HONOURS ALGEBRA 2020-21

Notes by Iain Gordon

used and developed by Harry Braden, Iain Gordon, Richard Gratwick, Milena Hering, Gergo Nemes and Andrew Ranicki

Contents

Preface

These are the notes for the Y3 Honours Algebra course. I recommend these ahead of any book, although in due course you may find some books mentioned on the LEARN page for this course. The notes are often quite discursive and they will contain all the content and more of what we cover in during lectures. They also overlap with Workshops. It is these notes that form the basis of the examinable material for the course.

Acknowledgments

I have been combining already existing lecture notes from a number of sources to produce: Professors Brown, Gillespie, Mason, Smith, Smyth, Soergel, Webber, Whitelaw, Wemyss. I found the point of view of Wolfgang Soergel particularly to the point and satisfying, and so followed his lead quite often.

CHAPTER 1

Vector Spaces

In this chapter I will discuss "real space" and simultaneous linear equations, and how the theory of abstract vector spaces provides a bridge between the two.

1.1. Solutions of Simultaneous Linear Equations

Let F be a field. I will discuss precisely what this means later; in what we are going to do for the moment you can just as well think of the field $F = \mathbb{Q}$ of rational numbers, or the field $F = \mathbb{R}$ of real numbers, or the field $F = \mathbb{C}$ of complex numbers.

Suppose we have been given n equations in m unknowns:

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m & = & b_2 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m & = & b_n \end{array}$$

I intend that $a_{ij}, b_i \in F$ are fixed, and that we are supposed to solve the equations by finding the x_j's. You, as a mathematically mature reader, know the general convention in Mathematics that we use letters from the beginning of the alphabet for "known indeterminates" and letters from the end of the alphabet for "unknown indeterminates"; don't get confused with the convention in Politics.

We call this a **system of linear equations**. Linear means that there are no complicated terms in the unknowns such as x_1^2 or $x_1x_2^7$. If all the b_i are zero in the right hand side of our equations, then we call our system **homogeneous**. We can construct a new system of linear equations from the old one by setting all the b_i to zero: this is called the associated **homogenised** system of equations.

What I want us to do is give a description of all m-tuples $(x_1, \ldots, x_m)$ of elements of F such each of the n equations is satisfied. A better way to express this is for me to ask you to give the most explicit description you can of the subset $L \subseteq F^m$ consisting of all m-tuples that satisfy the n equations. The set L is called **solution set** of our system of equations.

EXAMPLES 1.1.1. Here are some examples of such systems.

(1) Here is a system of linear equations with three equations and three unknowns:

$$\begin{array}{rcl} x_1 + 3x_2 & = & 1 \\ 2x_1 + 2x_2 + x_3 & = & 2 \\ 4x_1 + 6x_2 + x_3 & = & 8 \end{array}$$

(2) Here is a homogeneous system of linear equations with two equations and three unknowns:

$$\begin{array}{rcl} 2y - 17z & = & 0 \\ 4x + 22y + z & = & 0 \end{array}$$

I've written x, y, z instead of x_1, x_2, x_3: it's more sensible to use a notation that needs as few indices as possible.

(3) Here is an inhomogeneous system of linear equations with one equation and one unknown:

$$0x = 1$$

It has an empty solution set.

It saves a lot of writing to omit the symbols x_i as well as the plus signs and the equality signs from the system of linear equations, and instead describe it in shorthand by its **extended coefficient matrix**

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1m} & b_1 \\ a_{21} & a_{22} & \dots & a_{2m} & b_2 \\ \vdots & & & \vdots & \\ a_{n1} & a_{n2} & \dots & a_{nm} & b_n \end{array}\right)$$

The specification "extended" refers to the last column containing the b_i. The family of a_{ij} alone is called the **coefficient matrix** of our system of equations. For instance, 1.1.1(1) is written as

$$\left(\begin{array}{ccc|c} 1 & 3 & 0 & 1 \\ 2 & 2 & 1 & 2 \\ 4 & 6 & 1 & 8 \end{array}\right)$$

REMARK 1.1.2. When you look at our a system of linear equations, don't read a_{12} as a–twelve, rather as a–one–two. It would of course be more precise to separate the two indices by a comma, writing $a_{1,2}$ and so on, but this makes the system of equations harder to read. When writing Mathematics there is often a choice between a precise hard-to-read statement and an easy-to-read imprecise statement: it seems better to me to be legible. In Physics, sadly, it is common to put indices as superscripts, writing a_1^2 and so on, but that can also cause confusion with squares $(a_1)^2$.

To calculate the solution set to a system of linear equations we can apply **Gaussian elimination**. This is based on the elementary observation that the solution set does not change if we apply either of the following operations to produce a new system of linear equations:

[*Row Addition*] Replace an equation by its sum with a multiple of another of our equations;
[*Row Swap*] Swap two of our equations.

By applying these operators, Gaussian elimination transforms a system of linear equations to **echelon form** without changing the solution set. To describe this formally, we say that a system of linear equations is "in echelon form" precisely when we can find $r \geqslant 0$ and indices $1 \leqslant s(1) < s(2) < \ldots < s(r) \leqslant m$ so that in our system of equations we have $a_{i,s(i)} \neq 0$ for $1 \leqslant i \leqslant r$ and that $a_{\nu\mu} \neq 0$ occurs only when there is an i with $\nu \leqslant i$ and $\mu \geqslant s(i)$.

In an example, this looks so:

$$\left(\begin{array}{cccccccc|c} 0 & 0 & \neq 0 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & \neq 0 & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & \neq 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \neq 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & * \end{array}\right) \Bigg\} r(=4)$$

$$\begin{array}{cccccccccc} & & s(1) & & s(2) & s(3) & & s(4) & & \end{array}$$

ETYMOLOGY. "Echelon" is French for "step": here it is the entries that are zero in the coefficient matrix that make "steps of height one but with variable breadth". The symbol $*$ that we see throughout the top-right indicates that it is irrelevant what these entries are.

Gaussian ELIMINATION solves a system of linear equations functions as follows:

• If all the coefficients in the first column are zero, we ignore this column and continue with the algorithm on the remainder of the coefficient matrix. If there is a coefficient in the first column that is not zero, we bring it to the first row by applying a [*Row Swap*] with the first row. Then apply [*Row Addition*] to add suitable multiples of the first row to the other rows so that we arrive at a system in which the entries below the top of the first column are zero. We then continue the algorithm by ignoring the first row and repeating the above process. Obviously we can use this to bring any system of linear equations into echelon form, without changing its solution set.

• Having carried out the above procedure, the solution set of a linear system of equations in echelon form is quick to calculate: If any of the numbers $b_{r+1}, \ldots, b_n$ are not zero there are no solutions at all. Assuming that $b_{r+1} = \cdots = b_n = 0$, we then can choose arbitrary values for x_μ with $\mu > s(r)$ and then calculate the unique value for $x_{s(r)}$ in terms of b_r and the x_μ with $\mu > s(r)$ by using the equation in the r-th row, then $x_{s(r-1)}$ in terms of b_{r-1} and x_μ with $\mu > s(r-1)$ by using the equation in the $r-1$-st row, and so on. This provides us with the general m-tuple $(x_1, \ldots, x_m)$ that is a solution of the system of equations.

EXAMPLE 1.1.3. A linear system of equations with three equations and three unknowns and the derivation of its solution with Gaussian elimination.

$$\begin{aligned} x_1 + 2x_2 &= -1 \\ 2x_1 + 7x_2 + x_3 &= -2 \\ 5x_1 + 8x_2 + x_3 &= -3 \end{aligned}$$

$\Big\downarrow$ transform to coefficient matrix

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

$\Big\downarrow$ $R2 \mapsto R2 - 2R1$, $R3 \mapsto R3 - 5R1$

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

$\Big\downarrow$ $R3 \mapsto R3 + \frac{2}{3}R2$

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

$\Big\downarrow$ solve for x_3, then x_2, then x_1

$$\begin{cases} x_3 = \frac{6}{5}, \\ x_2 = -\frac{2}{5}, \\ x_1 = -\frac{1}{5}. \end{cases}$$

Often in the examples we study it won't be necessary to swap rows. If there are exactly as many equations as unknowns we usually expect exactly one solution, just as above.

A mapping from the product of sets $\{1, \ldots, n\} \times \{1, \ldots, m\}$ to a set Z is called an $(n \times m)$-**matrix with coefficients in** Z. Given such a matrix A we will write A_{ij} or a_{ij} instead of $A(i, j)$ and visualise this data as a rectangular arrangement of elements from Z, just as in the case when Z is the field F. We will call the i the **row index** since it indicates in which row our entry a_{ij} stands, and the j will be called the **column index** of our matrix entry. The set of all $(n \times m)$-matrices with coefficients in Z will be denoted

$$\mathsf{Mat}(n \times m; Z) := \mathrm{Maps}(\{1, \ldots, n\} \times \{1, \ldots, m\}, Z). \tag{1}$$

In the case when $n = m$ we will speak of a **square matrix** and shorten our notation from $\mathsf{Mat}(n \times n; Z)$ to $\mathsf{Mat}(n; Z)$.

ETYMOLOGY. The terminology "Matrix" was introduced by the English mathematician Arthur Cayley in an article "Remarques sur la notation des functions algébriques" in Crelle's Journal in 1855, Volume 50, page 282. The terminology seems to originate from the Latin word "mater" for the English "mother": at least Cayley writes on page 284 from loc. cit. : "Il y aurait bien des choses à dire sur cette théorie des matrices, laquelle doit, il me semble, précéder la théorie des Déterminants". On page 313 he introduces the so-called "minors", so one supposes that he wanted the role of the matrix to the fore, with the image of the "mother of the determinant and her general minors". We'll discuss the determinant later, but probably not the minors.

THEOREM 1.1.4 (Solution sets of inhomogeneous systems of linear equations). *If the solution set of a linear system of equations is non-empty, then we obtain all solutions by adding componentwise an arbitrary solution of the associated homogenised system to a fixed solution of the system.*

PROOF. If $c = (c_1, \ldots, c_m)$ is a solution of our system of linear equations and $h = (h_1, \ldots, h_m)$ is a solution of the homogenised system, then it is obvious that the componentwise sum $c \dot{+} h = (c_1 + h_1, \ldots, c_m + h_m)$ is a solution of the original system. On the other hand if $c' = (c'_1, \ldots, c'_m)$ is another solution of our system of linear equations then it is clear that the componentwise difference $h = (c'_1 - c_1, \ldots, c'_m - c_m)$ is a solution of the homogenised system which furthermore satisfies $c' = c \dot{+} h$. □

HERE IS WHERE THE THINKING STARTS!

These considerations show how to determine the solution set of any system of linear equations. If the solution set is non-empty, we use Gaussian elimination to bring the system in to echelon form. This then produces a bijection between t-tuples of elements of F and particular solutions, where $t = m - r$ is the number of variables less the "number of stairs", corresponding to values of x_j where j is different from the "column indices of stairs" $j \neq s(1), \ldots, s(r)$.

Now observe that when we run the Gaussian algorithm we get to choose which [*Row Swaps*] we make as it runs. This leads us immediately to ask: do we always arrive at the same echelon form for our matrix, independent of the choice of row swaps? The answer is "no", but nonetheless the "widths of the individual stairs", that is the column indices of the stairs $s(1), \ldots, s(r)$ are independent of all choices. In fact these can be directly described if we consider the associated homogenised system of equations and run through the variables from last to first. We ask if for

each $(x_{j+1}, \ldots, x_m)$ which can be extended to a solution $(x_1, x_2, \ldots, x_m)$, there exists a unique x_j such that $(x_j, x_{j+1}, x_{j+2}, \ldots, x_m)$ extends to a solution $(x_1, x_2, \ldots, x_m)$? The answer is "yes" precisely when a new step begins at the j-th column.

It is also obvious that if we relabel the variables in our system of linear equations, nothing should really change. Another way to think about this is that if we swap the columns of our coefficient matrix, nothing should really change in the solution. But if we now run Gaussian elimination we will get, just as above, a bijection between u-tuples of elements of F and the solution set. The question then staring us in the face is: is it true that $u = t$? In other words, do we get an echelon form with the same number of stairs if we arbitrarily swap the columns of our matrix before we run Gaussian elimination?

The answer is of course "yes", but I don't know an elementary argument. In fact, I'm really quite happy that I don't! We can take this question as a motivation to develop the abstract theory of vector spaces, and of course, that is what we are about to do. In doing this, we will introduce the notion of "dimension" of a "vector space", and show that the number of stairs is independent of all choices because it can be interpreted in terms of the "dimension of the solution set" of the associated homogenised system of equations.

1.2. Fields and Vector Spaces

DEFINITION 1.2.1. (i) *A* **field** F *is a set with functions*

$$\begin{aligned} &\textit{addition} \;=\; + :\; F \times F \to F\;;\; (\lambda, \mu) \mapsto \lambda + \mu \\ &\textit{multiplication} \;=\; .\; :\; F \times F \to F\;;\; (\lambda, \mu) \mapsto \lambda\mu \end{aligned}$$

such that $(F, +)$ *and* $(F\backslash\{0\}, .)$ *are abelian groups, with*

$$\lambda(\mu + \nu) \;=\; \lambda\mu + \lambda\nu \in F$$

for any $\lambda, \mu, \nu \in F$*. The neutral elements are called* 0_F, 1_F*. In particular, for all* $\lambda, \mu \in F$

$$\lambda + \mu \;=\; \mu + \lambda\;,\; \lambda.\mu \;=\; \mu.\lambda\;,\; \lambda + 0_F \;=\; \lambda\;,\; \lambda.1_F \;=\; \lambda \in F\;.$$

For every $\lambda \in F$ *there exists* $-\lambda \in F$ *such that*

$$\lambda + (-\lambda) \;=\; 0_F \in F\;.$$

For every $\lambda \neq 0 \in F$ *there exists* $\lambda^{-1} \neq 0 \in F$ *such that*

$$\lambda(\lambda^{-1}) \;=\; 1_F \in F\;.$$

(ii) *A* **vector space** V **over a field** F *is a pair consisting of an abelian group* $V = (V, \dot{+})$ *and a mapping*

$$F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$$

such that for all $\lambda, \mu \in F$ *and* $\vec{v}, \vec{w} \in V$ *the following identities hold:*

$$\begin{aligned} \lambda(\vec{v} \dot{+} \vec{w}) &= (\lambda\vec{v}) \dot{+} (\lambda\vec{w}) \\ (\lambda + \mu)\vec{v} &= (\lambda\vec{v}) \dot{+} (\mu\vec{v}) \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1_F\vec{v} &= \vec{v} \end{aligned}$$

The first two laws are the **Distributive Laws***; the third law is called the* **Associativity Law***. I will often also call a vector space* V *over a field* F *an* F**-vector space**.

I will typically call the elements of a vector space **vectors** and the elements of the field F **scalars**. I will call the field itself the **ground field**. The mapping $(\lambda, \vec{v}) \mapsto \lambda\vec{v}$ is called **multiplication by scalars** or alternatively the **action of the field F on V**. You absolutely must not confuse this with the "scalar product" that you have met in other courses: that produces a scalar from two vectors. For didactic reasons, I have written the addition of vectors by $\dot{+}$. This distinguishes it from the addition of elements of the field. But, since it needs extra typing, I will not do it for much longer. Typically I'll use the usual convention of "order of operations", the simpler notation for addition of vectors $+$, and the shorthand $1_F = 1$, in order to get a formulation that seems much easier-on-the-eye: for all scalars λ, μ and all vectors $\vec{v}, \vec{w}$ the following hold:

$$\begin{aligned} \lambda(\vec{v} \dot{+} \vec{w}) &= \lambda\vec{v} \dot{+} \lambda\vec{w} \\ (\lambda + \mu)\vec{v} &= \lambda\vec{v} \dot{+} \mu\vec{v} \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1\vec{v} &= \vec{v} \end{aligned}$$

For more serious didactic reasons, I've written vectors with a little arrow, but sometimes I lapse; you should certainly remember to imagine the arrow there. I will write $\vec{0}$ for the zero element of the abelian group V and call it the **zero vector**. Observe that the last law $1\vec{v} = \vec{v}$ excludes the possibility that we take V to be some non-zero abelian group and then set $\lambda\vec{v} = \vec{0}$ for all $\lambda \in F$ and $\vec{v} \in V$.

ETYMOLOGY. The terminology "vector" comes from the Latin "vehere" which means "to transport" or "to carry". This comes from thinking of a vector in the plane as transporting all points in the plane in the direction and length of the vector. So in English an intuitive translation would be "pusher". But since I'd then be giving a course on "Pusher Algebra", I'm much happier with the traditional terminology and I thank the Romans, once again. The use of the word "scalar" for the elements of the ground field comes from the Latin word "scala" for "ladder". From here the meaning developed into the name for a tape measure and then into what one can read off of a tape measure, and hence the real numbers. In Mathematics and Physics we don't use only real vector spaces, and so we adapt this word for general use as the terminology for an element of ground field.

We now need to make a few deductions to check vector spaces' hygiene.

LEMMA 1.2.2 (Product with the scalar zero). *If V is a vector space and $\vec{v} \in V$, then $0\vec{v} = \vec{0}$.*

In words "zero times a vector is the zero vector".

PROOF. To prove this, we use the second distributive law

$$0\vec{v} = (0 + 0)\vec{v} = 0\vec{v} \dot{+} 0\vec{v}$$

and then subtract $0\vec{v}$ from both sides to leave $\vec{0} = 0\vec{v}$. □

LEMMA 1.2.3 (Product with the scalar (-1)). *If V is a vector space and $\vec{v} \in V$, then $(-1)\vec{v} = -\vec{v}$.*

PROOF. To prove this we find with the last and the second laws from the definition of a vector space that

$$\vec{v} \dot{+} (-1)\vec{v} = 1\vec{v} \dot{+} (-1)\vec{v} = (1 + (-1))\vec{v} = 0\vec{v} = \vec{0}$$

and thus $(-1)\vec{v}$ is the additive inverse of $\vec{v}$. □

LEMMA 1.2.4 (Product with the zero vector). *If V is a vector space over a field F, then $\lambda\vec{0} = \vec{0}$ for all $\lambda \in F$. Furthermore, if $\lambda\vec{v} = \vec{0}$ then either $\lambda = 0$ or $\vec{v} = \vec{0}$.*

PROOF. Exercise. □

EXAMPLE 1.2.5. Given a field F, the abelian group $V = F$ is an F-vector space with multiplication by scalars given by the usual multiplication in F. The one-element abelian group $V = 0$ equipped with the obvious operation is a vector space over every field, and called the **trivial vector space** or the **zero vector space**.

EXERCISE 1. Given a set X and a vector space V over F, show that: the set $\mathrm{Maps}(X, V)$ of all mappings from $X \to V$ is an F-vector space, if we define addition by $(f+g)(x) = f(x)+g(x)$ and multiplication by scalars by $(\lambda f)(x) = \lambda(f(x))$.

In particular, it follows from this exercise that the set $\mathsf{Mat}(n \times m; F)$ of all $(n \times m)$-matrices with entries from the field F from (1) has the structure of an F-vector space.

1.3. Product of Sets and of Vector Spaces

So far you will be used to the **cartesian product** $X \times Y$ of two sets X and Y. But of course we can also introduce the cartesian product of the sets $X_1, \ldots, X_n$

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_i \in X_i \text{ for } 1 \leqslant i \leqslant n\}.$$

We call the elements of such a product n**-tuples**. An individual entry x_i of an n-tuple $(x_1, \ldots, x_n)$ is called a **component**.

There are special mappings called **projections** for a cartesian product

$$\begin{array}{rcl} \mathrm{pr}_i : X_1 \times \cdots \times X_n & \to & X_i \\ (x_1, \ldots, x_n) & \mapsto & x_i. \end{array}$$

The cartesian product of n copies of a set X is written in short as

$$X^n$$

The elements of X^n are n-tuples of elements from X. In the special case $n = 0$ we use the general convention that X^0 is "the" one element set, so that for all $n, m \geqslant 0$ we then have the canonical bijection

$$X^n \times X^m \xrightarrow{\sim} X^{n+m}\,;\, ((x_1, x_2, \ldots, x_n), (x_{n+1}, x_{n+2}, \ldots, x_{n+m})) \mapsto (x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m})\,.$$

EXAMPLE 1.3.1 (The vector space of n-tuples). A particularly important example is the vector space

$$V = F^n$$

over the field F. Here I am using the notation from above, so that elements of V are n-tuples of elements from the field F. The vector space operations are as follows:

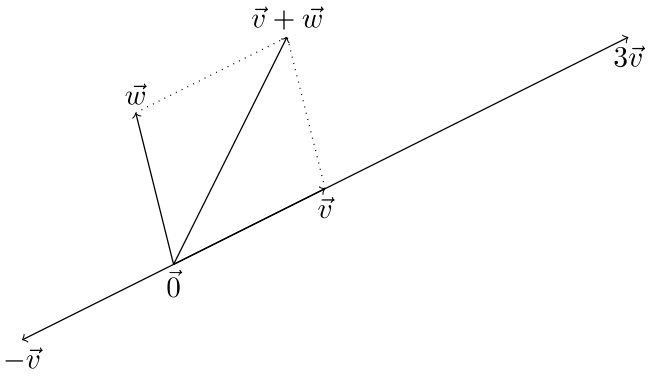
$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \dot{+} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} := \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix} \qquad \text{and} \qquad \lambda \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} := \begin{pmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{pmatrix}$$

for $\lambda, v_1, \ldots, v_n, w_1, \ldots, w_n \in F$.

I have written the components of our n-tuples vertically here because it's easier to read, rather than putting them side-by-side separated by commas. The first of our equations defines the sum of two n-tuples, and thus addition in our vector space $V = F^n$, and it does so using the addition in the field F. The second equation provides multiplication by scalars. I've continued with the didactic notation $\dot{+}$ instead of $+$, but from now on I'm giving up and I will write $+$ instead of $\dot{+}$. You need to know that if $\vec{v} \in F^n$, I will write $v_1, v_2, \ldots, v_n$ for its components and since these are not furnished with arrows, they are elements of the ground field F. If ever I write $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$, then

these are not the components of an n-tuple $\vec{v}$, but rather n vectors from a vector space. Eventually, however, I'm probably going to drop the arrows, and then it is up to you, dear Reader, to decide from the context what is intended.

EXAMPLE 1.3.2 (Vector space as SPACE AROUND US). Do not misunderstand the following waffle as the basis for a philosophical theory of anything! I think of a real vector space mostly as the space all around us – whatever that is and whatever that means –, together with a predetermined fixed point of origin. More exactly, I think of vectors as arrows attached to the fixed point and ending at some other point. To add two vectors I then push one in a parallel direction until it reaches the endpoint of the first, and then I take the point where it ends to determine a new arrow that ends there. I take the product of a vector with a scalar to mean change the length of the arrow by the amount given by the scalar. The negative of an arrow just an arrow of the same length pointing in the opposite direction. I think of the zero vector as the distinguished fixed point itself.



EXERCISE 2. Given a field F and F-vector spaces $V_1, \ldots, V_n$, show that: the cartesian product $V_1 \times \cdots \times V_n$ is an F-vector space if we define addition and multiplication by scalars componentwise.

In formulas, these look just like the formulas in Example 1.3.1 except that wherever we see v_i and w_i there we put arrows, and instead of writing $v_i, w_i \in F$ we write $\vec{v}_i, \vec{w}_i \in V_i$. We have a special notation for this new vector space

$$V_1 \oplus \cdots \oplus V_n$$

and we name it the **product** or the **direct sum** or most-precisely-of-all the **external direct sum** (because we will discuss the distinct notion of "internal direct sum of subspaces" in Definition 1.7.6). In particular F^n is the external direct sum $F \oplus \cdots \oplus F$ of n copies of the F-vector space F.

1.4. Vector Subspaces

DEFINITION 1.4.1. *A subset U of a vector space V is called a* **vector subspace** *or* **subspace** *if U contains the zero vector and whenever $\vec{u}, \vec{v} \in U$ and $\lambda \in F$ we have $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$.*

REMARK 1.4.2. From a higher standpoint the "correct" definition of a vector subspace looks a bit different and is as follows: let F be a field. A subset of an F-vector space is called a vector subspace if it can be given the structure of an F-vector space such that the embedding is a "homomorphism of F-vector spaces". I can't give you this better definition because we haven't learnt about homomorphisms of F-vector spaces. So in fact this definition is more complicated! But I think it is better because it also applies to subgroups, subfields, sub-almost-any-other-structure-you-want, as you will learn later.

EXAMPLE 1.4.3 (Solution sets as vector subspaces). As we discussed in the first section of this chapter, by a homogeneous system of linear equations over a field F, we mean a system of equations of the form

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m & = & 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m & = & 0 \\ \vdots \qquad \vdots \qquad\qquad \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m & = & 0 \end{array}$$

where there are only zeros on the right. The solution set of such a homogeneous system of linear equations is obviously a vector subspace $L \subseteq F^m$.

EXAMPLE 1.4.4 (Vector subspaces of SPACE AROUND US). Do not misunderstand the following waffle as the basis for a philosophical theory of anything! In Example 1.3.2 of a vector space as the space around us with a predetermined fixed point of origin, a subspace would be one of the following: (1) the one-element subset consisting only of the fixed point of origin, (2) all straight lines that pass through the fixed point of origin, (3) all planes that pass through the fixed point of origin, and (4) the whole of space around us.

PROPOSITION 1.4.5 (Generating a vector subspace from a subset). *Let T be a subset of a vector space V over a field F. Then amongst all vector subspaces of V that include T there is a smallest vector subspace*

$$\langle T \rangle = \langle T \rangle_F \subseteq V.$$

It can be described as the set of all vectors $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ with $\alpha_1, \ldots, \alpha_r \in F$ and $\vec{v}_1, \ldots, \vec{v}_r \in T$, together with the zero vector in the case $T = \emptyset$.

An expression of the form $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ is called a **linear combination** of vectors $\vec{v}_1, \ldots, \vec{v}_r$. We only allow sums with a finite number of terms. The smallest vector subspace $\langle T \rangle \subseteq V$ containing T is called the **vector subspace generated by** T or the vector subspace **spanned by** T or even the **span of** T. If we allow the zero vector to be the "empty linear combination of $r = 0$ vectors", which is what we will mean from hereon, then the span of T is exactly the set of all linear combinations of vectors from T.

PROOF. It is clear that all linear combinations of vectors from T form a vector subspace of V which contains T. It is just as clear that every vector subspace of V that contains T must contain all linear combinations of vectors from T. □

Other possible notation for the subspace generated by a subset T includes $\mathsf{span}(T)$ and $\mathsf{lin}(T)$.

EXAMPLE 1.4.6. We will use the following fact a lot: If $v \in \langle T \rangle$, then $\langle T \cup \{v\} \rangle = \langle T \rangle$.

DEFINITION 1.4.7. *A subset of a vector space is called a* **generating set** *of our vector space if its span is all of the vector space. A vector space that has a finite generating set is said to be* **finitely generated**.

EXAMPLE 1.4.8 (Finite generation in SPACE AROUND US). Do not misunderstand the following waffle as the basis for a philosophical theory of anything! In Example 1.3.2 of a vector space as the space around us with a predetermined fixed point of origin: the vector subspace generated by the zero vector consists only of the zero vector and so is just our fixed point of origin; the vector subspace generated by one non-zero vector can be thought of as the infinite straight line that passes through the fixed point of origin and the endpoint of our arrow; the vector subspace generated by two vectors, neither of which is a multiple of the other, is the infinite plane in which our fixed point of origin and the endpoints of both arrows lie.

EXERCISE 3. A subset of a vector subspace is called a **hyperplane** or more precisely a **linear hyperplane** if it is a proper subspace and such that it, together with one single further vector, generates our whole vector space. Show that: a hyperplane together with *any* vector not belonging to the given hyperplane generates all of our original vector space.

DEFINITION 1.4.9. *Let me recall that if X is a set, then the set of all subsets $\mathcal{P}(X) = \{U : U \subseteq X\}$ of X is the so-called* **power set** *of X. I get bewildered talking about sets of sets, so I will say that a subset of $\mathcal{P}(X)$ is a* **system of subsets of** *X. Given such a system $\mathcal{U} \subseteq \mathcal{P}(X)$ we can create two new subsets of X, the* **union** *and the* **intersection** *of the sets of our system $\mathcal{U}$, as follows:*

$$\bigcup_{U\in\mathcal{U}} U = \{x \in X : \text{there is } U \in \mathcal{U} \text{ with } x \in U\}$$
$$\bigcap_{U\in\mathcal{U}} U = \{x \in X : x \in U \text{ for all } U \in \mathcal{U}\}$$

In particular the intersection of the empty system of subsets of X is X, and the union of the empty system of subsets of X is the empty set.

EXERCISE 4. Show that: each intersection of vector subspaces of a vector space is again a vector subspace. Note that this has the following consequence: for a subset T of a vector space V over F the intersection of all vector subspaces of V that contain T is obviously the smallest vector subspace of V that contains T. This provides us with a new proof of Proposition 1.4.5 on the existence of such a smallest subspace. This proof has the advantage that it is easier to generalise.

1.5. Linear Independence and Bases

DEFINITION 1.5.1. *A subset L of a vector space V is called* **linearly independent** *if for all pairwise different vectors $\vec{v}_1, \ldots, \vec{v}_r \in L$ and arbitrary scalars $\alpha_1, \ldots, \alpha_r \in F$,*

$$\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r = \vec{0} \rightarrow \alpha_1 = \cdots = \alpha_r = 0.$$

DEFINITION 1.5.2. *A subset L of a vector space V is called* **linearly dependent** *if it is not linear independent. This means there exist pairwise different vectors $\vec{v}_1, \ldots, \vec{v}_r \in L$ and scalars $\alpha_1, \ldots, \alpha_r \in F$, not all zero, such that $\alpha_1\vec{v}_1 + \cdots \alpha_r\vec{v}_r = \vec{0}$.*

EXAMPLE 1.5.3 (Don't fall asleep!). The empty set is linearly independent in every vector space.

EXAMPLE 1.5.4 (Keep your eyes open!). A one-element subset is linearly independent precisely when it does not comprise the zero vector. There is trouble for the zero vector because of multiplication by the scalar 1, namely $1\cdot\vec{0} = \vec{0}$, and since $1 \neq 0$ in a field we see that a set consisting only of the zero vector is not linearly independent. That every other one-element subset is linear independent follows from Lemma 1.2.4.

EXAMPLE 1.5.5 (Now it's interesting). A two-element subset of a vector space is linearly independent if neither of its vectors is a multiple of the other.

EXAMPLE 1.5.6 (Well, it was). A subset of a vector space is linearly dependent if at least one of its vectors can be written as a linear combination of others remaining. I want you to check you can prove this.

EXAMPLE 1.5.7. If we think about Example 1.3.2 where we had the example of space around us together with a fixed point of origin, we say sloppily that three vectors are linearly independent precisely when "together with the fixed point of origin they do not lie on a plane".

DEFINITION 1.5.8. *A* **basis of a vector space** *of a vector space V is a linearly independent generating set in V.*

EXAMPLE 1.5.9. If we think about Example 1.3.2 where we had the example of space around us together with a fixed point of origin, then a basis is a set with three vectors that, together with the fixed point of origin, do not lie on a plane.

Let A and I be sets. Then I will refer to a mapping $I \to A$ as a **family of elements of A indexed by I** and use the notation

$$(a_i)_{i\in I}.$$

I will use this mainly when the set I plays a secondary role to A. In the case $I = \emptyset$, I will talk about the **empty family** of elements of A.

I have introduced this notation because it is sometimes practical and it sometimes makes for more elegant reading to use families of vectors $(\vec{v}_i)_{i\in I}$ instead of subsets of our vector space. For instance the family $(\vec{v}_i)_{i\in I}$ would be called a generating set if the set $\{\vec{v}_i : i \in I\}$ is a generating set. Similarly it would be called **linearly independent** or pedantically a **linearly independent family** if, for pairwise distinct indices $i(1), \dots, i(r) \in I$ and arbitrary scalars $\alpha_1, \dots, \alpha_r \in F$,

$$\alpha_1\vec{v}_{i(1)} + \cdots + \alpha_r\vec{v}_{i(r)} = \vec{0} \to \alpha_1 = \cdots = \alpha_r = 0.$$

An essential but wee-bit-subtle difference between families and subsets is that the same vector may be represented by different indices in a family, in which case linear independence as a family is not possible. A family of vectors that is not linearly independent is called a **linearly dependent family**. A family of vectors that is a generating set and linearly independent is called either a **basis** or a **basis indexed by** $i \in I$.

We will often later use bases that are indexed by a set $\{1, \dots, n\}$ where $n \in \mathbb{N}$. The essential difference between this and Definition 1.5.8 is that we can then say which basis vector is first, which is second, and so on. In this way, we speak of an **ordered basis**.

EXAMPLE 1.5.10. Let F be a field and $n \in \mathbb{N}$. We consider the following vectors in F^n

$$\vec{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$$

with one 1 in the i-th place and zero everywhere else. Then $\vec{e}_1, \dots, \vec{e}_n$ form an ordered basis of F^n, the so-called **standard basis** of F^n.

THEOREM 1.5.11 (Linear Combinations of Basis Elements). *Let F be a field, V a vector space over F and $\vec{v}_1, \dots, \vec{v}_r \in V$ vectors. The family $(\vec{v}_i)_{1\leqslant i\leqslant r}$ is a basis of V if and only if the following "evaluation" mapping*

$$\begin{aligned} \Phi : F^r &\to V \\ (\alpha_1, \dots, \alpha_r) &\mapsto \alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r \end{aligned}$$

is a bijection.

If we label our ordered family by $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_r)$, then we denote the above mapping by $\Phi = \Phi_{\mathcal{A}} : F^r \to V$.

PROOF. In gory detail, this goes as follows:

$$\begin{aligned} (\vec{v}_i)_{1\leqslant i\leqslant r} \text{ is a generating set} &\Leftrightarrow \Phi \text{ is a surjection } F^r \twoheadrightarrow V \\ (\vec{v}_i)_{1\leqslant i\leqslant r} \text{ is linearly independent} &\Leftrightarrow \Phi \text{ is a injection } F^r \hookrightarrow V \\ (\vec{v}_i)_{1\leqslant i\leqslant r} \text{ is a basis} &\Leftrightarrow \Phi \text{ is a bijection } F^r \xrightarrow{\sim} V \end{aligned}$$

The first equivalence comes directly from the definition of a generating set. To see the implication $\Leftarrow$ of the second equivalence, I observe that Φ sends $(0, \dots, 0)$ to the zero vector and so there cannot

be any other vector in F^r that Φ sends to the zero vector. To see the implication $\Rightarrow$ we argue by contradiction: suppose that Φ were not injective, so that there exists $(\alpha_1, \ldots, \alpha_r) \neq (\beta_1, \ldots, \beta_r)$ with the same image $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r = \beta_1\vec{v}_1 + \cdots + \beta_r\vec{v}_r$ under Φ. Then we would have

$$(\alpha_1 - \beta_1)\vec{v}_1 + \cdots + (\alpha_r - \beta_r)\vec{v}_r = \vec{0}$$

as a non-trivial representation of the zero vector. But this is a linear combination of the $\vec{v}_i$ and so our vectors could not have been linearly independent. The last equivalence is a direct consequence of the first two. □

THEOREM 1.5.12 (Characterisation of Bases). *The following are equivalent for a subset E of a vector space V:*

(1) Our subset E is a basis, i.e. a linearly independent generating set;
(2) Our subset E is minimal among all generating sets, meaning that $E\backslash\{\vec{v}\}$ does not generate V, for any $\vec{v} \in E$;
(3) Our subset E is maximal among all linearly independent subsets, meaning that $E \cup \{\vec{v}\}$ is not linearly independent for any $\vec{v} \in V$.

You must understand the terms minimal and maximal here as referring to inclusion between subsets, not as something to do with the number of elements. In order to emphasise that, although I don't like it, I will also speak of a minimal generating set as an **unshortenable** generating set.

PROOF. (1) $\Leftrightarrow$ (2). We have to show: a generating set is linearly independent if and only if it is minimal. So it is also enough to show: a generating set is linearly dependent if and only if it is not minimal. Now let $E \subseteq V$ be a generating set which is linearly dependent, so that there is a relation $\lambda_1\vec{v}_1 + \cdots + \lambda_r\vec{v}_r = \vec{0}$ with $r \geqslant 1$, the $\vec{v}_i \in E$ pairwise distinct, and some $\lambda_i \neq 0$. Without loss of generality we may take $i = 1$. It follows that

$$\vec{v}_1 = -\lambda_1^{-1}\lambda_2\vec{v}_2 - \ldots - \lambda_1^{-1}\lambda_r\vec{v}_r \in \langle E \setminus \{\vec{v}_1\}\rangle$$

and so $E \setminus \{\vec{v}_1\}$ is also a generating set for V, and hence E is not minimal. Conversely, if E is not minimal, there exists $\vec{v} \in E$ such that $E \setminus \{\vec{v}\}$ is still a generating set. In particular there exists a representation

$$\vec{v} = \lambda_1\vec{v}_1 + \cdots + \lambda_n\vec{v}_n$$

with $n \geqslant 0$ and $\vec{v}_i \in E \setminus \vec{v}$ pairwise distinct. It thus follows that $\vec{v} - \lambda_1\vec{v}_1 - \cdots - \lambda_n\vec{v}_n = 0$ and E is not linearly independent.

(1) $\Leftrightarrow$ (3). We have to show: a linearly independent subset is a generating set if and only if it is maximal. We argue again by contradiction. If $L \subset V$ is linearly independent but not a generating set, then for each $\vec{v} \in V \setminus \langle L\rangle$ we also have that $L \cup \{\vec{v}\}$ is linearly independent and so L was not maximal. Conversely, if L is not maximal then there is a vector $\vec{v}$ such that $L \cup \{\vec{v}\}$ is linearly independent and therefore L cannot be a generating set since this vector $\vec{v}$ can not have been generated. □

If you look carefully, our Theorem 1.5.12 implies in particular that every finitely generated vector space has a finite basis: simply start with a finite generating set, then take vectors away until we have an unshortenable generating set.

COROLLARY 1.5.13 (The existence of a basis). *Let V be a finitely generated vector space over a field F. Then V has a basis.*

PROOF. Let $E = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_r\} \subset V$ be a finite generating set. If it is not linearly independent then

$$\lambda_1\vec{e}_1 + \cdots + \lambda_r\vec{e}_r \ = \ \vec{0} \in V$$

for some $\lambda_i \in F$ which are not all $0 \in F$. Without loss of generality we may assume that $\lambda_1 \neq 0 \in F$, and then the subset $E \setminus \{\vec{e}_1\} = \{\vec{e}_2, \vec{e}_2, \ldots, \vec{e}_r\} \subset V$ is a smaller finite generating set. Proceed in this manner, until you end up with a linearly independent subset of E which generates V – a basis! □

With more sophisticated set theory we can even show the general **Existence-of-a-Basis Theorem**, which states that every vector space has a basis. We'll discuss that in a workshop.

THEOREM 1.5.14 (A useful variant on the Characterisation of Bases). *Let V be a vector space.*

(1) If $L \subset V$ is a linearly independent subset and E is minimal amongst all generating sets of our vector space with the property that $L \subseteq E$, then E is a basis.
(2) If $E \subseteq V$ is a generating set and if L is maximal amongst all linearly independent subsets of vector space with the property $L \subseteq E$, then L is a basis.

PROOF. (1) If E were not a basis, then there would be a non-trivial relation between its vectors $\lambda_1\vec{v}_1 + \cdots + \lambda_r\vec{v}_r = \vec{0}$ with $r \geqslant 1$, the $\vec{v}_i \in E$ pairwise distinct, and all $\lambda_i \neq 0$. Not all the vectors $\vec{v}_i$ could belong to L because L is linearly independent. Thus there is a $\vec{v}_i$ belonging to $E \setminus L$ and it can be written as a linear combination of the other elements of E. But then $E \setminus \{\vec{v}_i\}$ is also a generating set that contains L and so E was not minimal.
(2) If L were not a basis, then L could not be a generating set and so there would necessarily be a vector $\vec{v} \in E$ that didn't lie in the subspace generated by L. If we add that vector to L then we obtain a bigger linearly independent subset contained in E and so L was not maximal. □

DEFINITION 1.5.15 (To infinity, but not beyond). *Let X be a set and F a field. The set $\mathrm{Maps}(X, F)$ of all mappings $f : X \to F$ becomes an F-vector space with the operations of pointwise addition and multiplication by a scalar. The subset of all mappings which send almost all elements of X to zero is a vector subspace*

$$F\langle X\rangle \subseteq \mathrm{Maps}(X, F).$$

This vector subspace is called the **free vector space on the set** X *or pedantically* **the free vector space over** F **on the set** X.

I want to remind you that "almost all" is a technical mathematical abbreviation meaning "all but finitely many". So when I write that almost all elements of X are sent to zero by f, this means that only finitely many elements of X take non-zero values by the mapping f. Of course, this is no condition at all if X itself is a finite set, but if X is infinite then it is a severe restriction.

We call $a \in F\langle X\rangle$ a "formal linear combination of elements from X" and instead of writing it as $(a_x)_{x\in X}$ I will use the more suggestive $\sum_{x\in X} a_x x$. For instance if $X = \{\heartsuit, \sharp, \bigstar\}$ then a typical element of $\mathbb{Q}\langle X\rangle$ is

$$\frac{14}{23}\heartsuit + 7\sharp - \frac{66}{5}\bigstar.$$

THEOREM 1.5.16 (A useful variant on Linear Combinations of Basis Elements). *Let F be a field, V an F-vector space and $(\vec{v}_i)_{i\in I}$ a family of vectors from the vector space V. The following are equivalent:*

(1) The family $(\vec{v}_i)_{i\in I}$ is a basis for V;
(2) For each vector $\vec{v} \in V$ there is precisely one family $(a_i)_{i\in I}$ of elements of our field F, almost all of which are zero and such that

$$\vec{v} = \sum_{i\in I} a_i\vec{v}_i.$$

PROOF. I use the notation $F\langle X\rangle$ to reformulate the theorem as follows: given an F-vector space V, a family $(\vec{v}_i)_{i\in I}$ of vectors is a basis if and only if the "evaluation" mapping

$$\begin{array}{rcl}\Phi : F\langle I\rangle & \to & V \\ (a_i)_{i\in I} & \mapsto & \displaystyle\sum_{i\in I} a_i\vec{v}_i\end{array}$$

is a bijection between the free vector space $F\langle I\rangle$ on the set I and the given vector space V.

In gory detail, this goes as follows:

$$\begin{aligned}(\vec{v}_i)_{i\in I} \text{ is a generating set} &\Leftrightarrow \Phi \text{ is a surjection } F\langle I\rangle \twoheadrightarrow V \\ (\vec{v}_i)_{i\in I} \text{ is linearly independent} &\Leftrightarrow \Phi \text{ is a injection } F\langle I\rangle \hookrightarrow V \\ (\vec{v}_i)_{i\in I} \text{ is a basis} &\Leftrightarrow \Phi \text{ is a bijection } F\langle I\rangle \xrightarrow{\sim} V\end{aligned}$$

The proof of these statements follows the proof of Theorem 1.5.11 word-for-word. □

1.6. Dimension of a Vector Space

THEOREM 1.6.1 (Fundamental Estimate of Linear Algebra). *No linearly independent subset of a given vector space has more elements than a generating set. Thus if V is a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set, then:*

$$|L| \leqslant |E|$$

The "Fundamental Estimate of Linear Algebra" is a thunderous title for such an obviously obvious theorem. In my statement of it, I am using the convention that for any infinite set X I simply set $|X| = \infty$. Then the theorem has content for finitely generated vector spaces only. But, with a more refined interpretation of $|X|$ as the cardinality of a set, it is still true.

PROOF. By contradiction. Let F be our ground field. Let's assume that we have a generating set $E = \{\vec{w}_1, \ldots, \vec{w}_m\}$ and a linearly independent subset $L = \{\vec{v}_1, \ldots, \vec{v}_n\}$ with $n > m$. By definition we can find $a_{ij} \in F$ with

$$\begin{array}{ccccc}\vec{v}_1 & = & a_{11}\vec{w}_1 + a_{21}\vec{w}_2 + \cdots + a_{m1}\vec{w}_m \\ \vdots & & \vdots \quad\quad \vdots & & \vdots \\ \vec{v}_n & = & a_{1n}\vec{w}_1 + a_{2n}\vec{w}_2 + \cdots + a_{mn}\vec{w}_m\end{array}$$

Now take from this the "vertically written" homogeneous system of linear equations

$$\begin{array}{ccccc}x_1a_{11} & x_1a_{21} & \cdots & x_1a_{m1} \\ + & + & & + \\ \vdots & \vdots & \cdots & \vdots \\ + & + & & + \\ x_na_{1n} & x_na_{2n} & \cdots & x_na_{mn} \\ = & = & & = \\ 0 & 0 & \cdots & 0\end{array}$$

In its usual form this looks like:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

This system of linear equations has fewer equations than unknowns, so Gaussian elimination shows that there is at least one non-zero solution $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. Then, for each such solution

$$x_1\vec{v}_1 + \cdots + x_n\vec{v}_n = \vec{0},$$

which contradicts the linear independence of the $\vec{v}_i$. □

A consequence of the Fundamental Estimate is the following theorem, which develops the statement of the Fundamental Estimate.

THEOREM 1.6.2 (Steinitz Exchange Theorem). *Let V be a vector space, $L \subset V$ a finite linearly independent subset and $E \subseteq V$ a generating set. Then there is an injection $\phi : L \hookrightarrow E$ such that $(E \setminus \phi(L)) \cup L$ is also a generating set for V.*

In other words, we can swap some elements of a generating set by the elements of our linearly independent set, and still keep a generating set. With more sophisticated methods from set theory, this theorem holds without the finiteness restriction on L.

PROOF. This follows by induction from the Exchange Lemma below: it lets us swap elements from E with elements from L, one-by-one. □

LEMMA 1.6.3 (Exchange Lemma). *Let V be a vector space, $M \subseteq V$ a linearly independent subset, and $E \subseteq V$ a generating subset, such that $M \subseteq E$. If $\vec{w} \in V \setminus M$ is a vector not belonging to M such that $M \cup \{\vec{w}\}$ is linearly independent, then there exists $\vec{e} \in E \setminus M$ such that $\{E \setminus \{\vec{e}\}\} \cup \{\vec{w}\}$ is a generating set for V.*

PROOF. Since E is a generating set for V, we can write $\vec{w}$ as a linear combination of vectors from E,

$$\vec{w} = \lambda_1\vec{e}_1 + \cdots + \lambda_r\vec{e}_r \ \ (\lambda_i \in F)$$

with pairwise distinct $\vec{e}_i \in E$ and all $\lambda_i \neq 0$. (The subset $\{\vec{e}_1, \ldots, \vec{e}_r\} \subseteq E$ depends on $\vec{w}$). Since $M \cup \{\vec{w}\}$ is linearly independent, it cannot be that all $\vec{e}_i$ belong to M. Without loss of generality we may then assume that $\vec{e}_1 \notin M$. Now we write the above identity as

$$\vec{e}_1 = \lambda_1^{-1}(\vec{w} - \lambda_2\vec{e}_2 - \cdots - \lambda_r\vec{e}_r)$$

from which we see that $(E \setminus \{\vec{e}_1\}) \cup \{\vec{w}\}$ is a generating set. □

COROLLARY 1.6.4 (Cardinality of Bases). *Let V be a finitely generated vector space.*

(1) V has a finite basis.
(2) V cannot have an infinite basis.
(3) Any two bases of V have the same number of elements.

PROOF. (1) This is Corollary 1.5.13.
(2) If V has a finite basis with r elements and an infinite basis then a subset of the infinite basis with $r+1$ elements would be linearly independent and $r + 1 \leqslant r$ by the Fundamental Estimate of Linear Algebra 1.6.1 – a contradiction!
(3) Suppose that B_1 and B_2 are two finite bases for V. Since B_1 is linearly independent and B_2

generates $|B_1| \leqslant |B_2|$ by the Fundamental Estimate of Linear Algebra 1.6.1. Similarly, since B_2 is linearly independent and B_1 generates, $|B_2| \leqslant |B_1|$. Hence $|B_1| = |B_2|$. □

With more sophisticated methods from set theory, we can remove the restriction to finitely generated vector spaces: for any two bases of a vector space there exists a bijection between one and the other.

DEFINITION 1.6.5. *The cardinality of one (and by Corollary 1.6.4 each) basis of a finitely generated vector space V is called the* **dimension** *of V and will be denoted by $\dim V$. If F is a field, and we want to denote that we mean dimension as an F-vector space, then we will write $\dim_F V$. If the vector space is not finitely generated, then we write $\dim V = \infty$ and call V* **infinite dimensional**. *As usual, we will ignore the difference between different infinities.*

REMARK 1.6.6. In Physics, sadly, the term "Dimensions" has a completely different use: physical dimensions are things like length, time, mass, frequency, and so on. In our use these all model "one-dimensional real vector spaces". I hope that you, dear Reader, use context to determine which notion of dimension is meant at any one time.

EXAMPLE 1.6.7. The zero vector space has as its basis the empty set. Its dimension therefore is zero. In general, thanks to Example 1.5.10, we have

$$\dim_F F^n = n.$$

COROLLARY 1.6.8 (Cardinality Criterion for Bases). *Let V be a finitely generated vector space.*

(1) Each linearly independent subset $L \subset V$ has at most $\dim V$ elements, and if $|L| = \dim V$ then L is actually a basis;
(2) Each generating set $E \subseteq V$ has at least $\dim V$ elements, and if $|E| = \dim V$ then E is actually a basis.

