatrix} 7 & 3 & -3 \\ -1 & 0 & 5 \\ 2 & 2 & 1 \end{pmatrix}$ be a real 3×3 matrix; its transpose A^T is the real 3×3 matrix given by
$$A^T = \begin{pmatrix} 7 & -1 & 2 \\ 3 & 0 & 2 \\ -3 & 5 & 1 \end{pmatrix}$$
3. Let $A = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ be a real 2×1 matrix; its transpose A^T is the real 1×2 matrix given by
$$A^T = \begin{pmatrix} 1 & 2 \end{pmatrix}.$$

Remark 8. Clearly, if A is a square matrix, then its transpose A^T is again a square matrix of the same size; i.e. if $A \in \mathcal{M}_n(\mathbb{R})$ then $A^T \in \mathcal{M}_n(\mathbb{R})$.

We are now ready to compute the inverse A^{-1} of an invertible matrix $A \in \mathcal{M}_n(\mathbb{R})$:

Theorem 34. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. Assume A is **invertible**. Then, the inverse A^{-1} of A is given by:
$$A^{-1} = \frac{1}{\det(A)} C^T,$$

where the matrix $C \in \mathcal{M}_n(\mathbb{R})$ is defined as follows: The entry $(C)_{i,j}$ of C on row i and column j is given by:

$$(C)_{i,j} = (-1)^{i+j} \det([A]_{i,j}),$$

and where (recall!) $[A]_{i,j}$ is the $(n-1) \times (n-1)$ matrix obtained from A by removing row i and column j.

Let us apply this result to compute the inverse of an invertible 2×2 matrix: Let then

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an **invertible** 2×2 matrix, i.e. such that $\det(A) \neq 0$, i.e. such that $ad - bc \neq 0$. Applying the previous result to compute the inverse A^{-1} of A, we obtain:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Let us verify that we indeed have $A^{-1}A = AA^{-1} = I$ (I being the 2×2 identity matrix); we have:

$$\begin{aligned}
A^{-1}A &= \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
AA^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\
&= \frac{1}{ad - bc} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

We end this lecture by stating (without proof) a number of **extremely important** properties of the determinant function:

Theorem 35. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. We have:

$$\det(A) = \det(A^T).$$

In other words, the determinant of a matrix is equal to the determinant of its transpose.

Theorem 36. Let $A, B \in \mathcal{M}_n(\mathbb{R})$ be real $n \times n$ matrices. We have:

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

In other words, the determinant of a product of matrices is the product of the invidual determinants.

It follows from this last theorem that if $A \in \mathcal{M}_n(\mathbb{R})$ is **invertible**, then $\det(A^{-1}) = \frac{1}{\det(A)}$, i.e. the determinant of the inverse is the inverse of the determinant. Indeed, since we have $AA^{-1} = I$ (where I is the $n \times n$ identity matrix), we obtain $\det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(I)$, and since we have already computed that $\det(I) = 1$, we obtain $\det(A)\det(A^{-1}) = 1$, from which it follows that $\det(A^{-1}) = \frac{1}{\det(A)}$.

Theorem 37. Let $A \in \mathcal{M}_n(\mathbb{R})$. We have, $\forall i \in \{1, 2, \cdots, n\}$:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det([A]_{i,j}),$$

and $\forall j \in \{1, 2, \cdots, n\}$:

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det([A]_{i,j}),$$

where $a_{i,j}$ denotes the entry of A on row i and column j, and (as before) $[A]_{i,j}$ denotes the $(n-1) \times (n-1)$ matrix obtained from A by removing row i and column j.

Remark 9. Note that the definition we gave for $\det(A)$ corresponds to the first formula above for $i = 1$, i.e. "expansion along the first row of A". What the first formula in the above theorem says is that we can compute $\det(A)$ by "expanding along any row of A" (not just the first one), and the second formula says that we can compute $\det(A)$ by "expanding along any column of A".

The previous result together with the previous remark lead us to the following observation: Since we can compute $\det(A)$ by expanding along any row or column of A that we please, we may as well choose the row or column of A having the most number of zero entries. We illustrate this idea on a few examples:

1. Let $A \in \mathcal{M}_n(\mathbb{R})$ be given by

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix};$$

such a matrix is called **lower triangular** (since all the entries above the diagonal are zero). Let us compute $\det(A)$. In line with the preceding observation, it is to our advantage to expand along the row or column of A having the most number of zero entries. Let us then compute $\det(A)$ by expanding along the first row of A. Since the only possibly non-zero entry on the first row of A is $a_{1,1}$, we obtain, upon applying the formula for the determinant:

$$\det(A) = a_{1,1} \det \begin{pmatrix} a_{2,2} & 0 & \cdots & 0 \\ a_{3,2} & a_{3,3} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,2} & a_{n,3} & \cdots & a_{n,n} \end{pmatrix},$$

and again computing this new determinant by row expansion along the first row yields:

$$\det(A) = a_{1,1}a_{2,2} \det \begin{pmatrix} a_{3,3} & 0 & \cdots & 0 \\ a_{4,3} & a_{4,4} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,3} & a_{n,4} & \cdots & a_{n,n} \end{pmatrix},$$

and iterating this procedure yields:

$$\det(A) = a_{1,1}a_{2,2}a_{3,3}\cdots a_{n,n},$$

i.e., in other words, the determinant of a **lower triangular** matrix A is the **product of the diagonal entries** of A.

2. Let now $A \in \mathcal{M}_n(\mathbb{R})$ be given by

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix};$$

such a matrix is called **upper triangular** (since all the entries below the diagonal are zero). Note that for this particular matrix, it would be most advantageous to compute the determinant by expanding along the first column. Note also that we can use our previous computation for lower triangular matrices to compute $\det(A)$. Indeed, note that the transpose A^T of matrix A is lower-triangular, and hence $\det(A^T)$ is the product of the diagonal entries of A^T. We have also seen that transposing a matrix does not change its determinant, i.e. $\det(A^T) = \det(A)$. Putting all this together, we obtain:

$$\det(A) = \det(A^T) = \det \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{1,2} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,n} & a_{2,n} & \cdots & a_{n,n} \end{pmatrix} = a_{1,1}a_{2,2}a_{3,3}\cdots a_{n,n},$$

i.e., in other words, the determinant of an **upper triangular** matrix A is also the **product of the diagonal entries** of A.

3. Let now $A \in \mathcal{M}_n(\mathbb{R})$ be given by

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & a_{2,2} & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix};$$

such a matrix is called **diagonal** (since all the entries outside the diagonal are zero). Note that a diagonal matrix is both upper- and lower-triangular. Hence, applying our previous results, we obtain:

$$\det(A) = a_{1,1}a_{2,2}a_{3,3}\cdots a_{n,n},$$

i.e., in other words, the determinant of an **diagonal** matrix A is also the **product of the diagonal entries** of A.

Let now $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix, and let us write A as

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

where $A_{;j}$ denotes the j^{th} column vector of A. If we now multiply the j^{th} column vector of A by some real number α (but only the j^{th} column vector of A), we obtain the matrix

$$\begin{pmatrix} A_{;1} & \cdots & \alpha A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

which has exactly the same column vectors as A **except** for the j^{th} one (which has been multiplied by α. The following theorem indicates how the determinants of those matrices are related:

Theorem 38. For any $\alpha \in \mathbb{R}$, we have:

$$\det(\begin{pmatrix} A_{;1} & \cdots & \alpha A_{;j} & \cdots & A_{;n} \end{pmatrix}) = \alpha \det(\begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix}).$$

Let now $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix, and let $\alpha \in \mathbb{R}$; recall that αA is the matrix obtained by multiplying each entry of A by α. How is $\det(\alpha A)$ related to $\det(A)$? The following theorem answers this question:

Theorem 39. $\forall A \in \mathcal{M}_n(\mathbb{R})$, $\forall \alpha \in \mathbb{R}$, we have:

$$\det(\alpha A) = \alpha^n \det(A).$$

Proof. Writing A in terms of its column vectors as

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

we obtain:

$$\alpha A = \begin{pmatrix} \alpha A_{;1} & \cdots & \alpha A_{;j} & \cdots & \alpha A_{;n} \end{pmatrix},$$

and it follows from the previous theorem that

$$\begin{aligned}\det(\alpha A) &= \det(\begin{pmatrix} \alpha A_{;1} & \cdots & \alpha A_{;j} & \cdots & \alpha A_{;n} \end{pmatrix}) \\ &= \alpha^n \det(\begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix}) \\ &= \alpha^n \det(A).\end{aligned}$$

□

Remark 10. Note that it follows from the previous theorem that for any $A \in \mathcal{M}_n(\mathbb{R})$, we have:

$$\det(-A) = (-1)^n \det(A).$$

Let now $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix, which we write again in terms of its column vectors as

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;i} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

where again $A_{;i}$ denotes the i^{th} column vector of A and $A_{;j}$ its j^{th} column vector; what happens to the determinant if we interchange these two column vectors, i.e. how is the determinant of the matrix

$$\begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;i} & \cdots & A_{;n} \end{pmatrix},$$

(which is obtained from A by interchanging column vectors i and j) related to the determinant of the matrix

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;i} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix}?$$

The answer is given in the following theorem:

Theorem 40. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix given (in terms of its column vectors) by

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;i} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

and let $\tilde{A}$ be the real $n \times n$ matrix obtained from A by interchanging column vectors i and j (where $i \neq j$), i.e.,

$$\tilde{A} = \begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;i} & \cdots & A_{;n} \end{pmatrix}.$$

Then:

$$\det(\tilde{A}) = -\det(A);$$

in other words, interchanging two distinct column vectors changes the sign of the determinant.

