MTH101: Symmetry

Chetan Balwe

Contents

LECTURE 1

Solving linear equations - basic examples

We will begin by looking at a problem that should be familiar from high school mathematics - solving systems of linear equations. Suppose we have variables $X_1, \ldots, X_n$, a linear equation in these n-variables is an equation of the form

$$a_1X_1 + \ldots + a_nX_n = b$$

where $a_1, \ldots, a_n, b$ are all "constants". Generally this means that they are fixed numbers of a certain kind, the value of which is either known or assumed to be known in the context of the given problem. In this lecture, for the sake of definiteness, we will say that all our constants are in the set of real numbers, which will be denoted by $\mathbb{R}$. We will see later that all the arguments in this lecture apply even if the constants lie in the set of rational numbers (denoted by $\mathbb{Q}$) or the set of complex numbers (denoted by $\mathbb{C}$).

A system of m linear equations in n variables looks something like this:

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1 \\ a_{12}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}X_1 & + & a_{n2}X_2 & + & \cdots & + & a_{mn}X_n & = & b_m \end{array}$$

Here a_{ij} and b_i is a constant (i.e. a real number, by our current convention) for every i and j where $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$.

Given any system of equations, one typically tries to solve them by manipulating them in some way and creating new equations. For instance consider the following example:

EXAMPLE 1.1. We want to solve the equation

$$X + 2 = 5. \tag{1.1}$$

We add -2 to both sides of the equation to get the equation $X+2+(-2) = 5+(-2)$, which can be rewritten as

$$X = 3. \tag{1.2}$$

We observe that the only real number that can be substituted in place of X in equation (1.2) to get a true statement is 3. However, is it automatically clear that this is also a solution for equation (1.1)? Not quite. This is something we have to check. So we substitute 3 in the first equation and see that

$$3 + 2 = 5$$

is a true statement. □

Why did we have to check the solution by substituting 3 in place of X in equation (1.1)? Because generally when we perform some operation on an equation to create a new equation, we can only say that *the old equation implies the new equation, and not the other way around*. In other words, solutions of the first equation will necessarily be solutions of the second equation, but solutions of the second equation may not be solutions of the first equation. The following example will illustrate this problem:

EXAMPLE 1.2. Let X denote a variable. Consider the equation

$$X = 5.$$

Obviously, the only real number which may be substituted in this equation to get a true statement is 5. However, suppose we square both sides of this equation to get a new equation as follows:

$$X^2 = 25$$

Now, this solution has two solutions - 5 and -5. However, -5 is not a solution of the original equation. □

However, in some situations, we can actually deduce that the new equation is *equivalent* to the old equation. For instance:

(1) Let c be a non-zero real number. Given an equation of the form $A = B$, if we multiply both sides by c, we get the equation $cA = cB$. This new equation is equivalent to the old one since we can multiply it by $1/c$ to deduce the old equation from it.
(2) Let c be any real number. Given an equation of the form $A = B$, if we add c to both sides of this equation, we get the equation $A + c = B + c$. This new equation is equivalent to the old one since we can add $-c$ to both sides to deduce the old equation from it.

We will use this observation to deal with some easy examples in which our system consists of only one equation. To make matters even simpler in the beginning, we focus on equations in which $n = 1$, i.e. there is only one variable.

EXAMPLE 1.3. Let us solve the equation

$$3X = 5. \tag{1.3}$$

This is very easy. We multiply both sides by $1/3$ to get

$$X = 5/3. \tag{1.4}$$

Notice that *equation (1.4) is equivalent to (1.3)* because of our observations above. So it is enough to solve this new equation. It is clear that the only real number which can be substituted in place of X in equation (1.4) is $5/3$. So, this is the only solution of equation (1.3) as well. Thus, the *solution set* (i.e. the set of all solutions) for this equation is $\{5/3\}$. □

EXAMPLE 1.4. The equation $0 \cdot X = 0$ cannot be solved by the above method since we cannot multiply both sides by $1/0$ (since there is no such thing as $1/0$). But we see at once that *any* number can be substituted for X in this equation to get a true statement. Thus, the solution set of this equation is $\mathbb{R}$. □

EXAMPLE 1.5. The equation $0 \cdot X = 2$ also cannot be solved by the method in Example 1.3, but this time it is easy to see that this equation has *no solutions*. Thus, the solution set for this equation is the empty set $\{\}$ which is denoted by $\varnothing$. □

Though we picked some specific examples, it should be easy for you to see that any linear equation in one variable is of the above three types. Its solution set could be of three kinds - the empty set, a singleton set or the whole of $\mathbb{R}$.

What about *systems* of equations? Let us consider a system of linear equations in one variable.

EXAMPLE 1.6. Consider the system

$$a_1 X = b$$
$$a_2 X = b$$

where a_1, a_2, b are all constants. We wish to find all values of X which satisfy these two equations *simultaneously*. So, we first solve any one of the two equations. Suppose we solve the first equation. We will have three cases:

(i) If equation $a_1X = b$ has no solutions, then clearly the system as a whole also has no solutions.
(ii) If the solution set of the equation $a_1X = b$ is of the form $\{c\}$ for some $c \in \mathbb{R}$, then we check whether c satisfies the equation $a_2X = b$ or not by directly substituting c in place of X in this equation. If it c satisfies the second equation, this means that the solution set of the system is $\{c\}$. If c does not satisfy the second equation, the solution set is $\varnothing$.
(iii) If the solution set of $a_1X = b$ is $\mathbb{R}$, then we solve the second equation using the above methods. The solution set of the system is then identical to the solution set of the second equation. □

Now let us try something a little more complicated – let us consider a single equation with two variables.

Example 1.7. We wish to solve equations of the form $a_1X_1 + a_2X_2 = b$ where a_1, a_2, b are constants. We look at various cases:

(i) If $a_1 = a_2 = b = 0$, then any ordered pair of real numbers (x_1, x_2) satisfies this equation. So, in this case the solution set is $\mathbb{R}^2$.
(ii) If $a_1 = a_2 = 0$, but $b \neq 0$, then there are no solutions. So, in this case the solution set is $\varnothing$.
(iii) Suppose $a_1 \neq 0$. (We are making no assumptions about a_2 in this case.) In this case, we can construct a solution by choosing an arbitrary value for X_2. Indeed, let t be any real number. We claim that there is unique real number s such that (s, t) is a solution. To see this, we substitute t in place of X_2 to get the equation

$$a_1X_1 + a_2t = b$$

which is equivalent to

$$a_1X_1 = b - a_2t.$$

We know from our analysis of single variable equations that, this second equation can be uniquely solved for X_1 (since $a_1 \neq 0$). Indeed, we have $X_1 = \frac{(b-a_2t)}{a_1}$. Thus, for any real number t, we can come up with a solution of the form $(\frac{(b-a_2t)}{a_1}, t)$.

Thus, the solution set is

$$S := \{(\frac{(b - a_2t)}{a_1}, t) : t \in \mathbb{R}\}.$$

If $t_1 \neq t_2$, clear the ordered pairs $((b - a_2t_1)/a_1, t_1)$ and $((b - a_2t_2)/a_1, t_2)$ cannot be equal. Thus, the function $t \mapsto ((b - a_2t)/a_1, t)$ is a bijection between the set S and the set $\mathbb{R}$. Thus, we see that in this case, the solution set is in bijection with $\mathbb{R}$.
(iii) If $a_1 = 0$ and $a_2 \neq 0$, we can interchange the roles of a_1 and a_2. A calculation similar to the one above shows that in this case the solution set is

$$\{(t, \frac{(b - a_1t)}{a_2}) : t \in \mathbb{R}\}$$

and that this set is in bijection with $\mathbb{R}$.

Thus, we see that the solution of this equation can be of three forms – an empty set, a set in bijection with $\mathbb{R}$ or the whole of $\mathbb{R}^2$. If you recall some high school coordinate geometry, you will see that when $a_1 \neq 0$ or $a_2 \neq 0$, the set is actually a

line in the Cartesian plane. Thus, the solution set is either the empty set, a line or the entire plane. □

LECTURE 2

Systems of linear equations - further examples

We continue our discussion with our study of systems with a single linear equation.

EXAMPLE 2.1. Consider the equation

$$a_1X_1 + a_2X_2 + a_3X_3 = b$$

where a_1, a_2, a_3, b are all in $\mathbb{R}$.

This equation should be solved exactly along the same lines as in 1.7. If $a_1 = 0$, then X_1 does not really play any role in this equation and so can take any value. Then we solve the equation $a_2X_3 + a_3X_3 = b$ as in 1.7. Solutions of the original equation can be easily derived from this. (Can you work out the rest of this case in detail?)

We will focus on the case $a_1 \neq 0$. In this case, we can assign arbitrary values to X_2 and X_3. Suppose we set $X_2 = t_2$ and $X_3 = t_3$ where t_2, t_3 are real numbers. Then, we can solve the equation

$$a_1X_1 = b - a_2t_2 - a_3t_3$$

to obtain the value of X_1. Thus, the solution set is

$$\left\{ \left(\frac{b - a_2t_2 - a_3t_3}{a_1}, t_2, t_3 \right) : t_2, t_3 \in \mathbb{R} \right\}.$$

Notice that here X_2 and X_3 can take arbitrary values. In some sense, we have only renamed them to t_2 and t_3. However, note that we know exactly which values t_2 and t_3 are allowed to take while we did not know what values X_2 and X_3 could take in the beginning. Also observe that t_2 and t_3 can take values independently of each other (meaning that choosing a particular value for t_2 does not affect our choice of t_3 - it can be chosen entirely freely as well). We say that the solution depends on *two parameters*. We will make all this more precise as we go along. □

We will now move on to solving systems containing more than one equation. For this, we first look into how we manipulate systems of equations. Just like the case of single-equation systems, we modify our given equations by performing operations on them to produce new systems of equations. The new system will generally be a consequence of the old one, but the reverse may not be true. Thus, any solution of the old system will definitely be a solution of the old system, but the new system may have some solutions which are not solutions of the old system. This can be avoided if the operations we perform are *reversible*, i.e. if there exists another operation which allows us to deduce the old system from the new system.

Suppose we have been given a system of n equations. We write them one below the other in n-rows. FOr instance, suppose they look like this:

$$A_1 = B_1 \qquad (E_1)$$
$$A_2 = B_2 \qquad (E_2)$$
$$\vdots \quad \vdots$$
$$A_n = B_n. \qquad (E_n)$$

We will list some reversible operations that we would like to perform on this system. (This is not an exhaustive list of all reversible operations. We are only listing the operations we need.)

(1) *Adding a constant multiple of one equation to another:* Let $x \in \mathbb{R}$. In this operation, we multiply x times equation (E_k) to the equation (E_l) to obtain a new equation, which we denote by (E_l'). Then we delete the equation (E_l) and write the equation (E_l') in its place. Thus, now the system will appear as follows:

$$\begin{aligned} A_1 &= B_1 && (E_1)\\ &\vdots \quad \vdots\\ A_k &= B_k && (E_k)\\ &\vdots \quad \vdots\\ A_l + xA_k &= B_l + xB_k && (E_l')\\ &\vdots \quad \vdots\\ A_n &= B_n. && (E_n) \end{aligned}$$

Notation: Since we have added x times the k-th row to the l-th row in our system, we will use the shorthand notation $R_l + xR_k$ to denote this operation.
Reversibility: Note that this operation is reversible. Indeed, if we perform the operation $R_l + (-x)R_k$, we will recover our original system of equations.

(2) *Replacing an equation by a non-zero multiple:* Let x be a non-zero constant. In this operation, we replace equation (E_k) by the equation

$$xA_k = xB_k.$$

Notation: We will use the shorthand notation xR_k to denote this operation.
Reversibility: This operation is reversible since we can recover the original system by applying the operation $(1/x)R_k$. Note that in order to do so, $(1/x)$ needs to be defined, which is why we need the condition $x \neq 0$.

(3) *Interchanging two equations:* In this operation, we simply change the positions of the equations (E_k) and (E_l). In other words, we write the equation (E_l) in the k-th row and the equation (E_k) in the l-th row.
Notation: We will denote this operation by $R_k \leftrightarrow R_l$.
Reversibility: This operation is reversible since we can apply it again to the new system to recover the old system.

Now let us apply these operations to system with two equations in two variables.

Example 2.2. We wish to solve the following system

$$\begin{aligned} aX_1 + cY &= e\\ bX + dY &= f \end{aligned}$$

where a, b, c, d, e, f are constants.

One simple way to solve this problem is to first solve the first equation (as we have done above), and then substitute its solutions in the second one to see which of them are solutions to both equations. This is a perfectly reasonable method, but we adopt a slightly different approach.

The idea is to use the above operations to reduce the coefficient of X in one of the equations to 0. Once this is done, the second equation can be easily solved for

Y. Then, we can substitute the value obtained for Y in the first equation and solve it to obtain the value of X.

Suppose $a = b = 0$. Then X does not really matter in this system and can take any value in $\mathbb{R}$. We may then simply focus on the system consisting of the equations $cY = e$ and $dY = f$. (Do you see how to write the solution set of the first system after solving this second system?)

Now suppose that at least one of the two numbers a and b is non-zero. We would like to focus on the situation in which the coefficient of X in the first equation is non-zero. So, if $a = 0$ and $b \neq 0$, we perform the operation $R_1 \leftrightarrow R_2$ to obtain the system

$$\begin{aligned} bX + dY &= f \\ aX + cY &= e. \end{aligned}$$

So, we may now assume that $a \neq 0$. We first perform the operation $(1/a)R_1$.

$$\begin{aligned} X + (c/a)Y &= (e/a) \\ bX + dY &= f \end{aligned}$$

It is now easy to see how we may reduce the coefficient of X in the second equation to 0. We perform the operation $R_2 + (-b)R_1$.

$$\begin{aligned} X + (c/a)Y &= (e/a) \\ 0 \cdot X + \left(d - \frac{bc}{a}\right) Y &= f - \frac{be}{a} \end{aligned}$$

This may be rewritten as follows:

$$\begin{aligned} X + (c/a)Y &= (e/a) \\ 0 \cdot X + \left(\frac{ad - bc}{a}\right) Y &= \frac{af - be}{a} \end{aligned}$$

Thus, if $ad - bc = 0$ and $af - be = 0$, then Y can take any value t in $\mathbb{R}$. For every value t, we may substitute it in place of Y in the first equation to get $X = \frac{e - tc}{a}$. Thus, in this case, the solution set will be

$$\left\{ \left(\frac{e - tc}{a}, t \right) : t \in \mathbb{R} \right\}.$$

If $ad - bc = 0$ but $af - be \neq 0$, then no real number can be substituted in place of Y in the second equation to get a true statement. Thus, in this case the solution set is $\varnothing$.

If $ad - bc \neq 0$, we may perform the operation $\frac{a}{ad-bc}R_2$ to get the system

$$\begin{aligned} X + (c/a)Y &= (e/a) \\ 0 \cdot X + Y &= \frac{af - be}{ad - bc}. \end{aligned}$$

Thus, we can immediately read off the value of Y in the solution to be $\frac{af-be}{ad-bc}$. So now we could just substitute this value in the first equation to solve for X. However, there is a more elegant approach. We can simply perform the operation $R_1 + (-c/a)R_2$ to remove Y from the first equation. This gives us the system

$$\begin{aligned} X + 0 \cdot Y &= (e/a) - \frac{c(af - be)}{a(ad - bc)} \\ 0 \cdot X + Y &= \frac{af - be}{ad - bc}. \end{aligned}$$

On simplifying, this takes the form

$$X + 0 \cdot Y = \frac{ed - cf}{ad - bc}$$
$$0 \cdot X + Y = \frac{af - be}{ad - bc}.$$

Thus, in this case, the solution set is

$$\left\{ \left(\frac{ed - cf}{ad - bc}, \frac{af - be}{ad - bc} \right) \right\}$$

This completes our solution for a system of two linear equations in two variables. □

LECTURE 3

Matrices

In this lecture, we will begin to work out an algorithm to solve systems of linear equations. Recall that we wish to manipulate systems of linear equations using certain *reversible* operations. These are listed below with the notation used to indicate them:

(1) $R_i + xR_j$: Adding x times equation (j) to equation (i), where x is any constant. The resulting equation replaces equation i.
(2) xR_i: Multiplying equation (i) by x where $x \neq 0$. The resulting equation replaces equation (i).
(3) $R_i \leftrightarrow R_j$: Interchanging equations (i) and (j).

Note that while we are doing these manipulations, we usually list the equations one below the other in increasing order of their label. Also, we usually fix an order on the variables and always write the equation so that the variables appear in that order from left to right. For instance, if the variables are X, Y and Z, we fix the order (X, Y, Z) and write any linear equation involving these variables as $aX + bY + cZ = d$ (so that X, Y and Z appear in that order from left to right). Thus, if we have 4 equations in these three variables, they will look like:

$$\begin{array}{ccccccc} a_{11}X & + & a_{12}Y & + & a_{13}Z & = & b_1 \\ a_{21}X & + & a_{22}Y & + & a_{23}Z & = & b_2 \\ a_{31} & + & a_{32}Y & + & a_{33}Z & = & b_3 \\ a_{41}X & + & a_{m2}Y & + & a_{m3}Z & = & b_4 \end{array}$$

Thus, the terms involving a fixed variable appear neatly in a vertical column. Thus, we could completely omit to write the variables and represent the above system as

$$\left[\begin{array}{ccc|c} a_{11} & a_{12} & a_{13} & b_1 \\ a_{21} & a_{22} & a_{23} & b_2 \\ a_{31} & a_{32} & a_{33} & b_3 \\ a_{41} & a_{42} & a_{43} & b_4 \end{array}\right]$$

This is called an *augmented matrix*. Before we explain this term, we first define a *matrix*.

DEFINITION 3.1. Let m and n be positive integers. An $m \times n$ *matrix* A is a collection of mn numbers arranged in a rectangular array as follows:

$$\begin{bmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{m1} & \cdots & \cdots & a_{mn} \end{bmatrix}$$

The number in the i-th row and j-th column is called the (i, j)-*entry* of the matrix and is denoted in the above representation as a_{ij}.

In the above definition, the word *number* can be interpreted to mean real number, complex number, integer, or whatever you like. For now, we will continue to assume that they are real numbers.

An *augmented matrix* is just a matrix in which the last column is considered to be special in some way and is separated from the rest of the matrix by a separator. If you like, you may also see an $m \times (n+1)$ augmented matrix as being made of a $m \times n$ matrix written on the left (which we will refer to as the *left block* of the augmented matrix), and a $m \times 1$ matrix written on the right (the *right block* of the augmented matrix) . Thus, we see that an augmented $m \times (n+1)$ matrix can be used to represent a system of m linear equations in n variables.

The *elementary row operations* listed above can now be performed on matrices. Recall the examples from the earlier lectures and Tutorial 1. The objective of these row operations is to reduce the left block of the augmented matrix into a particularly simple form so that the solutions of the linear system can be computed easily. We now describe this "simple form" in the following definition:

DEFINITION 3.2. A matrix is said to be a *row reduced echelon matrix* (or to be in *row reduced echelon form*) if it satisfies the following conditions:

(a) The leftmost non-zero entry in every row is equal to 1. Such an entry is called a *pivot*.
(b) If a column contains a pivot, all other entries in that column are equal to 0.
(c) If $i < j$ are positive integers and the i-th and j-th rows contain pivots, the pivot in the j-th row is to the right of the pivot in the i-th row. (More precisely, if the pivot in the i-th row occurs in the k_i-th column and the pivot in the j-th row j the k_j-th column, then $k_i < k_j$.)
(d) All the zero rows (i.e. rows filled with 0's) occur at the bottom of the matrix. In other words, no non-zero row occurs below a zero row.

We list some matrices and check whether they are in row reduced echelon form or not. All the pivots are indicated by a box around them.

EXAMPLE 3.3. The following matrices are in row reduced echelon form:

$$\begin{bmatrix} \boxed{1} & 4 & 3 & 0 & 2 & 0 \\ 0 & 0 & 0 & \boxed{1} & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & \boxed{1} & 1 & 0 & 0 & 3 \\ 0 & 0 & 0 & \boxed{1} & 0 & 2 \\ 0 & 0 & 0 & 0 & \boxed{1} & 8 \end{bmatrix}$$

A somewhat odd example is the following:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Do you understand why this is in row reduced echelon form?

EXAMPLE 3.4. We now list some matrices that are not in row reduced echelon form.

(1) The matrix

$$\begin{bmatrix} \boxed{1} & 8 & 2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{bmatrix}$$

does not satisfy condition (a).

(2) The matrix

$$\begin{bmatrix} 0 & \boxed{1} & 6 & 0 & 5 & 2 \\ 0 & 0 & 0 & \boxed{1} & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{bmatrix}$$

fails to satisfy condition (b).

(3) The matrix

$$\begin{bmatrix} \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & \boxed{1} & 3 \\ 0 & \boxed{1} & 0 & 2 \end{bmatrix}$$

fails to satisfy condition (c).

(4) The matrix

$$\begin{bmatrix} \boxed{1} & 4 & 3 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boxed{1} & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{bmatrix}$$

fails to satisfy condition (d).

We will show in the next lecture that any matrix can be transformed into a row reduced echelon matrix using elementary row transformations.

LECTURE 4

Row reduction algorithm

We will now see that there exists a systematic procedure, i.e. an algorithm, that allows us to reduce any given matrix to a row reduced echelon matrix using elementary row transformations.

Recall that the elementary row transformations are as follows:

(1) Adding a constant multiple of the j-th row to the i-th row: This is operation is written as $R_i + xR_j$ or $R_i \to R_i + xR_j$, where x is a constant.
(2) Multiplying row i by a non-zero constant: This operation is written as xR_i or $R_i \to xR_i$ where x is a non-zero constant.
(3) Switching the i-th and j-th rows: This operation is written as $R_i \leftrightarrow R_j$.

We will not define *algorithms* formally. Roughly speaking, an algorithm is a formal set of instructions that starts with some data (called as the *input*), performs certain operations on the data and then produces a result (called as the *output*). The instructions to perform those operations need to be concrete enough that they can be executed by a computer. When we come up with an algorithm, we should be able to show that it will terminate in a finite amount of time and that it will indeed produce the desired result. We will first only present the algorithm and look into the proof of its validity in the next lecture. Our presentation will be extremely informal to begin with and the instructions of the algorithm will be accompanied with a detailed commentary to explain what is happening.

INPUT: *We are given an $m \times n$ matrix A with entries in $\mathbb{R}$ with m and n are positive integers.*

Note that the algorithm will work just as well if we are given a matrix with entries from $\mathbb{Q}$ or $\mathbb{C}$.

STEP 0: *Set $\mathcal{P} = \varnothing$.*

Our strategy is to bring the given matrix into the required form one column at a time. Within every column, we will try to create a *pivot*. (Recall from the last lecture that an entry in the matrix is a pivot if it is the leftmost non-zero entry in a row and if it is equal to 1.) While we are computing, we need to keep track of two things - (1) which column we are working on right now, and (2) which rows have acquired pivots. In our first draft of the algorithm, the column number being considered will be the same as the number of the step we are executing, and so it is easy to keep track of it. The set $\mathcal{P}$ will be used to remember which rows have pivots. Once we create a pivot in row number i, we will add the integer i to $\mathcal{P}$. Since we have not done anything yet, $\mathcal{P}$ is empty.

STEP 1: *There are two cases to consider in this step:*

(*Case 1*) *If all the entries of column 1 are equal to 0, go to step 1.*
(*Case 2*) *If <u>not all</u> the entries of column 1 are equal to 0, let the first non-zero entry from the top occur in row j. Denote this entry by x. Perform the following operations (in the given sequence):*
- *If $j > 1$, then perform the operation $R_1 \leftrightarrow R_j$.*
- *Perform the operation $(1/x)R_1$.*
- *Add the element 1 to $\mathcal{P}$*

- *For every integer p satisfying $1 \leqslant p \leqslant m$, let a_{p1} denote the $(p,1)$ entry. For every such p, perform the operation $R_p - a_{p1}R_1$.*
- *Go to Step 2.*

Our intention in this step is to change column 1 so that it will be consistent with the row reduced echelon form. (Case 1) just checks if there is any non-zero term. If there is no such term, we simply move on to the next column, i.e to Step 2. Thus, the matrix looks like the following:

$$\left[\begin{array}{c|ccc} 0 & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{array}\right]$$

Notice that in this case, we do not create a pivot and so $\mathcal{P}$ remains empty.

In (Case 2), we the topmost non-zero element in the first column is in row i. We shifted this element to the first row, turned it into 1 and then used it to reduce all other elements in the first column to 0. Thus, in this case the matrix will look like the following:

$$\left[\begin{array}{c|ccc} \boxed{1} & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{array}\right]$$

Thus, in this case we have created a pivot and so we added the element 1 to the set $\mathcal{P}$. Thus, in this case, the set $\mathcal{P}$ changes to $\{1\}$.

STEP 2: *Let i be the smallest integer such that $i \notin \mathcal{P}$. There are two cases to consider in this step:*

(*Case 1*) *For every integer l such that $i \leqslant l \leqslant m$, the $(l,2)$-entry is equal to 0. In this case, go to step 3.*

(*Case 2*) *If the condition in (Case 1) does not hold, let j be the smallest integer such that $i \leqslant j \leqslant m$ and the $(j,2)$-entry is non-zero. Denote this entry by x. Perform the following operations (in the given sequence):*
- *If $j > i$, then perform the operation $R_i \leftrightarrow R_j$.*
- *Perform the operation $(1/x)R_i$.*
- *Add the element i to $\mathcal{P}$*
- *For every integer p satisfying $1 \leqslant p \leqslant m$ and $p \neq i$, let a_{p2} denote the $(p,2)$ entry. For every such p, perform the operation $R_p - a_{p2}R_i$.*
- *Go to Step 2.*

In this step, we work on column 2. We want to create a pivot in column 2, if possible. However, this pivot must be in a new row. Thus, we avoid all the rows whose label is contained in the set $\mathcal{P}$ (the "pivoted rows"). The row immediately after all the pivoted row is the i-th row. We look at all the entries in column 2 which occur in the i-th row or below. If none of them are non-zero, this means that we are in (Case 1) of Step 2 and we move on to Step 3. Note that it could also happen that the matrix has only one row which is already pivoted (i.e. $i = m+1$). In that case too, one can check that (Case 1) is valid. (Do you see why? Because the set of all integers j satisfying $m+1 \leqslant j \leqslant m$ is *empty*! It is certainly true that "all numbers in an empty set are equal to zero"! It sounds silly, but it is true!)

If (Case 1) is not valid, it means that there exists a non-zero entry in column 2 which does not lie in a pivoted row. Suppose this entry lies in row j. We moved it up to column i and turned it into 1. Then we used it to turn all the other entries in column 2 into 0.

The two cases in Step 1 and the two cases in Step 2 have given rise to four possibilities. Can you figure out what the matrix will look like in each case?

For every integer k satisfying $2 < k \leqslant m$, Step k is similar to Step 2.

STEP k: *Let i be the smallest integer such that $i \notin \mathcal{P}$. There are two cases to consider in this step:*

(*Case 1*) *For every integer l such that $i \leqslant l \leqslant m$, the (l,k)-entry is equal to 0. In this case, go to step 3.*

(*Case 2*) *If the condition in (Case 1) does not hold, let j be the smallest integer such that $i \leqslant j \leqslant m$ and the (j,k)-entry is non-zero. Denote this entry by x. Perform the following operations (in the given sequence):*
- *If $j > i$, then perform the operation $R_i \leftrightarrow R_j$.*
- *Perform the operation $(1/x)R_i$.*
- *Add the element i to $\mathcal{P}$*
- *For every integer p satisfying $1 \leqslant p \leqslant m$ and $p \neq i$, let a_{pk} denote the (p,k) entry. For every such p, perform the operation $R_p - a_{pk}R_i$.*
- *Go to Step $k+1$.*

Once again, the idea is the same - we try to create a pivot in column k directly below all the previously pivoted rows. If we find no non-zero entries, we simply move on to the next column without changing the set $\mathcal{P}$. If we succeed in creating a pivot, we update the set $\mathcal{P}$ and then move on to the next column.

Obviously, this process has to end when we run out of columns. Thus, we have the last step:

STEP $m+1$: *STOP.*

OUTPUT: *The resulting matrix is the output of this algorithm.*

Of course, we need to check that this is a row-reduced echelon matrix.

EXAMPLE 4.1. We will execute the algorithm on the following matrix:

$$\begin{bmatrix} 1 & -2 & 1 & 2 \\ 1 & 1 & -1 & 1 \\ 1 & 7 & -5 & -1 \end{bmatrix}$$

STEP 0: Set $\mathcal{P} = \varnothing$.

STEP 1: We are in (Case 2). We observe that $j = 1$. Thus we do not need to switch rows. We first perform the operation $(1/1)R_1$. (Notice that this does nothing, but we will do it anyway!) This gives us the matrix

$$\begin{bmatrix} \boxed{1} & -2 & 1 & 2 \\ 1 & 1 & -1 & 1 \\ 1 & 7 & -5 & -1 \end{bmatrix}$$

and we set $\mathcal{P} = \{1\}$.

Now we perform the operations $R_2 - 1 \cdot R_1$ and $R_3 - 1 \cdot R_1$ to obtain the matrix

$$\begin{bmatrix} \boxed{1} & -2 & 1 & 2 \\ 0 & 3 & -2 & -1 \\ 0 & 9 & -6 & -3 \end{bmatrix}$$

(Strictly speaking, I should have performed the operations one at a time and written two matrices.) This concludes Step 1.

STEP 1: We are in (Case 2). We observe that $i = 2$, $j = 2$ and $x = 3$. As $i = j$, we do not have to switch rows. We move on to perform the operation $(1/3) \cdot R_2$. This

gives us the matrix

$$\begin{bmatrix} \boxed{1} & -2 & 1 & 2 \\ 0 & \boxed{1} & -2/3 & -1/3 \\ 0 & 9 & -6 & -3 \end{bmatrix}$$

and we set $\mathcal{P} = \{1, 2\}$.

Finally, we perform the operation $R_1 - (-2)R_2$ and $R_3 - 9 \cdot R_2$ to get the matrix

$$\begin{bmatrix} \boxed{1} & 0 & 1/3 & 4/3 \\ 0 & \boxed{1} & -2/3 & -1/3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

STEP 3: We are in (Case 1). So we move on to Step 4.

STEP 4: We are in (Case 1). So we move on to Step 5.

STEP 5: *STOP*

OUTPUT: The output is the matrix

$$\begin{bmatrix} \boxed{1} & 0 & 1/3 & 4/3 \\ 0 & \boxed{1} & -2/3 & -1/3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

which is in row reduced echelon form.

LECTURE 5

Verification and applications of the row reduction algorithm

We will now verify that the algorithm given above really gives us a row reduced echelon matrix. Recall that a matrix is said to be in row reduced echelon form if it satisfies the following conditions:

(a) The leftmost non-zero entry in every row is equal to 1. Such an entry is called a *pivot*.
(b) If a column contains a pivot, all other entries in that column are equal to 0.
(c) If $i < j$ are positive integers, the i-th row contains a pivot in the k_i-th column and the j-th row contains a pivot in the j-th column, then $k_i < k_j$.
(d) All the zero rows (i.e. rows filled with 0's) occur at the bottom of the matrix. In other words, no non-zero row occurs below a zero row.

Now let us recall the algorithm. We will write it a little more concisely than last time.

INPUT: *We are given an $m \times n$ matrix A with entries in $\mathbb{R}$ with m and n are positive integers.*

STEP 0: *Set $\mathcal{P} = \varnothing$.*

For $1 \leqslant k \leqslant n$, we have the following steps:

STEP k: *Let i be the smallest positive integer such that $i \notin \mathcal{P}$. There are two cases to consider in this step:*

(*Case 1*) *For every integer l such that $i \leqslant l \leqslant m$, the (l,k)-entry is equal to 0. In this case, go to step 3.*
(*Case 2*) *If the condition in (Case 1) does not hold, let j be the smallest integer such that $i \leqslant j \leqslant m$ and the (j,k)-entry is non-zero. Denote this entry by x. Perform the following operations (in the given sequence):*
- *If $j > i$, then perform the operation $R_i \leftrightarrow R_j$.*
- *Perform the operation $(1/x)R_i$.*
- *Add the element i to $\mathcal{P}$*
- *For every integer p satisfying $1 \leqslant p \leqslant m$ and $p \neq i$, let a_{pk} denote the (p,k) entry. For every such p, perform the operation $R_p - a_{pk}R_i$.*
- *Go to Step $k+1$.*

STEP $n+1$: *STOP*

OUTPUT: *The resulting matrix is the output of this algorithm.*

We will now outline an argument showing that the output of this algorithm satisfies properties (a)-(d) listed above. The proof has not been written out formally

Verifying (a): First let us understand what needs to be verified here. For every k satisfying $1 \leqslant k \leqslant n$, if we are in (Case 2), we create a '1' in the (i,k)-position. In the previous lecture, we referred to this entry as a "pivot". However, we never

actually proved that this is a pivot! In other words, we need to verify at the end of the algorithm, every entry to the left of this one is equal to 0.

For this, we have the following observation:

> *Observation:* Let k be an integer satisfying $1 \leqslant k \leqslant n$. Let i be any integer such that $1 \leqslant i \leqslant m$ and i is not in $\mathcal{P}$ at the end of Step k. Let j be any integer such that $1 \leqslant j \leqslant k$. Then the (i, j)-entry is equal to 0 at the end of Step k.