PROOF. Following Theorem 1.6.1 for L a linearly independent subset, B a basis and E a generating set, we have

$$|L| \leqslant |B| \leqslant |E|.$$

Since there is a finite generating set, if $|L| = |B|$ then it must be that $|L|$ is a maximal linearly independent subset, and so a basis by Theorem 1.5.12. If $|B| = |E|$ then E must be a minimal generating set and so by Theorem 1.5.12 a basis. □

COROLLARY 1.6.9 (Dimension Estimate for Vector Subspaces). *A proper vector subspace of a finite dimensional vector space has itself a strictly smaller dimension.*

REMARK 1.6.10. If $U \subseteq V$ is a vector subspace of an arbitrary vector space, then we have $\dim U \leqslant \dim V$ and if we have $\dim U = \dim V < \infty$ then it follows that $U = V$.

PROOF. Since V is finite dimensional, it is finitely generated and so, thanks to Corollary 1.6.8, U contains a maximal linearly independent subset and each such subset must have at most $\dim V$ elements. By Theorem 1.5.12 each such subset is a basis of U and so this shows that $\dim U \leqslant \dim V$. If this were an equality, then since V is finite dimensional it would mean by Corollary 1.6.8 that each basis of U was also a basis of B, showing that $U = V$. □

EXERCISE 5. Show that each one dimensional vector space has exactly two vector subspaces.

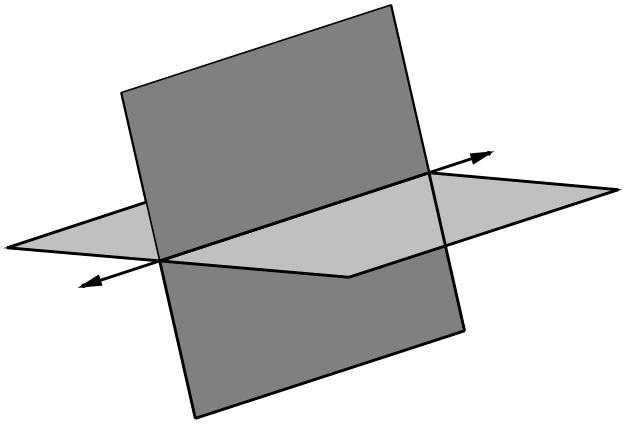
If V is a vector space and U, W are subspaces of V, then we define $U + W$ to be the subspace $\langle U \cup W \rangle$ of V generated by U and W together.

THEOREM 1.6.11 (The Dimension Theorem). *Let V be a vector space containing vector subspaces $U, W \subseteq V$. Then*

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W.$$

In 1.8.5 we'll prove this theorem again as a corollary of the Rank-Nullity Theorem for linear mappings.

EXAMPLE 1.6.12. If we think about Example 1.3.2 of space around us with a fixed point of origin, then the two-dimensional vector subspaces are the planes that pass through our fixed point of origin. Given a two distinct two-dimensional vector spaces U, W, their sum spans the whole space so that $\dim(U + W) = 3$. Now two distinct planes passing through the same fixed point of origin obviously meet in a straight line, and that confirms the statement of the above theorem, which in this case then states $3 + 1 = 2 + 2$.



PROOF. If either of U or W are infinite dimensional, then the statement is clear. Otherwise, choose a basis $s_1, \ldots, s_d$ of $U \cap W$ and extend it by the elements $u_1, \ldots, u_r \in U$ to a basis of U and then by the elements $w_1, \ldots, w_t \in W$ to a basis of $U + W$. We'll have won if we can show that $s_1, \ldots, s_d, w_1, \ldots, w_t$ is a basis of W. Since this subset is linearly independent by construction, we only need to show that it generates W. We can definitely write $w \in W$ as a linear combination

$$\begin{aligned} w =& \lambda_1 u_1 + \cdots + \lambda_r u_r \\ &+ \mu_1 s_1 + \cdots + \mu_d s_d \\ &+ \nu_1 w_1 + \cdots + \nu_t w_t \end{aligned}$$

From this it is clear that $\lambda_1 u_1 + \cdots + \lambda_r u_r \in W \cap U$ and so we can write this element as a linear combination of the s_i. It follows then that w is itself a linear combination of the s_i and the w_j, which is what we wanted to show. □

EXERCISE 6. Given F-vector spaces $V_1, \ldots, V_n$ show that: the dimension of their cartesian product, in the sense of Section 1.3, is given by

$$\dim(V_1 \oplus \cdots \oplus V_n) = \dim(V_1) + \cdots + \dim(V_n).$$

EXERCISE 7. Recall that $\mathbb{R} \subset \mathbb{C}$. Thus we can think of any $\mathbb{C}$-vector space as a vector space over $\mathbb{R}$. Show that: $\dim_{\mathbb{R}} V = 2 \dim_{\mathbb{C}} V$

1.7. Linear Mappings

DEFINITION 1.7.1. *Let V, W be vector spaces over a field F. A mapping $f : V \to W$ is called* **linear** *or more precisely F-***linear** *or even a* **homomorphism of F-vector spaces** *if for all $\vec{v}_1, \vec{v}_2 \in V$ and $\lambda \in F$*

we have

$$f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$$
$$f(\lambda\vec{v}_1) = \lambda f(\vec{v}_1)$$

A bijective linear mapping is called an **isomorphism** *of vector spaces. If there is an isomorphism between two vector spaces, we call them* **isomorphic**. *A homomorphism from one vector space to itself is called an* **endomorphism** *of our vector space. An isomorphism of a vector space to itself is called an* **automorphism** *of our vector space.*

ETYMOLOGY. This terminology "homomorphism" comes from the Greek "μορφη" for "form, shape" and the Greek " ὁμο " for "same, similar". Then "isomorphism" arises from the Greek "ἴσο" for "equal". The word "endomorphism" comes from the Greek "ἔνδον" for "within, inside", while "automorphism" comes from "αὐτός" for "self". The word "linear" for a mapping seems to come from the case of an $\mathbb{R}$-linear mapping $f : \mathbb{R} \to \mathbb{R}$ whose graph must be a straight line. But it's a little annoying, because the functions $f : \mathbb{R} \to \mathbb{R}, x \mapsto ax + b$ are all straight lines, but they are only linear in our sense in the case $b = 0$. Maybe in your past you called them linear when $b \neq 0$, but now you will not; those ones are "affine".

EXAMPLE 1.7.2. (i) The projections $\mathsf{pr}_i : F^n \to F; (\lambda_1, \lambda_2, \ldots, \lambda_n) \mapsto \lambda_i$ are linear.
(ii) The squaring function $F \to F; \lambda \mapsto \lambda^2$ is not linear, unless $2 = 0 \in F$, e.g. if $F = \mathbb{F}_2 = \{0, 1\}$ is the field with two elements.

EXAMPLE 1.7.3. Given vector spaces V, W, the projection mappings $\mathsf{pr}_V : (V \oplus W) \to V$ and $\mathsf{pr}_W : (V \oplus W) \to W$ are linear. The same holds for more general projections $\mathsf{pr}_i : V_1 \oplus \cdots \oplus V_n \to V_i$. Furthermore the **canonical injections** $\mathsf{in}_V : V \to (V \oplus W), v \mapsto (v, 0)$ and $\mathsf{in}_W : W \to (V \oplus W), w \mapsto (0, w)$ are linear and again the same holds with more summands for the analogously defined $\mathsf{in}_i : V_i \to V_1 \oplus \cdots \oplus V_n$.

EXAMPLE 1.7.4. The map Φ from Theorem 1.5.11 is an isomorphism.

EXERCISE 8. Every composition of a vector space homomorphisms is again a vector space homomorphism. In other words if $f : V \to W$ and $g : U \to V$ are linear mappings, then so too is $f \circ g : U \to W$.

EXERCISE 9. Show that: If $f : V \to W$ is a vector space isomorphism, then the inverse mapping $f^{-1} : W \to V$ is also a vector space isomorphism. In particular, the automorphisms of a vector space V form a subgroup of its permutation group. This group is called the **general linear group** or the **automorphism group** of our vector space V and is denoted by

$$\mathrm{GL}(V) = \mathrm{Aut}(V) \subseteq \mathrm{Maps}^\times(V, V).$$

If I want to draw attention to the ground field, I will write $\mathrm{Aut}_F(V)$. These groups are amongst my all-time personal favourites.

EXERCISE 10. Show that: the image of a vector subspace under a linear mapping is again a vector subspace, and that the preimage of a vector subspace under a linear mapping is again a vector subspace.

DEFINITION 1.7.5. *A point that is sent to itself by a mapping is called a* **fixed point** *of the mapping. Given a mapping $f : X \to X$, we denote the set of fixed points by*

$$X^f = \{x \in X : f(x) = x\}.$$

EXERCISE 11. Let V be a vector space and $f \in \mathrm{End}(V)$ an endomorphism. Show that: the fixed point set $V^f \subseteq V$ is a vector subspace.

EXERCISE 12 (Homomorphisms from direct sums). Show that: given vector spaces $V_1, \ldots, V_n, W$ and linear mappings $f_i : V_i \to W$ then we can form a new linear mapping $f : V_1 \oplus \cdots \oplus V_n \to W$ by the recipe $f(v_1, \ldots, v_n) = f_1(v_1) + \cdots + f_n(v_n)$. In this way we even get a bijection

$$\mathrm{Hom}(V_1, W) \times \cdots \times \mathrm{Hom}(V_n, W) \xrightarrow{\sim} \mathrm{Hom}(V_1 \oplus \cdots \oplus V_n, W)$$

whose inverse can be written as $f \mapsto (f \circ \mathsf{in}_1, f \circ \mathsf{in}_2, \ldots, f \circ \mathsf{in}_n)$.

EXERCISE 13 (Homomorphisms for products). Show that: given vector spaces $V, W_1, \ldots, W_n$ and linear mappings $g_i : V \to W_i$ then we can form a new linear mapping $g : V \to W_1 \oplus \cdots \oplus W_n$ by the recipe $g(v) = (g_1(v), \ldots, g_n(v))$. In this way we even get a bijection

$$\mathrm{Hom}(V, W_1) \times \cdots \times \mathrm{Hom}(V, W_n) \xrightarrow{\sim} \mathrm{Hom}(V, W_1 \oplus \cdots \oplus W_n)$$

whose inverse can be written as $g \mapsto (\mathsf{pr}_i \circ g)_i$.

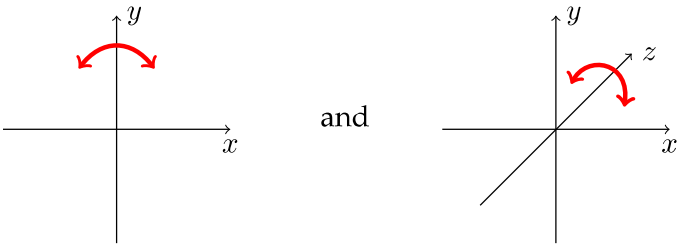
DEFINITION 1.7.6. *Two vector subspaces V_1, V_2 of a vector space V are called* **complementary** *if addition defines a bijection*

$$V_1 \times V_2 \xrightarrow{\sim} V.$$

Taking $W = V$ in Exercise 12, we then produce an vector space isomorphism $V_1 \oplus V_2 \xrightarrow{\sim} V$. We abuse notation a little by writing $V = V_1 \oplus V_2$ and say that the vector space V is the **direct sum**, *or more precisely the* **internal direct sum** *of the vector subspaces V_1 and V_2.*

Let V be a vector space with vector subspaces $V_1, \ldots, V_n$. Then the vector subspace of V they generate is called the **sum** of our vector subspaces and denoted by $V_1 + \cdots + V_n$. This generalises the sum defined just before Theorem 1.6.11. If the natural homomorphism given by addition $V_1 + \cdots + V_n \to V$ is an injection then we say the **the sum of the vector subspaces V_i is direct** and we write their sum also as $V_1 \oplus \cdots \oplus V_n$.

EXERCISE 14. How many vector subspaces are there in $\mathbb{R}^2$ that are sent to themselves under the reflection $(x, y) \mapsto (x, -y)$? Which vector subspaces in $\mathbb{R}^3$ are sent to themselves by the reflection $(x, y, z) \mapsto (x, y, -z)$?



THEOREM 1.7.7 (The Classification of Vector Spaces by their Dimension). *Let n be a natural number. Then a vector space over a field F is isomorphic to F^n if and only if it has dimension n.*

PROOF. It's easy to check that a surjective homomorphism sends a generating set to a generating set and that an injective homomorphism sends a linearly independent subset to a linearly independent subset. So a vector space isomorphism sends a basis to a basis. Thus if two vector spaces are isomorphic then they have the same dimension. Conversely, if a vector space V has an ordered basis $B = (\vec{v}_1, \ldots, \vec{v}_n)$ consisting of n vectors, then the mapping $(\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1\vec{v}_1 + \cdots + \lambda_n\vec{v}_n$ of Theorem 1.5.11 produces a vector space isomorphism $F^n \xrightarrow{\sim} V$. □

Now we are in a position to solve the problem raised at the end Section 1.1: is the "number of free parameters" in our representation of the solution set of a system of linear equations well-defined, or more precisely whether the number of stairs appearing in Gaussian elimination does not depend on the enumeration of the variables, i.e. on the ordering of the columns. Now if we

can show this for homogeneous systems then it obviously follows for arbitrary systems. As we already pointed out in Example 1.4.3 the solution set $L \subseteq F^m$ of a homogeneous system is a vector subspace of F^m. We obtain a vector space isomorphism $L \xrightarrow{\sim} F^{m-r}$ by "removing all entries where a stair begins", in other words by omitting $x_{s(1)}, x_{s(2)}, \ldots, x_{s(r)}$ from our m-tuple $(x_1, \ldots, x_m) \in L$. Here r is the number of stairs. Hence we see that it has an independent description via the dimension of the solution set, namely $r = m - \dim_F L$.

Let V, W be vector spaces over a field F. The set of all homomorphisms from V to W is denoted by

$$\mathrm{Hom}_F(V, W) = \mathrm{Hom}(V, W) \subseteq \mathrm{Maps}(V, W).$$

LEMMA 1.7.8 (Linear mappings and bases). *Let V, W be vector spaces over F and let $B \subset V$ be a basis. Then restriction of a mapping gives a bijection*

$$\begin{array}{ccc} \mathrm{Hom}_F(V, W) & \xrightarrow{\sim} & \mathrm{Maps}(B, W) \\ f & \mapsto & f|_B. \end{array}$$

In other words each linear mapping determines and is completely determined by the values it takes on a basis.

PROOF. Let $f, g : V \to W$ be linear. If $f(\vec{v}) = g(\vec{v})$ for all $\vec{v} \in B$ then it follows by linearity that $f(\lambda_1\vec{v}_1 + \cdots + \lambda_r\vec{v}_r) = g(\lambda_1\vec{v}_1 + \cdots + \lambda_r\vec{v}_r)$ for all $\lambda_1, \ldots, \lambda_r \in F$ and $\vec{v}_1, \ldots, \vec{v}_r \in B$. Thus $f(\vec{v}) = g(\vec{v})$ for all $\vec{v}$ in the linear span of B, in other words for all $\vec{v} \in V$. This proves the injectivity of the restriction mapping $\mathrm{Hom}_k(V, W) \to \mathrm{Maps}(B, W)$ when B is any generating set for V. Now suppose conversely that we have a mapping of sets $g : B \to W$. We extend it to a linear mapping $\tilde{g} : V \to W$ as follows: each vector $\vec{v} \in V$ may be written thanks to Theorem 1.5.16 uniquely as a linear combination of basis vectors, $\vec{v} = \lambda_1\vec{v}_1 + \cdots + \lambda_r\vec{v}_r$ with pairwise different $\vec{v}_i \in B$. Now simply set

$$\tilde{g}(\vec{v}) = \lambda_1 g(\vec{v}_1) + \cdots + \lambda_r g(\vec{v}_r).$$

This produces the linear extension of g we were seeking. □

EXERCISE 15. Let V, W be vector spaces over a field F. Show that $\mathrm{Hom}_F(V, W)$ is a vector subspace of the set of all mappings $\mathrm{Maps}(V, W)$ from V to W with its vector space structure given similarly to Definition 1.5.15. Show that:

$$\dim \mathrm{Hom}_F(V, W) = (\dim V)(\dim W),$$

where I am using the convention $0 \cdot \infty = \infty \cdot 0 = 0$. In fact, it is possible to make a more sophisticated version of this equality using the relationship with cardinality given by Lemma 1.7.8.

EXERCISE 16. Let V be a finite dimensional vector space, and let U be a proper vector subspace. Show that: there exists at least one (and in fact many different) vector subspace(s) of V complementary to U. If you're brave, try to do this also for not necessarily finite dimensional vector spaces.

PROPOSITION 1.7.9. *(1) Every injective linear mapping $f : V \hookrightarrow W$ has a* **left inverse**, *in other words a linear mapping $g : W \to V$ such that $g \circ f = \mathrm{id}_V$.*
(2) Every surjective linear mapping $f : V \twoheadrightarrow W$ has a **right inverse**, *in other words a linear mapping $g : W \to V$ such that $f \circ g = \mathrm{id}_W$.*

I will give the proof for finite dimensional vector spaces V, W. The general case will follow by the same argument, but as usual you need a little more from set theory.

PROOF. (1) By Exercise 16, we may choose a complement $U \subseteq W$ to the subspace $f(V)$ of W. We then define $g : W \to V$ by the rule $g(u + f(v)) = v$ for all $u \in U, v \in V$. This is well-defined, since U and $f(V)$ are complementary and so the mapping $U \times V \to W, (u, v) \mapsto u + f(v)$ is an isomorphism.

(2) Choose a basis $B \subset W$. Then since f is surjective we can define a mapping of sets $\tilde{g} : B \to V$ such that $f(\tilde{g}(b)) = b$ for all $b \in B$. Now let $g : W \to V$ be the unique linear mapping which satisfies $g(b) = \tilde{g}(b)$, whose existence follows from Lemma 1.7.8. It follows that $f(g(b)) = b$ for all $b \in B$ and therefore $f(g(w)) = w$ for all $w \in W$. □

EXERCISE 17. Show that: each linear mapping from a vector subspace U of a vector space V to another vector space W, $f : U \to W$, can be extended to a linear mapping $\tilde{f} : V \to W$ on the whole vector space V.

1.8. Rank-Nullity Theorem

DEFINITION 1.8.1. *The* **image** *of a linear mapping $f : V \to W$ is the subset $\mathrm{im}(f) = f(V) \subseteq W$. It is a vector subspace of W by Exercise 10. The preimage of the zero vector of a linear mapping $f : V \to W$ is denoted by*

$$\ker(f) := f^{-1}(0) = \{v \in V : f(v) = 0\}$$

and is called the **kernel** *of the linear mapping f. The kernel is a vector subspace of V by Exercise 10.*

LEMMA 1.8.2. *A linear mapping $f : V \to W$ is injective if and only if its kernel is zero.*

REMARK 1.8.3. Of course, you already know this result from Y2 Fundamentals of Pure Mathematics.

PROOF. If any element other than the zero vector of V is in the kernel of f, then f would send it to the zero vector of W and hence f would not be injective. Conversely if the mapping f is not injective, then there exist $v_1 \neq v_2$ in V with $f(v_1) = f(v_2)$. It follows that $v_1 - v_2 \neq 0$ but $f(v_1 - v_2) = 0$. Thus $v_1 - v_2 \in \ker(f)$ is different from zero, so the kernel is not zero. □

THEOREM 1.8.4 (Rank-Nullity Theorem). *Let $f : V \to W$ be a linear mapping between vector spaces. Then:*

$$\dim V = \dim(\ker f) + \dim(\mathrm{im}\, f).$$

This is called the "Rank-Nullity Theorem" because it is common to call the dimension of $\mathrm{im}\, f$ the **rank** of f, and the dimension of $\ker f$ the **nullity** of f.

PROOF. If V is finitely generated then so too is $\mathrm{im}\, f$, since the image $f(E)$ of a generating set $E \subset V$ is a generating set for $f(V) = \mathrm{im}\, f$. Furthermore $\ker f$ is also finitely generated thanks to Corollary 1.6.9, since it is a subspace of V. Thus if $\dim(\ker f) = \infty$ or $\dim(\mathrm{im}\, f) = \infty$ then we deduce that $\dim V = \infty$ and the theorem is proved in those two cases. Thus we may assume that both $\ker f$ and $\mathrm{im}\, f$ are finite dimensional.

Let A be a basis of the kernel of f, B a basis of the image of f, and $g : B \hookrightarrow V$ a choice of preimage of our basis of the image, so that $(f \circ g)(b) = b$ for all $b \in B$. I will show that $g(B) \cup A$ is a basis of V: For $\vec{v} \in V$ we can write $f(\vec{v}) = \lambda_1 \vec{w}_1 + \cdots + \lambda_r \vec{w}_r$ with $\vec{w}_i \in B$. Obviously, the element $\vec{v} - \lambda_1 g(\vec{w}_1) - \cdots - \lambda_r g(\vec{w}_r)$ belongs to the kernel of f, and so it follows that $g(B) \cup A$ generates all of V. In order to show that $g(B) \cup A$ is linearly independent, assume that

$$\lambda_1 g(\vec{w}_1) + \cdots + \lambda_r g(\vec{w}_r) + \mu_1 \vec{v}_1 + \cdots + \mu_s \vec{v}_s = \vec{0}$$

where the $\vec{v}_i \in A$ and $\vec{w}_j \in B$ are pairwise distinct. On applying f to this we deduce that $\lambda_1 \vec{w}_1 + \cdots + \lambda_r \vec{w}_r = \vec{0}$ and so $\lambda_1 = \cdots = \lambda_r = 0$ since the $\vec{w}_j$ are linearly independent. Putting this

information back in to the displayed equation shows $\mu_1 = \cdots = \mu_s = 0$ because of the linear independence of the vectors $\vec{v}_i$.

The theorem follows since $|g(B) \cup A| = |B| + |A|$.

□

COROLLARY 1.8.5 (The Dimension Theorem, again). *Let V be a vector space, and $U, W \subseteq V$ vector subspaces. Then*

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W.$$

I already proved this on-the-hoof in Theorem 1.6.11; with the Rank-Nullity Theorem Theorem 1.8.4 I can give an alternative proof.

PROOF. Consider the linear mapping

$$f : U \oplus W \to V$$

given by $f(u, w) = u + w$, so that $(\operatorname{im} f) = U + W$ and so that the mapping $k \mapsto (k, -k)$ defines an isomorphism $(U \cap W) \xrightarrow{\sim} \ker f$. Then the formula in Exercise 6 for the dimension of a direct sum, together with the Rank-Nullity Theorem give

$$\dim U + \dim W = \dim(U \oplus W) = \dim(U \cap W) + \dim(U + W).$$

□

EXERCISE 18. Let $f : V \to W$ be a linear mapping. Show that: if $\vec{v}_1, \ldots, \vec{v}_s$ is a basis of the kernel $\ker f$ and $\vec{v}_{s+1}, \ldots, \vec{v}_n$ an extension to a linearly independent subset of V, then the family $f(\vec{v}_{s+1}), \ldots, f(\vec{v}_n)$ is linearly independent in W. If the extension is moreover a basis of V, then show that $(f(\vec{v}_i))_{s+1 \leqslant i \leqslant n}$ is a basis of the image of f. Use this to deduce another proof of the Rank-Nullity Theorem in the finite dimensional case.

EXERCISE 19. Show that: two subspaces U, W of a vector space V are complementary if and only if $V = U + W$ and $U \cap W = 0$.

EXERCISE 20. Show that: two subspaces U, W of a finite dimensional vector space V are complementary if and only if $V = U + W$ and $\dim U + \dim W \leqslant \dim V$.

EXERCISE 21. Show that: the kernel of a non-zero linear mapping $V \to F$ is a hyperplane, in the sense of Exercise 3.

EXERCISE 22. Let $\phi : V \to V$ be an endomorphism of a finite dimensional vector space V. Show that $\ker(\phi \circ \phi) = \ker \phi$ is equivalent to $V = \ker \phi \oplus \operatorname{im} \phi$.

EXERCISE 23. An element f of a set with composition or product is called an **idempotent** if $f^2 = f$. (Here I've written f^2 for $f \circ f$.) An example of a set with composition is $\operatorname{End}(V)$, the set of endomorphisms of a finite dimensional vector space V. By Exercise 22 the idempotent endomorphisms of V correspond uniquely to decompositions of V into a direct sum of two complementary subspaces. Show that: the mapping $f \mapsto (\operatorname{im} f, \ker f)$ affords a bijection

$$\{f \in \operatorname{End} V : f^2 = f\} \xrightarrow{\sim} \left\{(I, K) \in \mathcal{P}(V)^2 : I, K \subseteq V \text{ are vector subspaces with } I \oplus K = V\right\}.$$

The inverse of this bijection associates to the decomposition $V = I \oplus K$ the **projection of V onto I along K**.

CHAPTER 2

Linear Mappings and Matrices

2.1. Linear Mappings $F^m \to F^n$ and Matrices

THEOREM 2.1.1 (Linear mappings $F^m \to F^n$ and Matrices). *Let F be a field and let $m, n \in \mathbb{N}$ be natural numbers. There is a bijection between the space of linear mappings $F^m \to F^n$ and the set of matrices with n rows and m columns and entries in F:*

$$\begin{array}{rcl} \mathsf{M} : \mathrm{Hom}_F(F^m, F^n) & \xrightarrow{\sim} & \mathsf{Mat}(n \times m; F) \\ f & \mapsto & [f]. \end{array}$$

This attaches to each linear mapping f its **representing matrix** $\mathsf{M}(f) := [f]$. *The columns of this matrix are the images under f of the standard basis elements of F^m (Example 1.5.10):*

$$[f] := (f(\vec{e}_1)|f(\vec{e}_2)|\cdots|f(\vec{e}_m)).$$

PROOF. This is immediate from Lemma 1.7.8 which, in this case, shows that every linear mapping $f : F^m \to F^n$ determines and is completely determined by its restriction to the basis $(\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_m)$. □

EXERCISE 24. Show that: the mapping M from Theorem 2.1.1 is even an isomorphism of vector spaces, where we use the vector space structures defined in Exercise 15 for linear mappings and Exercise 1 for matrices.

EXAMPLE 2.1.2. The representing matrix of the identity mapping on F^m is the **Identity Matrix**

$$I = I_m := [\mathrm{id}_{F^m}] = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix}$$

whose entries are $I_{i,j} = \delta_{i,j}$, where $\delta_{i,j}$ is the **Kronecker delta** and is defined generally by

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

EXAMPLE 2.1.3. When $m \geqslant n$ the matrix representing the mapping which "forgets the extra coordinates" $f : F^m \to F^n, (x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_n)$ is

$$[f] = \begin{pmatrix} 1 & & 0 & & 0 \cdots 0 \\ & \ddots & & & \\ & & \ddots & & \\ 0 & & & 1 & 0 \ldots 0 \end{pmatrix}$$

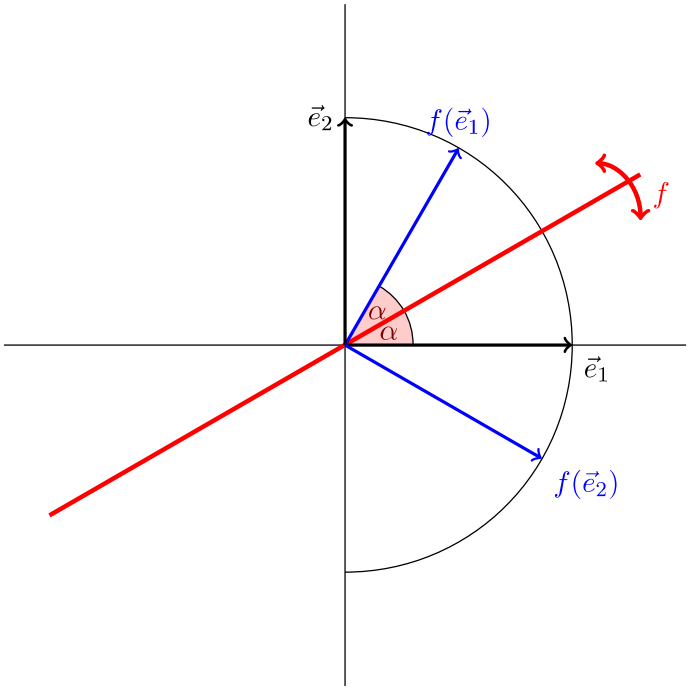
EXAMPLE 2.1.4. The matrix that represents "permuting the coordinates" $g : F^2 \to F^2, (x, y) \mapsto (y, x)$ is:

$$[g] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

EXAMPLE 2.1.5. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be reflection about the straight line making an angle α with the x-axis. Then

$$[f] = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

Indeed this is obvious from the diagram, because for instance $f(\vec{e}_1) = (\cos 2\alpha)\vec{e}_1 + \sin 2\alpha \vec{e}_2$.



DEFINITION 2.1.6. *Let $n, m, \ell \in \mathbb{N}$, F a field, and let $A \in \mathsf{Mat}(n \times m; F)$ and $B \in \mathsf{Mat}(m \times \ell; F)$ be matrices. The* **product** *$A \circ B = AB \in \mathsf{Mat}(n \times \ell; F)$ is the matrix defined by*

$$(AB)_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$$

where the entry in the matrix product AB in the i-th row and the k-th column is calculated from the entries of the matrices A and B. Specifically, for each j from 1 to m multiply the j-th entry of the i-th row of A by the j-th entry of the k-th column of B, sum all of these m products together, and voila, this is the entry of the product AB in the i-th row and k-th column. Matrix multiplication produces a mapping

$$\begin{array}{rcl} \mathsf{Mat}(n \times m; F) \times \mathsf{Mat}(m \times \ell; F) & \to & \mathsf{Mat}(n \times \ell; F) \\ (A, B) & \mapsto & AB \end{array}$$

EXAMPLE 2.1.7. Here is the product of two matrices. The entries in green in the second row of the first matrix and the third column of the second matrix are used to produce the green entry in the second row and third column on the right: $3 \times 3 + 4 \times 3 = 21$.

$$\begin{pmatrix} 1 & 2 \\ \mathbf{3} & \mathbf{4} \\ 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 0 & 2 & \mathbf{3} & 1 \\ 1 & 7 & \mathbf{3} & 4 \end{pmatrix} = \begin{pmatrix} 2 & 16 & 9 & 9 \\ 4 & 34 & \mathbf{21} & 19 \\ 6 & 52 & 33 & 29 \end{pmatrix}$$

At first sight the product of two matrices appears simply to be nuts. But the notation $AB = A \circ B$, combined with the connection to composition of mappings presented in Theorem 2.1.1 explains it.

THEOREM 2.1.8 (Composition of Linear Mappings and Products of Matrices). *Let $g : F^\ell \to F^m$ and $f : F^m \to F^n$ be linear mappings. The representing matrix of their composition is the product of their representing matrices:*

$$[f \circ g] = [f] \circ [g].$$

PROOF. Let (A_{ij}) be the matrix $[f]$ and (B_{jk}) the matrix $[g]$. I will denote the standard bases of F^n, F^m and F^ℓ by $\vec{u}_i, \vec{v}_j$ and $\vec{w}_k$. I hope this will make the calculation clearer; it would be a mess to use our usual notation of $\vec{e}_i$ when there are three different standard bases kicking around. In this notation we have

$$\begin{aligned} g(\vec{w}_k) &= (B_{*k}) = B_{1k}\vec{v}_1 + \cdots + B_{mk}\vec{v}_m \\ f(\vec{v}_j) &= (A_{*j}) = A_{1j}\vec{u}_1 + \cdots + A_{nj}\vec{u}_n. \end{aligned}$$

From this it follows that

$$\begin{aligned} (f \circ g)(\vec{w}_k) &= f(B_{1k}\vec{v}_1 + \cdots + B_{mk}\vec{v}_m) \\ &= B_{1k}f(\vec{v}_1) + \cdots + B_{mk}f(\vec{v}_m) \\ &= \sum_{j=1}^{m} B_{jk} f(\vec{v}_j) \\ &= \sum_{j=1}^{m} B_{jk} \sum_{i=1}^{n} A_{ij}\vec{u}_i \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} A_{ij}B_{jk} \right) \vec{u}_i. \end{aligned}$$

On the other hand, the entries (C_{ik}) of the matrix $[f \circ g]$ are defined by rule

$$(f \circ g)(\vec{w}_k) = C_{1k}\vec{u}_1 + \cdots + C_{nk}\vec{u}_n.$$

Comparing coefficients in these two ways to calculate $(f \circ g)(\vec{w}_k)$ confirms that $C_{ik} = \sum_{j=1}^{m} A_{ij}B_{jk}$. □

PROPOSITION 2.1.9 (Calculating with Matrices). *Let $k, \ell, m, n \in \mathbb{N}$, $A, A' \in \mathsf{Mat}(n \times m; F)$, $B, B' \in \mathsf{Mat}(m \times \ell; F)$, $C \in \mathsf{Mat}(\ell \times k; F)$ and $I = I_m$ the $(m \times m)$-identity matrix. Then the following hold for matrix multiplication:*

$$\begin{aligned} (A + A')B &= AB + A'B \\ A(B + B') &= AB + AB' \\ IB &= B \\ AI &= A \\ (AB)C &= A(BC). \end{aligned}$$

FIRST PROOF! I'll do it by bloody-minded calculation and not a smidgeon of thought. But I won't do all the equalities, just the second, third and fifth. You can do the other two for yourself.

To the second:

$$\begin{aligned}(A(B+B'))_{ik} &= \sum_{j=1}^{m} A_{ij}(B+B')_{jk} \\ &= \sum_{j=1}^{m} A_{ij}(B_{jk}+B'_{jk}) \\ &= \sum_{j=1}^{m} (A_{ij}B_{jk}+A_{ij}B'_{jk}) \\ &= (AB+AB')_{ik}\end{aligned}$$

which shows that $A(B+B') = AB+AB'$. For the third: $(IB)_{ik} = \sum_j I_{ij}B_{jk} = \sum_j \delta_{ij}B_{jk} = B_{ik}$ and this gives $IB = B$. Now I'll spice up the job of typing by taking $\kappa, \lambda, \mu, \nu$ as indices for the next matrices:

$$\begin{aligned}((AB)C)_{\nu\kappa} &= \sum_{\lambda=1}^{\ell} (AB)_{\nu\lambda}C_{\lambda\kappa} \\ &= \sum_{\lambda=1}^{\ell} (\sum_{\mu=1}^{m} A_{\nu\mu}B_{\mu\lambda})C_{\lambda\kappa} \\ &= \sum_{\mu,\lambda=1}^{m,\ell} A_{\nu\mu}B_{\mu\lambda}C_{\lambda\kappa} \\ (A(BC))_{\nu\kappa} &= \sum_{\mu=1}^{m} A_{\nu\mu}(BC)_{\mu\kappa} \\ &= \sum_{\mu=1}^{m} A_{\nu\mu}\left(\sum_{\lambda=1}^{\ell} B_{\mu\lambda}C_{\lambda\kappa}\right) \\ &= \sum_{\mu,\lambda=1}^{m,\ell} A_{\nu\mu}B_{\mu\lambda}C_{\lambda\kappa}\end{aligned}$$

and this shows that $(AB)C = A(BC)$. □

SECOND PROOF! I can prove the rules for matrices by applying Theorem 2.1.1 and Theorem 2.1.8. For instance to show $(AB)C = A(BC)$, I use Theorem 2.1.1 to take the corresponding linear mappings $a : F^m \to F^n, b : F^\ell \to F^m, c : F^k \to F^\ell$ such that $A = [a], B = [b], C = [c]$. Then, by Theorem 2.1.8:

$$\begin{aligned}(AB)C = ([a] \circ [b]) \circ [c] = [a \circ b] \circ [c] = [(a \circ b) \circ c] \\ A(BC) = [a] \circ ([b] \circ [c]) = [a] \circ ([b \circ c]) = [a \circ (b \circ c)]\end{aligned}$$

so that the equality $(AB)C = A(BC)$ follows from the associativity of composition of mappings $(a \circ b) \circ c = a \circ (b \circ c)$. □

REMARK 2.1.10 (Linear Mappings $F^m \to F^n$ as Matrix Multiplication). Since we've discussed matrix multiplication properly now, I can show you the inverse of the bijection of Theorem 2.1.1 $\mathsf{M} : \mathrm{Hom}_F(F^m, F^n) \xrightarrow{\sim} \mathsf{Mat}(n \times m; F), f \mapsto [f]$, which attaches a representing matrix to each linear mapping. To do so, I think of the elements of F^m and F^n as column vectors. Then, given a matrix

$A \in \mathsf{Mat}(n \times m; F)$ I consider matrix multiplication $(A\circ) : \mathsf{Mat}(m \times 1; F) \to \mathsf{Mat}(n \times 1; F)$, which I choose to write instead as:

$$(A\circ) : F^m \to F^n.$$

It follows straight from the definition that the mapping

$$\mathsf{Mat}(n \times m; F) \to \mathrm{Hom}_F(F^m, F^n), A \mapsto (A\circ) \tag{2}$$

is the inverse to the mapping M above. *You should get to the point where the identification between linear mappings $F^m \to F^n$ and matrices is in your bones.*

By the way, given $x \in F^m$, I'll write Ax instead of $A \circ x$, just as you are used to.

EXERCISE 25. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be the reflection $(x, y) \mapsto (x, -y)$ as in Exercise 14. Show that: $\{g \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2) : f \circ g = g \circ f\}$ is a subspace of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2)$ and give a basis of this subspace.

EXERCISE 26. Given a matrix $A \in \mathsf{Mat}(n \times m; F)$ define the **transposed matrix** $A^\mathsf{T} \in \mathsf{Mat}(m \times n; F)$ by the rule $(A^\mathsf{T})_{ij} = A_{ji}$. I refer to that by saying that A^T is obtained from A by "reflection about the main diagonal". For instance, the transposition of a column vector, i.e. an $(n \times 1)$-matrix, is a **row vector**, i.e. a $(1 \times n)$-matrix. Show that: $(A^\mathsf{T})^\mathsf{T} = A$. Show further that: $(AB)^\mathsf{T} = B^\mathsf{T}A^\mathsf{T}$.

$$\begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \end{pmatrix}^\mathsf{T} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{pmatrix}$$

2.2. Basic Properties of Matrices

We've just seen that matrices arise naturally when we think of linear mappings between F^m and F^n. In this section I'll recall or introduce several important properties of matrices that we will use in the rest of the course.

DEFINITION 2.2.1. *A matrix A is called* **invertible** *if there exist matrices B and C such that $BA = I$ and $AC = I$.*

If we think of A as a linear mapping $a : F^m \to F^n$, then Theorem 2.1.8 shows that A is invertible if and only if the mapping a is an isomorphism. In particular it follows from Theorem 1.7.7 that $n = m$, and so only square matrices can be invertible. For a square matrix A the following conditions are then equivalent:

(1) There exists a square matrix B such that $BA = I$;
(2) There exists a square matrix C such that $AC = I$;
(3) The square matrix A is invertible.

Let's check this. That (3) implies (1) and (2) follows from the definition of A being invertible. Now suppose that instead that (1) holds. Using Theorem 2.1.8 we see that the linear mapping $a : F^n \to F^n$ has a left inverse and so is injective. Applying the Rank-Nullity Theorem then shows that $\dim(\mathrm{im}\, a) = n$ and so, by Remark 1.6.10, $\mathrm{im}\, a = F^n$ and a is surjective, and hence an isomorphism. Thus (3) follows. Similarly, assuming that (2) holds, we see the linear mapping $a : F^n \to F^n$ has a right inverse and so is surjective. Applying the Rank-Nullity Theorem then shows that $\dim(\ker a) = 0$ so that, by Lemma 1.8.2, a is injective and hence an isomorphism, proving (3) in this case.

If A is invertible and $a : F^n \xrightarrow{\sim} F^n$ is the associated vector space isomorphism, then the matrix $[a^{-1}]$ of the inverse mapping a^{-1} is the unique square matrix B satisfying $BA = I$ and also the

unique square matrix satisfying $AB = I$. We denote this matrix by A^{-1} and call it **the inverse matrix of** A.

The invertible $(n \times n)$-matrices with entries in the field F form a group under matrix multiplication, called the **general linear group of** $(n \times n)$**-matrices**, which we write as

$$\mathrm{GL}(n; F) := \mathsf{Mat}(n; F)^{\times}.$$

This group was mentioned in the Year 2 course Fundamentals of Pure Mathematics.

EXERCISE 27. Show that: there is a group isomorphism between $GL(2; \mathbb{F}_2)$ and S_3, where $\mathbb{F}_2$ is the field with two elements $\{\overline{0}, \overline{1}\}$ and S_3 the symmetric group on 3 letters.

Systems of Linear Equations. Let's go back to our original motivation of solving the following:

$$\begin{array}{ccccc} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m & = & b_2 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m & = & b_n \end{array}$$

I now write this in our new shorthand notation

$$Ax = b$$

where the left hand side features the product of the coefficient matrix A with the column vector $x = (x_1, \ldots, x_m)^{\mathsf{T}}$ and where the right hand side features the column vector $b = (b_1, \ldots b_n)^{\mathsf{T}}$. Solving this system of equations amounts to describing the preimage of $b \in F^n$ of the linear mapping $(A\circ) : F^m \to F^n$. In particular, the solution set of the associated homogenised system of equations is the preimage of $\vec{0} \in F^n$, in other words it is the kernel of $(A\circ) : F^m \to F^n$.

The operations of Gaussian elimination can also be interpreted in this language: let

$$E_{ij}$$

denote the **basis matrix** with the entry 1 in the i-th row and j-th column and 0's everywhere else. For $i \neq j$, the rule [*Row Addition*] asks to add λ-times the j-th row to the i-th row, and in matrix notation this can be written as

$$(I + \lambda E_{ij})Ax = (I + \lambda E_{ij})b$$

Since $(I - \lambda E_{ij})(I + \lambda E_{ij}) = I$, it's clear that this new system of equations has exactly the same solutions as the original system. Similarly, for $i \neq j$ let P_{ij} denote the matrix corresponding to the linear mapping $F^m \to F^m$ that swaps the i-th coordinates with the j-th coordinates and leaves everything else alone. Then [*Row Swap*] can be described in matrix notation as

$$P_{ij}Ax = P_{ij}b.$$

Since $P_{ij}P_{ij} = I$ it is again clear that the new system of equations has the same solutions as the original system.

DEFINITION 2.2.2. *I will define an* **elementary matrix** *to be any square matrix that differs from the identity matrix in at most one entry.*

All the elementary matrices with entries in a field are, with the exception of those where you take one 1 in the identity matrix and replace it by 0, invertible. Be warned, dear Reader, that this definition of elementary matrix differs from the Wikipedia entry, but the world is indeed complicated and there is not universal agreement on the definition of an elementary matrix.

THEOREM 2.2.3. *Every square matrix with entries in a field can be written as a product of elementary matrices.*

PROOF. First, I want to write the permutation matrix P_{ij} as a product of elementary matrices, and I do it as follows:

$$P_{ij} = \mathsf{diag}(1, \ldots, 1, -1, 1, \ldots, 1)(I + E_{ij})(I - E_{ji})(I + E_{ij})$$

In this equation you should put the (-1) in the j-th place and you should know that $\mathsf{diag}(\lambda_1, \ldots, \lambda_n)$ denotes the **diagonal matrix** with entries $a_{ij} = 0$ for $i \neq j$ and $a_{ii} = \lambda_i$.

Next I assert that the inverse of each invertible elementary matrix is again an elementary matrix. You saw that already when I wrote $(I - \lambda E_{ij})(I + \lambda E_{ij}) = I$.

Now let A be an arbitrary square matrix. By Gaussian elimination we can find invertible elementary matrices $S_1, \ldots, S_t$ such that $S_t \cdots S_1 A$ has echelon form. It's easy to see that multiplying on the right by invertible elementary matrices corresponds to applying column operations, by which I mean the addition of a multiple of one column to another or the swap of two columns or the multiplication of one column by a non-zero scalar. These operations can be applied to bring the matrix into the form $\mathsf{diag}(1, \ldots, 1, 0, \ldots 0)$ and so we deduce that there exists elementary matrices $T_1, \ldots, T_s$ such that $S_t \cdots S_1 A T_1 \cdots T_s = \mathsf{diag}(1, \ldots, 1, 0, \ldots 0)$. We can write this diagonal matrix as a product of non-invertible diagonal elementary matrices $D_1, \ldots, D_r$, giving $S_t \cdots S_1 A T_1 \cdots T_s = D_1 \cdots D_r$. From this it follows that

$$A = S_1^{-1} \cdots S_t^{-1} D_1 \cdots D_r T_s^{-1} \cdots T_1^{-1}$$

□

This proof proves more: for a fixed n there exists an N such that each $(n \times n)$-matrix can be written as a product of at most N elementary matrices.

DEFINITION 2.2.4. *Any matrix whose only non-zero entries lie on the diagonal, and which has first 1's along the diagonal and then 0's, is said to be in* **Smith Normal Form**.

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

THEOREM 2.2.5 (Transformation of a Matrix into Smith Normal Form). *For each matrix $A \in \mathsf{Mat}(n \times m; F)$ there exist invertible matrices P and Q such that PAQ is a matrix in Smith Normal Form.*

PROOF. Just argue as in the proof of Theorem 2.2.3: use Gaussian elimination to first find invertible elementary matrices $S_1, \ldots, S_t$ such that $S_t \cdots S_1 A$ is in echelon form; then find invertible elementary matrices $T_1, \ldots, T_s$ to perform column operations such that $S_t \cdots S_1 A T_1 \cdots T_s$ is in Smith Normal Form. Then $P = S_t \cdots S_1$ and $Q = T_1 \cdots T_s$. □

DEFINITION 2.2.6. *The* **column rank** *of a matrix $A \in \mathsf{Mat}(n \times m; F)$ is the dimension of the subspace of F^n generated by the columns of A. Similarly, the* **row rank** *of A is the dimension of the subspace of F^m generated by the rows of A.*

EXERCISE 28. Show that: the column rank of a matrix $A \in \mathsf{Mat}(n \times m; F)$ equals the rank of the linear mapping $(A\circ) : F^m \to F^n$. Hence deduce that the Rank-Nullity theorem you met in Introduction to Linear Algebra is the special case of Theorem 1.8.4 where $V = F^m, W = F^n$ and $f = (A\circ)$.

THEOREM 2.2.7. *The column rank and the row rank of any matrix are equal.*

PROOF. We can interpret the column rank of the matrix $A \in \mathsf{Mat}(n \times m; F)$ as the dimension of the image of

$$(A\circ) : F^m \to F^n$$

This interpretation shows immediately that PAQ has the same column rank as A whenever P and Q are invertible matrices. Furthermore, by transposing our matrices, we then also know that PAQ and A have the same row rank.

By Theorem 2.2.5, we can find invertible matrices P, Q such that PAQ is in Smith Normal Form. But it is obvious that the column rank and the row rank are equal for a matrix in Smith Normal Form, since they both equal the number of non-zero entries on the diagonal. By the above paragraph, the same holds true for A itself. □

DEFINITION 2.2.8. *I will drop the tag "column" or "row" now and just refer to the* **rank of a matrix** *and write it as* $\mathrm{rk}A$. *When the rank is as big as possible, meaning that it is equal either to the number of rows or number of columns, whichever is smaller, then the matrix has* **full rank**.

EXERCISE 29. Find a (3×3)-matrix with all entries non-zero integers but which has rank 2.

Inverting Matrices. There is a simple procedure to calculate the inverse of an invertible $(n \times n)$-matrix A: write the identity matrix I next to it, thereby producing an $(n \times 2n)$-matrix $(A|I)$. Apply elementary row operations, including multiplying a row by a non-zero scalar, in order to bring A into echelon form, and then possibly further row operations to bring it into reduced echelon form: this will actually be the identity matrix. The inverse to A is then what is standing in the right half of the $(n \times 2n)$-matrix. To see why this is so, suppose that the elementary operations you carried out correspond to left-multiplication by the elementary matrices $S_1, S_2, \ldots, S_t$. Then the $(n \times 2n)$-matrix becomes

$$(S_t \cdots S_2 S_1 A | S_t \cdots S_2 S_1 I)$$

When you reach the equality $S_t \cdots S_2 S_1 A = I$, i.e. when you have brought A into reduced echelon form, then by multiplying both sides of this equality by A^{-1} you see that

$$S_t \cdots S_2 S_1 I = S_t \cdots S_2 S_1 A A^{-1} = I A^{-1} = A^{-1}$$

and so the matrix in the second half is indeed A^{-1}.

2.3. Abstract Linear Mappings and Matrices

In Section 2.1 you saw that linear mappings $F^m \to F^n$ were the same as $(n \times m)$-matrices over F. By Theorem 1.5.11, choosing an ordered basis for a finite dimensional F-vector space V produces an isomorphism between F^n and V where $n = \dim V$. Using this it is therefore clear that linear mappings $V \to W$ between abstract vector spaces with given ordered bases can also be represented by matrices.

The only danger in representing linear mappings by matrices is keeping track of which ordered bases are being used. But a notation has been invented for this, and similarly to the electricians' colour-coding for the wiring of plugs, this notation makes it impossible for a mathematician to err.

THEOREM 2.3.1 (Abstract Linear Mappings and Matrices). *Let F be a field, V and W vector spaces over F with ordered bases $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$ and $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$. Then to each linear mapping $f : V \to W$ we associate a* **representing matrix** ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ *whose entries a_{ij} are defined by the identity*

$$f(\vec{v}_j) \;=\; a_{1j}\vec{w}_1 + \cdots + a_{nj}\vec{w}_n \in W\,.$$

This produces a bijection, which is even an isomorphism of vector spaces:

$$\begin{array}{rcl} \mathsf{M}_{\mathcal{B}}^{\mathcal{A}} : \mathrm{Hom}_F(V,W) & \tilde{\to} & \mathsf{Mat}(n\times m;F) \\ f & \mapsto & {}_{\mathcal{B}}[f]_{\mathcal{A}} \end{array}$$

We call $\mathsf{M}_{\mathcal{B}}^{\mathcal{A}}(f) = {}_{\mathcal{B}}[f]_{\mathcal{A}}$ the **representing matrix of the mapping f with respect to the bases $\mathcal{A}$ and $\mathcal{B}$.** The columns of this matrix give the coordinates of the image of a basis vector from $\mathcal{A}$ with respect to the basis $\mathcal{B}$. If V is m-dimensional and W is n-dimensional then $\mathsf{M}_{\mathcal{B}}^{\mathcal{A}}(f) = (a_{ij})$ is an $n \times m$ matrix, i.e. has n rows and m columns.