Let now $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix given (again in terms of its column vectors) by

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

and let $\mathbf{v} \in \widehat{\mathbb{R}^n}$ be a column vector; let us add $\mathbf{v}$ to the j^{th} column vector of A (and only to that column vector); we obtain the $n \times n$ matrix

$$\begin{pmatrix} A_{;1} & \cdots & A_{;j} + \mathbf{v} & \cdots & A_{;n} \end{pmatrix}$$

which differs from A only in the j^{th} column vector. How is the determinant of this last matrix related to the determinant of A ?

Theorem 41. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix given in terms of its column vectors by

$$A = \begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix},$$

and let $\mathbf{v} \in \widehat{\mathbb{R}^n}$ be a column vector; consider the matrix obtained from A by adding $\mathbf{v}$ to the j^{th} column vector of A, i.e. the matrix

$$\begin{pmatrix} A_{;1} & \cdots & A_{;j} + \mathbf{v} & \cdots & A_{;n} \end{pmatrix},$$

and let

$$\begin{pmatrix} A_{;1} & \cdots & \mathbf{v} & \cdots & A_{;n} \end{pmatrix},$$

be the matrix obtained by **replacing** the j^{th} column vector of A by $\mathbf{v}$ (and keeping all other column vectors the same as those of A). We have:

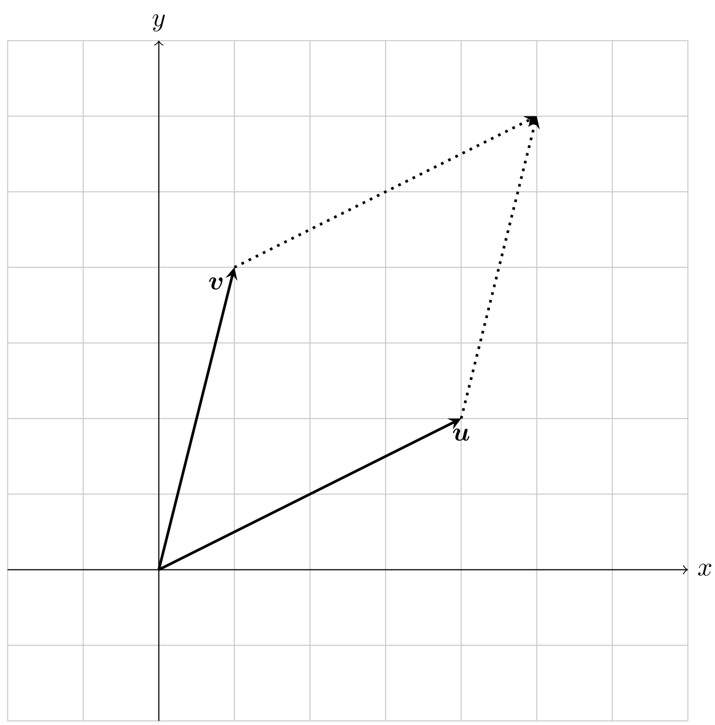
$$\begin{aligned} \det(\begin{pmatrix} A_{;1} & \cdots & A_{;j} + \mathbf{v} & \cdots & A_{;n} \end{pmatrix}) &= \det(\begin{pmatrix} A_{;1} & \cdots & A_{;j} & \cdots & A_{;n} \end{pmatrix}) \\ &+ \det(\begin{pmatrix} A_{;1} & \cdots & \mathbf{v} & \cdots & A_{;n} \end{pmatrix}). \end{aligned}$$

Where does the expression for the determinant come from ?

At this point, we have every right to ask ourselves: **Where does the formula for the determinant come from** ? i.e., in other words, **why is the determinant defined the way it is** ? As we shall see, the answer is very simple. For simplicity, we first treat the case of the determinant of 2×2 matrices; we will discuss the general case afterwards.

So we can ask the question: Why is $\det(\begin{pmatrix} a & b \\ c & d \end{pmatrix})$ defined to be $ad - bc$? To answer this question, we consider the following problem: Suppose we endow the plane with a Cartesian coordinate system, and suppose we **represent** geometrically a vector $\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix}$ of $\widehat{\mathbb{R}^2}$ by a oriented line segment joining an arbitrary point of the plane, say with coordinates (p, q), to the point with coordinates $(p+a, q+b)$. Note that the oriented line segmented joining the point with coordinates (x, y) to the point with coordinates $(x+a, y+b)$ would then represent the same vector as the oriented line segmented joining the point with coordinates (x', y') to the point with coordinates $(x'+a, y'+b)$.

Let us now give ourselves two vectors $\mathbf{u}, \mathbf{v}$ in $\widehat{\mathbb{R}^2}$, and let us represent them geometrically as oriented line segments starting from the origin of our Cartesian coordinate system. Suppose we now pose ourselves the following problem: **How can we determine the area of the parallelogram spanned by $\mathbf{u}, \mathbf{v}$?** (see diagram below)



For this purpose, let us begin by **formalizing the problem**: Let us then **define a function** $A : \widehat{\mathbb{R}^2} \times \widehat{\mathbb{R}^2} \to \mathbb{R}$ (the "area function"!), and let's see what properties it must have. For any two elements $\mathbf{u}, \mathbf{v}$ of $\widehat{\mathbb{R}^2}$, $A(\mathbf{u}, \mathbf{v})$ would then be the area of the parallelogram spanned by $\mathbf{u}, \mathbf{v}$ (or, rather, their geometric representations as oriented line segments starting at the origin). So let us see what properties A must satisfy. Let us first decide that the area of the parallelogram spanned by the vectors $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ should be equal to some strictly positive real number, i.e. $A(\mathbf{e}_1, \mathbf{e}_2) > 0$. Choosing a value for $A(\mathbf{e}_1, \mathbf{e}_2)$ only amounts to choosing a unit for our area; we could choose 1, for simplicity, but we don't have to.

1. Suppose first that $\mathbf{u}$ in any element of $\widehat{\mathbb{R}^2}$; clearly, the area of the parallelogram spanned by $\mathbf{u}$ and $\mathbf{u}$ is zero (the parallelogram is "flat"). Hence, we should have $A(\mathbf{u}, \mathbf{u}) = 0$ for any $\mathbf{u} \in \widehat{\mathbb{R}^2}$.

2. Suppose now that $\mathbf{u}, \mathbf{v}$ are two elements of $\widehat{\mathbb{R}^2}$, and that the parallelogram they span has area $A(\mathbf{u}, \mathbf{v})$. It is clear (from geometrical considerations), that if we scale $\mathbf{u}$ by any positive real number α, then the area of the spanned parallelogram will scale accordingly, i.e. $A(\alpha\mathbf{u}, \mathbf{v}) = \alpha A(\mathbf{u}, \mathbf{v})$. For consistency, we assume this holds for negative α as well (this is why we defined A as a mapping to $\mathbb{R}$ and not just to $\mathbb{R}^+$, to allow it to take negative as well as positive values). Similarly, if we scale $\mathbf{v}$ by α, then the area of the spanned parallelogram will scale accordingly, i.e. $A(\mathbf{u}, \alpha\mathbf{v}) = \alpha A(\mathbf{u}, \mathbf{v})$.