Observe that an integer i is in $\mathcal{P}$ if at some point in the algorithm, we have created a '1' in the i-th row through (Case 2) of Step k for some k satisfying $1 \leqslant k \leqslant n$. Since we have not actually proved that these entries are pivots, let us temporary call such rows as "special rows". Also recall that in Step k, we work on the entries in column k. The above observation says that at the end of Step k, any entry that occurs below the special rows and to the left of column $k+1$ is equal to 0.

First let us verify this for Step 1. If we are in (Case 1) of Step 1, we end up with $\mathcal{P} = \varnothing$ (so there are no special rows). However, in that case we know that the first column is entirely filled with zeros. So the above observation is certainly true in that case. If we are in (Case 2), then we end up with $\mathcal{P} = \{1\}$ at the end of Step 1. Thus, the first row is a special row. However, we know that in that case every term in the first column, except for the topmost term, is equal to 0. Thus, the observation is verified for Step 1.

Now suppose that we know the observation to be true for Step 1, Step 2... and so on till Step k. Suppose $k+1 \leqslant n$. Let us verify the observation for Step $k+1$. Suppose that at the beginning of Step $k+1$, we have $\mathcal{P} = \{1, \ldots, i\}$. Thus, the first i rows are special and we know that any entry which occurs below the first i rows and within the first k columns is equal to 0. Suppose we are in (Case 1) of Step $k+1$. Then that means that every entry below the first i rows and in the $(k+1)$-th column is also 0. This verifies the observation in (Case 1). If we are in (Case 2), then at the end of Step $k+1$, the $(i+1, k+1)$-entry is equal to 1 and all entries below it are 0. Also, now the first $i+1$ rows are special (and $\mathcal{P} = \{1, \ldots, i+1\}$). It is once again clear that every entry below the first $i+1$ rows and within the first $k+1$ columns is equal to 0. Thus, the observation is true in (Case 2) also. Thus, we see that the observation remains true at the end of Step $k+1$. This argument can be repeated for the $k+2$-th column and so on.

This verifies the observation for all k satisfying $1 \leqslant k \leqslant n$. (What we have done above is an example of *proof by inducion*. We will not discuss the details of that for now.)

Now, we can use this observation to verify property (a). Suppose that at the beginning of Step l, we have $\mathcal{P} = \{1, \ldots, i\}$ and we are in (Case 2) and we create a '1' in the $(i+1, l)$-position. Applying the observation with $k = l-1$, we see that all the entries to the left of the $(i+1), l$ position are equal to 0. This shows that the newly created '1' is a pivot at the end of Step l. However, we should check that this remains a pivot till the end of the algorithm. Suppose that $j < l$. We want to show that the $(i+1, j)$-entry remains 0 until the end of the algorithm. However, for all later steps in the algorithm, only change row $(i+1)$ by adding a constant multiple of some lower row (say, row p for $p > i+1$) to the $(i+1)$-th row. However, the (p, j)-entry is known to be 0 by the above observation. Thus, adding any multiple of this to the $(i+1, j)$-entry is not going to change it. Thus, we see that the $(i+1, j)$-entry remains 0 until the end of the algorithm. In particular, this verifies property (a) for the output matrix.

Verifying (b): Property (b) is immediately obvious since every time we create a pivot, we immediately change all other entries in its column to 0. Also, no further row operations can change them back to something non-zero.

Verifying (c): Suppose $1 \leqslant i < j \leqslant m$ and that the i-th and j-th rows both contain pivots. It is easy to see from the algorithm that the pivot in the j-th row was created at a later step of the algorithm than the pivot in the i-th row. So the column containing the pivot in the j-th row is to the right of the column containing the pivot in the i-th row.

Verifying (d): In the algorithm, we continue to create pivots in consecutive rows until we come to a point where we cannot find any non-zero entries below the "special rows" (i.e. rows with pivots). Thus, all the zero rows must occur below all the non-zero rows in the output matrix.

Thus, we have now verified that the output matrix is in row-reduced echelon form.

Applications to solving systems of linear equations: We now return to our original purpose in studying row reduction – solving systems of linear equations. As we saw earlier, a system of linear equations of the form

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1 \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}X_1 & + & a_{m2}X_2 & + & \cdots & & a_{mn}X_n & = & b_m \end{array}$$

can be represented by the augmented matrix

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right]$$

Then, we perform the row reduction algorithm on the left block of this augmented matrix. However, the same row operations should be simultaneously performed on the right block as well. As a result, we will end up with an augmented matrix in which the left block is in row reduced echelon form. We then try to solve this *row reduced system* of equations.

First of all, we check the equations at the bottom of the row reduced system. If in any of the equations at the bottom, the left hand side is equal to 0, but the right hand side is not, the system of equations cannot have any solutions.

So, now suppose that if, in any of the equations at the bottom, the left hand side is equal to 0, then the right hand side of that equation is also equal to 0. Then, we shift our focus to the equations in which the left hand side is non-zero.

Each column of the left block corresponds to a variable in the given system of linear equations. Suppose $X_{i_1}, X_{i_2} \ldots, X_{i_r}$ are the variables corresponding to the columns which *do not have a pivot*. To construct a general solution of the given system, we simply set $X_{i_1} = t_1$, $X_{i_2} = t_2, \ldots, X_{i_r} = t_r$ where $t_1, \ldots, t_r$ can take arbitrary values in $\mathbb{R}$. Now, if $X_{j_1}, \ldots, X_{j_x}$ are variables corresponding to the columns with pivots, of the X_{j_i} can occur in exactly one equation each. Also, no two of them can occur in the same equation. Thus, we can easily solve the equations for those equations.

Example 5.1. We will solve the system

$$\begin{array}{ccccccccc} 3X_1 & - & 2X_2 & + & 4X_3 & + & 7X_4 & = & 11 \\ X_1 & + & 5X_2 & - & X_3 & + & 6X_4 & = & 4 \\ -X_1 & + & 3X_2 & + & 3X_3 & + & 2X_4 & = & -1 \end{array}$$

using the above method. The augmented matrix representing this system is

$$\left[\begin{array}{cccc|c} 3 & -2 & 4 & 7 & 11 \\ 1 & 5 & -1 & 6 & 4 \\ -1 & 3 & 3 & 2 & -1 \end{array}\right]$$

STEP 0: Set $\mathcal{P} = \varnothing$.

STEP 1: First perform $(1/3)R_1$.

$$\left[\begin{array}{cccc|c} \boxed{1} & -2/3 & 4/3 & 7/3 & 11/3 \\ 1 & 5 & -1 & 6 & 4 \\ -1 & 3 & 3 & 2 & -1 \end{array}\right]$$

This has created a pivot in the first row. So we set $\mathcal{P} = \{1\}$. Then we perform the operations $R_2 + (-1)R_1$ and $R_3 + R_1$.

$$\left[\begin{array}{cccc|c} \boxed{1} & -2/3 & 4/3 & 7/3 & 11/3 \\ 0 & 17/3 & -7/3 & 11/3 & 1/3 \\ 0 & 7/3 & 13/3 & 13/3 & 8/3 \end{array}\right]$$

This concludes Step 1.

STEP 2: Perform $(3/17)R_2$.

$$\left[\begin{array}{cccc|c} \boxed{1} & -2/3 & 4/3 & 7/3 & 11/3 \\ 0 & \boxed{1} & -7/17 & 11/17 & 1/17 \\ /0 & 7/3 & 13/3 & 13/3 & 8/3 \end{array}\right]$$

This has created a pivot in the second row. So we set $\mathcal{P} = \{1, 2\}$. Then we perform the operations $R_1 + (2/3)R_2$ and $R_3 + (-7/3)R_2$.

$$\left[\begin{array}{cccc|c} \boxed{1} & 0 & 18/17 & 47/17 & 63/17 \\ 0 & \boxed{1} & -7/17 & 11/17 & 1/17 \\ 0 & 0 & 90/17 & 48/17 & 43/17 \end{array}\right]$$

This concludes Step 2.

STEP 3: Perform $(17/90)R_3$.

$$\left[\begin{array}{cccc|c} \boxed{1} & 0 & 18/17 & 47/17 & 63/17 \\ 0 & \boxed{1} & -7/17 & 11/17 & 1/17 \\ 0 & 0 & \boxed{1} & 8/15 & 43/90 \end{array}\right]$$

This creates a pivot in the third row. So, we set $\mathcal{P} = \{1, 2, 3\}$. Then we perform the operations $R_1 + (-18/17)R_3$ and $R_2 + (7/17)R_3$.

$$\left[\begin{array}{cccc|c} \boxed{1} & 0 & 0 & 11/5 & 16/5 \\ 0 & \boxed{1} & 0 & 13/15 & 23/90 \\ 0 & 0 & \boxed{1} & 8/15 & 43/90 \end{array}\right]$$

This concludes Step 3.

STEP 4: All the rows have pivots. So we are in (Case 1) of Step 4. Thus, we do nothing and move on.

STEP 5: *STOP.*

Thus, we now have to solve the system that is represented by the following augmented matrix:

$$\left[\begin{array}{cccc|c} \boxed{1} & 0 & 0 & 11/5 & 16/5 \\ 0 & \boxed{1} & 0 & 13/15 & 23/90 \\ 0 & 0 & \boxed{1} & 8/15 & 43/90 \end{array}\right]$$

Since column 4 has no pivots, we may set $X_4 = t$. Then the system is reduced to

$$\begin{aligned} X_1 + (11/5)t &= 16/5 \\ X_2 + (13/5)t &= 23/90 \\ X_3 + (8/5)t &= 43/90. \end{aligned}$$

Thus, we have the solution set

$$\left\{ \left(\frac{16}{5} - \frac{11t}{5}, \frac{23}{90} - \frac{13t}{5}, \frac{43}{90} - \frac{8t}{5}, t \right) : t \in \mathbb{R} \right\}.$$

LECTURE 6

Matrix multiplication

Notation: The set of $m \times n$ matrices with entries from $\mathbb{R}$ will be denoted by $M_{m\times n}(\mathbb{R})$. (Similarly, we can denote the set of matrices with entries from the rational numbers, integers, etc. by $M_{m\times n}(\mathbb{Q})$, $M_{m\times n}(\mathbb{Z})$, etc. respectively. However, for now, we will only work with matrices having entries from $\mathbb{R}$.) If A is an $m \times n$ matrix and the (i, j)-entry of which is a_{ij}, we will express this briefly as

$$A := (a_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}.$$

If the number or rows and columns of A is understood from the context, we will simply write $A := (a_{ij})_{i,j}$.

We will discuss some basic operations on matrices.

Addition of matrices: The sum of matrices is defined only if they are of the same shape, i.e. if they have the same number of rows and columns. Let $A = (a_{ij})_{i,j}$ and $B := (b_{ij})_{i,j}$ be two $m \times n$ matrices. Their *sum* is defined to the $m \times n$ matrix $C = (c_{ij})_{i,j}$ where $c_{ij} = a_{ij} + b_{ij}$. Example:

$$\begin{bmatrix} 2 & 3 & 0 \\ -1 & 1 & 2 \end{bmatrix} + \begin{bmatrix} -1 & 2 & 7 \\ 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 2+(-1) & 3+2 & 0+7 \\ -1+3 & 1+4 & 2+5 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 5 & 7 \\ 2 & 5 & 7 \end{bmatrix}$$

Let $\mathbf{0}_{m\times n}$ denote the $m \times n$ matrix in which every entry is equal to 0. (Again, if the shape of the matrix is clear from the context, we may just write $\mathbf{0}$ instead of $\mathbf{0}_{m\times n}$.) If $A = (a_{ij})_{i,j}$, let $-A$ denote the matrix (of the same shape) given by $-A = (-a_{ij})_{i,j}$. Then the following properties are easy to verify:

(i) $A + B = B + A$. ("Addition is commutative.")
(ii) $(A + B) + C = A + (B + C)$. ("Addition is associative.")
(iii) $A + \mathbf{0} + \mathbf{0} + A = A$. ("$\mathbf{0}$ is the identity for addition.)
(iv) $A + (-A) = (-A) + A = \mathbf{0}$. ("$-A$ is the additive inverse of A.)

Matrix Multiplication:

Definition 6.1. Let $A = (a_{ij})_{i,j}$ be an $m \times n$ matrix and let $B = (b_{ij})_{i,j}$ be an $n \times p$ matrix. We define the product AB to be an $m \times p$ matrix $C = (c_{ij})_{i,j}$ where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Observe that the product AB of two matrices A and B is defined only if the number of columns of A is equal to the number of rows of B. In other words, the length of every row of A needs to be equal to the length of every column of B. If this condition is met, the (i, j)-entry of the product is computed using the i-th row of A and the j-th column of B.

Example 6.2. When it comes to the matrix product, the order in which the matrices are written is extremely important. So AB and BA mean very different things. Indeed, while the product AB may be well-defined, the product BA may

not be defined since the number of columns of B may not be equal to the number of rows of A. For instance, consider the following product:

$$\begin{bmatrix} 2 & 1 \\ 0 & -3 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 11 & 14 \\ -15 & -18 \\ 2 & 2 \end{bmatrix}$$

This product is well-defined because the number of columns in the matrix on the left is equal to the number or rows in the matrix on the right. However, the product

$$\begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & -3 \\ -1 & 1 \end{bmatrix}$$

is not defined.

Even if BA is defined, there is no reason for it to be equal to AB (except in some very rare cases). For instance the products

$$\begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

are both defined, but they are clearly not equal since they are matrices of different shapes.

However, even if both the products AB and BA are defined and are of the same shape, they may still be unequal. For instance

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 1 \end{bmatrix}$$

but

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$$

DEFINITION 6.3. Let n be a positive integer. The $n \times n$ matrix identity matrix I_n is defined by $I_n = (\delta_{ij})_{i,j}$ where

$$\delta_{ij} = \begin{cases} 1 & \text{for } i = j \\ 0 & \text{otherwise.} \end{cases}$$

In other words, this is the $n \times n$ square matrix having 1's on the diagonal and 0's in all other positions.

We now list some basic properties of matrix multiplication. We will only prove the first property (which is perhaps the hardest of the lot) in detail. You may verify the rest.

(1) *Suppose A is an $m \times n$ matrix, B is a $n \times p$ matrix and C is a $p \times q$ matrix. Then $A(BC) = (AB)C$.*

PROOF. Let $A = (a_{ij})_{i,j}$, $B = (b_{ij})_{i,j}$ and $C = (c_{ij})_{i,j}$. We wish to show that the matrices $A(BC)$ and $(AB)C$ are identical. It suffices to show that for each pair (i, j) with $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant q$, the (i, j)-entry

of $A(BC)$ is equal to the (i,j)-entry of $(AB)C$.

$$\begin{aligned}(i,j)-\text{entry of } A(BC) &= \sum_{k=1}^{n} a_{ik}\cdot((k,j)-\text{entry of } BC)\\ &= \sum_{k=1}^{n} a_{ik}\left(\sum_{l=1}^{p} b_{kl}c_{lj}\right)\\ &= \sum_{k=1}^{n}\left(\sum_{l=1}^{p} a_{ik}b_{kl}c_{lj}\right)\\ &= \sum_{1\leqslant k\leqslant n, 1\leqslant l\leqslant p} a_{ik}b_{kl}c_{lj}\\ &= \sum_{l=1}^{p}\left(\sum_{k=1}^{n}(a_{ik}b_{kl}\right)c_{lj}\\ &= \sum_{l=1}^{p}((i,l)-\text{entry of } AB)\cdot c_{lj}\\ &= (i,j)-\text{entry of } (AB)C\end{aligned}$$

This proves that $A(BC)=(AB)C$. □

(2) *Suppose A is an $m\times n$ matrix and B, C are $n\times p$ matrices. Then*

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

(3) *Suppose A, B are $m\times n$ matrices and C is an $n\times p$ matrix Then*

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

(4) *Suppose A is an $m\times n$ matrix. Then*

$$I_mA=A=A\cdot I_n.$$

Property (1) is usually phrased as "matrix multiplication is associative". Property (2) and (3) say that "matrix multiplication is distributive over matrix addition".

Using matrix multiplication to represent matrix multiplication:

Consider the following system of linear equations:

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1\\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & b_2\\ \vdots & & \vdots & & & & \vdots & & \vdots\\ a_{m1}X_1 & + & a_{m2}X_2 & + & \cdots & & a_{mn}X_n & = & b_m \end{array}$$

Let A denote the $m\times n$ matrix $(a_{ij})_{i,j}$. Let X denote the $n\times 1$ matrix having X_i in the $(i,1)$-position. Let B denote the $m\times 1$ matrix having b_i in the $(i,1)$-position. Then, the above system of equation can be concisely expressed as the single matrix equation

$$AX=B.$$

Computationally, this does not necessarily make it any easier to solve the system of equations. However, this is a good book-keeping tool and will help us conceptually understand the situation better in later lectures.

Row operations as matrix multiplication:

Let $A=(a_{ij})_{i,j}$ be an $m\times n$ matrix and let $1\leqslant k\leqslant m$, $1\leqslant l\leqslant m$ with $k\neq l$. Let x be a real number. Let $B=(b_{ij})_{i,j}$ be the matrix obtained by performing the operation R_k+xR_l on A. Recall that I_m denotes the $m\times m$ identity matrix. Let

$E = (\epsilon_{ij})_{i,j}$ be the matrix obtained by performing the operation $R_k + xR_j$ on I_m. Then ϵ_{ij} is given as follows:

$$\epsilon_{ij} = \begin{cases} 1 & \text{for } i = j \\ x & \text{for } i = k,\ j = l \\ 0 & \text{otherwise.} \end{cases}$$

We compute the (i, j)-entry of the product EA. Suppose $i \neq k$. Then

$$(i, j) - \text{entry of } EA = \sum_{p=1}^{m} \epsilon_{ip} a_{pj}$$

If $i \neq k$, then $\epsilon_{ii} = 1$ for and $\epsilon_{ip} = 0$ for $i \neq p$. Thus, we have

$$(i, j) - \text{entry of } EA = a_{ij}$$

For $i = k$, we have $\epsilon_{kk} = 1$, $\epsilon_{kl} = x$ and $\epsilon_{kp} = 0$ for all other values of p. Thus,

$$(k, j) - \text{entry of } EA = 1 \cdot a_{kj} + x \cdot a_{lj}.$$

However, by definition

$$b_{ij} = \begin{cases} a_{ij} & \text{for } i \neq k \\ a_{kj} + xa_{lj} & \text{for } i = k. \end{cases}$$

Thus, we see that $EA = B$.

By similar arguments, one can show that a similar result holds for the other elementary row operations as well. So we have the result

THEOREM 6.4. *Let A be an $m \times n$ matrix. Let B be the matrix obtained by performing a certain elementary row operation on A. Let E be the matrix obtained by performing the same operation on I_m. Then we have*

$$B = EA.$$

LECTURE 7

Invertible matrices

In the last lecture, we saw that performing an elementary row operation on a matrix is equivalent to multiplying it on the left by a specially constructed matrix. We will first obtain an easy generalization of this to multiple row operations.

THEOREM 7.1. *Let A be an $m \times n$ matrix. Let $Op_1, Op_2, \ldots, Op_k$ denote elementary row operations and let B be the matrix obtained from A by performing these operations in the given order. For every i, $1 \leqslant i \leqslant k$, let E_i denote the matrix obtained by performing the operation Op_i on I_m. Then, we have*

$$B = E_k \cdots E_1 \cdot A.$$

PROOF. Let B_1 be the matrix obtained from A by performing the operation Op_1. For each i, $2 \leqslant i \leqslant k$, let B_i be the matrix obtained from B_{i-1} by performing the operation Op_i. Thus, we see that B_k is the matrix obtained by performing the operations $Op_1, Op_2, \ldots, Op_k$ successively on A. Thus, $B_k = B$.

By Theorem 6.4, $B_1 = E_1 A$ and $B_i = E_i B_{i-1}$ for every i, $2 \leqslant i \leqslant k$. Thus,

$$\begin{aligned} B = B_k &= E_k B_{k-1} \\ &= E_k E_{k-1} B_{k-2} \\ &\quad (\textit{and so on}) \\ &= E_k \cdots E_1 A. \end{aligned}$$

This proves our result. □

REMARK 7.2. It is generally not good practice to write a mathematical argument with phrases like "and so on" since they are far too vague. Strictly speaking, an argument with such phrases would not be considered rigorous. However, this argument can be made rigorous by using the *principal of mathematical induction*. For now, this informal argument will suffice for our purposes.)

In the context of the above proof, let E be the matrix $E_k \cdots E_1$. Thus, $B = EA$. Since

$$E = E_k \cdots E_1 \cdot I_m,$$

the above theorem implies that the matrix E can be obtained by performing the operations $Op_1, \ldots, Op_k$ on the matrix I_m. Thus, the above theorem could be restated as follows:

THEOREM 7.3. *Let A be an $m \times n$ matrix. Let $Op_1, Op_2, \ldots, Op_k$ denote elementary row operations and let B be the matrix obtained from A by performing these operations in the given order. Let E be the matrix obtained from I_m by performing the same operations in the given order. Then, we have*

$$B = E \cdot A.$$

Recall that given any matrix A, one can perform a sequence of elementary row operations on it and transform it into a row reduced echelon matrix. Thus, the above theorem has the following corollary:

COROLLARY 7.4. *For any $A \in M_{m\times n}(\mathbb{R})$, there exists a matrix $E \in M_{m\times n}(\mathbb{R})$ such that EA is in row reduced echelon form. Also, E is of the form $E_1 \cdots E_k$ where each E_i can be obtained from I_n by an elementary row operation.*

REMARK 7.5. One can easily prove an analogue for "column operations". First, of course, we need to define *elementary column operations* which are analogous to the elementary operations. I will leave that as an easy exercise. Then one can prove that if B is obtained from A by a sequence of elementary column operations, then $B = AE$ where E is obtained from I_n by the same column operations. The proof is entirely similar to the one given above.

Invertible matrices:

In the previous lecture, we saw that a system of m linear equations in n variables and real coefficients can be represented by a single matrix equation of the form $AX = B$ where A is a $m \times n$ matrix with real entries, X is an $n \times 1$ matrix with variable entries, and B is an $m \times 1$ matrix with real entries. If one momentarily forgets that these are matrices, one might be tempted to divide by A on both sides to compute the value of X. Of course, we cannot always do this since it is not possible to "divide" by a matrix in general. However, we will now try to see when this does make sense.

What does it mean to "divide" by a number c? To divide by c is the same as multiplying by $1/c$, which is called the *multiplicative inverse* of c. What is the multiplicative inverse of c? It is the unique number such that its product with c is equal to 1. We will try to create an analogous concept for a matrix A. However, we run into a small obstacle when we try to define the multiplicative inverse of a matrix. The role of 1 is played by the identity matrix. For a matrix B to be the multiplicative inverse of A, should we require AB to be equal to the identity matrix or should we require BA to be equal to the identiy matrix?

The situation is further complicated by the fact that there are identity matrices of different sizes. If A is an $m \times n$ matrix, the matrix AB can be a square matrix only if B is an $n \times m$ matrix. In this case, AB will be an $m \times m$ matrix. Similarly, BA can be a square matrix only if B is an $n \times m$ matrix, but in this case, BA will be an $n \times n$ matrix. So should we require that $AB = I_m$ and $BA = I_n$? As it turns out, if $m \neq n$, there cannot exist a matrix B with such properties. (This will become clear later in the course.) Hence, we will only focus on square matrices.

DEFINITION 7.6. Let n be a positive integer and let $A \in M_{n\times n}(\mathbb{R})$.

(1) A matrix $B \in M_{n\times n}(\mathbb{R})$ is said to be the *left inverse* of A if $BA = I_n$.
(2) A matrix B is said to be the *right inverse* of A if $AB = I_n$.
(3) A matrix B is said to be the *inverse* of A if it is both the left inverse as well as the right inverse of A. If a matrix A has an inverse, we say that it is *invertible*.

Thus, a priori, it seems as if we have defined three concepts. However, we will see that these notions are the same.

LEMMA 7.7. *Suppose $A \in M_{n\times n}(\mathbb{R})$ has a left inverse B and a right inverse C. Then $B = C$.*

PROOF. By definition, we have $BA = I_n$ and $AC = I_n$. Thus,

$$B = BI_n = B(AC) = (BA)C = I_nC = C.$$

□

LEMMA 7.8. *Suppose a matrix A has a left inverse B. Then, for any matrix $Y \in M_{n\times 1}(\mathbb{R})$, there exists a matrix $X \in M_{n\times n}(\mathbb{R})$ such that $AX = Y$.*

PROOF. We will prove this by contradiction. Suppose Y is such that there is no X for which $AX = Y$. Suppose $A = (a_{ij})_{i,j}$ and $Y = (y_j)_{j,1}$. To find an X such that $AX = Y$ is equivalent to finding a solution to the following system:

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & y_1 \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & y_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{n1}X_1 & + & a_{n2}X_2 & + & \cdots & & a_{nn}X_n & = & y_n \end{array}$$

Thus, if we assume that there does not exist any such X, we conclude that the above system has no solutions.

Let us recall how we solve systems of linear equations. We form the augmented matrix $[A|Y]$ and perform row operations on it to transform A into a row reduced echelon matrix. Suppose that these operations turn the augmented matrix $[A|Y]$ into the augmented matrix $[B|Y']$ where B is in row reduced echelon form. Then, we know that the system fails to have a solution only if B has at least one zero row and Y' has a non-zero entry in the corresponding row. Thus, we see that the row reduced form of A has a zero row at the bottom.

Now consider the following system:

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & 0 \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{n1}X_1 & + & a_{n2}X_2 & + & \cdots & & a_{nn}X_n & = & 0 \end{array}$$

Once again, we transform the system using the row reduction algorithm. This time, we end up with the augmented matrix $[B|\mathbf{0}]$ where $\mathbf{0}$ denotes the $n \times 1$ matrix in which every entry is equal to 0. Clearly, this system always has a solution. Moreover, note that B has at most $n-1$ pivots. Since it has n columns, it follows there exists a column which does not have a pivot. The variable corresponding to this column can take arbitrary values (i.e. it is a *free variable*). Thus, we see that there exists an $n \times 1$ matrix K such that $K \neq \mathbf{0}$, but $AK = \mathbf{0}$.

However, now observe that

$$K = I_n K = (BA)K = B(AK) = B\mathbf{0} = \mathbf{0}.$$

This is a contradiction since we know that $K \neq \mathbf{0}$. This shows that our initial assumption, that there exists no X for which $AX = Y$, must be wrong. This proves the lemma. □

LEMMA 7.9. *Let $J \in M_{n\times n}(\mathbb{R})$ be such that for any $X \in M_{n\times 1}(\mathbb{R})$, we have $JX = X$. Then $J = I_n$.*

PROOF. Let $E_i \in M_{n\times 1}(\mathbb{R})$ be the matrix having 1 in the i-th row and 0 elsewhere. Then it is easy to check that JE_i is equal to the i-th column of J (check this!). By assumption, $JE_i = E_i$. Thus, E_i is the i-th column of J for every i. This shows that $J = I_n$. □

PROPOSITION 7.10. *Suppose $A \in M_{n\times n}(\mathbb{R})$ has a left inverse B. Then B is also a right inverse for A.*

PROOF. Choose any $Y \in M_{n\times 1}(\mathbb{R})$. By Lemma 7.8, there exists an $X \in M_{n\times 1}(\mathbb{R})$ such that $AX = Y$. Since $BA = I_n$, we have

$$X = I_n X = (BA)X = BY.$$

Thus,

$$(AB)Y = A(BY) = AX = Y.$$

By Lemma 7.9, we see that $AB = I_n$. □

COROLLARY 7.11. *Suppose $A \in M_{n\times n}(\mathbb{R})$ has a right inverse B. Then B is also a left inverse for A.*

PROOF. Since $AB = I_n$, A is a left inverse for B. Thus, by Proposition 7.10, A is also a right inverse for B. Hence $BA = I_n$. □

This shows that for square matrices, the notions of left inverse, right inverse and inverse are all equivalent. (Please note that this only happens for square matrices!)

Now let us note some basic properties of inverses.

LEMMA 7.12. *Let $A \in M_{n\times n}(\mathbb{R})$ and let B_1 and B_2 be inverses of A. Then $B_1 = B_2$.*

PROOF. $B_1 = I_n B_1 = (B_2 A)B_1 = B_2(AB_1) = B_2 I_n = B_2$. □

Thus, if a matrix has an inverse, it is unique. This justifies the following notation:

NOTATION 7.13. Let $A \in M_{n\times n}(\mathbb{R})$. If the inverse of A exists, it will be denoted by A^{-1}.

LEMMA 7.14. *Suppose A and B are invertible matrices. Then AB is also invertible and $(AB)^{-1} = B^{-1}A^{-1}$.*

PROOF. $(B^{-1}A^{-1})(AB) = B^{-1}(AA^{-1})B = B^{-1}I_n B = BB^{-1} = I_n$. □

LEMMA 7.15. *Let E be a matrix obtained from I_n by performing an elementary row operation. Then E is an invertible matrix.*

PROOF. Suppose E is obtained from I_n by performing a certain elementary row operation Op_1. Recall that the elementary row operations are reversible. Thus, there exists an elementary row operation Op_2 such that if Op_1 and Op_2 are both performed on a matrix, the matrix remains unchanged. Let E' by the matrix obtained by applying Op_2 on I_n. Thus, we see that for any matrix A (which has n rows), we have $EE'A = A$. In particular, taking $A = I_n$, we see that $EE' = I_n$. Thus, E is invertible. □

LEMMA 7.16. *Let $A \in M_{n\times n}(\mathbb{R})$ be a* row reduced echelon matrix. *Then the following two conditions are equivalent:*

(1) *$A = I_n$.*
(2) *A has no zero rows.*

PROOF. Clearly, if $A = I_n$, it has no zero rows. Thus, (1) $\implies$ (2).

Suppose A has no zero rows. Then every row has a pivot. Thus, the number of pivots is equal to n. Thus every column also has a pivot. The only $n \times n$ row reduced echeleon matrix having a pivot in every row and every column is I_n. (Do you see why?) □

THEOREM 7.17. *Let $A \in M_{n\times n}(\mathbb{R})$ and let B be the row reduced echelon matrix obtained from A by a sequence of elementary row operations. Then A is invertible if and only if $B = I_n$.*

PROOF. We saw in Corollary 7.4 that B is of the form EA for some $E = E_1 \cdots E_k$, where each E_i has been obtained from I_n by an elementary row operation. By Lemma 7.15, we know that each E_i is invertible. By Lemma 7.14, E is invertible.

First suppose that $B = I_n$. Then $A = EB = EI_n = E$, which is invertible. This proves one half of our theorem.

On the other hand, suppose A is invertible. Then if $B \neq I_n$, by Lemma 7.16, B must have a zero row. By the definition of matrix product, for any matrix C, the matrix BC must have a zero row. Thus $BC \neq I_n$. Thus B is not invertible. However, as we saw above, $B = EA$ where E is invertible. As A is assumed to be

invertible, Lemma 7.14 implies that B is also invertible. This is a contradiction. Thus, $B = I_n$. This completes the proof of the theorem. □

This gives us an algorithm to check whether a given matrix is invertible and also to compute its inverse if it exists. Indeed, given any $A \in M_{n\times n}(\mathbb{R})$ we use the row reduction algorithm to transform it into a row reduced echelon matrix B. If $B \neq I_n$, we may conclude that A is not invertible. If $B = I_n$, we look at the list of elementary row operations which were used to transform A into I_n and perform them in the same order on I_n. If I_n is transformed into B by these operations, it follows that $B = A^{-1}$.

LECTURE 8

Determinants

Note: The notes for this lecture are somewhat demanding and contain far more details than were presented in the lecture. However, you may choose to ignore the proofs for now if they seem too long and demanding. You may simply focus on understanding the definitions and the statements of the results.

For any square matrix with entries in $\mathbb{R}$, we can associate a real number which is called the *determinant* of a matrix. Thus, for any positive integer n, the determinant is a function from $M_{n\times n}(\mathbb{R})$ to $\mathbb{R}$. This function has some important properties, which we will now explore. However, the proofs of these properties will involve a technique called *the principle of mathematical induction*. If you are not familiar with the technique of mathematical induction, you may review the appendix at the end of this lecture.

There are many ways to define determinants. We will choose to define them by a formula. The formula for the determinant of the $n \times n$ matrix is given in terms of the determinant of the $(n-1) \times (n-1)$ matrix. Thus, the definition is inductive in nature.

DEFINITION 8.1. Let $n \geqslant 1$ be an integer. Let $A \in M_{n\times n}(\mathbb{R})$. We define the determinant of A, denoted by $\det(A)$ as follows:

(1) Suppose $n = 1$. Then $A = [a]$ for some $a \in \mathbb{R}$. In this case, we define $\det(A) = a$.
(2) Suppose that determinants have been defined for $(n-1)\times(n-1)$ matrices. For the given matrix $A = (a_{ij})_{i,j}$ for any pair of indices i, j satisfying $1 \leqslant i, j \leqslant n$, let A_{ij} denote the $(n-1) \times (n-1)$ matrix obtained by deleting the i-th row and j-th column of A. Then, we define

$$\begin{aligned}\det(A) &= a_{11}\det(A_{11}) - a_{12}\det(A_{12}) + \cdots + (-1)^{n-1}\det(A_{1n}) \\ &= \sum_{i=1}^{n}(-1)^{i-1}a_{1i}\det(A_{1i}).\end{aligned}$$

Given a matrix A, any matrix obtained by deleting some of its rows and columns is said to be a *minor* of A. Hence, the above formula is called the formula for *expansion by minors*. We have used terms in the first row and the minors obtained by deleting the row and column containing each of those terms. Hence, we say that this is the formula for *expansion of the determinant by the first row*. One can also write down the formula for expansion by any of the other rows or even by any column of the matrix. We will look into this later. For now, the formula for expansion by the first row is our definition of the determinant.