If $f : F^m \to F^n$ is a linear mapping, we could work with the standard bases from Example 1.5.10 for F^m and F^n . I will label these by $\mathcal{S}(m)$ and $\mathcal{S}(n)$. A look at the definitions shows that the representing matrix $[f]$ of Theorem 2.1.1 reappears:

$$[f] = {}_{\mathcal{S}(n)}[f]_{\mathcal{S}(m)}.$$

Because of this, I'll usually omit reference to the standard bases, and continue to write $[f]$ instead of ${}_{\mathcal{S}(n)}[f]_{\mathcal{S}(m)}$. Moreover, for a linear mapping $f : F^m \to W$ I will abbreviate ${}_{\mathcal{B}}[f]_{\mathcal{S}(m)}$ by ${}_{\mathcal{B}}[f]$, and for $f : V \to F^n$ I will abbreviate ${}_{\mathcal{S}(n)}[f]_{\mathcal{A}}$ by $[f]_{\mathcal{A}}$.

PROOF. One way to do this would be to write out a variation of the proof of Theorem 2.1.1, but as I mentioned at the beginning of this section there is a better way. Recall the isomorphisms $\Phi_{\mathcal{A}} : F^m \tilde{\to} V$ and $\Phi_{\mathcal{B}} : F^n \tilde{\to} W$ of Theorem 1.5.11. Then the representing matrix is, by definition,

$${}_{\mathcal{B}}[f]_{\mathcal{A}} = [\Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}].$$

From this it follows that we can write our mapping in the theorem as a composition of bijections:

$$\begin{array}{rcl} \mathrm{Hom}_F(V,W) & \tilde{\to} & \mathrm{Hom}_F(F^m,F^n) \overset{\mathsf{M}}{\tilde{\to}} \mathsf{Mat}(n\times m;F) \\ f & \mapsto & \Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}} \mapsto [\Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}], \end{array}$$

where $\mathsf{M} : g \mapsto [g]$ of Theorem 2.1.1 is our mapping that attaches to each linear mapping $g : F^m \to F^n$ its representing matrix. □

THEOREM 2.3.2 (The Representing Matrix of a Composition of Linear Mappings). *Let F be a field and U, V, W finite dimensional vector spaces over F with ordered bases $\mathcal{A}, \mathcal{B}, \mathcal{C}$. If $f : U \to V$ and $g : V \to W$ are linear mappings, then the representing matrix of the composition $g \circ f : U \to W$ is the matrix product of the representing matrices of f and g:*

$${}_{\mathcal{C}}[g \circ f]_{\mathcal{A}} = {}_{\mathcal{C}}[g]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}}$$

FIRST PROOF! First unpack the notation:

$${}_{\mathcal{C}}[g \circ f]_{\mathcal{A}} = [\Phi_{\mathcal{C}}^{-1} \circ (g \circ f) \circ \Phi_{\mathcal{A}}] \quad \text{and} \quad {}_{\mathcal{C}}[g]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}} = [\Phi_{\mathcal{C}}^{-1} \circ g \circ \Phi_{\mathcal{B}}] \circ [\Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}];$$

then apply Theorem 2.1.8. □

SECOND PROOF! Copy the proof of Theorem 2.1.8, but this time interpreting $\vec{u}_i, \vec{v}_j$ and $\vec{w}_k$ there as the vectors of our ordered bases $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$. □

DEFINITION 2.3.3. *Let V be a finite dimensional vector space with an ordered basis $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$. We will denote the inverse to the bijection of Theorem 1.5.11 $\Phi_{\mathcal{A}} : F^m \tilde{\to} V, (\alpha_1, \ldots, \alpha_m)^{\mathsf{T}} \mapsto \alpha_1\vec{v}_1 + \cdots + \alpha_m\vec{v}_m$ by*

$$\vec{v} \mapsto {}_{\mathcal{A}}[\vec{v}]$$

The column vector ${}_{\mathcal{A}}[\vec{v}]$ is called the **representation of the vector $\vec{v}$ with respect to the basis $\mathcal{A}$.**

THEOREM 2.3.4 (Representation of the Image of a Vector). *Let V, W be finite dimensional vector spaces over F with ordered bases $\mathcal{A}, \mathcal{B}$ and let $f : V \to W$ be a linear mapping. The following holds for $\vec{v} \in V$:*

$$_{\mathcal{B}}[f(\vec{v})] = {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\vec{v}]$$

PROOF. First unpack the notation:

$$_{\mathcal{B}}[f(\vec{v})] = \Phi_{\mathcal{B}}^{-1}(f(\vec{v})) \quad \text{and} \quad {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\vec{v}] = [\Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}] \circ \Phi_{\mathcal{A}}^{-1}(\vec{v}),$$

then apply Equation (2). □

Let $\mathcal{A} = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_m)$ and $\mathcal{B} = (\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_n)$, and let ${}_{\mathcal{B}}[f]_{\mathcal{A}} = (a_{ij})$ be the $n \times m$ matrix of the coefficients in

$$f(\vec{v}_j) \;=\; \sum_{i=1}^{n} a_{ij}\vec{w}_i \in W \;.$$

For an arbitrary $\vec{v} \in V$ the expression of $\vec{v}$ as a linear combination of the $\vec{v}_j$'s

$$\vec{v} \;=\; \sum_{j=1}^{m} x_j\vec{v}_j \in V$$

with coefficients $(x_1, x_2, \ldots, x_m) \in F^m$ is transformed by f into an expression of $f(\vec{v}) \in W$ as a linear combination of the $\vec{w}_i$'s

$$\begin{aligned} f(\vec{v}) \;&=\; \sum_{j=1}^{m} x_j f(\vec{v}_j) \\ &=\; \sum_{j=1}^{m} x_j (\sum_{i=1}^{n} a_{ij}\vec{w}_i) \\ &=\; \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij}x_j)\vec{w}_i \\ &=\; y_1\vec{w}_1 + \cdots + y_n\vec{w}_n \in W \end{aligned}$$

with coefficients $(y_1, y_2, \ldots, y_n) \in F^n$, where

$$y_i \;=\; \sum_{j=1}^{m} a_{ij}x_j \;, \text{ or equivalently as the matrix product } \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \;=\; (a_{ij}) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \in F^n \;,$$

confirming Theorem 2.3.4. Note that it is necessary to write the coefficients as column vectors. (Actually, it is also possible to write them as row vectors, but then the transformation rule is given by the matrix product

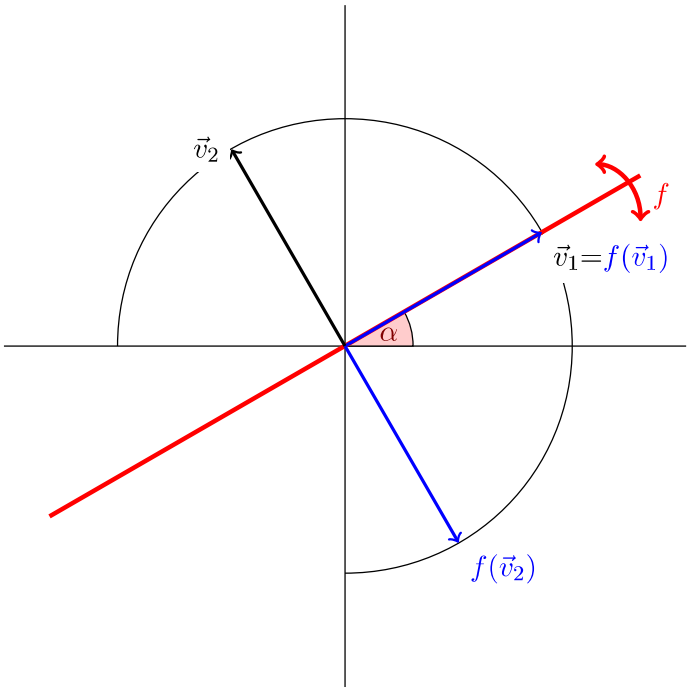
$$(y_1 \; y_2 \; \ldots \; y_n) \;=\; (x_1 \; x_2 \; \ldots \; x_m)(a_{ij})^T$$

with $(a_{ij})^T$ the transpose $m \times n$ matrix).

EXAMPLE 2.3.5. (Cf. Example 2.1.5.) Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be reflection about the straight line making an angle α with the x-axis. Let $\mathcal{A} = (\vec{v}_1, \vec{v}_2)$ be the ordered basis of $\mathbb{R}^2$ where $\vec{v}_1 = (\cos\alpha, \sin\alpha)^\mathsf{T}$ and $\vec{v} = (-\sin\alpha, \cos\alpha)^\mathsf{T}$. Then

$${}_{\mathcal{A}}[f]_{\mathcal{A}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This is clear because, when you look at the picture you'll see that $f(\vec{v}_1) = \vec{v}_1$ and $f(\vec{v}_2) = -\vec{v}_2$.



2.4. Change of a Matrix by Change of Basis

DEFINITION 2.4.1. *Let $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_n)$ and $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$ be ordered bases of the same F-vector space V. Then the matrix representing the identity mapping with respect to these bases*

$$_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}}$$

is called a **change of basis matrix**. *By definition, its entries are given by the equalities $\vec{v}_j = \sum_{i=1}^{n} a_{ij}\vec{w}_i$.*

EXAMPLE 2.4.2. (Cf. Example 2.1.5 and Example 2.3.5.) The change of basis matrix on $\mathbb{R}^2$ for the $\mathcal{A} = (\vec{e}_1, \vec{e}_2)$ the standard basis and $\mathcal{B} = (\vec{v}_1, \vec{v}_2)$ the basis of Example 2.3.5 is given by

$$_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}.$$

THEOREM 2.4.3 (Change of Basis). *Let V and W be finite dimensional vector spaces over F and let $f : V \to W$ be a linear mapping. Suppose that $\mathcal{A}, \mathcal{A}'$ are ordered bases of V and $\mathcal{B}, \mathcal{B}'$ are ordered bases of W. Then*

$$_{\mathcal{B}'}[f]_{\mathcal{A}'} = {}_{\mathcal{B}'}[\mathrm{id}_W]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$$

PROOF. This follows immediately from Theorem 2.3.2 and the blindingly obvious equality $f = \mathrm{id}_W \circ f \circ \mathrm{id}_V$. □

COROLLARY 2.4.4. *Let V be a finite dimensional vector space and let $f : V \to V$ be an endomorphism of V. Suppose that $\mathcal{A}, \mathcal{A}'$ are ordered bases of V. Then*

$$_{\mathcal{A}'}[f]_{\mathcal{A}'} = {}_{\mathcal{A}}[\mathrm{id}_V]^{-1}_{\mathcal{A}'} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$$

PROOF. Obviously $_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}} = I_n$ is the identity matrix. Theorem 2.3.2 then gives the equality

$$_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'} \circ {}_{\mathcal{A}'}[\mathrm{id}_V]_{\mathcal{A}} = I_n$$

from which it follows that $_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$ is the inverse matrix of $_{\mathcal{A}'}[\mathrm{id}_V]_{\mathcal{A}}$, that is $_{\mathcal{A}'}[\mathrm{id}_V]^{-1}_{\mathcal{A}} = {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$. The result now follows as a special case of Theorem 2.4.3. □

EXERCISE 30. Check that this corollary agrees with the calculations made in Examples 2.1.5, 2.3.5 and 2.4.2.

I will write this out a little more explicitly: suppose that $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}$ and $M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$, then

$$N = T^{-1}MT \tag{3}$$

where $T = {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{B}}$.

EXERCISE 31. Let V be an F-vector space with ordered basis $(\vec{v}_1, \ldots, \vec{v}_n)$. Show that: change of basis matrices provide a bijection

$$\begin{array}{ccc} \{\text{ordered bases of } V\} & \tilde{\to} & \mathrm{GL}(n;F) \\ \mathcal{B} & \mapsto & {}_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}} \end{array}$$

where $GL(n;F)$ is the group of invertible $(n \times n)$-matrices, as discussed in the previous section. Which matrices are the images of the ordered bases obtained from $(\vec{v}_1, \ldots, \vec{v}_n)$ by reordering?

THEOREM 2.4.5 (Smith Normal Form). *Let $f : V \to W$ be a linear mapping between finite dimensional F-vector spaces. There exist an ordered basis $\mathcal{A}$ of V and an ordered basis $\mathcal{B}$ of W such that the representing matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ has zero entries everywhere except possibly on the diagonal, and along the diagonal there are 1's first, followed by 0's.*

PROOF. The key step is the claim proved in the second paragraph of the proof of Theorem 1.8.4. There I showed that if I choose an ordered basis $(\vec{w}_1, \ldots, \vec{w}_r)$ of the image of f, and an ordered basis $(\vec{k}_1, \ldots, \vec{k}_s)$ of the kernel of f, then I can find a family of linearly independent vectors $(\vec{v}_1, \ldots, \vec{v}_r)$ such that $f(\vec{v}_i) = \vec{w}_i$ and such that $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_r, \vec{k}_1, \ldots, \vec{k}_s)$ is an ordered basis of V.

Given the above data, I extend $(\vec{w}_1, \ldots, \vec{w}_r)$ to an ordered basis $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_r, \vec{w}_{r+1}, \ldots, \vec{w}_n)$ of W. Then it is immediate that the matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ has the required form, where there are r 1's on the diagonal. □

EXERCISE 32. An endomorphism $f : V \to V$ of an F-vector space is called **nilpotent** if and only if there exists $d \in \mathbb{N}$ such that $f^d = 0$. Suppose that $f : V \to V$ is a nilpotent endomorphism of a finite dimensional vector space. Show that: the vector space V has an ordered basis $\mathcal{A}$ such that the representing matrix ${}_{\mathcal{A}}[f]_{\mathcal{A}}$ of f with respect to this basis has the form of an upper triangular matrix with only 0's along the diagonal. Show that: conversely, any $(n \times n)$-matrix M that is upper triangular and has only 0's along the diagonal satisfies $M^n = 0$.

This exercise is closely related to the material of Chapter 6 on the Jordan Normal Form.

DEFINITION 2.4.6. *The* **trace** *of a square matrix is defined to be the sum of its diagonal entries. We denote this by*

$$\mathrm{tr}(A)$$

EXERCISE 33. Let A be an $(n \times m)$-matrix and B an $(m \times n)$-matrix, both with entries in the field F. Show that: $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Taking $A = T^{-1}M$ and $B = T$ in Exercise 33 it follows that:

$$\mathrm{tr}(T^{-1}MT) = \mathrm{tr}(M) \tag{4}$$

for any $(n \times n)$-matrix M and invertible $(n \times n)$-matrix T. Therefore, any endomorphism $f : V \to V$ of a finite dimensional F-vector space has a **trace**, written

$$\mathrm{tr}(f) = \mathrm{tr}(f|V) = \mathrm{tr}_F(f|V)$$

where we use the different notations to emphasise the vector space V or even the ground field F whenever necessary. This is defined by choosing first an ordered basis $\mathcal{A}$ of V and then setting

$\mathrm{tr}(f) = \mathrm{tr}({}_{\mathcal{A}}[f]_{\mathcal{A}})$. Thanks to (3) and (4) this definition of $\mathrm{tr}(f)$ is independent of the choice of ordered basis.

EXERCISE 34. Let $f : V \to W$ and $g : W \to V$ be two linear mappings where V and W are both finite dimensional F-vector spaces. Show that: $\mathrm{tr}(fg) = \mathrm{tr}(gf)$.

EXERCISE 35. Let V be a finite dimensional F-vector space and let $f : V \to V$ be an idempotent, that is $f^2 = f$. Show that $\mathrm{tr}(f) = \dim(\mathrm{im}\, f)$.

EXERCISE 36. Let V be a finite dimensional F-vector space and $f : V \to V$ a linear mapping. Show that

$$\mathrm{tr}((f\circ)|\mathrm{End}_F(V)) = (\dim_F V)\mathrm{tr}(f|V)$$

CHAPTER 3

Rings and Modules

In this chapter I will introduce rings and modules, new algebraic structures that you may not have seen before. They generalise fields and vector spaces, and in order to understand and develop the more sophisticated properties of linear algebra it is important to use these notions. As well as presenting definitions and examples, I'll also take the chance to introduce a new technique called taking quotients which will be useful for the rest of your mathematical career, whether that's two more years or a happy lifetime.

3.1. Rings

In the previous chapters, I've been vague about what exactly a field is. I stressed that you already knew: not only did you have lots of excellent examples hardwired, such as $\mathbb{R}, \mathbb{Q}$ and $\mathbb{C}$, but it was easy to pick-up new examples, such as $\mathbb{F}_3$. From the point of view of linear algebra, fields all seem quite similar and so I decided we'd gain little by studying them in that context. Hence the vagueness.

Well, you already know rings, in fact more so. For instance, the integers $\mathbb{Z}$ form a ring and so do polynomials $\mathbb{C}[X]$, the set of $(n \times n)$-matrices $\mathsf{Mat}(n; F)$ is a ring, and every field is a ring. But, dear Reader, you are officially now warned: rings are a zoo! And not just any zoo. They are lots and lots of wild animals within. So to proceed, you need bravery and a definition; then we can investigate.

DEFINITION 3.1.1. *A* **ring** *is a set with two operations $(R, +, \cdot)$ that satisfy:*

(1) $(R, +)$ is an abelian group;
(2) $(R, \cdot)$ is a **monoid***; this means that the second operation $\cdot : R \times R \to R$ is associative and that there is an* **identity element** *$1 = 1_R \in R$, often called just the* **identity***, with the property that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.*
(3) The distributive laws hold, meaning that for all $a, b, c \in R$

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

The two operations are called **addition** *and* **multiplication** *in our ring. A ring in which multiplication is commutative, that is in which $a \cdot b = b \cdot a$ for all $a, b \in R$, is a* **commutative ring**.

The element $1 \in R$ is uniquely determined as the identity element of the monoid $(R, \cdot)$. The additive identity of $(R, +)$ is called zero, and written either as 0_R or just 0 when it's clear which ring I am referring to. I will very quickly forget to write the operation $\cdot$, writing instead $a \cdot b = ab$. Thus, for instance, I will write the first distributive law as $a(b + c) = ab + ac$.

In some reference books the definition of a ring is slightly different. There, instead of $(R, \cdot)$ being a monoid, it is taken only to be **semigroup**, which means that multiplication is associative but there may not exist an identity element. People who use this definition, call Definition 3.1.1 above a **unital ring**. You should know, however, that Definition 3.1.1 is by far the most common.

EXAMPLE 3.1.2. Just as there is the extreme example of the zero vector space, so too is there the **null ring** or **zero ring**. Here R is a single element set, say $\{0\}$, with the operations $0+0=0$ and $0\times 0=0$. I'll call any ring that is not the zero ring a **non-zero ring**. Many results will start with something like "Let R be a non-zero ring, then ...": this is because the zero ring is a degenerate example of a ring with degenerate properties which are just dull and should be ruled out.

EXAMPLE 3.1.3. The integers $\mathbb{Z}$ form a commutative ring under usual addition and multiplication. If R is a ring and X a set, then the set $\mathrm{Maps}(X,R)$ form a ring under pointwise addition and multiplication, compare with Exercise 1. If R is a ring and $n\in\mathbb{N}$ then the set of $(n\times n)$-matrices with entries in R form a ring, $\mathsf{Mat}(n;R)$ under the usual operations of matrix addition and matrix multiplication, see Proposition 2.1.9. If $n\geqslant 2$ then $\mathsf{Mat}(n;R)$ is not commutative provided that R is not the zero ring.

ETYMOLOGY. The word ring tracks back at least as far as Hilbert who, at the end of the 19th Century, used the German word "Zahlring" which translates to Number Ring. He was working with a very specific example from number theory in mind, and the above abstract list of axioms is a later invention for a large class of mathematical objects that include the objects he was studying. Why he used "Zahlring" is still a bit of a mystery to me. I've seen it written that in German "Ring" often refers to an association or group of people with shared interests. We use that in English too, as in "Ring of Thieves". Other people write that it refers to the fact that, for the examples of that Hilbert studied, appropriate powers of each element "cycled back" to be written as a linear combination lower powers.

EXAMPLE 3.1.4. Let $m\in\mathbb{Z}$ be an integer. Then the set of **integers modulo** m, written

$$\mathbb{Z}/m\mathbb{Z}$$

is a ring. The elements of $\mathbb{Z}/m\mathbb{Z}$ consist of **congruence classes** of integers modulo m: that is the elements are the subsets T of $\mathbb{Z}$ of the form $T=a+m\mathbb{Z}$ with $a\in\mathbb{Z}$. I think of these as the set of integers that have the same remainder when you divide them by m. I denote the above congruence class by $\overline{a}$. Obviously, $\overline{a}=\overline{b}$ is the same as $a-b\in m\mathbb{Z}$, and often I'll write

$$a\equiv b \pmod{m}.$$

If $m\in\mathbb{N}_{\geqslant 1}$ then there are m congruence classes modulo m, in other words $|\mathbb{Z}/m\mathbb{Z}|=m$, and I could write out the set as

$$\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\overline{1},\ldots,\overline{m-1}\}$$

To define addition and multiplication I set

$$\overline{a}+\overline{b}=\overline{a+b} \text{ and } \overline{a}\cdot\overline{b}=\overline{ab}.$$

Distributivity for $\mathbb{Z}/m\mathbb{Z}$ then follows from distributivity for $\mathbb{Z}$. (There's something lurking in that definition of addition and multiplication that I want to come back to later, in Section 3.4. Do you see what it is?)

EXAMPLE 3.1.5. Working modulo $m=2$ gives two congruence classes: the elements of the congruence class $\overline{0}$ are the **even numbers**, those of the congruence class $\overline{1}$ are the **odd numbers**. The ring $\mathbb{Z}/2\mathbb{Z}$ is the binary ring (actually a field).

EXAMPLE 3.1.6. You might find it helps to think of the ring $\mathbb{Z}/12\mathbb{Z}$ as the "Ring of Time". It has twelve elements $\{\overline{0},\overline{1},\ldots,\overline{11}\}$ and we have, for instance, $\overline{10}+\overline{4}=\overline{14}=\overline{2}$. In other words "4 hours after 10 o'clock is 2 o'clock". We also have $\overline{3}\cdot\overline{8}=\overline{24}=\overline{0}$. This shows that in a ring it can sometimes happen that a product of two non-zero numbers is zero.

The construction of the ring $\mathbb{Z}/m\mathbb{Z}$ from the ring $\mathbb{Z}$ is an example of a general procedure called "taking quotients" or the "quotient construction", to be introduced in Section 3.6. As an example of its usefulness, I'll illustrate its use in a property of numbers you've probably known since you were a child.

PROPOSITION 3.1.7 (Divisibility by Sum). *A natural number is divisible by 3 (respectively 9) precisely when the sum of its digits is divisible by 3 (respectively 9).*

PROOF. I'll just prove the case for 9, and I'll prove it by example. You can work out the details yourself, and supply the case for 3.

Suppose the natural number is 12746. Write out its decimal expansion:

$$12746 = 1 \times 10^4 + 2 \times 10^3 + 7 \times 10^2 + 4 \times 10 + 6$$

Since 10 is congruent to 1 modulo 9 I deduce that

$$12746 \equiv 1 + 2 + 7 + 4 + 6 \pmod 9$$

The left hand side is divisible by 9 precisely when the right hand side is divisible by 9, proving the proposition. □

Variations of this lead to all sorts of other rules, such as:

EXERCISE 37. Show that: a natural number is divisible by 11 if and only if the alternating sum of its digits are divisible by 11.

EXERCISE 38. Show that: an integer of the form $abcabc$, such as 123123, is always divisible by 7.

EXERCISE 39. Show that: an integer congruent to 3 modulo 4 is never the sum of two squares. Show also that: an integer congruent to 7 modulo 8 is never the sum of three squares.

DEFINITION 3.1.8. *A* **field** *is a non-zero commutative ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$, that is an element a^{-1} with the property that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.*

So there you are.

REMARK 3.1.9. In France a field is called a **commutative field**. This is because there are lots of examples of rings that are not commutative but still have the property: for every non-zero element $a \in F$ there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. In English we call such a ring either a **skewfield** or a **division ring**; in France they are fields! The most famous example is the ring of **quaternions** which you will meet in due course.

EXAMPLE 3.1.10. The ring $\mathbb{Z}/3\mathbb{Z}$ is a field, which we have been calling $\mathbb{F}_3$. The ring $\mathbb{Z}/12\mathbb{Z}$ is not a field, because neither $\overline{3}$ nor $\overline{8}$ can be invertible as $\overline{3} \cdot \overline{8} = \overline{0}$.

PROPOSITION 3.1.11. *Let m be a positive integer. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.*

PROOF. Suppose that $\mathbb{Z}/m\mathbb{Z}$ is a field. Let $1 < a < m$ be an integer. Since $\overline{a}$ is non-zero in $\mathbb{Z}/m\mathbb{Z}$, its inverse $\overline{a}^{-1}$ exists. Take $b \in \mathbb{Z}$ such that $\overline{b} = \overline{a}^{-1}$, so that

$$\overline{ab} = \overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{a}^{-1} = \overline{1}$$

It follows that $ab = km+1$ for some integer k. Since a divides ab but does not divide 1, this identity shows that a cannot divide m. Thus m is prime.

Conversely, suppose that m is prime. Let $1 < a < m$ be an integer. The highest common factor (a, m) is 1 and so, by the Euclidean algorithm, there exists integers b and c such that

$$ab + mc = 1$$

In other words $\overline{a}\overline{b} = \overline{ab} = \overline{1}$, so that $\overline{a}$ is invertible. □

If p is a prime number we typically write $\mathbb{F}_p$ for the field $\mathbb{Z}/p\mathbb{Z}$ with p elements.

EXERCISE 40. Find the inverse of 24 in the field $\mathbb{F}_{37}$.

3.2. Properties of Rings

Whether or not you enjoy this section depends on your psychology. We need to derive some basic properties of rings, much like we did for vector spaces or like you must have done for groups in Fundamentals of Pure Mathematics. These derivations are all elementary. If you use your intuition from group theory and from the vector spaces, then watch out for Definition 3.2.12: this behaviour is critical in rings and is a residue of the fact that rings are not fields.

Let's get started! The following result is similar, but not the same, as the Lemmas 1.2.2, 1.2.3 and 1.2.4.

LEMMA 3.2.1 (Multiplying by zero and negatives (i.e. additive inverses)). *Let R be a ring and let $a, b \in R$. Then*

(1) $0a = 0 = a0$.
(2) $(-a)b = -(ab) = a(-b)$.
(3) $(-a)(-b) = ab$.

PROOF. (1) $0 = 0 + 0$. Therefore $0a = (0 + 0)a$, i.e. $0a = 0a + 0a$. Subtracting $0a$ from both sides we obtain $0 = 0a$. Similarly $a0 = 0$.

(2) Using Part (1) of this lemma gives $ab + (-a)b = (a + (-a))b = 0b = 0$. So by the uniqueness of negatives $(-a)b = -(ab)$. Similarly for $a(-b)$.

(3) Just follow your nose:

$$\begin{aligned} (-a)(-b) &= -(a(-b)) && \text{by (2)} \\ &= -(-(ab)) && \text{by (2)} \\ &= ab. \end{aligned}$$

□

REMARK 3.2.2. (1) The distributive axiom for rings has familiar and equally easily proved consequences such as

$$(a + b)(c + d) = ac + ad + bc + bd$$
$$a(b - c) = ab - ac$$

But remember, dear Reader, multiplication may not be commutative, so multiplicative factors must be kept in the correct order: ac may not equal ca.

(2) Suppose we have a ring R such that $1_R = 0_R$. Then R must be the zero ring. Why? Well, if $a \in R$ then $a = a \cdot 1_R = a \cdot 0_R = 0_R$. So 0_R is the only element of R.

DEFINITION 3.2.3. *Let $m \in \mathbb{Z}$. The m***–th multiple** ma **of an element** *a in an abelian group R is:*

$$ma = \underbrace{a + a + + \cdots + a}_{m \text{ terms}} \quad \text{if } m > 0$$

$0a = 0$, and negative multiples are defined by $(-m)a = -(ma)$.

LEMMA 3.2.4 (Rules for multiples). *Let R be a ring, let $a, b \in R$ and let $m, n \in \mathbb{Z}$. Then:*

(1) $m(a + b) = ma + mb$;
(2) $(m + n)a = ma + na$;

(3) $m(na) = (mn)a$;
(4) $m(ab) = (ma)b = a(mb)$;
(5) $(ma)(nb) = (mn)(ab)$.

PROOF. This is trivial and boring, so I will leave the details to you. In short, (2) and (3) are the index laws in the abelian group $(R, +)$. (1) comes from the definition of multiple and the fact that R is abelian under $+$. (4) and (5) are consequences of the distributivity law for R: when you fill out the details you'll experience tedium – the results have to be divided into cases $m > 0, m = 0, m < 0$ and similarly for n. □

REMARK 3.2.5. Does this remind you of Definition 1.2.1? The first three rules here are analogous to the first three axioms of a vector space. The difference is that we are only allowing multiplication by elements of $\mathbb{Z}$ instead of a field F. But at least it shows that you can try to use your intuition from scalar multiplication.

DEFINITION 3.2.6. *Let R be a ring. An element $a \in R$ is called a* ***unit*** *if it is* ***invertible*** *in R or in other words* **has a multiplicative inverse in** *R, meaning that there exists $a^{-1} \in R$ such that*

$$aa^{-1} = 1 = a^{-1}a.$$

EXAMPLE 3.2.7. In a field, such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, every non–zero element is a unit. In $\mathbb{Z}$ only 1 and -1 are units.

REMARK 3.2.8. It's obvious that the identity element 1 is *always* a unit, since $1^{-1} = 1$. It's similarly clear that if R is a non-zero ring, the element 0 is not a unit, since by Lemma 3.2.1(1) $0b = 0 \neq 1$ for all $b \in R$.

REMARK 3.2.9. In Physics, sadly, they have a completely different use of the word unit, indicating unit of measure. Following the discussion in Remark 1.6.6, a Mathematician thinks of their units as a basis element in a one-dimensional vector space over $\mathbb{R}$: for instance a second is a basis vector for the time-line, which I'll call $\vec{\mathbb{T}}$. The choice of basis vector produces an isomorphism $\mathbb{R} \xrightarrow{\sim} \vec{\mathbb{T}}$ thanks to Theorem 1.5.11, and so allows time to be measured by a real number. Of course, you should always make sure you know which meaning is intended.

PROPOSITION 3.2.10. *The set $R^\times$ of units in a ring R forms a group under multiplication.*

PROOF. Let $a, b \in R^\times$. So a, b are units and hence a^{-1} and b^{-1} exist in R. So $b^{-1}a^{-1}$ exists in R. Then $(ab)(b^{-1}a^{-1}) = abb^{-1}a = a1a^{-1} = aa^{-1} = 1$ and similarly $(b^{-1}a^{-1})(ab) = 1$. Therefore ab is a unit in R with $(ab)^{-1} = b^{-1}a^{-1}$, as usual. Thus $R^\times$ is closed under multiplication.

Multiplication in $R^\times$ is associative since multiplication in R is associative, and $1 \in R^\times$ is the identity element of $R^\times$. Finally, it is obvious that if $a \in R^\times$ then $a^{-1} \in R^\times$, thus verifying the group axioms. □

I will call $R^\times$ the **group of units of the ring** R.

EXAMPLE 3.2.11. $\mathbb{Z}^\times = \{1, -1\}$ and $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$. If $R = \mathsf{Mat}(n; F)$ then $R^\times = GL(n; F)$, the general linear group described in Section 2.2.

EXERCISE 41. Let p be a prime. Show that: $\mathbb{F}_p^\times$, the group of units of the field $\mathbb{F}_p$ where p is prime, is a cyclic group of order $p - 1$.

So far I presume you have been thinking this is quite abstract. Well, you're right, but as I hope we can discuss in a Workshop, Exercise 41 is the basis of the Diffie–Hellman key exchange, the mother and father of internet security! I'm pleased to be able to tell you that, because you will become ambassadors for Mathematics when you leave the university, whether you like it or not,

and I'd like you to see that most areas of mathematics can have a surprising utilitarian value, even if it is far from their raison d'être.

DEFINITION 3.2.12. *In a ring R a non–zero element a is called a **zero–divisor** or **divisor of zero** if there exists a non–zero element b such that either $ab = 0$ or $ba = 0$.*

Perfectly respectable rings can have zero-divisors: in $\mathsf{Mat}(2;\mathbb{R})$

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

so that both $\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ are zero–divisors. *Welcome to the zoo!* Mathematicians understand very well a ring like $\mathsf{Mat}(2;\mathbb{R})$ – after all, it can't be so hard, it's only a 4-dimensional $\mathbb{R}$-vector space. But the existence of zero–divisors makes it behave differently to most of the other examples you may have seen before. The ones you know so far tend, instead, to satisfy the following hypothesis:

DEFINITION 3.2.13. *An **integral domain** is a non–zero commutative ring that has no zero–divisors.*

In an integral domain there are no zero–divisors and therefore the laws

(1) $ab = 0 \Rightarrow a = 0$ or $b = 0$, and
(2) $a \neq 0$ and $b \neq 0 \rightarrow ab \neq 0$

hold. These properties may remind you of Lemma 1.2.4.

EXAMPLE 3.2.14. $\mathbb{Z}$ is an integral domain. Any field is an integral domain, since a unit in a ring R cannot be a zero–divisor. To see this, let R be a non–zero ring and let $a \in R^\times$ be a unit. Suppose that $ab = 0$ or $ba = 0$ for some $b \in R$. Multiplying on the left or on the right respectively by a^{-1} shows that $a^{-1}ab = a^{-1}0$ or $baa^{-1} = 0a^{-1}$, so in both cases $b = 0$.

EXAMPLE 3.2.15. The ring $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain, since $\overline{3} \cdot \overline{8} = \overline{0}$.

PROPOSITION 3.2.16 (Cancellation Law for Integral Domains). *Let R be an integral domain and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$.*

PROOF. If $ab = ac$ then $a(b - c) = 0$ so that either $a = 0$ or $b - c = 0$, that is either $a = 0$ or $b = c$. □

This Law fails for rings that are not integral domains. For instance, in $R = \mathbb{Z}/12\mathbb{Z}$, there is the equality

$$\overline{8} \cdot \overline{2} = \overline{8} \cdot \overline{5}.$$

We will now reprove Proposition 3.1.11 as a special case of a general theorem

PROPOSITION 3.2.17. *Let m be a natural number. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.*

PROOF. Suppose m is prime. Obviously $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring. Suppose that $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ is a divisor of zero. Then $\overline{k} \neq \overline{0}$ and there exists $\overline{\ell} \in \mathbb{Z}/m\mathbb{Z}$ with $\overline{\ell} \neq \overline{0}$ and $\overline{k} \cdot \overline{\ell} = \overline{0}$. Then

$$k\ell \equiv 0 \pmod{m},$$

so that m divides $k\ell$. Since m is prime it follows that m divides k or m divides ℓ, i.e. $k \equiv 0$ mod m or $\ell \equiv 0$ mod m and hence $\overline{k} = \overline{0}$ or $\overline{\ell} = \overline{0}$, a contradiction. So $\mathbb{Z}/m\mathbb{Z}$ has no divisors of zero and is an integral domain.

Suppose now that m is not prime. Then $m = k\ell$ for some integers k, ℓ with $1 < k, \ell < m$. Then k and ℓ are not divisible by m so that $\overline{k} \neq \overline{0}$, $\overline{\ell} \neq \overline{0}$. But $\overline{k\ell} = \overline{k\ell} = \overline{m} = \overline{0}$. So $\overline{k}$ and $\overline{\ell}$ are divisors of zero and $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain. □

THEOREM 3.2.18. *Every **finite** integral domain is a field.*

PROOF. Let R be a finite integral domain. To prove that R is a field what we need to show is that every non–zero element is invertible.

Let a be a non–zero element of R and define the mapping $\lambda_a : R \to R$ by $\lambda_a(b) = ab$ for all $b \in R$. If $\lambda_a(b_1) = \lambda_a(b_2)$ for some $b_1, b_2 \in R$ then $ab_1 = ab_2$. Since $a \neq 0$ the cancellation law for integral domains yields $b_1 = b_2$. This means that λ_a is injective. Since R is finite it follows automatically that λ_a must also be surjective.

In particular $1 \in \operatorname{im} \lambda_a$, meaning that there exists $b \in R$ with $1 = \lambda_a(b) = ab$. Since R is an integral domain, multiplication is commutative and we have $ba = 1$ as well. Therefore a is invertible, with inverse b. □

Proposition 3.1.11 follows immediately.

3.3. Polynomials

DEFINITION 3.3.1. *Let R be a ring. A* **polynomial over** *R is an expression of the form*

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

for some non–negative integer m and elements $a_i \in R$ for $0 \leqslant i \leqslant m$. The set of all polynomials over R is denoted by $R[X]$. In case a_m is non–zero, the polynomial P has **degree** *m, written $\deg(P)$, and a_m is its* **leading coefficient**. *When the leading coefficient is 1 the polynomial is a* **monic polynomial**. *A polynomial of degree one is called* **linear**, *a polynomial of degree two is called* **quadratic**, *and a polynomial of degree three is called* **cubic**.

You will see that I have used X for the variable, but I could use other letters sometimes, although they will usually be capital letters from the end of the alphabet.

Polynomials are added and multiplied as follows:

$$(a_0 + a_1X + \cdots + a_mX^m) + (b_0 + b_1X + \cdots + b_nX^n) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots$$

and

$$\begin{aligned}(a_0 + a_1X + \quad \cdots \quad &+a_mX^m)(b_0 + b_1X + \cdots + b_nX^n) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + a_mb_nX^{m+n}\end{aligned}$$

where $m, n \geqslant 0, a_i, b_j \in R$ for $0 \leqslant i \leqslant m$ and $0 \leqslant j \leqslant n$.

DEFINITION 3.3.2. *With these definitions the set $R[X]$ becomes a ring called the* **ring of polynomials with coefficients in** *R,* **or over** *R. The zero and the identity of $R[X]$ are the zero and identity of R, respectively.*

Remarks: The elements of R can be identified with polynomials of degree 0. I will call these polynomials **constant**. *You should notice from the multiplication rule that if R is commutative, then so too is $R[X]$.*

You might ask why one would want to study polynomial rings with coefficients from an arbitrary ring R. One good reason is that polynomials in more one than variable play an important rôle in many areas of mathematics, and particularly in Algebraic Geometry. An example of a cubic polynomial in two variables is $Y^2 - X^3 - X - 1$; usually I would write this belongs to $\mathbb{C}[X, Y]$. But sometimes it is useful to prove properties of polynomial rings in several variables by induction: to do this I identify $\mathbb{C}[X, Y]$ with $R[X]$ where $R = \mathbb{C}[Y]$ and then try to show that a property that R has can be inherited by $R[X]$. You've just seen this: if R is commutative then so too is $R[X]$. Lemma 3.3.3 below gives another example of this behaviour: if R is an integral domain then so too is $R[X]$.

LEMMA 3.3.3. *(i) If R is a ring with no zero-divisors, then $R[X]$ has no zero-divisors and $\deg(PQ) = \deg(P) + \deg(Q)$ for non-zero $P, Q \in R[X]$.*
(ii) If R is an integral domain then so is $R[X]$.

PROOF. (i) If R has no zero-divisors then the leading coefficient of the product PQ is the product of the leading coefficients of P and of Q, so that $PQ \neq 0$ if and only if $P \neq 0$ and $Q \neq 0$.
(ii) Immediate from the observation that if R is commutative then so is $R[X]$, and from (i). □

EXERCISE 42. Show that: if R is an integral domain then $R[X]^\times = R^\times$. Show by counterexample that this is false if R is not an integral domain.

THEOREM 3.3.4 (Division and Remainder). *Let R be an integral domain and let $P, Q \in R[X]$ with Q monic. Then there exists unique $A, B \in R[X]$ such that $P = AQ + B$ and $\deg(B) < \deg(Q)$ or $B = 0$.*

PROOF. I begin by choosing a polynomial A that makes $\deg(P - AQ)$ as small as possible. Since the degree is a non-negative integer this is always possible. Suppose that $\deg(P - AQ) \geqslant \deg(Q)$, say $P - AQ = a_r X^r + \cdots + a_0$ with $a_r \neq 0$ and $r \geqslant d = \deg(Q)$. Then $P - (A + a_r X^{r-d})Q$ has smaller degree than $P - AQ$, contradicting my original choice of A. So it must be that $P - AQ$ has degree strictly less than the degree of Q. This shows the existence of an A and a $B = P - AQ$ as in the statement of the theorem.

I have also claimed that both A and B are unique, so let's check that now. Suppose that A' and B' also satisfy the conclusions of the theorem, that is $P = A'Q + B'$ with $\deg(B') < d$. Then

$$0 = P - P = (A - A')Q + (B - B')$$

so that $(A - A')Q = B' - B$. But $(B' - B)$ has degree strictly less than d, while $(A - A')Q$ has degree greater than or equal to d, unless $A - A' = 0$ (cf Lemma 3.3.3). I deduce that $A = A'$ and from this it follows that $B = P - AQ = P - A'Q = B'$ too. □

EXAMPLE 3.3.5. The above proof is not only pretty slick, but, if you look closely, it also tells you how to divide in practice, finding A and B. It's a variation on long division of integers. Here's an example for polynomials with real coefficients. Let $P = X^5 - 7X^4 - 16X^3 - 17X + 2$ and $Q = X^3 - 5X + 4$. Then

$$\begin{aligned} X^5 - 7X^4 - 16X^3 - 17X + 2 &= X^2(X^3 - 5X + 4) - 7X^4 - 11X^3 - 4X^2 - 17X + 2 \\ &= X^2(X^3 - 5X + 4) - 7X(X^3 - 5X + 4) - 11X^3 - 39X^2 + 11X + 2 \\ &= (X^2 - 7X - 11)(X^3 - 5X + 4) - 39X^2 - 44X + 46 \end{aligned}$$

So $A = X^2 - 7X - 11$ and $B = -39X^2 - 44X + 46$.

DEFINITION 3.3.6. *Let R be a commutative ring and $P \in R[X]$ a polynomial. Then the polynomial P can be* **evaluated** *at the element $\lambda \in R$ to produce $P(\lambda)$ by replacing the powers of X in the polynomial P by the corresponding powers of λ. In this way we have a mapping*

$$R[X] \to \mathrm{Maps}(R, R)$$

This is the precise mathematical description of thinking of a polynomial as a function. An element $\lambda \in R$ is a **root** *of P is $P(\lambda) = 0$.*

EXAMPLE 3.3.7. Let $R = \mathbb{C}$ and $P = X^3 + 1$. Then $\pi \in \mathbb{C}$ and $P(\pi) = \pi^3 + 1 \in \mathbb{C}$. The complex number $e^{2\pi\sqrt{-1}/3}$ is a root of P.

EXAMPLE 3.3.8. Let $R = \mathbb{R}[Y]$ and $P = (Y^2 + 1)X^2 - (Y^3 + 2Y^2 + Y)X - 2Y - 4 \in R[X]$. Then

$$P(Y + 2) = (Y^2 + 1)(Y + 2)^2 - (Y^3 + 2Y^2 + Y)(Y + 2) - 2Y - 4 = 0$$

so that $Y + 2 \in R$ is a root of P.

EXERCISE 43. Show that: the mapping $R[X] \to \mathrm{Maps}(R, R)$ from Definition 3.3.6 is not injective when $R = \mathbb{F}_p$, p a prime. Hint: Fermat's Little Theorem. (This means that in general, even over fields, a polynomial is not just a special type of function!)

PROPOSITION 3.3.9. *Let R be a commutative ring, let $\lambda \in R$ and $P(X) \in R[X]$. Then λ is a root of $P(X)$ if and only if $(X - \lambda)$ divides $P(X)$.*

PROOF. If $X - \lambda$ divides $P(X)$ then $P(X) = (X - \lambda)Q(X)$ for some $Q(X) \in R[X]$ and

$$P(\lambda) \;=\; 0 \cdot Q(\lambda) \;=\; 0 \in R\,.$$

Conversely, suppose $P(X) = \sum_{k=0}^{n} a_k X^k \in R[X]$ is such that $P(\lambda) = 0 \in R$. For any $k \geqslant 0$

$$X^k - \lambda^k \;=\; \begin{cases} (X-\lambda)\sum_{j=0}^{k-1} \lambda^j X^{k-j-1} & \text{if } k \geqslant 1 \\ 0 & \text{if } k = 0 \end{cases} \in R[X]\,,$$

so that

$$\begin{aligned} P(X) &= P(X) - P(\lambda) \\ &= \sum_{k=0}^{n} a_k X^k - \sum_{k=0}^{n} a_k \lambda^k \\ &= (X-\lambda)\Big(\sum_{k=1}^{n} a_k \Big(\sum_{j=0}^{k-1} \lambda^j X^{k-j-1}\Big)\Big) \in R[X]\,, \end{aligned}$$

so that $(X - \lambda)$ divides $P(X)$. □

This has a pleasant consequence.

THEOREM 3.3.10. *Let R be a field, or more generally an integral domain. Then a non-zero polynomial $P \in R[X] \smallsetminus \{0\}$ has at most $\deg(P)$ roots in R.*

PROOF. Suppose that $\lambda_1, \ldots, \lambda_m$ are distinct roots of P in R. By Proposition 3.3.9 $P = A(X - \lambda_1)$ for some $A \in R[X]$ with $\deg(A) = \deg(P) - 1$ by Lemma 3.3.3. Evaluating this equality at λ_i with $i \geqslant 2$ gives an equality in R: $0 = P(\lambda_i) = A(\lambda_i)(\lambda_i - \lambda_1)$. Since $\lambda_i - \lambda_1$ is not zero and R is an integral domain, it follows that $A(\lambda_i) = 0$ and $\lambda_2, \ldots, \lambda_m$ are distinct roots of A. The theorem follows by induction. □

DEFINITION 3.3.11. *A field F is* **algebraically closed** *if each non-constant polynomial $P \in F[X] \backslash F$ with coefficients in our field has a root in our field F.*

EXAMPLE 3.3.12. The field of real numbers, $\mathbb{R}$, is not algebraically closed. For instance, $X^2 + 1$ has no root in $\mathbb{R}$.

THEOREM 3.3.13 (Fundamental Theorem of Algebra). *The field of complex numbers, $\mathbb{C}$, is algebraically closed.*

There are a lot of proofs of this absolutely basic result: see this Mathoverflow question and this Wikipedia entry. Probably the most elementary is by complex analysis and you will meet it in Honours Complex Variables. Isn't it a beautiful thing how different mathematical topics are interwoven?

THEOREM 3.3.14. *If F is an algebraically closed field, then every non-zero polynomial $P \in F[X] \backslash \{0\}$* **decomposes into linear factors**

$$P = c(X - \lambda_1) \cdots (X - \lambda_n)$$

with $n \geqslant 0, c \in F^\times$ and $\lambda_1, \ldots, \lambda_n \in F$. This decomposition is unique up to reordering the factors.

PROOF. If P is a constant polynomial, there is nothing to show. So assume that P is not constant. Since F is algebraically closed P has a root $\lambda_1 \in F$. By Proposition 3.3.9 $P = A(X - \lambda_1)$. Now induct on $\deg(P)$. □

3.4. Homomorphisms, Ideals and Subrings

To venture further into the jungle of rings, we need to add ring homomorphisms to our toolkit. These are easy to define – I hope you can already guess the definition – but they lead us inevitably to subrings and to ideals. Subrings and ideals are similar to subgroups and normal subgroups from Fundamentals of Pure Mathematics, and they play a key role in a great deal of algebra.

DEFINITION 3.4.1. *Let R and S be rings. A mapping $f : R \longrightarrow S$ is a **ring homomorphism** if the following hold for all $x, y \in R$:*

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y) \end{aligned}$$

EXAMPLE 3.4.2. The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is a ring homomorphism.

EXAMPLE 3.4.3. For each $m \in \mathbb{Z}$, the mapping $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $f(a) = \overline{a}$ is a ring homomorphism.

EXERCISE 44. Let R be a commutative ring and $\lambda \in R$. The mapping $f : R[X] \to R$ defined by $f(P) = P(\lambda)$ for all $P \in R[X]$, as defined in Definition 3.3.6, is a ring homomorphism.

EXERCISE 45. Let R be a commutative ring, n a positive integer and $M \in \mathsf{Mat}(n; R)$. The mapping $f : R[X] \to \mathsf{Mat}(n; R)$ defined by

$$f(a_t X^t + a_{t-1}X^{t-1} + \cdots + a_1 X + a_0) = a_t M^t + a_{t-1}M^{t-1} + \cdots + a_1 M + a_0$$

is a ring homomorphism. You used this in the second exercise of the second Workshop.

REMARK 3.4.4.

(1) As usual, a homomorphism is simply a mapping that "preserves the structure". Rings have the operations of addition and multiplication and I ask that these are preserved; vector spaces have addition and scalar multiplication and a linear mapping must preserve these.

(2) However, the definition of a ring R 3.1.1 includes the requirement that R have an identity element $1 = 1_R \in R$, but the definition of a ring homomorphism 3.4.1 $f : R \to S$ does not require that $f(1_R) = 1_S \in S$. For example, the zero function $0 : R \to S; x \mapsto 0$ is a ring homomorphism. The element $f(1_R) \in S$ is an idempotent, meaning that $f(1_R)^2 = f(1_R) \in S$ (Exercise 23) or equivalently such that $f(1_R)(f(1_R) - 1_S) = 0_S \in S$. Thus if S has no zero-divisors either $f(1_R) = 0_S$ (in which case $f = 0$ is the zero ring homomorphism) or $f(1_R) = 1_S$.