   Let us recapitulate our findings so far: If the mapping $A : \widehat{\mathbb{R}^2} \times \widehat{\mathbb{R}^2} \to \mathbb{R}$ is such that for any $\mathbf{u}, \mathbf{v} \in \widehat{\mathbb{R}^2}$ $A(\mathbf{u}, \mathbf{v})$ be the area of the parallelogram spanned by $\mathbf{u}, \mathbf{v}$, then we must have, $\forall \alpha \in \mathbb{R}$, $\forall \mathbf{u}, \mathbf{v} \in \widehat{\mathbb{R}^2}$:

   $$A(\alpha\mathbf{u}, \mathbf{v}) = \alpha A(\mathbf{u}, \mathbf{v}), \quad \text{and} \quad A(\mathbf{u}, \alpha\mathbf{v}) = \alpha A(\mathbf{u}, \mathbf{v}).$$

3. Let now $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}$ be any three vectors in $\widehat{\mathbb{R}^2}$, and let us consider the area $A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v})$ of the parallelogram spanned by the vectors $\mathbf{u}_1 + \mathbf{u}_2$ and $\mathbf{v}$. How is this area related to the areas of the parallelograms spanned by $\mathbf{u}_1, \mathbf{v}$ and $\mathbf{u}_2, \mathbf{v}$, respectively ? In other words, how is $A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v})$ related to $A(\mathbf{u}_1, \mathbf{v})$ and $A(\mathbf{u}_2, \mathbf{v})$? Carefully drawing these vectors and examining the areas of the parallelograms formed will allow one to reach the conclusion that $A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v})$ is nothing other than the sum of $A(\mathbf{u}_1, \mathbf{v})$ and $A(\mathbf{u}_2, \mathbf{v})$, i.e. we have

   $$A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}) = A(\mathbf{u}_1, \mathbf{v}) + A(\mathbf{u}_2, \mathbf{v}).$$

   Similarly, if we now take arbitrary vectors $\mathbf{u}, \mathbf{v}_1, \mathbf{v}_2$ in $\widehat{\mathbb{R}^2}$ and examine the area of the parallelogram spanned by the vectors $\mathbf{u}$ and $\mathbf{v}_1 + \mathbf{v}_2$, we will discover that this area is nothing other than the sum of the areas of the parallelograms spanned by $\mathbf{u}, \mathbf{v}_1$ and $\mathbf{u}, \mathbf{v}_2$, respectively. In other words, we have also

   $$A(\mathbf{u}, \mathbf{v}_1 + \mathbf{v}_2) = A(\mathbf{u}, \mathbf{v}_1) + A(\mathbf{u}, \mathbf{v}_2).$$

Let us recapitulate our findings so far: If $A(\mathbf{u}, \mathbf{v})$ is to be equal to the area of the parallelogram spanned by $\mathbf{u}$ and $\mathbf{v}$, then **we must have**, for all $\mathbf{u}, \mathbf{v}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2 \in \widehat{\mathbb{R}^2}$, and for all $\alpha \in \mathbb{R}$:

1. $A(\mathbf{u}, \mathbf{u}) = 0$,

2. $A(\alpha\mathbf{u}, \mathbf{v}) = \alpha A(\mathbf{u}, \mathbf{v})$,
3. $A(\mathbf{u}, \alpha\mathbf{v}) = \alpha A(\mathbf{u}, \mathbf{v})$,
4. $A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}) = A(\mathbf{u}_1, \mathbf{v}) + A(\mathbf{u}_2, \mathbf{v})$,
5. $A(\mathbf{u}, \mathbf{v}_1 + \mathbf{v}_2) = A(\mathbf{u}, \mathbf{v}_1) + A(\mathbf{u}, \mathbf{v}_2)$.

Note that it follows from the above that for any $\mathbf{u}_1, \mathbf{u}_2 \in \widehat{\mathbb{R}^2}$, $A(\mathbf{u}_2, \mathbf{u}_1) = -A(\mathbf{u}_1, \mathbf{u}_2)$ (i.e. switching the two entries changes the sign), since we have:

$$\begin{aligned} 0 &= A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_1 + \mathbf{u}_2) \\ &= A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_1) + A(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_2) \\ &= A(\mathbf{u}_1, \mathbf{u}_1) + A(\mathbf{u}_2, \mathbf{u}_1) + A(\mathbf{u}_1, \mathbf{u}_2) + A(\mathbf{u}_2, \mathbf{u}_2) \\ &= A(\mathbf{u}_2, \mathbf{u}_1) + A(\mathbf{u}_1, \mathbf{u}_2), \end{aligned}$$

and hence,

$$A(\mathbf{u}_2, \mathbf{u}_1) = -A(\mathbf{u}_1, \mathbf{u}_2).$$

We can summarize the properties of A by saying that A is a **bilinear alternating form** on $\widehat{\mathbb{R}^2}$.

Consider now the real 2×2 matrix M given by $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and consider the vectors $M\mathbf{e}_1$ and $M\mathbf{e}_2$ (recall that $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$). What is the area of the parallelogram spanned by $M\mathbf{e}_1$ and $M\mathbf{e}_2$? A quick calculation shows that we have:

$$M\mathbf{e}_1 = \begin{pmatrix} a \\ c \end{pmatrix}, \quad M\mathbf{e}_2 = \begin{pmatrix} b \\ d \end{pmatrix}$$

which we can re-express (using the definition of $\mathbf{e}_1, \mathbf{e}_2$ as:

$$\begin{aligned} M\mathbf{e}_1 &= a\mathbf{e}_1 + c\mathbf{e}_2 \\ M\mathbf{e}_2 &= b\mathbf{e}_1 + d\mathbf{e}_2 \end{aligned}$$

The area of the parallelogram spanned by $M\mathbf{e}_1, M\mathbf{e}_2$, is therefore given by (using the properties of A):

$$\begin{aligned} A(M\mathbf{e}_1, M\mathbf{e}_2) &= A(a\mathbf{e}_1 + c\mathbf{e}_2, b\mathbf{e}_1 + d\mathbf{e}_2) \\ &= A(a\mathbf{e}_1 + c\mathbf{e}_2, b\mathbf{e}_1) + A(a\mathbf{e}_1 + c\mathbf{e}_2, d\mathbf{e}_2) \\ &= A(a\mathbf{e}_1, b\mathbf{e}_1) + A(c\mathbf{e}_2, b\mathbf{e}_1) + A(a\mathbf{e}_1, d\mathbf{e}_2) + A(c\mathbf{e}_2, d\mathbf{e}_2) \\ &= aA(\mathbf{e}_1, b\mathbf{e}_1) + cA(\mathbf{e}_2, b\mathbf{e}_1) + aA(\mathbf{e}_1, d\mathbf{e}_2) + cA(\mathbf{e}_2, d\mathbf{e}_2) \\ &= abA(\mathbf{e}_1, \mathbf{e}_1) + bcA(\mathbf{e}_2, \mathbf{e}_1) + adA(\mathbf{e}_1, \mathbf{e}_2) + cdA(\mathbf{e}_2, \mathbf{e}_2) \\ &= -bcA(\mathbf{e}_1, \mathbf{e}_2) + adA(\mathbf{e}_1, \mathbf{e}_2) \\ &= (ad - bc)A(\mathbf{e}_1, \mathbf{e}_2) \\ &= \det(M)A(\mathbf{e}_1, \mathbf{e}_2), \end{aligned}$$

and hence, we have shown that the area $A(M\mathbf{e}_1, M\mathbf{e}_2)$ of the parallelogram spanned by $\mathbf{e}_1, \mathbf{e}_2$ is related to the area $A(\mathbf{e}_1, \mathbf{e}_2)$ of the parallelogram spanned by $\mathbf{e}_1, \mathbf{e}_2$ by a multiplicative factor which is none other than the determinant $\det(M)$ of M. With very little extra work (do it as an exercise!), it is possible to show that this relation is true not just for $\mathbf{e}_1$ and $\mathbf{e}_2$, and that for any two vectors $\mathbf{u}, \mathbf{v} \in \widehat{\mathbb{R}^2}$, we have:

$$A(M\mathbf{u}, M\mathbf{v}) = \det(M)A(\mathbf{u}, \mathbf{v}).$$

Let now M, N be two arbitrary real 2×2 matrices. Based on what we have uncovered above, we have both

$$A(MN\mathbf{e}_1, MN\mathbf{e}_2) = \det(MN)A(\mathbf{e}_1, \mathbf{e}_2),$$

and

$$A(MN\mathbf{e}_1, MN\mathbf{e}_2) = \det(M)A(N\mathbf{e}_1, N\mathbf{e}_2) = \det(M)\det(N)A(\mathbf{e}_1, \mathbf{e}_2),$$

and since $A(\mathbf{e}_1, \mathbf{e}_2)$ was assumed non-zero, we have proved the relation:

$$\det(MN) = \det(M)\det(N).$$

We can follow exactly the same steps for general $n \times n$ matrices (and not just 2×2), and define an "$n-$dimensional" volume function which would associate to every $n - tuple$ $(\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_n)$ of vectors in $\widehat{\mathbb{R}^n}$ the "volume" of the parallepiped spanned by $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_n$; proceeding as above, we would end up with a **multilinear alternating form** on $\widehat{\mathbb{R}^n}$, and we would obtain the general expression of the determinant for $n \times n$ matrices, just as we did for 2×2 matrices in detail above.

PROBLEMS:

1. For each of the following choices for the matrix A, establish whether or not A is invertible in the following two distinct ways:

   (i) Check whether or not the column vectors of A are linearly independent.

   (ii) Compute the determinant $\det(A)$ of A to see whether or not it is non-zero.

   (a) $A = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}$.

   (b) $A = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$.

   (c) $A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$.

(d) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(e) $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(f) $A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$.

(g) $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$.

(h) $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(i) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

(j) $A = \begin{pmatrix} 3 & 2 \\ 6 & 4 \end{pmatrix}$.

(k) $A = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}$.

(l) $A = \begin{pmatrix} -3 & 0 \\ 7 & 0 \end{pmatrix}$.

(m) $A = \begin{pmatrix} -1 & 2 \\ 2 & -4 \end{pmatrix}$.

(n) $A = \begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 2 \\ 3 & 3 & 3 \end{pmatrix}$.

(o) $A = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

(p) $A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 3 & 5 & 2 \end{pmatrix}$.

(q) $A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 7 & 0 \\ 3 & -3 & 0 \end{pmatrix}$.