EXAMPLES 8.2. We will interpret the formula for small values of n.

(1) For $n = 1$, there is not much to see: $\det([a]) = a$.
(2) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a 2×2 matrix. Then, by definition

$$\begin{aligned}\det(A) &= a \cdot \det([d]) - b \cdot \det([c]) \\ &= ad - bc.\end{aligned}$$

(3) Now let us look at the case $n = 3$.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

By definition

$$\begin{aligned} \det(A) &= a_{11} \det \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} - a_{12} \det \begin{bmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{bmatrix} + a_{13} \det \begin{bmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix} \\ &= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}). \end{aligned}$$

Before we state the basic properties of the determinant, let us observe something about the formula. First let us count the number of terms in the expansion. Suppose that the number of terms in the expansion of the $n \times n$ determinant is $f(n)$. The number of terms in the expansion of A is equal to the sum of the number of terms in the expansion of $A_{11}, A_{12}, \ldots, A_{1n}$. Thus, we see that $f(n) = n \cdot f(n-1)$. Using the principle of induction, one can prove from this that

$$f(n) = 1 \times 2 \times 3 \times \cdots \times n.$$

This number is denoted by $n!$ (read as "n factorial").

Secondly, observe that each of the $n!$ terms is a product of entries of the matrix. How many entries appear in each product? The number of entries appearing in the terms in the expansion of A is exactly one more than the number of entries appearing in the expansions of A_{11}, A_{12}, etc. Thus, using the principle of induction, we may verify that each of the $n!$ terms in the expansion of the determinant of an $n \times n$ matrix is the product of exactly n terms.

Our third observation is a little more interesting. In each of the $n!$ terms, there is exactly one term from each row and exactly one term from each column. You can verify this easily using induction. As an example, look at the two terms appearing in the expansion of the 2×2 matrix. The first term is $a_{11}a_{22}$. Here a_{11} appears in the first row and a_{22} appears in the second row. Also a_{11} appears in the first column and a_{22} appears in the second column. Thus, the first term certainly has the above-mentioned property. You can also easily verify this for the term $a_{12}a_{21}$.

We summarize our observations:

(Ob1) The expansion of the determinant of an $n \times n$ matrix has exactly $n!$ terms.
(Ob2) Each of the $n!$ terms is a product of exactly n entries of the matrix.
(Ob3) Each term has exactly one entry from each row and exactly one entry from each column.

We will now derive some basic properties of determinants. The proofs of some of these statements are deliberately a little sketchy. While they are essentially complete, I have avoided writing everything in complete detail since it will make the topic seem too burdensome. However, if you are interested, you should be able to write complete versions of the proofs based on what is written below.

LEMMA 8.3. $\det(I_n) = 1$.

PROOF. This is an easy consequence of the definition. To prove it rigorously, one may use induction on n. I will leave this as an exercise. □

LEMMA 8.4. *Let $A \in M_{n\times n}(\mathbb{R})$ and let B be the matrix obtained by multiplying one of the rows or one of the columns of A by some $x \in \mathbb{R}$. Then* $\det(B) = x \det(A)$.

PROOF. This follows from (Ob3). □

Notice that this tells us that if any single row or column of a matrix has only zero entries, the determinant of the matrix is equal to 0.

LEMMA 8.5. *Suppose B and C are two $n \times n$ matrices. Let $1 \leqslant i \leqslant n$ and suppose that for any $j \neq i$, the j-th rows of B and C is identical. Suppose that A is the $n \times n$ matrix such that:*

(1) *for every $j \neq i$, the j-th row of A is equal to the j-th row of B (and hence also of C), and*
(2) *the i-th row of A is equal to the (term by term) sum of the i-th rows of B and C.*

Then $\det(A) = \det(B) + \det(C)$.

For the sake of clarity, let us write down an example with 3×3 matrices. Suppose

$$B = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ b_{21} & b_{22} & b_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},$$

$$C = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ c_{21} & c_{22} & c_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

and

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ b_{21} + c_{21} & b_{22} + c_{22} & b_{23} + c_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

Then, the lemma says that $\det(A) = \det(B) + \det(C)$.

PROOF. This lemma too follows from (Ob2). Indeed, suppose that in the expansion of the determinant of A, there exists a term that contains the (i, j)-entry of A. Note that this term cannot contain any other entry from the i-th row or j-th column. Thus, this entry looks like $x(b_{ij} + c_{ij})$ where x is a product of entries which do not lie in the i-th row or j-th column. But then for any $j \neq i$, the j-th rows of A, B and C are identical. Thus, the terms xb_{ij} and xc_{ij} occur in the expansions of the determinants of B and C respectively. The equality $\det(A) = \det(B) + \det(C)$ can be proved by matching the terms on both sides in this manner. □

The analogous statement for columns is also true and the proof is identical. Lemmas 8.4 and 8.5 are expressed by saying that "the determinant is *linear* in the rows of the matrix". The word "linear" refers to the fact that the entries from every row only occur with degree 1 in each term in the expansion of the product (which is the fact which was crucially used in the proofs of these lemmas).

We now wish to prove that if two rows of the matrix are switched, the determinant changes sign (i.e. it gets multiplied by (-1)). The proof of this fact is a little harder and so we will go about it in steps. Let us fix two indices i and j, satisfying $1 \leqslant i, j \leqslant n$ and $i \neq j$. Consider the following two statements:

(Alt1) If the matrix B is obtained from the matrix A by interchanging the i-th and j-the rows, then $\det(A) = -\det(B)$.
(Alt2) If the i-th and j-th rows of a matrix A are identical, then $\det(A) = 0$.

We will observe that these two statements are equivalent, i.e. they imply each other. To show this, let us write the matrices as columns in which the entries are actually rows of the matrix. Thus, the matrix A is written as

$$A = \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}$$

where R_i is the row $(a_{i1}, \ldots, a_{in})$. Let us show the equivalence of (Alt1) and (Alt2) assuming $i = 1$ and $j = 2$ (the proof of the general case is absolutely identical).

The proof of (Alt1) $\implies$ (Alt2) is very easy. Indeed, let us assume (Alt1) and suppose that the first and second rows of A are identical and that B is obtained by interchanging them. Then $B = A$, but (Alt1) implies that $\det(A) = -\det(B)$. Thus, $\det(A) = -\det(A)$ which implies that $\det(A) = 0$.

Now assume (Alt2). Then let C be the following matrix:

$$C = \begin{bmatrix} R_1 + R_2 \\ R_1 + R_2 \\ \vdots \\ R_n \end{bmatrix}$$

By Lemma 8.5, we see that

$$\det(C) = \det \begin{bmatrix} R_1 \\ R_1 + R_2 \\ \vdots \\ R_n \end{bmatrix} + \begin{bmatrix} R_2 \\ R_1 + R_2 \\ \vdots \\ R_n \end{bmatrix}.$$

Again, by Lemma 8.5,

$$\det \begin{bmatrix} R_1 \\ R_1 + R_2 \\ \vdots \\ R_n \end{bmatrix} = \det \begin{bmatrix} R_1 \\ R_1 \\ \vdots \\ R_n \end{bmatrix} + \det \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}.$$

Here, the first term is equal to 0 since we are assuming (Alt2). Thus,

$$\det \begin{bmatrix} R_1 \\ R_1 + R_2 \\ \vdots \\ R_n \end{bmatrix} = \det(A).$$

By a similar argument

$$\det \begin{bmatrix} R_2 \\ R_1 + R_2 \\ \vdots \\ R_n \end{bmatrix} = \det(B).$$

Thus, $\det(C) = \det(A) + \det(B)$. However, since C has two identical rows, we know that $\det(C) = 0$. Thus $\det(A) = -\det(B)$. Thus, we see that (Alt2) implies (Alt1).

Thus, it will suffice to prove (Alt2) for any pair of indices (i, j). To begin with, we prove it for adjacent pairs, i.e pairs of the form $(i, i + 1)$.

LEMMA 8.6. *If two adjacent rows of an $n \times n$ matrix A are identical, then* $\det(A) = 0$.

PROOF. This statement is proved by induction on n. The statement does not have much relevance to the case $n = 1$, and so we look at the case $n = 2$. It is easy to verify by explicit calculation that if a 2×2 matrix has identical rows, its determinant is equal to 0.

Now suppose that the result is known for $(n-1) \times (n-1)$ matrices. Suppose that the i-th and $(i+1)$-th rows are identical. If $i > 1$, this immediately implies that in the matrices A_{1i}, two adjacent rows are identical. Then, the induction hypothesis says that $\det(A_{1i}) = 0$ for every i and so $\det(A) = 0$.

Suppose that the first and second rows are identical. For any pair i, j satisfying $1 \leqslant i, j \leqslant n$ and $i \neq j$, let B_{ij} denote the $(n-2)\times(n-2)$ minor obtained by deleting the rows 1 and 2 and the columns i and j of A. Then, the expansion of $a_{1i}\det(A_{1i})$ contains the term $a_{1i}a_{2j}\det(B_{ij})$ and the expansion of $a_{1j}\det(A_{1j}$ contains the term $a_{1j}a_{2i}\det(B_{ij})$. But as the first two rows are assumed to be identical, we see that $a_{1i} = a_{2i}$ and $a_{1j} = a_{2j}$. Thus, the terms $a_{1i}a_{2j}\det(B_{ij})$ and $a_{1j}a_{2i}\det(B_{ij})$ are identical. If one can check that they come with opposite signs, it will follow that they cancel each other out. I will leave this as an interesting exercise. (Drawing a picture of the matrix may help you figure this out.) In this manner, one can show that all the terms cancel out and so $\det(A) = 0$. □

As we have already proved that (Alt2) implies (Alt1) for any pair of indices, we have also obtained the following lemma:

LEMMA 8.7. *Let A be an $n \times n$ matrix and suppose B is obtained from A by switching two adjacent rows. Then* $\det(A) = -\det(B)$.

Now, suppose we want to switch two non-adjacent rows. This can be achieved by successively switching adjacent pairs. For instance, suppose a matrix has three rows and I want to switch the first and the third row. This can be achieved by switching in the following manner.

$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \end{bmatrix} \rightsquigarrow \begin{bmatrix} R_2 \\ R_1 \\ R_3 \end{bmatrix} \rightsquigarrow \begin{bmatrix} R_2 \\ R_3 \\ R_1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} R_3 \\ R_2 \\ R_1 \end{bmatrix}$$

Observe that this required an odd number of adjacent row switches. For each switch the sign of the determinant changed once. Thus, we finally end up with a minus sign.

Suppose we wish to switch the i-th row and the j-th row with $i < j$. We start by switching the i-th row with the $(i+1)$-th row and keep switching it forward until it gets to the j-place. This requires $(j - i)$ adjacent row switches. At this point, the j-th row will be in the $(j - 1)$-th place. Thus, to move it to the i-th place will require $(j - 1 - i)$ adjacent row switches. Thus, we need a total of $2(j - 1) - 1$ adjacent row switches to switch the i-th and j-th row. As this is an odd number, we finally end up with a minus sign. This shows that

LEMMA 8.8. *Let A be an $n \times n$ matrix and suppose B is obtained from A by switching any two rows. Then* $\det(A) = -\det(B)$.

As we have observed, (Alt1) implies (Alt2) for any pair of indices. Thus, we also obtain

LEMMA 8.9. *If any two rows of an $n\times n$ matrix A are identical, then* $\det(A) = 0$.

Observe that we have seen what two of the elementary row operations do to the determinant of a matrix. Now let us look at the last remaining operation:

LEMMA 8.10. *Let A be an $n \times n$ matrix and let B by obtained from A by performing the operation $R_i + xR_j$ for some $x \in \mathbb{R}$. Then* $\det(B) = \det(A)$.

PROOF. We will write the proof for $i = 1$ and $j = 2$. The proof in the general case is entirely identical. As before, we write the matrices as columns in which the entries are the rows of the matrices.

$$B = \begin{bmatrix} R_1 + xR_2 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}$$

Now we use Lemma 8.5 to obtain the following equality:

$$\det\begin{bmatrix} R_1 + xR_2 \\ R_2 \\ \vdots \\ R_n \end{bmatrix} = \det\begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix} + \det\begin{bmatrix} xR_2 \\ R_2 \\ \vdots \\ R_n \end{bmatrix} = \det(A) + \det\begin{bmatrix} xR_2 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}$$

Now, observe that by Lemma 8.4, we have

$$\det\begin{bmatrix} xR_2 \\ R_2 \\ \vdots \\ R_n \end{bmatrix} = x \cdot \det\begin{bmatrix} R_2 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}$$

which is equal to 0 by Lemma 8.9. □

Thus, we now know how various row operations affect the determinant:

(1) Adding a constant multiple of a row to another leaves the determinant unchanged.
(2) Multplying one of the row by a constant x has the effect of multiplying the determinant by x. (This works even if $x = 0$.)
(3) Switching two rows has the effect of multiplying the determinant by -1.

Note that we have observed the analogue of (2) for columns as well. Actually the analogues of (1) and (2) also hold for columns, as we will see later.

8.A. Mathematical Induction

Suppose we want to prove the following statement:

> For any positive integer n, the sum of all integers i satisfying $1 \leqslant i \leqslant n$ is $n(n+1)/2$.

Since this is a statement about the integer n, we call this statement $P(n)$. Let us see how we could prove this statement. We observe that

$$1 + 2 + \cdots + n = (1 + 2 + \cdots + (n-1)) + n.$$

Suppose we assume that $P(n-1)$ is true. In other words, suppose we already know that

$$1 + 2 + \cdots + (n-1) = \frac{(n-1)(n-1+1)}{2} = \frac{n(n-1)}{2}.$$

Then,

$$1+2+\cdots+n = (1+2+\cdots+(n-1))+n = \frac{n(n-1)}{2}+n = n(\frac{n-1}{2}+1) = \frac{n(n+1)}{2}.$$

Note that this is <u>not</u> a proof of the statement $P(n)$ yet. We have only proved that <u>if</u> the statement $P(n-1)$ is true, <u>then</u> the statement $P(n)$ is also true.

So, suppose I want to check whether $P(5)$ is true. The above argument tells me that it would be enough to verify $P(4)$. But then to verify $P(4)$, it would be enough to very $P(3)$. To verify $P(3)$ it would be enough to verify $P(2)$. To verify $P(2)$ it would be enough to verify $P(1)$. But $P(1)$ is very easy to verify. Indeed, it just says that $1 = 1$, which is evidently true. Thus, we conclude that $P(5)$ is true.

Intuitively, it is clear that this method can be applied to prove $P(n)$ for any n. For instance, if I want to prove $P(100)$, I would have to write the following:

To verify $P(100)$, it is enough to verify $P(99)$. To verify $P(99)$, it is enough to verify $P(98)$. ... (*and so on, through all integers between 100 and 1*) ... To verify $P(2)$ it is enough to verify $P(1)$. But $P(1)$ states $1 = 1$, which is evidently true.

The argument will get longer as we try to prove $P(n)$ for larger and larger numbers, but the method of proof is quite clear and it is "obvious" that it will

work. However, one must admit that as a written proof, it is not rigorous. The phrase "and so on" might be enough to convince you of the validity of the argument, but it does not represent a complete argument.

Mathematical induction is a principle that allows us to make this rigorous. The principle can be stated as follows:

> *Mathematical Induction:* Let $S(n)$ be a statement about the integer n. Suppose that the statement $S(k_0)$ is known to be true for an integer k_0. Suppose it is also known that for any $k > k_0$, the statement $S(k)$ implies the statement $S(k+1)$. Then, the statement $S(n)$ is true for all integers $n \geqslant k_0$.

Clearly, if we accept this principle as rigorous, the above argument with the phrase "and so on" can be rewritten in a rigorous form. This principle is a fundamental property of the integers. A discussion of why this principle should be accepted would lead us into the question of what the integers really are. We will not treat this issue in this course. We will simply accept this principle as a fact and use it in our proofs. As an example, we prove the following rigorously:

THEOREM. For any positive integer n, the sum of all integers i satisfying $1 \leqslant i \leqslant n$ is $n(n+1)/2$.

PROOF. We will prove this using the principle of mathematical induction. We first verify this statement for $n = 1$. In this case, we wish to prove that $1 = 1$, which is certainly true.

Suppose the result is known for $n = k$. We wish to prove it for $n = k + 1$. So, we may assume that

$$1 + \cdots + (n-1) = \frac{(n-1)((n-1)+1)}{2} = \frac{n(n-1)}{2}.$$

Then

$$1 + \cdots + (n-1) + n = \frac{n(n-1)}{2} + 1 = \frac{n(n+1)}{2}.$$

This completes the proof of the inductive step. Thus, the principle of mathematical induction imples that the statement is true for all integers $\geqslant 1$. □

Proofs involving induction should be written in this format:

(1) Check the statement for the initial integer k_0 (which is equal to 1 in the above example).
(2) Check that if the statement is true for an integer $k \geqslant k_0$, then it is true for the integer $k + 1$. (Note that it is very important that this part of the argument works for $k = k_0$, and not just $k > k_0$. Otherwise, we have no way to deduce the statement for $k_0 + 1$.)

Part (2) of the argument is referred to as the *inductive step*. The assumption that the statement is true for the integer k is referred to as the *inductive hypothesis*.

LECTURE 9

Further properties of determinants

We begin by recalling some facts we have established so far. Then we will put them together to obtain the proofs for two of the most important properties of determinants.

Let n be a positive integer. Then, we know the following facts about $n \times n$ matrices.

Facts:

(a) Let A and B be $n \times n$ matrices.
  (i) If B is obtained from A by performing an operation of the form $R_i + xR_j$ for some $x \in \mathbb{R}$, then $\det(A) = \det(B)$.
  (ii) If B is obtained from A by performing an operation of the form xR_i for $x \in \mathbb{R}$, then $\det(B) = x\det(A)$. (Note that generally when we refer to elementary row operations, we require that $x \neq 0$, but this particular result holds even if we take $x = 0$.)
  (iii) If B is obtained from A by performing an operation of the form $R_i \leftrightarrow R_j$, then $\det(B) = -\det(A)$.

(b) $\det(I_n) = 1$.

(c) Any matrix can be reduced to a matrix in row reduced echelon form using the row reduction algorithm (i.e. by a sequence of elementary row transformations).

(d) A matrix is invertible if and only if it is transformed into the identity matrix by the row reduction algorithm. If it is not invertible, its row reduced echelon form has a zero row.

(e) If a matrix B is obtained from a matrix A by performing an elementary row operation, and if E is the matrix obtained from I_n after performing the same row operation, then $B = EA$.

LEMMA 9.1. *Let A be a square matrix and let B be a matrix obtained from A by performing an elementary row operation. Then* $\det(B)$ *is a non-zero multiple of* $\det(A)$. *In other words, there exists a non-zero real number α such that* $\det(B) = \alpha \cdot \det(A)$.

PROOF. By Fact (a), part (i), if B is obtained from A by the operation $R_i + xR_j$ for some $x \in \mathbb{R}$, then $\det(B) = \det(A)$. Thus, in this case we obtain the result with $\alpha = 1$.

If B is obtained from A by the operation xR_i for some $x \in \mathbb{R}$, $x \neq 0$, then by Fact (a), part (ii), $\det(B) = x\det(A)$. Thus, in this case, we obtain the result with $\alpha = x \neq 0$.

Finally, if B is obtained from A by an operation of the form $R_i \leftrightarrow R_j$, then $\det(B) = -\det(A)$. Thus, we obtain the result with $\alpha = -1$.

Thus, we have verified the result for all the elementary row operations. □

We are now able to put together all these results to deduce an important criterion for invertibility of matrices.

THEOREM 9.2. *A square matrix is invertible if and only if its determinant is non-zero.*

PROOF. Let A be a given $n \times n$ matrix. By Fact (c), we know that there exist finitely many elementary row operations, which we denote by $Op_1, \ldots, Op_k$ such that performing them sucessively on A transforms it into a row reduced echelon matrix B. We will show that $\det(A)$ is non-zero if and only if $\det(B)$ is non-zero.

Suppose that B_1 is the matrix obtained from A by performing Op_1. For each i satisfying $2 \leqslant i \leqslant k$, let B_i be the matrix obtained by performing Op_i on the matrix B_{i-1}. We will prove by induction that for each i satisfying $1 \leqslant i \leqslant n$, there exists a real number $\alpha_i \neq 0$ such that $\det(B_i) = \alpha_i \det(A)$.

For $i = 1$, B_1 is obtained from A by performing a single elementary row operation. Thus, Lemma 9.1 shows that there exists some $\alpha_1 \neq 0$ such that $\det(B_1) = \alpha_1 \det(A)$.

Suppose that $i \geqslant 1$ and it is know that $\det(B_i) = \alpha_i \det(A)$. Then, Lemma 9.1 implies that there exists a real number $\beta_{i+1} \neq 0$ such that $\det(B_{i+1}) = \beta_{i+1} \det(B_i)$. Thus,

$$\det(B_{i+1}) = \beta_{i+1} \det(B_i) = \beta_{i+1}\alpha_i \det(A).$$

Thus, if we define $\alpha_{i+1} = \beta_{i+1}\alpha_i$, then we obtain the equality

$$\det(B_{i+1}) = \alpha_{i+1} \det(A).$$

This completes the inductive step and proves our claim. (Observe that here induction has been used to prove something about a finite set of integers rather than the entire set of integers.)

Thus, in particular, taking $i = k$, we see that $\det(B) = \alpha_k \det(A)$ for some $\alpha_k \neq 0$. Thus, it follows that $\det(B)$ is non-zero if and only if $\det(A)$ is non-zero.

We know that $\det(A)$ is invertible if and only if $B = I_n$, in which case $\det(B) = 1 \neq 0$. If $B \neq I_n$, it has a zero row and hence $\det(B) = 0$. This completes the proof. □

LEMMA 9.3. *Let A be an $n \times n$ matrix and let E be a matrix obtained by performing an elementary row operation on I_n. Then* $\det(EA) = \det(E) \cdot \det(A)$.

PROOF. This is an immediate consequence of Fact (a). Indeed, the essence of the argument is already present in the proof of Lemma 9.1. We write the argument in detail for the sake of completeness. Let $B = EA$. Then B is obtained from A by the same operation that was performed on I_n to obtain E.

If E is obtained from I_n by performing the operation $R_i + xR_j$, then $\det(E) = \det(I_n) = 1$. Similarly, performing this operation on A, we get $\det(B) = \det(A)$. Thus, $\det(B) = \det(E) \cdot \det(A)$ in this case.

If E is obtained from I_n by performing the operation xR_i for some $x \neq 0$, then $\det(E) = x \det(I_n) = x$. Similarly, performing this operation on A, we get $\det(B) = x \det(A)$. Thus, $\det(B) = \det(E) \cdot \det(A)$ in this case.

If E is obtained from I_n by performing the operation $R_i \leftrightarrow R_j$, then $\det(E) = -\det(I_n) = -1$. Similarly, performing this operation on A, we get $\det(B) = -\det(A) = (-1) \cdot \det(A)$. Thus, $\det(B) = \det(E) \cdot \det(A)$ in this case.

Thus, we have verified the result for all the elementary row operations. □

THEOREM 9.4. *Let A and B be $n \times n$ matrices. Then* $\det(AB) = \det(A) \cdot \det(B)$.

PROOF. If A is invertible, then we can write $A = E_1 \cdots E_k$ where each E_i is obtained from I_n by performing some elementary row operation. Then, by repeatedly

using Lemma 9.3, we get

$$\begin{aligned}\det(AB) &= \det(E_1 \cdots E_k \cdot B)\\ &= \det(E_1) \cdot \det(E_2 \cdots E_k \cdot B)\\ &= \det(E_1) \cdot \det(E_2) \cdot \det(E_3 \cdots E_k \cdot B)\\ &\quad \textit{(and so on)}\\ &= \det(E_1) \cdots \det(E_k) B.\end{aligned}$$

(Exercise: Can you write the above argument rigorously, i.e. avoiding the phrase "and so on", by using induction?)

Actually, if we apply the above argument for $B = I_n$, we get

$$\det(A) = \det(E_1) \cdots \det(E_k).$$

Thus, we see that for any matrix B,

$$\det(AB) = \det(E_1) \cdots \det(E_k) \cdot \det(B) = \det(A) \cdot \det(B)$$

if A is invertible.

If A is not invertible, let C denote its row reduced echelon form. Then, there exist matrices $E_1, \ldots E_k$ such that each E_i is obtained from I_n by an elementary row operation and such that $A = E_1 \cdots E_k \cdot C$. Then

$$AB = E_1 \cdots E_k \cdot (CB).$$

As C is a square matrix in row reduced echelon form and it is not equal to the identity matrix, it must have a zero row. Thus, CB also has a zero row and so $\det(CB) = 0$. As the matrix $E_1 \cdots E_k$ is invertible, the first part of the proof shows that

$$\det(AB) = \det(E_1 \cdots E_k) \cdot \det(CB) = 0.$$

On the other hand, as A is not invertible, we also have $\det(A) = 0$. Thus, in this case also, we have $\det(AB) = \det(A) \cdot \det(B)$. This completes the proof. □

LECTURE 10

Cramer's rule

In this lecture, we will see how determinants can be used to obtain a formula for the inverse of a square matrix. As a consequence, we will be able to deduce the well-known Cramer's rule for solving systems of n-linear equations in n unknowns. However, first we need to deal with a couple of preliminary topics.

Transposes:

Given an $m \times n$ matrix A, we can form an $n \times m$ matrix called the *transpose of* A, denoted by A^{tr}, by just interchanging the rows and columns of A. Another way of saying this is that we reflect A along the diagonal line that begins at the top left corner. A precise way of saying this might be to write that if $A = (a_{ij})_{i,j}$ (i.e. if the (i,j)-entry of A is a_{ij}), then $A^{tr} = (a_{ji})_{i,j}$ (i.e the (i,j)-entry of A^{tr} is a_{ji}).

EXAMPLE 10.1. Some examples of transposes:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \qquad A^{tr} = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 8 & 7 \end{bmatrix} \qquad B^{tr} = \begin{bmatrix} 1 \\ 8 \\ 7 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 2 \\ -1 & 4 & 1 \end{bmatrix} \qquad C^{tr} = \begin{bmatrix} 1 & 4 & -1 \\ 2 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix}$$

It is important to know how this operation behaves with respect to multiplication (see part (b) in the following lemma).

LEMMA 10.2. *Let $A \in M_{m\times n}(\mathbb{R})$ and $B \in M_{n\times p}(\mathbb{R})$. Then:*

(a) $(A^{tr})^{tr} = A$.
(b) $AB = B^{tr}A^{tr}$.

PROOF. Part (a) follows immediately from the definition. The proof of part (b) is left as an easy exercise. □

LEMMA 10.3. *Let E be a matrix obtained from I_n by an elementary row operation. Then* $\det(E) = \det(E^{tr})$.

PROOF. Suppose E is obtained from I_n by the operation $R_i + xR_j$. Then E has 1's on the diagonal, x in the (i,j)-position and 0's elsewhere. Thus, E^{tr} has 1's on the diagonal, x in the (j,i)-position, and 0's elsewhere. Thus, E^{tr} can be obtained from I_n by the operation $R_j + xR_i$. In this case, we have $\det(E) = 1$ and $\det(E^{tr}) = 1$, which verifies the result for this particular row operation.

The verification for the other two row operations is left as an easy exercise. □

PROPOSITION 10.4. *Let A be a square matrix. Then* $\det(A) = \det(A^{tr})$.

PROOF. Suppose that A is an invertible matrix. Then $A = E_1 \cdots E_k$ where each E_i has been obtained from I_n by an elementary row operation. By Lemmma 10.2, $A^{tr} = \det(E_k^{tr} \cdots E_1^{tr})$. Thus,

$$\begin{aligned}\det(A^{tr}) &= \det(E_k^{tr} \cdots \det(E_1^{tr}) \\ &= \det(E_k) \cdots \det(E_1) \\ &= \det(A).\end{aligned}$$

Here, we used Lemma 10.3 to deduce that $\det(E_i^{tr}) = \det(E_i)$ for every i.

Suppose A is not invertible. Then its row reduced echelon form B has a zero row and so $\det(B) = 0$. As above, we can write $A = E_1 \dots E_k B$ where each E_i has been obtained from I_n by an elementary row operation. Then $A^{tr} = B^{tr} E_k^{tr} \cdots E_1^{tr}$. Thus,

$$\det(A^{tr}) = \det(E_k^{tr} \cdots E_1^{tr}) \det(B^{tr}).$$

As B has a zero row, B^{tr} has a zero column. Thus, $\det(B^{tr}) = 0$. (Recall that this is because every term in the expansion of a determinant has exactly one entry from each column as a factor.) Thus $\det(A^{tr}) = 0$. As A is not invertible, we know that $\det(A) = 0$. Thus, we have verified the result even when A is not invertible. □

Formula for the inverse of a matrix:

Let $A = (a_{ij})_{i,j}$ be an $n \times n$ matrix. As before, let A_{ij} denote the matrix obtained by deleting the i-th row and j-th column of A. For any two indices i, j, let

$$c_{ij} = (-1)^{i+j} \det A_{ij}.$$

The matrix $C = (c_{ij})_{i,j}$ (having the number c_{ij} in the (i,j)-position) is called the *cofactor matrix* of A. Let us look at an example. The number c_{ij} is called the (i,j)-*cofactor* of the matrix A.

EXAMPLE 10.5.

$$A = \begin{bmatrix} 3 & 4 & -1 \\ 2 & 1 & 3 \\ 1 & -1 & 0 \end{bmatrix}$$

Then,

$$c_{11} = (-1)^{1+1} \det \begin{bmatrix} 1 & 3 \\ -1 & 0 \end{bmatrix} = 3,$$

$$c_{12} = (-1)^{1+2} \det \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} = 3,$$

$$c_{13} = (-1)^{1+3} \det \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} = -3,$$

$$c_{21} = (-1)^{2+1} \det \begin{bmatrix} 4 & -1 \\ -1 & 0 \end{bmatrix} = 1,$$

$$c_{22} = (-1)^{2+2} \det \begin{bmatrix} 3 & -1 \\ 1 & 0 \end{bmatrix} = 1,$$

$$c_{23} = (-1)^{2+3} \det \begin{bmatrix} 3 & 4 \\ 1 & -1 \end{bmatrix} = 7,$$

$$c_{31} = (-1)^{3+1} \det \begin{bmatrix} 4 & -1 \\ 1 & 3 \end{bmatrix} = 13,$$

$$c_{32} = (-1)^{3+2} \det \begin{bmatrix} 3 & -1 \\ 2 & 3 \end{bmatrix} = -11,$$

and

$$c_{33} = (-1)^{3+3} \det \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} = -5.$$

Thus, the cofactor matrix is

$$C = \begin{bmatrix} 3 & 3 & -3 \\ 1 & 1 & 7 \\ 13 & -11 & -5 \end{bmatrix}.$$

We need one further definition before we can use the above concept to state an important theorem.

DEFINITION 10.6. Let $A = (a_{ij})_{i,j}$ be an $m \times n$ matrix. Then, for any $c \in \mathbb{R}$, cA denotes the matrix $(ca_{ij})_{i,j}$.

In other words, cA is the matrix obtained by multiplying every entry of A by the constant c.

We will prove the following theorem in a later lecture:

THEOREM 10.7. *Let A be an $n \times n$ matrix and let C be its cofactor matrix. Then $AC^{tr} = C^{tr}A = \det(A) \cdot I_n$.*

The matrix C^{tr} is called the *adjugate matrix* of A.

This immediately gives us the following formula for the inverse of square invertible matrix:

COROLLARY 10.8. *Let $A \in M_{n\times n}(\mathbb{R})$ be an invertible matrix and let C be its cofactor matrix. Then $A^{-1} = \det(A)^{-1} \cdot C^{tr}$.*

PROOF. Suppose $D = \det(A)^{-1} \cdot C$. Then,

$$DA = \det(A)^{-1} \cdot (CA) = \det(A)^{-1} \cdot \det(A) \cdot I_n = I_n.$$

This shows that $D = A^{-1}$. □

EXAMPLE 10.9. We apply this formula for a general 2×2 matrix. Suppose

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then, the matrix of cofactors is

$$C = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$$

Thus, the inverse of A is given by the following formula:

$$A^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

Cramer's rule:

As we have seen before, a system of n linear equations in n variables can be written in the form $AX = B$ where A is an $n \times n$ square matrix with entries from $\mathbb{R}$, X is an $n \times 1$ matrix with variable entries and B is an $n \times 1$ matrix with entries from $\mathbb{R}$. Then, if A is invertible, the solution of the system is given by $X = A^{-1}B$. This allows us to deduce the following formula for the solutions of such a system. We will only look at the formula for now and postpone the proof to a later lecture.