(3) In Fundamentals of Pure Mathematics you saw that a group homomorphism had to preserve the group multiplication. Once you understand this pattern, its pays off handsomely to observe the similarities and differences that occur in examples of homomorphisms: this leads to Category Theory which is a profound and powerful way of viewing swathes of mathematics, and whose influence is increasing.

(4) Given the above, you know that you already know that an isomorphism is used in the same way for ring homomorphisms as for linear mappings or group homomorphisms, including the notation $\cong$ for isomorphism between two rings.

(5) As you did in Exercise 8 and Exercise 9 for linear mappings, it is easy to check that the composition of two ring homomorphisms is a ring homomorphism, and that the inverse of a ring isomorphism is a ring isomorphism.

If you temporarily ignore multiplication, a ring homomorphism is a group homomorphism between rings, regarded as groups under addition. So Group Theory gives:

LEMMA 3.4.5. *Let R and S be rings and $f : R \to S$ a ring homomorphism. Then for all $x, y \in R$ and $m \in \mathbb{Z}$:*

(1) $f(0_R) = 0_S$, where 0_R and 0_S are the zeros of R and S respectively;
(2) $f(-x) = -f(x)$;
(3) $f(x - y) = f(x) - f(y)$;
(4) $f(mx) = mf(x)$,

where mx denotes the m-th multiple of x, as in Definition 3.2.3.

REMARK 3.4.6. (1) It is easy to deduce from the multiplicative property of a ring homomorphism that

$$f(x)^n = (f(x))^n$$

for all $x \in R$ and $n \in \mathbb{N}$.

(2) But, dear Reader, you do need to tread carefully around the behaviour of identity elements under ring homomorphisms. Examples 3.4.2–3.4.3 and Exercises 44–45 all have the property that $f(1_R) = 1_S$, but this need not always be true. It is possible to find rings R, S and a ring homomorphism $f : R \to S$ such that $f(1_R) \neq 1_S$. An example is $f : \mathbb{R} \to \mathsf{Mat}(2; \mathbb{R})$ defined by

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{for all } x \in \mathbb{R}.$$

Now I arrive at the first necessary consequence of ring homomorphisms. I hope you are already convinced of the importance of the image and kernel for homomorphisms. You spent considerable time on this in Fundamentals of Pure Mathematics, and in this course an early highlight has been the Rank Nullity Theorem. So what are kernels and images for ring homomorphisms? The annoying thing is that they are probably not *exactly* what you first think them to be.

First we take kernels.

DEFINITION 3.4.7. *A subset I of a ring R is an **ideal**, written $I \trianglelefteq R$, if the following hold:*

(1) $I \neq \emptyset$;
(2) I is closed under subtraction;
(3) for all $i \in I$ and $r \in R$ we have $ri, ir \in I$.

*Condition (3) says that I **is closed under multiplication by elements of** R.*

EXAMPLE 3.4.8. In any ring R, $\{0\}$ and R are ideals of R. Condition (3) in Definition 3.4.7 holds for $\{0\}$ because $r0 = 0r = 0 \in \{0\}$ thanks to Lemma 3.2.1.1.

EXAMPLE 3.4.9. The set $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Condition (3) in Definition 3.4.7 holds because $b(ma) = (ma)b = m(ab) \in m\mathbb{Z}$ for all $a, b \in \mathbb{Z}$.

EXAMPLE 3.4.10. The set

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} : b, d \in \mathbb{R} \right\} \subset \mathsf{Mat}(2; \mathbb{R})$$

is not an ideal. It fails Condition (3) in Definition 3.4.7: although it is true that $ri \in I$ for all $i \in I$ and $r \in R$, it is not true that $ir \in I$ for all $i \in I$ and $r \in R$. For instance:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin I$$

As for vector spaces in Proposition 1.4.5, there is a cheap but useful way to construct ideals.

DEFINITION 3.4.11. *Let R be a commutative ring and let $T \subset R$. Then the* **ideal of R generated by** *T is the set*

$$ {}_R\langle T\rangle = \{r_1t_1 + \cdots + r_mt_m : t_1, \ldots, t_m \in T, r_1, \ldots, r_m \in R\}, $$

together with the zero element in the case $T = \emptyset$. If $T = \{t_1, \ldots, t_n\}$, a finite set, I will often abuse notation by writing ${}_R\langle t_1, \ldots, t_n\rangle$ instead of ${}_R\langle\{t_1, \ldots, t_n\}\rangle$.

EXAMPLE 3.4.12. Let $m \in \mathbb{Z}$. Then ${}_{\mathbb{Z}}\langle m\rangle = m\mathbb{Z}$.

EXAMPLE 3.4.13. Let $P \in \mathbb{R}[X]$. Then ${}_{\mathbb{R}[X]}\langle P\rangle = \{AP : A \in \mathbb{R}[X]\} = \{Q : P \text{ divides } Q \text{ in } \mathbb{R}[X]\}$.

PROPOSITION 3.4.14. *Let R be a commutative ring and let $T \subseteq R$. Then ${}_R\langle T\rangle$ is the smallest ideal of R that contains T.*

PROOF. The Proposition contains two claims: the first that ${}_R\langle T\rangle$ is an ideal of R; the second that it is the smallest such ideal. This is just as clear as the proof of Proposition 1.4.5, and follows also from Lemma 3.4.21. Let me give a few details.

To prove that ${}_R\langle T\rangle$ is an ideal, note first that it is non-empty since $0_R \in {}_R\langle T\rangle$. Given two arbitrary elements $r_1t_1+\cdots+r_mt_m, r'_1t'_1+\cdots+r'_nt'_n \in {}_R\langle T\rangle$ their difference equals $r_1t_1+\cdots+r_mt_m+(-r'_1)t'_1+\cdots+(-r'_n)t'_n$ which is in ${}_R\langle T\rangle$ by definition. Finally, if $r \in R$ then $r(r_1t_1 + \cdots + r_mt_m) = (rr_1)t_1 + \cdots + (rr_m)t_m \in I$ and similarly for right multiplication by r.

For minimality, observe that if I is an ideal and $t_1, \ldots, t_m \in I$ then necessarily $r_1t_1 + \cdots + r_mt_m \in I$. □

DEFINITION 3.4.15. *Let R be a commutative ring. An ideal I of R is called a* ***principal ideal*** *if $I = \langle t\rangle$ for some $t \in R$.*

EXAMPLE 3.4.16. $\{0\}$ and R are always principal ideals in a commutative ring, generated by the element 0 and the element 1_R respectively.

You'll find out later that it is a difficult but important problem to decide whether an ideal is a principal ideal or not. Every ideal of $\mathbb{C}[X]$ is principal; conversely there are ideals in the polynomial ring $\mathbb{C}[X, Y]$ that are not principal.

Now I'm going to show you why ideals are necessary, fundamental and unavoidable:

DEFINITION 3.4.17. *Let R and S be rings with zero elements 0_R and 0_S respectively and let $f : R \to S$ be a ring homomorphism. Since f is in particular a group homomorphism from $(R, +)$ to $(S, +)$, the* ***kernel*** *of f already has a meaning:*

$$ \ker f = \{r \in R : f(r) = 0_S\}. $$

PROPOSITION 3.4.18. *Let R and S be rings and $f : R \to S$ a ring homomorphism. Then $\ker f$ is an ideal of R.*

PROOF. You saw in Fundamentals of Pure Mathematics that $\ker f$ is a subgroup of $(R, +)$. So that gives Conditions (1) and (2) in Definition 3.4.7. All that I have left to prove is that if $k \in \ker f$ and $r \in R$, then $kr, rk \in \ker f$. But this is clear to you and me:

$$ f(kr) = f(k)f(r) = 0_Sf(r) = 0_S \qquad \text{and} \qquad f(rk) = f(r)f(k) = f(r)0_S = 0_S. $$

□

EXAMPLE 3.4.19. Let $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the homomorphism of Example 3.4.3. Then

$$ \ker f = \{a \in \mathbb{Z} : f(a) = \overline{0}\} = \{a \in \mathbb{Z} : a \text{ divisible by } m\} = m\mathbb{Z}. $$

There are some easy-to-prove results about ideals and kernels that you have seen for vector spaces (see Lemma 1.8.2, Exercise 4 and Exercise 2) or for groups. I'm going to write them out but not prove them: their proofs are obtained by modifying the proofs you already know in those other cases, so there's no point sentencing you to twenty year's of boredom; there are far more interesting things to be thinking about.

LEMMA 3.4.20. *f is injective if and only if* $\ker f = \{0\}$.

LEMMA 3.4.21. *The intersection of any collection of ideals of a ring R is an ideal of R.*

LEMMA 3.4.22. *Let I and J be ideals of a ring R. Then*

$$I + J = \{a + b : a \in I, b \in J\}$$

is an ideal of R.

Then we take images.

DEFINITION 3.4.23. *Let R be a ring. A subset R' of R is a **subring** of R if R' itself is a ring under the operations of addition and multiplication defined in R.*

EXAMPLE 3.4.24. In any ring R, $\{0\}$ and R are subrings.

EXERCISE 46. $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. This subring is called the ring of **Gaussian integers**. It is fundamental in elementary Number Theory.

EXAMPLE 3.4.25. If F is a field, then for any $m, n \in \mathbb{N}$ with $m \leqslant n$ $\mathsf{Mat}(m; F)$ is a subring of $\mathsf{Mat}(n; F)$. How? Well consider $\mathsf{Mat}(m; F)$ as the subset of $\mathsf{Mat}(n; F)$ all of whose entries beyond the m-th column or below the m-th row are zero.

If you ever need to decide whether or not a subset R' of a ring R is a subring, I'd suggest that you use the following!

PROPOSITION 3.4.26 (Test for a subring). *Let R' be a subset of a ring R. Then R' is a subring if and only if*

(1) R' has a multiplicative identity, and
(2) R' is closed under subtraction: $a, b \in R' \to a - b \in R'$, and
(3) R' is closed under multiplication.

PROOF. If R' is a subring then its obvious that (1), (2), (3) hold.

Conversely suppose (1), (2) and (3) hold. By (1) and (2) and the subgroup test for a group from Fundamentals of Pure Mathematics, R' under addition is a subgroup of R and therefore an abelian group. The associative law for multiplication holds for elements of R' since it holds for elements of R. That, coupled with (1) and (3), proves that R' is a monoid under multiplication. Finally, the distributive laws hold for elements of R' since they hold for elements of R.

It follows that R' is a ring, and therefore a subring of R. □

EXAMPLE 3.4.27. Suppose that I is an ideal of R. Then it is usually not a subring of R. For although it satisfies Properties (2) and (3) in Proposition 3.4.26, it may well fail Property (1). For instance, $m\mathbb{Z}$ has a multiplicative identity if and only if $m = 0$ or 1.

REMARK 3.4.28. At the risk of being tedious, dear Reader, let me point out that for subrings you need tread carefully around the identity elements of a ring and a subring. Just because R' is a subring of R does not mean that 1_R and $1_{R'}$ are equal. For a counterexample to equality, see Example 3.4.25.

PROPOSITION 3.4.29. *Let R and S be rings and $f : R \longrightarrow S$ a ring homomorphism.*

(1) *If R' is a subring of R then $f(R')$ is a subring of S. In particular,* $\operatorname{im} f$ *is a subring of S.*
(2) *Assume that $f(1_R) = 1_S$. Then if x is a unit in R, $f(x)$ is a unit in S and $(f(x))^{-1} = f(x^{-1})$. In this case f restricts to a group homomorphism $f|_{R^\times} : R^\times \to S^\times$.*

PROOF. (1) This follows easily from the Test for a Subring.
(2) If $x \in R^\times$ then x^{-1} exists and

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(1_R) = 1_S$$

and similarly $f(x^{-1})f(x) = 1_S$ so that $f(x) \in S^\times$ with inverse $f(x^{-1})$. □

REMARK 3.4.30. It is *not* true that the intersection of two subrings of R is a subring of R. For example, let

$$R' = \left\{ \begin{pmatrix} a & b & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{pmatrix} : a, b \in \mathbb{Q} \right\}, \qquad R'' = \left\{ \begin{pmatrix} c & d & e \\ 0 & c & f \\ 0 & 0 & c \end{pmatrix} : c, d, e, f \in \mathbb{Q} \right\}.$$

Then R', R'' are both subrings of $\mathsf{Mat}(3; \mathbb{Q})$, but their intersection $R' \cap R''$ is not since it does not have an identity.

3.5. Equivalence Relations

This is a short section, you have met this material in Proofs and Problem Solving. I will use the material in the section on factor rings and I will also give here the avatar for the first isomorphism theorem, which you will meet properly in that section too.

DEFINITION 3.5.1. *A* **relation** *R on a set X is a subset $R \subseteq X \times X$. In this context, and only in this context, instead of writing $(x, y) \in R$, I will write xRy. Then R is an* **equivalence relation on** *X when for all elements $x, y, z \in X$ the following hold:*

(1) **Reflexivity***: xRx;*
(2) **Symmetry***: $xRy \Leftrightarrow yRx$;*
(3) **Transitivity***: $(xRy$ and $yRz) \to xRz$.*

EXAMPLE 3.5.2. Let F be a field and n a positive integer. Define $\simeq$ to be the relation of **conjugacy** on $\mathsf{Mat}(n; F)$: $A \simeq B$ if and only if there exists an invertible matrix $X \in \mathsf{Mat}(n; F)$ such that $B = XAX^{-1}$. Then $\simeq$ is an equivalence relation. This is obvious! $A \simeq A$ using $X = I_n$; if $A \simeq B$ then there exists invertible X with $B = XAX^{-1}$ so that $A = X^{-1}BX$; finally if $A \simeq B$ and $B \simeq C$ then there exist invertible X and Y with $B = XAX^{-1}$ and $C = YBY^{-1}$. It follows that $C = (YX)A(YX)^{-1}$, so that $A \simeq C$.

EXERCISE 47. Show that: the relation $\approx$ on $\mathsf{Mat}(n \times m; F)$, defined by $A \approx B$ if there exist $P \in GL(n; F)$ and $Q \in GL(m; F)$ such that $B = PAQ$, is an equivalence relation.

EXERCISE 48. Show that: isomorphism is an equivalence relation on finite dimensional vector spaces over a field F.

DEFINITION 3.5.3. *Suppose that $\sim$ is an equivalence relation on a set X. For $x \in X$ the set $E(x) := \{z \in X : z \sim x\}$ is called the* **equivalence class of** *x. A subset $E \subseteq X$ is called an* **equivalence class** *for our equivalence relation if there is an $x \in X$ for which $E = E(x)$. An element of an equivalence class is called a* **representative** *of the class. A subset $Z \subseteq X$ containing precisely one element from each equivalence class is called a* **system of representatives** *for the equivalence relation.*

As you know: reflexivity gives $x \in E(x)$, from which it follows easily that for $x, y \in X$ the following are equivalent:

(1) $x \sim y$;

(2) $E(x) = E(y)$;
(3) $E(x) \cap E(y) \neq \emptyset$.

EXAMPLE 3.5.4. Given an integer $m \in \mathbb{Z}$, let $\equiv$ be the relation on $\mathbb{Z}$ of "congruence modulo m" from Example 3.1.4. This is an equivalence relation where I denoted the equivalence classes $E(x)$ by $\overline{x}$ in Example 3.1.4. If m is positive, then $\{0, 1, \ldots, m-1\}$ is a system of representatives, as is $\{a, a+1, \ldots, a+m-1\}$ for any integer a.

EXERCISE 49. Show that: the $(n \times m)$-matrices over F in Smith Normal Form form a system of representatives for the equivalence relation of Exercise 47.

EXERCISE 50. Show that: The set $\{F^n : n \in \mathbb{Z}_{\geqslant 0}\}$ is a system of representatives for the equivalence relation of Exercise 48. Show that: $\{F[X]_{<n} : n \in \mathbb{Z}_{\geqslant 0}\}$ is another system of representatives for the equivalence relation of Exercise 48.

DEFINITION 3.5.5. *Given an equivalence relation $\sim$ on the set X I will denote the* **set of equivalence classes**, *which is a subset of the power set $\mathcal{P}(X)$, by*

$$(X/\sim) := \{E(x) : x \in X\}$$

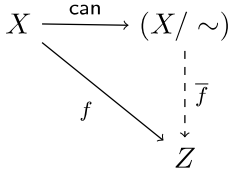
There is a canonical mapping $\mathsf{can} : X \to (X/\sim), x \mapsto E(x)$. *It is obviously a surjection.*

Here are some examples of equivalence relations on a set X with an algebraic structure such that the set of equivalence classes $X/\sim$ has the same algebraic structure and the canonical mapping $\mathsf{can} : X \to (X/\sim)$ is a surjective homomorphism preserving the structure:

(1) Given an abelian group A and a subgroup $B \subseteq A$ define an equivalence relation $\sim$ on A by $x \sim y$ if $x - y \in B$, so that the equivalence class of $x \in A$ is $E(x) = B + x = \{b + x \,|\, b \in B\} \subseteq A$. The quotient set $A/\sim = A/B$ is an abelian group with $E(x)+E(y) = E(x+y)$, and $\mathsf{can} : A \to A/B$ is a surjective homomorphism of abelian group with kernel $\mathsf{can}^{-1}(0) = B$. The abelian group A/B is the **quotient abelian group** of A by the subgroup H.
(2) Given a group G and a normal subgroup $H \subseteq G$ define an equivalence relation $\sim$ on G by $x \sim y$ if $xy^{-1} \in H$, so that the equivalence class of $x \in G$ is the coset $E(x) = xH = Hx \subseteq G$. The quotient set $G/\sim = G/H$ is a group with $E(x)E(y) = E(xy)$, and $\mathsf{can} : G \to G/H$ a surjective homomorphism of groups with kernel $\mathsf{can}^{-1}(1) = H$. ((1) is just the abelian version). The group G/H is the **quotient group** of G by the normal subgroup H. Lagrange's Theorem: if G is finite then
$$|G| = |H|\,|G/H|\,,$$
which is proved by noting that each coset $E(x)$ has exactly $|H|$ elements, and that G is the disjoint union of $|G/H|$ cosets.
(3) Given an F-vector space V and a subspace $W \subseteq V$ define an equivalence relation $\sim$ on V by $x \sim y$ if $x - y \in W$, so that the equivalence class of $x \in V$ is the subset $E(x) = W + x \subset V$ (exactly as in (a)). The quotient set $V/\sim = V/W$ is an F-vector space with $\lambda E(x) = E(\lambda x)$ $(\lambda \in F)$, and $\mathsf{can} : V \to V/W$ a surjective linear map with kernel $\mathsf{can}^{-1}(0) = W$. The vector space V/W is the **quotient vector space** of V by the subspace W. If V is finite-dimensional then so are W and V, and by Example 58 below
$$\dim(V/W) = \dim(V) - \dim(W)\,.$$
(4) In Section 3.6 below we shall consider the equivalence relations $\sim$ on rings R such that the quotient $R/\sim$ is a ring and the canonical mapping $\mathsf{can} : R \to (R/\sim)$ is a surjective homomorphism of rings.

EXAMPLE 3.5.6. Let $\equiv$ be the equivalence relation on $\mathbb{Z}$ of "congruence modulo m" from Example 3.5.4. Then $(\mathbb{Z}/\equiv) = \mathbb{Z}/m\mathbb{Z}$.

A very important Remark! Suppose that $\sim$ is an equivalence relation on X. If $f : X \to Z$ is a mapping with the property that $x \sim y \to f(x) = f(y)$, then there is a unique mapping $\overline{f} : (X/\sim) \to Z$ with $f = \overline{f} \circ \mathsf{can}$. Its definition is easy: $\overline{f}(E(x)) = f(x)$. This property is called the **universal property of the set of equivalence classes**.



Now suppose that $f : X \to Z$ is an arbitrary mapping. I can define a relation on X by $x \sim y \Leftrightarrow f(x) = f(y)$. It is trivial to check that this is an equivalence relation (do it!). Moreover

$$\overline{f} : (X/\sim) \xrightarrow{\sim} \operatorname{im} f \tag{5}$$

is a bijection where, as usual, $\operatorname{im} f = \{f(x) : x \in X\}$. This bijection is the avatar of the first isomorphism theorem.

DEFINITION 3.5.7. *I say that $g : (X/\sim) \to Z$ is* **well-defined** *if I can find a mapping $f : X \to Z$ such that f has the property $x \sim y \to f(x) = f(y)$ and $g = \overline{f}$.*

EXERCISE 51. Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by $(x, y) \sim (a, b) \Leftrightarrow x + b = y + a$.

(a) Show that: $\sim$ is an equivalence relation.
(b) Let $\overline{\mathbb{N}} = \mathbb{N} \times \mathbb{N}/\sim$. Show that: addition on $\mathbb{N}$ induces a well-defined addition on $\overline{\mathbb{N}}$.
(c) Show that: with this addition, $\overline{\mathbb{N}}$ is an abelian group.
(d) Show that: $\mathsf{nat} : \mathbb{N} \to \overline{\mathbb{N}}$ is an additive mapping where $\mathsf{nat}(a) = E((a + n, n))$ for any $n \in \mathbb{N}$ (that is $\mathsf{nat}(a + b) = \mathsf{nat}(a) + \mathsf{nat}(b)$).
(e) Show that $\overline{\mathbb{N}}$ is isomorphic as a group to $(\mathbb{Z}, +)$.

3.6. Factor Rings and the First Isomorphism Theorem

I mentioned in the lectures why Lagrange's Theorem from Fundamentals of Pure Mathematics is very useful: it reduces one aspect of complex objects, groups, to something substantially simpler, arithmetic. But I think its proof is not completely satisfying for such a fundamental result, at least at first. If you don't remember the proof, go back to last year's notes or look here. It uses left or right cosets. Cosets make the proof pretty clear – you can't forget it...right? – but nonetheless they seem to appear as if by magic. One of the jobs of this section is to demystify them. The other job is to prove the most powerful algebraic theorem you've seen yet. Oh, and by the way, by the end of this section you will be considerably more mature as a mathematician than you were when you began reading it. All that in only five pages?

I'm going to deal with rings rather than groups – we are, after all, in a chapter entitled "Rings and Modules". But everything I write translates naturally to groups, and so in particular explains cosets and normal subgroups in that context.

I want to take as a starting point ring homomorphisms

$$f : R \to S.$$

I've already stressed the importance of homomorphisms for vector spaces; the same is true for rings, so it is a reasonable beginning. I showed you in Equation (5) how a mapping between two

sets produced a bijection. I can apply this logic to f, since it is in particular a mapping between two sets. This tells me to consider the following equivalence relation on R:

$$x \sim y \Leftrightarrow f(x) = f(y).$$

So far, so good; but now I will use that f is not just any mapping, but a ring homomorphism. This means that

$$x \sim y \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x-y) = 0_S \Leftrightarrow x - y \in \ker f.$$

So what are the equivalence classes in this example? I claim that

$$E(x) = x + \ker f := \{x + k : k \in \ker f\}.$$

I think this is obvious: by definition, $y \in E(x)$ if and only if $y \sim x$ if and only if $y - x \in \ker f$; this happens if and only $y = x + k$ for some $k \in \ker f$ and so indeed $E(x) = x + \ker f$.

Now stand back for a minute and look what we have just deduced:

- the rule $x \sim y \Leftrightarrow x - y \in \ker f$ is an equivalence relation;
- the equivalence classes are the sets $x + \ker f$ for $x \in R$;
- the set of equivalence classes $(R/\sim)$ is a ring, isomorphic to a subring of S.

Actually, I haven't mentioned the last property. But (5) shows that $(R/\sim) \xrightarrow{\sim} \operatorname{im} f$ is a bijection. By Proposition 3.4.29.1 $\operatorname{im} f$ is a subring of S and I can use this bijection to make $(R/\sim)$ a ring by declaring this bijection to be an isomorphism.

Now stand even further back. Remember that $\ker f$ is an ideal of R by Proposition 3.4.18. Everything I say below now becomes completely natural, and I hope obvious[1].

DEFINITION 3.6.1. *Let $I \trianglelefteq R$ be an ideal in a ring R. The set*

$$x + I := \{x + i : i \in I\} \subseteq R$$

is a **coset of I in R** *or the* **coset of x with respect to I in R.**

REMARK 3.6.2. This a special case of cosets of a subgroup of a group. By Definition 3.4.7 (1) and (2), I is a subgroup of the abelian group $(R, +)$. So $x + I$ is the left coset of x with respect to I in sense of group theory; since $(R, +)$ is abelian it is also the right coset of x with respect to I. From this it follows from the Rules for Cosets that you learned in Fundamentals of Pure Mathematics that there is an equivalence relation on R defined by

$$x \sim y \Leftrightarrow x - y \in I$$

whose equivalences classes $E(x)$ are the cosets $x + I$. In particular, by the comments following Definition 3.5.3 for each $x, y \in R$ either $x + I = y + I$ or $(x + I) \cap (y + I) = \emptyset$ according to $x \sim y$ or not.

DEFINITION 3.6.3. *Let R be a ring, $I \trianglelefteq R$ an ideal, and $\sim$ the equivalence relation defined by $x \sim y \Leftrightarrow x - y \in I$. Then R/I,* **the factor ring of R by I** *or* **the quotient of R by I,** *is the set $(R/\sim)$ of cosets of I in R.*

Obviously, by what I've just written, there's a theorem to prove to justify the name "factor ring". Here it is:

[1] Possibly after several re-readings!

THEOREM 3.6.4. *Let R be a ring and $I \trianglelefteq R$ an ideal. Then R/I is a ring, where the operation of addition is defined by*

$$(x+I) \dot{+} (y+I) = (x+y)+I \qquad \textit{for all } x, y \in R$$

and multiplication is defined by

$$(x+I) \cdot (y+I) = xy+I \qquad \textit{for all } x, y \in R.$$

I've included $\dot{+}$ and $\cdot$ here for the usual didactic reason: it will help you keep track of the addition and multiplication defined in R/I as opposed to in R. I'll drop them again immediately after the proof.

There's quite a lot to do to prove this result, but it mostly revolves around checking that the above definitions are well defined. This means, for example, the following: it might be that there is an equality of sets $x+I = x'+I$ with distinct $x, x' \in R$. If so, it had better be that $(x+I)(y+I)$ and $(x'+I)(y+I)$ give the same answer. But the first is $xy+I$ while the second is $x'y+I$. It's my job to explain why $xy+I = x'y+I$. If that were not true, then the multiplication would not be well-defined because I would not get a unique answer on multiplying the cosets $x+I$ and $y+I$ together. Writing this differently, I need to explain in this case why the mapping $g : R/I \to R/I$ defined by $g(x+I) = xy+I$ is well-defined, in the sense of Definition 3.5.7.

PROOF. I first prove that R/I is an abelian group under addition.

I begin by showing that addition is well-defined. Suppose the $x, x' \in R$ are such that $x+I = x'+I$ and $y, y \in R$ are such that $y+I = y'+I$. I need to prove that

$$(x+I) \dot{+} (y+I) = (x'+I) \dot{+} (y'+I)$$

This, by definition, is the same as proving that $(x+y)+I = (x'+y')+I$, which in turn is the same as checking that $(x+y)-(x'+y') \in I$. This last statement is obvious, since we know by assumption that $x-x' \in I$ and $y-y' \in I$ and since I is an ideal we get $(x-x')+(y-y') \in I$.

That's the first piece of hard work. It is obvious that $0+I$ is the additive identity:

$$(0+I) \dot{+} (x+I) = x+I = (x+I) \dot{+} (0+I)$$

It is similarly obvious that $-x+I$ is the inverse to $x+I$:

$$(-x+I) \dot{+} (x+I) = (-x+x)+I = 0+I = (x+I) \dot{+} (-x+I).$$

Finally, associativity of addition follows from the associativity in R:

$$\begin{aligned} ((x+I) \dot{+} (y+I)) \dot{+} (z+I) &= ((x+y)+I) \dot{+} (z+I) \\ &= ((x+y)+z)+I \\ &= (x+(y+z))+I \\ &= (x+I) \dot{+} ((y+I) \dot{+} (z+I)) \end{aligned}$$

Now to multiplication. Suppose that

$$x+I = x'+I \qquad \text{and} \qquad y+I = y'+I \tag{6}$$

for some $x, x', y, y' \in R$. I must show that

$$(x+I) \cdot (y+I) = (x'+I) \cdot (y'+I).$$

By (6) we have $x-x' = i$ and $y-y' = j$ for some $i, j \in I$. Thus

$$\begin{aligned} xy - x'y' &= (x'+i)(y'+j) - x'y' \\ &= x'y' + iy' + x'j + ij - x'y' \\ &= iy' + x'j + ij. \end{aligned}$$

Since I is an ideal and $i, j \in I$ I know $iy', x'j, ij \in I$ and hence $iy' + x'j + ij \in I$. Thus $xy - x'y' \in I$, which is to say $xy + I = x'y' + I$. Thus

$$(x + I) \cdot (y + I) = xy + I = x'y' + I = (x' + I) \cdot (y' + I)$$

as required.

R/I is clearly closed under multiplication. For all $x, y, z \in R$

$$\begin{aligned}(x + I) \cdot ((y + I) \cdot (z + I)) &= (x + I) \cdot (yz + I) \\ &= x(yz) + I \\ &= xyz + I\end{aligned}$$

and similarly for $((x + I) \cdot (y + I)) \cdot (z + I)$ so that multiplication is associative. Furthermore, for any $x \in R$

$$(x + I) \cdot (1 + I) = (x1) + I = x + I = (1x) + I = (1 + I) \cdot (x + I),$$

so that $(R/I, \cdot)$ is a monoid.

Finally, the distributive axioms hold:

$$\begin{aligned}(x + I) \cdot ((y + I) \dot{+} (z + I)) &= (x + I) \cdot ((y + z) + I) \\ &= x(y + z) + I \\ &= (xy + xz) + I \\ &= (xy + I) \dot{+} (xz + I) \\ &= (x + I) \cdot (y + I) \dot{+} (x + I) \cdot (z + I)\end{aligned}$$

So, as I claimed, R/I is a ring. □

EXAMPLE 3.6.5. For any $m \in \mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ is a ring. But you knew that, didn't you? But do think again about the comment in parentheses made at the end of Example 3.1.4.

EXAMPLE 3.6.6. Let $R = \mathbb{R}[X]$ and $I = {}_{\mathbb{R}[X]}\langle X^2 + 1\rangle$. Then R/I is isomorphic to the complex numbers! See Example 3.6.10 for the explanation.

EXERCISE 52. Let R be a ring and let I be an ideal of R. Show that: if R is commutative then so is R/I.

EXERCISE 53. Let R be a ring and let I be an ideal of R. Show that: R/I is a non–zero ring if and only $I \neq R$

EXERCISE 54. Let R be a ring and let I be a proper ideal of R, that is $I \neq R$. Show that: if $r \in R^\times$, then $r + I \in (R/I)^\times$ with $(r + I)^{-1} = r^{-1} + I$.

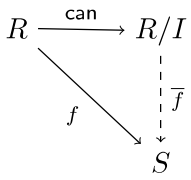
You should compare the following theorem with the very important remark in Section 3.5

THEOREM 3.6.7 (The Universal Property of Factor Rings). *Let R be a ring and I an ideal of R.*

(1) The mapping $\mathsf{can} : R \to R/I$ *sending r to $r + I$ for all $r \in R$ is a surjective ring homomorphism with kernel I.*

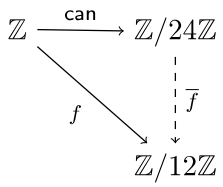
(2) If $f : R \to S$ is a ring homomorphism with $f(I) = \{0_S\}$, so that $I \subseteq \ker f$, then there is a unique ring homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \mathsf{can}$.

I like to remember this theorem by drawing a diagram:



The second part of the Theorem states that f **factorises uniquely** through the canonical mapping to the factor whenever the ideal I is sent to zero.

EXAMPLE 3.6.8. We have



where $f : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ is the canonical mapping. Here the induced mapping $\overline{f}$ sends the coset $a + 24\mathbb{Z}$ to the coset $a + 12\mathbb{Z}$.

PROOF. The first statement is pretty clear: it is certainly a surjective mapping where the elements of I are precisely those being sent to $0_{R/I}$. That it is a ring homomorphism follows from the definition of addition and multiplication in R/I:

$$\mathsf{can}(x) + \mathsf{can}(y) = (x + I) + (y + I) = (x + y) + I = \mathsf{can}(x + y)$$

and

$$\mathsf{can}(x)\mathsf{can}(y) = (x + I)(y + I) = (xy) + I = \mathsf{can}(xy)$$

For the second claim, note that because of the condition $f(I) = \{0\}$, any coset of I in R gets sent to a single element in S:

$$f(x + I) = f(x) + f(I) = \{f(x)\}$$

I'll call this element $\overline{f}(x + I)$ so that $\overline{f}(x + I) = f(x)$ and $f(x + I) = \{\overline{f}(x + I)\}$. This produces the only possible mapping $\overline{f}$ satisfying $f = \overline{f} \circ \mathsf{can}$. To check that $\overline{f}$ is a ring homomorphism, use that

$$\overline{f}((x + I) + (y + I)) = \overline{f}((x + y) + I) = f(x + y) = f(x) + f(y) = \overline{f}(x + I) + \overline{f}(y + I)$$

and

$$\overline{f}((x + I)(y + I)) = \overline{f}(xy + I) = f(xy) = f(x)f(y) = \overline{f}(x + I)\overline{f}(y + I)$$

□

THEOREM 3.6.9 (First Isomorphism Theorem for Rings). *Let R and S be rings. Then every ring homomorphism $f : R \longrightarrow S$ induces a ring isomorphism*

$$\overline{f} : R/\ker f \xrightarrow{\sim} \operatorname{im} f.$$

EXAMPLE 3.6.10. Let's go back to Example 3.6.6. Evaluation at $\sqrt{-1}$ produces a ring homomorphism $f : \mathbb{R}[X] \to \mathbb{C}$. By Theorem 3.3.4 each polynomial $P \in \mathbb{R}[X]$ can be written uniquely as $P = A(X^2+1)+B$ where $B = a+bX$ is a linear polynomial. Then $f(P) = f(B) = a+b\sqrt{-1}$ which shows that f is surjective and that $P \in \ker f$ if and only if $a = b = 0$, so that ${}_{\mathbb{R}[X]}\langle X^2 + 1\rangle = \ker f$. Applying the First Isomorphism Theorem completes the claim that $R/I \cong \mathbb{C}$.

PROOF. Clearly $\overline{f}$ is surjective. It's injective by Lemma 3.4.20 since the only element in the kernel of $\overline{f}$ is the coset $0 + \ker f$, the zero element of $R/\ker f$. □

This completes the explanation and generalisation of all the comments I made at the introduction to this Section. And better still, you learned one additional fact: thanks to Theorem 3.6.7.1, each ideal I of R is the kernel of at least one ring homomorphism, namely $\mathsf{can} : R \to R/I$. So ideals really are kernels, and kernels really are ideals.

3.7. Modules and All That

Do not misunderstand the following waffle as the basis for a philosophical theory of anything! I've now shown many of the basic properties of rings and their homomorphisms. I also showed in Definition 3.1.8 that the definition of a ring generalises that of a field. Generalisation for its own sake is at best a derivative activity, but it is a strong argument to propose part of the art of mathematics to find the **correct level of generality**. So what might that vague phrase mean? Well, I'd suggest *power, beauty and ubiquity*. A theory being developed should:

(a) have decent theorems (the *power*),
(b) proceed naturally and hang together well (the *beauty*)
(c) unify many examples or be widely applicable (the *ubiquity*).

For the generalisation from fields to rings, think about the First Isomorphism Theorem for (a) and (b), and the natural examples I introduced such as $\mathbb{Z}$ and $\mathbb{C}[X]$ – which are only the very beginning – for (c).

Now ratiocinate! You might speculate that I should be able to define something like a vector space, generalising scalars from fields to rings. But for this to be at the correct level of generality, I'd need to have natural theorems and convincing examples of whatever this structure is.

DEFINITION 3.7.1. *A* **(left) module** M **over a ring** R *is a pair consisting of an abelian group* $M = (M, \dot{+})$ *and a mapping*

$$\begin{aligned} R \times M &\to M \\ (r, a) &\mapsto ra \end{aligned}$$

such that for all $r, s \in R$ *and* $a, b \in M$ *the following identities hold:*

$$\begin{aligned} r(a \dot{+} b) &= (ra) \dot{+} (rb) \\ (r+s)a &= (ra) \dot{+} (sa) \\ r(sa) &= (rs)a \\ 1_R a &= a \end{aligned}$$

The first two laws are the **Distributive Laws***; the third law is called the* **Associativity Law**. *I will often also call a left module* M *over a ring* R *an* R**-module**.

REMARK 3.7.2. Don't worry: there is a notion of right R-module! I'll leave you to work out what it must be. Everything I do in this course for left R-modules could also have been done equally for right R-modules; but since I've just mentioned that, I won't discuss right R-modules again.

EXAMPLE 3.7.3. If $R = F$ is a field then R–modules are just F-vector spaces. This is obvious: when I latexed Definition 3.7.1 I cut-and-pasted the definition of a vector space and then replaced the each appearance of the field F in the original with the ring R.

EXAMPLE 3.7.4. Let $R = \mathbb{Z}$. A $\mathbb{Z}$-module is exactly the same as an abelian group. Since any module is an abelian group by definition, I am therefore claiming the converse: any abelian group M is a $\mathbb{Z}$-module. This is straightforward, and just depends on the Rules for Multiples in abelian groups, which you saw in Fundamentals of Pure Mathematics and I which outlined again in Lemma 3.2.4.

EXAMPLE 3.7.5. Let I be an ideal in a ring R. Then I is an R–module using the multiplication in the ring. In particular, R itself is an R–module.

EXAMPLE 3.7.6. The singleton $\{0\}$ is an R-module for any R, with addition and multiplication defined by $0 \dot{+} 0 = 0$ and $r0 = 0$ for all $r \in R$. It is the **zero module** or **trivial module**.

EXERCISE 55. Let S be a ring and let $R = \mathsf{Mat}(n; S)$, the ring of $(n \times n)$-matrices with coefficients in S. Let $M = S^n$. Show that: M is an R-module under the operations of componentwise addition and matrix multiplication.

EXERCISE 56. Let V be an F-vector space for some field F and let $\phi \in \mathrm{End}(V)$ be an endomorphism of V. Show that: V is an $F[X]$-module under the operation

$$(a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0)\vec{v} = a_m \phi^m(\vec{v}) + a_{m-1}\phi^{m-1}(\vec{v}) + \cdots + a_1\phi(\vec{v}) + a_0\vec{v}.$$

I will denote this $F[X]$-module by V_ϕ.

EXAMPLE 3.7.7. Given a ring R and R-modules $M_1, \ldots, M_n$, the cartesian product $M_1 \times M_2 \times \cdots \times M_n$ is an R–module if I define addition and multiplication as follows:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

and

$$r(a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$$

for all $r \in R$ and $a_i, b_i \in M$. This is denoted $M_1 \oplus \cdots \oplus M_n$ and called the **direct sum**. It generalises the construction for vector spaces given in Exercise 2.

You should be able to guess what I am going to say now. After all, the first thing I did after defining vector spaces was to conduct a hygiene-check.

LEMMA 3.7.8. *Let R be a ring and M an R–module.*

(1) $0_R a = 0_M$ *for all* $a \in M$.
(2) $r0_M = 0_M$ *for all* $r \in R$.
(3) $(-r)a = r(-a) = -(ra)$ *for all* $r \in R, a \in M$. *Here the first negative is a negative in R, the last two are negatives in M.*

PROOF. Exactly the same as the proofs for Lemma 1.2.2, Lemma 1.2.3 or Lemma 3.2.1.2, and the first statement of Lemma 1.2.4. □

What happened to the analogue of the second statement of Lemma 1.2.4? That stated: if $\lambda \in F$ and $\vec{v} \in V$ satisfy $\lambda\vec{v} = \vec{0}$ then either $\lambda = 0$ or $\vec{v} = 0$. Well, remember how you proved it: you assumed that λ was non-zero, multiplied by $\lambda^{-1} \in F$ and then deduced that $\vec{v} = \vec{0}$. See the appearance of λ^{-1} in that argument? That's why you can't deduce such a result for R-modules in general.

EXAMPLE 3.7.9. Let $R = \mathsf{Mat}(2; \mathbb{C})$ and $M = \mathbb{C}^2$ as in Exercise 55. Then

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

EXAMPLE 3.7.10. Let $V = \mathbb{C}^2$ and $\phi \in \mathrm{End}(V)$ whose representative with respect to the standard basis is

$$[\phi] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Then $X\vec{e}_1 = \vec{0}$ in the $F[X]$-module V_ϕ, defined as in Exercise 56.

I next introduce homomorphisms between R-modules. You know what the definition will be: a structure-preserving mapping.

DEFINITION 3.7.11. *Let R be a ring and let M, N be R–modules. A mapping $f : M \to N$ is an* **R–homomorphism** *or* **homomorphism** *if the following hold for all $a, b \in M$ and $r \in R$*

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ra) &= rf(a) \end{aligned}$$

The **kernel** *of f is $\ker f = \{a \in M : f(a) = 0_N\} \subseteq M$ and the* **image** *of f is $\operatorname{im} f = \{f(a) : a \in M\} \subseteq N$. If f is a bijection then it is an R-***module isomorphism** *or* **isomorphism**, *I write $M \cong N$ and say M and N are* **isomorphic**.

As usual, the composition of two R-homomorphisms is again an R-homomorphism.

EXAMPLE 3.7.12. If M and N are R–modules then the map $f : M \to N$ defined by $f(a) = 0_N$ for all $a \in M$ is *always* an R–homomorphism.

EXAMPLE 3.7.13. If R is a field then F-homomorphisms are just linear mappings, of course.

EXAMPLE 3.7.14. Let M, N be abelian groups. Then any *group* homomorphism $f : M \to N$ is also a $\mathbb{Z}$–homomorphism.

EXERCISE 57. Let F be a field and let V and W be the F-vector spaces F^2 and F^3 respectively. Let

$$\phi = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

and consider the $F[X]$-modules V_ϕ and W_ψ as in Exercise 56. Show that: the mappings

$$f : V_\phi \to W_\psi, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} \qquad \text{and} \qquad g : W_\psi \to V_\phi, \quad \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} z \\ 0 \end{pmatrix}$$

are $F[X]$-homomorphisms.

What now? That's right, find out what structure the kernel and the image inherit.

DEFINITION 3.7.15. *A non–empty subset M' of an R–module M is a* **submodule** *if M' is an R–module with respect to the operations of the R–module M* **restricted** *to M'.*

EXAMPLE 3.7.16. If V is a vector space over a field R, then the submodules of V are the vector subspaces of V.

EXAMPLE 3.7.17. Let M be an abelian group. Regarding M as a $\mathbb{Z}$–module, its submodules are precisely the subgroups of M.

EXAMPLE 3.7.18. For any ring R, regarded as an R–module, the ideals of R are precisely the submodules of R.

EXAMPLE 3.7.19. Let F be a field and let W_ψ be defined as in Example 57. The subspaces $\langle \vec{e}_1 \rangle$ and $\langle \vec{e}_1, \vec{e}_2 \rangle$ are $F[X]$-submodules of W_ψ, whereas $\langle \vec{e}_2 \rangle$ is not.

PROPOSITION 3.7.20 (Test for a submodule). *Let R be a ring and let M be an R–module. A subset M' of M is a submodule if and only if*

(1) $0_M \in M'$
(2) $a, b \in M' \Rightarrow a - b \in M'$
(3) $r \in R, a \in M' \Rightarrow ra \in M'$.

PROOF. This is just as easy as it was in Proposition 3.4.26 If M' is a submodule of M then the properties (1)–(3) are obvious. Suppose on the other hand that M' satisfies (1)–(3). Then, by the test for a subgroup, (1) and (2) show that M' is a subgroup of the abelian group M. The binary operation $R \times M \to M$ restricts to an operation $R \times M' \to M'$ by Property (3). The axioms for an R-module then hold for M' since they hold for the bigger set M. □

Now go back to Remark 1.4.2 and see if that makes sense, now that you've seen **subobjects** defined for vector spaces, for rings, and for modules.

LEMMA 3.7.21. *Let $f : M \to N$ be an R–homomorphism. Then $\ker f$ is a submodule of M and $\operatorname{im} f$ is a submodule of N.*

PROOF. Obviously, I should use Lemma 3.7.20 in both cases.

For the kernel: (1) $f(0_M) = 0_N$, since f is a homomorphism of abelian groups. So $0_M \in \ker f$. (2) Let $a, b \in \ker f$. Then $f(a-b) = f(a) - f(b) = 0_N$. Hence $a - b \in \ker f$. (3) Let $a \in \ker f, r \in R$. Then $f(ra) = rf(a) = r0_N = 0_N$ so that $ra \in \ker f$.

It's not going to be any more exciting for the image: (1) $0_N = f(0_M)$. So $0_N \in \operatorname{im} f$. (2) Let $a, b \in \operatorname{im} f$. Then $a = f(c), b = f(d)$ for some $c, d \in M$. Then $a - b = f(c) - f(d) = f(c-d) \in \operatorname{im} f$. (3) Let $a \in \operatorname{im} f, r \in R$. Then $a = f(c)$ for some $c \in M$. Then $ra = rf(c) = f(rc) \in \operatorname{im} f$. □

As usual, the following lemma holds true because it only needs that f is a homomorphism of abelian groups:

LEMMA 3.7.22. *Let R be a ring, let M and N be R-modules and let $f : M \to N$ be an R-homomorphism. Then f is injective if and only if $\ker f = \{0_M\}$.*

DEFINITION 3.7.23. *Let R be a ring, M an R-module and let $T \subseteq M$. Then the* **submodule of M generated by** *T is the set*

$$ {}_R\langle T \rangle = \{r_1 t_1 + \cdots + r_m t_m : t_1, \ldots, t_m \in T, r_1, \ldots, r_m \in R\}, $$

together with the zero element in the case $T = \emptyset$. If $T = \{t_1, \ldots, t_n\}$, a finite set, I will often abuse notation by writing ${}_R\langle t_1, \ldots, t_n \rangle$ instead of ${}_R\langle \{t_1, \ldots, t_n\} \rangle$. The module M is **finitely generated** *if it is generated by a finite set: $M = {}_R\langle t_1, \ldots, t_n \rangle$. It is called* **cyclic** *if it is generated by a singleton: $M = {}_R\langle t \rangle$.*

EXAMPLE 3.7.24. A cyclic group is the same thing as a cyclic $\mathbb{Z}$-module.

EXAMPLE 3.7.25. Let R be a commutative ring. Then the ideal generated by $T \subseteq R$ is the same thing as the submodule of R generated by T. A principal ideal is the same thing as a cyclic submodule of R.

EXAMPLE 3.7.26. Let F be a field and let W_ψ be defined as in Example 57. Then W_ψ is a cyclic $F[X]$-module, generated by the element $\vec{e}_3 \in W_\psi$.

EXAMPLE 3.7.27. $\{0_M\}$ is always a cyclic submodule of an R-module M, generated by the element 0_M.

There are some easy-to-prove results about submodules that you have seen for vector subspaces and for ideals in this course or for groups. I'm going to write them out but not prove them: their proofs are obtained by modifying the proofs you already know in those other cases, so there's no point sentencing you to another twenty years of boredom; there are far more interesting things to be thinking about. In all of the statements R is a ring and M is an R-module.

LEMMA 3.7.28. *Let $T \subseteq M$. Then ${}_R\langle T \rangle$ is the smallest submodule of M that contains T.*

LEMMA 3.7.29. *The intersection of any collection of submodules of M is a submodule of M.*

LEMMA 3.7.30. *Let M_1 and M_2 be submodules of a M. Then*

$$M_1 + M_2 = \{a + b : a \in M_1, b \in M_2\}$$

is a submodule of M.

Finally we reach factor modules and the First Isomorphism Theorem for modules.

THEOREM-DEFINITION 3.7.31. *Let R be a ring, M an R-module and N a submodule of M. For each $a \in M$ the* **coset of a with respect to N in M** *is*

$$a + N = \{a + b : b \in N\}$$

It is a coset of N in the abelian group M and so is an equivalence class for the equivalence relation $a \sim b \Leftrightarrow a - b \in N$. I define M/N, **the factor of M by N** *or* **the quotient of M by N,** *to be the set $(M/\sim)$ of all cosets of N in M. This becomes an R–module by introducing the operations of addition and multiplication as follows:*

$$\begin{aligned} (a + N) \dot{+} (b + N) &= (a + b) + N \\ r(a + N) &= ra + N \end{aligned}$$

for all $a, b \in M, r \in R$. I must check that this is well-defined. For addition this follows by the same argument as in the first half of the Proof of Theorem 3.6.4. For multiplication, let $a, b \in M$ be such that $a + N = b + N$. This means that $a - b \in N$, and since N is a submodule I have that $r(a - b) \in N$. So

$$\begin{aligned} r(a + N) - r(b + N) &= (ra + N) - (rb + N) \\ &= (ra - rb) + N \\ &= r(a - b) + N \\ &= 0 + N. \end{aligned}$$

Thus $r(a + N) = r(b + N)$ as required.

The zero of M/N is the coset $0_{M/N} = 0_M + N$. The negative of $a + N \in M/N$ is the coset $-(a + N) = (-a) + N$.

The R-module M/N is the **factor module** *of M by the submodule N.*

EXERCISE 58. Let $R = F$ be a field, V an F-vector space (= F-module) and $W \subseteq V$ a submodule of V, which is just a subspace of V. The quotient V/W is again an F-vector space, naturally called the *quotient vector space*. The canonical projection $\mathsf{can} : V \to V/W$ is a linear mapping. Assume that $\dim V = m$ is finite, although if I had mentioned the correct things from set theory an appropriate version of the following would be true in general. By the Dimension Estimate for Vector Subspace $\dim W = n \leqslant m$. Let $\{\vec{v}_1, \ldots, \vec{v}_n\}$ be a basis for W and extend it to a basis $\{\vec{v}_1, \ldots, \vec{v}_n, \vec{v}_{n+1}, \ldots, \vec{v}_m\}$ of V by using the Steinitz Exchange Theorem. Show that: $\{\vec{v}_{n+1} + W, \ldots, \vec{v}_m + W\}$ is a basis for the vector space V/W. In particular, deduce that $\dim V/W = \dim V - \dim W$.