(r) $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

(s) $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(t) $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

(u) $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

(v) $A = \begin{pmatrix} 2 & 1 & 3 \\ 7 & -1 & -1 \\ 5 & -2 & 2 \end{pmatrix}$.

(w) $A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 3 \\ -1 & 5 & 4 \end{pmatrix}$.

(x) $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 2 & -3 & 0 \\ 1 & 5 & -7 & -2 \end{pmatrix}$.

(y) $A = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & -1 & 1 & 2 \\ 0 & -2 & 2 & 3 \\ 1 & 0 & 0 & -1 \end{pmatrix}$.

(z) $A = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & -2 & 5 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 1 & -1 & -1 \end{pmatrix}$.

2. The following problems involve the design of scrambling and unscrambling matrices for secure message communication (see Section 13 for more details on this topic; the example matrices given there should not be used). In the problems that follow, the matrices of similar dimension should be distinct.

   (a) Design a 2×2 scrambling matrix A and a corresponding 2×2 unscrambling matrix B, and use A to scramble the following message (by considering consecutive 1×2 blocks): $\begin{pmatrix} 0 & 1 & 15 & 2 & 4 & 4 & 7 & 20 \end{pmatrix}$.

   (b) Design a 2×2 scrambling matrix A and a corresponding 2×2 unscrambling matrix B, and use A to scramble the following message (by considering consecutive 2×2 blocks): $\begin{pmatrix} 0 & 1 & 15 & 2 \\ 4 & 4 & 7 & 20 \end{pmatrix}$.

   (c) Design a 3×3 scrambling matrix A and a corresponding 3×3 unscrambling matrix B, and use A to scramble the following message (by considering consecutive 1×3 blocks): $\begin{pmatrix} 7 & 2 & 9 & 18 & 13 & 23 \end{pmatrix}$.

   (d) Design a 3×3 scrambling matrix A and a corresponding 3×3 unscrambling matrix B, and use A to scramble the following message (by considering a 2×3 block): $\begin{pmatrix} 7 & 2 & 9 \\ 18 & 13 & 23 \end{pmatrix}$.

   (e) Design a 4×4 scrambling matrix A and a corresponding 4×4 unscrambling matrix B, and use A to scramble the following message (by considering consecutive 1×4 blocks): $\begin{pmatrix} 0 & 1 & 15 & 2 & 4 & 4 & 7 & 20 \end{pmatrix}$.

(f) Design a 4×4 scrambling matrix A and a corresponding 4×4 unscrambling matrix B, and use A to scramble the following message (by considering a 2×4 block): $\begin{pmatrix} 0 & 1 & 15 & 2 \\ 4 & 4 & 7 & 20 \end{pmatrix}$.

Section 15

Study Topics

- Eigenvalues and eigenvectors of an endomorphism
- Eigenvalues and eigenvectors of a square matrix

Let $\mathbf{V}$ be a real vector space, and let $L : \mathbf{V} \to \mathbf{V}$ be a **linear** transformation (note here that L maps from $\mathbf{V}$ back to $\mathbf{V}$ and not to some other vector space; a linear mapping from a vector space back to itself is also called an **endomorphism**). We have the following important definition:

Definition 35. Let $\mathbf{v} \in \mathbf{V}$ with $\mathbf{v} \neq \mathbf{0}$ (i.e. $\mathbf{v}$ is not the zero vector of $\mathbf{V}$); $\mathbf{v}$ is said to be an **eigenvector** of the linear transformation L if there exists a **real** number λ such that:

$$L(\mathbf{v}) = \lambda \mathbf{v}.$$

The real number λ in the above relation is called an **eigenvalue** of L.
We then say that $\mathbf{v}$ is **an** eigenvector of L **associated to the eigenvalue** λ.

Let us note the following **key points** before going further:

1. L is a mapping from $\mathbf{V}$ to $\mathbf{V}$, and not from $\mathbf{V}$ to some other vector space $\mathbf{W}$.
2. An eigenvector a of linear transformation $L : \mathbf{V} \to \mathbf{V}$ is **by definition** a vector other than the zero vector $\mathbf{0}$ of $\mathbf{V}$; hence, even though $L(\mathbf{0}) = \mathbf{0} = \lambda\mathbf{0}$, $\mathbf{0}$ is **not** considered to be an eigenvector of L.
3. For a real number $\lambda \in \mathbb{R}$ to be an **eigenvalue** of L, there **must** exist a **non-zero** vector $\mathbf{v} \in \mathbf{V}$ such that $L(\mathbf{v}) = \lambda \mathbf{v}$; if no such vector exists, λ cannot be an eigenvalue of L.

Let us now consider a number of examples:

1. Let $\mathbf{V}$ be a real vector space, and let $\alpha \in \mathbb{R}$ be a real number. Let $L : \mathbf{V} \to \mathbf{V}$ be the mapping defined by $L(\mathbf{v}) = \alpha \mathbf{v}$, $\forall \mathbf{v} \in \mathbf{V}$. It is easy to verify that L is a **linear** mapping. Furthermore (by definition of L), for any $\mathbf{v} \in \mathbf{V}$ with $\mathbf{v} \neq \mathbf{0}$, we have:

   $$L(\mathbf{v}) = \alpha \mathbf{v},$$

   which shows that $\mathbf{v}$ is an **eigenvector** of L associated to the **eigenvalue** α. Hence, for the linear mapping L of this example, **any** non-zero vector in $\mathbf{V}$ is an **eigenvector** of L (associated to the **eigenvalue** α).

2. Let $C^\infty(\mathbb{R}; \mathbb{R})$ denote the real vector space of all functions $f : \mathbb{R} \to \mathbb{R}$ which are differentiable of any order (i.e. f can be differentiated as many times as we want). Let $L : C^\infty(\mathbb{R}; \mathbb{R}) \to C^\infty(\mathbb{R}; \mathbb{R})$ be the mapping defined by:

   $$L(f) = f',$$

   where f' denotes the **first derivative** of f. It is easy to verify that L is a **linear** mapping. Let us try to find an **eigenvector** of L. Let $\alpha \in \mathbb{R}$ be a real number, and let $f \in C^\infty(\mathbb{R}; \mathbb{R})$ be defined by:

   $$f(t) = e^{\alpha t}, \quad \forall t \in \mathbb{R}.$$

Let us compute $L(f)$. We have, $\forall t \in \mathbb{R}$:

$$(L(f))(t) = \frac{d}{dt}(e^{\alpha t}) = \alpha e^{\alpha t} = \alpha f(t) = (\alpha f)(t),$$

which shows that

$$L(f) = \alpha f.$$

Since f is **not the zero vector** of $C^\infty(\mathbb{R};\mathbb{R})$, and since $L(f) = \alpha f$, we conclude that f is an **eigenvector** of L associated to the **eigenvalue** α.

3. Let $L : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $L((x, y)) = (2x, 3y)$ for all $(x, y) \in \mathbb{R}^2$. It is easy to verify that L is **linear**. Let now $\mathbf{v}_1 \in \mathbb{R}^2$ be defined by $\mathbf{v}_1 = (1, 0)$. Clearly $\mathbf{v}_1$ is **not** equal to the zero vector $(0, 0)$ of $\mathbb{R}^2$. Furthermore,

$$L(\mathbf{v}_1) = L((1, 0)) = (2, 0) = 2(1, 0) = 2\mathbf{v}_1,$$

which shows that $\mathbf{v}_1$ is an **eigenvector** of L associated to the **eigenvalue** 2.

Let now $\mathbf{v}_2 \in \mathbb{R}^2$ be defined by $\mathbf{v}_2 = (0, 1)$. Clearly $\mathbf{v}_2$ is **not** equal to the zero vector $(0, 0)$ of $\mathbb{R}^2$. Furthermore,

$$L(\mathbf{v}_2) = L((0, 1)) = (0, 3) = 3(0, 1) = 3\mathbf{v}_2,$$

which shows that $\mathbf{v}_2$ is an **eigenvector** of L associated to the **eigenvalue** 3.

Let now $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix (note that A is a **square** matrix), and consider the linear mapping $L_A : \widehat{\mathbb{R}^n} \to \widehat{\mathbb{R}^n}$ defined by A; Note that L_A maps from $\widehat{\mathbb{R}^n}$ back to itself (this is why we chose A to be a square matrix!), and as a result, we can try to find eigenvectors and eigenvalues of L_A.

- **NOTE:** We will just say "eigenvalue (resp. eigenvector) of A" instead of "eigenvalue (resp. eigenvector) of L_A".