THEOREM 10.10 (Cramer's rule). *Consider the following system of linear equations*

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1 \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{n1}X_1 & + & a_{n2}X_2 & + & \cdots & & a_{nn}X_n & = & b_n \end{array}$$

where all a_{ij} and all b_i are constants and $X_1, \ldots, X_n$ are variables. Let $A = (a_{ij})_{i,j}$ and for every i satisfying $1 \leqslant i \leqslant n$, let A_i denote the square matrix obtained from A

by substituting the column matrix $[b_1, \ldots, b_n]^{tr}$ *in place of the* i*-th column of* A*. If* A *is invertible, the above system has a unique solution given by* $X_i = \det(A_i)/\det(A)$ *for every* i*.*

EXAMPLE 10.11. Consider the following system:

$$X_1 + 3X_2 = 1$$
$$2X_1 - X_2 = 5$$

We compute the determinant of the matrix of coefficients

$$\det \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix} = -7$$

and find that it is not equal to zero. Thus, this matrix is invertible and so Cramer's rule may be applied. Then the solution is given by

$$X_1 = \left(\frac{1}{-7}\right) \cdot \det \begin{bmatrix} 1 & 3 \\ 5 & -1 \end{bmatrix} = 16/7,$$
$$X_1 = \left(\frac{1}{-7}\right) \cdot \det \begin{bmatrix} 1 & 1 \\ 2 & 5 \end{bmatrix} = -3/7.$$

LECTURE 11

Proof of Cramer's rule

We defined the determinant of a matrix using the formula for expansion by the first row. We will now show that it is possible to compute the determinant by expanding by any row or column. Indeed, suppose that in a 3×3 determinant, I want to expand the determinant by the third row. Then, we can use row operations to shift the third row to the top and then use our formula for expansion by the first row. Let us try this out.

Suppose we have the following matrix:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

We want to expand by the third row, and so we bring the third row to the top to get a new matrix. We do this by the operation $R_1 \leftrightarrow R_3$.

$$B = \begin{bmatrix} a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \\ a_{11} & a_{12} & a_{13} \end{bmatrix}$$

Then, we know that $\det(B) = -\det(A)$. Thus, it will suffice to compute $\det(B)$. We use our formula for expansion by the first row.

$$\det(B) = a_{31} \det \begin{bmatrix} a_{22} & a_{23} \\ a_{12} & a_{13} \end{bmatrix} - a_{32} \det \begin{bmatrix} a_{21} & a_{23} \\ a_{11} & a_{13} \end{bmatrix} + a_{33} \det \begin{bmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{bmatrix}$$

This formula is a little inconvenient because the 2×2 matrix obtained by deleting the row and column containing a_{31} in C is a bit different from the 2×2 matrix obtained by deleting it in A. To fix this problem, we would need to work with the following matrix:

$$C = \begin{bmatrix} a_{31} & a_{32} & a_{33} \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

This matrix can be obtained from A by performing the operations $R_3 \leftrightarrow R_2$ followed by $R_2 \leftrightarrow R_1$. Thus, $\det(C) = \det(A)$. We use our formula on this matrix.

$$\det(C) = a_{31} \det \begin{bmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{bmatrix} - a_{32} \det \begin{bmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{bmatrix} + a_{33} \det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

If we use our usual notation from Definition 8.1, we see that

$$\det(A) = \det(C) = a_{31} \det(A_{31}) - a_{32} \det(A_{32}) + a_{33} \det(A_{33}).$$

On the other hand, if we had wanted to expand by the second row, we would have used the matrix

$$D = \begin{bmatrix} a_{21} & a_{22} & a_{23} \\ a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Then we know that $\det(A) = -\det(D)$ and expanding $\det(D)$ by the first row, we get

$$\det(A) = -\det(D) = -a_{21} \det(A_{21}) + a_{22} \det(A_{22}) - a_{23} \det(A_{23}).$$

It should now be clear how this argument may be generalized for $n \times n$ matrices. Suppose we have an $n \times n$ matrix $A = (a_{ij})_{i,j}$. Suppose we want to compute its determinant by expanding by the k-th row. So we perform the operations $R_k \leftrightarrow R_{k-1}, R_{k-1} \leftrightarrow R_{k-2}, \dots R_2 \leftrightarrow R_1$. Thus, $\det(B) = (-1)^{k-1} \det(A)$. It is easy to see that for any l, $1 \leqslant l \leqslant n$, $(n-1) \times (n-1)$ matrix obtained by deleting the first row and l-th column in B is the same as the $(n-1) \times (n-1)$ matrix obtained by deleting the k-th row and l-column in A. Thus,

$$det(B) = a_{k1} \det(A_{k1}) - a_{k2} \det(A_{k2}) + \cdots + (-1)^{n-1} a_{kn} \det(A_{kn}).$$

Hence,

$$\det(A) = (-1)^{k-1} a_{k1} \det(A_{k1}) - (-1)^{k-1} a_{k2} \det(A_{k2}) + \cdots + (-1)^{k+n-2} a_{kn} \det(A_{kn}).$$

This can be rewritten (for aesthetic reasons) as

$$\det(A) = (-1)^{k+1} a_{k1} \det(A_{k1}) + (-1)^{k+2} a_{k2} \det(A_{k2}) + \cdots + (-1)^{k+n} a_{kn} \det(A_{kn}).$$

(Note that these formulas are the same since, for instance, $(-1)^{k-1} = (-1)^{k+1}$, etc.) Thus, we have proved the following:

THEOREM 11.1 (Expansion by rows). *Let $A = (a_{ij})_{i,j}$ be an $n \times n$ matrix. For any pair of integers i, j satisfying $1 \leqslant i, j \leqslant n$, let A_{ij} be the matrix obtained by deleting the i-th row and j-column of A. Then for any k satisfying $1 \leqslant k \leqslant n$, we have*

$$\det(A) = \sum_{l=1}^{n} (-1)^{k+l} a_{kl} \det(A_{kl}).$$

Taking the transpose of a matrix turns its rows into columns. As the determinant of a matrix is equal to that of its transpose, we obtain the following result for expansion by columns:

THEOREM 11.2 (Expansion by columns). *Let $A = (a_{ij})_{i,j}$ be an $n \times n$ matrix. For any pair of integers i, j satisfying $1 \leqslant i, j \leqslant n$, let A_{ij} be the matrix obtained by deleting the i-th row and j-column of A. Then for any k satisfying $1 \leqslant k \leqslant n$, we have*

$$\det(A) = \sum_{l=1}^{n} (-1)^{k+l} a_{lk} \det(A_{lk}).$$

Using this we can now prove Theorem 10.7 which states that if A is an $n \times n$ matrix and C is its cofactor matrix, then $AC^{tr} = C^{tr}A = \det(A) \cdot I_n$.

PROOF OF THEOREM 10.7. We recall some of the notation we had set up before stating Theorem 10.7. We have been given the $n \times n$ matrix $A = (a_{ij})_{i,j}$. For any ordered pair (i, j) with $1 \leqslant i, j \leqslant n$, we define A_{ij} to be the $(n-1) \times (n-1)$ matrix obtained by deleting the i-th row and j-th column of A. Then, for any such ordered pair (i, j), we define $c_{ij} = (-1)^{i+j} \det(A_{ij})$. Then, C is the matrix defined which has c_{ij} in the (i, j)-position. Thus, C^{tr} has c_{ji} in the (i, j)-position.

Let $D = (d_{ij})_{i,j}$ be the product AC^{tr}. Then, by the definition of matrix multiplication,

$$\begin{aligned} d_{ij} &= \sum_{k=1}^{n} a_{ik} \cdot \big((k, j) - \text{entry of } C^{tr}\big) \\ &= \sum_{k=1}^{n} a_{ik} c_{jk} \\ &= \sum_{k=1}^{n} (-1)^{j+k} a_{ik} \det(A_{jk}). \end{aligned}$$

If $i = j$, we see by Theorem 11.1 that this $d_{ii} = \det(A)$. Thus, all the diagonal entries of D are equal to $\det(A)$.

Now, let us fix some ordered pair (i, j) satisfying $1 \leqslant i, j \leqslant n$ and $i \neq j$. Let A' be the matrix obtained by replacing the j-th row of A by a copy of the i-th row. Then, it is easy to see for any k, the (j, k)-cofactor of A' is just

$$(-1)^{i+j} \det(A_{jk}) = c_{jk}.$$

Thus, we by using the formula for the expansion of the determinant by the j-th row that

$$\det(A') = \sum_{k=1}^{n} (-1)^{j+k} a_{ik} \det(A_{jk})$$

But the i-th and j-th rows of A' are identical. Thus, $\det(A') = 0$. Thus, for $i \neq j$, $d_{ij} = 0$. This completes the proof the theorem. □

Recall that this gives us a formula (see Corollary 10.8) for the inverse matrix (if it exists). We can now use this to prove Theorem 10.10.

Proof of Theorem 10.10. Let X denote the column matrix $[X_1, \ldots, X_n]^{tr}$ and let B be the column matrix $[b_1, \ldots, b_n]^{tr}$. Then the system may be written as $AX = B$. If A is invertible, we multiply both sides of this equation by A^{-1} to get $X = A^{-1}B$. Using the formula for the inverse from Corollary 10.8, we see that

$$\begin{aligned} X_i &= \sum_{j=1}^{n} \frac{c_{ij}}{\det(A)} b_j \\ &= \frac{1}{\det(A)} \sum_{j=1}^{n} (-1)^{i+j} A_{ji} b_j. \end{aligned}$$

Expanding $\det(A_i)$ by the i-th column, we see that

$$\det(A_i) = \sum_{j=1}^{n} (-1)^{i+j} b_j A_{ji}.$$

This completes the proof of the theorem. □

LECTURE 12

Permutation matrices

We will now write down a formula for the complete expansion of a determinant. To illustrate the method, we will demonstrate for 2×2 matrices.

Suppose

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

be a given matrix. First, we write the first column of A as a sum as follows:

$$\begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} = \begin{bmatrix} a_1 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ a_{21} \end{bmatrix}$$

Then, using Lemma 8.5, we see that

$$\det(A) = \det \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} + \det \begin{bmatrix} 0 & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Now, we split the second column of the matrix in a similar manner.

$$\begin{bmatrix} a_{12} \\ a_{22} \end{bmatrix} = \begin{bmatrix} a_{12} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ a_{22} \end{bmatrix}$$

Thus, applying Lemma 8.5 again, we get

$$\det(A) = \det \begin{bmatrix} a_{11} & a_{12} \\ 0 & 0 \end{bmatrix} + \det \begin{bmatrix} a_{11} & 0 \\ 0 & a_{22} \end{bmatrix} + \det \begin{bmatrix} 0 & a_{12} \\ a_{21} & 0 \end{bmatrix} + \det \begin{bmatrix} 0 & 0 \\ a_{21} & a_{22} \end{bmatrix}$$

Recall that if any row or column of a matrix is multiplied by a constant c, its determinant also gets multiplied by c. Thus, we obtain the following expression:

$$\begin{aligned} \det(A) =& a_{11}a_{12} \det \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + a_{11}a_{22} \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + a_{12}a_{21} \det \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ &+ a_{21}a_{22} \det \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \end{aligned}$$

The first and the fourth determinants on the right hand side are clearly equal to zero because the matrices have two identical columns each. Thus, we are left with

$$\det(A) = a_{11}a_{22} \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + a_{12}a_{21} \det \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Computing these two determinants gives us the familiar formula for the determinant of a 2×2 matrix.

We now use this method on an $n \times n$ matrix. Any column matrix can be written as a sum of n column matrices, each of which has at most one non-zero term. Indeed, we can write

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ a_2 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a_n \end{bmatrix}$$

Given any $n \times n$ matrix $A = (a_{ij})_{i,j}$ we apply this method to each of the columns of A successively, to write

$$\det(A) = \sum_{1 \leqslant i_1, \ldots, i_n \leqslant n} \det(A_{i_1 \ldots i_n})$$

where $A_{i_1 \ldots i_n}$ is the matrix in which the (i_j, j)-entry is equal to $a_{i_j j}$ for every j, and all other entries are 0. Thus, every column has at most one non-zero entry. As above, we may pull out these entries as common factors from each column to write

$$\det(A) = \sum_{1 \leqslant i_1, \ldots, i_n \leqslant n} a_{i_1 1} a_{i_2 2} \cdots a_{i_n n} \det(P_{i_1 \ldots i_n})$$

where $P_{i_1 \ldots i_n}$ is the matrix in which the (i_j, j)-entry is equal to 1 for every j, and all other entries are 0. If for some matrix $P_{i_1 \ldots i_n}$, we have $i_k = i_l$ for some $k \neq l$, the k-th and l-th columns of this matrix are identical and hence its determinant is equal to 0. Thus, in the summation on the right, we only need to retain those terms in which all the $i_1, \ldots, i_n$ are distinct. To describe such choices of $i_1, \ldots, i_n$, we will use *permutations*.

DEFINITION 12.1. Let T be any set. A *permutation* of T is a function $f : T \to T$ which is one-one and onto (i.e. it is *bijective*).

NOTATION 12.2. The set of all permutations of the set $\{1, \ldots, n\}$ will be denoted by S_n.

Thus, if $\sigma \in S_n$, all the elements of the set $\{1, \ldots, n\}$ occur exactly once in the sequence $\sigma(1), \ldots, \sigma(n)$, in some order. Conversely, if we take any sequence $i_1, \ldots, i_n$ in which all the elements of the set $\{1, \ldots, n\}$ occur exactly once in some order, the function $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, defined by $\sigma(j) = i_j$ for all $1 \leqslant j \leqslant n$ is a permutation.

DEFINITION 12.3. For any $\sigma \in S_n$, we define the *permutation matrix* associated by σ to be the matrix which has 1's in the $(\sigma(i), i)$ position for every i, $1 \leqslant i \leqslant n$, and 0's elsewhere.

Thus, we have obtained the formula

$$\det(A) = \sum_{\sigma \in S_n} a_{\sigma(1)1} a_{\sigma(2)2} \ldots a_{\sigma(n)n} \det(P_\sigma).$$

For any permutation σ, the permutation matrix P_σ can be obtained from the identity matrix by successively switching rows. Thus, $\det(P_\sigma) = \pm 1$ for any permutation σ.

DEFINITION 12.4. The *sign* of a permutation $\sigma \in S_n$ is defined to be $\det(P_\sigma)$ where P_σ is the permutation matrix corresponding to σ and is denoted by $sign(\sigma)$.

Thus, we have proved the following:

THEOREM 12.5. *Let $(a_{ij})_{i,j}$ be an $n \times n$ matrix. Then*

$$\det(A) = \sum_{\sigma \in S_n} sign(\sigma) \cdot a_{\sigma(1)1} a_{\sigma(2)2} \ldots a_{\sigma(n)n}.$$

While this formula is conceptually elegant, it is not necessarily the most efficient tool for actually computing the determinant of a matrix, particularly for large n. However, it is good to know that the signs of all the terms in the expansion do have a simple description.

LECTURE 13

Vector spaces: Introduction and motivation

We begin this lecture by re-examining some of the objects we have already studied, in order to motivate the abstract notion of a vector space. We have already been studying some concrete examples of vector spaces, namely the sets $\mathbb{R}^n$. We begin by observing the algebraic structure that exists on these sets.

The sets $\mathbb{R}^n$ are equipped with the following operations:

(a) *Addition*: This is a function from the product $\mathbb{R}^n \times \mathbb{R}^n$ to the set $\mathbb{R}^n$. In other words, it takes a pair of elements $\mathbf{x}$ and $\mathbf{y}$ of $\mathbb{R}^n$ and produces a third element of the set $\mathbb{R}^n$, which we denote as $\mathbf{x} + \mathbf{y}$. If

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \qquad \text{and} \qquad \mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

then we define as follows:

$$\mathbf{x} + \mathbf{y} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}$$

(b) *Scalar multiplication*: This is a function from $\mathbb{R} \times \mathbb{R}^n$ to $\mathbb{R}^n$. In other words, it takes an element $c \in \mathbb{R}$, an element $\mathbf{x} \in \mathbb{R}^n$ and produces an element of $\mathbb{R}^n$, which we denote as $c\mathbf{x}$. If

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad \text{then we define} \quad c\mathbf{x} = \begin{bmatrix} cx_1 \\ cx_2 \\ \vdots \\ cx_n \end{bmatrix}.$$

These operations satisfy certain standard properties, which we will not list in detail for now.

Let A be an $m \times n$ matrix with entries from $\mathbb{R}$. We define a function $T_A : \mathbb{R}^n \to \mathbb{R}^m$ by $T_A(\mathbf{x}) = A\mathbf{x}$. It is easy to verify that this function satisfies the following:

(i) $T_A(\mathbf{x} + \mathbf{y}) = T_A(\mathbf{x}) + T_A(\mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.
(ii) $T_A(c\mathbf{x}) = cT_A(\mathbf{x})$ for $c \in \mathbb{R}$ and $\mathbf{x} \in \mathbb{R}^n$.

These two properties could also be expressed more concisely by saying that $T_A(a\mathbf{x} + b\mathbf{y}) = aT_A(\mathbf{x}) + bT_A(\mathbf{y})$ for all $a, b \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

We note that the matrix A and the linear transformation T_A fully characterize each other. Indeed, we will now show that if the linear transformation T_A is given to us, the matrix A can be recovered from it.

DEFINITION 13.1. Let n be a positive integer. For $1 \leqslant i \leqslant n$ let $\mathbf{e}_i$ be the $n \times 1$ matrix having 1 in the $(i, 1)$-position and 0's elsewhere. The ordered tuple $(\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ is called the *standard basis of* $\mathbb{R}^n$.

We will discuss the notion of a "basis" in greater detail later and at that point this terminology will make much more sense. For now, we note that this basis is useful for recovering the matrix A from the linear transformation T_A. Indeed, a simple calculation shows that for each i satisfying $1 \leqslant i \leqslant n$, the column matrix $T_A(\mathbf{e}_i)$ is just the i-th column of the matrix A. (Check this by explicit matrix multiplication.) Thus, if we are given the linear transformation T_A, we may recover A by simply computing the column matrices $T(\mathbf{e}_i)$ for all i and then putting them together into an $n \times n$ matrix.

We now observe a useful property of the standard basis of $\mathbb{R}^n$. Given any $\mathbf{x} = [x_1, \ldots, x_n]^{tr} \in \mathbb{R}^n$, we write

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + x_n \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

Thus, every vector can be written as a sum of multiples of the $\mathbf{e}_i$. It is clear that this can be done in a unique manner. In other words, if $y_1, \ldots, y_n$ are real numbers such that $\mathbf{x} = y_1\mathbf{e}_1 + y_2\mathbf{e}_2 + \cdots + y_n\mathbf{e}_n$, then we must have $x_i = y_i$ for all i.

DEFINITION 13.2. A function $T : \mathbb{R}^n \to \mathbb{R}^m$ is said to be a *linear transformation (or a linear map)* if

$$T(a\mathbf{x} + b\mathbf{y}) = aT(\mathbf{x}) + bT(\mathbf{y})$$

for all $a, b \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

EXERCISE 13.3. Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear function. Let k be a positive integer. Let $c_1, \ldots, c_k \in \mathbb{R}$ and let $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{R}^n$. Show that

$$T(c_1\mathbf{x}_1 + \cdots + c_k\mathbf{x}_k) = c_1T(\mathbf{x}_1) + \cdots + c_kT(\mathbf{x}_k).$$

(Hint: You may use induction on k.)

We saw above that any $m \times n$ matrix gives rise to a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$. We will now see that the converse is also true.

THEOREM 13.4. *Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Let A be the $m \times n$ matrix which has $T(\mathbf{e}_i)$ as its i-th column. Then $T(\mathbf{x}) = T_A(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$.*

PROOF. Suppose $\mathbf{x} = [x_1, \ldots, x_n]^{tr}$ where $x_i \in \mathbb{R}$ for all i. Then, as above, we see that $\mathbf{x} = \sum_{i=1}^n x_i\mathbf{e}_i$. By Exercise 13.3, we have

$$T(\mathbf{x}) = T(\sum_{i=1}^n x_i\mathbf{e}_i) = \sum_{i=1}^n x_iT(\mathbf{e}_i).$$

By definition $T(\mathbf{e}_i)$ is the i-th column of A and is hence equal to $A\mathbf{e}_i$. Thus, as T_A is known to be a linear transformation, we get

$$T(\mathbf{x}) = \sum_{i=1}^n x_iT_A(\mathbf{e}_i) = T_A(\sum_{i=1}^n x_i\mathbf{e}_i) = T_A(\mathbf{x}).$$

□

Given any linear transformation T, the above theorem shows that we can construct a matrix A such that $T = T_A$. We observe that there can be only one matrix with this property. Indeed, if $T = T_B$ for some other matrix B, then $T_A(\mathbf{e}_i) = T_B(\mathbf{e}_i)$ for every i. Hence the i-th columns of A and B are equal for every i. Thus, A and B are the same matrix. Thus we have established a 1-1 correspondence between the set of $m \times n$ matrices and linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Now we will begin to construct some abstract objects on the basis of these concrete examples.

Fields:

In most of our discussion, we have restricted our scalars to the set of real numbers. However, we have only used a few basic properties of the set of real numbers, which are also satisfied by the set of rational numbers. Thus, our entire discussion would remain valid if we were to replace $\mathbb{R}$ by $\mathbb{Q}$. More generally, we would be able to do this with any *field*, which is defined as follows:

DEFINITION 13.5. A field is a set F which comes equipped with two functions, called *addition* and *multiplication*, from $F \times F$ to F. The addition function will be written as $(x, y) \mapsto x + y$ and the multiplication function will be written as $(x, y) \mapsto x \cdot y$. (Sometimes, we may also write $x \times y$ or xy in place of $x \cdot y$.) These functions are required to satisfy the following properties:

(1) *Properties of addition*:
   (a) *Associativity*: $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$.
   (b) *Commutativity*: $x + y = y + x$ for all $x, y \in F$.
   (c) *Additive identity*: There exists a unique element 0 such that $x + 0 = 0 + x = x$ for all $x \in F$.
   (d) *Additive inverse*: For every $x \in F$, there exists a unique element $-x$ satisfying $x + (-x) = (-x) + x = 0$.
(2) *Properties of multiplication*:
   (a) *Associativity*: $(xy)z = x(yz)$ for all $x, y, z \in F$.
   (b) *Commutativity*: $xy = yx$ for all $x, y \in F$.
   (c) *Multiplicative identity*: There exists a unique element 1 such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in F$.
   (d) *Multiplicative inverse*: For every $x \in F$ such that $x \neq 0$, there exists a unique element x^{-1} satisfying $x \cdot x^{-1} = x^{-1} \cdot x = 1$. (It is customary to write x/y instead of $x \cdot y^{-1}$ for $x, y \in F$ with $y \neq 0$.)
(3) *Distrbutive property*: $x(y + z) = xy + xz$ for $x, y, z \in F$.

EXAMPLES 13.6.

(1) As mentioned before the set of real numbers and the set of rational numbers, equipped with the usual operations of addition and multiplication, form fields which are denoted by $\mathbb{R}$ and $\mathbb{Q}$ respectively.
(2) We start with the set $\mathbb{R}^2$. We define the addition on this set by
$$(x, y) + (z, w) = (x + z, y + w)$$
and multiplication by
$$(x, y) \cdot (z, w) = (xz - yw, xw + yz).$$
It can be easily verified that this set is a field with the additive identity being $(0, 0)$ and the multiplicative identity being $(1, 0)$. The set $\mathbb{R}^2$, with these operations, is called the *field of complex numbers*, and is denoted by $\mathbb{C}$.

   For any element $x \in \mathbb{R}$ and any element $\alpha = (y, z) \in \mathbb{R}^2$, we write $x \cdot \alpha$ for (xy, xz). Thus, any element $(x, y) \in \mathbb{C}$ can be written as
$$(x, y) = x \cdot (1, 0) + y \cdot (0, 1).$$
We denote the element $(0, 1)$ by i. Since $(1, 0)$ is the multiplicative identity in $\mathbb{C}$, we abuse notation to write $x \cdot (1, 0) + y \cdot (0, 1)$ as $x + yi$. Observe that
$$(0, 1) \cdot (0, 1) = (-1, 0) = -1 \cdot (1, 0).$$
Thus, if we identify every real number $x \in \mathbb{R}$ with the element $x \cdot (1, 0) = (x, 0)$ of $\mathbb{C}$, we see that i is a square-root of -1 in $\mathbb{C}$.

(3) Let p be any prime number. We consider the set $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$. For any two elements $a, b \in \mathbb{F}_p$, we define the sum $a \oplus b$ to be the remainder left when we divide the integer $a+b$ by p. Similarly, we define the product $a \odot b$ to be the remainder left when we divide the integer ab by p. It can be verified that, with these operations, $\mathbb{F}_p$ forms a field.

In everything that we have done so far in this course, we can replace $\mathbb{R}$ by any field. So from now on, we will work with a general field F.

Vector spaces:

DEFINITION 13.7. Let F be a field. A vector space over F (or an F-vector space) is a set V, equipped with a function called *addition* from $V \times V \to V$ and a function called *scalar multiplication* from $F \times V \to V$. The addition function will be written as $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} + \mathbf{y}$ and the multiplication function will be written as $(c, \mathbf{x}) \mapsto c \cdot \mathbf{x}$. (Sometimes, we may also write $c\mathbf{x}$ in place of $c \cdot \mathbf{x}$.) These functions are required to satisfy the following properties:

(1) *Properties of addition*:
   (a) *Associativity*: $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.
   (b) *Commutativity*: $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ for all $\mathbf{x}, \mathbf{y} \in V$.
   (c) *Additive identity*: There exists an element $\mathbf{0} \in \mathbb{R}^n$ such that $\mathbf{x} + \mathbf{0} = \mathbf{0} + \mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in V$.
   (d) *Additive inverse*: For every $\mathbf{x} \in V$, there exists an element, which we denote by $-\mathbf{x}$, and which satsifies $\mathbf{x} + (-\mathbf{x}) = (-\mathbf{x}) + \mathbf{x} = \mathbf{0}$.
(2) *Properties of scalar multiplication*:
   (a) *Associativity*: $c(d\mathbf{x}) = (cd)\mathbf{x}$ for all $c, d \in F$ and $\mathbf{x} \in V$.
   (b) *Unital property:* $1\mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in V$.
(3) *Distributive properties*:
   (a) $(c + d)\mathbf{x} = c\mathbf{x} + d\mathbf{x}$ for $c, d \in F$ and $\mathbf{x} \in V$.
   (b) $c(\mathbf{x} + \mathbf{y}) = c\mathbf{x} + c\mathbf{y}$ for $c \in F$ and $\mathbf{x}, \mathbf{y} \in V$.

Given any vector space V, its elements will often be referred to as *vectors*.

EXAMPLES 13.8. Let F be a field. In the following examples, when we say *vector space*, we always mean an F-vector space.

(1) Consider the set $\{0\}$ on which addition is defined by $0 + 0 = 0$ and scalar multiplication is defined by $x \cdot 0 = 0$ for any $x \in F$. This clearly forms a vector space, which is called the *zero vector space*.
(2) For any integer n, the set F^n of $n \times 1$ matrices with entries from F is an F-vector space.
(3) For any fixed positive integers m and n, the set $M_{m\times n}(F)$ of $m \times n$ matrices with entries from F is a vector space. Addition is defined as in Lecture 6. Given any matrix $m \times n$ matrix $A = (a_{ij})_{i,j}$ and $c \in F$, we define cA to be the $m \times n$ matrix having the entry ca_{ij} in the (i, j) position. It is easy to check that this is an F-vector space.
(4) Let S be any set. Consider the set $Func(S, F)$ of all functions from S to F. For $f, g \in Func(S, F)$, we define the sum $f + g$ to be a function from $S \to F$ defined by $(f + g)(s) = f(s) + g(s)$ for all $s \in S$. For $c \in F$ and $f \in Func(S, F)$ we define $cf \in Func(S, F)$ by $(cf)(s) = c(f(s))$ for all $s \in S$. It is easy to verify that this is an F-vector space.

LECTURE 14

Basic properties of vector spaces; subspaces

In Lecture 13, we defined linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$. It is easy to see that this definition can now be generalized to vector spaces.

Let F denote an arbitrary field.

DEFINITION 14.1. Let V and W be F-vector spaces. A *linear transformation (or linear map)* from V to W is a function $T : V \to W$ such that

$$T(a\mathbf{x} + b\mathbf{y}) = aT(\mathbf{x}) + bT(\mathbf{y})$$

for all $a, b \in F$ and $\mathbf{x}, \mathbf{y} \in V$.

The following lemma is easy to prove and the proof is left as an exercise:

LEMMA 14.2. *Let V and W be F-vector spaces. Let $T : V \to W$ be a function. Then, T is a linear transformation if and only if both of the following conditions hold:*

(a) $T(\mathbf{x} + \mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y} \in V$.
(b) $T(c\mathbf{x}) = cT(\mathbf{x})$ *for all* $c \in F$ *and* $\mathbf{x} \in V$.

DEFINITION 14.3. Let V and W be F-vector spaces. An isomorphism from V to W is a linear transformation $T : V \to W$ which is a bijection. If there exists an isomorphism from V to W, we say that V and W are *isomorphic*.

REMARK 14.4. It is easy to check that if $T : V \to W$ is an isomorphism, then the inverse function $T^{-1} : W \to V$ (which is well-defined because T is a bijection) is also linear. Thus, T^{-1} is also an isomorphism of vector spaces.

If two spaces are isomorphic, they have the same mathematical properties, though they may be distinct objects. Note that there may be more than one isomorphism between two vector spaces.

EXAMPLE 14.5. Let V be a vector space and let $Id_V : V \to V$ be the identity map defined by $Id_V(\mathbf{x}) = \mathbf{x}$. It is easy to see that Id_V is an isomorphism of vector spaces.

EXAMPLE 14.6. Let $V = F^2$. Let $T : V \to V$ be defined by

$$T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$$

It is easy to see that this is an isomorphism. If $F = \mathbb{R}$, we may think of $\mathbb{R}^2$ as the Euclidean plane and you should be able to recognize this transformation as the reflection in the x-axis.

EXAMPLE 14.7. Let m and n be positive integers. Let $T : M_{m\times n}(F) \to M_{n\times m}(F)$ be defined by $T(A) = A^{tr}$. It is easy to see that T is a bijection. You may check that T is also a linear transformation. (This is very easy.) Thus T is an isomorphism of vector spaces.

EXAMPLE 14.8. Let n be an integer and let $S = \{1, 2, \ldots, n\}$. Let $V = Func(S, F)$ and let $W = F^n$. We will construct an isomorphism from V to W.

We first define a function $\phi : V \to W$. Given any $f \in V = Func(S, F)$, we want to construct an element of $W = F^n$. f is a function from S to F. Thus, for every $i \in S = \{1, 2, \ldots, n\}$, $f(i)$ is an element of F. We define

$$\phi(f) = \begin{bmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{bmatrix}.$$

Let us check that ϕ is linear. Let $f, g \in V$ and let $a, b \in F$. We want to show that $\phi(af + bg) = a\phi(f) + b\phi(g)$. By definition, for every $i \in S$, we have $(af + bg)(i) = (af)(i) + (bg)(i) = af(i) + bg(i)$. Thus,

$$\phi(af + bg) = \begin{bmatrix} af(1) + bg(1) \\ af(2) + bg(2) \\ \vdots \\ af(n) + bg(n) \end{bmatrix} = a \begin{bmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{bmatrix} + b \begin{bmatrix} g(1) \\ g(2) \\ \vdots \\ g(n) \end{bmatrix} = a\phi(f) + b\phi(g).$$

Thus, ϕ is linear.

If $\phi(f) = \phi(g)$ then the column matrices

$$\begin{bmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} g(1) \\ g(2) \\ \vdots \\ g(n) \end{bmatrix}$$

are equal. Hence their corresponding entries must be equal. Thus $f(i) = g(i)$ for all i, $1 \leqslant i \leqslant n$. Thus $f = g$. This shows that ϕ is a $1-1$ function.

Given any $\mathbf{x} = [x_1, \ldots, x_n]^{tr} \in W$, we can define $f : S \to F$ by $f(i) = x_i$. Then it is clear that $\phi(f) = \mathbf{x}$. As $\mathbf{x}$ was arbitrary, this shows that ϕ is onto. Thus we have now shown that ϕ is a bijection. Thus, ϕ is an isomorphism.

Another way to check that ϕ is $1-1$ and onto is to directly construct the inverse function of ϕ. If $\mathbf{x} = [x_1, \ldots, x_n]^{tr}$, we define $\psi(\mathbf{x})$ to be a function $S \to F$ defined by $\psi(\mathbf{x})(i) = x_i$. Then one needs to check that $\psi(\phi(f)) = f$ for all $f \in V$ and $\phi(\psi(\mathbf{x})) = \mathbf{x}$ for every $\mathbf{x} \in W$. (You may check this as an easy exercise.)

We will now prove some simple results about vector spaces.