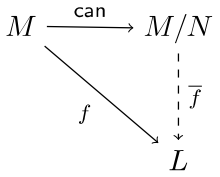
You should compare the following theorem with the very important remark in Section 3.5 and with Theorem 3.6.7.

THEOREM 3.7.32 (The Universal Property of Factor Modules). *Let R be a ring, let L and M be R-modules, and N a submodule of M.*

(1) The mapping $\mathsf{can} : M \to M/N$ sending a to $a + N$ for all $a \in M$ is a surjective R-homomorphism with kernel N.

(2) If $f : M \to L$ is an R-homomorphism with $f(N) = \{0_L\}$, so that $N \subseteq \ker f$, then there is a unique homomorphism $\overline{f} : M/N \to L$ such that $f = \overline{f} \circ \mathsf{can}$.

I like to remember this theorem by drawing a diagram:



The second part of the Theorem states that f **factorises uniquely** through the canonical mapping to the factor whenever the submodule N is sent to zero.

PROOF. This is proved in a completely analogous manner to the proof of Theorem 3.6.7. □

THEOREM 3.7.33 (First Isomorphism Theorem for Modules). *Let R be a ring and let M and N be R-modules. Then every R-homomorphism $f : M \longrightarrow N$ induces an R-isomorphism*

$$\overline{f} : M/\ker f \xrightarrow{\sim} \operatorname{im} f.$$

PROOF. There's not really anything to do! If follows from everything we've done, just as in Theorem 3.6.9. □

REMARK 3.7.34. If we apply this theorem in the special case when $R = F$ is a field, then we get the **First Isomorphism Theorem for F-vector spaces**. By Exercise 58 the dimension of $M/\ker f$ is $\dim M - \dim \ker f$, and as isomorphic vector spaces have the same dimension we deduce from the First Isomorphism Theorem a new proof of the Rank-Nullity Theorem as a corollary:

$$\dim M - \dim(\ker f) = \dim(\operatorname{im} f).$$

REMARK 3.7.35. If we apply this theorem in the special case when $R = \mathbb{Z}$, the integers, then we get the **First Isomorphism Theorem for Abelian Groups**, which is a special case of the **First Isomorphism Theorem for Groups**.

EXAMPLE 3.7.36. Let $g : W_\psi \to V_\phi$ be the $F[X]$-homomorphism defined in Exercise 57. Then

$$\ker g = \left\{ \begin{pmatrix} a \\ b \\ 0 \end{pmatrix} : a, b \in F \right\} \text{ and } \operatorname{im} g = \left\{ \begin{pmatrix} c \\ 0 \end{pmatrix} : c \in F \right\}.$$

So in this case the First Isomorphism Theorem states that

$$\frac{F^3}{\{(a,b,0)^\mathsf{T}\}} \xrightarrow{\sim} \{(c,0)^\mathsf{T}\}.$$

I hope this looks natural to you! Note that on both the left hand side and the right side multiplication by the element $X \in F[X]$ sends any element to 0.

EXERCISE 59 (Second Isomorphism Theorem for Modules). Let N, K be submodules of an R–module M. Show that: K is a submodule of $N + K = \{b + c : b \in N, c \in K\}$ and $N \cap K$ is a submodule of N. Show further that:

$$\frac{N+K}{K} \cong \frac{N}{N \cap K}.$$

EXERCISE 60 (The Third Isomorphism Theorem for Modules). Let N, K be submodules of an R–module M, where $K \subseteq N$. Show that: N/K is a submodule of M/K and

$$\frac{M/K}{N/K} \cong M/N.$$

CHAPTER 4

Determinants and Eigenvalues Redux

You met determinants of real $(n \times n)$-matrices in Introduction to Linear Algebra. You must have had several reactions, I'd guess: (i) "Huh?"; (ii) "That's horrible to calculate"; (iii) "Oh, but it's quite useful". There is no "Huh?" with determinants, and in this chapter you will see why: I'll explain why the definition is inevitable. I will also deal rigorously with the content of Introduction to Linear Algebra, and then I'll show you how matrices over a specific commutative ring – that is not a field – prove the Cayley-Hamilton Theorem for matrices over a field.

4.1. The Sign of a Permutation

The definition of determinants begins with the symmetric group, which you met this in Fundamentals of Pure Mathematics:

DEFINITION 4.1.1. *The group of all permutations of the set $\{1, 2, \ldots, n\}$, also known as bijections from $\{1, 2, \ldots, n\}$ to itself, is denoted by $\mathfrak{S}_n$ and called the n-th* **symmetric group**. *It is a group under composition and it has $n!$ elements.*

A **transposition** *is a permutation that swaps two elements of the set and leaves all the others unchanged.*

DEFINITION 4.1.2. *An* **inversion** *of a permutation $\sigma \in \mathfrak{S}_n$ is a pair (i, j) such that $1 \leqslant i < j \leqslant n$ and $\sigma(i) > \sigma(j)$. The number of inversions of the permutation σ is called the* **length of** *σ and written $\ell(\sigma)$. In formulas:*

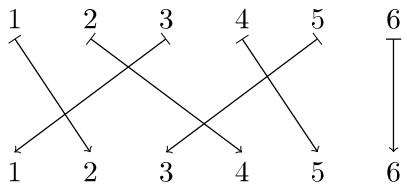
$$\ell(\sigma) = |\{(i, j) : i < j \text{ but } \sigma(i) > \sigma(j)\}|$$

The **sign of** *σ is defined to be the parity of the number of inversions of σ. In formulas:*

$$\mathsf{sgn}(\sigma) = (-1)^{\ell(\sigma)}$$

A permutation whose sign is $+1$, in other words which has even length, is called an **even permutation**, *while a permutation whose sign is -1, in other words which has odd length, is called an* **odd permutation**.

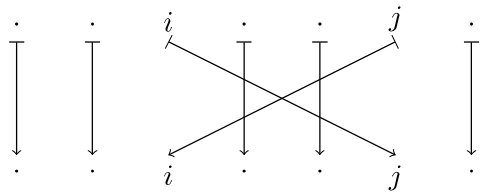
EXAMPLE 4.1.3. If I represent the permutation by a diagram, as I do below for $(1\,2\,4\,5\,3) \in \mathfrak{S}_6$, then the length is the number of crossings:



So $\ell((1\,2\,4\,5\,3)) = 4$: the inversions are $(1, 3), (2, 3), (2, 5), (4, 5)$.

EXAMPLE 4.1.4. The identity of $\mathfrak{S}_n$ is always the only permutation with length zero. The transposition that swaps i and j, leaving everything else unchanged, has length $2|i - j| - 1$, which

you can see best from the picture below. In particular, all transpositions are odd permutations.



LEMMA 4.1.5 (Multiplicativity of the Sign). *For each $n \in \mathbb{N}$ the sign of a permutation produces a group homomorphism $\mathsf{sgn} : \mathfrak{S}_n \to \{+1, -1\}$ from the symmetric group to the two-element group of signs. In formulas:*

$$\mathsf{sgn}(\sigma\tau) = \mathsf{sgn}(\sigma)\mathsf{sgn}(\tau) \quad \textit{for all } \sigma, \tau \in \mathfrak{S}_n$$

PROOF. I need to introduce a new notation. Given a non-zero real number $a \in \mathbb{R} \setminus 0$ let $[a] \in \{+1, -1\}$ be the sign of a. I can then restate the definition of the sign of a permutation σ by

$$\mathsf{sgn}(\sigma) = \prod_{i<j} [\sigma(j) - \sigma(i)] \tag{7}$$

Given another permutation τ it's clear that

$$\prod_{i<j} [\sigma\tau(j) - \sigma\tau(i)] = \prod_{i<j} \frac{[\sigma(\tau(j)) - \sigma(\tau(i))]}{[\tau(j) - \tau(i)]} \prod_{i<j} [\tau(j) - \tau(i)]$$

So, using (7), that means that I must show that

$$\prod_{i<j} [\sigma(j) - \sigma(i)] = \prod_{i<j} \frac{[\sigma(\tau(j)) - \sigma(\tau(i))]}{[\tau(j) - \tau(i)]} \tag{8}$$

This is elementary. Since τ is a bijection there is an equality

$$\{(i,j) : i < j\} = \{(\tau(i), \tau(j)) : i < j \text{ and } \tau(i) < \tau(j)\} \cup \{(\tau(j), \tau(i)) : i < j \text{ and } \tau(i) > \tau(j)\}$$

I can then replace the indexing set $\{(i,j) : i < j\}$ on the right hand side of (8) by this to obtain the equality I want. □

REMARK 4.1.6. There's a better proof which was presented to you in Fundamentals of Pure Mathematics. For each $\sigma \in \mathfrak{S}_n$ there is an associated ring homomorphism $\sigma : \mathbb{Z}[X_1, \ldots, X_n] \to \mathbb{Z}[X_1, \ldots, X_n]$ that is defined by swapping the variables according to σ, namely $\sigma : X_i \mapsto X_{\sigma(i)}$. It's clear that $\tau(\sigma P) = (\tau\sigma)P$ for each polynomial $P \in \mathbb{Z}[X_1, \ldots, X_n]$. Consider a special polynomial, called the **discriminant**:

$$P = \prod_{i<j} (X_i - X_j)$$

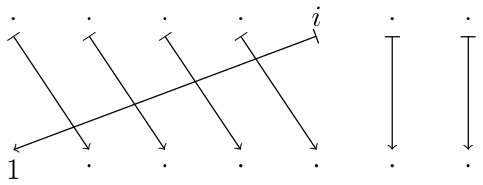
which automatically has the property that $\sigma P = \mathsf{sgn}(\sigma)P$. From this it follows that

$$\mathsf{sgn}(\tau)\mathsf{sgn}(\sigma)P = \tau(\sigma P) = (\tau\sigma)P = \mathsf{sgn}(\tau\sigma)P$$

From this, I earn the statement of Lemma 4.1.5.

DEFINITION 4.1.7. *For $n \in \mathbb{N}$, the set of even permutations in $\mathfrak{S}_n$ forms a subgroup of $\mathfrak{S}_n$ because it is the kernel of the group homomorphism $\mathsf{sgn} : \mathfrak{S}_n \to \{+1, -1\}$. This group is the* **alternating group** *and is denoted A_n.*

EXERCISE 61. Show that: the permutation that brings i to the first place while changing the order of no other number has $i-1$ inversions. In particular $\mathsf{sgn}(\sigma) = (-1)^{i-1}$.



EXERCISE 62. Show that: every permutation in $\mathfrak{S}_n$ can be described as a product of transpositions of neighbouring numbers, that is of the permutations $(i\ i{+}1)$ swapping i and $i+1$ for some $1 \leqslant i \leqslant n-1$.

4.2. Determinants and What They Mean

DEFINITION 4.2.1. *Let R be a commutative ring and $n \in \mathbb{N}$. The* **determinant** *is a mapping $\mathsf{det} : \mathsf{Mat}(n;R) \to R$ from square matrices with coefficients in R to the ring R that is given by the following formula:*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mapsto \mathsf{det}(A) = \sum_{\sigma\in\mathfrak{S}_n} \mathsf{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

The sum is over all permutations of n, and the coefficient $\mathsf{sgn}(\sigma)$ is the sign of the permutation σ defined above in Definition 4.1.2. This formula is called the **Leibniz formula**. *The degenerate case $n = 0$ assigns the value 1 as the determinant of the "empty matrix".*

REMARK 4.2.2. The determinant determines whether or not a linear system of n equations in n unknowns has a unique solution. Hence the name.

EXAMPLE 4.2.3. It is simple to calculate:

$$\begin{aligned} \mathsf{det}(a) &= a \\ \mathsf{det}\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= ad - bc \\ \mathsf{det}\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= \begin{array}{l} a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12} \end{array} \end{aligned}$$

The (3×3)-case is easy to remember – it looks just like a trellis fence:

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

For $n \geqslant 4$ there are $n! \geqslant 24$ terms in the Leibniz formula, and it's not fun to calculate. I'll remind you in Remark 4.4.5 how to calculate determinants more efficiently in such cases.

EXAMPLE 4.2.4. An $n \times n$ matrix $A = (a_{ij})$ is upper triangular if $a_{ij} = 0$ for $i > j$. The determinant of A is the product of the entries a_{ii} along the diagonal. This follows because the only permutation $\sigma \in \mathfrak{S}_n$ that satisfies $i \leqslant \sigma(i)$ for all i is the identity permutation, so the only

non-zero summand in the definition of the determinant occurs for $\sigma = \mathrm{id}$. The same holds for a lower triangular matrix.

EXERCISE 63. By adapting the argument in the above example, show that: the determinant of a block-upper triangular matrix with square blocks along the diagonal is the product of the determinants of the blocks along the diagonal

$$\mathsf{det}\left(\begin{array}{c|c|c|c} A_1 & * & * & * \\ \hline 0 & A_2 & * & * \\ \hline 0 & 0 & \ddots & * \\ \hline 0 & 0 & 0 & A_t \end{array}\right) = \mathsf{det}(A_1)\mathsf{det}(A_2)\cdots\mathsf{det}(A_t).$$

I'll now explain the meaning of the determinant in order to motivate my development of the theory. To do this I need to use real matrices and I'm going to consider only (2×2)-matrices. Using the standard basis for $\mathbb{R}^2$ such matrices correspond to linear mappings $L : \mathbb{R}^2 \to \mathbb{R}^2$ and since my spatial intuition of two-dimensional space is well-developed I will use this description.

The connection between determinants and volumes. Each such linear mapping L has an "area scaling factor" $sc(L)$ which I define as the amount that L changes the area, $\mathsf{vol}(U)$, of a region U in $\mathbb{R}^2$. In other words $\mathsf{area}(LU) = sc(L)\mathsf{area}(U)$. I claim that

$$sc(L) = |\mathsf{det}(L)|$$

To see this I consider the properties that the mapping $sc : \mathsf{Mat}(2;\mathbb{R}) \to \mathbb{R}_{\geqslant 0}$, defined by $L \mapsto sc(L)$, must have:

(1) It should be "multiplicative": $sc(LM) = sc(L)sc(M)$;
(2) Dilating an axis should increase the area of a region by the amount of the dilation: $sc(\mathsf{diag}(a,1)) = sc(\mathsf{diag}(1,a)) = |a|$;
(3) A shear transformation should leave the area of a region unchanged: $sc(D) = 1$ for D an upper or a lower triangular matrix with ones on the diagonal.

These should be obvious to you; if not, experiment with this applet, written by Henri Maurer, a former Honours Algebra student, which visualises linear mappings.

Recall from Theorem 2.2.3 that each square matrix can be written as a product of elementary matrices. Since each elementary matrix either dilates one of the axes or is a shear transformation, there can be therefore at most one mapping $sc : \mathsf{Mat}(2;\mathbb{R}) \to \mathbb{R}_{\geqslant 0}$ satisfying the three properties above. In Theorem 4.4.1 I will prove that $\det(LM) = \det(L)\det(M)$, and together with Example 4.2.4 which calculates the determinant for an upper or lower triangular matrix, this shows that $M \mapsto |\mathsf{det}(M)|$ is a mapping with the three prescribed properties. So it must be that $sc = |\mathsf{det}|$, as claimed. In other words the absolute value of the determinant is the area scaling factor of the corresponding linear mapping.

The connection between determinants and orientation. The sign of the determinant of an invertible real (2×2)-matrix shows whether the corresponding endomorphism of $\mathbb{R}^2$ preserves or reverses orientation. To comprehend orientation I imagine a clock face inside the region U I'm going to apply L to: if, after applying U, the clock face is still the correct way round then L preserves orientation; if it is the wrong way round, then L reverses orientation. I think of this property as a mapping sending an invertible linear transformation $L : \mathbb{R}^2 \to \mathbb{R}^2$ to $\epsilon(L) \in \{+1, -1\}$ as follows:

$$\epsilon(L) = \begin{cases} +1 & L \text{ preserves the orientation} \\ -1 & L \text{ reverses the orientation} \end{cases}$$

In the proof of Lemma 4.1.5 I used the notation $[a]$ for the sign of a non-zero real number a and I'll do that again here. I claim that

$$\epsilon(L) = [\mathsf{det}(L)]$$

To see this let's consider the properties that the mapping $\epsilon : GL(2;\mathbb{R}) \to \{+1,-1\}$, defined by $L \mapsto \epsilon(L)$, must have:

(1) It should be "multiplicative": $\epsilon(LM) = \epsilon(L)\epsilon(M)$;
(2) Dilating an axis should change the orientation by the sign of the amount of the dilation: $\epsilon(\mathsf{diag}(a,1)) = \epsilon(\mathsf{diag}(1,a)) = [a]$;
(3) A shear transformation should preserve the orientation: $\epsilon(D) = 1$ for D an upper or a lower triangular matrix with ones on the diagonal.

Again if these are not obvious to you, look at the dot and the cross on the square in the applet.

Since each square matrix can be written as a product of elementary matrices by Theorem 2.2.3, there can be at most one mapping $\epsilon : GL(2;\mathbb{R}) \to \{+1,-1\}$ that satisfies the three properties above. But Theorem 4.4.1 will show that $\det(LM) = \det(L)\det(M)$, and together with Example 4.2.4 which calculates the determinant for an upper or lower triangular matrix, this shows that $M \mapsto [\mathsf{det}(M)]$ is a mapping with the three prescribed properties. So $\epsilon = [\mathsf{det}]$, as claimed. In other words, the sign of the determinant determines if the linear mapping preserves or reverses orientation.

A similar analysis works in higher dimensions, and in particular for real (3×3)-matrices where instead of "area scaling factor" I would write "volume scaling factor" and where instead of a clock face I would use the right-hand-rule. You can find the details of this point of view worked out succinctly in arbitrary dimension in Chapter 5 of the Linear Algebra book by Peter Lax.

It should now be intuitively clear why $\mathsf{det}(L) \neq 0$ is equivalent to L being invertible, which I will show rigorously in Theorem 4.4.2.

REMARK 4.2.5. Perhaps you should now think about the child's question "Why does a mirror switch left and right, but not up and down?". The correct answer is that the mirror no more switches left and right than it does up and down, but rather it switches backwards and forwards.

4.3. Characterising the Determinant

In the previous section I've shown you that the determinant of a real square matrix is related both to volume and to orientation. Determinants exist and are critical for more than just real matrices, however, so now I'm going to explain another important interpretation of the determinant which makes sense for an arbitrary field.

DEFINITION 4.3.1. *Let U, V and W be F-vector spaces. A* **bilinear form on $U \times V$ with values in** *W is a mapping $H : U \times V \to W$ which is a linear mapping in both of its entries. This means that it must satisfy the following properties for all $u_1, u_2 \in U$ and $v_1, v_2 \in V$ and all $\lambda \in F$:*

$$\begin{aligned} H(u_1+u_2, v_1) &= H(u_1,v_1) + H(u_2,v_1) \\ H(\lambda u_1, v_1) &= \lambda H(u_1,v_1) \\ H(u_1, v_1+v_2) &= H(u_1,v_1) + H(u_1,v_2) \\ H(u_1, \lambda v_1) &= \lambda H(u_1,v_1) \end{aligned}$$

The first two conditions state that for any fixed $v \in V$ the mapping $H(-,v) : U \to W$ is linear; the final two conditions state that for any fixed $u \in U$ the mapping $H(u,-) : V \to W$ is linear. If U, V and W are clear from the context I will simply say that H is a **bilinear form**. *A bilinear form H is* **symmetric** *if $U = V$ and*

$$H(u,v) = H(v,u) \quad \textit{for all } u, v \in U$$

while it is **alternating** *or* **antisymmetric** *if* $U = V$ *and*

$$H(u,u) = 0 \quad \textit{for all } u \in U$$

REMARK 4.3.2. Suppose that $H : U \times U \to W$ is an antisymmetric bilinear form on U with values in W. Then for all $u, v \in U$:

$$\begin{aligned} 0 &= H(u+v, u+v) \\ &= H(u, u+v) + H(v, u+v) \\ &= H(u,u) + H(u,v) + H(v,u) + H(v,v) \\ &= H(u,v) + H(v,u) \end{aligned}$$

Therefore an antisymmetric form always satisfies $H(u,v) = -H(v,u)$, hence the name. On the other hand, if H is a bilinear form satisfying $H(u,v) = -H(v,u)$ for all $u, v \in U$, then taking $u = v$ gives $H(u,u) = -H(u,u)$ from which it follows that $H(u,u) + H(u,u) = 0$. As long as $1_F + 1_F \neq 0_F$ I deduce that $H(u,u) = 0$ and so the form is antisymmetric. But remember that you know a field $F = \mathbb{F}_2$ in which $1_F + 1_F = 0_F$ so you do need to be careful.

DEFINITION 4.3.3. *Let $V_1, \ldots, V_n, W$ be F-vector spaces. A mapping $H : V_1 \times V_2 \times \cdots \times V_n \to W$ is a* **multilinear form** *or just* **multilinear** *if for each j the mapping $V_j \to W$ defined by $v_j \mapsto H(v_1, \ldots, v_j, \ldots, v_n)$, with the $v_i \in V_i$ arbitrary fixed vectors of V_i for $i \neq j$, is linear. In the case $n = 2$, this is exactly the definition of a bilinear mapping given above.*

DEFINITION 4.3.4. *Let V and W be F-vector spaces. A multilinear form $H : V \times \cdots \times V \to W$ is* **alternating** *if it vanishes on every n-tuple of elements of V that has at least two entries equal, in other words if:*

$$(\exists\, i \neq j \text{ with } v_i = v_j) \to H(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = 0$$

In the case $n = 2$, this is exactly the definition of an alternating or antisymmetric bilinear mapping given above.

REMARK 4.3.5. An alternating multilinear form H has the property

$$H(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -H(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n) \tag{9}$$

for all $v_1, \ldots, v_n \in V$. Combining this with Lemma 4.1.5 and Exercise 62 shows that for any $\sigma \in \mathfrak{S}_n$

$$H(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = \mathsf{sgn}(\sigma) H(v_1, \ldots, v_n)$$

Conversely, if (9) holds for a multilinear form H and arbitrary $v_1, \ldots, v_n \in V$ then H is alternating provided $1_F + 1_F \neq 0_F$.

THEOREM 4.3.6 (Characterisation of the Determinant). *Let F be a field. The mapping*

$$\mathsf{det} : \mathsf{Mat}(n; F) \to F$$

is the unique alternating multilinear form on n-tuples of column vectors with values in F that takes the value 1_F on the identity matrix.

There is a little jiggery-pokery going on here: I am simultaneously considering elements of $\mathsf{Mat}(n; F)$ as $(n \times n)$-matrices over F and as ordered lists n column vectors – the columns of the matrix. That's why I can think of the determinant as a mapping

$$\mathsf{det} : F^n \times \cdots \times F^n \to F, (v_1, \ldots, v_n) \mapsto \mathsf{det}(v_1 | \cdots | v_n)$$

PROOF. It's obvious from the Leibniz formula in Definition 4.2.1 that the determinant is multilinear and that it evaluates to 1_F on the identity matrix. To show that it is alternating, suppose that column i and j of an $(n \times n)$-matrix A are equal. If I take $\tau \in \mathfrak{S}_n$ to be the transposition that switches i and j, the equality of columns means that $a_{ij} = a_{i\tau(j)}$ for any i and j. This implies that

$a_{1\sigma(1)}\dots a_{n\sigma(n)} = a_{1\tau\sigma(1)}\dots a_{n\tau\sigma(n)}$ for any $\sigma \in \mathfrak{S}_n$. Furthermore $\mathsf{sgn}(\sigma) = -\mathsf{sgn}(\tau\sigma)$ by Lemma 4.1.5 and Example 4.1.4. Since $\tau^2 = \mathrm{id}_{\mathfrak{S}_n}$, $H = \{\mathrm{id}_{\mathfrak{S}_n}, \tau\} \leqslant \mathfrak{S}_n$ is the subgroup of $\mathfrak{S}_n$ generated by τ. Let $X \subset \mathfrak{S}_n$ be a set of right coset representatives of H in $\mathfrak{S}_n$, so that there is a disjoint union

$$\bigcup_{\sigma\in X} H\sigma = \mathfrak{S}_n$$

Then

$$\begin{aligned}\mathsf{det}(A) &= \sum_{\sigma\in\mathfrak{S}_n} \mathsf{sgn}(\sigma)a_{1\sigma(1)}\dots a_{n\sigma(n)} \\ &= \sum_{\sigma\in X} \big(\mathsf{sgn}(\sigma)a_{1\sigma(1)}\dots a_{n\sigma(n)} + \mathsf{sgn}(\tau\sigma)a_{1\tau\sigma(1)}\dots a_{n\tau\sigma(n)}\big) = 0.\end{aligned}$$

This confirms that det is alternating and multilinear.[1]

Now I must prove that there exists no other mapping $d : \mathsf{Mat}(n;F) \to F$ with the stated properties. Thanks to multilinearity, the mapping d will be completely determined by its values on n-tuples of basis vectors (this is a simple generalisation of the argument of Lemma 1.7.8). In other words d is determined by its values

$$d(e_{\sigma(1)}|\cdots|e_{\sigma(n)})$$

where $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ is an *arbitrary* mapping. But d is assumed to be alternating, so that means that if $\sigma(i) = \sigma(j)$ for some $i \neq j$, then $d(e_{\sigma(1)}|\cdots|e_{\sigma(n)}) = 0$. In other words if σ is not bijective, i.e. $\sigma \notin \mathfrak{S}_n$, then $d(e_{\sigma(1)}|\cdots|e_{\sigma(n)}) = 0$. It follows from Remark 4.3.5 that

$$d(e_{\sigma(1)}|\cdots|e_{\sigma(n)}) = \begin{cases}\mathsf{sgn}(\sigma)d(e_1|\cdots|e_n) & \sigma \in \mathfrak{S}_n \\ 0 & \text{otherwise}\end{cases}$$

Finally, $d(e_1|\cdots|e_n) = 1$ by assumption, and so d and det agree on all n-tuples of basis vectors and hence $d = \mathsf{det}$, as claimed. □

EXERCISE 64. Adapt the second part of the proof of Theorem 4.3.6 to show that: if $d : \mathsf{Mat}(n;F) \to F$ is an alternating multilinear form on n-tuples of column vectors with values in F, then

$$d(A) = d(e_1|\cdots|e_n)\mathsf{det}(A)$$

for all $A \in \mathsf{Mat}(n;F)$.

4.4. Rules for Calculating with Determinants

THEOREM 4.4.1 (Multiplicativity of the Determinant). *Let R be a commutative ring and let $A, B \in \mathsf{Mat}(n;R)$. Then*

$$\mathsf{det}(AB) = \mathsf{det}(A)\mathsf{det}(B).$$

[1] The argument here works verbatim to show that if A is an $(n \times n)$-matrix with coefficients in a commutative ring, then $\mathsf{det}(A) = 0$ if two columns of A are equal.

FIRST PROOF. Let $\mathfrak{T}_n = \text{Maps}(\{1,\dots,n\},\{1,\dots,n\})$. I calculate!

$$\begin{aligned}
\mathsf{det}(AB) &= \sum_{\sigma\in\mathfrak{S}_n} \mathsf{sgn}(\sigma)\prod_{i=1}^{n}(AB)_{i\sigma(i)}\\
&= \sum_{\sigma\in\mathfrak{S}_n} \mathsf{sgn}(\sigma)\prod_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{j\sigma(i)}\\
&= \sum_{\sigma\in\mathfrak{S}_n,\kappa\in\mathfrak{T}_n} \mathsf{sgn}(\sigma)a_{1\kappa(1)}b_{\kappa(1)\sigma(1)}\dots a_{n\kappa(n)}b_{\kappa(n)\sigma(n)}\\
&= \sum_{\kappa\in\mathfrak{T}_n} a_{1\kappa(1)}\dots a_{n\kappa(n)}\sum_{\sigma\in\mathfrak{S}_n}\mathsf{sgn}(\sigma)b_{\kappa(1)\sigma(1)}\dots b_{\kappa(n)\sigma(n)}\\
&= \sum_{\kappa\in\mathfrak{T}_n} a_{1\kappa(1)}\dots a_{n\kappa(n)}\mathsf{det}(B_\kappa)
\end{aligned}$$

where B_κ is the matrix obtained by using the rows of B labelled $\kappa(1),\dots,\kappa(n)$ for its rows 1 to n. It follows from the footnote in the proof of Theorem 4.3.6 that $\mathsf{det}(B_\kappa)=0$ if $\kappa\notin\mathfrak{S}_n$ and that $\mathsf{det}(B_\kappa)=\mathsf{sgn}(\kappa)\mathsf{det}(B)$ if $\kappa\in\mathfrak{S}_n$. From this it follows that

$$\sum_{\kappa\in\mathfrak{T}_n} a_{1\kappa(1)}\dots a_{n\kappa(n)}\mathsf{det}(B_\kappa) = \sum_{\kappa\in\mathfrak{S}_n}\mathsf{sgn}(\kappa)a_{1\kappa(1)}\dots a_{n\kappa(n)}\mathsf{det}(B) = \det(A)\det(B)$$

which is exactly what was required. □

SECOND PROOF, FOR FIELDS ONLY. Consider the mappings $\mathsf{Mat}(n;F)\to F$ given by $B\mapsto \mathsf{det}(A)\mathsf{det}(B)$ and by $B\mapsto\det(AB)$. Both are multilinear and alternating as functions in the columns of B, and produce $\mathsf{det}(A)$ when evaluated at $B=I_n$. It follows from Exercise 64 that the mappings must be equal. □

THEOREM 4.4.2 (Determinantal Criterion for Invertibility). *The determinant of a square matrix with entries in a field F is non-zero if and only if the matrix is invertible.*

PROOF. Let F be the field and let $A\in\mathsf{Mat}(n;F)$ be the matrix. I must show that

$$\mathsf{det}(A)\neq 0 \Leftrightarrow A \text{ is invertible}$$

Suppose first that A is invertible. Then there exists a matrix $B=A^{-1}$ such that $AB=I_n$. I use the multiplicativity of the determinant to deduce that $\mathsf{det}(A)\mathsf{det}(B)=\mathsf{det}(I_n)=1$ from which it follows that $\mathsf{det}(A)\neq 0$. This proves $\Leftarrow$. Conversely, if A is not invertible then it does not have full rank, as in Definition 2.2.8. Therefore I can find a column vector of A, which without loss of generality I will assume to be the first column, that is linearly dependent on the other column vectors. This means there exist $\lambda_2,\dots,\lambda_n\in F$ such that $a_{*1}=\lambda_2 a_{*2}+\dots+\lambda_n a_{*n}$. The multilinearity and alternating properties of the determinant then show

$$\begin{aligned}
\mathsf{det}(A) &= \mathsf{det}(\lambda_2 a_{*2}+\dots+\lambda_n a_{*n}|a_{*2}|\dots|a_{*n})\\
&= \lambda_2\mathsf{det}(a_{*2}|a_{*2}|\dots|a_{*n})+\dots+\lambda_n\mathsf{det}(a_{*n}|a_{*2}|\dots|a_{*n})\\
&= \lambda_2 0+\dots+\lambda_n 0\\
&= 0
\end{aligned}$$

This proves the other implication $\to$. □

REMARK 4.4.3. There are two quick consequences of Theorem 4.4.1 and Theorem 4.4.2 . First, if A is invertible then $\mathsf{det}(A^{-1})=\mathsf{det}(A)^{-1}$. From this, the second consequence follows: if B is a

square matrix B then

$$\det(A^{-1}BA) = \det(B) \tag{10}$$

You should recognise this second fact as **very important**. Why? Well, remember that if $f \in \mathrm{End}(V)$ is an endomorphism of some finite dimensional vector space V, then a choice of ordered basis $\mathcal{A}$ for V produces a square matrix ${}_{\mathcal{A}}[f]_{\mathcal{A}}$ and hence I can associate the scalar $\det({}_{\mathcal{A}}[f]_{\mathcal{A}})$ to f and $\mathcal{A}$. If $\mathcal{B}$ is another ordered basis of V, then I get another scalar $\det({}_{\mathcal{B}}[f]_{\mathcal{B}})$. But combining (3) with (10) shows that these two scalars are equal. In other words, I can define the **determinant of the endomorphism** f, $\det(f|V)$ or just $\det(f)$ if the vector space V is clear from the context, as this scalar and this is independent of the choice of basis I use to calculate it (in other words, well-defined!). If you think back to the description of the determinant of an endomorphism of $\mathbb{R}^2$ as a measuring scaling and orientation, this shouldn't surprise you.

EXERCISE 65. Recall from Exercise 7 that a finite dimensional $\mathbb{C}$-vector space V can be considered as an $\mathbb{R}$-vector space too, which I will denote $V_{\mathbb{R}}$. Let $f \in \mathrm{End}_{\mathbb{C}}(V)$ be an endomorphism of V as $\mathbb{C}$-vector space. Show that: f is also an endomorphism of $V_{\mathbb{R}}$ and that $\det(f|V_{\mathbb{R}}) = |\det(f|V)|^2$.

LEMMA 4.4.4. *The determinant of a square matrix and of the transpose of the square matrix are equal, that is for all $A \in \mathsf{Mat}(n; R)$ with R a commutative ring*

$$\det(A^{\mathsf{T}}) = \det(A)$$

PROOF. By definition,

$$\det(A^{\mathsf{T}}) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$$

If $\tau = \sigma^{-1}$ then $\mathrm{sgn}(\tau) = \mathrm{sgn}(\sigma)$ (this is obvious: think of the pictures I used, for instance, when discussing sgn) and also $a_{\sigma(1)1} \dots a_{\sigma(n)n} = a_{1\tau(1)} \dots a_{n\tau(n)}$, where this equality might swap the order of multiplication, which is fine since all $a_{ij} \in R$, a commutative ring. It follows that

$$\det(A^{\mathsf{T}}) = \sum_{\tau \in \mathfrak{S}_n} \mathrm{sgn}(\tau) a_{1\tau(1)} \dots a_{n\tau(n)} = \det(A)$$

□

REMARK 4.4.5. Apart from showing that the determinant is a natural object, and apart from being a powerful abstract tool, Theorem 4.3.6 is very useful for calculation. Why? Recall from Example 4.2.3 that the determinant of an $(n \times n)$-matrix is unpleasant to calculate if $n \geqslant 4$. Combined with Lemma 4.4.4, however, the theorem demonstrates that Gaussian elimination fits perfectly with the determinant: performing [*Row Addition*] doesn't change the determinant, while performing [*Row Swap*] changes the sign only. When Gaussian elimination is completed the final matrix has staircase form so is upper triangular from which the determinant can be easily calculated as in Example 4.2.4 by multiplying the entries of the diagonal together.

Any niggling doubt you might have harboured about the definition of a determinant should now disappear, for I am now going to compare the determinant with the version you were shown in Introduction to Linear Algebra.

DEFINITION 4.4.6. *Let $A \in \mathsf{Mat}(n; R)$ for some commutative ring R and natural number n. Let i and j be integers between 1 and n. Then the (i, j)* **cofactor of** *A is $C_{ij} = (-1)^{i+j} \det(A\langle i, j\rangle)$ where $A\langle i, j\rangle$ is*

the matrix I obtain from A be deleting the i-th row and the j-th column.

$$C_{23} = (-1)^{2+3}\mathsf{det}\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = -a_{11}a_{32} + a_{31}a_{12}$$

THEOREM 4.4.7 (Laplace's Expansion of the Determinant). *Let $A = (a_{ij})$ be an $(n \times n)$-matrix with entries from a commutative ring R. For a fixed i the* **i-th row expansion of the determinant** *is*

$$\mathsf{det}(A) = \sum_{j=1}^{n} a_{ij}C_{ij}$$

and for a fixed j the **j-th column expansion of the determinant** *is*

$$\mathsf{det}(A) = \sum_{i=1}^{n} a_{ij}C_{ij}$$

PROOF. Since $\mathsf{det}(A) = \mathsf{det}(A^{\mathsf{T}})$ I only need to prove the second of the two formulas. Now I've already shown you in Exercise 61 that the determinant of a square matrix only changes by a factor of $(-1)^{j-1}$ when I move the j-th column of the matrix all the way through to the first column. So that means that it will be enough for me to prove the second statement for the case $j = 1$, that is by expanding down the first column.

Write the matrix as a list of column vectors $A = (a_{*1}|a_{*2}|\dots|a_{*n})$. I write the first column as a linear combination of the standard basis vectors

$$a_{*1} = a_{11}e_1 + \cdots + a_{n1}e_n$$

The multilinearity of the determinant then shows that

$$\mathsf{det}(A) = \sum_{i=1}^{n} a_{i1}\mathsf{det}(e_i|a_{*2}|\dots|a_{*n})$$

Now I move the i-th row of the matrix $(e_i|a_{*2}|\dots|a_{*n})$ to the top, at the cost of multiplying by the factor $(-1)^{i-1}$. The matrix now has the form of a block-upper triangular matrix

$$\left(\begin{array}{c|c} 1 & * \\ \hline 0 & A\langle i,j\rangle \end{array}\right)$$

It follows from Exercise 63 then that

$$\mathsf{det}(e_i|a_{*2}|\dots|a_{*n}) = (-1)^{i-1}\det(A\langle i,j\rangle)$$

as required. □

DEFINITION 4.4.8. *Let A be an $(n \times n)$-matrix with entries in a commutative ring R. The* **adjugate matrix** $\mathsf{adj}(A)$ *is the $(n \times n)$-matrix whose entries are $\mathsf{adj}(A)_{ij} = C_{ji}$ where C_{ji} the (j,i)-cofactor as defined in Definition 4.4.6.*

THEOREM 4.4.9 (Cramer's Rule). *Let A be an $(n \times n)$-matrix with entries in a commutative ring R. Then*

$$A \cdot \mathsf{adj}(A) = (\mathsf{det}A)I_n$$

REMARK 4.4.10. In many sources, such as Wikipedia, Cramer's Rule means the formula:

$$x_i = \frac{\mathsf{det}(a_{*1}|\dots|b_*|\dots|a_{*n})}{\mathsf{det}(a_{*1}|\dots|a_{*i}|\dots|a_{*n})}$$

for solving in a field F the system $A\vec{x} = \vec{b}$ of n linear equations in n unknowns, provided that a unique solution exists. A unique solution exists if and only if A is invertible. So, instead of applying the Gaussian algorithm, you can calculate lots of determinants, replacing the i-th column of A by the given solution vector $\vec{b}$. It turns out that if you implement this rule on a computer, it has the same efficiency as the Gaussian algorithm. The relationship between this version of Cramer's rule and Theorem 4.4.9 is gotten by successively taking the vector $\vec{b}$ in the system of linear equations to be the standard basis elements $\vec{e}_i$ with $1 \leqslant i \leqslant n$.

PROOF. I have to prove for each i and k that $\sum_{j=1}^{n} a_{ij}\mathsf{adj}(A)_{jk} = \delta_{ik}\mathsf{det}(A)$. In other words that

$$\sum_{j=1}^{n} a_{ij}C_{kj} = \delta_{ik}\mathsf{det}(A)$$

The case $i = k$ then states that

$$\sum_{j=1}^{n} a_{ij}C_{ij} = \mathsf{det}(A)$$

and this is just the formula for the i-th row expansion of the determinant. Now suppose that $i \neq k$ and let $\tilde{A}$ be the matrix all of whose entries agree with those of A except along the k-th row, where I replace the entries a_{kj} for $1 \leqslant j \leqslant n$ with a_{ij}. Then the k-th row expansion of the determinant of $\tilde{A}$ gives

$$\mathsf{det}(\tilde{A}) = \sum_{j=1}^{n} \tilde{a}_{kj}C_{kj} = \sum_{j=1}^{n} a_{ij}C_{kj}$$

But the i-th and k-th rows of $\tilde{A}$ are equal, so the multilinearity of the determinant implies that $\mathsf{det}(\tilde{A}) = 0$, as required. □

COROLLARY 4.4.11 (Invertibility of Matrices). *A square matrix with entries in a commutative ring R is invertible if and only if its determinant is a unit in R. That is, $A \in \mathsf{Mat}(n; R)$ is invertible if and only if $\mathsf{det}(A) \in R^{\times}$.*

So for instance, an integral matrix $A \in \mathsf{Mat}(n; \mathbb{Z})$ is invertible if and only $\mathsf{det}(A)$ is 1 or -1, since $\mathbb{Z}^{\times} = \{\pm 1\}$. On the other hand, a matrix $A \in \mathsf{Mat}(n; F)$ with entries in a field F is invertible if and only if $\mathsf{det}(A) \neq 0$ since $F^{\times}$ consists of the non-zero elements of F.

PROOF. If $A, B \in \mathsf{Mat}(n; R)$ are matrices such that $AB = I_n$, then $\mathsf{det}(A)\mathsf{det}(B) = \mathsf{det}(I_n) = 1_R$ by Theorem 4.4.1. Therefore $\mathsf{det}(A)$ is a unit in R. On the other hand, if $\mathsf{det}(A)$ is a unit in R then I can consider the matrix $B = \mathsf{det}(A)^{-1}\mathsf{adj}(A) \in \mathsf{Mat}(n; R)$, and by Cramer's Rule it has the property that $AB = I_n$. This is not yet enough for invertibility because I need also to prove that there exists some $C \in \mathsf{Mat}(n; R)$ such that $CA = I_n$, see Definition 2.2.1. Since $\mathsf{det}(A^{\mathsf{T}}) = \mathsf{det}(A)$ is a unit, I can use Cramer's Rule again to find another matrix $\tilde{C} \in \mathsf{Mat}(n; R)$ such that $A^{\mathsf{T}}\tilde{C} = I_n$. Taking the transpose of this equation gives $\tilde{C}^{\mathsf{T}}A = I_n$ since $(A^{\mathsf{T}})^{\mathsf{T}} = A$ and $I_n^{\mathsf{T}} = I_n$ and transposition swaps the order of multiplication. So $C = \tilde{C}^{\mathsf{T}}$ does the trick. □

REMARK 4.4.12. Of course, in the above proof B and C must be equal. For if I multiply the equation $CA = I_n$ on the right by B I get the equation $C = B$.

4.5. Eigenvalues and Eigenvectors

DEFINITION 4.5.1. *Let $f : V \to V$ be an endomorphism of an F-vector space V. A scalar $\lambda \in F$ is an* **eigenvalue of** *f if and only if there exists a non-zero vector $\vec{v} \in V$ such that $f(\vec{v}) = \lambda\vec{v}$. Each such*

vector is called an **eigenvector of f with eigenvalue λ.** *For any $\lambda \in F$, the* **eigenspace of f with eigenvalue λ** *is*

$$E(\lambda, f) = \{\vec{v} \in V : f(\vec{v}) = \lambda\vec{v}\}$$

EXAMPLE 4.5.2. An eigenvector of a linear mapping with eigenvalue 1 is the exactly the same as a non-zero fixed point of f. An eigenvector of a linear mapping with eigenvalue 0 is the exactly the same as a non-zero element in the kernel of the linear mapping.

EXAMPLE 4.5.3. Here are few intuitive examples. Turning a sheet of paper by 90 degrees anti-clockwise has no real eigenvalues. On the other hand, rotating it by 180 degrees has the eigenvalue -1. Reflecting the piece of paper has an eigenvector with eigenvalue of 1, gotten from any non-zero vector along the axis-of-symmetry. Differentiation of real polynomials has only one eigenvalue, 0, with a corresponding eigenvector being any non-zero constant polynomial.

EXERCISE 66. Let $f : V \to V$ be an endomorphism of an F-vector space V. Show that for any $\lambda \in F$ $E(\lambda, f)$ is a subspace of V.

When V is finite dimensional for almost all $\lambda \in F$ the subspace $E(\lambda, f)$ is zero because there are no eigenvectors with eigenvalue λ. Said more precisely, the non-zero elements of $E(\lambda, f)$ are the eigenvectors of f with eigenvalue λ. But there is a fantastic theorem on eigenvectors and eigenvalues. It should surprise you, except for the fact that you met it in Introduction to Linear Algebra and you have been using all over Honours Differential Equations. I will prove this a bit later in this section, but I was impatient to show it to you.

THEOREM 4.5.4 (Existence of Eigenvalues). *Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue.*

REMARK 4.5.5. You saw already in Example 4.5.3 that the algebraically closed hypothesis in the theorem is necessary: rotation in $\mathbb{R}^2$ by 90 degrees had no eigenvalues. That the vector space should be non-zero in the statement of the theorem is natural – how else could I produce a non-zero vector? – but that the space should be finite dimensional is not obvious. But you can quickly find an example of an endomorphism of an infinite dimensional vector space with no eigenvalue: namely, let $V = \mathbb{C}[X]$ and take the endomorphism to multiplication by X, that is $P \mapsto XP$.

DEFINITION 4.5.6. *Let R be a commutative ring and let $A \in \mathsf{Mat}(n; R)$ be a square matrix with entries in R. The polynomial $\det(A - xI_n) \in R[x]$ is called the* **characteristic polynomial of the matrix** *A. It is denoted by*

$$\chi_A(x) := \det(A - xI_n)$$

where χ stands for χaracteristic.

REMARK 4.5.7. Previously in the notes I wrote $R[X]$ for the ring of polynomials on one variable with coefficients in the ring R, and suddenly $R[x]$ has appeared instead. I'm going to use this notation for the rest of this chapter. I prefer lower case x for the variable to upper case X right now, simply to make it absolutely clear that x is a variable and not a matrix. Personally I find that displaying $\det(A - XI_n)$ makes me confused as I start to think that X is a square matrix. Which it is not supposed to be. So I'll stick with $\det(A - xI_n)$.

THEOREM 4.5.8 (Eigenvalues and Characteristic Polynomials). *Let F be a field and $A \in \mathsf{Mat}(n; F)$ a square matrix with entries in F. The eigenvalues of the linear mapping $A : F^n \to F^n$ are exactly the roots of the characteristic polynomial χ_A.*

PROOF. This turns out to be easy! The following are equivalent for a scalar, $\lambda \in F$:

$$\begin{aligned}
(\lambda \text{ is an eigenvalue of } A) &\Leftrightarrow \exists\, v \neq 0 \text{ with } Av = \lambda v \\
&\Leftrightarrow \exists\, v \neq 0 \text{ with } (A - \lambda I_n)v = 0 \\
&\Leftrightarrow \ker(A - \lambda I_n) \neq 0 \\
&\Leftrightarrow \det(A - \lambda I_n) = 0 \\
&\Leftrightarrow \chi_A(\lambda) = 0
\end{aligned}$$

□

EXERCISE 67. Let F be a field and $A \in \mathsf{Mat}(n; F)$ a square matrix with coefficients in F. Show that: the characteristic polynomial of A has the form

$$\chi_A(x) = (-x)^n + \mathrm{tr}(A)(-x)^{n-1} + \cdots + \det(A).$$

Prosaically, the leading coefficient is $(-1)^n$, the next term has the trace of A as its coefficient, and the constant term is the determinant of A.

REMARK 4.5.9. (1) Recall from Example 3.5.2 that square matrices $A, B \in \mathsf{Mat}(n; R)$ of the same size are *conjugate* if

$$B \;=\; P^{-1}AP \in \mathsf{Mat}(n; R)$$

for an invertible $P \in \mathsf{GL}(n; R)$. Conjugacy is an equivalence relation on $\mathsf{Mat}(n; R)$. (The definition makes sense for any commutative ring R, although we shall be mainly concerned with the case of a field).

(2) The motivation for conjugacy comes from the various matrix representations of an endomorphism $f : V \to V$ of an n-dimensional vector space V over a field F. Let $A = (a_{ij}) =_{\mathcal{A}} [f]_{\mathcal{A}}$, $B = (b_{ij}) =_{\mathcal{B}} [f]_{\mathcal{B}} \in \mathsf{Mat}(n; F)$ be the matrices of f with respect to bases $\mathcal{A} = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)$, $\mathcal{B} = (\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_n)$ for V

$$f(\vec{v}_j) \;=\; \sum_{i=1}^{n} a_{ij}\vec{v}_i \;,\; f(\vec{w}_j) \;=\; \sum_{i=1}^{n} b_{ij}\vec{w}_i \in V \;.$$

The change of basis matrix $P = (p_{ij}) =_{\mathcal{A}} [\mathrm{id}_V]_{\mathcal{B}} \in \mathsf{Mat}(n; F)$ is invertible, with

$$\vec{w}_j \;=\; \sum_{i=1}^{n} p_{ij}\vec{v}_i \in V \;.$$

We have the identity

$$B \;=\; P^{-1}AP \in \mathsf{Mat}(n; F) \;,$$

so A, B are conjugate.

(3) **Key observation**: the characteristic polynomials of conjugate $A, B \in \mathsf{Mat}(n, R)$ are the same

$$\begin{aligned}
\chi_B(x) \;&=\; \det(B - xI_n) \;=\; \det(P^{-1}AP - xI_n) \\
&=\; \det(P^{-1}(A - xI_n)P) \;=\; \det(P)^{-1}\det(A - xI_n)\det(P) \\
&=\; \det(A - xI_n) \;=\; \chi_A(x) \in R[x] \;.
\end{aligned}$$

(4) In view of (2) and (3) we can define the characteristic polynomial of an endomorphism $f : V \to V$ of an n-dimensional vector space over a field F to be

$$\chi_f(x) \;=\; \chi_A(x) \in F[x]$$

with $A =_{\mathcal{A}} [f]_{\mathcal{A}} \in \mathsf{Mat}(n; R)$ the matrix of f with respect to *any* basis $\mathcal{A}$ for V. Thanks to Theorem 4.5.8 the eigenvalues of f are exactly the roots of χ_f, the characteristic polynomial of f.