Let then $\lambda \in \mathbb{R}$; **Assume** λ is an **eigenvalue** of A. This means that there **must** exist a **non-zero** vector $\mathbf{v} \in \widehat{\mathbb{R}^n}$ such that

$$L_A(\mathbf{v}) = \lambda \mathbf{v},$$

i.e. (using matrix notation) such that

$$A\mathbf{v} = \lambda \mathbf{v}.$$

This in turn implies that

$$\lambda \mathbf{v} - A\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}},$$

i.e., that

$$(\lambda I - A)\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}},$$

where I denotes the $n \times n$ identity matrix. But then, this last equality means nothing other than that $\mathbf{v}$ is in the **kernel** $\ker(\lambda I - A)$ of the matrix $\lambda I - A$. Since $\mathbf{v}$ is assumed to be distinct from the zero vector of $\widehat{\mathbb{R}^n}$ and since it lies in the kernel $\ker(\lambda I - A)$ of $\lambda I - A$, it follows that $\ker(\lambda I - A)$ must contain more than just the zero vector of $\widehat{\mathbb{R}^n}$! But then this means that $\lambda I - A$ is **not invertible** (otherwise $\ker(\lambda I - A)$ would have contained only the zero vector of $\widehat{\mathbb{R}^n}$), i.e. that $\det(\lambda I - A) = 0$!
Conversely, assume the real number $\lambda \in \mathbb{R}$ is such that $\det(\lambda I - A) = 0$; this then implies that the kernel $\ker(\lambda I - A)$ of the matrix $\lambda I - A$ is **not** equal to $\{\mathbf{0}_{\widehat{\mathbb{R}^n}}\}$, i.e. there does exist a vector $\mathbf{v} \neq \mathbf{0}_{\widehat{\mathbb{R}^n}}$ in $\ker(\lambda I - A)$; in other words, we have both $\mathbf{v} \neq \mathbf{0}_{\widehat{\mathbb{R}^n}}$ **and** $(\lambda I - A)\mathbf{v} = \mathbf{0}_{\widehat{\mathbb{R}^n}}$, and this last equality implies $A\mathbf{v} = \lambda\mathbf{v}$.
To recapitulate: We have shown that if $\lambda \in \mathbb{R}$ is such that $\det(\lambda I - A) = 0$, then there exists a $\mathbf{v} \in \widehat{\mathbb{R}^n}$ such that $\mathbf{v} \neq \mathbf{0}_{\widehat{\mathbb{R}^n}}$ **and** $A\mathbf{v} = \lambda\mathbf{v}$; this shows that λ is an **eigenvalue** of A.
We have therefore proved the following **important** theorem:

Theorem 42. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. Let $\lambda \in \mathbb{R}$. We have:

- λ is an **eigenvalue** of A **if and only if** $\det(\lambda I - A) = 0$ (where again I denotes the $n \times n$ identity matrix).

The importance of this theorem lies in that it will provide us a systematic way to compute the eigenvalues of any $n \times n$ matrix. This theorem has the following useful corollary:

Theorem 43. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. Then 0 is an eigenvalue of A if and only if A is **not** invertible.

Proof. 0 being an eigenvalue of A is equivalent (by the last theorem) to $\det(0I - A) = 0$, i.e. to $\det(-A) = 0$, i.e. to $(-1)^n \det(A) = 0$, i.e to $\det(A) = 0$, which itself is equivalent to A being not invertible (by what we saw in the last lecture). □

Let now $A \in \mathcal{M}_n(\mathbb{R})$ be given by

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}.$$

We can then write, $\forall \lambda \in \mathbb{R}$:

$$\det(\lambda I - A) = \det \begin{pmatrix} \lambda - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & \lambda - a_{2,2} & \cdots & -a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ -a_{n,1} & -a_{n,2} & \cdots & \lambda - a_{n,n} \end{pmatrix}.$$

An **explicit computation** of this last determinant yields that $\det(\lambda I - A)$ has the form:

$$\det(\lambda I - A) = \lambda^n + c_{n-1}\lambda^{n-1} + c_{n-2}\lambda^{n-2} + \cdots + c_2\lambda^2 + c_1\lambda + c_0,$$

where the real numbers $c_0, c_1, \cdots, c_{n-2}, c_{n-1}$ are determined by the entries of matrix A (i.e. by the $a_{i,j}$).
It is important to note the following **key points**:

1. For any real $n \times n$ matrix A, $\det(\lambda I - A)$ is a **polynomial of degree** n in λ,

2. the coefficients of the polynomial $\det(\lambda I - A)$ are determined by the entries of matrix A,

3. the coefficient of the highest order term (i.e. λ^n) in the polynomial $\det(\lambda I - A)$ is always equal to 1 (we say that the polynomial $\det(\lambda I - A)$ is **monic**),

4. the **roots** of the polynomial $\det(\lambda I - A)$ are exactly the **eigenvalues** of A.

Due to the importance of the polynomial (in λ) defined by $\det(\lambda I - A)$, we give it a special name:

Definition 36. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. The polynomial of degree n in λ given by $\det(\lambda I - A)$ is called the **characteristic polynomial** of A.

Now we know **how to compute the eigenvalues** of a given matrix $A \in \mathcal{M}_n(\mathbb{R})$; all we have to do is proceed as follows:

(i) **Compute the characteristic polynomial** of A,

(ii) **Find the roots** of the characteristic polynomial of A, i.e. find all the scalars λ which satisfy $\det(\lambda I - A) = 0$; these are the eigenvalues of A.

Let us consider a few examples to illustrate the procedure highlighted above:

1. Let $A \in \mathcal{M}_2(\mathbb{R})$ be given by $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$; suppose we wish to find all the eigenvalues of A. How would we proceed ? Well, as detailed above, all we have to do is:

   (i) Compute the characteristic polynomial $\det(\lambda I - A)$ of A (where I is the 2×2 identity matrix),

   (ii) find the roots of that characteristic polynomial, i.e. all λ which satisfy $\det(\lambda I - A) = 0$.

The characteristic polynomial $\det(\lambda I - A)$ is easily computed to be:

$$\begin{aligned}\det(\lambda I - A) &= \det(\begin{pmatrix} \lambda - 2 & -1 \\ -1 & \lambda - 2 \end{pmatrix}) \\ &= (\lambda - 2)^2 - 1 \\ &= \lambda^2 - 4\lambda + 3.\end{aligned}$$

Note that this characteristic polynomial is, as expected, a monic polynomial of degree 2 (since A is 2×2).

The eigenvalues of A are given by solving the equation

$$\det(\lambda I - A) = 0,$$

i.e. by solving

$$\lambda^2 - 4\lambda + 3 = 0;$$

we immediately find that the only solutions are given by $\lambda = 1$ and $\lambda = 3$. Hence, we conclude that the set of eigenvalues of A is given by the set $\{1, 3\}$.

2. Let now $I \in \mathcal{M}_n(\mathbb{R})$ denote (as usual) the $n \times n$ **identity matrix**; let us try to find the eigenvalues of I. Again, as detailed above, all we have to do is:

   (i) Compute the characteristic polynomial $\det(\lambda I - I)$ of I,

   (ii) find the roots of that characteristic polynomial, i.e. all λ which satisfy $\det(\lambda I - I) = 0$.

   The characteristic polynomial $\det(\lambda I - I)$ of I is easily computed to be:

$$\begin{aligned}\det(\lambda I - I) &= \det((\lambda - 1)I) \\ &= (\lambda - 1)^n \det(I) \\ &= (\lambda - 1)^n,\end{aligned}$$

   since, as we have already seen, $\det(I) = 1$.

   The eigenvalues of I are given by solving the equation

$$\det(\lambda I - I) = 0,$$

   i.e. by solving

$$(\lambda - 1)^n = 0$$

   we immediately find that the only solution is given by $\lambda = 1$. Hence, we conclude that the real number 1 is the only eigenvalue of the $n \times n$ identity matrix I, i.e. the set of eigenvalues of I is given by the set $\{1\}$.

3. Let now $A \in \mathcal{M}_n(\mathbb{R})$ denote the $n \times n$ **zero matrix** (i.e. all entries of A are zero); let us try to find the eigenvalues of A. Again, as detailed above, all we have to do is:

   (i) Compute the characteristic polynomial $\det(\lambda I - A)$ of A,

   (ii) find the roots of that characteristic polynomial, i.e. all λ which satisfy $\det(\lambda I - A) = 0$.

   The characteristic polynomial $\det(\lambda I - A)$ of A is easily computed to be:

$$\begin{aligned} \det(\lambda I - A) &= \det(\lambda I) \\ &= \lambda^n \det(I) \\ &= \lambda^n. \end{aligned}$$

   The eigenvalues of A are given by solving the equation

$$\det(\lambda I - A) = 0,$$

   i.e. by solving

$$\lambda^n = 0.$$

   We immediately find that the only solution is given by $\lambda = 0$. Hence, we conclude that the real number 0 is the only eigenvalue of the $n \times n$ zero matrix A, i.e. the set of eigenvalues of A is given by the set $\{0\}$.

4. Let now $A \in \mathcal{M}_3(\mathbb{R})$ be given by $A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$ for some real numbers a, b, c, d, e, f; again, suppose we wish to find all the eigenvalues of A. Again, as detailed above, all we have to do is:

   (i) Compute the characteristic polynomial $\det(\lambda I - A)$ of A (where I is the 3×3 identity matrix),

   (ii) find the roots of that characteristic polynomial, i.e. all λ which satisfy $\det(\lambda I - A) = 0$.