The following result shows that the additive identity in a vector space is unique:

PROPOSITION 14.9. *Let V be a vector space. Let $\mathbf{w} \in V$ be such that $\mathbf{v} + \mathbf{w} = \mathbf{v}$ for all $\mathbf{v} \in V$. Then $\mathbf{w} = \mathbf{0}$.*

PROOF. We take $\mathbf{v} = \mathbf{0}$. Then the assumption on $\mathbf{w}$ tells us that $\mathbf{0} + \mathbf{w} = \mathbf{0}$. However, by the definition of $\mathbf{0}$, we also know that $\mathbf{0} + \mathbf{w} = \mathbf{w}$. Thus we see that

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

This proves the result. □

The next result shows that the additive inverse of any element is unique:

PROPOSITION 14.10. *Let V be a vector space and let $\mathbf{v} \in V$. If w is such that $\mathbf{v} + \mathbf{w} = \mathbf{0}$, then $\mathbf{w} = -\mathbf{v}$.*

PROOF. We observe that

$$\begin{aligned}\mathbf{w} &= \mathbf{0} + \mathbf{w}\\ &= (-\mathbf{v} + \mathbf{v}) + \mathbf{w}\\ &= (-\mathbf{v}) + (\mathbf{v} + \mathbf{w})\\ &= (-\mathbf{v}) + \mathbf{0}\\ &= -\mathbf{v}.\end{aligned}$$

This completes the proof. □

PROPOSITION 14.11. *Let V be a vector space and let $\mathbf{v} \in V$. Then $0\mathbf{v} = \mathbf{0}$.*

PROOF. We observe that

$$\begin{aligned}0\mathbf{v} &= (0+0)\mathbf{v}\\ &= 0\mathbf{v} + 0\mathbf{v}.\end{aligned}$$

Adding $-0\mathbf{v}$ on both sides, we get $\mathbf{0} = 0\mathbf{v}$. □

PROPOSITION 14.12. *Let V be a vector space and let $\mathbf{v}$ in$V$. Then, we have $(-1)\cdot\mathbf{v} = -\mathbf{v}$.*

PROOF. From the definition of vector spaces, we know that $1\cdot\mathbf{v} = \mathbf{v}$. Thus, we observe that

$$\begin{aligned}\mathbf{v} + (-1)\cdot\mathbf{v} &= 1\cdot\mathbf{v} + (-1)\cdot\mathbf{v}\\ &= (1 + (-1))\cdot\mathbf{v}\\ &= 0\cdot\mathbf{v}\\ &= \mathbf{0}.\end{aligned}$$

By Proposition 14.10, we see that $(-1)\cdot\mathbf{v} = -\mathbf{v}$. □

Subspaces:

Let V be a vector space. A subset U of V is said to be a *subspace* of V if the addition and scalar multiplication on V, when evaluated on elements of U, turns U into a vector space. Thus, for this to happen, for any $\mathbf{x}_1, \mathbf{x}_2 \in U$, we must have $\mathbf{x}_1 + \mathbf{x}_2 \in U$. Also, for any $c \in F$ and any $\mathbf{x} \in U$, we must have $c\mathbf{x} \in U$. A priori, it may seem that, once this is verified, one must also check that the various properties of addition and scalar multiplication also hold for U. But this is not necessary since they are already known to hold in V! Thus, we may actually define subspaces as follows:

DEFINITION 14.13. Let V be a vector space. A subset $U \subset V$ is said to be a *subspace* of V if the following two conditions hold:

(1) For any $\mathbf{x}_1, \mathbf{x}_2 \in U$, we have $\mathbf{x}_1 + \mathbf{x}_2 \in U$.
(2) For any $c \in F$ and any $\mathbf{x} \in U$, we have $c\mathbf{x} \in U$.

The following lemma gives shows that these two conditions may be expressed in a more concise manner. The proof is left as an exercise.

LEMMA 14.14. *Let V be a vector space. A subset $U \subset V$ is a subspace of V if and only if for any $\mathbf{x}_1, \mathbf{x}_2 \in U$ and any $a, b \in F$, we have $a\mathbf{x}_1 + b\mathbf{x}_2 \in U$.*

EXAMPLE 14.15. Let $V = F^2$. Let

$$U = \left\{[x_1, x_2]^{tr} : x_1 \in F, x_2 = 0\right\}.$$

It is easy to check that U is a subspace.

LECTURE 15

Subspaces, spans of subsets, linear independence

More examples of subspaces:

DEFINITION 15.1. Let V and W be vector spaces and let $T : V \to W$ be a linear transformation.

(a) The *kernel of* T, denoted by $ker(T)$ is defined by

$$ker(T) = \{\mathbf{v} \in V : T(\mathbf{v}) = \mathbf{0}\}.$$

(b) The *image of* T, denoted by $im(T)$ is defined by

$$im(T) = \{T(\mathbf{v}) : \mathbf{v} \in V\}.$$

LEMMA 15.2. *Let V and W be vector spaces and let $T : V \to W$ be a linear transformation. Then $ker(T)$ is a subspace of V and $im(T)$ is a subspace of W.*

PROOF. Suppose $\mathbf{v}_1, \mathbf{v}_2 \in ker(T)$ and $a_1, a_2 \in F$. Then

$$T(a_1\mathbf{v}_1 + a_2\mathbf{v}_2) = a_1T(\mathbf{v}_1) + a_2T(\mathbf{v}_2) = \mathbf{0}.$$

Thus $ker(T)$ is a subspace of V.

Suppose $\mathbf{w}_1, \mathbf{w}_2 \in im(T)$ and $a_1, a_2 \in F$. By assumption, there exist $\mathbf{v}_1, \mathbf{v}_2 \in V$ such that $T(\mathbf{v}_1) = \mathbf{w}_1)$ and $T(\mathbf{v}_2) = \mathbf{w}_2)$. Thus,

$$T(a_1\mathbf{v}_1 + a_2\mathbf{v}_2) = a_1T(\mathbf{v}_1) + a_2T(\mathbf{v}_2) = a_1\mathbf{w}_1 + a_2\mathbf{w}_2.$$

Thus, $a_1\mathbf{w}_1 + a_2\mathbf{w}_2 \in im(T)$. Thus, $im(T)$ is a subspace of W. □

Studying the kernel and image of a linear transformation can be very useful for understanding its properties, as the following lemma shows:

LEMMA 15.3. *Let V and W be vector spaces and let $T : V \to W$ be a linear transformation.*

(a) *T is $1-1$ (injective) if and only if $ker(T)$ is the zero subspace of V.*
(b) *T is onto (surjective) if and only if $im(T) = W$.*

PROOF. Part (b) is obvious from the definition, and so we focus on proving (a).

Suppose T is $1-1$. Then if $T(\mathbf{v}) = T(\mathbf{0}) = 0$, we must have $\mathbf{v} = 0$, which shows that $ker(T)$ is the zero subspace.

Conversely, suppose that $ker(T)$ is the zero subspace. If T is not $1-1$, there exist $\mathbf{v}_1, \mathbf{v}_2$ such that $\mathbf{v}_1 \neq \mathbf{v}_2$, but $T(\mathbf{v}_1) = T(\mathbf{v}_2)$. Thus,

$$T(\mathbf{v}_1 - \mathbf{v}_2) = T(\mathbf{v}_1) - T(\mathbf{v}_2) = \mathbf{0}.$$

However, $\mathbf{v}_1 - \mathbf{v}_2 \neq \mathbf{0}$. Thus, $ker(T)$ is not the zero subspace of V. □

PROPOSITION 15.4. *Let V be a vector space and let $\{W_i\}_{i\in I}$ be a collection of subspaces of V. Then, the intersection $W = \bigcap_{i\in I} W_i$ is a subspace of V.*

PROOF. Let $\mathbf{w}_1, \mathbf{w}_2 \in W$ and let $a_1, a_2 \in F$. For any $i \in I$, $\mathbf{w}_1, \mathbf{w}_2 \in W_i$. Thus $a_1\mathbf{w}_1 + a_2\mathbf{w}_2 \in W_i$ for every $i \in I$. Thus $a_1\mathbf{w}_1 + a_2\mathbf{w}_2 \in W$. This shows that W is a subspace of V. □

Span of a set:

DEFINITION 15.5. Let V be a vector space and let S be a subset of V. The *span of* S, denoted by $span(S)$ is the intersection of all subspaces of V which contain S.

It follows from Proposition 15.4 that the span of a subset S is actually a *subspace* of V. Since it is contained inside every other subspace which contains S, we see that it is the *smallest* subspace of V which contains S. We will now obtain a more concrete description of this subspace.

DEFINITION 15.6. Let V be a vector space and let S be a subset of V. An element $\mathbf{v} \in V$ is said to be a *linear combination* of elements of S if there exist finitely many elements $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of S and elements $a_1, \ldots, a_n \in F$ such that

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots a_n\mathbf{v}_n.$$

PROPOSITION 15.7. *Let V be a vector space and let S be a subset of V. Then $span(S)$ is equal to the set of all the linear combinations of elements of S.*

PROOF. Let W be some subspace of V containing S. Then for any elements $\mathbf{v}_1, \mathbf{v}_2 \in S$ and elements $a_1, a_2 \in F$, the element $a_1\mathbf{v}_1 + a_2\mathbf{v}_2$ lies in W. A simply induction argument allows us to deduce from this that if $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are elements of S and $a_1, \ldots, a_n \in F$, then the element $\sum_{i=1}^n a_i\mathbf{v}_i$ is in W. (Exercise: Use induction on n to prove this.) Thus, we see that the set of linear combinations of S is contained in $span(S)$.

We now claim that the set of all linear combinations of elements of S is actually a subspace of V. Since this set contains S itself, and since $span(S)$ is contained in any subspace of V containing S, this will imply that $span(S)$ is contained in the set of linear combinations of S. Thus, it will follow that $span(S)$ is actually equal to the set of linear combinations of S.

Thus, it now remains to show that the set of linear combinations of S is a subspace. Suppose $\mathbf{v}$ and $\mathbf{w}$ are linear combinations of elements of S. Thus, there exist elements $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n$ in S and $a_1, \ldots, a_m, b_1, \ldots, b_n \in F$ such that $\mathbf{v} = \sum_{i=1}^m a_i\mathbf{v}_i$ and $\mathbf{w} = \sum i = 1^n b_i\mathbf{w}_i$. Then, for any $a, b \in F$, the element

$$a\mathbf{v} + b\mathbf{w} = \sum_{i=1}^{m}(aa_i)\mathbf{v}_i + \sum_{i=1}^{n}(bb_i)\mathbf{w}_i$$

is clearly a linear combination of elements of S. This completes the proof. □

EXAMPLE 15.8. Let $V = F^3$. Let

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \qquad \mathbf{v}_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \qquad \mathbf{v}_3 = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}.$$

First we compute $span(\mathbf{v}_1, \mathbf{v}_2)$. Suppose $\mathbf{w}$ is in $span(\mathbf{v}_1, \mathbf{v}_2)$. Thus, there exist $a, b \in F$ such that

$$\mathbf{w} = a\mathbf{v}_1 + b\mathbf{v}_2 = \begin{bmatrix} a \\ a+b \\ b \end{bmatrix}.$$

Now we compute $span(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$. We see that $\mathbf{w}$ lies in $span(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ if and only if there exist $a, b, c \in F$ such that

$$\mathbf{w} = a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3 = \begin{bmatrix} a-c \\ a+b \\ b+c \end{bmatrix}.$$

A careful examination of these expressions shows that $span(\mathbf{v}_1, \mathbf{v}_2)$ is the same as $span(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$. There is a very simple explanation for this. Indeed, we have $\mathbf{v}_3 = \mathbf{v}_2 - \mathbf{v}_1$. Thus, in any linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$, we may substitute $\mathbf{v}_2 - \mathbf{v}_1$ in place of $\mathbf{v}_3$ and thus rewrite it as a linear combination of $\mathbf{v}_1, \mathbf{v}_2$.

The above example suggests that if an element of S is a linear combination of the remaining elements of S, then it may be removed from S without diminishing the span. We will establish this rigorously, but first we set up some notation for dealing with linear combinations of an arbitary set.

CONVENTION 15.9. Let V be a vector space. Let I be a set of indices (i.e. labels) and let $S = \{\mathbf{v}_i\}_{i\in I}$ be a family of elements of V *indexed by* I, possibly with repetitions. (Thus, we may have $\mathbf{v}_i = \mathbf{v}_j$ for some $i \neq j$.) Then, in general, if I is an infinite set, the sum $\sum_{i\in I} \mathbf{v}_i$ makes no sense at all. However, if all but finitely many of the $\mathbf{v}_i$ are equal to zero, it can be interpreted in a meaningful way – we just interpret it as the sum of the non-zero terms.

This convention is particularly useful for expressing linear combinations of sets. Let S be an arbirary set of elements of V. Then an arbitrary linear combination of elements of S may be written as $\sum_{\mathbf{v}\in S} a_{\mathbf{v}}\mathbf{v}$ where we assume that all but finitely many of the $a_{\mathbf{v}}$ are equal to 0. Thus, all but finitely many of the vectors $a_{\mathbf{v}}\mathbf{v}$ are equal to $\mathbf{0}$ and so the given expression is interpreted as the sum of the finitely many non-zero terms. This makes it unnecessary to keep track of the n in Definition 15.6 when we speak of an arbitrary linear combination of elements of S. The constant $a_{\mathbf{v}}$ will be called as the *coefficient* of $\mathbf{v}$ in the given expression.

LEMMA 15.10. *Let V be a vector space and let S be a subset of V. Suppose $\mathbf{v}$ is an element of S such that it is a linear combination of the elements of the set $S\backslash\{\mathbf{v}\}$. Then $span(S) = span(S\backslash\{\mathbf{v}\})$.*

PROOF. Let $T = S\backslash\{\mathbf{v}\}$. It is clear that $span(T) \subset span(S)$. We need to show that $span(S) \subset span(T)$.

By assumption, $\mathbf{v} = \sum_{\mathbf{w}\in T} a_{\mathbf{w}}\mathbf{w}$ where $a_{\mathbf{w}} \in F$ for all $\mathbf{w}$ and all but finitely many of them are zero. Now let $\mathbf{u}$ be in $span(S)$. We write $\mathbf{u} = \sum_{\mathbf{w}\in S} b_{\mathbf{w}}\mathbf{w}$ where $b_{\mathbf{w}} \in F$ for all $\mathbf{w}$ and all but finitely many of them are zero.

Thus,

$$\begin{aligned}\mathbf{u} &= \sum_{\mathbf{w}\in S} b_{\mathbf{w}}\mathbf{w}\\ &= b_{\mathbf{v}}\mathbf{v} + \sum_{\mathbf{w}\in T} b_{\mathbf{w}}\mathbf{w}\\ &= \left(\sum_{\mathbf{w}\in T} (b_{\mathbf{v}}a_{\mathbf{w}})\mathbf{w}\right) + \left(\sum_{\mathbf{w}\in T} b_{\mathbf{w}}\mathbf{w}\right)\\ &= \sum_{\mathbf{w}\in T} (b_{\mathbf{v}}a_{\mathbf{w}} + b_{\mathbf{w}})\mathbf{w}.\end{aligned}$$

As only finitely many of the $a_{\mathbf{w}}$ and $b_{\mathbf{w}}$ are non-zero, only finitely many of the expressions $(b_{\mathbf{v}}a_{\mathbf{w}} + b_{\mathbf{w}})$ are non-zero. Thus, the final expression we have obtained still makes sense and represents a linear combination of elements of T. Thus, it follows that $\mathbf{w} \in span(T)$. □

Thus, as far as the span is concerned, elements of S that are linear combinations of the other elements are superfluous and may be removed from S. We now consider sets which cannot be shrunk in this manner.

DEFINITION 15.11. Let V be a vector space and let S be a subset of V. We say that S is a *linearly independent set* if for every element $\mathbf{v}$ of S, we have $\mathbf{v} \notin span(S\backslash\{\mathbf{v}\})$. In this case, the elements of S are also said to be *linearly independent*. If the elements of S are not linearly independent, we say that they are *linearly dependent*.

PROPOSITION 15.12. *Let V be a vector space and let S be a subset of V. Then the following statements are equivalent:*

(1) *Every element of span(S) can be uniquely written in the form* $\sum_{\mathbf{v}\in S} a_{\mathbf{v}}\mathbf{v}$.
(2) *Suppose that some linear combination* $\sum_{\mathbf{v}\in S} a_{\mathbf{v}}\mathbf{v}$ *of elements of* S *is equal to* $\mathbf{0}$. *Then* $a_{\mathbf{v}}$ *is equal to* 0 *for all* $\mathbf{v}\in S$.
(3) *The set* S *is linearly independent.*

PROOF. Suppose (1) is true. Then $\sum_{\mathbf{v}\in S} a_{\mathbf{v}}\mathbf{v}$ and $\sum_{\mathbf{v}\in S} 0\cdot\mathbf{v}$ are two ways of expressing $\mathbf{0}$ as a linear combination of elements of S. Since we are assuming (1), it follows that these are the same and hence $a_{\mathbf{v}} = 0$ for all $\mathbf{v}\in S$. Thus (1) implies (2).

Suppose (2) is true. If (3) is not true, there exists an element $\mathbf{v}\in S$ such that $\mathbf{v} = \sum_{\mathbf{w}\in S\setminus\{\mathbf{v}\}} a_{\mathbf{w}}\mathbf{w}$. Then the linear combination

$$(-1)\cdot\mathbf{v} + \sum_{\mathbf{w}\in S\setminus\{\mathbf{v}\}} a_{\mathbf{w}}\mathbf{w}$$

is equal to $\mathbf{0}$. But then since we are assuming (2), all the coefficients in this expression must be equal to 0. This implies $-1 = 0$, which is a contradiction. Thus, (3) must be true. Thus (2) implies (3).

Suppose (3) is true. If (1) is not true, there exists an element which can be expressed as a linear combination of elements of S in two distinct ways. In other words, there exist expressions $\sum_{\mathbf{w}\in S} a_{\mathbf{w}}\mathbf{w}$ and $\sum_{\mathbf{w}\in S} b_{\mathbf{w}}\mathbf{w}$ which are equal, but the coefficients do not match. In other words, there is some $\mathbf{v}\in S$ such that $a_{\mathbf{v}} \neq b_{\mathbf{v}}$. Thus

$$(a_{\mathbf{v}} - b_{\mathbf{v}})\cdot\mathbf{v} = \sum_{\mathbf{w}\in S\setminus\{\mathbf{v}\}} (b_{\mathbf{w}} - a_{\mathbf{w}})\cdot\mathbf{w},$$

and hence

$$\mathbf{v} = \sum_{\mathbf{w}\in S\setminus\{\mathbf{v}\}} \left(\frac{b_{\mathbf{w}} - a_{\mathbf{w}}}{a_{\mathbf{v}} - b_{\mathbf{v}}}\right)\cdot\mathbf{w}.$$

This shows that S is not linearly independent, which contradicts (3). Thus, (1) must be true. So, we see that (3) implies (1).

Thus, the three given statements are equivalent. □

EXAMPLE 15.13. Let V be a vector space and let $\mathbf{v}$ be a non-zero element of V. Then the set $\{\mathbf{v}\}$ is linearly independent.

EXAMPLE 15.14. The *standard basis* of F^n is a linearly independent set.

LECTURE 16

Bases of vector spaces

We saw in Proposition 15.12 that a set S is linearly independent if and only if whenever we have an equation of the form

$$\sum_{\mathbf{v}\in S} a_{\mathbf{v}}\mathbf{v} = \mathbf{0},$$

we must have $a_{\mathbf{v}} = 0$ for all $\mathbf{v}$. In general, any equation of the above sort is called a *linear relation between the elements of* S. If all the $a_{\mathbf{v}}$ are equal to 0, we say that this relation is *trivial*. Thus, our result can be summarized by saying that a set S is linearly independent if and only if *every linear relation between its elements is trivial*.

LEMMA 16.1. *Let V be a vector space and let S be a subset of V which is linearly independent. If $\mathbf{v} \in V\backslash span(S)$, then $S \cup \{\mathbf{v}\}$ is linearly independent.*

PROOF. Let us denote the set $S \cup \{\mathbf{v}\}$ by T. Suppose we have some linear relation $\sum_{\mathbf{w}\in T} a_{\mathbf{w}}\mathbf{w} = \mathbf{0}$. We will prove that $a_{\mathbf{w}} = 0$ for all $\mathbf{w} \in T$.

If the coefficient $a_{\mathbf{v}}$ of $\mathbf{v}$ is 0, then we see that $\sum_{\mathbf{w}\in S} a_{\mathbf{w}}\mathbf{w} = \mathbf{0}$. As S is assumed to be linearly independent, we see that $a_{\mathbf{w}} = 0$ for all $\mathbf{w} \in S$. Thus, as we already have assumed that conclude that $a_{\mathbf{v}} = 0$, we conclude that $a_{\mathbf{w}} = 0$ for all $\mathbf{w} \in S \cup \{\mathbf{v}\} = T$.

Now suppose that $a_{\mathbf{v}} \neq 0$. Then we may write

$$\mathbf{v} = \sum_{\mathbf{w}\in S} \left(\frac{a_{\mathbf{w}}}{a_{\mathbf{v}}}\right) \cdot \mathbf{w}$$

which shows that $\mathbf{v} \in Span(S)$, which contradicts our assumption. Thus, we cannot have $a_{\mathbf{v}} \neq 0$. This completes the proof. □

DEFINITION 16.2. Let V be a vector space. A subset S of V is said to be a *spanning set* of V if $span(S) = V$. In this case, we also say that the set S *spans* V.

A *basis* of V is defined to be a spanning set which is linearly independent.

CONVENTION 16.3. The plural form of the word "basis" is "bases".

Clearly, every vector space has at least one spanning set. Indeed, the whole space V can be considered as a spanning set of itself! However, it is not clear that every vector space has a basis. This is true, and we will give a heuristic argument below for this. However, we will not give a rigorous proof. First we deduce some basic properties of bases from the definition.

PROPOSITION 16.4. *Let V be a vector space and let S be a basis of V.*

(a) *Let $\mathbf{v} \in S$. Then $S\backslash\{v\}$ does not span V.*
(b) *Let $\mathbf{w} \in V\backslash S$. Then the set $S \cup \{\mathbf{w}\}$ is not linearly independent.*

PROOF. If $S\backslash\{\mathbf{v}\}$ spans V, then $\mathbf{v} \in span(S\backslash\{v\})$. But then, by definition, S is not linearly independent and hence cannot be a basis. This is a contradiction and so our assumption that $S\backslash\{\mathbf{v}\}$ must be wrong. This proves (a).

Suppose $T := S \cup \{\mathbf{w}\}$ is linearly independent. Then $\mathbf{w}$ cannot be in the span of $T\backslash\{\mathbf{w}\} = S$. This contradicts the given fact that $span(S) = V$. Thus, our assumption that T is linearly independent must be incorrect. This proves (b). □

This shows that a basis of a vector space is finely balanced between being a spanning set and being linearly independent. If we try to enlarge it, it ceases to be linearly independent. If we try to diminish it, it ceases to be a spanning set. The following discussion will clarify this further.

Let us say that a subset S of V is a *minimal spanning set* if no proper subset T of S is a spanning set of V. (*Definition*: A B is said to be a *proper subset* of a set A if $B \subset A$, but $B \neq A$.) So the above proposition shows that every basis is a minimal spanning set. Conversely, suppose that S is a minimal spanning set. Then, we claim that it must be linearly independent. Indeed, if it is not so, then there exists some $\mathbf{v} \in S$ such that $\mathbf{v} \in span(S\backslash\{\mathbf{v}\})$. But then $span(S\backslash\{v\} = span(S) = V$. Thus, $S\backslash\{\mathbf{v}\}$ is also a spanning set of V, which contradicts the minimality of S. So, S is linearly independent. Thus, *a spanning set is a basis if and only if it is minimal.*

On the other hand, we say that a subset S of V is a *maximal linearly independent set* if no set T which *properly contains* S (i.e. $S \subset T$ but $S \neq T$) is linearly independent. The above proposition shows that every basis is a maximal linearly independent set. Conversely, suppose that S is a maximal linearly independent set. Then we claim that $span(S) = V$. Indeed, if this is not so, let $\mathbf{v} \in V\backslash span(S)$. Then Lemma 16.1 shows that $S \cup \{\mathbf{v}\}$ is also a linearly independent set. This contradicts the maximality of S. So, $span(S) = V$. Thus, *a linearly independent set is a basis if and only if it is maximal.*

Existence of bases – a heuristic argument: Clearly every vector space V has at least one linearly independent set, i.e. $\varnothing$. We saw in Lemma 16.1 that if a linearly idependent set is not a basis, it can be enlarged. So if $\varnothing$ is not a basis for V (i.e. if V is not the zero space), then we enlarge it to a bigger linearly independent set S_1. If S_1 is not a basis, we enlarge it to a bigger linearly independent set S_2 ... and so on. This is almost a proof, but the phrase "and so on" at the end is not very rigorous. It takes some work to get rid of that phrase and we will not do that in this course.

We may also try to construct a basis "from the opposite end". Since a basis is a minimal spanning set, we could start with a large spanning set and then try to shrink it till it becomes minimal, and hence linearly independent. So for instance, we can start with the set V. If V is not a basis for itself, we can find a $\mathbf{v}$ in V such that $T_1 := V\backslash\{\mathbf{v}\}$ is spans V. If T_1 is not a basis, we can find remove yet another vector from it, ... and so on. Again, this argument can also be made rigorous with some work.

Though we are not going to prove it in full generality, we will formally state the result.

THEOREM 16.5. *Every vector space has a basis.*

A special case:

DEFINITION 16.6. A vector space V is said to be *finite dimensional* if it has a finite spanning set.

THEOREM 16.7. *Let V be a finite dimensional vector space. Then V has a basis. Indeed, any spanning set of V contains a subset which is a basis.*

PROOF. By assumption, there exists a finite set S such that $span(S) = V$. Suppose $|S| = n$. (*Notation:* For any set A, we will denote its cardinality by $|A|$.) If S is not a basis, there exists an element $\mathbf{v} \in S$ such that $S_1 := S\backslash\{\mathbf{v}\}$ spans V. If S_1 is not a basis, we can again remove an element from it in such a way that the resulting set S_2 spans V. We continue in this manner. This process can continue for at most n steps since S has only n elements. Thus, we will find a basis within n steps. □

QUESTION 16.8. Can we also construct a basis by enlarging linearly independent sets?

Yes, we can, but it will take some work to show that the process terminates.

PROPOSITION 16.9. *Let V be a vector space and let $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ be an ordered sequence (an n-tuple) of elements of V. There exists a unique linear transformation $T : F^n \to V$ such that $T(\mathbf{e}_i) = \mathbf{v}_i$ for $1 \leqslant i \leqslant n$. Also, if S denotes the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, then $im(T) = span(S)$.*

PROOF. Any element $\mathbf{x} \in F^n$ can be uniquely written as a linear combination of the elements of the standard basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ in the form

$$\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n.$$

Indeed, it is easy to see that the only x_i which will satisfy this equation are the ones that occur as entries of the matrix $\mathbf{x}$.

Then, we define

$$T(\mathbf{x}) = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n.$$

Now we need to show that the function T defined by the above formula is linear. So, let $\mathbf{x}$ and $\mathbf{y}$ be two elements of F^n and let $a, b \in F$. Then we see that

$$a\mathbf{x} + b\mathbf{y} = \sum_{i=1}^{n}(ax_i + by_i)\mathbf{e}_i.$$

As there can be only one way $a\mathbf{x} + b\mathbf{y}$ can be written as a linear combination of the $\mathbf{e}_i$, we see that

$$\begin{aligned} T(a\mathbf{x} + b\mathbf{y}) &= \sum_{i=1}^{n}(ax_i + by_i)\mathbf{v}_i \\ &= a\left(\sum_{i=1}^{n} x_i\mathbf{e}_i\right) + b\left(\sum_{i=1}^{n} y_i\mathbf{e}_i\right) \\ &= aT(\mathbf{x}) + bT(\mathbf{y}). \end{aligned}$$

Thus, T is linear.

Now we need to show that T is unique. Suppose $T_1 : F^n \to V$ is another linear transformation with the same properties. Then, given any $\mathbf{x} \in F^n$, we first write $\mathbf{x}$ as a linear combination of the $\mathbf{e}_i$ as above and then compute

$$T_1(\mathbf{x}) = T_1(\sum_{i=1}^{n} x_i\mathbf{e}_i) = \sum_{i=1}^{n} x_iT_1(\mathbf{e}_i) = \sum_{i=1}^{n} x_i\mathbf{v}_i = T(\mathbf{x}).$$

This shows that $T_1 = T$. Thus T is the only linear transformation with the given property.

Now we first show that that $im(T) \subset span(S)$. Suppose $\mathbf{x} \in im(T)$. Thus, there exists some $\mathbf{a} = [a_1, \ldots, a_n]^{tr}$ in F^n such that $T(\mathbf{a}) = \mathbf{x}$. As $\mathbf{a} = \sum_{i=1}^{n} a_i\mathbf{e}_i$, we see that

$$\mathbf{x} = T(\mathbf{a}) = T(\sum_{i=1}^{n} a_i\mathbf{e}_i) = \sum_{i=1}^{n} a_iT(\mathbf{e}_i) = \sum_{i=1}^{n} a_i\mathbf{v}_i.$$

This shows that $\mathbf{x} \in span(S)$. As $\mathbf{x} \in im(T)$ was arbitary, we see that $im(T) \subset span(S)$.

Now we show that $span(S) \subset im(T)$. Suppose $\mathbf{x} \in span(S)$. Thus, there exist $a_1, \ldots, a_n$ such that $\mathbf{x} = \sum_{i=1}^{n} a_i\mathbf{v}_i$. Then, if $\mathbf{a} = \sum_{i=1}^{n} a_i\mathbf{e}_i$, we see that

$$T(\mathbf{a}) = T(\sum_{i=1}^{n} a_i\mathbf{e}_i) = \sum_{i=1}^{n} a_iT(\mathbf{e}_i) = \sum_{i=1}^{n} a_i\mathbf{v}_i = \mathbf{x}.$$

As $\mathbf{x} \in span(S)$ was arbitrary, we see that $span(S) \subset im(T)$. □

EXAMPLE 16.10. The above result is particularly obvious when V is equal to F^m. Indeed, suppose we are given m vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Then the required transformation T taking $\mathbf{e}_i$ to $\mathbf{v}_i$ is exactly the one associated with the matrix A which has $\mathbf{v}_i$ as its i-th column.

PROPOSITION 16.11. *Let V be a vector space and let $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an n-tuple of elements of V. Let T be the unique linear map from F^n to V such that $T(\mathbf{e}_i) = \mathbf{v}_i$ for $1 \leqslant i \leqslant n$. Then the set $S := \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly independent if and only if $ker(T) = \{\mathbf{0}\}$.*

PROOF. Suppose $ker(T) \neq \{\mathbf{0}\}$. Then, there exists a vector $\mathbf{a} = [a_1, \ldots, a_n]^{tr}$ in F^n such that $T(\mathbf{a}) = 0$, but $\mathbf{a} \neq 0$. But, we see that $\mathbf{a} = \sum_{i=1}^n a_i \mathbf{e}_i$, and hence, by definition,

$$T(\mathbf{a}) = \sum_{i=1}^n a_i T(\mathbf{e}_i) = \sum_{i=1}^n a_i \mathbf{v}_i.$$

Thus, $\sum_{i=1}^n a_i \mathbf{v}_i = 0$. But as $\mathbf{a} \neq \mathbf{0}$, we must have $a_i \neq 0$ for some i. Thus,

$$\sum_{i=1}^n a_i \mathbf{v}_i = \mathbf{0}.$$

This is a non-trivial linear relation between the $\mathbf{v}_i$ and hence they are not linearly independent. Thus, if the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly independent, we must have $ker(T) = \{\mathbf{0}\}$.

Conversely, suppose that the $ker(T) = \{\mathbf{0}\}$. Suppose that the $\mathbf{v}_i$ are not linearly independent and so there exists a non-trivial linear relation

$$\sum_{i=1}^n a_i \mathbf{v}_i = \mathbf{0}.$$

Then, if we set $\mathbf{a} = \sum_{i=1}^n a_i \mathbf{e}_i = [a_1, \ldots, a_n]^{tr}$, we see that $T(\mathbf{a}) = 0$. However as the given linear relation is non-trivial, there is some $a_i \neq 0$ and hence $\mathbf{a} \neq \mathbf{0}$. This contradicts our assumption that $ker(T) = \{\mathbf{0}\}$. Thus, we see that the $\mathbf{v}_i$ must be linearly independent. □

We have a corresponding result for spanning sets.

PROPOSITION 16.12. *Let V be a vector space and let $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an n-tuple of elements of V. Let T be the unique linear map from F^n to V such that $T(\mathbf{e}_i) = \mathbf{v}_i$ for $1 \leqslant i \leqslant n$. Then the set $S := \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a spanning set of V if and only if $im(T) = V$.*

PROOF. We saw in Proposition 16.9 that $im(T) = span(S)$. Thus, we see that S is a spanning set if and only if $im(T) = span(S)$ is equal to V. □

We will put the last two propositions together into a rather neat criterion or a set to be a basis:

COROLLARY 16.13. *Let V be a vector space and let $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an n-tuple of elements of V. Let T be the unique linear map from F^n to V such that $T(\mathbf{e}_i) = \mathbf{v}_i$ for $1 \leqslant i \leqslant n$. Then the set $S := \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V if and only if T is an isomorphism of vector spaces.*

PROOF. This is an immediate consequence of Proposition 16.11 and Proposition 16.12. □

In the next lecture, we will be able to resolve Question 16.8.

LECTURE 17

Dimension

We look at an example which illustrates the core idea behind Proposition 16.9.

EXAMPLE 17.1. Let $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbb{R}^2$ be as follows:

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \qquad \mathbf{v}_2 = \begin{bmatrix} 2 \\ 0 \end{bmatrix} \qquad \mathbf{v}_3 = \begin{bmatrix} 5 \\ -1 \end{bmatrix}$$

Let $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$ in $\mathbb{R}^2$ be as follows:

$$\mathbf{w}_1 = \begin{bmatrix} 3 \\ 2 \\ 0 \end{bmatrix} \qquad \mathbf{w}_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \qquad \mathbf{w}_3 = \begin{bmatrix} 6 \\ 0 \\ -2 \end{bmatrix}$$

Does there exist a linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^3$ such that $T(\mathbf{v}_1) = \mathbf{w}_1$, $T(\mathbf{v}_2) = \mathbf{w}_2$ and $T(\mathbf{v}_3) = \mathbf{w}_3$?

Observe that $\mathbf{v}_1 + 2\mathbf{v}_2 = \mathbf{v}_3$. However, $\mathbf{w}_1 + 2\mathbf{w}_2 \neq \mathbf{w}_3$. Clearly, this implies that no such T can exist.