EXERCISE 68. Show that: every endomorphism of an odd-dimensional real vector space has a real eigenvalue. Show furthermore that: if the determinant of the endomorphism is a positive real number, then the endomorphism even has a positive real eigenvalue.

REMARK 4.5.10. Let $f : V \to V$ be an endomorphism of an n-dimensional vector space V over a field F. Suppose given an m-dimensional subspace $W \subseteq V$ such that $f(W) \subseteq W$, so that there are defined endomorphisms of the subspace and the quotient space

$$\begin{aligned} g &: W \to W \; ; \; \vec{w} \mapsto f(\vec{w}) \; , \\ h &: V/W \to V/W \; ; \; W + \vec{v} \mapsto W + f(\vec{v}) \; . \end{aligned}$$

Any ordered basis $\mathcal{A} = (\vec{w}_1, \vec{w}_2, \dots, \vec{w}_m)$ for W can be extended to an ordered basis for V

$$\mathcal{B} \; = \; (\vec{w}_1, \vec{w}_2, \dots, \vec{w}_m, \vec{v}_{m+1}, \vec{v}_{m+2} \dots, \vec{v}_n) \; .$$

The images of the $\vec{v}_j$'s under the canonical projection $\mathsf{can} : V \to V/W$ are then an ordered basis for V/W

$$\mathcal{C} \; = \; (\mathsf{can}(v_{m+1}), \mathsf{can}(v_{m+2}), \dots, \mathsf{can}(\vec{v}_n)) \; .$$

Let $a_{ij}, b_{jk}, c_{ik} \in F$ be the coefficients in the linear combinations

$$f(\vec{w}_j) \; = \; \sum_{i=1}^{m} a_{ij}\vec{w}_i \in W \; , \; f(\vec{v}_k) \; = \; \sum_{j=m+1}^{n} b_{jk}\vec{v}_j + \sum_{i=1}^{m} c_{ik}\vec{w}_i \in V$$

and define the linear map

$$e \; : \; V/W \to W \; ; \; W + \vec{v}_k \mapsto \sum_{i=1}^{m} c_{ik}\vec{w}_i \; .$$

The $n \times n$ matrix of f with respect to the basis $\mathcal{A}$ is

$${}_{\mathcal{B}}[f]_{\mathcal{B}} \; = \; \begin{pmatrix} {}_{\mathcal{A}}[g]_{\mathcal{A}} & {}_{\mathcal{A}}[e]_{\mathcal{C}} \\ 0 & {}_{\mathcal{C}}[h]_{\mathcal{C}} \end{pmatrix} \; = \; \begin{pmatrix} a_{ij} & c_{ik} \\ 0 & b_{jk} \end{pmatrix}$$

blocked as an $\begin{pmatrix} m \times m & m \times (n-m) \\ (n-m) \times m & (n-m) \times (n-m) \end{pmatrix}$ matrix. Applying Exercise 63 to the $n \times n$ matrix with entries in $F[x]$

$${}_{\mathcal{B}}[f]_{\mathcal{B}} - xI_n \; = \; \begin{pmatrix} {}_{\mathcal{A}}[g]_{\mathcal{A}} - xI_m & {}_{\mathcal{A}}[e]_{\mathcal{C}} \\ 0 & {}_{\mathcal{C}}[h]_{\mathcal{C}} - xI_{n-m} \end{pmatrix} \; = \; \begin{pmatrix} a_{ij} - xI_m & c_{ik} \\ 0 & b_{jk} - xI_{n-m} \end{pmatrix}$$

we have that the characteristic polynomial of f is the product of the characteristic polynomials of g and h

$$\begin{aligned} \chi_f(x) \; &= \; \mathsf{det}({}_{\mathcal{B}}[f]_{\mathcal{B}} - xI_n) \\ &= \; \mathsf{det}({}_{\mathcal{A}}[g]_{\mathcal{A}} - xI_m)\mathsf{det}({}_{\mathcal{C}}[h]_{\mathcal{C}} - xI_{n-m}) \\ &= \; \chi_g(x)\chi_h(x) \in F[x] \; . \end{aligned}$$

PROOF OF THEOREM 4.5.4. Theorem 4.5.4 states that every endomorphism of a non-zero vector space over an algebraically closed field F has an eigenvalue. To see why this is true, you only need to notice that the characteristic polynomial $\chi_f \in F[x]$ is not constant. Then the definition of algebraically closed kicks in to say that since F is algebraically closed χ_f must have at least one root in F, say $\lambda \in F$. But then Remark 4.5.9 (4) demonstrates that λ is an eigenvalue of f. □

4.6. Triangularisable, Diagonalisable, and the Cayley-Hamilton Theorem

Remember that in Exercise 2 of the 2nd Workshop you proved that $A \in \mathsf{Mat}(n;F)$ satisfies a polynomial equation: there exists $P \in F[x]$ such that $P(A) = 0$. I will now tell you what that polynomial is, and I will show you that it is even possible to replace F with R, an arbitrary commutative ring.

PROPOSITION 4.6.1 (Triangularisability). *Let $f : V \to V$ be an endomorphism of a finite dimensional F-vector space V. The following two statements are equivalent:*

(1) The vector space V has an ordered basis $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)$ such that

$$\begin{aligned} f(\vec{v}_1) &= a_{11}\vec{v}_1 \,, \\ f(\vec{v}_2) &= a_{12}\vec{v}_1 + a_{22}\vec{v}_2 \,, \\ &\vdots \\ f(\vec{v}_n) &= a_{1n}\vec{v}_1 + a_{2n}\vec{v}_2 + \cdots + a_{nn}\vec{v}_n \in V \end{aligned}$$

(so that the first basis vector $\vec{v}_1$ is an eigenvector, with eigenvalue a_{11}) or equivalently such that the $n \times n$ matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}} = (a_{ij})$ representing f with respect to $\mathcal{B}$ is upper triangular

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ 0 & a_{22} & a_{23} & \ldots & a_{2n} \\ 0 & 0 & a_{33} & \ldots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & a_{nn} \end{pmatrix} .$$

When this happens, I will say that f is **triangularisable**.

(2) The characteristic polynomial $\chi_f(x)$ of f decomposes into linear factors in $F[x]$.

PROOF. $1 \to 2$: This is clear from Example 4.2.4 which describes the determinant of an upper triangular matrix: if ${}_{\mathcal{B}}[f]_{\mathcal{B}} = (a_{ij})$ is upper triangular with diagonal entries $a_{ii} = \lambda_i$ then $\chi_f(x) = (\lambda_1 - x)\cdots(\lambda_n - x)$.

$2 \to 1$: I'm going to prove this by induction on $n = \dim(V)$.

The case $n = 1$: the matrix is (1×1) with respect to any basis, so is upper triangular!

Induction hypothesis: Assume $n > 1$ and that the result is true for endomorphisms of $(n-1)$-dimensional vector spaces.

I will now prove the result for n. By hypothesis there is a root $a_{11} \in F$ of the polynomial $\chi_f(x) \in F[x]$, and so Theorem 4.5.8 and Remark 4.5.10 show that a_{11} is an eigenvalue of f, with an eigenvector $\vec{v}_1 \neq \vec{0} \in V$ such that $f(\vec{v}_1) = a_{11}\vec{v}_1 \in V$. The 1-dimensional subspace $W = \{\mu\vec{v}_1 | \mu \in F\} \subseteq V$ is such that $f(W) \subseteq W$, so we can proceed as in Remark 4.5.9 (2) to define endomorphisms $g : W \to W$, $h : V/W \to V/W$. It follows from

$$\chi_f(x) = \chi_g(x)\chi_h(x) = (a_{11} - x)\chi_h(x) \in F[x]$$

and the hypothesis that $\chi_f(x)$ decomposes into linear factors in $F[x]$ that $\chi_h(x)$ also decomposes into linear factors in $F[x]$, namely all the linear factors of $\chi_f(x)$ except for one $(a_{11} - x)$. (We are using Theorem 3.3.4 here, the division algorithm for polynomials with coefficients in the field F). The subspace $W \subseteq V$ has basis $\mathcal{A} = (\vec{v}_1)$ such that ${}_{\mathcal{A}}[g]_{\mathcal{A}} = (a_{11})$. The quotient space V/W is $(n-1)$-dimensional, and by the inductive hypothesis there is an ordered basis $\mathcal{D} = (\vec{u}_2, \vec{u}_3, \ldots, \vec{u}_n)$

for V/W such that the $(n-1)\times(n-1)$-matrix ${}_{\mathcal{D}}[h]_{\mathcal{D}}$ is upper triangular, say

$$ {}_{\mathcal{D}}[h]_{\mathcal{D}} \;=\; \begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix} . $$

For each $\vec{u}_j \in V/W$ $(2 \leqslant j \leqslant n)$ choose a vector $\vec{v}_j \in V$ with $\mathsf{can}(\vec{v}_j) = \vec{u}_j$. It follows from

$$ h(\vec{u}_j) - \sum_{i=2}^{n} a_{ij}\vec{u}_i \;=\; \vec{0}_{V/W} \in V/W $$

that

$$ \mathsf{can}(f(\vec{v}_j) - \sum_{i=2}^{n} a_{ij}\vec{v}_i) \;=\; h(\vec{u}_j) - \sum_{i=2}^{n} a_{ij}\vec{u}_i \;=\; \vec{0}_{V/W} \;=\; W + \vec{0}_V \in V/W \,, $$

so that $f(\vec{v}_j) - \sum\limits_{i=2}^{n} a_{ij}\vec{v}_i \in W \subseteq V$, say

$$ f(\vec{v}_j) - \sum_{i=2}^{n} a_{ij}\vec{v}_i \;=\; a_{1j}\vec{v}_1 \; (2 \leqslant j \leqslant n) \in W \,. $$

Putting all this together gives

$$ f(\vec{v}_j) \;=\; \sum_{i=1}^{n} a_{ij}\vec{v}_i \in V \; (1 \leqslant j \leqslant n) $$

with $a_{ij} = 0 \in F$ for $i > j$. The ordered basis $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$ for V is such that the $n \times n$-matrix

$$ {}_{\mathcal{B}}[f]_{\mathcal{B}} \;=\; \begin{pmatrix} {}_{\mathcal{A}}[g]_{\mathcal{A}} & {}_{\mathcal{A}}[e]_{\mathcal{D}} \\ 0 & {}_{\mathcal{D}}[h]_{\mathcal{D}} \end{pmatrix} \;=\; \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix} . $$

is upper triangular, with $e : V/W \to W; \vec{u}_j \mapsto a_{1j}\vec{v}_1$. □

REMARK 4.6.2. (1) An endomorphism $A : F^n \to F^n$ is triangularisable if and only if $A = (a_{ij})$ is conjugate to an upper triangular matrix $B = (b_{ij})$ ($b_{ij} = 0$ for $i > j$), with $P^{-1}AP = B$ for an invertible matrix P.
(2) Combining Proposition 4.6.1 with Theorem 3.3.14 shows that any endomorphism of a finite dimensional $\mathbb{C}$-vector space is triangularisable. On the other hand there are endomorphisms of $\mathbb{R}$-vector spaces that are non triangularisable, for instance the endomorphism of $\mathbb{R}^2$ given by rotation anticlockwise by θ radians is represented in the standard basis by the matrix

$$ R := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} $$

and therefore has characteristic polynomial $\chi_R(x) = x^2 - 2x\cos\theta + 1$. You can check that this has real roots if and only if $\cos\theta = \pm 1$, that is if and only if θ is an integral multiple of π. So, by Proposition 4.6.1 this endomorphism is not triangularisable unless $\theta = n\pi$ for some $n \in \mathbb{Z}$.
(3) An endomorphism $f : V \to V$ of an n-dimensional F-vector space V is triangularisable if and only if there is a sequence of subspaces

$$ V_0 \;=\; \{0\} \subset V_1 \subset V_2 \subset \cdots \subset V_n \;=\; V $$

such that V_i is i-dimensional and $f(V_i) \subseteq V_i$. In the proof of Proposition 4.6.1 V_i is the subspace of V spanned by $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_i$. Each quotient space V_i/V_{i-1} is 1-dimensional with the endomorphism

$$f_i \ : \ V_i/V_{i-1} \to V_i/V_{i-1} \ ; \ V_{i-1} + \vec{v} \mapsto V_{i-1} + f(\vec{v}) \ = \ V_{i-1} + \lambda_i \vec{v}$$

given by scalar multiplication by the ith root $\lambda_i \in F$ of the characteristic polynomial

$$\chi_f(x) \ = \ (\lambda_1 - x)(\lambda_2 - x) \ldots (\lambda_n - x) \in F[x] \ .$$

(4) We have already seen the value of triangular matrices (not just square ones) in Gaussian elimination. Triangular matrices play an important role in numerical analysis. For example, if $A = (a_{ij}) \in \mathsf{Mat}(n; F)$ is an upper triangular $n \times n$ matrix which is invertible (so that each $a_{ii} \neq 0 \in F$), then a system of simultaneous linear equations

$$\sum_{j=i}^{n} a_{ij} x_j \ = \ b_i \in F \ (i = 1, 2, \ldots, n)$$

can be solved for $x_n, x_{n-1}, \ldots, x_1 \in F$ using only division by the non-zero diagonal entries a_{ii} and addition and subtraction

$$\begin{aligned} x_n \ &= \ b_n/a_{nn} \ , \\ x_{n-1} \ &= \ (b_{n-1} - a_{n-1\,n} x_n)/a_{n-1\,n-1} \ , \\ &\vdots \\ x_1 \ &= \ (b_1 - \sum_{j=2}^{n} a_{1j} x_j)/a_{11} \in F \ . \end{aligned}$$

EXAMPLE 4.6.3. Let $f : \mathbb{R}^3 \to \mathbb{R}^3$ be represented in the standard basis by the matrix

$$[f] = \begin{pmatrix} 14 & 8 & 3 \\ -17 & -9 & -3 \\ 1 & 0 & 0 \end{pmatrix}$$

I've highlighted the entries that show that the matrix is not in upper triangular form yet. Then, using your pen and paper, or Wolfram Alpha, $\chi_f(x) = -x^3 + 5x^2 - 7x + 3 = (1-x)^2(3-x)$ so that the eigenvalues of f are 1 and 3 and Proposition 4.6.1 implies that f is triangularisable. To find a basis for $\mathbb{R}^3$ that produces an upper triangular matrix representing f, I study the eigenvalue 3:

$$[f] - 3I_3 = \begin{pmatrix} 11 & 8 & 3 \\ -17 & -12 & -3 \\ 1 & 0 & -3 \end{pmatrix}$$

Let W be the image of this matrix. By looking at the columns of the matrix I see that W has a basis $\mathcal{A} = \{\vec{w}_1 = (2, -3, 0)^{\mathsf{T}}, \vec{w}_2 = (1, -1, -1)^{\mathsf{T}}\}$. According to the proof of Proposition 4.6.1 I should now consider $f|_W$:

$$f(\vec{w}_1) = \begin{pmatrix} 14 & 8 & 3 \\ -17 & -9 & -3 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ -3 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix} = 3\vec{w}_1 - 2\vec{w}_2$$

and

$$f(\vec{w}_2) = \begin{pmatrix} 14 & 8 & 3 \\ -17 & -9 & -3 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 3 \\ -5 \\ 1 \end{pmatrix} = 2\vec{w}_1 - \vec{w}_2$$

So, if I extend the basis $\mathcal{A}$ of W to a basis $\mathcal{B}$ of V, say $\mathcal{B} = \{\vec{w}_1, \vec{w}_2, \vec{e}_1\}$, I use $f(\vec{e}_1) = 6\vec{w}_1 - \vec{w}_2 + 3\vec{e}_1$ to find

$$_{\mathcal{B}}[f]_{\mathcal{B}} = \left(\begin{array}{cc|c} 3 & 2 & 6 \\ -2 & -1 & -1 \\ \hline 0 & 0 & 3 \end{array}\right) = \left(\begin{array}{c|c} {}_{\mathcal{A}}[f]_{\mathcal{A}} & * \\ \hline 0 & 3 \end{array}\right)$$

The characteristic polynomial of $f|_W$ is $\chi_{f|_W}(x) = x^2 - 2x + 1 = (1-x)^2$. I now study the eigenvalue 1:

$$_{\mathcal{A}}[f|_W]_{\mathcal{A}} - 1I_2 = \begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix}$$

The image of this mapping, which I'll call U, is $\langle (1,-1)^T = \vec{w}_1 - \vec{w}_2 \rangle$. Again, according to the proof of Proposition 4.6.1, I should consider $f|_U$:

$$f(\vec{w}_1 - \vec{w}_2) = \begin{pmatrix} 14 & 8 & 3 \\ -17 & -9 & -3 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} = \vec{w}_1 - \vec{w}_2$$

So I should pick a basis whose first element is $\vec{w}_1 - \vec{w}_2$ is a basis of U, whose second element extends this to a basis of W, say $\vec{w}_1$, and whose third element extends this to a basis of V, say $\vec{e}_1$. Now I calculate the matrix representing f with respect to the basis $\mathcal{B}' = \{\vec{w}_1 - \vec{w}_2, \vec{w}_1, \vec{e}_1\} = \{(1,-2,1)^{\mathsf{T}}, (2,-3,0)^{\mathsf{T}}, (1,0,0)^{\mathsf{T}}\}$ to be:

$$_{\mathcal{B}'}[f]_{\mathcal{B}'} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 5 \\ 0 & 0 & 3 \end{pmatrix}$$

As Proposition 4.6.1 shows it must be, this matrix is upper triangular.

REMARK 4.6.4. Combining Exercise 32 with Proposition 4.6.1 shows that a matrix $A \in \mathsf{Mat}(n;F)$ is nilpotent if and only if $\chi_A(x) = (-x)^n$.

DEFINITION 4.6.5. *An endomorphism $f : V \to V$ of an F-vector space V is* **diagonalisable** *if and only if there exists a basis of V consisting of eigenvectors of f. If V is finite dimensional then this is the same as saying that there exists an ordered basis $\mathcal{B} = \{\vec{v}_1, \ldots, \vec{v}_n\}$ such that corresponding matrix representing f is diagonal, that is ${}_{\mathcal{B}}[f]_{\mathcal{B}} = \mathsf{diag}(\lambda_1, \ldots, \lambda_n)$. In this case, of course, $f(\vec{v}_i) = \lambda_i \vec{v}_i$.*

A square matrix $A \in \mathsf{Mat}(n;F)$ is **diagonalisable** *if and only if the corresponding linear mapping $F^n \to F^n$ given by left multiplication by A is diagonalisable. Thanks to Corollary 2.4.4 this just means that A is conjugate to a diagonal matrix, there exists an invertible matrix $P \in \mathsf{GL}(n;F)$ such that $P^{-1}AP = \mathsf{diag}(\lambda_1, \ldots, \lambda_n)$. In this case the columns of P are the vectors of a basis of F^n consisting of eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_n$.*

EXAMPLE 4.6.6. A nilpotent matrix is diagonalisable if and only if it is the zero matrix. (Think about it!)

EXAMPLE 4.6.7. Let A be the real matrix

$$A = \begin{pmatrix} 7 & 2 \\ -18 & -6 \end{pmatrix}$$

I calculate that $\chi_A(x) = (7-x)(-6-x) + 36 = x^2 - x - 6 = (x-3)(x+2)$ so that the eigenvalues of A are 3 and -2. To calculate eigenvectors with eigenvalue 3 I calculate

$$A - 3I_n = \begin{pmatrix} 4 & 2 \\ -18 & -9 \end{pmatrix}$$

and observe then that $(A - 3I_n)\vec{v} = \vec{0}$ if and only if $\vec{v} = \alpha(1,-2)^\mathsf{T}$ for some $\alpha \in \mathbb{R}$, so that $E(3,A) = \{\alpha(1,-2)^\mathsf{T} : \alpha \in \mathbb{R}\}$. Similarly, I calculate that $E(-2,A) = \{\alpha(2,-9)^\mathsf{T} : \alpha \in \mathbb{R}\}$. It follows that if I take $P = \begin{pmatrix} 1 & 2 \\ -2 & -9 \end{pmatrix}$ then $P^{-1}AP = \operatorname{diag}(3,-2)$, which can be easily checked.

LEMMA 4.6.8 (Linear independence of Eigenvectors). *Let $f : V \to V$ be an endomorphism of a vector space V and let $\vec{v}_1, \ldots, \vec{v}_n$ be eigenvectors of f with pairwise different eigenvalues $\lambda_1, \ldots, \lambda_n$. Then the vectors $\vec{v}_1, \ldots, \vec{v}_n$ are linearly independent.*

PROOF. Suppose that $\alpha_1\vec{v}_1 + \cdots + \alpha_n\vec{v}_n = \vec{0}$. Let's see what happens when I apply the endomorphism $(f - \lambda_2 \operatorname{id}_V) \circ \cdots \circ (f - \lambda_n \operatorname{id}_V)$ of V to $\vec{v}_i$:

$$(f - \lambda_2 \operatorname{id}_V) \circ \cdots \circ (f - \lambda_n \operatorname{id}_V)(\vec{v}_i) = \prod_{j=2}^{n}(\lambda_i - \lambda_j)\vec{v}_i = \begin{cases} \prod_{j=2}^{n}(\lambda_1 - \lambda_j)\vec{v}_1 & i = 1 \\ \vec{0} & i \neq 1 \end{cases}.$$

From this observation and the equation $\alpha_1\vec{v}_1 + \cdots + \alpha_n\vec{v}_n = \vec{0}$, I deduce that $\alpha_1 \prod_{j=2}^{n}(\lambda_1 - \lambda_j)\vec{v}_1 = \vec{0}$. Since $\lambda_1 \neq \lambda_j$ for all $j > 1$, it follows that $\alpha_1 = 0$. A similar argument shows also that $\alpha_2 = \cdots = \alpha_n = 0$. In other words, the vectors are linearly independent. □

This means that if $f : V \to V$ is an endomorphism of a finite dimensional vector space V whose characteristic polynomial decomposes into linear factors $\chi_f(x) = \prod_{j=1}^{n}(\lambda_j - x)$ with pairwise different roots, then f is a diagonalisable.

THEOREM 4.6.9 (The Cayley-Hamilton Theorem). *Let $A \in \mathsf{Mat}(n;R)$ be a square matrix with entries in a commutative ring R. Then evaluating its characteristic polynomial $\chi_A(x) \in R[x]$ at the matrix A gives zero.*

EXAMPLE 4.6.10. Let $A = \begin{pmatrix} 14 & 8 & 3 \\ -17 & -9 & -3 \\ 1 & 0 & 0 \end{pmatrix}$, the matrix appearing in Example 4.6.3. Its characteristic polynomial is $\chi_A(x) = -x^3 + 5x^2 - 7x + 3$. Now I calculate

$$\begin{aligned} -A^3 + 5A^2 - 7A + 3I &= -\begin{pmatrix} 220 & 144 & 69 \\ -321 & -209 & -99 \\ 63 & 40 & 18 \end{pmatrix} + 5\begin{pmatrix} 63 & 40 & 18 \\ -88 & -55 & -24 \\ 14 & 8 & 3 \end{pmatrix} \\ &\quad -7\begin{pmatrix} 14 & 8 & 3 \\ -17 & -9 & -3 \\ 1 & 0 & 0 \end{pmatrix} + 3\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Just as the Cayley-Hamilton Theorem predicts.

EXAMPLE 4.6.11. The polynomial extension ring $F[x]$ of a field F is an (infinite-dimensional) F-vector space. For a degree n polynomial

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x] \ (a_n \neq 0 \in F)$$

the principal ideal generated by $P(x)$ is a subspace

$$(P(x)) = \{P(x)Q(x) \,|\, Q(x) \in F[x]\} \subset F[x]$$

(which is also infinite-dimensional). The quotient space $V = F[x]/(P(x))$ is an n-dimensional F-vector space with basis

$$\mathcal{B} = (\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{n-1}) = (1, x, x^2, \ldots, x^{n-1}) .$$

The endomorphism

$$f = \text{multiplication by } x : V \to V ; x^i \mapsto x^{i+1}$$

is such that

$$f(\vec{v}_i) = x^{i+1} = \vec{v}_{i+1} \, (0 \leqslant i \leqslant n-2) ,$$

$$f(\vec{v}_{n-1}) = x^n = -(a_n)^{-1}(\sum_{i=0}^{n-1} a_i x^i) = -(a_n)^{-1}(\sum_{i=0}^{n-1} a_i \vec{v}_i) \in V ,$$

so it has $n \times n$ matrix

$$A = {}_{\mathcal{B}}[f]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & 0 & \ldots & -c_0 \\ 1 & 0 & 0 & \ldots & -c_1 \\ 0 & 1 & 0 & \ldots & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -c_{n-1} \end{pmatrix} \text{ with } c_i = (a_n)^{-1} a_i \in F \, (0 \leqslant i \leqslant n-1) .$$

Exercise 6 in Homework 8 is to calculate the characteristic polynomial $\chi_f(x) = \chi_A(x) \in F[x]$. After you have done this verify the Cayley-Hamilton Theorem for f !

INTUITIVE PROOF. The first thing to observe is that if A is a diagonal matrix then it is straightforward to check that the theorem holds. For suppose that $A = \mathsf{diag}(\lambda_1, \ldots, \lambda_n)$. Then $\chi_A(x) = \prod_{j=1}^n (\lambda_j - x)$. I must show then that $\prod_{j=1}^n (\lambda_j I_n - A) = 0$. But the matrix $\lambda_j I_n - A$ is a diagonal matrix whose j-th entry is zero. Therefore multiplying all n of these diagonal matrices together produces

$$\begin{pmatrix} 0 & & & \\ & \lambda_2 - \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_n - \lambda_1 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 - \lambda_2 & & & \\ & 0 & & \\ & & \ddots & \\ & & & \lambda_n - \lambda_2 \end{pmatrix} \cdots = \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$$

So in this diagonal case the theorem holds.

Now suppose that $A \in \mathsf{Mat}(n; F)$ where F is an algebraically closed field. Then $P := \chi_A(x) \in F[x]$ decomposes into linear factors $P = \prod_{j=1}^n (\lambda_j - x)$ and so has n roots. It is more likely than not that the roots $\{\lambda_j\}_{1 \leqslant j \leqslant n}$ are pairwise different, and in that case it follows from Lemma 4.6.8 that the matrix A is a diagonalisable. Hence I can find $S \in \mathsf{GL}(n; F)$ such that $S^{-1}AS = \mathsf{diag}(\lambda_1, \ldots, \lambda_n)$. Observing that

$$(S^{-1}AS)^n = \underbrace{(S^{-1}AS)(S^{-1}AS)\cdots(S^{-1}AS)}_{n \text{ times}} = S^{-1}A^nS$$

because all the SS^{-1} products cancel, I see that $P(S^{-1}AS) = S^{-1}P(A)S$. Therefore $P(A) = 0$ if and only if $P(S^{-1}AS) = 0$, so that I need only check that $P(\mathsf{diag}(\lambda_1, \ldots, \lambda_n)) = 0$. But that's what I did in the first paragraph. □

REMARK 4.6.12. This proof won't cut the mustard in general for a couple of reasons. First I have written "more likely than not" and that is not a mathematical statement: one can make this precise using Algebraic Geometry, but that's for your future. Second, in order to decompose the characteristic polynomial, this proof required me to use an algebraically closed field F rather than a commutative ring. So even if I had just wanted to consider matrices over fields I would have struggled! I could certainly have considered an $(n \times n)$-real matrix as a complex matrix and

deduced the result for real matrices from the result for complex matrices, but what if the field had been a finite field $\mathbb{F}_p$? This argument would only have worked if I knew that $\mathbb{F}_p$ could sit inside an algebraically closed, just as $\mathbb{R}$ sits inside $\mathbb{C}$. This is true, but it is proved in Jewels of Algebra, so again that's in your future.

FORMALLY COMPLETE, UNINTUITIVE PROOF. Let $S = R[x]$, the ring of polynomials with coefficients in R. Given $A \in \mathsf{Mat}(n;R)$ let $B = A - xI_n \in \mathsf{Mat}(n;S)$. Let $\mathsf{adj}(B)$ be the adjugate of B, as defined in Definition 4.4.8. By Cramer's Rule

$$B \cdot \mathsf{adj}(B) = (\det(A - xI_n))I_n = \chi_A(x)I_n \tag{11}$$

The adjugate $\mathsf{adj}(B) \in \mathsf{Mat}(n;S)$ and so it is an $(n \times n)$-matrix with entries in $S = R[x]$. I can consider such a matrix equally well as an element of the ring $\mathsf{Mat}(n;R)[x]$ of polynomials with coefficients with entries in $\mathsf{Mat}(n;R)$. For instance

$$\begin{pmatrix} 1+x+3x^2 & -x \\ x^{10} & 2+x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + x\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} + x^2\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} + x^{10}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

In this way $\mathsf{adj}(B) = \sum_{i\geqslant 0} x^i C_i$ where each $C_i \in \mathsf{Mat}(n;R)$. Equation (11) then gives an equality of polynomials with coefficients in $\mathsf{Mat}(n;R)$

$$\begin{aligned} \chi_A(x)I_n &= (A - xI_n)\cdot \mathsf{adj}(B) \\ &= (A - xI_n)\cdot\left(\sum_{i\geqslant 0} x^i C_i\right) \\ &= \sum_{i\geqslant 0} x^i AC_i - \sum_{i\geqslant 0} x^{i+1}C_i \\ &= AC_0 + \sum_{i\geqslant 1} x^i(AC_i - C_{i-1}) \end{aligned}$$

If I write $\chi_A(x) = x^n + x^{n-1}c_{n-1} + \cdots + xc_1 + c_0$ with each $c_i \in R$, then I get a sequence of $n+1$ equalities by comparing coefficients of the various powers of x:

$$AC_0 = c_0 I_n; \quad AC_1 - C_0 = c_1 I_n; \quad \ldots \quad ; \quad AC_{n-1} - C_{n-2} = c_{n-1}I_n; \quad AC_n - C_{n-1} = I_n$$

Multiplying the i-th one of these equalities by A^i produces $A^i(AC_i - C_{i-1}) = A^i c_i$ which is the i-th term in the evaluation of $\chi_A(x)$ at the matrix A. I deduce that

$$\begin{aligned} A^n + A^{n-1}c_{n-1} + \cdots Ac_1 + c_0 &= A^n(AC_n - C_{n+1}) + A^{n-1}(AC_{n-1} - C_{n-2}) \\ &\quad + A^{n-2}(AC_{n-2} - C_{n-3}) + \cdots + A(AC_1 - C_0) + AC_0 \\ &= A^{n+1}C_n \end{aligned}$$

So the theorem will be complete if I can show that $A^{n+1}C_n = 0$. In fact $C_n = 0$ for the following reason. Recall that C_n is the coefficient of x^n in $\mathsf{adj}(A - xI_n)$. But the entries of $\mathsf{adj}(A - xI_n)$ are by definition the different cofactors of the matrix $A - xI_n$. These cofactors are obtained as the determinant of $(A - xI_n)\langle i,j\rangle$, the matrices gotten from $A - xI_n$ by deleting the i-th row and j-th column. But $(A - xI_n)\langle i,j\rangle$ is an $((n-1)\times(n-1))$-matrix, so its determinant is a sum of products of $n-1$ entries of $(A - xI_n)\langle i,j\rangle$. Each of these entries has degree at most 1 as a polynomial in x, and so each of the products in the determinant has degree at most $n-1$, from which I deduce that the degree of each cofactor is at most $n-1$, and hence $C_n = 0$. □

Well, I did warn you. In any case you now see that Cayley-Hamilton is true and that this proof, even if you were only considering a matrix with entries in a field $R = F$, required considering matrices and determinants of matrices with entries in the ring $R[t]$ which is not a field. So, at last,

rings have become useful! In fact, an intuitive and formally correct proof for this theorem exists, but really requires the development of some serious commutative ring theory, currently beyond the scope of the undergraduate syllabus in Edinburgh.

4.7. Google's PageRank Algorithm

What is the internet? *It is a library like no other*: it is big, with, I've heard, over 25 billion documents. Contrast this with Edinburgh University Library which, I've heard, has around 200,000 books in its Special Collection. *It is a library like no other*: anyone can add a document at any time, telling nobody. Contrast this with Edinburgh University Library. *It is a library like no other*: the documents change frequently, with, I've heard, 40% of webpages changing their data each week. Contrast this with Edinburgh University Library.

What about the data? Search engines typically have an army of spiders deployed all over the web, retrieving pages, indexing the words in each document, and then scuttling back to a depot somewhere to store the information. Whenever you input into a search engine a phrase such as "honours algebra", the engine uses this information to determine all the documents on the web containing the words "honours" and the word "algebra" (on Google 368,000 hits for "honours algebra" without inverted commas; 3,980 for " "honours algebra" "). Add to this that 95% of the text in webpages is composed from 10,000 words and you see the problem: how can a ranking of the importance of the pages that fit the search criteria be made, placing the most important pages first?

How does this happen? Google's PageRank algorithm assesses the importance of webpage in a purely automated fashion, without human interference. One incredibly useful difference between a traditional library and the internet, or at the very least a resource that is not used by librarians, is all the cross-referencing that goes on between different webpages via hyperlinks. It is this information that Google uses to rank its pages, not the content of the pages themselves.

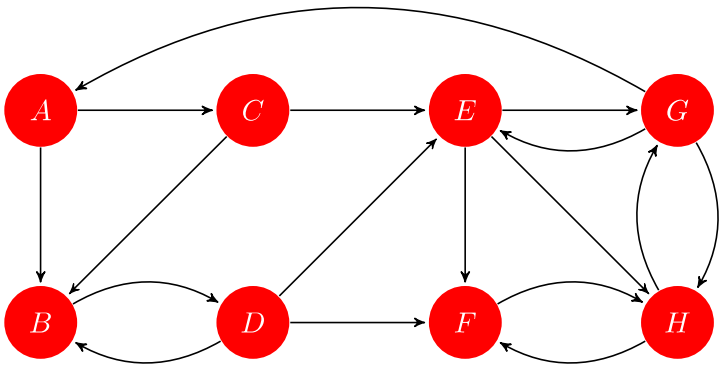
Graphs and Matrices If I focus on hyperlinks as connections between webpages then I should think of the web as a graph, in the sense of discrete mathematics. So each document on the web is a vertex of the graph and there is an arrow from the vertex i to vertex j if there is a hyperlink on page i going to page j. So this a graph with perhaps 25 billion nodes!

Any graph can be encoded in a square matrix L with real entries:

$$\ell_{ij} = \begin{cases} 1 & \text{if page } j \text{ has a link to page } i \\ 0 & \text{if not.} \end{cases}$$

For the web, $L \in \mathsf{Mat}(n; \mathbb{R})$ where n is approximately a 25×10^9.

EXAMPLE 4.7.1. Here is a smaller example:



The associated matrix L is

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

REMARK 4.7.2. Note that most entries are 0. In fact, I've heard, an average webpage links to 10 other webpages, so an average column of the 25 billion by 25 billion matrix representing the web will have only 10 non-zero entries.

What's this to do with importance? Well I think of any link pointing to page i as a recommendation for it, and so the total number of recommendations that page i gets is its row sum $\ell_{i1} + \cdots + \ell_{in}$. This is a first approximation to a measure of the importance of page i:

$$v_i = \ell_{i1} + \cdots + \ell_{in}$$

There is a concise mathematical way to write this

$$\vec{v} = L\vec{u}$$

where $\vec{u} \in \mathbb{R}^n$ is the vector each of whose components is 1. In the example above there would be a ranking of importance: (B = E = F = H > G > A = C = D) with values $(3; 2; 1)$.

EXERCISE 69. The information of a directed graph Γ as above can be recorded by a matrix: $\Gamma \mapsto L(\Gamma)$. Here $L(\Gamma) \in \mathsf{Mat}(n, \mathbb{R})$ where n is the number of vertices of Γ where $L(\Gamma)_{ij}$ is the number of edges from vertex j to vertex i. Show that: the (i, j) entry of $L(\Gamma)^k$ is the number of distinct paths of length k going from vertex j to vertex i in the graph Γ.

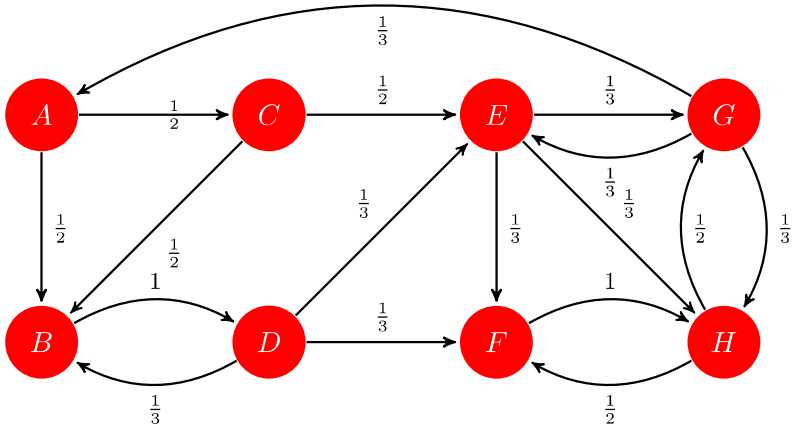
"I don't want to belong to any club that will accept me as a member" It's obvious that the above measure of importance is not very sophisticated. Suppose you are looking for a restaurant to go to: Person A gives 25 recommendations; Person B gives only 2. Which recommendations do you value more? Presumably, all other things being equal, one of the 2 selected by Person B.

To implement this into mathematics I should therefore not attach a value 1 to each link from page j to page i, but rather the number $1/t_j$ where $t_j = \sum_{k=1}^{n} \ell_{kj}$ is the total number of links from page j. This produces a new matrix $M \in \mathsf{Mat}(n; \mathbb{R})$ where

$$m_{ij} = \begin{cases} 1/t_j & \text{if page } j \text{ has a link to page } i \\ 0 & \text{if not.} \end{cases}$$

EXAMPLE 4.7.3. Example continued I continue with the example above, but now I indicate on each edge the value I give to that edge, as determined by the number of outgoing links from its

starting vertex.

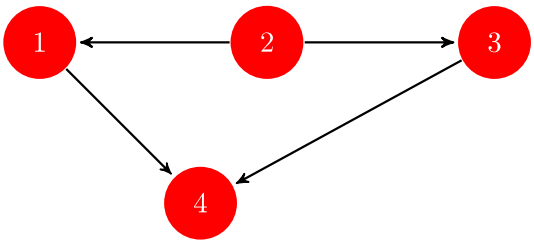


So now the matrix M for this example is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1/3 & 0 \\ 1/2 & 0 & 1/2 & 1/3 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 1/3 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 1/3 & 0 \end{pmatrix}$$

There is a problem with this definition to "weight" the edges of the graph: what if a page has no outgoing links at all? This is common enough – think for instance of PDFs online – and such a page is called a **dangling node**. I'll get round this by pretending then that such a page is linked to every node and then calculate the matrix M as suggested.

EXAMPLE 4.7.4. In this example vertex 4 is a dangling node:



The new matrix M associated to this would be

$$\begin{pmatrix} 0 & 1/2 & 0 & 1/4 \\ 0 & 0 & 0 & 1/4 \\ 0 & 1/2 & 0 & 1/4 \\ 1 & 0 & 1 & 1/4 \end{pmatrix}$$

So importance is now measured by

$$v_i = \frac{\ell_{i1}}{t_1} + \cdots + \frac{\ell_{in}}{t_n}$$

Written in concise mathematical form this states

$$\vec{v} = M\vec{u}$$

where $\vec{u}$ is still the vector of ones. Now in Example 4.7.1 the ranking is more refined than before, becoming: (H $>$ B $>$ E = F $>$ D $>$ G $>$ C$>$ A) with values $(5/3; 4/3; 7/6; 1; 5/6; 1/2; 1/3)$.

"Oh, you're a member. I didn't know. Well, maybe I'll join" When I discussed Person A and Person B giving restaurant recommendations, I wrote "all other things being equal". Well, of course they're not. What if Person A was a food critic, and like me Person B grew up on a strict Scottish diet of potatoes? Wouldn't you want to take Person A's recommendation a little more seriously than before? In other words, what should happen is that each recommendation made should reflect the importance of the recommender. But since v_j is supposed to be the importance of page j, this would mean that I should multiply the previous value ℓ_{ij}/t_j of a recommendation from page j to page i by v_j. This sounds circular to me, at least until I write out its mathematical formulation:

$$v_i = \frac{\ell_{i1}}{t_1}v_1 + \cdots + \frac{\ell_{in}}{t_n}v_n$$

Written in concise mathematical form this states

$$\vec{v} = M\vec{v}$$

In other words, the vector that measures importance should be an eigenvector of M with eigenvalue 1.

It's just like I always said: mathematics rules the world! Well actually, Google rules the world *and* mathematics rules Google; but sadly "rules the world" is not a transitive relation.

In the two running examples, there are unique (up to scalar) eigenvectors with eigenvalue 1:

$$\frac{1}{400}(24, 27, 12, 27, 39, 81, 72, 118)^{\mathsf{T}} \text{ and } \frac{1}{16}(3, 2, 3, 8)^{\mathsf{T}}$$

So in Example 4.7.1 the order of importance is (H>F>G> E> B = D >A > C).

As prospective mathematicians you will automatically ask yourself the following questions:

- Does M always have an eigenvalue 1?
- How many eigenvectors of M with eigenvalue 1 are there? In other words, what is $\dim\{\vec{v} : M\vec{v} = \vec{v}\}$?
- Is it true that there is always an eigenvector of M whose entries are non-negative; even positive?
- How can I calculate such an eigenvector given that I may want to work with square matrices of size 25×10^9?

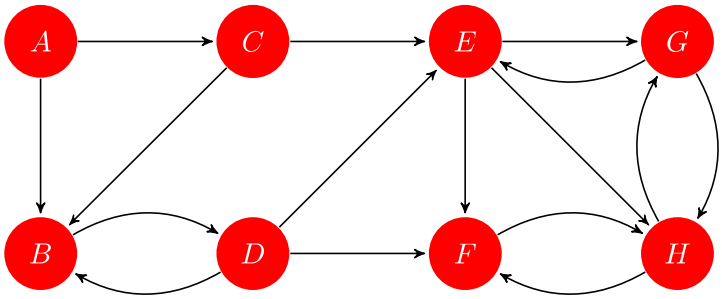
Now, I need to do mathematics. This is because most of the answers to the above questions are not the answers I'd want them to be. But at least the first question has a positive answer, provided you notice something staring you in the face.

DEFINITION 4.7.5. *A matrix M whose entries are non-negative and such that the sum of the entries of each column equals 1 is a* **Markov matrix** *or a* **stochastic matrix**.

LEMMA 4.7.6. *Suppose that $M \in \mathsf{Mat}(n; \mathbb{R})$ is a Markov matrix. Then $\lambda = 1$ is an eigenvalue of M.*

PROOF. The sum of the entries of each column of $M - I_n$ is 0. Therefore if I add all the row vectors of the matrix together I must get the zero vector. This means that there is a linear dependence amongst the rows, which in turn means that $\det(M - I_n) = 0$ so that $\chi_M(1) = 0$, as required. □

EXAMPLE 4.7.7. I take the following variation on Example 4.7.1, the only difference being that I remove the arrow from G to A:



Its associated Markov matrix is:

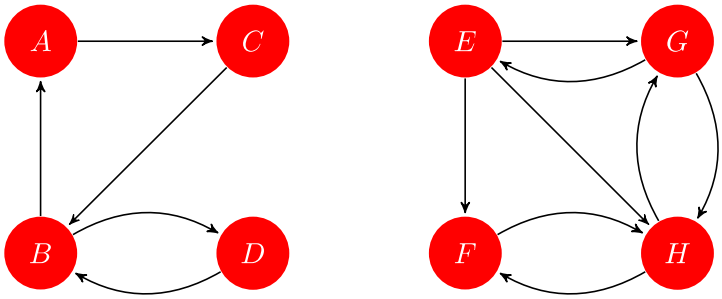
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 1/3 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 1/3 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 1/2 & 0 \end{pmatrix}$$

It still has a unique (up to scalar) eigenvector with eigenvalue 1, which is $\frac{1}{25}(0, 0, 0, 0, 3, 6, 6, 10)^{\mathsf{T}}$. This is, of course, not what I want because it says that A, B, C and D have no importance whatsoever.

To understand what has happened in the above example, think of the Markov matrix M as describing a random walk over the web in which I move from page to page as follows. On a given page, I choose at random one of the links from that page and then follow that link. For example, if there are six links, I roll a die to choose which link to follow. If I reach a dead end, meaning there are no links out, I choose a page at random from the entire web and move to it. Now imagine lots and lots of web surfers moving around the web in this way: m_{ij} gives the expected fraction of those surfers on page j who will then move to page i. A solution $\vec{v}$ to the equation $\vec{v} = M\vec{v}$ can be then regarded as describing an equilibrium or steady state distribution of surfers on the various pages.

Now what would you expect a steady state of surfers to look like in the above example? Note there are no dangling nodes, so there's no trouble with ending up on a page with no links out. Surf randomly, for some time! You expect you'll get to one of E, F, G or H at some point. But once you're on one of those pages you'll never get back to A, B, C or D. So the steady state has to expect that all surfers are on pages E, F, G or H and nowhere else. That's what the eigenvector demonstrates! The four zeros at the start appear because once I reach E, F, G or H I can never get back to A, B, C or D; and I have to reach E, F, G or H sometime if I'm moving around randomly.

EXAMPLE 4.7.8. I now take the following more brutal variation on Example 4.7.1, splitting the graph into two separate pieces, but reversing the arrow between A and B:



Its associated Markov matrix is:

$$\begin{pmatrix} 0 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 1/2 & 0 \end{pmatrix}$$

This now has a two-dimensional eigenspace $\{\vec{v} : M\vec{v} = \vec{v}\}$ for eigenvalue 1 with basis

$$\frac{1}{25}(0,0,0,0,3,6,6,10)^{\mathsf{T}} \text{ and } \frac{1}{5}(1,2,1,1,0,0,0,0)^{\mathsf{T}}$$

Obviously, a similar but different problem has arisen: this time there are parts of the web that are just not talking to each other and so I can't make a comparison between A, B, C, D and E, F, G, H.

Very smart idea Going back to thinking of M as a random walk over the web, one way to solve the problem that some parts of the web might get forgotten completely, as in Example 4.7.7, or that some parts do not communicate with each other at all, as in Example 4.7.8, Sergey Brin and Larry Page – the founders of Google – introduced the key idea of teleportation. To understand it,

imagine that you have a biased coin so that the probability of heads is α with $0 \leqslant \alpha \leqslant 1$. Typically α is $1/2$, but that's not what I want here. If I'm on page j I toss the coin. If page j is a dangling node or if the coin comes up tails, then I pick a page at random from the whole web and teleport to it; otherwise I do what I always did, follow a link at random. In mathematics, I replace the Markov matrix M with the new matrix

$$\mathsf{Google}(\alpha) = \alpha M + (1-\alpha)T$$

where T is the teleportation matrix each of whose entries is $\frac{1}{n}$. Notice that whatever I choose for α, $\mathsf{Google}(\alpha)$ is still a Markov matrix, so it will still have 1 as an eigenvalue. If I chose $\alpha = 1$ then $\mathsf{Google}(\alpha) = M$, so nothing new. If I chose $\alpha = 0$ then $\mathsf{Google}(\alpha) = T$ and so I'd forget all about the hyperlink structure and be moving around the web at random. The obviously good thing about choosing $\alpha < 1$ is that the matrix $\mathsf{Google}(\alpha)$ has all entries positive.

EXAMPLE 4.7.9. In Example 4.7.7 an example of the new Markov matrix with $\alpha = 17/20$ is:

$$\begin{pmatrix}
3/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 \\
71/160 & 3/160 & 71/160 & 29/96 & 3/160 & 3/160 & 3/160 & 3/160 \\
71/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 \\
3/160 & 139/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 & 3/160 \\
3/160 & 3/160 & 71/160 & 29/96 & 3/160 & 3/160 & 71/160 & 3/160 \\
3/160 & 3/160 & 3/160 & 29/96 & 29/96 & 3/160 & 3/160 & 71/160 \\
3/160 & 3/160 & 3/160 & 3/160 & 29/96 & 3/160 & 3/160 & 71/160 \\
3/160 & 3/160 & 3/160 & 3/160 & 29/96 & 139/160 & 71/160 & 3/160
\end{pmatrix}$$

It looks quite complicated, but it has a unique (up to scaling) eigenvector with eigenvalue 1 which is approximately:

$$(0.019, 0.057, 0.027, 0.067, 0.128, 0.206, 0.187, 0.309)^{\mathsf{T}}$$

This orders the vertices H > F > G > E > D > B > C > A.

THEOREM 4.7.10 (Perron, 1907). *If $M \in \mathsf{Mat}(n;\mathbb{R})$ is a Markov matrix all of whose entries are positive, then the eigenspace $E(1,M)$ is one dimensional. There exists a unique basis vector $\vec{v} \in E(1,M)$ all of whose entries are positive real numbers, $v_i > 0$ for all i, and such that the sum of its entries is 1, $\sum_{i=1}^{n} v_i = 1$.*

I've presented here a cannibalisation of the **Perron-Frobenius Theorem** which has a weaker hypothesis on the initial matrix N and which deduces more consequences than those I present here. [If you look closely at the proof, you'll see that I already prove a little bit more than the statement of the Theorem: what extra do I do?] The proof of the full Perron-Frobenius theorem is not really harder than what follows, but it does involve more definitions. The Theorem is important in all sorts of places: graph theory, statistical mechanics, commodity pricing, power control in wireless networks, population growth (think haggii). Really anywhere that iterative processes involving positive matrices appear.