   The characteristic polynomial $\det(\lambda I - A)$ is easily computed to be:

$$\begin{aligned} \det(\lambda I - A) &= \det(\begin{pmatrix} \lambda - a & -b & -c \\ 0 & \lambda - d & -e \\ 0 & 0 & \lambda - f \end{pmatrix}) \\ &= (\lambda - a)(\lambda - d)(\lambda - f) \\ &= \lambda^3 - (a + d + f)\lambda^2 + (ad + af + df)\lambda - adf. \end{aligned}$$

   Note that this characteristic polynomial is, as expected, a monic polynomial of degree 3 (since A is 3×3).

The eigenvalues of A are given by solving the equation

$$\det(\lambda I - A) = 0,$$

i.e. by solving

$$(\lambda - a)(\lambda - d)(\lambda - f) = 0$$

we immediately find that the only solutions are given by $\lambda = a$ and $\lambda = d$, and $\lambda = f$. Hence, we conclude that the set of eigenvalues of A is given by the set $\{a, d, f\}$.

Remark 11. Before going further, let us consider the 2×2 real matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and let us try to compute its eigenvalues. According to the procedure outlined above, we begin by computing the characteristic polynomial $\det(\lambda I - A)$ of A (where I denotes the 2×2 identity matrix). We obtain:

$$\begin{aligned} \det(\lambda I - A) &= \det \begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} \\ &= \lambda^2 + 1. \end{aligned}$$

The eigenvalues of A are then given by all the scalars λ which satisfy

$$\det(\lambda I - A) = 0,$$

i.e. which satisfy

$$\lambda^2 + 1 = 0.$$

But **there is no real number** λ which satisfies $\lambda^2 + 1 = 0$! Hence, we can say that A has **no real eigenvalue**. On the other hand, the **complex numbers** i and $-i$ are the two solutions to the above equation (recall that $i^2 = -1$); hence we can say that this particular matrix A has only **complex eigenvalues** and **no real eigenvalue**.
In this lecture, we will restrict ourselves to $n \times n$ matrices which have **only real eigenvalues**.

Now that we have a "recipe" for computing all the eigenvalues of a given real $n \times n$ matrix A, **how do we compute** the corresponding **eigenvectors** ? We begin with a definition:

Definition 37. Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix, and let $\lambda \in \mathbb{R}$ be an **eigenvalue** of A. The vector subspace of $\widehat{\mathbb{R}^n}$ given by $\ker(\lambda I - A)$ is called the **eigenspace of A associated to the eigenvalue λ of A**.

It is important to note the following points:

(i) $\ker(\lambda I - A)$ is indeed a vector subspace of $\widehat{\mathbb{R}^n}$ (see the lecture on the Kernel of a linear mapping).

(ii) Any **non-zero** vector $\mathbf{v}$ in $\ker(\lambda I - A)$ is an **eigenvector** of A associated with eigenvalue λ; indeed, let $\mathbf{v} \in \ker(\lambda I - A)$ with $\mathbf{v} \neq \mathbf{0}$. We then have

$$(\lambda I - A)\mathbf{v} = \mathbf{0},$$

which implies

$$A\mathbf{v} = \lambda I \mathbf{v},$$

which implies

$$A\mathbf{v} = \lambda \mathbf{v},$$

and since $\mathbf{v} \neq \mathbf{0}$, this shows that $\mathbf{v}$ is an **eigenvector** of A associated with eigenvalue λ.

These observations naturally lead us to a "recipe" for computing eigenvectors of a given real $n \times n$ matrix A. How do we do it ? Well, as suggested above, we first compute all the eigenvalues of A, and then compute the eigenspace associated to each eigenvalue. Each non-zero vector in the eigenspace associated to a given eigenvalue will be an eigenvector associated to that eigenvalue.
Let us illustrate this "recipe" on an example:

1. Let $A \in \mathcal{M}_2(\mathbb{R})$ be given by $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ (as before); we have already computed all the eigenvalues of A, and we know that the set of eigenvalues of A is the set $\{1, 3\}$. Let us now compute the eigenspaces associated to each of these eigenvalues:

   The eigenspace associated to the eigenvalue 1 of A is the vector subspace of $\widehat{\mathbb{R}^2}$ given by:

   $$\ker(1I - A) = \ker(\begin{pmatrix} 1-2 & -1 \\ -1 & 1-2 \end{pmatrix}) = \ker(\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}),$$

   in other words, the **eigenspace of** A associated to eigenvalue 1 is nothing other than the **kernel of the matrix** $\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$, and we already know very well how to compute kernels of matrices! So let's do it! We have:

   $$\ker(\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}) \quad = \quad \{\begin{pmatrix} x \\ y \end{pmatrix} \in \widehat{\mathbb{R}^2} | -x - y = 0\},$$

   and therefore, $\begin{pmatrix} x \\ y \end{pmatrix} \in \ker(\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix})$ implies

   $$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -x \end{pmatrix} = x \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Let $\mathbf{v}_1 \in \widehat{\mathbb{R}^2}$ be defined by $\mathbf{v}_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. The above calculation shows that $\{\mathbf{v}_1\}$ is a **generating set** for the eigenspace of A associated with eigenvalue 1; furthermore, it is easy to verify that $\{\mathbf{v}_1\}$ is a linearly independent set. Hence, $(\mathbf{v}_1)$ is a **basis for the eigenspace** of A associated to the eigenvalue 1, and we conclude therefore that that eigenspace is one-dimensional. In particular, $\mathbf{v}_1$ itself is an **eigenvector** of A associated with eigenvalue 1. Let us verify this last claim: Clearly $\mathbf{v}_1 \neq \mathbf{0}$, and we have

$$A\mathbf{v}_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2-1 \\ 1-2 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \mathbf{v}_1 = 1\mathbf{v}_1,$$

as expected.

Let us now compute the eigenspace of A associated to the eigenvalue 3 of A. The eigenspace associated to the eigenvalue 3 of A is the vector subspace of $\widehat{\mathbb{R}^2}$ given by:

$$\ker(3I - A) = \ker(\begin{pmatrix} 3-2 & -1 \\ -1 & 3-2 \end{pmatrix}) = \ker(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}),$$

in other words, the **eigenspace of** A associated to eigenvalue 3 is nothing other than the **kernel of the matrix** $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$; again, this is something we know very well how to compute! We have:

$$\ker(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}) = \{\begin{pmatrix} x \\ y \end{pmatrix} \in \widehat{\mathbb{R}^2} | x - y = 0\},$$

and therefore, $\begin{pmatrix} x \\ y \end{pmatrix} \in \ker(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix})$ implies

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x \end{pmatrix} = x \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Let $\mathbf{v}_2 \in \widehat{\mathbb{R}^2}$ be defined by $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. The above calculation shows that $\{\mathbf{v}_2\}$ is a **generating set** for the eigenspace of A associated with eigenvalue 3; furthermore, it is easy to verify that $\{\mathbf{v}_2\}$ is a linearly independent set. Hence, $(\mathbf{v}_2)$ is a **basis for the eigenspace** of A associated to the eigenvalue 3, and we conclude therefore that that eigenspace is one-dimensional. In particular, $\mathbf{v}_2$ itself is an **eigenvector** of A associated with eigenvalue 3. Let us verify this last claim: Clearly $\mathbf{v}_2 \neq \mathbf{0}$, and we have

$$A\mathbf{v}_2 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2+1 \\ 1+2 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3\mathbf{v}_2,$$

as expected.

Let now $A \in \mathcal{M}_n(\mathbb{R})$, let $k \geq 1$ be an integer, and let us consider the k^{th} power A^k of A (i.e. $AA\cdots A$ (k times)); is there a simple relation between the eigenvalues A and those of A^k ? The answer is given by the following theorem:

Theorem 44. Let $A \in \mathcal{M}_n(\mathbb{R})$ and let λ be an eigenvalue of A. Then for any integer $k \geq 1$, λ^k is an eigenvalue of A^k.