More generally, suppose V and W are vector spaces and let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ and $\mathbf{w}_1, \ldots, \mathbf{w}_n \in W$. Suppose there exists a linear transformation $T : V \to W$ such that $T(\mathbf{v}_i) = \mathbf{w}_i$ for all i. Then if we have a linear relatoin

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots a_n\mathbf{v}_n = 0,$$

we must also have

$$a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \ldots a_n\mathbf{w}_n = 0.$$

Thus, in informal terms, we may say the existence of such a transformation T implies that *every linear relation satisfied by* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *is also satisfied by* $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$. However, note that the *converse need not be true.*

There is one obvious relation satisfied by the $\mathbf{v}_i$, namely the one in which all $a_i = 0$. This is the *trivial relation.* Clearly, this relation is also satisfied by the $\mathbf{w}_i$. However, any *other* relation satisfied by the $\mathbf{v}_i$ imposes a condition on the $\mathbf{w}_i$, which they must satisfy if the transformation T is to exist. However, suppose that there are no non-trivial relations on the $\mathbf{v}_i$. In other words, suppose that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent. Would that guarantee the existence of the transformation T? Yes, it would. However, in general this transformation need not be unique. See the following example.

EXAMPLE 17.2. Let $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{R}^3$ be as follows:

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \qquad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Let $\mathbf{w}_1, \mathbf{w}_2$ in $\mathbb{R}^3$ be as follows:

$$\mathbf{w}_1 = \begin{bmatrix} 3 \\ 2 \\ 0 \end{bmatrix} \qquad \mathbf{w}_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Again, we ask whether there exists a linear transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ such that $T(\mathbf{e}_1) = \mathbf{w}_1$, $T(\mathbf{e}_2) = \mathbf{w}_2$?

Actually, it turns out that there are infinitely many such linear transformations. Indeed, let $\mathbf{e}_3 = \begin{bmatrix}0 & 0 & 1\end{bmatrix}^{tr}$. Choose *any* element $\mathbf{w}_3$ of $\mathbb{R}^3$. Then, we can easily construct a linear transformation T such that $T(\mathbf{e}_i) = \mathbf{w}_i$ for $i = 1, 2, 3$. This is the linear transformation $T(\mathbf{x}) = A\mathbf{x}$ where A is the 3×3 matrix which has $\mathbf{w}_i$ as its i-th column. As $\mathbf{w}_3$ was arbitrary, clearly there are infinitely many such linear transformations.

A careful examination of the last example reveals why T was not unique. Picking the images of $\mathbf{v}_1$ and $\mathbf{v}_2$ only fixes the images for all the vectors that are in the span of $\mathbf{v}_1$ and $\mathbf{v}_2$. However, for any $\mathbf{v}$ which is not in the span of these two vectors, the image can be chosen freely, which allows us to create infinitely many transformations having the required property. So, if one wants to ensure that T is unique, the $\mathbf{v}_i$ must also span V. Hence, they must form a basis of V. This is exactly what we have in Proposition 16.9 since the "standard basis" is actually a basis of F^n. In general, the analogue of Proposition 16.9 will hold for *any* basis. This is proved below:

PROPOSITION 17.3. *Let V and W be vector spaces. Let $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ be an ordered sequence (an n-tuple) of elements of V such that the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V. Let $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n)$ be an ordered sequence of elements of W. There exists a unique linear transformation $T : F^n \to V$ such that $T(\mathbf{v}_i) = \mathbf{w}_i$ for $1 \leqslant i \leqslant n$. Also, if S denotes the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, then $im(T) = span(S)$.*

PROOF. As usual, let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the standard basis of F^n. By Corollary 16.13, there exists a unique isomorphism $S_1 : F^n \to V$ such that $S_1(\mathbf{e}_i) = \mathbf{v}_i$ for $1 \leqslant i \leqslant n$. By Proposition 17.3, there exists a unique linear transformation $S_2 : F^n \to W$ such that $S_2(\mathbf{e}_i) = \mathbf{w}_i$ for $1 \leqslant i \leqslant n$. Let S_1^{-1} denote the inverse of S_1. Then, we define T to be the composition $S_2 \circ S_1^{-1}$. In other words, $T(\mathbf{v})$ is defined to be $S_2(S^{-1}(\mathbf{v}))$ for every $\mathbf{v} \in V$. Then, it is easy to see that $T(\mathbf{v}_i) = \mathbf{w}_i$ for every i.

To see the uniqueness, suppose that $T_1 : V \to W$ is some other linear transformation which satisfies $T_1(\mathbf{v}_i) = \mathbf{w}_i$ for every i. Then, consider the linear transformation $T_1 \circ S_1 : F^n \to W$. We see that

$$T_1 \circ S_1(\mathbf{e}_i) = T_1(S_1(\mathbf{e}_i)) = T_1(\mathbf{v}_i) = \mathbf{w}_i$$

for all i. However, we know that S_2 is the unique linear transformation from F^n to W such that $S_2(\mathbf{e}_i) = \mathbf{w}_i$. Thus, we must have $S_2 = T_1 \circ S_1$. Thus $S_2 \circ S_1^{-1} = T_1 \circ S_1 \circ S_1^{-1} = T_1$. Thus $T_1 = T$. This proves the uniqueness of T. □

We will now use the results from the previous lecture to define the notion of dimension and to resolve Question 16.8.

LEMMA 17.4. *Let m and n be two positive integers such that $m > n$. Let $T : F^m \to F^n$ be a linear transformation. Then T cannot be injective.*

PROOF. We know that there exists an $n \times m$ matrix A such that $T(\mathbf{x}) = A\mathbf{x}$. Let $X_1, \ldots, X_m$ be variables and let $\mathbf{X}$ be the column matrix defined by

$$\mathbf{X} = \begin{bmatrix}X_1 & X_2 & \cdots & X_m\end{bmatrix}^{tr}.$$

Consider the matrix equation $A\mathbf{X} = \mathbf{0}$. This is essentially a system of n linear equations in m variables. If we apply the row reduction algorithm to this system, there must be at least one free variable in the row reduced echelon form because $m > n$. This means that this system has at least one non-trivial solution, i.e. a solution in which at least some X_i takes a non-zero value. This implies that there exists some $\mathbf{x} \in F^m$ such that $\mathbf{x} \neq \mathbf{0}$ and $A\mathbf{x} = 0$. Thus, $ker(T)$ is not the zero space. By Lemma 15.3, this implies that T is not injective. □

This lemma has a useful corollary:

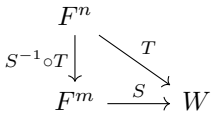
COROLLARY 17.5. *Let m and n be positive integers such that $m \neq n$. Then F^m and F^n are not isomorphic.*

PROOF. We may assume without loss of generality that $m > n$. (If this is not so, i.e. if $n > m$, we may simply interchange the role of m and n in this argument.) Then, Lemma 17.4 shows that there is no injective linear transformation from F^m to F^n. In particular, there is no isomorphism from F^m to F^n. □

THEOREM 17.6. *Let m be a positive integer. Let V be a vector space having a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$. Let n be another positive integer and let $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ be a linearly independent set in V. Then $n \leqslant m$.*

PROOF. Suppose that $n > m$. We will obtain a contradiction.

Let $\mathbf{e}_1, \ldots, \mathbf{e}_m$ be the standard basis of F^m and let $\mathbf{f}_1, \ldots, \mathbf{f}_n$ be the standard basis of F^n. Then, we know from Corollary 16.13 that there exists a unique isomorphism $S : F^m \to V$ such that $S(\mathbf{e}_i) = \mathbf{v}_i$ for $1 \leqslant i \leqslant m$. By Proposition 16.9, there exists a unique linear transformation $T : F^n \to V$ such that $T(\mathbf{f}_i) = \mathbf{w}_i$ for $1 \leqslant i \leqslant n$. By Proposition 16.11, as $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ is linearly independent, $ker(T) = \{\mathbf{0}\}$. By Lemma 15.3, we see that T is injective. Then, the linear transformation $S^{-1} \circ T : F^n \to F^m$ is injective. (Exercise: Do you see why this linear transformation is injective?)



However, we know from Lemma 17.4 that this linear transformation cannot be injective. This is a contradiction. Thus, we must have $n \leqslant m$. □

The following corollary is an immediate consequence:

COROLLARY 17.7. *Let V be a finite dimensional vector space. Then, any linearly independent set in V is finite. In particular, any basis of V is finite.*

PROOF. Since V is finite dimensional, it has a finite spanning set S. By Theorem 16.7, there exists a subset of S which is a basis of V. Thus, V has a finite basis. Suppose that it has a basis consisting of m elements where m is a positive integer. Then, Theorem 17.6 shows that any linearly independent subset of V can have at most m elements. Thus, any linearly independent subset of V is finite. □

THEOREM 17.8. *Let V be a finite dimensional vector space. Any two bases of V have the same number of elements.*

PROOF. Let B_1 and B_2 be two bases of V. By Corollary 17.7, both B_1 and B_2 are finite sets. Suppose B_1 has m elements and B_2 has n elements. By Theorem 17.6, we see that $m \leqslant n$ and $n \leqslant m$. Thus $m = n$. □

Finally, we are now able to define the dimension of a finite dimensional space!

DEFINITION 17.9. The *dimension* of a finite dimensional space V is the number of elements in any basis of V.

As promised, we also answer Question 16.8.

Constructing a basis by expanding a linearly independent set:

We will show that in a finite dimensional vector space, any linearly independent set can be expanded to a basis. (This result is actually true even for spaces which are not finite dimensional.)

Let n be an integer and let V be an n-dimensional vector space. Let S be a linearly independent subset of V. Suppose that $|S| = m$. We will use induction to

construction a sequence $S_0 \subset S_1 \subset S_2 \ldots$ of subsets of V with $S_0 = S$ and show that this sequence actually must terminate at some finite stage to give a basis of V.

If S is a spanning set, it is also a basis. If not, we find a non-zero element $\mathbf{v}_1$ of V such that $\mathbf{v}_1 \notin span(S)$. We define $S_1 = S \cup \{\mathbf{v}_1\}$. We know from Lemma 16.1 that S_1 is a linearly independent set.

Now, suppose that the linearly independent set S_k has been constructed for some integer k. If S_k spans V, then S_k is a basis of V. If not, there exists some $\mathbf{v}_{k+1} \in V$ such that $\mathbf{v}_{k+1} \notin span(S_k)$. We define $S_{k+1} = S_k \cup \{\mathbf{v}_{k+1}\}$. We know from Lemma 16.1 that S_{k+1} is a linearly independent set.

Note that $|S_k| = k + m$ for every k. However, as S_k is a linearly independent subset of V, by Theorem 17.6, we must have $k + m \leqslant n$. Thus, this process can continue only for $n - m$ steps and S_{n-m} will actually be a basis of V. We record our result as follows:

THEOREM 17.10. *Let V be a finite dimensional vector space. Let S be a linearly independent subset of V. Then, there exists a basis B of V such that $S \subset B$.*

LECTURE 18

Matrix representation with respect to a basis

Let V be a vector space. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of V. Let $\mathbf{v}$ be any element of V. By Proposition 15.12 we know that there exist unique elements $a_1, \ldots, a_n \in F$ such that

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n.$$

Thus, the sequence of elements of F $(a_1, \ldots, a_n)$ can be said to be the list of coordinates of the element $\mathbf{v}$ with respect to the basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. However, note that the order in which the elements $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are listed does matter. For instance, if we were to list these elements as $\mathbf{v}_2, \mathbf{v}_1, \mathbf{v}_3, \ldots, \mathbf{v}_n$, then the associated sequence of coordinates becomes $(a_2, a_1, a_3, \ldots, a_n)$. Thus, we should be working with an *ordered basis* (i.e. a basis with a given fixed order). If fix an order on the basis, such as $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$, then we can associate the column matrix $\begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix}^{tr}$ to the element $\mathbf{v}$. This gives us a bijection between the vector space V and the set F^n. However, the column matrix $\begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix}^{tr}$ depends on the choice of the ordered basis $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$. We will now explore how this column matrix associated to $\mathbf{v}$ changes if a different ordered basis is used.

Above, the ordered basis has been represented by an n-tuple (i.e. a list of n-elements) $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$. It will be more convenient to look at this n-tuple as a an $1 \times n$ matrix (i.e. a "row matrix") with entries from the vector space V, for reasons that will soon become clear. To this end, we introduce the notion of matrices with vector entries.

DEFINITION 18.1. Let V be a vector space. Let m and n be positive integers. An $m \times n$ *matrix* $\mathcal{A}$ with entries from V is a collection of mn elements of V arranged in a rectangular array as follows:

$$\begin{bmatrix} \mathbf{v}_{11} & \cdots & \cdots & \mathbf{v}_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \mathbf{v}_{m1} & \cdots & \cdots & \mathbf{v}_{mn} \end{bmatrix}$$

The element in the i-th row and j-th column is called the (i, j)-*entry* of the matrix and is denoted in the above representation as $\mathbf{v}_{ij}$. The above matrix may also be written in the short form $(\mathbf{v}_{ij})_{i,j}$ if the number of rows and columns is understood.

The set of all $m \times n$ matrices with entries from V will be denoted by $M_{m\times n}(V)$.

REMARK 18.2. Recall that for positive integers m and n, the set $M_{m\times n}(F)$ of $m \times n$ matrices having entries from F forms a vector space with the obvious notions of addition and scalar multiplication. It is easy to see that $M_{m\times n}(V)$ too is a vector space.

EXAMPLE 18.3. Let us take $V = \mathbb{R}^2$. Then an example of a 2×3 matrix with entries in V would look like the following:

$$\begin{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 3 \\ 1 \end{bmatrix} & \begin{bmatrix} 2 \\ 0 \end{bmatrix} & \begin{bmatrix} 3 \\ 3 \end{bmatrix} \end{bmatrix}$$

Of course, this looks cumbersome. Normally, we will give the 2×1 matrices inside the big matrix some names like $\mathbf{v}_{11}, \mathbf{v}_{12}$, etc. and write this matrix as

$$\begin{bmatrix} \mathbf{v}_{11} & \mathbf{v}_{12} & \mathbf{v}_{13} \\ \mathbf{v}_{21} & \mathbf{v}_{22} & \mathbf{v}_{23} \end{bmatrix}$$

which looks a little better, but means the same thing.

Of course, it is not necessary that we will work only with vector spaces of the form $\mathbb{R}^2$, $\mathbb{R}^3$, etc. We may also be working with an abstract vector spaces V, in which case the matrix will not look like the first one in this example.

Obviously, for any positive integers m and n, the set of all $m \times n$ matrices with entries from V forms a vector space. However, it is clear that we cannot meaningfully define the product of two matrices with entries from V since the product of two vectors is not defined. On the other hand, using scalar multiplication, we can multiply a matrix having entries from V with a matrix having entries from F, as long as their shapes are compatible.

CONVENTION 18.4.

(a) In general, we will denote matrices with entries in a vector space V with capital letters in a calligraphic font, such as $\mathcal{A}$, $\mathcal{B}$, etc. Matrices with entries in a field F will be denoted with ordinary capital letters, such as A, B, etc.
(b) If V is a vector spaces and $\mathbf{v}$, is in V, the 1×1 matrix $\begin{bmatrix} \mathbf{v} \end{bmatrix}$ will simply be written as $\mathbf{v}$ (without the square brackets). This abuse of notation will be seen to be useful below.

DEFINITION 18.5. (Definition of matrix product) Let V be a vector space and let $\mathcal{A} = (\mathbf{v}_{ij})_{i,j}$ be an $m \times n$ matrix having entries from V. We will define its product with matrices having entries from F as follows:

(1) Let $B = (b_{jk})_{j,k}$ be an $n \times p$ matrix with entries in F. The product $\mathcal{A}B$ is an $m \times p$ matrix $\mathcal{X} = (\mathbf{w}_{ik})_{i,k}$ having entries in V such that

$$\mathbf{w}_{ik} = \sum_{j=1}^{n} b_{jk} \mathbf{v}_{ij}.$$

(2) Let $C = (c_{ki})_{k,i}$ be an $p \times m$ matrix with entries in F. The product $C\mathcal{A}$ is a $p \times n$ matrix $\mathcal{X} = (\mathbf{w}_{kj})_{k,j}$ having entries in V such that

$$\mathbf{w}_{kj} = \sum_{i=1}^{m} c_{ki} \mathbf{v}_{ij}.$$

LEMMA 18.6. *The above product satisfies the associative property and also the distributive property with respect to addition of matrices.*

PROOF. (The proof is left as an an easy exercise.) □

Generally, we will not be interested in very big matrices having entries in V. Indeed, we will only consider *row matrices* (i.e. matrices having a single row) with entries in V. The most common use will be the following:

DEFINITION 18.7 (Ordered basis). Let n be a positive integer. Let V be a an n-dimensional vector space. An *ordered basis* of V is a $1 \times n$ matrix

$$\mathcal{B} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \end{bmatrix}$$

having entries in V such that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V.

EXAMPLE 18.8. Recall that $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ denotes the standard basis of $\mathbb{R}^3$ (so that $\mathbf{e}_i$ has 1 in the i-th row and 0's elsewhere). Then,

$$\begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \end{bmatrix}$$

is an ordered basis of $\mathbb{R}^3$, and so is

$$\begin{bmatrix} \mathbf{e}_3 & \mathbf{e}_2 & \mathbf{e}_1 \end{bmatrix}.$$

Note that these *ordered* bases are different even though they have the same entries.

EXAMPLE 18.9. The 1×2 matrix

$$\begin{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ -1 \end{bmatrix} \end{bmatrix}$$

is an ordered basis of $\mathbb{R}^2$.

DEFINITION 18.10. Let n be a positive integer. Let V be an n-dimensional vector space. Let $\mathcal{B} = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix}$ be an ordered basis of V. Let $\mathbf{v}$ any element of V. We write $\mathbf{v}$ as a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ as follows:

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n.$$

Then, we define the *matrix representation of* $\mathbf{v}$ *with respect to* $\mathcal{B}$ by

$$M_{\mathcal{B}}(\mathbf{v}) = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

(This is well-defined because the a_i are uniquely determined by $\mathbf{v}$.)

With the notation in the above definition, we see that

$$\begin{aligned} \mathcal{B} \cdot M_{\mathcal{B}}(\mathbf{v}) &= \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \\ &= \begin{bmatrix} a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{v} \end{bmatrix}. \end{aligned}$$

However, by Convention 18.4, Part (b), we are choosing to write the 1×1 matrix $\begin{bmatrix} \mathbf{v} \end{bmatrix}$ as just $\mathbf{v}$. Thus, we have proved the following rather elegant result.

LEMMA 18.11. *Let V be a finite dimensional vector space. Let $\mathcal{B}$ be an ordered basis of V and let $\mathbf{v}$ be an element of V. Then,*

$$\mathbf{v} = \mathcal{B} \cdot M_{\mathcal{B}}(\mathbf{v}).$$

We will now strengthen this result as follows:

THEOREM 18.12. *Let n be a positive integer. Let V be an n-dimensional vector space. Let $\mathcal{B}$ be an ordered basis of V. Then, we define functions $\phi : V \to F^n$ and $\psi : F^n \to V$ by*

$$\phi(\mathbf{v}) = M_{\mathcal{B}}(\mathbf{v})$$

for every $\mathbf{v} \in V$, and

$$\psi(\mathbf{x}) = \mathcal{B} \cdot \mathbf{x}$$

for every $\mathbf{x} \in F^n$. Then, ϕ and ψ are linear transformations. Also, ϕ and ψ are inverses of each other and thus define an isomorphism of vector spaces between V and F^n.

PROOF. Before we prove the linearity, we will show that ϕ and ψ are inverses of each other. This will show that they set up a bijection between V and F^n (though we will still need to check the linearity after that to establish that these are isomorphisms of vector spaces). For $\mathbf{v} \in V$, we have

$$\psi(\phi(\mathbf{v})) = \mathcal{B} \cdot \phi(\mathbf{v}) = \mathcal{B} \cdot M_{\mathcal{B}}(\mathbf{v}) = \mathbf{v}$$

where the last equality follows from the previous lemma. Thus, $\psi \circ \phi$ is the identity function on V. On the other hand, suppose $\mathbf{x} \in F^n$. Suppose

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Then

$$\psi(\mathbf{x}) = \mathcal{B} \cdot \mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n.$$

By definition, we have

$$M_{\mathcal{B}}(x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \mathbf{x}.$$

This shows that $\phi \circ \phi$ is the identity function on F^n. Thus ϕ and ψ are inverses of each other, and are hence bijections.

Suppose $\mathbf{v}$ and $\mathbf{w}$ are elements of V and let $a, b \in F$. We first write $\mathbf{v}$ and $\mathbf{w}$ as linear combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_n$:

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$$
$$\mathbf{w} = b_1\mathbf{v}_1 + \cdots + b_n\mathbf{v}_n$$

Then, we have

$$a\mathbf{v} + b\mathbf{w} = (a \cdot a_1 + b \cdot b_1)\mathbf{v}_1 + \cdots + (a \cdot a_n + b \cdot b_n)\mathbf{v}_n.$$

By definition, we have the following equalities:

$$M_{\mathcal{B}}(\mathbf{v}) = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \qquad M_{\mathcal{B}}(\mathbf{w}) = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \qquad M_{\mathcal{B}}(a\mathbf{v} + b\mathbf{w}) = \begin{bmatrix} a \cdot a_1 + b \cdot b_1 \\ \vdots \\ a \cdot a_n + b \cdot b_n \end{bmatrix}$$

Thus, we see that $M_{\mathcal{B}}(a\mathbf{v} + b\mathbf{w}) = aM_{\mathcal{B}}(\mathbf{v}) + bM_{\mathcal{B}}(\mathbf{w})$ and hence

$$\phi(a\mathbf{v} + b\mathbf{w}) = a\phi(\mathbf{v}) + b\phi(\mathbf{w}).$$

This shows that ϕ is linear, and hence is a vector space isomorphism. □

REMARK 18.13. The fact that the map ψ is a bijection implies that if $\mathbf{x}$ and $\mathbf{y}$ are in F^n such that $\mathcal{B} \cdot \mathbf{x} = \mathcal{B} \cdot \mathbf{y}$, then $\mathbf{x} = \mathbf{y}$. Thus, it is as if we can "cancel" $\mathcal{B}$ from the equation $\mathcal{B} \cdot \mathbf{x} = \mathcal{B} \cdot \mathbf{y}$. Of course, one should understand that this "cancellation" is not really "division by $\mathcal{B}$". Instead, it just means that we are applying the function ϕ to both sides of the equation and applying Lemma 18.11.

We will now generalize this construction a little further.

DEFINITION 18.14. Let n be a positive integer and let V be an n-dimensional vector space. Let $\mathcal{B}$ be an ordered basis of V. Let k be a positive integer and let

$$\mathcal{A} = \begin{bmatrix} \mathbf{w}_1 & \cdots & \mathbf{w}_k \end{bmatrix}$$

be a $1 \times k$ matrix having entries in V. Then, we define the *matrix representation of $\mathcal{A}$ with respect to $\mathcal{B}$* to be a $n \times k$ matrix, denoted by $M_{\mathcal{B}}(\mathcal{A})$ such that its i-th column is equal to $M_{\mathcal{B}}(\mathbf{w}_i)$.

EXAMPLE 18.15. Let us take $V = \mathbb{R}^2$ let $\mathcal{B} = \begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_2 \end{bmatrix}$ be the standard basis with the usual order. Suppose

$$\mathcal{A} = \begin{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} & \begin{bmatrix} 2 \\ 0 \end{bmatrix} & \begin{bmatrix} 3 \\ 3 \end{bmatrix} \end{bmatrix}.$$

Then,

$$M_{\mathcal{B}}(\mathcal{A}) = \begin{bmatrix} 3 & 2 & 3 \\ 1 & 0 & 3 \end{bmatrix}.$$

Now consider the ordered basis

$$\mathcal{C} = \begin{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ -1 \end{bmatrix} \end{bmatrix}.$$

Then, we observe the following equalities:

$$\begin{bmatrix} 3 \\ 1 \end{bmatrix} = 2 \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$
$$\begin{bmatrix} 2 \\ 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$
$$\begin{bmatrix} 3 \\ 3 \end{bmatrix} = 3 \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} + 0 \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Thus,

$$M_{\mathcal{C}}(\mathcal{A}) = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 1 & 0 \end{bmatrix}.$$

EXAMPLE 18.16. The most important use of this concept will be when $\mathcal{A}$ is taken to be an ordered basis. So, suppose V is an n-dimensional vector space and $\mathcal{B}_1$ and $\mathcal{B}_2$ are two ordered bases of V. Then $M_{\mathcal{B}_1}(\mathcal{B}_2)$ and $M_{\mathcal{B}_2}(\mathcal{B}_1)$ are both $n \times n$ matrices. These matrices will be very useful in result that we will prove below.

For example, consider the ordered bases

$$\mathcal{B} = \begin{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix}.$$

and

$$\mathcal{C} = \begin{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ -1 \end{bmatrix} \end{bmatrix}$$

of $\mathbb{R}^2$. Then,

$$M_{\mathcal{B}}(\mathcal{C}) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and

$$M_{\mathcal{C}}(\mathcal{B}) = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{bmatrix}.$$

The following result is a generalization of Theorem 18.12:

THEOREM 18.17. *Let n be a positive integer and let V be an n-dimensional vector space. Let k be a positive integer. Let $\mathcal{B}$ be an ordered basis of V. Then, we define functions $\phi : M_{1\times k}(V) \to M_{n\times k}(F)$ and $\psi : M_{n\times k}(F) \to M_{1\times k}(V)$ by*

$$\phi(\mathcal{A}) = M_{\mathcal{B}}(\mathcal{A})$$

for every $\mathcal{A} \in M_{1\times k}(V)$, and

$$\psi(X) = \mathcal{B} \cdot A$$

for every $X \in M_{n\times k}(F)$. Then, ϕ and ψ are linear transformations. Also, ϕ and ψ are inverses of each other and thus define an isomorphism of vector spaces between $M_{1\times k}(V)$ and $M_{n\times k}(F)$.

PROOF. This proof is very similar in structure to the proof of Theorem 18.12 and so I will merely sketch it.

Suppose $\mathcal{B} = \begin{bmatrix}\mathbf{v}_1 & \cdots & \mathbf{v}_n\end{bmatrix}$. Let $\mathcal{A} \in M_{1\times k}(V)$. So

$$\mathcal{A} = \begin{bmatrix}\mathbf{w}_1 & \cdots & \mathbf{w}_k\end{bmatrix}$$

for $\mathbf{w}_1, \ldots, \mathbf{w}_k \in V$. We write each $\mathbf{w}_i$ as a linear combination of the elements of the basis.

$$\mathbf{w}_i = a_{1i}\mathbf{v}_1 + \cdots + a_{ni}\mathbf{v}_n$$

Thus, by definition, we have

$$\phi(\mathcal{A}) = M_{\mathcal{B}}(\mathcal{A}) = \begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nk} \end{bmatrix}.$$

Thus,

$$\begin{aligned}\psi(\phi(\mathcal{A})) &= \mathcal{B} \cdot M_{\mathcal{B}}(\mathcal{A}) \\ &= \begin{bmatrix}\mathbf{v}_1 & \cdots & \mathbf{v}_n\end{bmatrix} \begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nk} \end{bmatrix}.\end{aligned}$$

It is easy to see that the matrix product above is equal to $\mathcal{A}$. Thus, we see that $\psi(\phi(\mathcal{A}) = \mathcal{A}$.

The rest of the proof is left as an exercise. To complete this proof, you need to do the following:

- Show that $\phi(\psi(X)) = X$ for any $X \in M_{n\times k}(F)$. This shows that ϕ and ψ are inverses of each other and are thus bijections.
- Show that ϕ is linear. (Look at the corresponding argument in the proof of Theorem 18.12.)

□

REMARK 18.18. The analogue of Remark 18.13 also holds in this situation. In other words, if X and Y are elements of $M_{n\times k}(F)$ such that $\mathcal{B} \cdot X = \mathcal{B} \cdot Y$, then we can apply ϕ to both sides to get $X = Y$.

Finally, we are able to answer the question raised at the beginning of this lecture.

THEOREM 18.19. *Let V be a finite dimensional vector space. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two ordered bases of V. Let $\mathbf{v} \in V$. Then,*

$$M_{\mathcal{B}_2}(\mathbf{v}) = M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}).$$

PROOF. We have the equalities

$$\mathbf{v} = \mathcal{B}_2 \cdot M_{\mathcal{B}_2}(\mathbf{v})$$

and

$$\begin{aligned}\mathbf{v} &= \mathcal{B}_1 \cdot M_{\mathcal{B}_1}(\mathbf{v}) \\ &= \left(\mathcal{B}_2 \cdot M_{\mathcal{B}_2}(\mathcal{B}_1)\right) \cdot M_{\mathcal{B}_1}(\mathbf{v}) \\ &= \mathcal{B}_2 \cdot \left(M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v})\right).\end{aligned}$$

By applying Remark 18.13 to these equations, we see that

$$M_{\mathcal{B}_2}(\mathbf{v}) = M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v})$$

as required. □

EXAMPLE 18.20. We consider the bases $\mathcal{B}$ and $\mathcal{C}$ of $\mathbb{R}^2$ defined in Example 18.16. Let $\mathbf{v} \in \mathbb{R}^2$ be given by

$$\mathbf{v} = \begin{bmatrix}1\\5\end{bmatrix}.$$

What is $M_{\mathcal{C}}(\mathbf{v})$?

The straightforward way to do this is to simply write $\mathbf{v}$ as a linear combination of the vectors appearing in $\mathcal{C}$. The required coefficients can be found by solving a system of linear equations.

Using the above theorem, we are able to do this computation a little faster. Observe that the given 2×1 matrix is actually the matrix representation of $\mathbf{v}$ with respect to the standard basis. Thus,

$$M_{\mathcal{B}}(\mathbf{v}) = \begin{bmatrix}1\\5\end{bmatrix}.$$

Thus,

$$\begin{aligned}M_{\mathcal{C}}(\mathbf{v}) &= M_{\mathcal{C}}(\mathcal{B}) \cdot M_{\mathcal{B}}(\mathbf{v}) \\ &= \begin{bmatrix}1/2 & 1/2\\ 1/2 & -1/2\end{bmatrix}\begin{bmatrix}1\\5\end{bmatrix} \\ &= \begin{bmatrix}3\\-2\end{bmatrix}.\end{aligned}$$

If $\mathcal{B}_1$ and $\mathcal{B}_2$ are ordered bases of a vector space V, the matrices $M_{\mathcal{B}_1}(\mathcal{B}_2)$ and $M_{\mathcal{B}_1}(\mathcal{B}_2)$ are called the *"change of basis" matrices* since they allow us to go back and forth between the matrices representations of a vector with respect to the two bases. We will note one important property of these matrices.

PROPOSITION 18.21. *Let V be a finite dimensional vector space. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two ordered bases of V. Then, the matrices $M_{\mathcal{B}_1}(\mathcal{B}_2)$ and $M_{\mathcal{B}_2}(\mathcal{B}_1)$ are multiplicative inverses of each other. (In particular, these two matrices are invertible.)*

PROOF. Let $n = \dim(V)$ and let I_n denote the $n \times n$ identity matrix. We observe that

$$\begin{aligned}\mathcal{B}_1 \cdot I_n &= \mathcal{B}_1 \\ &= \mathcal{B}_2 \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \\ &= \left(\mathcal{B}_1 \cdot M_{\mathcal{B}_1}(\mathcal{B}_2)\right) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \\ &= \mathcal{B}_1 \cdot \left(M_{\mathcal{B}_1}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1)\right).\end{aligned}$$

Thus, by Remark 18.18, we see that

$$I_n = M_{\mathcal{B}_1}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1).$$

This proves the result. □

LECTURE 19

Matrix representation of a linear transformation

Let V be an m-dimensional vector space and let W be an n-dimensional vector space. Let

$$\mathcal{B} = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_m \end{bmatrix}$$

and

$$\mathcal{C} = \begin{bmatrix} \mathbf{w}_1 & \cdots & \mathbf{w}_n \end{bmatrix}$$

be ordered bases of V and W respectively.

Let $T : V \to W$ be a linear transformation. We saw in Theorem 18.12 that we have linear maps $\phi_{\mathcal{B}} : V \to F^m$ and $\psi_{\mathcal{B}} : F^m \to V$ given by

$$\phi_{\mathcal{B}}(\mathbf{v}) = M_{\mathcal{B}}(\mathbf{v})$$

and

$$\psi_{\mathcal{B}}(\mathbf{x}) = \mathcal{B} \cdot \mathbf{x}.$$

These two linear transformations are actually inverses of each other. Similarly, we have linear transformations $\phi_{\mathcal{C}} : W \to F^n$ and $\psi_{\mathcal{C}} : F^n \to W$ given by similar formulas. Thus, we have the following diagram

$$\begin{array}{ccc} V & \underset{\psi_{\mathcal{B}}}{\overset{\phi_{\mathcal{B}}}{\rightleftarrows}} & F^m \\ {\scriptstyle T}\downarrow & & \\ W & \underset{\psi_{\mathcal{C}}}{\overset{\phi_{\mathcal{C}}}{\rightleftarrows}} & F^m \end{array}$$

All the functions in the above diagram are linear transformations. Thus, we obtain a linear transformation from F^m to F^n defined by $\phi_{\mathcal{C}} \circ T \circ \psi_{\mathcal{B}}$.

$$\begin{array}{ccc} V & \underset{\psi_{\mathcal{B}}}{\overset{\phi_{\mathcal{B}}}{\rightleftarrows}} & F^m \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{C}} \circ T \circ \psi_{\mathcal{B}}} \\ W & \underset{\psi_{\mathcal{C}}}{\overset{\phi_{\mathcal{C}}}{\rightleftarrows}} & F^m \end{array}$$

Any linear transformation from F^m to F^n is given by left-multiplication by an $n \times m$ matrix. We will denote this matrix by $M_{\mathcal{C}}^{\mathcal{B}}(T)$ and call it the *matrix representation of T with respect to $\mathcal{B}$ and $\mathcal{C}$*. Thus, the above diagram can also be written as

$$\begin{array}{ccc} V & \underset{\psi_{\mathcal{B}}}{\overset{\phi_{\mathcal{B}}}{\rightleftarrows}} & F^m \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle \mathbf{x} \mapsto M_{\mathcal{C}}^{\mathcal{B}}(T)\mathbf{x}} \\ W & \underset{\psi_{\mathcal{C}}}{\overset{\phi_{\mathcal{C}}}{\rightleftarrows}} & F^m \end{array}$$

First we observe that the above diagram is an example of a "commutative diagram", which means that if we go from one point in the diagram to the other following different paths, the result is the same.