PROOF. I will split the proof into several steps. But before doing so I need to introduce notation for $\vec{v}, \vec{w} \in \mathbb{R}^n$:

$$\begin{aligned}
\vec{v} > \vec{w} &\quad\Leftrightarrow\quad v_i > w_i \text{ for all } 1 \leqslant i \leqslant n \\
\vec{v} \geqslant \vec{w} &\quad\Leftrightarrow\quad v_i \geqslant w_i \text{ for all } 1 \leqslant i \leqslant n
\end{aligned}$$

Given $\vec{v} \in \mathbb{R}^n$, I will write $|\vec{v}|$ for $\sum_{i=1}^{n} v_i$.

STEP 1. *I claim that if $\vec{v} \geqslant \vec{w}$ and $\vec{v} \neq \vec{w}$ then $M\vec{v} > M\vec{w}$.* By definition of matrix multiplication, the i-th entry of $M\vec{v} - M\vec{w}$ is $\sum_{j=1}^{n} M_{ij}(v_j - w_j)$. Each term in the sum is a product of $M_{ij} > 0$

and $v_j - w_j \geqslant 0$ and so non-negative. At least one of the terms is positive since by hypothesis there is some j such that $v_j - w_j > 0$. It follows that $\sum_{j=1}^n M_{ij}(v_j - w_j) > 0$ for each i. Therefore $M\vec{v} > M\vec{w}$. □

STEP 2. *There exists an eigenvector $\vec{v} \geqslant 0$ for M.* For $\vec{x} \geqslant 0$ and $\vec{x} \neq 0$ let

$$R(\vec{x}) = \max\{c \in \mathbb{R} : M\vec{x} \geqslant c\vec{x}\} = \min_{1 \leqslant i \leqslant n, x_i \neq 0} \frac{(M\vec{x})_i}{x_i}$$

If $M\vec{x} \geqslant c\vec{x}$ then by Step 1 $M(M\vec{x}) \geqslant cM\vec{x}$ with equality if and only if $M\vec{x} = c\vec{x}$. This means that

$$R(M\vec{x}) \geqslant R(\vec{x}) \tag{12}$$

and that the inequality is strict unless $M\vec{x} = c\vec{x}$.

Let

$$C = \{\vec{x} : \vec{x} \geqslant 0 \text{ and } |\vec{x}| = 1\}$$

This is a **compact set** as you will see using the Heine–Borel Theorem from Honours Analysis. You will also see in Honours Analysis that a continuous real-valued function on a compact set always achieves a maximum, a higher dimensional version of the Extreme Value Theorem from Fundamentals of Pure Mathematics. Thus, since R is a continuous function on C, it achieves a maximum on C. This means there exists $\vec{v} \in C$ such that

$$R(\vec{v}) \geqslant R(\vec{x}) \text{ for all } \vec{x} \in C$$

By definition $R(\alpha\vec{x}) = R(\vec{x})$ for any $\alpha > 0$ and any non-zero $\vec{x} \geqslant \vec{0}$. Then, as $|M\vec{x}| > 0$ by Step 1, I see $\frac{M\vec{x}}{|M\vec{x}|} \in C$. So in particular I deduce

$$R(M\vec{v}) = R\left(\frac{M\vec{v}}{|M\vec{v}|}\right) \leqslant R(\vec{v}).$$

Combining this with equation (12) shows that $M\vec{v} = c\vec{v}$ for some $c \in \mathbb{R}$, as required. □

STEP 3. *I claim that if $\vec{v} \geqslant \vec{0}$ is an eigenvector of M then its eigenvalue must be 1.* Let $\vec{u}^{\mathsf{T}} = (1, 1, \ldots, 1)$ be the row vector of length n all of whose entries are 1. Since M is a Markov matrix the sum of the entries of each column is 1, and so $\vec{u}^{\mathsf{T}}M = \vec{u}^{\mathsf{T}}$. By assumption $M\vec{v} = \lambda\vec{v}$ for some λ and so

$$\lambda\vec{u}^{\mathsf{T}}\vec{v} = \vec{u}^{\mathsf{T}}(M\vec{v}) = (\vec{u}^{\mathsf{T}}M)\vec{v} = \vec{u}^{\mathsf{T}}\vec{v}$$

Since $\vec{u}^{\mathsf{T}}\vec{v} = \sum_{i=1}^n u_i v_i = \sum_{i=1}^n v_i > 0$ it follows that $\lambda = 1$. □

STEP 4. *If $\vec{v} \geqslant \vec{0}$ is an eigenvalue of M, then $\vec{v} > \vec{0}$.* This is a consequence of Steps 1 and 3 because $\vec{v} = M\vec{v} > M\vec{0} = \vec{0}$. □

STEP 5. *If $\vec{v} \geqslant \vec{0}$ is an eigenvector of M, then $E(1, M) = \langle\vec{v}\rangle$. In other words the eigenspace of eigenvalue 1 is one dimensional.* By Step 3 $\vec{v} \in E(1, M)$. Suppose that $\vec{x} \in E(1, M)$ is non-zero. By multiplying by -1 if necessary, I can assume that there exists at least one positive entry x_j in $\vec{x}$. Obviously $\vec{v} + \alpha\vec{x} \in E(1, M)$ for all $\alpha \in \mathbb{R}$. If I set $\alpha = \min\{-v_i/x_i : x_i > 0\}$ then $\vec{v} + \alpha\vec{x} \geqslant 0$. But then at least one entry of $\vec{v} + \alpha\vec{x}$ is zero: this contradicts Step 4 unless $\vec{v} + \alpha\vec{x} = \vec{0}$. Hence $\vec{x}$ is a scalar multiple of $\vec{v}$, as required. □

This completes the proof of the theorem. Steps 2 and 4 shows the existence of the positive eigenvalue, and Step 5 shows that it is a basis for $E(1, M)$. □

This now answers the first three questions you asked as prospective mathematicians, at least for the matrix Google(α) with $0 \leqslant \alpha < 1$.

The last question is a little more practical in nature and the sort of question that is important in Numerical Linear Algebra and Applications. The basic point is that if $\vec{w} \geqslant \vec{0}$ with $|\vec{w}| = 1$ then

$$\lim_{k\to\infty} M^k \vec{w} = \vec{v}$$

So calculating powers of the Markov matrix Google(α) cleverly – remembering it's origin in the sparse matrix M that represented hyperlinks between webpages – allows one to approximate the eigenvector $\vec{v}$ that is required for PageRank. The smaller the number α, the faster the convergence of the above limit and so the fewer multiplications that have to be made to find a good approximation of $\vec{v}$. But remember, choosing α closer to 1 gives a better page ranking. Google, I've read, uses $\alpha = 17/20$.

CHAPTER 5

Inner Product Spaces

Inner product spaces are a halfway-house between the Euclidean geometry of $\mathbb{R}^2$ and $\mathbb{R}^3$ and the mathematics of Hilbert spaces, objects that are particularly important in analysis and in quantum mechanics. As you saw in the proof of the Perron Theorem special things happen in linear algebra when the general is replaced by the specific: there it was combining linear algebra and the ordering on real numbers, that is the notion of $x > y$. Inner product spaces are similar in that this is no longer the study of general vector spaces, but ones with just enough extra structure for the notion of angle to make sense: inner product spaces are a natural extension of Euclidean geometry. In fact, this fits very well with a huge theme of twentieth century mathematics in which usual spatial "geometry" is generalised: one approach comes from Klein's "Erlangen Program" which understands geometry through group theory; another is via Riemannian Geometry which is, for instance, what Einstein required for General Relativity. Inner product spaces are tied up with Erlangen program via the associated group of orthogonal symmetries. What is incredible however, at least to me, is that inner product spaces are useful far beyond this, especially when they are infinite dimensional. In that case, if they satisfy an additional hypothesis called completeness, they are Hilbert Spaces, an incredibly interesting topic that spans algebra, analysis and is half of the language of quantum theory (the other half being groups and their representations). You really do want to study it next year. But before you do, it helps to have gripped the finite dimensional case first. So that means you really do want absorb what is about to happen!

5.1. Inner Product Spaces: Definitions

DEFINITION 5.1.1. *Let V be a vector space over $\mathbb{R}$. An* **inner product** *on V is a mapping*

$$(-,-) : V \times V \to \mathbb{R}$$

that satisfies the following for all $\vec{x}, \vec{y}, \vec{z} \in V$ and $\lambda, \mu \in \mathbb{R}$:

(1) $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
(2) $(\vec{x}, \vec{y}) = (\vec{y}, \vec{x})$
(3) $(\vec{x}, \vec{x}) \geqslant 0$, *with equality if and only if* $\vec{x} = \vec{0}$

A **real inner product space** *is a real vector space endowed with an inner product.*

EXAMPLE 5.1.2. I can endow $V = \mathbb{R}^n$ with the **standard inner product**

$$(\vec{v}, \vec{w}) = v_1w_1 + v_2w_2 + \cdots + v_nw_n$$

You have already seen this, usually written as $\vec{v} \cdot \vec{w}$ and called the dot product. If I was so inclined, I could also write it as via matrix multiplication $(\vec{v}, \vec{w}) = \vec{v}^T \circ \vec{w}$, where I implicitly use the obvious identification $\mathsf{Mat}(1; \mathbb{R}) = \mathbb{R}$.

Recall that in Definition 4.3.1 I introduced the notion of a symmetric bilinear form. You will see that Conditions (1) and (2) on the inner product are precisely the same as asserting that $(-,-) : V \times V \to \mathbb{R}$ is a symmetric bilinear form. Linearity in the second entry of $(-,-)$ follows from linearity in the first entry by using the symmetry condition to swap "first" and "second". Condition (3) says that the symmetric bilinear form is **positive definite**.

EXERCISE 70. Confirm the following claims:

(1) On $\mathbb{R}^2$ define $(\vec{x}, \vec{y}) = x_1y_1 + 4x_2y_2$ where $\vec{x} = (x_1, x_2)^\mathsf{T}$ and $\vec{y} = (y_1, y_2)^\mathsf{T}$. This is an inner product.
(2) On $\mathbb{R}^2$ define $(\vec{x}, \vec{y}) = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$ where $\vec{x} = (x_1, x_2)^\mathsf{T}$ and $\vec{y} = (y_1, y_2)^\mathsf{T}$. This is an inner product.
(3) On $\mathbb{R}^2$ define $(\vec{x}, \vec{y}) = x_1y_1 + 2x_1y_2 + 2x_2y_1 + x_2y_2$ where $\vec{x} = (x_1, x_2)^\mathsf{T}$ and $\vec{y} = (y_1, y_2)^\mathsf{T}$. This is not an inner product.
(4) Fix real numbers $a < b$. For $P, Q \in \mathbb{R}[X]_{<n}$ define

$$(P, Q) = \int_a^b P(X)Q(X)dX$$

This is an inner product.

It is easy to extend the definition of an inner product space from real vector spaces to complex vector spaces. Unfortunately, I don't have a really convincing intuitive picture for it, unlike geometry for real spaces. The only justification I can give is a posteriori. It turns out that the combination of the algebraic closure of the complex numbers with the positivity of an inner product ends up proving powerful theorems, and theorems which even have consequences for real vector spaces.

DEFINITION 5.1.3. *Let V be a vector space over $\mathbb{C}$. An* **inner product** *on V is a mapping*

$$(-,-) : V \times V \to \mathbb{C}$$

that satisfies the following for all $\vec{x}, \vec{y}, \vec{z} \in V$ and $\lambda, \mu \in \mathbb{C}$:

(1) $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
(2) $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{x})}$
(3) $(\vec{x}, \vec{x}) \geqslant 0$, *with equality if and only if* $\vec{x} = \vec{0}$

Here $\overline{z}$ denotes the complex conjugate of z. A **complex inner product space** *is a complex vector space endowed with an inner product.*

EXAMPLE 5.1.4. I can endow $V = \mathbb{C}^n$ with the **standard inner product**

$$(\vec{v}, \vec{w}) = v_1\overline{w_1} + v_2\overline{w_2} + \cdots + v_n\overline{w_n}$$

If I was so inclined, I could also write it as via matrix multiplication $(\vec{v}, \vec{w}) = \vec{v}^T \circ \overline{\vec{w}}$, where $\overline{\vec{w}} = (\overline{w_1}, \ldots, \overline{w_n})^\mathsf{T}$ and where I implicitly use the obvious identification $\mathsf{Mat}(1; \mathbb{C}) = \mathbb{C}$.

The form $(-,-)$ in a real inner product space is necessarily a symmetric bilinear form. For a complex inner product space this is false:

$$(\vec{z}, \lambda\vec{x} + \mu\vec{y}) = \overline{(\lambda\vec{x} + \mu\vec{y}, \vec{z})} = \overline{\lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})} = \overline{\lambda}(\vec{z}, \vec{x}) + \overline{\mu}(\vec{z}, \vec{y})$$

In other words, it is not $\mathbb{C}$-linear in the second variable. I will call a mapping $f : V \to W$ between complex vector spaces **skew-linear** if $f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$ and $f(\lambda\vec{v}_1) = \overline{\lambda}f(\vec{v}_1)$ for all $\vec{v}_1, \vec{v}_2 \in V$ and all $\lambda \in \mathbb{C}$. So a complex inner product is skew-linear in its second variable. Such forms are called **sesquilinear** [1]. When a sesquilinear form satisfies (2) it is **hermitian**, named after the French mathematician Hermite. Condition (3) says that the symmetric bilinear form is **positive definite**.

EXERCISE 71. Confirm the following claims:

[1] Sesqui is Latin for "one-and-a-half": for instance this year is the sesquicentennial of the birth of the Canadian mathematician J.C.Fields, after whom the Fields Medal is named.

(1) On $\mathbb{C}^2$ define $(\vec{z},\vec{w}) = z_1\overline{w_1} + 4z_2\overline{w_2}$ where $\vec{z} = (z_1,z_2)^\mathsf{T}$ and $\vec{w} = (w_1,w_2)^\mathsf{T}$. This is an inner product.
(2) Let $V = C_{\mathbb{C}}[a,b]$ be the vector space of all continuous complex valued functions defined on $[a,b]$ where $a < b$ are real. (In case you don't know, continuity for complex valued functions is defined as the natural extension of the definition of the real valued functions, using the modulus in $\mathbb{C}$ to measure "nearness".) For $f,g \in V$ define

$$(f,g) = \int_a^b f(t)\overline{g(t)}dt$$

(For a complex valued function ϕ on an interval $[a,b]$, the integral $\int_a^b \phi(t)dt$ is defined to be $\int_a^b \Re e(\phi(t))dt + \sqrt{-1}\int_a^b \Im m(\phi(t))dt$.) This is an inner product.

For future orientation, I give you some of the names that are associated to what I have just defined. A finite dimensional real inner product space is a **Euclidean vector space** or, with belts-and-braces, a **real Euclidean vector space**. A complex inner product space is a **unitary space** or, because of its connection to Hilbert spaces, a **pre-Hilbert space**. A finite dimensional complex inner product space is a **finite dimensional Hilbert space**.

DEFINITION 5.1.5. *In a real or complex inner product space the* **length** *or* **inner product norm** *or* **norm** $\|\vec{v}\| \in \mathbb{R}$ *of a vector* $\vec{v}$ *is defined as the non-negative square root*

$$\|\vec{v}\| = \sqrt{(\vec{v},\vec{v})}$$

Vectors whose length is 1 *are called* **units**. *Two vectors* $\vec{v},\vec{w}$ *are* **orthogonal** *and I write*

$$\vec{v} \perp \vec{w}$$

if and only if $(\vec{v},\vec{w}) = 0$. *I'll also say that* $\vec{v}$ *and* $\vec{w}$ *are at right-angles to each other. Sometimes I will use the symbol* $\perp$ *for general subsets* S,T *of an inner product space and write* $S \perp T$ *as a shorthand for* $\vec{v} \perp \vec{w}$ *for all* $\vec{v} \in S$ *and* $\vec{w} \in T$.

EXERCISE 72. In an inner product space V show that: $\|\lambda\vec{v}\| = |\lambda|\|\vec{v}\|$ for all $\vec{v} \in V$ and all $\lambda \in \mathbb{R}$ or $\mathbb{C}$, as relevant depending on whether it is a real or complex inner product space.

EXAMPLE 5.1.6. If two vectors $\vec{v}$ and $\vec{w}$ in an inner product space are at right-angles then Pythagoras' Theorem holds

$$\|\vec{v}+\vec{w}\|^2 = \|\vec{v}\|^2 + \|\vec{w}\|^2$$

To see this, follow your linear nose:

$$(\vec{v}+\vec{w},\vec{v}+\vec{w}) = (\vec{v},\vec{v}) + (\vec{v},\vec{w}) + (\vec{w},\vec{v}) + (\vec{w},\vec{w}) = (\vec{v},\vec{v}) + (\vec{w},\vec{w})$$

See! Just like ordinary Euclidean geometry.

DEFINITION 5.1.7. *A family* $(\vec{v}_i)_{i\in I}$ *for vectors from an inner product space is an* **orthonormal family** *if all the vectors* $\vec{v}_i$ *have length* 1 *and if they are pairwise orthogonal to each other, which, using the Kronecker delta symbol defined in Example 2.1.2, means*

$$(\vec{v}_i,\vec{v}_j) = \delta_{ij}$$

An orthonormal family that is a basis is an **orthonormal basis**.

EXAMPLE 5.1.8. When contemplating SPACE AROUND US I often imagine that the coordinate axes are there. After all the energy I exerted in Chapter Two explaining that it's really not good to have a specific basis in mind all the time, I know that I shouldn't do this, but I can't help it! There they are. One of their most obvious properties is that they are at right-angles. So at least I did something sophisticated: the standard basis $(\vec{e}_1,\vec{e}_2,\vec{e}_3)$ in SPACE AROUND US is an orthonormal basis for the standard inner product defined in Example 5.1.2.

REMARK 5.1.9. There is a very useful, very easy observation to make about orthonormal bases. Suppose that V is an inner product space and that $(\vec{v}_i)_{i\in I}$ is an orthonormal basis. Then I can write any $\vec{w} \in V$ in the form

$$\vec{w} = \sum_{i\in I} \lambda_i \vec{v}_i \tag{13}$$

The observation is that it is easy to calculate the λ_i. As soon as I apply the inner product with $\vec{v}_i$ to the left and right sides of (13) I get that $(\vec{w}, \vec{v}_i) = \lambda_i$ because of the orthonormality of $(\vec{v}_i)_{i\in I}$. In other words

$$\vec{w} = \sum_{i\in I} (\vec{w}, \vec{v}_i)\vec{v}_i \tag{14}$$

THEOREM 5.1.10. *Every finite dimensional inner product space has an orthonormal basis.*

PROOF. I'll call the inner product space V. It may be a real or a complex vector space, so I will let F denote the relevant field. I will prove the theorem by induction on $\dim_F(V)$.

The theorem is trivial when $\dim(V) = 0$, beginning the induction. Assume that $\dim(V) = n > 0$, so that there exists a non-zero vector $\vec{v} \in V$. Rescaling

$$\vec{v}_1 := \frac{1}{\|\vec{v}\|}\vec{v}$$

produces a unit vector by Exercise 72. The linear mapping

$$(-, \vec{v}_1) : V \to \mathbb{R}, \quad \vec{w} \mapsto (\vec{w}, \vec{v}_1)$$

is not zero since it sends $\vec{v}_1$ to 1. Therefore, by the Rank-Nullity Theorem, its kernel U has dimension $n - 1$. The axioms for an inner product hold for all elements of U since U is a subspace of V, and so U is also an inner product space. Therefore by induction U has an orthonormal basis $(\vec{v}_i)_{i=2}^n$. Since $(\vec{u}, \vec{v}_1) = 0$ for any $\vec{u} \in U$ it follows that $(\vec{v}_i)_{i=1}^n$ is an orthonormal basis for V. □

5.2. Orthogonal Complements and Orthogonal Projections

The proof of Theorem 5.1.10 above illustrates an important technique in inner product spaces. In that proof we took a vector $\vec{v}_1$ and then created a complementary subspace U to $\langle\vec{v}_1\rangle$ all of whose vectors were at right-angles to $\vec{v}$. This is an example of an orthogonal complement.

DEFINITION 5.2.1. *Let V be an inner product space and let $T \subseteq V$ be an arbitrary subset. Define*

$$T^\perp = \{\vec{v} \in V : \vec{v} \perp \vec{t} \text{ for all } \vec{t} \in T\},$$

calling this set the **orthogonal** *to T.*

EXERCISE 73. Show that: in an inner product space, V, $T^\perp$ is a subspace for *any* $T \subseteq V$. Show too that: $T^\perp = \langle T\rangle^\perp$.

PROPOSITION 5.2.2. *Let V be an inner product space and let U be a finite dimensional subspace of V. Then U and $U^\perp$ are complementary in the sense of Definition 1.7.6. In other words*

$$V = U \oplus U^\perp$$

PROOF. I am going to use the criteria given in Exercise 19. I must show that $U \cap U^\perp = 0$ and $V = U + U^\perp$.

Suppose first that $\vec{v} \in U \cap U^\perp$. Then $(\vec{v}, \vec{v}) = 0$. By the axioms for an inner product space, this means that $\vec{v} = \vec{0}$, as required. Now I'll show that every vector can be written as

$$\vec{v} = \vec{p} + \vec{r}$$

with $\vec{p} \in U$ and $\vec{r} \in U^\perp$. Thanks to Theorem 5.1.10 there exists an orthonormal basis for U, say $\vec{v}_1, \ldots, \vec{v}_n$. Following Remark 5.1.9 it is natural to try $\vec{p} = \sum_{i=1}^n \lambda_i \vec{v}_i$ where $\lambda_i = (\vec{v}, \vec{v}_i)$. If I do this, I'd better take $\vec{r} = \vec{v} - \sum_{i=1}^n \lambda_i \vec{v}_i$. What remains for me to show is that $\vec{r}$ does indeed belong to $U^\perp$. For this, I calculate:

$$(\vec{r}, \vec{v}_j) = (\vec{v}, \vec{v}_j) - \sum_{i=1}^n \lambda_i (\vec{v}_i, \vec{v}_j) = (\vec{v}, \vec{v}_j) - \sum_{i=1}^n \lambda_i \delta_{ij} = (\vec{v}, \vec{v}_j) - \lambda_j = 0.$$

Thus $\vec{r}$ is perpendicular to each $\vec{v}_j$ and hence to U, the space spanned by the $\vec{v}_j$'s. □

DEFINITION 5.2.3. *Let U be a finite dimensional subspace of an inner product space V. The space $U^\perp$ is the* **orthogonal complement to** *U. The* **orthogonal projection from** *V* **onto** *U is the mapping*

$$\pi_U : V \to V$$

that sends $\vec{v} = \vec{p} + \vec{r}$ to $\vec{p}$.

In the terminology of Exercise 23 π_U is the projection of V onto U along $U^\perp$. In particular, this means that π_U satisfies Properties (1) and (3) below. Property (2) has already been checked in the proof of Proposition 5.2.2

PROPOSITION 5.2.4. *Let U be a finite dimensional subspace of an inner product space V and let π_U be the orthogonal projection from V onto U.*

(1) π_U is a linear mapping with $\mathrm{im}(\pi_U) = U$ and kernel $\ker(\pi_U) = U^\perp$.
(2) If $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is an orthonormal basis of U, then π_U is given by the following formula for all $\vec{v} \in V$

$$\pi_U(\vec{v}) = \sum_{i=1}^n (\vec{v}, \vec{v}_i)\vec{v}_i$$

(3) $\pi_U^2 = \pi_U$, that is π_U is an idempotent.

I am now going to explain a few different uses of the orthogonal projection.

The Cauchy-Schwarz Inequality. I think this is the finest elementary inequality in mathematics. It is easy to prove – in many ways, in fact, as you'll see in a Workshop – and it permeates all of modern mathematics. The classical version of the inequality, called Cauchy's Inequality for real numbers, states that

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \leqslant \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}\sqrt{y_1^2 + y_2^2 + \cdots y_n^2}$$

A serious contemplation of this identity could lead you to invent real inner product spaces, as expounded in this lovely book. That's not a direction I'll take, but I do encourage you to investigate that book. As far as the notes are concerned, you should recognise the left hand side as the inner product $(\vec{x}, \vec{y})$ and the right hand side as $\|\vec{x}\|\|\vec{y}\|$. **The power of abstraction** strikes again: this inequality generalises. This is where Schwarz enters (and also Bunyakovsky – it's also sometimes called the Cauchy-Bunyakovsky-Schwarz inequality), as he proved that a similar inequality held for integrals:

$$\int_a^b f(t)g(t)dt \leqslant \left(\int_a^b f^2(t)dt\right)^{1/2} \left(\int_a^b g^2(t)dt\right)^{1/2}$$

This reminds you of Exercise 70(4) and Exercise 71(2), right? Well, it generalises much further, to evert sort of weird or wonderful, important or useless inner product space.

THEOREM 5.2.5 (Cauchy-Schwarz Inequality). *Let $\vec{v}, \vec{w}$ be vectors in an inner product space. Then*

$$|(\vec{v}, \vec{w})| \leqslant \|\vec{v}\|\|\vec{w}\|$$

with equality if and only $\vec{v}$ and $\vec{w}$ are linearly dependent.

PROOF. If $\vec{w} = \vec{0}$ then the statement is trivially true, so assume that $\vec{w} \neq \vec{0}$. Let $U = \langle \vec{w} \rangle$ and let $\vec{x} = \vec{v} - \pi_U(\vec{v})$. Then $\vec{x} \perp U$ and so Pythagoras' theorem yields:

$$\|\vec{v}\|^2 = \|\vec{x} + \pi_U(\vec{v})\|^2 = \|\vec{x}\|^2 + \|\pi_U(\vec{v})\|^2 \tag{15}$$

What is $\pi_U(\vec{v})$? To use Proposition 5.2.4(2) I need an orthonormal basis of U: the vector $\vec{w}/\|\vec{w}\|$ will do. Then I see

$$\pi_U(\vec{v}) = (\vec{v}, \frac{\vec{w}}{\|\vec{w}\|})\frac{\vec{w}}{\|\vec{w}\|} = \frac{(\vec{v}, \vec{w})}{\|\vec{w}\|^2}\vec{w}$$

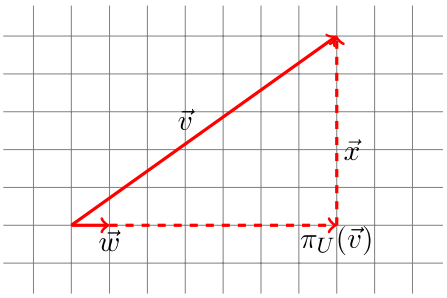
It follows that

$$\|\pi_U(\vec{v})\|^2 = (\frac{(\vec{v}, \vec{w})}{\|\vec{w}\|^2}\vec{w}, \frac{(\vec{v}, \vec{w})}{\|\vec{w}\|^2}\vec{w}) = \frac{|(\vec{v}, \vec{w})|^2}{\|\vec{w}\|^4}(\vec{w}, \vec{w}) = \frac{|(\vec{v}, \vec{w})|^2}{\|\vec{w}\|^2}$$

So (15) leads to:

$$\|\vec{v}\|^2 = \|\vec{x}\|^2 + \frac{|(\vec{v}, \vec{w})|^2}{\|\vec{w}\|^2} \geqslant \frac{|(\vec{v}, \vec{w})|^2}{\|\vec{w}\|^2}$$

with equality if and only if $\vec{x} = \vec{0}$. Multiplying through by $\|\vec{w}\|^2$ and taking square roots gives the Cauchy-Schwarz inequality; equality occurs precisely when $\vec{x} = \vec{v} - \pi_U(\vec{v}) = \vec{0}$, that is when $\vec{v} \in U$ and hence, since $U = \langle \vec{w} \rangle$, when $\vec{v}$ is linearly dependent on $\vec{w}$. □



Above is an illustration of the critical equality (15) in the proof of the Cauchy-Schwarz inequality, where I have taken the standard inner product on $\mathbb{R}^2$, $\vec{v} = (7, 5)^\mathsf{T}$ and $\vec{w} = (1, 0)^\mathsf{T}$. I find $\pi_U(\vec{v}) = (7, 0)^\mathsf{T}$ and $\vec{x} = (0, 5)^\mathsf{T}$.

As a simple application of this result – showing that more basic Euclidean geometry appears – I can now define the angle θ between two non-zero vectors $\vec{v}$ and $\vec{w}$ in a real inner product space: the Cauchy-Schwarz inequality implies that $-1 \leqslant (\vec{v}, \vec{w})/\|\vec{v}\|\|\vec{w}\| \leqslant 1$ and so there exists a unique $0 \leqslant \theta \leqslant \pi$ such that

$$\cos\theta = \frac{(\vec{v}, \vec{w})}{\|\vec{v}\|\|\vec{w}\|}.$$

This generalises the simple vector algebra fact in $\mathbb{R}^2$ that you probably wrote in school as:

$$\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}||\mathbf{b}| \cos\theta$$

where θ is the angle between $\mathbf{a}, \mathbf{b} \in \mathbb{R}^2$.

I'll just point out the following corollary for form's sake. It's not critical for the course but it is critical for mathematics: the items listed are exactly the axioms for a **normed vector space** which is the heart of functional analysis.

COROLLARY 5.2.6. *The norm $\|\cdot\|$ on an inner product space V satisfies, for any $\vec{v},\vec{w}\in V$ and scalar λ:*

(1) $\|\vec{v}\|\geqslant 0$ *with equality if and only if* $\vec{v}=\vec{0}$.
(2) $\|\lambda\vec{v}\|=|\lambda|\|\vec{v}\|$
(3) $\|\vec{v}+\vec{w}\|\leqslant\|\vec{v}\|+\|\vec{w}\|$, *the* **triangle inequality**

PROOF. (1) is an axiom for an inner product space; (2) is Exercise 72; (3) is a consequence of Cauchy-Schwarz as follows. First, expanding out the brackets as in Example 5.1.6

$$\|\vec{v}+\vec{w}\|^2=\|\vec{v}\|^2+(\vec{v},\vec{w})+(\vec{w},\vec{v})+\|\vec{w}\|^2=\|\vec{v}\|^2+2\Re e(\vec{v},\vec{w})+\|\vec{w}\|^2.$$

Then observe (by the usual triangle inequality in the plane if the underlying field is $\mathbb{C}$ and) by the Cauchy-Schwarz inequality that $\Re e(\vec{v},\vec{w})\leqslant|(\vec{v},\vec{w}))|\leqslant\|\vec{v}\|\|\vec{w}\|$. Therefore

$$\|\vec{v}+\vec{w}\|^2\leqslant|\vec{v}\|^2+2\|\vec{v}\|\|\vec{w}\|+\|\vec{w}\|^2=(\|\vec{v}\|+\|\vec{w}\|)^2$$

Taking square roots gives the result. □

Gram-Schmidt Process. In Theorem 5.1.10 I showed you that every finite dimensional inner product space has an orthonormal basis. I'll now show you how to find such a basis by massaging any existing basis.

THEOREM 5.2.7. *Let $\vec{v}_1,\ldots,\vec{v}_k$ be a linearly independent vectors in an inner product space V. Then there exists an orthonormal family $\vec{w}_1,\ldots,\vec{w}_k$ with the property that for all $1\leqslant i\leqslant k$*

$$\vec{w}_i\in\mathbb{R}_{>0}\vec{v}_i+\langle\vec{v}_{i-1},\ldots,\vec{v}_1\rangle$$

PROOF. Following Definition 5.2.3, I can decompose any $\vec{v}_i$ as $\vec{v}_i=\vec{p}_i+\vec{r}_i$ where $\vec{p}_i$ is the orthogonal projection of $\vec{v}_i$ onto the subspace $\langle\vec{v}_{i-1},\ldots,\vec{v}_1\rangle$ and where $\vec{r}_i$ belongs to the orthogonal complement of this subspace. The vectors $\vec{w}_i=\vec{r}_i/\|\vec{r}_i\|$ are then an orthonormal family with the displayed property. □

EXERCISE 74. Prove that there is a unique orthonormal family whose elements satisfy the property displayed in the statement of Theorem 5.2.7.

The proof of Theorem 5.2.7 actually gives an algorithm for constructing an orthonormal family from an arbitrary ordered linearly independent subset of an inner product space. If the linearly independent subset happened to be a basis, then this process produces an orthonormal basis. Of course, it is best illustrated through an example, but let me first explain in words what is going to happen. I'll start out with an arbitrary linearly independent ordered subset $\vec{v}_1,\vec{v}_2,\ldots$ of an inner product space. I'll take the first element $\vec{v}_1$ and normalise it so that it has length 1. That will be the first element $\vec{w}_1$ of the new orthonormal family I'm going to produce. Now I take the second vector $\vec{v}_2$ from the subset. I want to adjust it to be at right-angles to $\vec{w}_1$. To do this I subtract from it the orthogonal projection of it onto the space $\langle\vec{w}_1\rangle$. This gives me the vector at right-angles that I wanted, and I normalise it so that it has length 1. This will be $\vec{w}_2$, the second element of the orthonormal family. Now I take the third vector $\vec{v}_3$ from the subset. I want to adjust it to be at right-angles to the first two vectors $\vec{w}_1,\vec{w}_2$. To do this I subtract from it the orthogonal projection of it onto the space $\langle\vec{w}_1,\vec{w}_2\rangle$. This gives the vector I wanted, and I normalise it so that it has length 1. This will be $\vec{w}_3$. I repeat this until I've dealt with all the vectors $\vec{v}_1,\vec{v}_2,\ldots$. Observe that each step I have $\langle\vec{w}_{i-1},\ldots,\vec{w}_1\rangle\subseteq\langle\vec{v}_{i-1},\ldots,\vec{v}_1\rangle$ and because the dimension of both sides is the same, this is actually an equality.

EXAMPLE 5.2.8. Consider $\mathbb{R}^4$ with the standard inner product. Let V be the subspace of $\mathbb{R}^4$ with basis $\{\vec{v}_1,\vec{v}_2,\vec{v}_3\}$ where

$$\vec{v}_1=(1,1,0,0)^{\mathsf{T}},\vec{v}_2=(1,0,1,1)^{\mathsf{T}},\vec{v}_3=(1,0,0,1)^{\mathsf{T}}$$

I want to construct an orthonormal basis $\{\vec{w}_1, \vec{w}_2, \vec{w}_3\}$ of V from the basis $\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ using the proof of the theorem.

To unclutter notation, I won't write T to transpose row vectors; that is always there implicitly, and I don't think it is going to cause you any confusion. Let $\vec{w}_1 = \vec{v}_1/||\vec{v}_1|| = \frac{1}{\sqrt{2}}(1,1,0,0)$. Now find a vector

$$\vec{w}_2' = \vec{v}_2 - \lambda\vec{v}_1 = (1,0,1,1) - \lambda(1,1,0,0) = (1-\lambda, -\lambda, 1, 1)$$

and choose λ so that $\vec{w}_2' \perp \vec{w}_1$. For this, I need

$$(\vec{w}_2', \vec{w}_1) = 1 - \lambda - \lambda = 0$$

so that $\lambda = \frac{1}{2}$. This gives $\vec{w}_2' = (\frac{1}{2}, -\frac{1}{2}, 1, 1)$. Normalising this for unit length gives $\vec{w}_2 = \vec{w}_2'/\|\vec{w}_2'\| = \frac{1}{\sqrt{10}}(1,-1,2,2)$. Now put

$$\begin{aligned}\vec{w}_3' = \vec{v}_3 - \lambda_1\vec{w}_1 - \lambda_2\vec{w}_2 &= (1,0,0,1) - \frac{\lambda_1}{\sqrt{2}}(1,1,0,0) - \frac{\lambda_2}{\sqrt{10}}(1,-1,2,2) \\ &= (1 - \frac{\lambda_1}{\sqrt{2}} - \frac{\lambda_2}{\sqrt{10}}, -\frac{\lambda_1}{\sqrt{2}} + \frac{\lambda_2}{\sqrt{10}}, -2\frac{\lambda_2}{\sqrt{10}}, 1 - 2\frac{\lambda_2}{\sqrt{10}})\end{aligned}$$

and choose λ_1, λ_2 so that $\vec{w}_3' \perp \vec{w}_1, \vec{w}_2$. For $\vec{w}_3' \perp \vec{w}_1$, I need

$$(\vec{w}_3', \vec{w}_1) = \frac{1}{\sqrt{2}}\left((1,0,0,1),(1,1,0,0)) - \frac{\lambda_1}{\sqrt{2}}((1,1,0,0),(1,1,0,0))\right) = 0$$

That is $1 - \sqrt{2}\lambda_1 = 0$, so $\lambda_1 = 1/\sqrt{2}$. (Note that I have used the fact that $\vec{w}_1 \perp \vec{w}_2$ when calculating here; the effect is that I get an equation with λ_1 alone.) For $\vec{w}_3' \perp \vec{w}_2$, I need

$$(\vec{w}_3', \vec{w}_2) = \frac{1}{\sqrt{10}}\left((1,0,0,1),(1,-1,2,2)) - \frac{\lambda_2}{\sqrt{10}}((1,-1,2,2),(1,-1,2,2))\right) = 0$$

That is $3 - \lambda_2\sqrt{10} = 0$, so $\lambda_2 = 3/\sqrt{10}$. Hence

$$\vec{w}_3' = (1,0,0,1) - \frac{1}{2}(1,1,0,0) - \frac{3}{10}(1,-1,2,2) = \frac{1}{5}(1,-1,-3,2)$$

Normalising this for length one gives $\vec{w}_3 = \frac{1}{\sqrt{15}}(1,-1,-3,2)$. So the orthonormal basis produced by the Gram-Schmidt process is

$$\vec{w}_1 = \frac{1}{\sqrt{2}}(1,1,0,0), \quad \vec{w}_2 = \frac{1}{\sqrt{10}}(1,-1,2,2), \quad \vec{w}_3 = \frac{1}{\sqrt{15}}(1,-1,-3,2)$$

You can double-check easily that these vectors have length one and are orthogonal to one another.

Just for a little extra pleasure, let's take a random vector in V, say $\vec{v} = \vec{v}_1 + \vec{v}_2 - \vec{v}_3 = (1,1,1,0)$. This can be written as $\alpha_1\vec{w}_1 + \alpha_2\vec{w}_2 + \alpha_3\vec{w}_3$ where the coefficients α_i are given by

$$\alpha_1 = (\vec{v}, \vec{w}_1) = \frac{2}{\sqrt{2}} = \sqrt{2}, \quad \alpha_2 = (\vec{v}, \vec{w}_2) = \frac{2}{\sqrt{10}} = \frac{\sqrt{10}}{5}, \quad \alpha_3 = (\vec{v}, \vec{w}_3) = \frac{-3}{\sqrt{15}} = -\frac{\sqrt{15}}{5}$$

5.3. Adjoints and Self-Adjoints

Do you remember my question in lectures about the dictionary between linear mapping and matrices: what does the transpose of a matrix mean for a linear mapping? I'm going to show you something very closely related by introducing the adjoint of a linear mapping on V. You'll already have come across this if you are taking Honours Differential Equations. To connect to that, I think of differential equations in two parts: a space of functions I want to use (periodic, complex valued, square-integrable, whatever) together with differential equations (such as $-\frac{d}{dx}(p(x)\frac{d}{dx}) + q(x)$) that I consider as mappings on the space of functions. The functions used often produce inner product

spaces similar to Exercise 70(4) and Exercise 71(3), and studying eigenvalues and eigenfunctions related to the differential equation is closely related to what I do here. For me, the most crucial is the case of a self-adjoint operator, which is at the heart of Sturm-Liouville Theory. A second place where this theory is critical is in Introduction to Lie Groups where the symmetry involved in adjoints are probed systematically.

DEFINITION 5.3.1. *Let V be an inner product space. Then two endomorphism $T, S : V \to V$ are called* **adjoint** *to one another if the following holds for all $\vec{v}, \vec{w} \in V$:*

$$(T\vec{v}, \vec{w}) = (\vec{v}, S\vec{w})$$

In this case I will write $S = T^*$ and call S the **adjoint** *of T.*

REMARK 5.3.2. Any endomorphism has at most one adjoint. This is because if both S and S' are adjoint to T then $(\vec{v}, S\vec{w} - S'\vec{w}) = 0$ for all $\vec{v}, \vec{w} \in V$, so the positivity axiom for an inner product space immediately implies that $S\vec{w} = S'\vec{w}$ for all $\vec{w}$.

EXERCISE 75. Show that: If T^* is the adjoint of T, then T^* has an adjoint and it is $(T^*)^* = T$.

I don't have a particularly persuasive intuitive reason why I must study adjoints: it's an obvious and nice definition, but there is not much more that I can write at this moment. Sigh! Probably the best thing I can say is taking the adjoint of an endomorphism is analogous to taking the conjugate of a complex number and leave it at that. Maybe you're smitten by complex conjugation, maybe not. So in fact probably the best thing I can do is present an example.

EXAMPLE 5.3.3. Suppose $V = \mathbb{R}^n$ or $\mathbb{C}^n$ with the standard inner product and suppose the endomorphism T of V is given by matrix multiplication $A\circ$ where $A \in \mathsf{Mat}(n;\mathbb{R})$ or $A \in \mathsf{Mat}(n;\mathbb{C})$.

Recall from Definition 5.1.2 that in $\mathbb{R}^n$, $(\vec{v}, \vec{w}) = \vec{v}^{\mathsf{T}} \circ \vec{w}$. Hence

$$(A \circ \vec{v}, \vec{w}) = (A \circ \vec{v})^{\mathsf{T}} \circ \vec{w} = \vec{v}^{\mathsf{T}} \circ A^{\mathsf{T}} \circ \vec{w} = \vec{v}^{\mathsf{T}} \circ (A^{\mathsf{T}} \circ \vec{w}) = (\vec{v}, A^{\mathsf{T}} \circ \vec{w})$$

Therefore the adjoint of multiplication by A in $\mathbb{R}^n$ is multiplication by A^{T}. At last, some meaning for the transpose!

In $\mathbb{C}^n$ Definition 5.1.4 tells me that $(\vec{v}, \vec{w}) = \vec{v}^{\mathsf{T}} \circ \overline{\vec{w}}$, so I find

$$(A \circ \vec{v}, \vec{w}) = (\vec{v}, \overline{A}^{\mathsf{T}} \circ \vec{w})$$

where $\overline{A}^{\mathsf{T}}$ denotes the **conjugate transpose** of A, the matrix obtained from A by first conjugating each entry and then transposing the resulting matrix. Therefore the adjoint of multiplication by A in $\mathbb{C}^n$ is multiplication by $\overline{A}^{\mathsf{T}}$.

THEOREM 5.3.4. *Let V be a finite dimensional inner product space. Let $T : V \to V$ be an endomorphism. Then T^* exists. That is, there exists a unique linear mapping $T^* : V \to V$ such that for all $\vec{v}, \vec{w} \in V$*

$$(T\vec{v}, \vec{w}) = (\vec{v}, T^*\vec{w})$$

PROOF. I will begin by defining $T^*\vec{w}$ for an arbitrary $\vec{w} \in V$. I'll use again the notation that F stands for either $\mathbb{R}$ or $\mathbb{C}$ depending on whether V is real or complex inner product space. Fix $\vec{w} \in V$ and consider the mapping

$$\phi = (T(-), \vec{w}) : V \to F$$

This is linear since it is the composition of the two linear mappings T and $(-, \vec{w})$.

I claim there is a unique vector $\vec{u} \in V$ such that $\phi(\vec{v}) = (\vec{v}, \vec{u})$ for all $\vec{v} \in V$. To see that $\vec{u}$ exists, take by Theorem 5.1.10 any orthonormal basis of V, say $\vec{e}_1, \ldots, \vec{e}_n$. By (14) $\vec{v} = \sum_{i=1}^n (\vec{v}, \vec{e}_i)\vec{e}_i$. By the linearity of ϕ and the sesquilinearity of the $(-,-)$ I get

$$\phi(\vec{v}) = \sum_{i=1}^n (\vec{v}, \vec{e}_i)\phi(\vec{e}_i) = (\vec{v}, \sum_{i=1}^n \overline{\phi(\vec{e}_i)}\vec{e}_i)$$

Hence $\vec{u} = \sum_{i=1}^n \overline{\phi(\vec{e}_i)}\vec{e}_i$ does the trick for existence. The uniqueness is quicker: if $\vec{u}$ and $\vec{u}'$ both produce ϕ, then

$$(\vec{v}, \vec{u} - \vec{u}') = (\vec{v}, \vec{u}) - (\vec{v}, \vec{u}') = \phi(\vec{v}) - \phi(\vec{v}) = 0$$

for all $\vec{v} \in V$. By positivity then, $\vec{u} - \vec{u}' = 0$, i.e. $\vec{u} = \vec{u}'$.

This defines T^*: for each $\vec{w} \in V$ I find the corresponding $\vec{u}$ from above and that's $T^*\vec{w}$. This is a well-defined and unique mapping $T^* : V \to V$ that satisfies the property

$$(T\vec{v}, \vec{w}) = (\vec{v}, T^*\vec{w})$$

for all $\vec{v}, \vec{w} \in V$. It remains for me to prove that T^* is linear. Let $\vec{w}_1, \vec{w}_2 \in V$ and $\lambda \in F$. Then disentangling the definition of T^* gives me for any $\vec{v} \in V$

$$(\vec{v}, T^*(\vec{w}_1 + \vec{w}_2)) = (T\vec{v}, \vec{w}_1 + \vec{w}_2) = (T\vec{v}, \vec{w}_1) + (T\vec{v}, \vec{w}_2) = (\vec{v}, T^*\vec{w}_1) + (\vec{v}, T^*\vec{w}_2) = (\vec{v}, T^*\vec{w}_1 + T^*\vec{w}_2)$$

and

$$(\vec{v}, T^*(\lambda\vec{w}_1)) = (T\vec{v}, \lambda\vec{w}_1) = \overline{\lambda}(T\vec{v}, \vec{w}_1) = \overline{\lambda}(\vec{v}, T^*\vec{w}_1) = (\vec{v}, \lambda T^*\vec{w}_1)$$

It follows from the uniqueness claim of the paragraph above that $T^*(\vec{w}_1 + \vec{w}_2) = T^*\vec{w}_1 + T^*\vec{w}_2$ and $T^*(\lambda\vec{w}_1) = \lambda T^*\vec{w}_1$. That's what I wanted to prove! □

DEFINITION 5.3.5. *An endomorphism of an inner product space $T : V \to V$ is* **self-adjoint** *if it equals its own adjoint, that is if $T^* = T$.*

If you liked the idea that taking the adjoint of an endomorphism is analogous to taking the conjugate of a complex number, then you'll buy in to self-adjoint operators being analogous to real numbers. Given Theorem 5.3.7 below, this analogy starts to seem realistic.

EXAMPLE 5.3.6. By Example 5.3.3, a real $(n \times n)$-matrix A describes a self-adjoint mapping on the standard inner product space $\mathbb{R}^n$ precisely when A is symmetric, that is when $A^\mathsf{T} = A$. A complex $(n \times n)$-matrix A describes a self-adjoint mapping on the standard inner product space $\mathbb{C}^n$ precisely when $A = \overline{A}^\mathsf{T}$ holds. Such matrices are called **hermitian**.

THEOREM 5.3.7. *Let $T : V \to V$ be a self-adjoint linear mapping on an inner product space V.*

(1) Every eigenvalue of T is real.
(2) If λ and μ are distinct eigenvalues of T with corresponding eigenvectors $\vec{v}$ and $\vec{w}$, then $(\vec{v}, \vec{w}) = 0$.
(3) T has an eigenvalue.

PROOF. (1) This first statement has content only for a complex inner product space. But let $\vec{v}$ be an eigenvector of T with eigenvalue λ. Then

$$\lambda(\vec{v}, \vec{v}) = (\lambda\vec{v}, \vec{v}) = (T\vec{v}, \vec{v}) = (\vec{v}, T\vec{v}) = (\vec{v}, \lambda\vec{v}) = \overline{\lambda}(\vec{v}, \vec{v})$$

Since $\vec{v} \neq \vec{0}$, I have $(\vec{v}, \vec{v}) > 0$ and so $\lambda = \overline{\lambda}$.

(2) Both λ and μ must be real by (1). Therefore

$$\lambda(\vec{v}, \vec{w}) = (T\vec{v}, \vec{w}) = (\vec{v}, T\vec{w}) = \mu(\vec{v}, \vec{w})$$

Since $\lambda \neq \mu$ this is only possible if $(\vec{v}, \vec{w}) = 0$.

(3) In the case of a complex inner product space this is simply a consequence of Theorem 4.5.4 since $\mathbb{C}$ is algebraically closed. The real case is much more interesting. If you are so-minded you

can find an algebraic proof in Lemma 7.12 of Linear Algebra Done Right. But I find that proof doesn't tell me anything except the statement is true, so I prefer the following proof, which may remind you of the proof of Perron's Theorem.