Proof. Since by assumption λ is an eigenvalue of A, there exists $\mathbf{v} \in \widehat{\mathbb{R}^n}$, $\mathbf{v} \neq \mathbf{0}$, such that $A\mathbf{v} = \lambda\mathbf{v}$; hence:

$$A^k\mathbf{v} = (A^{k-1}A)\mathbf{v} = A^{k-1}(A\mathbf{v}) = A^{k-1}(\lambda\mathbf{v}) = \lambda(A^{k-1}\mathbf{v}),$$

(where we have used both the associativity and linearity of matrix multiplication) and upon iterating this procedure, we obtain

$$A^k\mathbf{v} = \lambda(A^{k-1}\mathbf{v}) = \lambda^2(A^{k-2}\mathbf{v}) = \lambda^3(A^{k-3}\mathbf{v}) = \cdots = \lambda^k\mathbf{v},$$

and since $\mathbf{v} \neq \mathbf{0}$, this shows that λ^k is an eigenvalue of A^k. Note in passing that we have also shown that if $\mathbf{v}$ is an eigenvector of A then $\mathbf{v}$ remains an eigenvector of A^k for any integer $k \geq 1$. $\square$

Matrix diagonalization

Let $A \in \mathcal{M}_n(\mathbb{R})$ be a real $n \times n$ matrix. Let $k \in \mathbb{N}$ be an integer ≥ 1. As we now know, the matrix power A^k (which, as we saw above is defined to be the $k-$fold product $AA\cdots A$) is not easy to compute in general, especially if n and k are large. As a concrete example, try computing A^{10}, where A is the 3×3 matrix given by

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

Consider now instead the 3×3 matrix B given by

$$B = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

As we may recall, B is said to be a **diagonal** matrix, since all the "off-diagonal" entries of B (i.e. all the entries $b_{i,j}$ with $i \neq j$) are equal to 0. It is easily seen after a quick calculation that B^2 is given by

$$B^2 = \begin{pmatrix} 2^2 & 0 & 0 \\ 0 & 3^2 & 0 \\ 0 & 0 & (-1)^2 \end{pmatrix},$$

that B^3 is given by

$$B^3 = \begin{pmatrix} 2^3 & 0 & 0 \\ 0 & 3^3 & 0 \\ 0 & 0 & (-1)^3 \end{pmatrix},$$

and so on, until B^{10}, which is given by

$$\begin{aligned} B^{10} &= \begin{pmatrix} 2^{10} & 0 & 0 \\ 0 & 3^{10} & 0 \\ 0 & 0 & (-1)^{10} \end{pmatrix} \\ &= \begin{pmatrix} 2^{10} & 0 & 0 \\ 0 & 3^{10} & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

There is no question that B^{10} was much easier to compute than A^{10}, and it was all due to the fact that B was a diagonal matrix, whereas A was not. As we have seen before (and as a very quick computation will show), for any $n \times n$ **diagonal** matrix C, i.e with C of the form

$$C = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & 0 & \cdots & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

(with $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{R}$), we have, for any integer $k \geq 1$:

$$C^k = \begin{pmatrix} \lambda_1^k & 0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2^k & 0 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3^k & 0 & \cdots & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & \lambda_n^k \end{pmatrix}.$$

We are thus very naturally led to the following question: Given a real matrix $A \in \mathcal{M}_n(\mathbb{R})$ and an integer $k \geq 1$, in order to compute A^k, can we first somehow "transform" A into a **diagonal** $n \times n$ matrix D, compute D^k (which will be easy to compute since D is diagonal), then "transform back" D^k in order to obtain A^k ? In order to make this question precise, we give the following definition:

Definition 38. Let $A \in \mathcal{M}_n(\mathbb{R})$. A is said to be **diagonalizable** if there exists an **invertible** matrix $P \in \mathcal{M}_n(\mathbb{R})$ and a **diagonal** matrix $D \in \mathcal{M}_n(\mathbb{R})$ such that $A = PDP^{-1}$.

Note that with A, P, D as in the definition above, the relation $A = PDP^{-1}$ implies (upon multiplying both sides on the left by P^{-1} and on the right by P) the relation $P^{-1}AP = D$. These two relations give precise meaning to what we stated in our motivating question as "transforming A to D" and "transforming back" from D to A.

Let us now return to our original question: Suppose we are given a matrix $A \in M_n(\mathbb{R})$ and an integer $k \geq 1$; suppose moreover that A is **diagonalizable**, and that we have been given a **diagonal** matrix $D \in \mathcal{M}_n(\mathbb{R})$ and an **invertible** matrix $P \in \mathcal{M}_n(\mathbb{R})$ such that $A = PDP^{-1}$. Recall that we then also have

$D = P^{-1}AP$. How can we make use of the diagonalizability of A to compute A^k ? Let us first start from small powers of A, i.e. A^2, A^3, etc., and let us hope we will find a general pattern.
We have, for A^2:

$$A^2 = (PDP^{-1})(PDP^{-1}) = PD(PP^{-1})DP^{-1} = PDIDP^{-1} = PD^2P^{-1},$$

where I denotes the $n \times n$ identity matrix, and where we have made use of the associativity of matrix multiplication. Hence, $A^2 = PD^2P^{-1}$. Note in passing that since D is diagonal, then so is D^2, and the relation $A^2 = PD^2P^{-1}$ shows that A^2 itself is also diagonalizable. Let us now go to A^3. Using our result for A^2, we can write:

$$A^3 = A^2A = (PD^2P^{-1})(PDP^{-1}) = PD^2(PP^{-1})DP^{-1} = PD^2IDP^{-1} = PD^2DP^{-1} = PD^3P^{-1}.$$

Continuing in this way, it is easy to see that for any integer $k \geq 1$, we have

$$A^k = PD^kP^{-1}.$$

This immediately suggests a three-step "algorithm" for computing A^k when A is **diagonalizable**:

1. Find $P \in \mathcal{M}_n(\mathbb{R})$ **invertible** and $D \in \mathcal{M}_n(\mathbb{R})$ **diagonal** such that $A = PDP^{-1}$;
2. Compute D^k;
3. Use the relation $A^k = PD^kP^{-1}$.

A very natural question at this point is: Is every real $n \times n$ matrix diagonalizable ? The answer is a a resounding NO! For example, the real 2×2 matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is **not** diagonalizable (we will see precisely why at the end of this section). So given a matrix $A \in \mathcal{M}_n(\mathbb{R})$, how can we determine whether or not A is diagonalizable ? The answer is given - very nicely and simply - by the following theorem:

Theorem 45. Let $A \in \mathcal{M}_n(\mathbb{R})$. A is diagonalizable if and only if there exists a basis $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n)$ of $\widehat{\mathbb{R}^n}$ with $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ eigenvectors of A.

In other words, if A is diagonalizable, then there exists a basis of $\widehat{\mathbb{R}^n}$ made of eigenvectors of A; conversely, if such a basis does exist, then A is diagonalizable.

Proof. Assume first that there exists a basis $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n)$ of $\widehat{\mathbb{R}^n}$, where $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ are eigenvectors of A. Note that this implies that $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ are all distinct from the zero vector of $\widehat{\mathbb{R}^n}$, and that there exist $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{R}$ (not necessarily pairwise distinct) such that

$$\begin{aligned} A\mathbf{v}_1 &= \lambda_1\mathbf{v}_1, \\ A\mathbf{v}_2 &= \lambda_2\mathbf{v}_2, \\ &\cdots \\ A\mathbf{v}_n &= \lambda_n\mathbf{v}_n, \end{aligned}$$

Let now P be the real $n \times n$ matrix with first column vector given by $\mathbf{v}_1$, second column vector given by $\mathbf{v}_2$, ..., and n^{th} column vector given by $\mathbf{v}_n$. In other words, writing P not as a table of real entries but as a row of column vectors, we have:

$$P = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \end{pmatrix}.$$

Note that since $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n)$ forms a basis of $\widehat{\mathbb{R}^n}$, the family $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ is linearly independent, i.e. the column vectors of P are linearly independent. Since P is a square matrix with linearly independent column vectors, it follows (from what we saw in Section 14) that P is **invertible**. Hence, the inverse P^{-1} of P does exist.
Let us now compute the matrix product AP. It is immediate to verify that the first column vector of AP is given by $A\mathbf{v}_1$, the second column vector of AP by $A\mathbf{v}_2$, ..., and the n^{th} column vector of AP by $A\mathbf{v}_n$. In other words, the matrix AP is given in terms of its column vectors by

$$AP = \begin{pmatrix} A\mathbf{v}_1 & A\mathbf{v}_2 & \cdots & A\mathbf{v}_n \end{pmatrix}.$$

Recalling now that $A\mathbf{v}_1 = \lambda_1\mathbf{v}_1, A\mathbf{v}_2 = \lambda_2\mathbf{v}_2, \cdots, A\mathbf{v}_n = \lambda_n\mathbf{v}_n$, we can write the matrix AP in terms of its column vectors as

$$AP = \begin{pmatrix} \lambda_1\mathbf{v}_1 & \lambda_2\mathbf{v}_2 & \cdots & \lambda_n\mathbf{v}_n \end{pmatrix}.$$

Let now $D \in \mathcal{M}_n(\mathbb{R})$ be the **diagonal** matrix given by

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & 0 & \cdots & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