For instance, in this diagram, there are two sequences of functions that lead from V to F^n:

(1) First go from V to F^m using $\phi_{\mathcal{B}}$, and then go from F^m to F^n using $\phi_{\mathcal{C}} \circ T \circ \psi_{\mathcal{B}}$. This gives us the composition $(\phi_{\mathcal{C}} \circ T \circ \psi_{\mathcal{B}}) \circ \phi_{\mathcal{B}}$.

(2) First go from V to W using T. and then go from W to F^n using $\phi_{\mathcal{C}}$. This gives us the composition $\phi_{\mathcal{C}} \circ T$.

As $\psi_{\mathcal{B}} \circ \phi_{\mathcal{B}}$ is the identity on V, it is easy to see that these two compositions are actually the same.

Let us understand what this means. Suppose we start with an element $\mathbf{v} \in V$. The first path in the diagram (going to the right and then going down) gives us the element $M_{\mathcal{C}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v})$. The second path (going down and then going to the right) gives us the element $M_{\mathcal{C}}(T(\mathbf{v}))$. Thus, we have

$$M_{@C}(T(\mathbf{v})) = M_{\mathcal{C}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v}).$$

Multiplying by the row matrix $\mathcal{C}$ on both sides gives us

$$T(\mathbf{v}) = \mathcal{C} \cdot M_{\mathcal{C}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v})$$

This should be seen as the analogue of Lemma 18.11 for linear transformations. It tells us the relationship between the linear transformation T and its matrix representation. We record it for future reference:

LEMMA 19.1. *Let V and W be finite dimensional vector spaces with ordered bases $\mathcal{B}$ and $\mathcal{C}$ respectively. Let $T : V \to W$ be a linear transformation. Then,*

$$T(\mathbf{v}) = \mathcal{C} \cdot M_{\mathcal{C}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v}).$$

As in the previous lecture, we would now like to understand how the matrix representation of a linear transformation changes if the basis is changed. However, note that the matrix representation of a linear transformation depends on a choice of basis in both the domain and the codomain. Thus, we need to obtain a formula that can handle changes of both these bases.

THEOREM 19.2. *Let V and W be finite dimensional vector spaces. Let $T : V \to W$ be a linear transformation. Let $\mathcal{B}_1$, $\mathcal{B}_2$ be ordered bases of V and let $\mathcal{C}_1$, $\mathcal{C}_2$ be ordered bases of W. Then,*

$$M_{\mathcal{C}_2}^{\mathcal{B}_2}(T) = M_{\mathcal{C}_2}(\mathcal{C}_1) \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot M_{\mathcal{B}_1}(\mathcal{B}_2).$$

PROOF. Let $\mathbf{v}$ be any element of V. By Lemma 19.1, we know that

$$T(\mathbf{v}) = \mathcal{C}_2 \cdot M_{\mathcal{C}_2}^{\mathcal{B}_2}(T) \cdot M_{\mathcal{B}_2}(\mathbf{v}).$$

Similarly, we have

$$\begin{aligned} T(\mathbf{v}) &= \mathcal{C}_1 \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot M_{\mathcal{B}_1}(\mathbf{v}) \\ &= \left(\mathcal{C}_2 \cdot M_{\mathcal{C}_2}(\mathcal{C}_1)\right) \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot \left(M_{\mathcal{B}_1}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathbf{v})\right). \end{aligned}$$

Thus, we have two expressions for $T(\mathbf{v})$. Equating them and then "cancelling out $\mathcal{C}_2$" by using Remark 18.13, we see that

$$M_{\mathcal{C}_2}^{\mathcal{B}_2}(T) \cdot M_{\mathcal{B}_2}(\mathbf{v}) = M_{\mathcal{C}_2}(\mathcal{C}_1) \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot M_{\mathcal{B}_1}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathbf{v}).$$

This equality holds for any element $\mathbf{v}$ of V.

Suppose $\dim(V) = m$. As $\mathbf{v}$ varies over all elements of V, the matrix $M_{\mathcal{B}_2}(\mathbf{v})$ varies over all elements of F^m. Thus, the above equation shows that for any element $\mathbf{x}$ of F^m, we have

$$M_{\mathcal{C}_2}^{\mathcal{B}_2}(T) \cdot \mathbf{x} = M_{\mathcal{C}_2}(\mathcal{C}_1) \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot M_{\mathcal{B}_1}(\mathcal{B}_2) \cdot \mathbf{x}.$$

If we take $\mathbf{x}$ to be the element $\mathbf{e}_i$ in the standard basis of F^m, we get that

$$M_{\mathcal{C}_2}^{\mathcal{B}_2}(T) \cdot \mathbf{e}_i = M_{\mathcal{C}_2}(\mathcal{C}_1) \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot M_{\mathcal{B}_1}(\mathcal{B}_2) \cdot \mathbf{e}_i.$$

Here, the left hand side of the equation is the i-th column of the matrix $M_{\mathcal{C}_2}^{\mathcal{B}_2}(T)$ and the right hand side is the i-th column of the matrix $M_{\mathcal{C}_2}(\mathcal{C}_1) \cdot M_{\mathcal{C}_1}^{\mathcal{B}_1}(T) \cdot M_{\mathcal{B}_1}(\mathcal{B}_2)$. Letting i vary from 1 to m, we see that these two matrices have identical columns, and hence must be equal. This proves the result. □

LECTURE 20

Further comments on change of basis

Changing bases successively:

Let V be a finite dimensional vector space and let $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ be three ordered bases of V. Let $\mathbf{v} \in V$. Then, we know that

$$\mathbf{v} = \mathcal{B}_3 M_{\mathcal{B}_3}(\mathbf{v}).$$

On the other hand

$$\begin{aligned}\mathbf{v} &= \mathcal{B}_1 M_{\mathcal{B}_1}(\mathbf{v}) \\ &= \mathcal{B}_2 \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}) \\ &= \mathcal{B}_3 \cdot M_{\mathcal{B}_3}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}).\end{aligned}$$

Comparing these two expressions for $\mathbf{v}$ and "cancelling out $\mathcal{B}_3$" on the left using Remark 18.13, we see that

$$M_{\mathcal{B}_3}(\mathbf{v}) = M_{\mathcal{B}_3}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}).$$

However, we also know that

$$M_{\mathcal{B}_3}(\mathbf{v}) = M_{\mathcal{B}_3}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}).$$

Thus, we have

$$M_{\mathcal{B}_3}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}) = M_{\mathcal{B}_3}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot M_{\mathcal{B}_1}(\mathbf{v}).$$

This equation holds for all $\mathbf{v} \in V$.

Now, suppose $\dim(V) = m$. Then, as $\mathbf{v}$ varies over all elements of V, the matrix $M_{\mathcal{B}_1}(\mathbf{v})$ varies over all elements of F^m. Thus, we see that for any $\mathbf{x} \in F^m$, we have

$$M_{\mathcal{B}_3}(\mathcal{B}_1) \cdot \mathbf{x} = M_{\mathcal{B}_3}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1) \cdot \mathbf{x}.$$

Now, an argument similar to the one used in the proof of Theorem 19.2, we see that the two matrices $M_{\mathcal{B}_3}(\mathcal{B}_1)$ and $M_{\mathcal{B}_3}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1)$ are equal. Thus, we have proved the following important result:

THEOREM 20.1. *Let V be a finite dimensional vector space and let $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ be ordered bases of V. Then,*

$$M_{\mathcal{B}_3}(\mathcal{B}_1) = M_{\mathcal{B}_3}(\mathcal{B}_2) \cdot M_{\mathcal{B}_2}(\mathcal{B}_1).$$

Here is an example of how this theorem can be useful:

EXAMPLE 20.2. Let us consider two ordered bases of $\mathbb{R}^2$ given by

$$\mathcal{B}_1 = \left[\begin{bmatrix}1\\1\end{bmatrix} \quad \begin{bmatrix}1\\-1\end{bmatrix}\right].$$

and

$$\mathcal{B}_2 = \left[\begin{bmatrix}2\\3\end{bmatrix} \quad \begin{bmatrix}1\\5\end{bmatrix}\right].$$

We would like to compute $M_{\mathcal{B}_1}(\mathcal{B}_2)$. In order to do this, we need to compute the matrix representations of every element of $\mathcal{B}_2$ with respect to $\mathcal{B}_1$. For this, we will need to solve a system of linear equations. This needs to be done for both elements of $\mathcal{B}_2$, and thus we have to solve two systems consisting of two equations each. If

we had been working with an n-dimensional space, such a problem would require us to solve n systems, each containing n linear equations. However, the above formula provides us with an easier way.

Let

$$\mathcal{S} = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right]$$

be the standard ordered basis of $\mathbb{R}^2$. Then, we easily see that

$$M_{\mathcal{S}}(\mathcal{B}_1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and

$$M_{\mathcal{S}}(\mathcal{B}_2) = \begin{bmatrix} 2 & 1 \\ 3 & 5 \end{bmatrix}.$$

Thus,

$$\begin{aligned} M_{\mathcal{B}_1}(\mathcal{B}_2) &= M_{\mathcal{B}_1}(\mathcal{S}) \cdot M_{\mathcal{S}}(\mathcal{B}_2) \\ &= M_{\mathcal{S}}(\mathcal{B}_1)^{-1} \cdot M_{\mathcal{S}}(\mathcal{B}_2) \\ &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{-1} \begin{bmatrix} 2 & 1 \\ 3 & 5 \end{bmatrix}. \end{aligned}$$

Characterizing "change of basis" matrices:

We have seen before that the "change of basis" matrices are invertible. We will now show that any invertible matrix is a change of basis matrix.

EXERCISE 20.3. Let V be an n-dimensional vector space. Let $\mathcal{B}$ be an ordered basis. Let A be an invertible matrix. Show that $\mathcal{B} \cdot A$ is an ordered basis of $\mathcal{B}$.

(Note that we already know that if $\mathcal{B} \cdot A$ is a basis of V, then A is invertible! Do you understand why?)

SOLUTION. Let

$$\mathcal{B} = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix}$$

and let

$$\mathcal{B} \cdot A = \begin{bmatrix} \mathbf{w}_1 & \cdots & \mathbf{w}_n \end{bmatrix}.$$

Suppose A is invertible. Thus, there exists an $n \times n$ matrix $B = (b_{ij})i, j$ such that $AB = I_n$. Thus,

$$\mathcal{B} = \mathcal{B} \cdot I_n = (\mathcal{B} \cdot A) \cdot B.$$

The product $(\mathcal{B} \cdot A) \cdot B)$ is a $1 \times n$ matrix, the $(1, j)$-entry of which is $\sum_{i=1}^{n} b_{ij} \mathbf{w}_i$. However, the above equation tells us that this matrix is actually equal to the $1 \times n$ matrix $\mathcal{B}$, the $(1, j)$-entry of which is just $\mathbf{v}_j$. Thus, $\mathbf{v}_j$ is in the span of the set $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$. As this is true for all j, we see that $span(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ contains every $\mathbf{v}_j$. Thus, is equal to the whole of V. We conclude that the set $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ is a spanning set of V. Since it has n elements, it is a basis of V. Thus, $\mathcal{B} \cdot A$ is an ordered basis of V. □

LECTURE 21

Rank-Nullity Theorem

THEOREM 21.1 (Rank-Nullity theorem). *Let V, W be vector spaces and let $T : V \to W$ be a linear transformation. Then,*

$$\dim(V) = \dim(ker(T)) + \dim(im(T)).$$

The number $\dim(im(T))$ is sometimes called the *rank* of T and $\dim(ker(T))$ is called the *nullity* of T.

PROOF. Let $\dim(V) = n$ and let $\dim(ker(T)) = m$. Then, we know that $m \leqslant n$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ be a basis of $ker(T)$. Then, the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a linearly independent subset of V. Any linearly independent subset is contained in some basis. Thus, we can expand this set to a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{v}_{m+1}, \ldots, \mathbf{v}_n\}$ of V.

We will show that the set $\{T(\mathbf{v}_{m+1}, \ldots, T(\mathbf{v}_n)\}$, which contains $n-m$ elements, is a basis of $im(T)$. This will prove complete the proof of the theorem.

Let $\mathbf{w} \in im(T)$. Thus, there exists $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \mathbf{w}$. As $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V, there exist $a_1, \ldots, a_n \in F$ such that

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots a_n\mathbf{v}_n.$$

Thus

$$\begin{aligned} \mathbf{w} &= T(\mathbf{v}) \\ &= T(a_1\mathbf{v}_1 + \cdots a_n\mathbf{v}_n) \\ &= a_1T(\mathbf{v}_1) + \cdots a_nT(\mathbf{v}_n). \end{aligned}$$

As $T(\mathbf{v}_i) = \mathbf{0}$ for $1, \leqslant i \leqslant m$, we see that

$$\mathbf{w} = a_{m+1}T(\mathbf{v}_{m+1}) + \cdots + a_nT(\mathbf{v}_n).$$

This shows that the set $\{T(\mathbf{v}_{m+1}, \ldots, T(\mathbf{v}_n)\}$ spans $im(T)$.

It remains to be proved that the set $\{T(\mathbf{v}_{m+1}, \ldots, T(\mathbf{v}_n)\}$ is linearly independent. Suppose there exist elements $a_{m+1}, \ldots, a_n \in F$ such that

$$a_{m+1}T(\mathbf{v}_{m+1}) + \cdots + a_nT(\mathbf{v}_n) = \mathbf{0}.$$

Thus,

$$T(a_{m+1}\mathbf{v}_{m+1} + \cdots + a_n\mathbf{v}_n) = \mathbf{0},$$

which implies that $a_{m+1}\mathbf{v}_{m+1} + \cdots + a_n\mathbf{v}_n \in ker(T)$. As $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is a basis of $ker(T)$, there exist elements $a_, \ldots, a_m \in F$ such that

$$a_1\mathbf{v}_1 + \ldots + a_m\mathbf{v}_m = a_{m+1}\mathbf{v}_{m+1} + \cdots + a_n\mathbf{v}_n.$$

Thus,

$$a_1\mathbf{v}_1 + \ldots + a_m\mathbf{v}_m + (-a_{m+1})\mathbf{v}_{m+1} + \cdots + (-a_n)\mathbf{v}_n = \mathbf{0}.$$

As $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a linearly independent set, this implies that $a_i = 0$ for all i, $1 \leqslant i \leqslant n$. In particular, we have $a_i = 0$ for all i, $1 \leqslant i \leqslant m$. This shows that the set $\{T(\mathbf{v}_{m+1}, \ldots, T(\mathbf{v}_n)\}$ is linearly independent. □

EXAMPLE 21.2. Consider the morphism $T : \mathbb{R}^2 \to \mathbb{R}$ given by $T(\mathbf{x}) = A\mathbf{x}$ where $A = \begin{bmatrix} 2 & 1 \end{bmatrix}$. Then it is clear that $im(T)$ is not the zero subspace of $\mathbb{R}$. For instance, we can see that $T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = 2 \neq 0$. Thus, as any non-zero subspace of $\mathbb{R}$ is equal to $\mathbb{R}$, we see that $im(T) = \mathbb{R}$. Thus, $\dim(im(T)) = 1$. Then, the above theorem shows that $ker(\dim(T)) = 1$. We already know from co-ordinate geometry that the set of all points $\begin{bmatrix} x \\ y \end{bmatrix}$ such that $2x + y = 0$ is a *line* in the plane.

LECTURE 22

Sums of subspaces

DEFINITION 22.1. (Sums of spaces) Let V be a vector space and let $\{W_i\}_{i\in I}$ be a family of subspaces of V (where I is any indexing set). The *sum* of the subspaces in this family is defined to be the subspace

$$\sum_{i\in I} W_i = span(\bigcup_{i\in I} W_i)$$

of V. If I is a finite set, say $I = \{1, \ldots, n\}$, we will write the sum of the subspaces W_i as $W_1 + W_2 + \cdots + W_n$.

The following description of the sum may be more useful:

LEMMA 22.2. *Let V be a vector space and let $\{W_i\}_{i\in I}$ be a family of subspaces of V. Then*

$$\sum_{i\in I} W_i = \{\sum_{i\in I} \mathbf{w}_i : \mathbf{w}_i \in W_i \text{ and } \mathbf{w}_i = 0 \text{ for all but finitely many } i\}.$$

Note that the condition that $\mathbf{w}_i = 0$ for all but finitely many i is imposed only to ensure that the expression $\sum_{i\in I} \mathbf{w}_i$ makes sense. If I happens to be a finite set, this second condition is not relevant and then we can say that $\sum_{i\in I} W_i$ is simply the collection of all elements of the form $\sum_{i\in I}$ where $\mathbf{w}_i \in W_i$ for every i.

PROOF. Let us denote the set on the right hand side of the above equation by W. Thus,

$$W := \{\sum_{i\in I} \mathbf{w}_i : \mathbf{w}_i \in W_i \text{ and } \mathbf{w}_i = 0 \text{ for all but finitely many } i\}.$$

We first claim that W is a subspace of V. Suppose $\mathbf{v}_1$ and $\mathbf{v}_2$ are elements of W. Then, for $j = 1, 2$, we have

$$\mathbf{v}_i = \sum_{i\in I} \mathbf{w}_{ij}$$

for some $\mathbf{w}_{ij} \in W_i$ such that $\mathbf{w}_{ij} = \mathbf{0}$ for all but finitely many i. Let $a_1, a_2 \in F$. Then,

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 = \sum_{i\in I}(a_1\mathbf{w}_{i1} + a_2\mathbf{w}_{i2}).$$

We observe that for every i, $a_1\mathbf{w}_{i1} + a_2\mathbf{w}_{i2} \in W_i$. Thus, the right hand side of the above equation clearly represents an element in W. As $a_1, a_2 \in F$ and W were arbitrary, we see that W is a subspace of V.

Clearly, $W_i \subset W$ for every $i \in I$. Thus, $\bigcup_{i\in I} W_i \subset W$. As $\sum_{i\in I} W_i = span(\bigcup_{i\in I} W_i$ is the intersection of all the subspaces of W which contain $\bigcup_{i\in I} W_i$, it follows that $\sum_{i\in I} W_i \subset W$.

On the other hand, every element of the form $\sum_{i\in I} \mathbf{w}_i$, with $\mathbf{w}_i \in W_i$ for all $i \in I$, is a linear combination of elements in $\bigcup_{i\in I} W_i$. Thus, we see that every element of W is contained in $span(\bigcup_{i\in I} W_i = \sum_{i\in I} W_i$. Thus, we see that $W = \sum_{i\in I} W_i$. □

EXAMPLES 22.3. We will look at two simple examples, which will illustrate a crucial issue. In both these examples, we will use the space $V = \mathbb{R}^3$. Let $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ be the standard basis of $\mathbb{R}^3$.

(1) Let $S_1 = span(\mathbf{e}_1)$ (i.e. the x-axis) and $S_2 = span(\mathbf{e}_2, \mathbf{e}_3)$ (i.e. the yz-plane). Then $span(S_1 \cup S_2)$ contains $span(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3) = V$ and hence must be equal to V. Thus, $S_1 + S_2 = V$. Observe that here $\dim(S_1) = 1$, $\dim(S_2) = 2$ and $\dim(V) = 3$. So, $\dim(V) = \dim(S_1) + \dim(S_2)$. Notice that, $S_1 \cap S_2 = \{\mathbf{0}\}$.
(2) Let $T_1 = span(\mathbf{e}_1, \mathbf{e}_2)$ (i.e. the xy-plane) and $T_2 = span(\mathbf{e}_1, \mathbf{e}_3)$ (i.e. the xz-plane). Then, by the same argument as above, we see that $T_1 + T_2 = V$. However, $\dim(T_1) = 2$, $\dim(T_2) = 2$ and $\dim(V) = 3$. So, $\dim(V) > \dim(T_1) + \dim(T_2)$. Here, we observe that $T_1 \cap T_2 = span(\mathbf{e}_1)$, which is a 1-dimensional space.

In order to explain this difference, we formulate a new notion which should remind you of the notion of linear independence of vectors.

DEFINITION 22.4. Let V be a vector space. Let $\{W_i\}_{i\in I}$ be a family of subspaces of V. Then, we say that the subspaces $\{W_i\}_{i\in I}$ are *independent* if the following condition holds:

> If we have an equality $\sum_{i\in I} \mathbf{w}_i = \mathbf{0}$ where $\mathbf{w}_i \in W_i$ for each $i \in I$, then we must have $\mathbf{w}_i = \mathbf{0}$ for every $i \in I$.

We will now focus on the case of a family consisting of two subspaces W_1, W_2 contained in a vector space V and examine what the notion of independence means in that case.

LEMMA 22.5. *Let V be a vector space. Let W_1, W_2 be subspaces of V. Let $\mathcal{B}_1$ be a basis of W_1 and let $\mathcal{B}_2$ be a basis of W_2. Then $span(B_1 \cup B_2) = W_1 + W_2$.*

PROOF. Any element of $W_1 + W_2$ can be written in the form $\mathbf{w}_1 + \mathbf{w}_2$ where $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$. Since $\mathcal{B}_1$ is a basis of W_1, $\mathbf{w}_1$ can be written as a linear combination of elements of $\mathcal{B}_1$. Similarly, $\mathbf{w}_2$ can be written as a linear combination of elements of $\mathcal{B}_2$. This shows that $\mathbf{w}_1 + \mathbf{w}_2$ can be written as a linear combination of elements of $\mathcal{B}_1 \cup \mathcal{B}_2$. Thus, $span(\mathcal{B}_1 \cup \mathcal{B}_2) = W_1 + W_2$. □

REMARK 22.6. More generally, suppose $\{W_i\}_{i\in I}$ is a family of subspaces of V and $\mathcal{B}_i$ is a basis of W_i for every $i \in I$, then $span(\bigcup_{i\in I} \mathcal{B}_i) = \sum_{i\in I} W_i$. The proof is similar to that of the special case proved above. (Exercise: Write the proof in the general case.)

PROPOSITION 22.7. *Let V be a vector space. Let W_1 and W_2 be subspaces. Then, the following statements are equivalent:*

(a) *W_1 and W_2 are independent.*
(b) *$W_1 \cap W_2 = \{\mathbf{0}\}$.*
(c) *Let $\mathcal{B}_1$ be a basis of W_1 and $\mathcal{B}_2$ be a basis of W_2. Then $\mathcal{B}_1 \cap \mathcal{B}_2 = \varnothing$ and $\mathcal{B}_1 \cup \mathcal{B}_2$ is a basis for $W_1 + W_2$.*

If any of these statements is true, then $\dim(W_1) + \dim(W_2) = \dim(W_1 + W_2)$.

PROOF. We will prove the equivalence of the statements in three steps.
STEP 1: (a) implies (b).

We assume that (a) is true. Suppose (b) is not true. Then there exists $\mathbf{w} \in W_1 \cap W_2$ such that $\mathbf{w} \neq \mathbf{0}$. Define $\mathbf{w}_1 = \mathbf{w}$ and $\mathbf{w}_2 = -\mathbf{w}$. Then $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$. Clearly $\mathbf{w}_1 + \mathbf{w}_2 = \mathbf{0}$. Thus, (a) implies that $\mathbf{w}_1 = \mathbf{w}_2 = \mathbf{0}$. Thus, $\mathbf{w} = \mathbf{0}$, which contradicts our assumption. This shows that (b) must be true. Thus, we have shown that (a) implies (b).
STEP 2: (b) implies (c).

We assume that (b) is true. By Lemma 22.5, we know that $\mathcal{B}_1 \cup \mathcal{B}_2$ spans $W_1 + W_2$. As $W_1 \cap W_2 = \{\mathbf{0}\}$, we see that $\mathcal{B}_1 \cap \mathcal{B}_2 \subset \{\mathbf{0}\}$. However, $\mathbf{0}$ cannot be the member of any basis. Thus, $\mathcal{B}_1 \cap \mathcal{B}_2 = \varnothing$.

STEP 3: (c) implies (a).

Suppose that (c) is true. Suppose that we have an equation $\mathbf{w}_1 + \mathbf{w}_2 = \mathbf{0}$ where $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$. Suppose $\mathcal{B}_1 = \{\mathbf{u}_i\}_{i\in I}$ and $\mathcal{B}_2 = \{\mathbf{v}_j\}_{j\in J}$. Then we have $\mathbf{w}_1 = \sum_{i\in I} a_i\mathbf{u}_i$ and $\mathbf{w}_2 = \sum_{j\in J} b_j\mathbf{v}_j$ where all the a_i and b_j are in F. Thus, we have the equation

$$\sum_{i\in I} a_i\mathbf{u}_i + \sum_{j\in J} b_j\mathbf{v}_j = \mathbf{0}.$$

Since $\mathcal{B}_1 \cup \mathcal{B}_2$ is a basis, we see that $a_i = 0$ for all $i \in I$ and $b_j = 0$ for all $j \in J$. Thus $\mathbf{w}_1 = \mathbf{w}_2 = \mathbf{0}$. This proves (a). Thus (c) implies (a). □

REMARK 22.8. Thus, we have proved that if W_1 and W_2 are independent, then $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2)$. In the next lecture, we will prove that the converse of this statement is also true.

REMARK 22.9. Proposition 22.7 can be generalized to an arbitrary family $\{W_i\}_{i\in I}$. The generalized versions of statements (a) and (c) in the proposition are obvious. However, the generalization of (b) is a bit more subtle. It is as follows:

$$\text{For every } i \in I,\ W_i \cap \left(\textstyle\sum_{j\in I\setminus\{i\}} W_j\right) = \{\mathbf{0}\}.$$

Thus, for instance, for a family of three subspaces W_1, W_2, W_3, independence is equivalent to

$$W_1 \cap (W_2 + W_3) = W_2 \cap (W_1 + W_3) = W_3 \cap (W_1 + W_2) = \{\mathbf{0}\}.$$

(Exercise: Write the complete statement of the generalization of Proposition 22.7 and prove it.)

LECTURE 23

Direct sums

DEFINITION 23.1. Let V be a vector space. Let W_1, W_2 be subspaces of V. We say that W_1, W_2 are *complementary subspaces* (or that they are *complements* of each other) if $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$.

PROPOSITION 23.2. *Let V be a vector space and let W be a subspace of V. Then, there exists a subspace W' of V such that W' is a complement of W.*

PROOF. Choose a basis $\mathcal{B}$ of W. Then, $\mathcal{B}$ is contained in a basis $\mathcal{C}$ of V. Let $W' = span(\mathcal{C}\backslash\mathcal{B})$. The set $\mathcal{C}\backslash\mathcal{B}$ is a subset of $\mathcal{C}$ and is hence linearly independent. Since it spans W', we see that it is a basis of W'. We have $\mathcal{B} \cap (\mathcal{C}\backslash\mathcal{B}) = \varnothing$ and $\mathcal{B} \cup (\mathcal{C}\backslash\mathcal{B}) = \mathcal{C}$. Thus, by Proposition 22.7, we see that W and W' are independent. As $span(C) = V$, we see that $W + W' = V$. Thus, W' is a complement of W. □

REMARK 23.3. Note that W does not have a unique complement. The complement constructed in the above proposition depends on the choice of $\mathcal{C}$. As $\mathcal{C}$ can generally be chosen in many ways (infinitely many ways if F is an infinite field), we see that W' is not unique.

For example, let $V = \mathbb{R}^2$ and let W be a line in $\mathbb{R}^2$. Then, any other line of $\mathbb{R}^2$ is a complement of W. (Exercise: Do you see why?)

Direct sums:

Let V and W be vector spaces. Then the cartesian product $V \times W$ has a vector space structure defined as follows:

- Addition: For $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $\mathbf{w}_1, \mathbf{w}_2 \in W$, we define $(\mathbf{v}_1, \mathbf{w}_1) + (\mathbf{v}_2, \mathbf{w}_2)$ to be $(\mathbf{v}_1 + \mathbf{v}_2, \mathbf{w}_1 + \mathbf{w}_2)$.
- Scalar multiplication: For $c \in F$, $\mathbf{v} \in V$ and $\mathbf{w} \in W$, we define $c \cdot (\mathbf{v}, \mathbf{w})$ to be $(c\mathbf{v}, c\mathbf{w})$.

This vector space is denoted by $V \oplus W$ and is called the *direct sum* of V and W. (Exercise: Check that the above definitions of addition and scalar multiplication satisfy really do make $V \times W$ into a vector space.)

REMARK 23.4. Sometimes the direct sum of V and W is also called as the *external direct sum* of V and W. This is in order to distinguish it from the "internal direct sum", which is defined as follows:

If V is a vector space and W_1, W_2 are independent subspaces of V, their sum $W_1 + W_2$ is called the *internal direct sum* of W_1 and W_2.

Of course, we can also construct the external direct sum $W_1 \oplus W_2$ of two subspaces. We will see below that if W_1 and W_2 are independent, then the internal and external direct sums of W_1 and W_2 are actually isomorphic.

To understand this vector space better, it will be useful to look at certain functions. We define $p_1 : V \oplus W \to V$ by $p_1((\mathbf{v}, \mathbf{w})) = \mathbf{v}$ and $p_2 : V \oplus W \to W$ by $p((\mathbf{v}, \mathbf{w})) = \mathbf{w}$. Let $s :_1 V \to V \oplus W$ be defined by $s_1(\mathbf{v}) = (\mathbf{v}, \mathbf{0})$ and $s_2 : W \to V \oplus W$ be defined by and $s_2(\mathbf{w}) = (\mathbf{0}, \mathbf{w})$.

EXERCISE 23.5. With the above notation, prove the following:

(a) Prove that p_1, p_2, s_1 and s_2 are linear transformations.

(b) Prove that $p_1 \circ s_1 : V \to V$ is the identity transformation on V. Similarly, show that $p_2 \circ s_2 : W \to W$ is the identity transformation on W.
(c) Prove that s_1 and s_2 are injective.

We will assume the results of the above exercise. Let $\widetilde{V} = s_1(V)$ and $\widetilde{W} = s_2(W)$. These are subspaces of $V \oplus W$. Explicitly,

$$\widetilde{V} = \{(\mathbf{v}, \mathbf{0}) : \mathbf{v} \in V\} \subset V \oplus W$$

and

$$\widetilde{W} = \{(\mathbf{0}, \mathbf{w}) : \mathbf{w} \in W\} \subset V \oplus W.$$

As s_1 and s_2 are injective, we see that the linear transformation $V \to \widetilde{V}$, $\mathbf{v} \mapsto (\mathbf{v}, \mathbf{0})$ is actually an isomorphism. Thus, $\dim(\widetilde{V}) = \dim(V)$. Similarly the linear transformation $W \to \widetilde{W}$, $\mathbf{w} \mapsto (\mathbf{0}, \mathbf{w})$ is an isomorphism. Thus, $\dim(\widetilde{W}) = \dim(W)$.

First we observe that $\widetilde{V} \cap \widetilde{W} = \{(\mathbf{0}, \mathbf{0}\}$ which is the zero subspace of $V \oplus W$. Thus, $\widetilde{V}$ and $\widetilde{W}$ are independent subspaces of $V \oplus W$. Also, any element $(\mathbf{v}, \mathbf{w})$ of $V \oplus W$ can be written as

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

Thus, $V \oplus W = \widetilde{V} + \widetilde{W}$. Thus, $\widetilde{V}$ and $\widetilde{W}$ are complementary subspaces. Thus, by Proposition 22.7, we see that

$$\dim(V \oplus W) = \dim(\widetilde{V}) + \dim(\widetilde{W}) = \dim(V) + \dim(W).$$

Dimension of the sum of subspaces:

THEOREM 23.6. *Let V be a vector space and let W_1, W_2 be subspaces. Then, we have*

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2).$$

We will give two proofs of this theorem. The first one is a little abstract and uses the Rank-Nullity Theorem. The second one follows a more pedestrian approach and involves a direct algebraic argument involving bases.

PROOF 1. We define a function $s : W_1 \oplus W_2 \to V$ by $s((\mathbf{w}_1, \mathbf{w}_2)) = \mathbf{w}_1 + \mathbf{w}_2$. Then, it is easy to see that s is a linear transformation. (Exercise: Prove this.) The Rank-Nullity Theorem tells us that

$$\dim(W_1 \oplus W_2) = \dim(im(s)) + \dim(ker(s)).$$

We know that $\dim(W_1 \oplus W_2) = \dim(W_1) + \dim(W_2)$. Thus, we see that the theorem will be proved if we can show that $\dim(im(S)) = \dim(W_1 + W_2)$ and $\dim(ker(s)) = \dim(W_1 \cap W_2)$.

Observe that

$$\begin{aligned} im(s) &= \{s((\mathbf{w}_1, \mathbf{w}_2)) : \mathbf{w}_1 \in W_1, \mathbf{w}_2 \in W_2\} \\ &= \{\mathbf{w}_1 + \mathbf{w}_2 : \mathbf{w}_1 \in W_1, \mathbf{w}_2 \in W_2\} \\ &= W_1 + W_2. \end{aligned}$$

This implies that $\dim(im(S)) = \dim(W_1 + W_2)$, which was one of the equalities we wanted to prove.

Now, we observe that

$$\begin{aligned} ker(s) &= \{(\mathbf{w}_1, \mathbf{w}_2) : s((\mathbf{w}_1, \mathbf{w}_2)) = \mathbf{0},\ \mathbf{w}_1 \in W_1, \mathbf{w}_2 \in W_2\} \\ &= \{(\mathbf{w}_1, \mathbf{w}_2) : \mathbf{w}_1 + \mathbf{w}_2 = \mathbf{0},\ \mathbf{w}_1 \in W_1, \mathbf{w}_2 \in W_2\}. \end{aligned}$$

If $(\mathbf{w}_1, \mathbf{w}_2) \in ker(s)$, we have $\mathbf{w}_1 + \mathbf{w}_2 = \mathbf{0}$ and hence $\mathbf{w}_1 = -\mathbf{w}_2$. Here, $\mathbf{w}_1 \in W_1$, but $-\mathbf{w}_2 \in W_2$. Thus, it follows that $\mathbf{w}_1 \in W_1 \cap W_2$. Thus,

$$ker(s) = \{(\mathbf{w}, -\mathbf{w}) : \mathbf{w} \in W_1 \cap W_2\}.$$

Now, define the function $\phi : W_1 \cap W_2 \to W_1 \oplus W_2$ by $\phi(\mathbf{w}) = (\mathbf{w}, -\mathbf{w})$. Then, we see that

$$\begin{aligned} im(\phi) &= \{\phi(\mathbf{w}) : \mathbf{w} \in W_1 \cap W_2\} \\ &= \{(\mathbf{w}, -\mathbf{w}) : \mathbf{w} \in W_1 \cap W_2\} \\ &= ker(s). \end{aligned}$$

Also, if $\phi(\mathbf{w}) = (\mathbf{0}, \mathbf{0})$, then it follows immediately that $\mathbf{w} = 0$. Thus, ϕ is injective. Thus, we see that ϕ induces an isomorphism of $W_1 \cap W_2$ with $im(\phi) = ker(s)$. Thus, $\dim(W_1 \cap W_2) = \dim(ker(s))$ as required. This completes the proof. □

Proof 2. Let $\mathcal{B}$ be a basis of $W_1 \cap W_2$. This is a linearly independent subset of W_1 and thus there exists a set $\mathcal{C}_1$ of W_1 such that $\mathcal{B} \cup \mathcal{C}_1$ is a basis of W_1. Similarly, there exists a subset $\mathcal{C}_2$ of W_2 such that $\mathcal{B} \cup \mathcal{C}_2$ is a basis of W_2.

Let $|\mathcal{B}| = m$, $|\mathcal{C}_1| = n_1$ and $|\mathcal{C}_2| = n_2$. Thus, $\dim(W_1) = m + n_1$ and $\dim(W_2) = m + n_2$. We will prove that the set $\mathcal{B} \cup \mathcal{C}_1 \cup \mathcal{C}_2$ is a basis of $W_1 + W_2$. This will show that

$$\dim(W_1 + W_2) = m + n_1 + n_2 = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$$

as required.

As $W_1 \cup W_2$ spans $W_1 + W_2$, and since $\mathcal{B} \cup \mathcal{C}_i$ spans W_i for $i = 1, 2$, we see that $\mathcal{B} \cup \mathcal{C}_1 \cup \mathcal{C}_2$ spans $W_1 + W_2$. Thus, it remains to be proved that the set $\mathcal{B} \cup \mathcal{C}_1 \cup \mathcal{C}_2$ is linearly independent.

Suppose $\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$, $\mathcal{C}_1 = \{\mathbf{v}_1, \ldots, \mathbf{v}_{n_1}\}$ and $\mathcal{C}_2 = \{\mathbf{w}_1, \ldots, \mathbf{w}_{n_2}\}$. If the set $\mathcal{B} \cup \mathcal{C}_1 \cup \mathcal{C}_2$ is linearly dependent, there exists a non-trivial linear relation

$$\sum_{i=1}^{m} a_i \mathbf{u}_i + \sum_{j=1}^{n_1} b_j \mathbf{v}_j + \sum_{k=1}^{n_2} c_k \mathbf{w}_k = \mathbf{0}$$

where all the a_i, b_j and c_k are in F. Thus,

$$\sum_{k=1}^{n_2} c_k \mathbf{w}_k = -\left(\sum_{i=1}^{m} a_i \mathbf{u}_i + \sum_{j=1}^{n_1} b_j \mathbf{v}_j \right).$$

The right-hand side of this equation is in W_1 and the left-hand side is in W_2. Thus, $\sum_{i=1}^{n_2} c_k \mathbf{w}_k$ is in $W_1 \cap W_2$. Thus, as $\mathcal{B}$ is a basis of $W_1 \cap W_2$, there exist elements $d_1, \ldots, d_m$ such that

$$\sum_{k=1}^{n_2} c_k \mathbf{w}_k = \sum_{i=1}^{m} d_i \mathbf{u}_i.$$

As the set $\mathcal{B} \cup \mathcal{C}_2$ is linearly independent, it follows that $c_k = 0$ for all k and $d_i = 0$ for all i. Thus,

$$\sum_{i=1}^{m} a_i \mathbf{u}_i + \sum_{j=1}^{n_1} b_j \mathbf{v}_j = \mathbf{0}.$$

As $\mathcal{B} \cup \mathcal{C}_1$ is a linearly independent set, we have $a_i = 0$ for all i and $b_j = 0$ for all j. This shows that the linear relation we started with was actually trivial, which is a contradiction.

This shows that the set $\mathcal{B} \cup \mathcal{C}_1 \cup \mathcal{C}_2$ is linearly independent, as required. □

LECTURE 24

Eigenvalues and eigenvectors, Diagonalization

Let V be a finite dimensional vector space and let $\mathcal{B}$ be a basis of V. Let $T : V \to V$ be a linear transformation. Then we saw in Chapter 19 that we can associate a matrix $M_{\mathcal{B}}^{\mathcal{B}}(T)$ to this transformation. If $\mathcal{C}$ is any other basis, we know that

$$M_{\mathcal{C}}^{\mathcal{C}}(T) = M_{\mathcal{C}}(\mathcal{B}) \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathcal{C}) = M_{\mathcal{B}}(\mathcal{C})^{-1} \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathcal{C}).$$

Here, we know that $M_{\mathcal{B}}(\mathcal{C})$ is an invertible matrix.

DEFINITION 24.1. Let n be a positive integer. If P is an $n \times n$ invertible matrix, the function $M_{n\times n}(F) \to M_{n\times n}(F)$ defined by $A \mapsto P^{-1}AP$ is called as *conjugation by* P.

DEFINITION 24.2. Let n be a positive integer. Let A and B be two $n \times n$ matrices. We say that A is *similar* or *conjugate* to B if there exists an invertible matrix P such that $A = PBP^{-1}$.

This relation has some nice properties:

(a) *Reflexive*: Every matrix A is conjugate to itself since $A = I_n^{-1}AI_n$.
(b) *Symmetry*:If A is obtained from B by conjugation by an invertible matrix P, i.e. if $A = P^{-1}BP$, then $B = PAP^{-1}$. Thus, B is obtained from A by conjugation by C^{-1} (which is also an invertible matrix). Thus, we see that if A is conjugate to B, then B is conjugate to A.
(c) *Transitivity*: If A is conjugate to B and B is conjugate to C then A is conjugate to C. Indeed, if $A = P^{-1}BP$ and $B = Q^{-1}CQ$, then $A = P^{-1}Q^{-1}CQP = (QP)^{-1}C(QP)$.

Any "relation" with these properties is said to be an *equivalence relation.*

REMARK 24.3. We will not discuss relations and equivalence relations in detail in this course. However, we observe that this notion allows us to partition the set $M_{n\times n}(F)$ into a family of mutually disjoint subsets. Indeed, for every matrix A, let us denote by $cl(A)$ the set of all $n \times n$ matrices which are conjugate to A. It is called the *conjugacy class* of A. It can be proved by using the above observations that for any two matrices A and B, the sets $cl(A)$ and $cl(B)$ are either disjoint (i.e. their intersection is the empty set) or they are actually equal. Indeed, $cl(A)$ and $cl(B)$ have a common element if and only if A and B are conjugate to each other (use transitivity to prove this), and in this case $cl(A) = cl(B)$. Thus, any two *distinct* conjugacy classes are disjoint. Clearly, any matrix A is contained in some conjugacy class – it is actually contained in the conjugacy class $cl(A)$. Thus, the union of all the conjugacy classes is $M_{n\times n}(F)$. This shows that all the conjugacy classes together give us a partition of $M_{n\times n}(F)$ into disjoint sets.

Given any linear transformation from V to itself, its matrix depends on the choice of the basis of V that we are using. So, is it possible to choose a basis which makes the matrix of T particularly simple? This is the question we will try to answer. (We will only give a partial answer to this question in this course.)

Eigenvalues:

DEFINITION 24.4. Let V be a vector space and let $T : V \to V$ be a linear transformation.

(1) A non-zero element $\mathbf{v} \in V$ is said to be an *eigenvector* for T if there exists an element $\lambda \in F$ such that $T(\mathbf{v}) = \lambda\mathbf{v}$. The element λ is said to be the *eigenvalue* associated to the eigenvector $\mathbf{v}$.
(2) An element of F is said to be an *eigenvalue of* T if it is the eigenvalue corresponding to some eigenvector of T.

CONVENTION 24.5. Let $A \in M_{n\times n}(F)$. Then the eigenvalues and eigenvectors of the linear transformation $\mathbf{x} \mapsto A\mathbf{x}$ will also be referred to as *eigenvalues and eigenvectors of* A.

REMARK 24.6. Observe that the eigenvector $\mathbf{v}$ is necessarily non-zero. However, there is no such restriction on λ. Indeed, if $ker(T) \neq \{\mathbf{0}\}$, then every non-zero element of $ker(T)$ is an eigenvector of T associated to the eigenvalue 0. Thus, 0 is an eigenvalue of T if and only if T is a non-zero kernel, i.e. if and only if T is not injective.

REMARK 24.7. Observe that if $\mathbf{v}$ is an eigenvector of T, the line (i.e. 1-dimensional subspace) $span(\mathbf{v})$ is mapped onto itself by T. Conversely, if $\mathbf{v}$ is a non-zero vector such that the $span(\mathbf{v})$ is mapped into itself by T, then $\mathbf{v}$ is an eigenvector of T.

So, if we are given a linear transformation $T : V \to V$, how should we find its eigenvectors? Actually, it is much easier to find the eigenvalues of T first.

PROPOSITION 24.8. *Let n be a positive integer. Let V be an n-dimensional vector space and let $\lambda \in F$. Let $A = M_{\mathcal{B}}^{\mathcal{B}}(T)$ for any basis $\mathcal{B}$ of V. An element $\lambda \in F$ is an eigenvalue of T if and only if* $\det(\lambda I_n - A) = 0$.

PROOF. Suppose $\det(\lambda I_n - A) = 0$. Then, the matrix $B = \lambda I_n - A$ is not invertible. In particular, the row reduced echelon form of B has some columns which do not contain a pivot. Thus, there exists a *non-zero* element $\mathbf{x} \in F^n$ such that $B\mathbf{x} = \mathbf{0}$. Thus $A\mathbf{x} = \lambda\mathbf{x}$. Let $\mathbf{v} = \mathcal{B}\mathbf{x}$. Thus, $M_{\mathcal{B}}(\mathbf{v}) = \mathbf{x}$. Note that $\mathbf{v} \neq \mathbf{0}$ since $\mathbf{x} \neq \mathbf{0}$. We know from Lemma 19.1 that

$$T(\mathbf{v}) = \mathcal{B} \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v}) = \mathcal{B} \cdot A \cdot \mathbf{x} = \mathcal{B} \cdot \lambda\mathbf{x} = \lambda \cdot \mathcal{B} \cdot \mathbf{x} = \lambda\mathbf{v}.$$

Thus, we see that λ is an eigenvalue corresponding to the eigenvector $\mathbf{v}$¿

The converse is essentially proved by reversing the above argument, but we will write the proof in detail. Suppose that λ is an eigenvalue corresponding to the eigenvector $\mathbf{v}$. Let $\mathbf{x} = M_{\mathcal{B}}(\mathbf{v})$. Observe that $\mathbf{x} \neq \mathbf{0}$ as $\mathbf{v} \neq \mathbf{0}$. By assumption, $T(\mathbf{v}) = \lambda\mathbf{v}$. Once again, recall that by Lemma 19, we know that

$$T(\mathbf{v}) = \mathcal{B} \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v}).$$

Thus,

$$\mathcal{B} \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v}) = \lambda\mathbf{v} = \lambda \cdot \mathcal{B} \cdot \mathbf{x} = \mathcal{B} \cdot (\lambda\mathbf{x}).$$

Thus (by Remark 18.13, we see that $M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v}) = \lambda\mathbf{x}$, i.e. $A\mathbf{x} = \lambda\mathbf{x}$. Thus $(\lambda I_n - A) \cdot \mathbf{x} = \mathbf{0}$. This shows that the matrix $(\lambda I_n - A)$ is not invertible. (Otherwise, we could multiply the equation $(\lambda I_n - A) \cdot \mathbf{x} = \mathbf{0}$ on the left by its inverse of this matrix, to get $\mathbf{x} = \mathbf{0}$, which we know is not true.) Thus $\det(\lambda I_n - A) = 0$. □

This leads us to define the following:

DEFINITION 24.9. Let n be a positive integer. Let $A \in M_{n\times n}(F)$. Let X denote a variable. The *characteristic polynomial of* A is defined to be the polynomial $\det(XI_n - A)$.

If A is a matrix, and λ is a root of the characteristic polynomial of A, then the matrix $\lambda I_n - A$ is not invertible. Thus, there exists an element $\mathbf{y} \neq \mathbf{0}$ of F^n such that $A\mathbf{y} = \lambda\mathbf{y}$. Thus $\mathbf{y}$ is an eigenvector of the linear transformation $T : F^n \to F^n$ defined by $T(\mathbf{x}) = A\mathbf{x}$.

It should be clear that we can use this method to find the eigenvalues of a linear transformation $T : V \to V$ for any abstract finite dimensional vector space V, not just F^n. To begin with, we simply fix the basis $\mathcal{B}$, which establishes an isomorphism of V with F^n (where $n = \dim(V)$) and then linear transformation T can be expressed as multiplication by an $n \times n$ matrix A. We compute the characteristic polynomial of A and find all its roots. By Proposition 24.8, the roots of this polynomial are exactly the eigenvalues of T.

What about the eigenvectors of T? Suppose A is as above and $\mathbf{x}$ is an eigenvector of the linear transformation $\mathbf{x} \mapsto A\mathbf{x}$ and the corresponding eigenvalue is λ. Then, we see from the proof of Proposition 24.8 that the element $\mathbf{v} = \mathcal{B} \cdot \mathbf{x}$ is an eigenvector of T and the corresponding eigenvalue is λ. Also, all eigenvectors of T can be obtained in this manner.

LEMMA 24.10. *Let n be a positive integer. Let $A, B \in M_{n\times n}(F)$ be two conjugate matrices. Then A and B have the same characteristic polynomial.*

PROOF. By assumption, there exists an invertible matrix P such that $A = P^{-1}BP$. Then we see that

$$\begin{aligned}\det(XI_n - A) &= \det(XI_n - P^{-1}BP)\\ &= \det(P^{-1} \cdot (XI_n - B) \cdot P)\\ &= \det(P^{-1}) \det(XI_n - B) \det(P)\\ &= \det(XI_n - B).\end{aligned}$$

This proves the result. □

LEMMA 24.11. *Let V be a finite dimensional vector space. Let $\mathcal{B}$ be a basis of V. Then, the characteristic polynomial of the matrix $M_{\mathcal{B}}^{\mathcal{B}}(T)$ does not depend on the choice of $\mathcal{B}$.*

PROOF. This follows from the previous lemma since if $\mathcal{C}$ is any other basis, the matrices $M_{\mathcal{B}}^{\mathcal{B}}(T)$ and $M_{\mathcal{C}}^{\mathcal{C}}(T)$ are conjugates. □

DEFINITION 24.12. Let V be a finite dimensional vector space. Let $T : V \to V$ be a linear transformation. The characteristic polynomial of T is defined to be the characteristic polynomial of the matrix $M_{\mathcal{B}}^{\mathcal{B}}(T)$ for any basis $\mathcal{B}$ of V.

EXAMPLE 24.13. Consider the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by $T(\mathbf{x}) = A\mathbf{x}$ where $A = \begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix}$. Let us find all the eigenvectors and eigenvalues of T.

The characteristic polynomial of A is

$$\det(XI_2 - A) = \det \begin{bmatrix} X-2 & -3 \\ -1 & X+2 \end{bmatrix} = (X-2)(X+2) - (-1)(-3) = X^2 - 7.$$

Thus, the eigenvalues of T are $\sqrt{7}$ and $-\sqrt{7}$.

Let us now find the eigenvectors of A. First we work with the eigenvalue $\sqrt{7}$. To find all the corresponding eigenvectors, we wish to solve the equation $A\mathbf{x} = \sqrt{7}\mathbf{x}$. This can be written as

$$\begin{bmatrix} \sqrt{7}-2 & -3 \\ -1 & \sqrt{7}+2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

As usual, we denote this by an augmented matrix.

$$\left[\begin{array}{cc|c} \sqrt{7}-2 & -3 & 0 \\ -1 & \sqrt{7}+2 & 0 \end{array}\right]$$

We perform the row operation $(\frac{1}{\sqrt{7}-2})R_1$.

$$\left[\begin{array}{cc|c} 1 & \frac{-3}{\sqrt{7}-2} & 0 \\ -1 & \sqrt{7}+2 & 0 \end{array}\right]$$

Perform the operation $R_2 + R_1$. (I have omitted the computations required to simplify the expression in the second row.)

$$\left[\begin{array}{cc|c} 1 & \frac{-3}{\sqrt{7}-2} & 0 \\ 0 & 0 & 0 \end{array}\right]$$

This gives us the eigenvector $\begin{bmatrix} \frac{3}{\sqrt{7}-2} \\ 1 \end{bmatrix}$.

A similar computation gives us the eigenvector $\begin{bmatrix} \frac{3}{-\sqrt{7}-2} \\ 1 \end{bmatrix}$ for the eigenvalue $-\sqrt{7}$. (Check this!)

EXAMPLE 24.14. Consider the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by $T(\mathbf{x}) = A\mathbf{x}$ where $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Let us find all the eigenvectors and eigenvalues of T. You may check that this is just the rotation around the origin through $\pi/2$ radians (i.e. 90 degrees) in the anti-clockwise sense. We know that if $\mathbf{v}$ is an eigenvector, the line $span(\mathbf{v})$ will be mapped into itself by T. But we know that the rotation through $\pi/2$ radians cannot map any line into itself – every line gets rotated through $\pi/2$ radians around the origin. So we do not expect to find any eigenvectors for this linear transformation. We will verify this algebraically.

The characteristic polynomial of A is

$$\det(XI_2 - A) = \det \begin{bmatrix} X & 1 \\ -1 & X \end{bmatrix} = X^2 + 1.$$

This polynomial has no root in $\mathbb{R}$ and so T has no eigenvectors.

Thus, we see that a linear transformation (or a matrix) can fail to have eigenvalues simply because the characteristic polynomial does not have any roots in the field F. This problem can be fixed by working over a field that is large enough so that all polynomials in $F[X]$ have roots. A field $F$is said to be *algebraically closed* if any non-constant polynomial in $F[X]$ has a root. It can be proved that every field is contained in a bigger field which is algebraically closed. Over an algebraically closed field, every square matrix will have at least one eigenvalue. We will not discuss this matter any further in this course.

Diagonalization:

DEFINITION 24.15. Let n be a positive integer. A matrix $A \in M_{n\times n}(F)$ is said to be a *diagonal matrix* if all of its non-zero entries are on the diagonal.

Note that for a matrix to be a diagonal matrix, the only requirement is that all the entries that are not on the diagonal should be zero. It is perfectly fine if there are some zeros on the diagonal as well.

LEMMA 24.16. *Let n be a positive integer. Let $A \in M_{n\times n}(F)$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ denote the standard basis of F^n. Then A is a diagonal matrix if and only if $\mathbf{e}_i$ is an eigenvector of the linear transformation $\mathbf{x} \mapsto A\mathbf{x}$ for every i.*

PROOF. Recall that the column matrix $A\mathbf{e}_i$ is just the i-th column of A.

If A is a diagonal matrix, $A\mathbf{e}_i$ can only have a non-zero term in the $(i,1)$-position and is hence a scalar multiple of $\mathbf{e}_i$. This shows that $\mathbf{e}_i$ is an eigenvector of the transformation $\mathbf{x} \mapsto A\mathbf{x}$.

Conversely, suppose that $\mathbf{e}_i$ is an eigenvector for the transformation $\mathbf{x} \mapsto A\mathbf{x}$. Thus, there exists an element $\lambda_i \in F$ such that $A\mathbf{e}_i = \lambda_i \mathbf{e}_i$. As this is the i-th column of A, we see that the i-th column of A has λ_i in the i-th row, and all other terms in this column are equal to 0. This shows that A is a diagonal matrix. □

DEFINITION 24.17. Let n be a positive integer. An $n \times n$ matrix is said to be diagonalizable if it is similar to a diagonal matrix.

DEFINITION 24.18. Let V be a finite dimensional vector space. Let $T : V \to V$ be a linear transformation. We say that T is diagonalizable if there exists a basis $\mathcal{B}$ such that $M_{\mathcal{B}}^{\mathcal{B}}(T)$ is diagonal.

LEMMA 24.19. *Let V be a finite dimensional vector space. Let $T : V \to V$ be a linear transformation. Let $\mathcal{B}$ be an ordered basis of V. Then $M_{\mathcal{B}}^{\mathcal{B}}(T)$ is a diagonal matrix if and only if every vector in $\mathcal{B}$ is an eigenvector of T.*

PROOF. Let $n = \dim(V)$ and let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ denote the standard basis of F^n. Recall (see Theorem 18.12) that we have an isomorphism between $\phi : V \to F^n$ given by $\phi(\mathbf{v}) = M_{\mathcal{B}}(\mathbf{v})$ and its inverse ψ is given by $\psi(\mathbf{x}) = \mathcal{B} \cdot \mathbf{x}$. Let $\mathcal{B} = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix}$. Then, $\phi(\mathbf{v}_i) = \mathbf{e}_i$ and $\psi(\mathbf{e}_i) = \mathcal{B} \cdot \mathbf{e}_i$.

Suppose that $M_{\mathcal{B}}^{\mathcal{B}}(T)$ is a diagonal matrix. Then, for every i, $\mathbf{e}_i$ is an eigenvector of the transformation $\mathbf{x} \mapsto M_{\mathcal{B}}^{\mathcal{B}}(T)\mathbf{x}$. Thus, for every i, there exists $\lambda_i \in F$ such that $M_{\mathcal{B}}^{\mathcal{B}}(T)\mathbf{e}_i = \lambda_i \mathbf{e}_i$. We know that

$$M_{\mathcal{B}}(T(\mathbf{v})) = M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathbf{v})$$

for every $\mathbf{v} \in V$. Using this for $\mathbf{v} = \mathbf{v}_i$, we get

$$M_{\mathcal{B}}(T(\mathbf{v}_i)) = M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot \mathbf{e}_i = \lambda_i \mathbf{e}_i.$$

Thus,

$$T(\mathbf{v}_i) = \mathcal{B} \cdot M_{\mathcal{B}}(T(\mathbf{v}_i)) = \mathcal{B} \cdot (\lambda \mathbf{e}_i) = \lambda_i \cdot \mathcal{B} \cdot \mathbf{e}_i = \lambda_i \mathbf{v}_i.$$

This shows that $\mathbf{v}_i$ is an eigenvector of T.

The converse is left as an exercise. □

LEMMA 24.20. *Let V be a finite dimensional vector space and let $\mathcal{B}$ be an ordered basis of V. Let $T : V \to V$ be a linear transformation. Then T is diagonalizable if and only if the matrix $M_{\mathcal{B}}^{\mathcal{B}}(T)$ is diagonalizable.*

PROOF. Suppose $M_{\mathcal{B}}^{\mathcal{B}}(T)$ is diagonalizable. Thus, there exists an invertible matrix P such that the matrix $P^{-1} M_{\mathcal{B}}^{\mathcal{B}}(T)$ is diagonal. Let $\mathcal{C} = \mathcal{B} \cdot P$. By Exercise 20.3, $\mathcal{C}$ is an ordered basis of V. Also $M_{\mathcal{B}}(\mathcal{C}) = P$.

We also know that

$$M_{\mathcal{C}}^{\mathcal{C}}(T) = M_{\mathcal{B}}(\mathcal{C})^{-1} \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot M_{\mathcal{B}}(\mathcal{C}) = P^{-1} \cdot M_{\mathcal{B}}^{\mathcal{B}}(T) \cdot P.$$

By assumption, this is a diagonal matrix. Thus, T is diagonalizable.

The converse is left as an exercise. □

By Lemma 24.19, we see that to diagonalize a linear transformation $T : V \to V$, we need to find a basis of V consisting eigenvectors of V. Such a basis will not always exist. The transformation is diagonalizable if and only if we can find a basis consisting of eigenvectors.

PROPOSITION 24.21. *Let V be a vector space and let $T : V \to V$ be a linear transformation. For any $\lambda \in F$, we define*

$$V_\lambda = \{\mathbf{v} \in V : T(\mathbf{v}) = \lambda \mathbf{v}\}.$$

(1) *For any $\lambda \in F$, the set V_λ is a subspace of V.*
(2) *For $\lambda \in F$, $V_\lambda \neq \{\mathbf{0}\}$ if and only if λ is an eigenvalue of T.*
(3) *Let $\lambda_1, \ldots, \lambda_k$ distinct eigenvalues of T. Then the subspaces V_{λ_i} are independent.*

PROOF. We first prove (a). Fix $\lambda \in F$ and define $S : V \to V$ by $S(\mathbf{v}) = T(\mathbf{v}) - \lambda\mathbf{v}$. Then, S is a linear transformation. (Do you see why?) Then V_λ is just the kernel of S and is hence a subspace of V. This completes the proof of (a).

Part (b) is an immediate consequence of the definition of an eigenvector.

We prove part (c) by induction on k. When $k = 1$, the claim is trivially true. Now suppose that the result is known to be true for $k \leqslant r$. We will verify the result for $k = r + 1$.

Let $\lambda_1, \ldots, \lambda_{r+1}$ distinct eigenvalues of T. Suppose we have an equation

$$\mathbf{v}_1 + \cdots + \mathbf{v}_{r+1} = \mathbf{0} \tag{24.1}$$

where $\mathbf{v}_i \in V_{\lambda_i}$ for every i. Applying T to both sides, we get

$$\lambda_1\mathbf{v}_1 + \cdots + \lambda_{r+1}\mathbf{v}_{r+1} = \mathbf{0}. \tag{24.2}$$

Subtracting λ_{r+1} times equation (24.1) from equation (24.2), we get

$$(\lambda_1 - \lambda_{r+1})\mathbf{v}_1 + \ldots + (\lambda_r - \lambda_{r+1})\mathbf{v}_r = \mathbf{0}.$$

We set $\mathbf{w}_i = (\lambda_i - \lambda_{r+1})\mathbf{v}_i$. Then, $\mathbf{w}_i \in V_{\lambda_i}$ for $i = 1, \ldots, r$ and we have the equation

$$\mathbf{w}_1 + \cdots + \mathbf{w}_r = \mathbf{0}.$$

By the induction hypothesis, we have $\mathbf{w}_i = 0$ for $i = 1, \ldots, r$. Thus, $(\lambda_i - \lambda_{r+1})\mathbf{v}_i = 0$ for $i = 1, \ldots, r$. But then, for every such i, we have $\lambda_i - \lambda_{r+1} \neq 0$. Thus, we see that $\mathbf{v}_i = \mathbf{0}$ for $i = 1, \ldots, r$. Then, equation (24.1) tells us that $\mathbf{v}_{r+1}$ is equal to $\mathbf{0}$ as well. Thus, $\mathbf{v}_i = \mathbf{0}$ for $i = 1, \ldots, r + 1$. This proves (c). □

We will need to use the following fact about polynomials. We will not prove it in this course:

FACT 24.22. *A non-constant polynomial in $F[X]$ of degree d has at most d distinct roots.*

Now, let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation. Let $\lambda_1, \ldots, \lambda_k$ be all the distinct eigenvalues of T. (Note that they are finite in number because of Fact 24.22.) By Proposition 24.21, we see that the spaces $V_{\lambda_1}, \ldots, V_{\lambda_k}$ are indepedent. Thus, by Remark 22.9, we see that

$$\dim(\sum_{i=1}^{k} V_{\lambda_i}) = \sum_{i=1}^{k} \dim(V_{\lambda_i}).$$

In particular, we see that

$$\sum_{i=1}^{k} \dim(V_{\lambda_i}) \leqslant \dim(V).$$

Suppose $\mathcal{B}$ is a basis of V consisting of eigenvectors of T. Each element of $\mathcal{B}$ lies in some V_{λ_i}. For every i, let $\mathcal{B}_i = \mathcal{B} \cap V_{\lambda_i}$ and let $W_i = \mathit{span}(\mathcal{B}_i)$. For $i \neq j$, we see that

$$\mathcal{B}_i \cap \mathcal{B}_j \subset V_{\lambda_i} \cap V_{\lambda_j} = \{\mathbf{0}\}.$$

As every element of $\mathcal{B}$ is non-zero, we conclude that $\mathcal{B}_i \cap \mathcal{B}_j = \varnothing$ for $i \neq j$. Thus $\mathcal{B}$ is a disjoint union of the $\mathcal{B}_i$ and hence $\sum_{i=1}^{k} |\mathcal{B}_i| = |\mathcal{B}| = \dim(V)$.

For every i, W_i is a subspace of V_i and we have $V_{\lambda_i} = W_i$ if and only if $\mathcal{B}_i$ is a basis of V_i. So,

$$\begin{aligned}\dim(V) &= |\mathcal{B}| \\ &= \sum_{i=1}^{k} |\mathcal{B}_i| \\ &= \sum_{i=1}^{k} \dim(W_i) \\ &\leqslant \sum_{i=1}^{k} \dim(V_{\lambda_i}) \\ &\leqslant \dim(V).\end{aligned}$$

This shows that equality holds at each stage in this sequence of inequalities. Thus $\mathcal{B}_i$ is a basis of V_{λ_i} for every i.

Algorithm for diagonalizing a linear transformation:

The above discussion gives us an algorithm for checking whether T is diagonalizable and, if it is so, to find a basis which actually diagonalizes it:

STEP 1 : Fix an ordered basis $\mathcal{B}$ of V. Compute the matrix $M_{\mathcal{B}}^{\mathcal{B}}(T)$ and then compute its eigenvalues. These are the eigenvalues of T. Let us denote them by $\lambda_1, \ldots, \lambda_k$.

STEP 2 : For $i = 1, \ldots, k$, we define $V_{\lambda_i} = ker(\lambda_i \cdot Id_V - T)$ where Id_V is the identity transformation on V (defined by $Id_V(\mathbf{v}) = \mathbf{v}$).

STEP 3 : If $\sum_{i=1}^{k} \dim(V_{\lambda_i}) < \dim(V)$, then T is not diagonalizable.

STEP 4 : If $\sum_{i=1}^{k} \dim(V_{\lambda_i}) = \dim(V)$, find a basis $\mathcal{B}_i$ of V_{λ_i}. Then $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{B}_i$ is a basis of V consisting of eigenvectors of T.

Algorithm for diagonalizing a matrix:

Suppose we are given an $n \times n$ matrix A. We wish to find whether this matrix is diagonalizable. We apply the above algorithm to the transformation $\mathbf{x} \mapsto A\mathbf{x}$ and obtain the following:

STEP 1 : Compute the characteristic polynomial of A and then compute all its roots. These are the eigenvalues of A. Let us denote them by $\lambda_1, \ldots, \lambda_k$.

STEP 2 : For $i = 1, \ldots, k$, we find the set V_i of all $\mathbf{x}$ such that $(\lambda_i I_n - A)\mathbf{x} = \mathbf{0}$. This is done by the row reduction algorithm. The set of all such $\mathbf{x}$ is a subspace of F^n. Let d_i be the dimension V_i. (One can check that d_i is just equal to n minus the number of pivots in the row-reduced echelon form of the matrix $\lambda_i I_n - A$.)

STEP 3 : If $\sum_{i=1}^{k} d_i < n$, then A is not diagonalizable.

STEP 4 : If $\sum_{i=1}^{k} \dim(V_i) = n$, find a basis $\mathcal{B}_i$ of V_i. Then $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{B}_i$ is a basis of F^n. Let $\mathcal{E}$ denote the standard basis of F^n. Then we set $P = \mathcal{M}_{\mathcal{E}}(\mathcal{B})$. (This matrix is very easy to write down if you actually have the elements of $\mathcal{B}$. The elements of $\mathcal{B}$ are $n \times 1$-matrices. Simply place them side-by-side to obtain an $n \times n$-matrix. This is precisely the matrix $M_{\mathcal{E}}(\mathcal{B})$.) Then $P^{-1}AP$ is a diagonal matrix.