It is easily verified (do it!) that the matrix product PD has first column vector $\lambda_1\mathbf{v}_1$, second column vector $\lambda_2\mathbf{v}_2$, ..., and n^{th} column vector $\lambda_n\mathbf{v}_n$. In other words, we have the relation:

$$PD = AP,$$

and multiplying both sides of the above relation on the right by the inverse P^{-1} of P, we obtain

$$(PD)P^{-1} = (AP)P^{-1},$$

and, using associativity of matrix multiplication, and the fact the $PP^{-1} = I$ (the $n \times n$ identity matrix), we obtain, upon simplification, the relation

$$A = PDP^{-1}.$$

In other words, we have found a **diagonal** matrix D and an **invertible** matrix A such that $A = PDP^{-1}$; it follows that A is **diagonalizable**.
We now prove the converse. **Assume therefore** that A is **diagonalizable**. Hence, by the very definition of what it means for A to be diagonalizable, there exists a real $n \times n$ **diagonal** matrix D and a real $n \times n$ **invertible** matrix P such that

$$A = PDP^{-1}.$$

Since D is diagonal, it is of the form

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & 0 & \cdots & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

with $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{R}$. Furthermore, since P is invertible, its column vectors form a linearly independent family of $\widehat{\mathbb{R}^n}$; since there are exactly n of them and since $\widehat{\mathbb{R}^n}$ has dimension n, it follows that the column vectors of P form a **basis** for $\widehat{\mathbb{R}^n}$. Let $\mathbf{v}_1$ be the first column vector of P, $\mathbf{v}_2$ the second column vector, ..., and finally $\mathbf{v}_n$ the n^{th} column vector of P. Hence we have that $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n)$ forms a **basis** of $\widehat{\mathbb{R}^n}$. Hence, writing P in terms of its column vectors, we have:

$$P = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \end{pmatrix}.$$

On the other hand, the relation

$$A = PDP^{-1}.$$

yields, upon multiplying both sides on the right by P (and making the necessary simplification)

$$AP = PD.$$

With the matrix P being given by its column vectors by

$$P = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \end{pmatrix},$$

a simple calculation (which we already did in the first part of the proof) shows that the matrix AP can be written using its column vectors as

$$AP = \begin{pmatrix} A\mathbf{v}_1 & A\mathbf{v}_2 & \cdots & A\mathbf{v}_n \end{pmatrix}.$$

Also, since D is the diagonal matrix with diagonal entries $\lambda_1, \lambda_2, \cdots, \lambda_n$ as indicated above, a simple calculation (which we also did in the first half of the proof) shows that PD can be written using its column vectors as:

$$PD = \begin{pmatrix} \lambda_1\mathbf{v}_1 & \lambda_2\mathbf{v}_2 & \cdots & \lambda_n\mathbf{v}_n \end{pmatrix}.$$

Hence, the relation $AP = PD$ is equivalent to the relation

$$\begin{pmatrix} A\mathbf{v}_1 & A\mathbf{v}_2 & \cdots & A\mathbf{v}_n \end{pmatrix} = \begin{pmatrix} \lambda_1\mathbf{v}_1 & \lambda_2\mathbf{v}_2 & \cdots & \lambda_n\mathbf{v}_n \end{pmatrix},$$

and for the matrix on the left to equal the matrix on the right, the first column vector of the matrix on the left has to equal the first column vector of the matrix on the right, the second column vector of the matrix on the left the second column vector of the matrix on the right, and so on. In other words, this last relation implies the relations:

$$\begin{aligned} A\mathbf{v}_1 &= \lambda_1\mathbf{v}_1, \\ A\mathbf{v}_2 &= \lambda_2\mathbf{v}_2, \\ &\cdots \\ A\mathbf{v}_n &= \lambda_n\mathbf{v}_n. \end{aligned}$$

These last relations (together with the fact that $(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n)$ was assumed to be a basis for $\widehat{\mathbb{R}^n}$ and hence none of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ is equal to the zero vector of $\widehat{\mathbb{R}^n}$) imply that $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ are eigenvectors of A (with respective eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_n$). Hence, we have found a basis of $\widehat{\mathbb{R}^n}$ made of eigenvectors of A. This completes the proof. □

Remark 12. The preceding proof reveals a very interesting fact: When A is diagonalizable, and hence can be written as PDP^{-1} with P invertible and D diagonal, the elements on the diagonal of D are none other than the **eigenvalues** of A; the order in which they appear corresponds to the order in which their corresponding eigenvectors appear in matrix P.

Consider for example the matrix $A \in \mathcal{M}_2(\mathbb{R})$ given by $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. It is easily seen that the eigenvalues of A are given by $\lambda_1 = 1$ and $\lambda_2 = 3$. Furthermore, the eigenspace $\ker(I - A)$ of A corresponding to eigenvalue 1 is $1-$dimensional, and, defining $\mathbf{v}_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, it is easily seen that $(\mathbf{v}_1)$ is a basis for $\ker(I - A)$. In particular, $\mathbf{v}_1$ is an eigenvector of A corresponding to eigenvalue 1. Similarly, the eigenspace $\ker(3I - A)$ of A corresponding to eigenvalue 3 is also $1-$dimensional, and, defining $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, it is easily seen that $(\mathbf{v}_2)$ is a basis for $\ker(3I - A)$. In particular, $\mathbf{v}_2$ is an eigenvector of A corresponding to eigenvalue 3.

It is immediate to verify that the eigenvectors $\mathbf{v}_1, \mathbf{v}_2$ of A form a generating family for $\widehat{\mathbb{R}^2}$ as well as a linearly independent family; it follows therefore that $(\mathbf{v}_1, \mathbf{v}_2)$ is a basis for $\widehat{\mathbb{R}^2}$. Hence A is diagonalizable, and indeed, we can write $A = PDP^{-1}$, with $P = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, and $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$.

Consider now instead the matrix $B \in \mathcal{M}_2(\mathbb{R})$ given by $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It is easily seen that $\lambda = 1$ is the only eigenvalue of B. Furthermore, the eigenspace $\ker(I - B)$ of B corresponding to eigenvalue 1 is $1-$dimensional, with basis $(\mathbf{v}_1)$, where $\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. B has no other eigenspace, since it has no other eigenvalue. Hence, any two eigenvectors of B will be (non-zero) scalar multiples of $\mathbf{v}_1$, and hence, linearly dependent. As a result, there is no basis of $\widehat{\mathbb{R}^2}$ made of eigenvectors of B. We conclude therefore that B is **not** diagonalizable.

Definition 39. Let $A \in \mathcal{M}_n(\mathbb{R})$, and assume A is diagonalizable. The expression **"to diagonalize A"** means **to find** $P \in \mathcal{M}_n(\mathbb{R})$ **invertible** and $D \in \mathcal{M}_n(\mathbb{R})$ **diagonal** such that $A = PDP^{-1}$.

Applications of eigenvalues and eigenvectors

The most common way to locate information on the web is to do a keyword search using a search engine such as Google^{TM}. But the web contains billions of pages, and, typically, tens of thousands of pages match the keywords searched. Yet, Google^{TM} manages to order the results of the search in a way which agrees very closely with our own notion of relative importance or relevance of the pages. How does Google^{TM} do it ? Well, for a start, search engines such as Google^{TM} constantly crawl the web, going from one link to the next, in order to inventory every single page. This is then used to set up a huge matrix (4 billion by 4 billion) that captures the links between the pages (rows and columns are indexed by the 4 billion pages, and a link from a page to another would be represented by a non-zero positive real number in the matrix entry corresponding to that row and column). The whole problem of ranking pages becomes that of finding an eigenvector of that huge matrix associated with eigenvalue 1. For a fascinating account of the mathematics behind Google^{TM}'s PageRank algorithm, the reader is strongly encouraged to read the article "The $ 25,000,000,000 Eigenvector: The Linear Algebra behind Google" by Kurt Bryan and Tanya Leise, published in SIAM Review, Volume 48, No. 6, 2006.

PROBLEMS:

1. For each of the following choices for the matrix A:

   (i) Compute the set of all eigenvalues of A.

   (ii) For each eigenvalue of A, determine a basis for the corresponding eigenspace.

   (a) $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(b) $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

(c) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(d) $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(e) $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

(f) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

(g) $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.

(h) $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.

(i) $A = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$.

(j) $A = \begin{pmatrix} 5 & 1 \\ 0 & 3 \end{pmatrix}$.

(k) $A = \begin{pmatrix} 7 & 0 \\ 0 & -2 \end{pmatrix}$.

(l) $A = \begin{pmatrix} 7 & 1 \\ 0 & -2 \end{pmatrix}$.

(m) $A = \begin{pmatrix} 7 & 0 \\ 1 & -2 \end{pmatrix}$.

(n) $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$.

(o) $A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$.

(p) $A = \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix}$.

(q) $A = \begin{pmatrix} 3 & 1 \\ 9 & 3 \end{pmatrix}$.

(r) $A = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$.

(s) $A = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}$.

(t) $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(u) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$

(v) $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$

(w) $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$

(x) $A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 7 \end{pmatrix}.$

(y) $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 7 \end{pmatrix}.$

(z) $A = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 5 & 0 \\ 0 & 0 & 7 \end{pmatrix}.$

(z1) $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 7 \end{pmatrix}.$

(z2) $A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 7 \end{pmatrix}.$

(z3) $A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}.$

(z4) $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}.$

(z5) $A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 6 \end{pmatrix}.$

(z6) $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 6 \end{pmatrix}.$

(z7) $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}$.

2. For each of the following choices for the matrix A:
   (i) Determine whether or not A is diagonalizable;
   (ii) If A is diagonalizable, find a diagonalization for it (i.e. find P invertible and D diagonal such that $A = PDP^{-1}$.

   (a) $A = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$.
   (b) $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
   (c) $A = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$.
   (d) $A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$.
   (e) $A = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}$.
   (f) $A = \begin{pmatrix} -1 & 0 \\ -1 & 2 \end{pmatrix}$.
   (g) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.
   (h) $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 1 & 3 \end{pmatrix}$.
   (i) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.
   (j) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.
   (k) $A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.
   (l) $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
   (m) $A = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$.