Assume that V is a finite dimensional real inner product space. Define the following real-valued function $R : V \setminus \{\vec{0}\} \to \mathbb{R}$

$$\vec{v} \mapsto R(\vec{v}) = \frac{(T\vec{v}, \vec{v})}{(\vec{v}, \vec{v})}$$

It's called the **Raleigh Quotient**. Restricting this function to the unit sphere $\{\vec{v} : \|\vec{v}\| = 1\}$ allows me to apply the Heine–Borel Theorem from Honours Analysis to deduce that there exists a point on the unit sphere, $\vec{v}_+$, where R achieves its maximum. Because the function R has the property that $R(\lambda\vec{v}) = R(\vec{v})$ for any $\lambda \in \mathbb{R}_{>0}$ this means that the function R actually achieves its maximum on all of $V \setminus \{\vec{0}\}$ at $\vec{v}_+$. Now take any vector $\vec{w} \in V$ and observe that for any really small $t \in \mathbb{R}$ the one-variable function $t \mapsto R_{\vec{w}}(t) = R(\vec{v}_+ + t\vec{w})$ is well-defined. Written out this is

$$R_{\vec{w}}(t) = \frac{(T(\vec{v}_+ + t\vec{w}), \vec{v}_+ + t\vec{w})}{(\vec{v}_+ + t\vec{w}, \vec{v}_+ + t\vec{w})}$$

The derivative of this function with respect to t has got to vanish at $t = 0$ because $\vec{v}_+$ is a maximum. By the quotient rule I can write out $R'_{\vec{w}}(0)$ explicitly for all $\vec{w} \in V$:

$$R'_{\vec{w}}(0) = \frac{(T\vec{w}, \vec{v}_+) + (T\vec{v}_+, \vec{w})}{(\vec{v}_+, \vec{v}_+)} - \frac{2(T\vec{v}_+, \vec{v}_+)(\vec{v}_+, \vec{w})}{(\vec{v}_+, \vec{v}_+)^2}$$

If I choose any $\vec{w} \perp \vec{v}_+$ I then deduce that

$$\frac{(T\vec{w}, \vec{v}_+) + (T\vec{v}_+, \vec{w})}{(\vec{v}_+, \vec{v}_+)} = 0$$

and so, by using that T is self-adjoint and $(\vec{v}_+, \vec{v}_+) \neq 0$, that $\vec{w} \perp T\vec{v}_+$. In other words, $T\vec{v}_+ \in (\langle\vec{v}_+\rangle^\perp)^\perp$. By Proposition 5.2.2 $(\langle\vec{v}_+\rangle^\perp)^\perp = \langle\vec{v}_+\rangle$ and so $T\vec{v}_+ \in \mathbb{R}\vec{v}_+$, as required. □

REMARK 5.3.8. (1) Why do I like this proof? It's completely geometric! Let me consider $\mathbb{R}^2$ with its standard inner product. To illustrate the theorem I'll take T to be represented by the symmetric matrix

$$T = \begin{pmatrix} 5 & -6 \\ -6 & 13 \end{pmatrix}$$

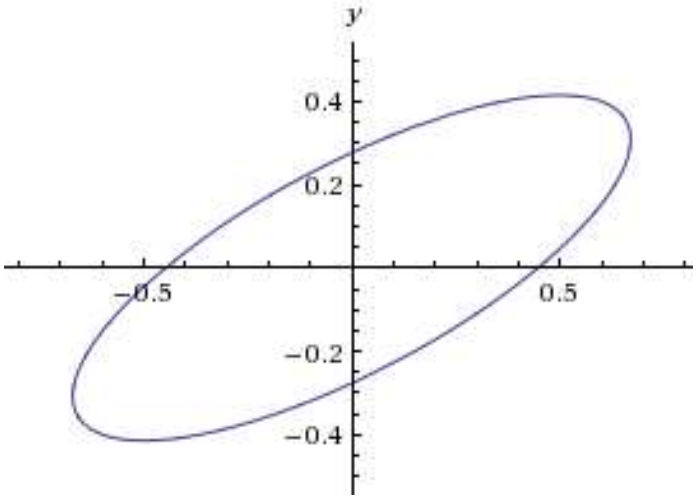
I chose this more-or-less at random; I need it to be symmetric for T to be self-adjoint and that's all. The proof above then tells me to maximise the Rayleigh quotient

$$R(\vec{v}) = \frac{(T\vec{v}, \vec{v})}{(\vec{v}, \vec{v})}$$

over the set of points $\|\vec{v}\| = 1$. Because of the invariance of $R(\vec{v})$ under dilation, maximizing the numerator of $R(\vec{v})$ while keeping the denominator fixed is the same as minimizing the denominator while keeping the numerator fixed. So I have to minimize $\|\vec{v}\|$ over the set of points $(T\vec{v}, \vec{v}) = 1$. If I write $\vec{v} = (x, y)^\mathsf{T}$ then I see that

$$(T\vec{v}, \vec{v}) = ((5x - 6y, -6x + 13y)^\mathsf{T}, (x, y)^\mathsf{T}) = 5x^2 - 12xy + 13y^2$$

Here is a plot of $5x^2 - 12xy + 13y^2 = 1$:



Now think back to school when you studied ellipses: remember that any ellipse is symmetric about two axes at right angles to one another, called the major and the minor axes. Here the major axis is a line roughly in the northeast-southwest direction and the minor axis in the northwest-southeast direction. Minimizing $\|\vec{v}\|$ on this curve chooses the two points on the curve closest to the origin; the line through those points is precisely what determines the minor axis. Of course, I could applied exactly the same argument as in the proof of Theorem 5.3.7 *except* for looking for a minimum for $R(\vec{v})$ instead of a maximum. This would then have produced a different eigenvector, this time determining the points on the curve furthest from the origin, i.e. the major axis. That the major and minor axes are at right angles to each other then just becomes a manifestation of Part (2) of Theorem 5.3.7. All that understanding just from thinking what $(T\vec{v}, \vec{v})$ actually is!
(2) Let $(V, (-,-)) = (\mathbb{R}^n, \bullet)$ be the standard n-dimensional inner product space, defined by the dot product

$$(x_1, x_2, \ldots, x_n) \bullet (y_1, y_2, \ldots, y_n) \;=\; \sum_{i=1}^{n} x_i y_i \in \mathbb{R}\,.$$

Given a symmetric $n \times n$ matrix $A = (a_{ij}) \in \mathsf{Mat}(n;\mathbb{R})$ let $T : \mathbb{R}^n \to \mathbb{R}^n$ be the self-adjoint endomorphism with matrix A defined by

$$T(x_1, x_2, \ldots, x_n) \;=\; (\sum_{j=1}^{n} a_{1j}x_j, \sum_{j=1}^{n} a_{2j}x_j, \ldots, \sum_{j=1}^{n} a_{nj}x_j) \in \mathbb{R}^n\,.$$

Consider the Rayleigh quotient function as in the proof of Theorem 5.3.7

$$R \;:\; \mathbb{R}^n\backslash\{\vec{0}\} \to \mathbb{R}\;;\; \vec{x} = (x_1, x_2, \ldots, x_n) \mapsto R(\vec{x}) \;=\; \frac{T\vec{x} \bullet \vec{x}}{\vec{x} \bullet \vec{x}} \;=\; \frac{\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} a_{ij}x_i x_j}{\sum\limits_{k=1}^{n}(x_k)^2}\,.$$

In view of the Spectral Theorem for Real Symmetric Matrices 5.3.12 below, the symmetric matrix A is diagonalizable, and $\mathbb{R}^n$ has an orthonormal basis $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)$ of eigenvectors of T (= eigenvectors of A) such that

$$T(\vec{v}_i) \;=\; \lambda_i \vec{v}_i \in \mathbb{R}^n$$

with the eigenvalues such that $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$. With respect to this basis $\mathcal{B}$ the Rayleigh quotient becomes

$$R(x_1, x_2, \ldots, x_n) \;=\; \frac{\sum_{j=1}^{n} \lambda_j (x_j)^2}{\sum_{k=1}^{n} (x_k)^2} \in \mathbb{R}$$

with maximum value λ_1 and minimum value λ_n. In particular, if $n = 2$ then the subset

$$E \;=\; \{(x_1, x_2) \in \mathbb{R}^2 \,|\, \lambda_1 (x_1)^2 + \lambda_2 (x_2)^2 = 1\} \subset \mathbb{R}^2$$

is a 'conic section'. (Conic sections have been studied for 2,000 years, since before Archimedes). As in the example in (1) if $\lambda_1 \geqslant \lambda_2 > 0$ E is an ellipse with maximum (resp. minimum) distance from the origin $1/\sqrt{\lambda_1}$ (resp. $1/\sqrt{\lambda_2}$). See Remark 5.3.16 below for a bit more about this. □

Upwards to one of the highlights of the course, your degree, your intellectual life:

Simple Cosmic Beauty

At this moment the theorem below might only appear as a good-looking result: general hypothesis; simple statement; natural outcome. And I hope you are meeting such handsome theorems each week at University. You are, aren't you? The Spectral Theorem, however, and its correct infinite dimensional extension to Hilbert Spaces, is ubiquitous. Is that apparent to you? Maybe not. Except you may at least be surprised by the result that all real symmetric matrices are diagonalisable. Oh, and you might be taking Honours Differential Equations and know that it is the foundation of Sturm-Liouville Theory. And if you have taken a course in quantum mechanics you may know that observables are self-adjoint operators on the space of states, a Hilbert space, and that eigenvalues are then possible measurement outcomes. And I know you've just seen that self-adjoint operators control parts of classical geometry. But that would be just the beginning! [2]

THEOREM 5.3.9 (The Spectral Theorem for Self-Adjoint Endomorphisms). *Let V be a finite dimensional inner product space and let $T : V \to V$ be a self-adjoint linear mapping. Then V has an orthonormal basis consisting of eigenvectors of T.*

PROOF. I'll induct on $\dim V$. If $\dim V$ is either 0 or 1 the result clearly holds. Now assume that $\dim V > 1$ and that the result holds on inner product spaces of smaller dimension.

Let λ be any eigenvalue of T. By Theorem 5.3.7 this exists and is real. Let $\vec{u}$ be an eigenvector with eigenvalue λ, normalized so that $\vec{u}$ has unit length. Let $U = \langle \vec{u} \rangle$. Suppose that $\vec{v} \in U^\perp$. Then because T is self-adjoint and $\vec{u}$ is an eigenvector, I have

$$(\vec{u}, T\vec{v}) = (T\vec{u}, \vec{v}) = (\lambda \vec{u}, \vec{v}) = \lambda (\vec{u}, \vec{v}) = 0$$

Therefore $T(U^\perp) \subseteq U^\perp$. Thus T restricted to $U^\perp$ defines a linear mapping $T|_{U^\perp} : U^\perp \to U^\perp$. This linear mapping is self-adjoint because T is, and so the induction hypothesis applies to give me an orthonormal basis of $U^\perp$ consisting of eigenvectors of $T|_{U^\perp}$. Combined with $\vec{u}$, this gives me the orthonormal basis of V that I was seeking. □

EXAMPLE 5.3.10. First of all I'll show you this theorem in action in the real case. Let T be the symmetric matrix appearing in Remark 5.3.8

$$T = \begin{pmatrix} 5 & -6 \\ -6 & 13 \end{pmatrix}$$

[2] And in any case "The Spectral Theorem" is a cool name

Its characteristic polynomial is $x^2 - 18x + 29$ (I told you it was more-or-less random!) The roots of this are $9 \pm 2\sqrt{13}$. So I have to find null vectors for

$$T - (9 + 2\sqrt{13})I_2 = \begin{pmatrix} -4 - 2\sqrt{13} & -6 \\ -6 & 4 - 2\sqrt{13} \end{pmatrix} \text{ and } T - (9 - 2\sqrt{13})I_2 = \begin{pmatrix} -4 + 2\sqrt{13} & -6 \\ -6 & 4 + 2\sqrt{13} \end{pmatrix}$$

For the first, I find $(6, -4 - 2\sqrt{13})^\mathsf{T}$; for the second, $(6, -4 + 2\sqrt{13})^\mathsf{T}$. Neither of these is a unit vector, so I have to normalize. This produces

$$\vec{u}_1 = \frac{1}{2\sqrt{26 + 4\sqrt{13}}}(6, -4 - 2\sqrt{13})^\mathsf{T} \text{ and } \vec{u}_2 = \frac{1}{2\sqrt{26 - 4\sqrt{13}}}(6, -4 + 2\sqrt{13})^\mathsf{T}$$

Observe explicitly that $\vec{u}_1 \perp \vec{u}_2$. If I get the computer to calculate a decimal expansion of these vectors I find $(0.47, -0.88)$ and $(0.88, 0.47)$. If you look back at the picture of the ellipse in Remark 5.3.8, you'll see that these tie up with the directions of the minor and major axes respectively.

If I wrote out what I've just done in terms of matrices it is $P^{-1}TP = D$ where D is the diagonal matrix consisting of the eigenvalues of T and P is the matrix whose columns are the corresponding eigenvectors of T. Explicitly:

$$D = \operatorname{diag}(9 + 2\sqrt{13}, 9 - 2\sqrt{13}), \quad P = \begin{pmatrix} \frac{6}{2\sqrt{26+4\sqrt{13}}} & \frac{6}{2\sqrt{26-4\sqrt{13}}} \\ \frac{-4-2\sqrt{13}}{2\sqrt{26+4\sqrt{13}}} & \frac{-4+2\sqrt{13}}{2\sqrt{26-4\sqrt{13}}} \end{pmatrix}$$

Remarkably, when I calculate P^{-1} I find

$$P^{-1} = \begin{pmatrix} \frac{6}{2\sqrt{26+4\sqrt{13}}} & \frac{-4-2\sqrt{13}}{2\sqrt{26+4\sqrt{13}}} \\ \frac{6}{2\sqrt{26-4\sqrt{13}}} & \frac{-4+2\sqrt{13}}{2\sqrt{26-4\sqrt{13}}} \end{pmatrix}$$

That is, $P^{-1} = P^\mathsf{T}$.

DEFINITION 5.3.11. *Show that: an* **orthogonal matrix** *is an $(n \times n)$-matrix P with real entries such that $P^\mathsf{T}P = I_n$. In other words, an orthogonal matrix is a square matrix P with real entries such that $P^{-1} = P^\mathsf{T}$.*

EXERCISE 76. The condition that $P^\mathsf{T}P = I_n$ is equivalent to the columns of P forming an orthonormal basis for $\mathbb{R}^n$ with its standard inner product.

EXERCISE 77. Show that: the set $\{P \in \mathsf{Mat}(n; \mathbb{R}) : P^\mathsf{T}P = I_n\}$ is a group. It is called the **orthogonal group**, $O(n)$.

COROLLARY 5.3.12 (The Spectral Theorem for Real Symmetric Matrices). *Let A be a real $(n \times n)$-symmetric matrix. Then there is an $(n \times n)$-orthogonal matrix P such that*

$$P^\mathsf{T}AP = P^{-1}AP = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$$

where $\lambda_1, \ldots, \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of the characteristic polynomial of A.

PROOF. This follows from combining the Spectral Theorem applied to $\mathbb{R}^n$ with its standard inner product with Exercise 76. □

EXAMPLE 5.3.13. Now I'll show you the Spectral Theorem in action in the complex case. Let T be the hermitian matrix

$$T = \frac{1}{2}\begin{pmatrix} 5 & 1 & -1 + i \\ 1 & 5 & 1 - i \\ -1 - i & 1 + i & 4 \end{pmatrix}$$

A calculation gives the characteristic polynomial of T to be $-x^3+7x^2-15x+9=(3-x)^2(1-x)$. I then calculate the eigenspace for $E(3,T)$ to be spanned by $(1,1,0)^\mathsf{T}$ and $(2,0,-1-i)^\mathsf{T}$. I calculate the eigenspace $E(1,T)$ to be spanned by $(1,-1,1+i)^\mathsf{T}$. So, I'm almost done: $E(1,T)\perp E(3,T)$. But I still don't have an orthonormal basis of eigenvectors. For this I need to find an orthonormal basis of $E(3,T)$ first and also to normalise the basis vector of $E(1,T)$ I've given. I use the Gram-Schmidt Process to deal with $E(3,T)$, starting with the basis $(1,1,0)^\mathsf{T}$ and $(2,0,-1-i)^\mathsf{T}$. This gives me an orthonormal basis of eigenvectors:

$$\vec{u}_1=\frac{1}{\sqrt{2}}(1,1,0)^\mathsf{T},\quad \vec{u}_2=\frac{1}{2}(1,-1,-1-i)^\mathsf{T},\quad \vec{u}_3=\frac{1}{2}(1,-1,1+i)^\mathsf{T}$$

If I wrote out what I've just done in terms of matrices it is $P^{-1}TP=D$ where D is the diagonal matrix consisting of the eigenvalues of T and P is the matrix whose columns are the corresponding eigenvectors of T. Explicitly:

$$D=\operatorname{diag}(3,3,1),\quad P=\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2}\\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & -\frac{1}{2}\\ 0 & -\frac{1+i}{2} & \frac{1+i}{2}\end{pmatrix}$$

Remarkably, when I calculate P^{-1} I find

$$P^{-1}=\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ \frac{1}{2} & -\frac{1}{2} & -\frac{1-i}{2}\\ \frac{1}{2} & -\frac{1}{2} & \frac{1-i}{2}\end{pmatrix}$$

That is, $P^{-1}=\overline{P}^\mathsf{T}$, the conjugate transpose.

DEFINITION 5.3.14. *An* **unitary matrix** *is an $(n\times n)$-matrix P with complex entries such that $\overline{P}^\mathsf{T}P=I_n$. In other words, a unitary matrix is a square matrix P with complex entries such that $P^{-1}=\overline{P}^\mathsf{T}$.*

EXERCISE 78. Show that: the condition that $\overline{P}^\mathsf{T}P=I_n$ is equivalent to the columns of P forming an orthonormal basis for $\mathbb{C}^n$ with its standard inner product.

EXERCISE 79. Show that: the set $\{P\in\mathsf{Mat}(n;\mathbb{C}):\overline{P}^\mathsf{T}P=I_n\}$ is a group. It is called the **unitary group**, $U(n)$.

COROLLARY 5.3.15 (The Spectral Theorem for Hermitian Matrices). *Let A be a $(n\times n)$-hermitian matrix. Then there is an $(n\times n)$-unitary matrix P such that*

$$\overline{P}^\mathsf{T}AP=P^{-1}AP=\operatorname{diag}(\lambda_1,\ldots,\lambda_n)$$

where $\lambda_1,\ldots,\lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of the characteristic polynomial of A.

PROOF. This follows from combining the Spectral Theorem applied to $\mathbb{C}^n$ with its standard inner product with Exercise 78. □

REMARK 5.3.16. (1) Orthogonal and unitary groups are some of the most important groups in mathematics. They are the cornerstones Introduction to Lie Groups and their properties determine the shape of that topic. You already know many examples of orthogonal matrices: those representing reflections and rotations in $\mathbb{R}^n$ with respect to the standard basis. The orthogonal matrices, together with "translations" $\tau_{\vec{w}}:\vec{x}\mapsto\vec{x}+\vec{w}$ determine the group that defines Euclidean geometry from the point of view of Klein's "Erlangen

Program". I'd love to tell you more, but it's really the topic for a different course in geometry.

(2) Given a real symmetric matrix $A = (a_{ij}) \in \mathsf{Mat}(n; \mathbb{R})$, I can define the following **quadratic form** on $\mathbb{R}^n$, using the standard inner product:

$$\vec{v} \mapsto Q(\vec{v}) = (A\vec{v}, \vec{v})$$

You already saw an $n = 2$ case of this Remark 5.3.8. Such quadratic forms appear throughout the mathematics, and are particularly important in Algebraic Topology, Differentiable Manifolds and General Relativity amongst other subjects. A simple consequence of the Spectral Theorem is Sylvester's Law of Inertia which states that you can make a change of basis in $\mathbb{R}^n$, sending $\vec{v}$ to $\vec{x}$, so that the quadratic form looks like:

$$Q(\vec{v}) = \sum_{i=1}^{n} a_i x_i^2$$

where each $a_i \in \{-1, 0, 1\}$ and such that the numbers of 1's, 0's and -1's is independent of the change of basis. For $n = 2$ this produces the tetraptych of ellipses, hyperbolae, parabolae and straight lines that you may have met before.

(3) There is one final topic related to orthogonal projection that it would have been good to go into detail about: nearest point to a subspace and the least squares approximation. Schade in German, dommage in French, but in any case a pity!

CHAPTER 6

Jordan Normal Form

6.1. Motivation

Differential Equations If you are taking the course Honours Differential Equations you have seen the exponential mapping for complex square matrices. It is defined by the series:

$$\begin{aligned} \exp : \mathsf{Mat}(n;\mathbb{C}) &\to \mathsf{Mat}(n;\mathbb{C}) \\ A &\mapsto \sum_{k=0}^{\infty} \frac{1}{k!} A^k \end{aligned}$$

This mapping plays a central role in describing the solutions to linear differential equations with constant coefficients. More precisely, if $A \in \mathsf{Mat}(n;\mathbb{C})$ is a square matrix and $\vec{c} \in \mathbb{C}^n$ a column vector, then there exists exactly one differentiable mapping $\gamma : \mathbb{R} \to \mathbb{C}^n$ with initial value $\gamma(0) = \vec{c}$ and which satisfies $\dot{\gamma}(t) = A\gamma(t)$ for all $t \in \mathbb{R}$: it is the mapping

$$\gamma(t) = \exp(tA)\vec{c}$$

This fact is motivation to get the best possible understanding of $\exp(A)$.

The formula $\exp(PAP^{-1}) = P(\exp(A))P^{-1}$ for invertible P follows straight from the definition of $\exp$. Another elementary property is that the formula $\exp(A+B) = \exp(A)\exp(B)$ holds for square matrices A and B that commute. This is not hard to check formally:

$$\begin{aligned} \exp(A+B) &= \sum_{k=0}^{\infty} \frac{1}{k!}(A+B)^k \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{i+j=k} \frac{k!}{i!j!} A^i B^j \\ &= \sum_{k=0}^{\infty} \sum_{i+j=k} \frac{1}{i!} A^i \frac{1}{j!} B^j \\ &= \exp(A)\exp(B) \end{aligned}$$

In Theorem 6.2.2 I will prove the Jordan Normal Form Theorem, which has as part of its proof the consequence that each complex square matrix can be decomposed uniquely as a sum $A = D + N$ with D diagonalisable and N nilpotent and $DN = ND$. In particular this means that there exists an invertible matrix P with $PDP^{-1} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. It then follows from the observations I made in the previous paragraph that:

$$\begin{aligned} \exp(A) &= \exp(D)\exp(N) \\ &= P^{-1}\exp(\mathrm{diag}(\lambda_1, \ldots, \lambda_n))P\exp N \\ &= P^{-1}\mathrm{diag}(e^{\lambda_1}, \ldots, e^{\lambda_n})P\exp(N) \end{aligned}$$

and

$$\exp(tA) = P^{-1}\mathrm{diag}(e^{t\lambda_1}, \ldots, e^{t\lambda_n})P\exp(tN)$$

That only leaves the expansion for $\exp(tN)$, which turns out to be something that can be worked with. Thus the Jordan Normal Form plus a little more calculation – of the sort that you meet in Honours Differential Equations – produces a very explicit solution of the differential equation $\dot{\gamma}(t) = A\gamma(t)$.

Algebra This is supposed to be an Algebra Course, so I will also mention explicitly the natural motivation that follows from the material in Chapter 2. Given a finite dimensional vector space V and an endomorphism $f : V \to V$, a choice of an ordered basis $\mathcal{B}$ for V determines a matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}}$ representing f with respect to $\mathcal{B}$. Another choice produces another matrix, but it will be conjugate to ${}_{\mathcal{B}}[f]_{\mathcal{B}}$. So this fact is motivation to find an ordered basis that simplifies the representing matrix as much as possible, or equivalently to find the simplest possible matrix that is conjugate to a given matrix. This is exactly what the Jordan Normal Form does! It is actually a special case of the Structure Theorem for Finitely Generated Modules over a Principal Ideal Domain. This is a lovely classification theorem that, amongst other things, unites a description of all finite abelian groups with a description of square matrices up to conjugacy. Examples of Principal Ideal Domains are the rings $\mathbb{Z}$ and $F[X]$: $\mathbb{Z}$-modules are abelian groups; typically $F[X]$-modules have the form described in Exercise 56.

REMARK 6.1.1. You should compare the Jordan Normal Form with the Smith Normal Form. The Smith Normal Form looks far simpler: the reason for this is that it finds the simplest possible matrix ${}_{\mathcal{A}}[f]_{\mathcal{B}}$ where $\mathcal{A}$ and $\mathcal{B}$ are ordered bases of V which may or may not be equal, whereas the Jordan Normal Form allows only for the case $\mathcal{A} = \mathcal{B}$.

6.2. Statement of the Jordan Normal Form and Strategy of Proof

From now on F will be an algebraically closed field, such as the field of complex numbers $F = \mathbb{C}$. Since I shall be discussing eigenvalues and eigenvectors for arbitrary matrices with entries in F, this is crucial!

Since F is algebraically closed every polynomial $F[x]$ splits as a product of linear factors. It follows from the Triangularisability Proposition 4.6.1 that every endomorphism $f : V \to V$ of an n-dimensional F-vector space is triangularisable, i.e. there exists a basis $(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)$ such that

$$\begin{aligned} f(\vec{v}_1) &= a_{11}\vec{v}_1 \,, \\ f(\vec{v}_2) &= a_{12}\vec{v}_1 + a_{22}\vec{v}_2 \,, \\ &\vdots \\ f(\vec{v}_n) &= a_{1n}\vec{v}_1 + a_{2n}\vec{v}_2 + \cdots + a_{nn}\vec{v}_n \in V \end{aligned}$$

with $\chi_f(x) = (a_{11} - x)(a_{22} - x)\ldots(a_{nn} - x) \in F[x]$. Roughly speaking, the Jordan Normal Form improves this by providing such a basis for V with the additional property that

$$a_{ij} = \begin{cases} 0 \text{ or } 1 & \text{if } i = j - 1 \\ 0 & \text{if } i < j - 1 \end{cases}$$

so that

$$\begin{aligned} f(\vec{v}_1) &= a_{11}\vec{v}_1 \,, \\ f(\vec{v}_2) &= a_{12}\vec{v}_1 + a_{22}\vec{v}_2 \,, \\ &\vdots \\ f(\vec{v}_n) &= a_{n-1n}\vec{v}_{n-1} + a_{nn}\vec{v}_n \in V \end{aligned}$$

DEFINITION 6.2.1. *Given an integer $r \geqslant 1$ define an $(r \times r)$-matrix $J(r)$, called the* **nilpotent Jordan block of size** r*, by the rule $J(r)_{ij} = 1$ for $j = i + 1$ and $J(r)_{ij} = 0$ otherwise.*

$$J(r) \;=\; \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} .$$

In particular $J(1)$ is (1×1)-matrix whose only entry is zero.

Given an integer $r \geqslant 1$ and a scalar $\lambda \in F$ define an $(r \times r)$-matrix $J(r, \lambda)$, called the **Jordan block of size** r **and eigenvalue** λ*, by the rule*

$$J(r, \lambda) \;=\; \lambda I_r + J(r) \;=\; D + N$$

with $\lambda I_r = \mathrm{diag}(\lambda, \lambda, \ldots, \lambda) = D$ diagonal and $J(r) = N$ nilpotent

$$J(r, \lambda) \;=\; \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

such that $DN = ND$.

If V is an r-dimensional F-vector space with basis $\mathcal{B} = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_r)$ and $\lambda \in F$ is a scalar, the endomorphism $f : V \to V$ defined by

$$\begin{aligned} f(\vec{v}_1) \;&=\; \lambda \vec{v}_1 \,, \\ f(\vec{v}_2) \;&=\; \vec{v}_1 + \lambda \vec{v}_2 \,, \\ &\vdots \\ f(\vec{v}_r) \;&=\; \vec{v}_{r-1} + \lambda \vec{v}_r \in V \end{aligned}$$

has matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}} = J(r, \lambda)$. The endomorphism

$$e \;=\; f - \lambda \,\mathrm{id}_V \;:\; V \to V \,;\; \vec{v} \mapsto f(\vec{v}) - \lambda \vec{v} \,,\; e(\vec{v}_i) \;=\; \vec{v}_{i-1}$$

has nilpotent matrix ${}_{\mathcal{B}}[e]_{\mathcal{B}} = J(r)$. The characteristic polynomial of f is $\chi_f(x) = (\lambda - x)^r \in F[x]$. It is significant that $e^r = 0$ (Cayley-Hamilton!) but $e^j \neq 0$ for $j = 1, 2, \ldots, r - 1$, with

$$V_j \;=\; \ker(e^j) = \langle \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_j \rangle \subseteq V \;(1 \leqslant j \leqslant r)$$

a j-dimensional subspace such that $f(V_j) \subseteq V_j$. In particular, the λ-eigenspace $E(\lambda, f) = V_1 = \langle \vec{v}_1 \rangle$ is 1-dimensional.

Here is the algebraic apex of the course.

THEOREM 6.2.2 (Jordan Normal Form). *Let F be an algebraically closed field. Let V be a finite dimensional vector space and let $\phi : V \to V$ be an endomorphism of V with characteristic polynomial*

$$\chi_\phi(x) \;=\; (\lambda_1 - x)^{a_1} (\lambda_2 - x)^{a_2} \ldots (\lambda_s - x)^{a_s} \in F[x] \;(a_i \geqslant 1, \sum_{i=1}^{s} a_i = n)$$

for distinct $\lambda_1, \lambda_2, \ldots, \lambda_s \in F$. Then there exists an ordered basis $\mathcal{B}$ of V such that the matrix of ϕ with respect to the basis $\mathcal{B}$ is block diagonal with Jordan blocks on the diagonal

$$_{\mathcal{B}}[\phi]_{\mathcal{B}} = \operatorname{diag}(J(r_{11}, \lambda_1), \ldots, J(r_{1m_1}, \lambda_1), J(r_{21}, \lambda_2), \ldots, J(r_{sm_s}, \lambda_s))$$

with $r_{11}, \ldots, r_{1m_1}, r_{21}, \ldots, r_{sm_s} \geqslant 1$ such that

$$a_i \;=\; r_{i1} + r_{i2} + \cdots + r_{im_i} \; (1 \leqslant i \leqslant s) \; .$$

This is a complicated theorem to prove. It involves quite a lot of abstract calculation and it is *very* algebraic. To help to make it easier to follow, I outline here the strategy of the proof. In the next section I give the proof and in the section after that I illustrate the proof with an example that involves everything that was used.

Step 1: The first step is to decompose the vector space V into a direct sum $V = \oplus_{i=1}^{s} V_i$ according to the factorization of the characteristic polynomial as a product of linear factors

$$\chi_\phi(x) \;=\; (\lambda_1 - x)^{a_1}(\lambda_2 - x)^{a_2} \ldots (\lambda_s - x)^{a_s} \in F[x]$$

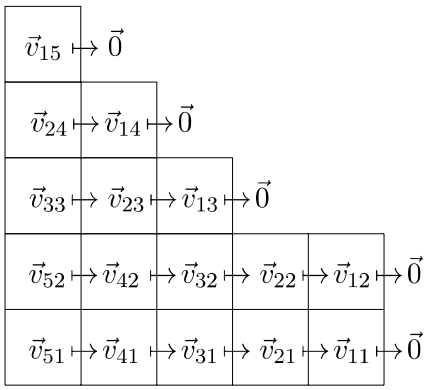
for distinct scalars $\lambda_1, \lambda_2, \ldots, \lambda_s \in F$, where for each i:

- $V_i = \ker((\phi - \lambda_i \operatorname{id}_V)^{a_i} : V \to V) \subseteq V$, and
- $\phi(V_i) \subseteq V_i$, and
- $(\phi - \lambda_i \operatorname{id}_{V_i})^{m_i}$ is zero on V_i for m_i large enough.

This behaviour is an example of a general phenomenon from module theory called the Krull-Remak-Schmidt Decomposition.

Step 2: The outcome of the first step is to focus attention on the individual spaces V_i instead of V. These spaces have the advantage that a power of the endomorphism $(\phi - \lambda_i \operatorname{id}_{V_i}) : V_i \to V_i$ is zero. In other words $\psi := \phi - \lambda_i \operatorname{id}_{V_i}$ is a nilpotent linear mapping on V_i. I already showed you this situation in Exercise 32. The proof will study a finite dimensional vector space W together with a nilpotent endomorphism $\psi : W \to W$. I will show that there is an ordered basis of W, written $\{\vec{v}_{11}, \vec{v}_{21}, \vec{v}_{31}, \ldots, \vec{v}_{12}, \vec{v}_{22}, \vec{v}_{32}, \ldots\}$ such that the matrix of ψ with respect to this basis is block diagonal with nilpotent Jordan blocks of various sizes along the diagonal.

In my head, I picture such a basis together with ψ as follows:



This picture would describe an example where $\dim W = 16$ because each of the 16 boxes represents one basis vector; the mapping ψ moves from left to right through the boxes, vanishing when it reaches the outer edge of the diagram. In the example the matrix would have the form $\operatorname{diag}(J(5), J(5), J(3), J(2), J(1))$. The vector space W has ordered basis (partitioned to match the Jordan blocks)

$$\begin{aligned} \mathcal{B} \;&=\; \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3 \cup \mathcal{B}_4 \cup \mathcal{B}_5 \\ &=\; (\vec{v}_{11}, \vec{v}_{21}, \vec{v}_{31}, \vec{v}_{41}, \vec{v}_{51}) \cup (\vec{v}_{12}, \vec{v}_{22}, \vec{v}_{32}, \vec{v}_{42}, \vec{v}_{52}) \cup (\vec{v}_{13}, \vec{v}_{23}, \vec{v}_{33}) \cup (\vec{v}_{13}, \vec{v}_{23}) \cup (\vec{v}_{15}) \end{aligned}$$

and $\psi : W \to W$ is given by

$$\begin{aligned}
\psi(\vec{v}_{11}) &= \vec{0}\,,\ \psi(\vec{v}_{21}) = \vec{v}_{11}\,,\ \psi(\vec{v}_{31}) = \vec{v}_{21}\,,\ \psi(\vec{v}_{41}) = \vec{v}_{31}\,,\ \psi(\vec{v}_{51}) = \vec{v}_{41}\,,\\
\psi(\vec{v}_{12}) &= \vec{0}\,,\ \psi(\vec{v}_{22}) = \vec{v}_{12}\,,\ \psi(\vec{v}_{32}) = \vec{v}_{22}\,,\ \psi(\vec{v}_{42}) = \vec{v}_{32}\,,\ \psi(\vec{v}_{52}) = \vec{v}_{42}\,,\\
\psi(\vec{v}_{13}) &= \vec{0}\,,\ \psi(\vec{v}_{23}) = \vec{v}_{13}\,,\ \psi(\vec{v}_{33}) = \vec{v}_{21}\,,\\
\psi(\vec{v}_{14}) &= \vec{0}\,,\ \psi(\vec{v}_{24}) = \vec{v}_{14}\,,\\
\psi(\vec{v}_{15}) &= \vec{0}\,.
\end{aligned}$$

Define an increasing sequence of subspaces

$$W_0 = \{0\} \subset W_1 \subset W_2 \subset W_3 \subset W_4 \subset W_5 = W$$

with

$$W_k = \ker(\psi^k : W \to W) = \{\vec{w} \in W \,|\, \psi^k(\vec{w}) = \vec{0}\}\,.$$

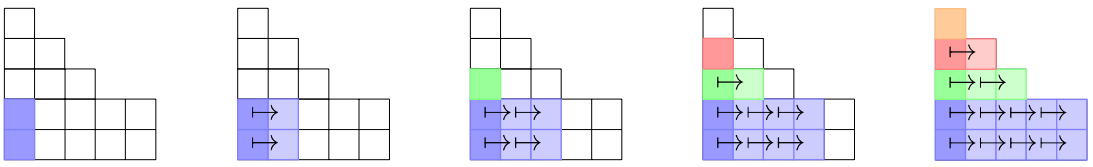
the kernel of the k-fold iteration of ψ

$$\psi^k = \psi \circ \psi \circ \cdots \circ \psi \ : \ W \to W\,.$$

Thus W_k is spanned by the basis elements $\vec{v}_{ij} \in \mathcal{B}$ with $\psi^k(\vec{v}_{ij}) = \vec{0} \in W$, and

$$\begin{aligned}
W_1 &= \langle \vec{v}_{11}, \vec{v}_{12}, \vec{v}_{13}, \vec{v}_{14}, \vec{v}_{15} \rangle\,,\\
W_2 &= \langle \vec{v}_{24}, \vec{v}_{23}, \vec{v}_{22}, \vec{v}_{21} \rangle \oplus W_1\,,\\
W_3 &= \langle \vec{v}_{33}, \vec{v}_{32}, \vec{v}_{31} \rangle \oplus W_2\,,\\
W_4 &= \langle \vec{v}_{42}, \vec{v}_{41} \rangle \oplus W_3\,,\\
W_5 &= \langle \vec{v}_{52}, \vec{v}_{51} \rangle \oplus W_4\,.
\end{aligned}$$

The subspaces are most easily illustrated by the coloured sequence of boxes in the diagram:



The first diagram on the left has W_4 in white, the next one has W_3 in white, the next one W_2, the next W_1, and the final one $\{0\}$. The coloured boxes produce a basis for the quotient vector spaces

$$\begin{aligned}
W/W_4 &= \langle W_4 + \vec{v}_{52}, W_4 + \vec{v}_{51} \rangle\,,\\
W/W_3 &= \langle W_3 + \vec{v}_{52}, W_3 + \vec{v}_{51}, W_3 + \vec{v}_{41}, W_3 + \vec{v}_{42} \rangle\,,\\
W/W_2 &= \langle W_2 + \vec{v}_{52}, W_2 + \vec{v}_{51}, W_2 + \vec{v}_{41}, W_2 + \vec{v}_{42}, W_2 + \vec{v}_{33}, W_2 + \vec{v}_{32}, W_2 + \vec{v}_{31} \rangle\,,\\
W/W_1 &= \langle W_1 + \vec{v}_{52}, W_1 + \vec{v}_{51}, W_1 + \vec{v}_{41}, W_1 + \vec{v}_{42}, W_1 + \vec{v}_{33}, W_1 + \vec{v}_{32}, W_1 + \vec{v}_{31},\\
&\qquad W_1 + \vec{v}_{24}, W_1 + \vec{v}_{23}, W_1 + \vec{v}_{22}, W_1 + \vec{v}_{21} \rangle\,.
\end{aligned}$$

The more darkly coloured boxes (all on the left column) are "generators" from which all other basis vectors (more lightly coloured with the same colour) are produced using the mapping ψ.

Step 3: Put Step 1 and Step 2 together.

6.3. OK, let's go! The proof of Jordan Normal Form

Step 1: Let $\phi : V \to V$ be an endomorphism of the finite dimensional F-vector space V. Since F is algebraically closed, the characteristic polynomial $\chi_\phi(x)$ decomposes into linear factors by Theorem 3.3.14. I write it as follows

$$\chi_\phi(x) = (-1)^n \prod_{i=1}^{s} (x - \lambda_i)^{a_i} \in F[x]$$

where each a_i is a positive integer, $\lambda_i \neq \lambda_j$ for $i \neq j$, and the λ_i are the eigenvalues of ϕ. For $1 \leqslant j \leqslant s$ define

$$P_j(x) = \prod_{\substack{i=1 \\ i \neq j}}^{s} (x - \lambda_i)^{a_i}$$

LEMMA 6.3.1. *There exists polynomials $Q_j(x) \in F[x]$ such that*

$$\sum_{j=1}^{s} P_j(x) Q_j(x) = 1.$$

PROOF. This is an application of the extended Euclidean algorithm for $F[x]$, based on Theorem 3.3.4. This algorithm computes the highest common factor of a set of polynomials in terms of the polynomials themselves and some subsidiary polynomials $Q_j(x)$:

$$\sum_{j=1}^{s} P_j(x) Q_j(x) = \text{h.c.f.}\{P_1(x), \ldots, P_s(x)\}$$

Since the highest common factor of the set of polynomials $\{P_1(x), P_2(x), \ldots, P_s(x)\}$ is 1, the lemma follows. □

The extended Euclidean algorithm for $F[x]$ works in exactly the same way as for $\mathbb{Z}$, but using Theorem 3.3.4 here, the division algorithm for polynomials with coefficients in the field F.

DEFINITION 6.3.2. *The* **generalized eigenspace** *of ϕ with eigenvalue λ_i, $E^{\text{gen}}(\lambda_i, \phi)$, is the following subspace of V*

$$E^{\text{gen}}(\lambda_i, \phi) = \{\vec{v} \in V \mid (\phi - \lambda_i \,\mathrm{id}_V)^{a_i}(\vec{v}) = \vec{0}\}$$

The dimension of $E^{\text{gen}}(\lambda_i, \phi)$ is called the **algebraic multiplicity of ϕ with eigenvalue** *λ_i while the dimension of the eigenspace $E(\lambda_i, \phi)$ is called the* **geometric multiplicity of ϕ with eigenvalue** *λ_i.*

REMARK 6.3.3. The actual eigenspace is defined by

$$E(\lambda_i, \phi) \;=\; \{\vec{v} \in V \mid (\phi - \lambda_i \,\mathrm{id}_V)(\vec{v}) = \vec{0}\}\,.$$

It is immediate that $E(\lambda_i, \phi) \subseteq E^{\text{gen}}(\lambda_i, \phi)$. In particular the algebraic multiplicity of any eigenvalue must always be greater than or equal to the corresponding geometric multiplicity.

DEFINITION 6.3.4. *Let $f : X \to X$ be a mapping from a set X to itself. A subset $Y \subseteq X$ is* **stable under** *f precisely when $f(Y) \subseteq Y$, that is if $y \in Y$ then $f(y) \in Y$.*

PROPOSITION 6.3.5 (The direct sum decomposition). *For each $1 \leqslant i \leqslant s$, let*

$$\mathcal{B}_i \;=\; \{\vec{v}_{ij} \in V \mid 1 \leqslant j \leqslant a_i\}$$

be a basis of $E^{\text{gen}}(\lambda_i, \phi)$, where a_i is the algebraic multiplicity of ϕ with eigenvalue λ_i, such that $\sum_{i=1}^{s} a_i = n$ is the dimension of V.

(1) *Each* $E^{\mathsf{gen}}(\lambda_i, \phi)$ *is stable under* ϕ.

(2) *For each* $\vec{v} \in V$ *there exist unique* $\vec{v}_i \in E^{\mathsf{gen}}(\lambda_i, \phi)$ *such that* $\vec{v} = \sum_{i=1}^{s} \vec{v}_i$. *In other words, there is a direct sum decomposition*

$$V \;=\; \bigoplus_{i=1}^{s} E^{\mathsf{gen}}(\lambda_i, \phi)$$

with ϕ *restricting to endomorphismsof the summands*

$$\phi_i \;=\; \phi| \;:\; E^{\mathsf{gen}}(\lambda_i, \phi) \to E^{\mathsf{gen}}(\lambda_i, \phi)\;.$$

(3) *Then*

$$\mathcal{B} \;=\; \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_s \;=\; \{\vec{v}_{ij} \,|\, 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant a_i\}$$

is a basis of V. *The matrix of the endomorphism* ϕ *with respect to this basis is given by the block diagonal matrix*

$${}_{\mathcal{B}}[\phi]_{\mathcal{B}} \;=\; \left(\begin{array}{c|c|c|c} B_1 & 0 & 0 & 0 \\ \hline 0 & B_2 & 0 & 0 \\ \hline 0 & 0 & \ddots & 0 \\ \hline 0 & 0 & 0 & B_s \end{array}\right) \in \mathsf{Mat}(n; F)$$

with $B_i =_{\mathcal{B}_i} [\phi_i]_{\mathcal{B}_i} \in \mathsf{Mat}(a_i; F)$.

PROOF. (1) Let $\vec{v} \in E^{\mathsf{gen}}(\lambda_i, \phi)$ so that $(\phi - \lambda_i \,\mathrm{id}_V)^{a_i}(\vec{v}) = \vec{0}$. Then

$$\phi(\phi - \lambda_i \,\mathrm{id}_V) \;=\; \phi^2 - \lambda_i \phi \;=\; (\phi - \lambda_i \,\mathrm{id}_V)\phi \;:\; V \to V\;,$$

so I deduce that for all $\vec{v} \in E^{\mathsf{gen}}(\lambda_i, \phi)$

$$(\phi - \lambda_i \,\mathrm{id}_V)^{a_i} \phi(\vec{v}) \;=\; \phi(\phi - \lambda_i \,\mathrm{id}_V)^{a_i}(\vec{v}) \;=\; \phi(\vec{0}) \;=\; \vec{0} \in V\;.$$

This shows that $\phi(\vec{v}) \in E^{\mathsf{gen}}(\lambda_i, \phi)$ so that $E^{\mathsf{gen}}(\lambda_i, \phi)$ is indeed stable under ϕ.

(2) By Lemma 6.3.1 I have $1 = \sum_{j=1}^{s} P_j(x) Q_j(x)$ and so evaluating this at the endomorphism ϕ gives

$$\mathrm{id}_V = \sum_{j=1}^{s} P_j(\phi) \circ Q_j(\phi) \tag{16}$$

Therefore, for all $\vec{v} \in V$ I have

$$\vec{v} = \sum_{j=1}^{s} P_j(\phi) \circ Q_j(\phi)(\vec{v})$$

Now I observe that

$$(\phi - \lambda_j \,\mathrm{id}_V)^{a_j} \circ P_j(\phi) \circ Q_j(\phi)(\vec{v}) = \chi_\phi(\phi) \circ Q_j(\phi)(\vec{v}) = 0(\vec{v}) = \vec{0}$$

where I used the Cayley-Hamilton Theorem for the second equality. Setting

$$\vec{v}_j \;:=\; P_j(\phi) \circ Q_j(\phi)(\vec{v}) \in E^{\mathsf{gen}}(\lambda_j, \phi)$$

we have

$$\vec{v} \;=\; \sum_{j=1}^{s} \vec{v}_j\;,$$

demonstrating that $V = \sum_{j=1}^{s} E^{\mathsf{gen}}(\lambda_j, \phi)$.

It remains to check uniqueness in this decomposition. So suppose that $\sum_{j=1}^s \vec{v}_i = \sum_{i=1}^s \vec{w}_i$ with $\vec{v}_i, \vec{w}_i \in E^{\mathsf{gen}}(\lambda_i, \phi)$ for each i. This means that $\sum_{i=1}^s (\vec{v}_i - \vec{w}_i) = \vec{0}$. Given any $\vec{x}_j \in E^{\mathsf{gen}}(\lambda_j, \phi)$ I have for $k \neq j$

$$P_k(\phi)(\vec{x}_j) = \prod_{\substack{\ell=1 \\ \ell \neq k}}^{s} (\phi - \lambda_\ell \operatorname{id}_V)^{a_\ell}(\vec{x}_j) = \vec{0}$$

since $(\phi - \lambda_j \operatorname{id}_V)^{a_j}(\vec{x}_j) = \vec{0}$ and $(\phi - \lambda_j \operatorname{id}_V)^{a_j}$ is a factor of $P_k(\phi)$. So, on applying (16), I find

$$\vec{x}_j = \sum_{k=1}^{s} P_k(\phi) \circ Q_k(\phi)(\vec{x}_j) = P_j(\phi) \circ Q_j(\phi)(\vec{x}_j)$$

I apply this to the equality $\sum_{i=1}^s (\vec{v}_i - \vec{w}_i) = \vec{0}$. For each j this gives

$$\vec{0} = P_j(\phi)Q_j(\phi)\left(\sum_{i=1}^{s}(\vec{v}_i - \vec{w}_i)\right) = \sum_{i=1}^{s} P_j(\phi)Q_j(\phi)(\vec{v}_i - \vec{w}_i) = \vec{v}_j - \vec{w}_j.$$

It follows that $\vec{v}_j = \vec{w}_j$ for each j, as required.

(3) Since the set $\{\vec{v}_{ij} : 1 \leqslant j \leqslant a_i\}$ is a basis of $E^{\mathsf{gen}}(\lambda_i, \phi)$ for each i, it should be clear to you that the union of these bases is a basis of $\oplus_{i=1}^s E^{\mathsf{gen}}(\lambda_i, \phi)$. If you're not sure, it is proved in the solution to Exercise 6. Since $V = \oplus_{i=1}^s E^{\mathsf{gen}}(\lambda_i, \phi)$ by Part (2), that deals with the basis $\mathcal{B}$ of V. What is the matrix with the respect to this basis? (I really need to take an ordered basis: I will take $\vec{v}_{11}, \vec{v}_{12}, \ldots, \vec{v}_{1n_1}, \vec{v}_{21}, \ldots, \vec{v}_{2n_2}, \ldots, \vec{v}_{sn_s}$ as the ordering.) If I calculate the matrix ${}_{\mathcal{B}}[\phi]_{\mathcal{B}}$ by the usual method of Theorem 2.3.1, I see that since $\phi(\vec{v}_{ij}) \in E^{\mathsf{gen}}(\lambda_i, \phi)$ by Part (1), $\phi(\vec{v}_{ij})$ can be expressed as a linear combination of the vectors $\vec{v}_{ij}$ where $1 \leqslant j \leqslant a_i$. Therefore the matrix is block diagonal with the i-th block having size $(a_i \times a_i)$. □

That completes the first step of the strategy. Each matrix B_i appearing in Part (3) of the Theorem 6.3.5 represents the restriction of ϕ to $E^{\mathsf{gen}}(\lambda_i, \phi)$. This endomorphism of $E^{\mathsf{gen}}(\lambda_i, \phi)$ is special because it has the property that a power of $\phi - \lambda_i \operatorname{id}_{E^{\mathsf{gen}}(\lambda_i,\phi)}$ is zero.

EXERCISE 80. Using Proposition 6.3.5 show that:

(1) each matrix $A \in \mathsf{Mat}(n; F)$ can be written as $A = D + N$ where D is a diagonalisable matrix and N is a nilpotent matrix and $DN = ND$;
(2) the decomposition $A = D + N$ is unique.

This decomposition is called the **Jordan decomposition** of A; it plays a basic role in the theory of Lie algebras.

So now to the next step, studying nilpotent endomorphisms.

Step 2: Let W be a finite dimensional vector space and $\psi : W \to W$ an endomorphism such that some power of ψ is zero, that is $\psi^m = 0$ for some m. This should remind you of Exercise 32 which was also Homework 3, Exercise 6.

I will fix m to be minimal: $\psi^m = 0$ but $\psi^{m-1} \neq 0$. For $0 \leqslant i \leqslant m$ define

$$W_i = \ker(\psi^i)$$

If $\vec{w} \in W_i$ then $\psi^{i+1}(\vec{w}) = \psi \circ \psi^i(\vec{w}) = \psi(\vec{0}) = \vec{0}$ so that $\vec{w} \in W_{i+1}$. It follows that $W_i \subseteq W_{i+1}$. Moreover, since $\psi^0 = \operatorname{id}_W$ and $\psi^m = 0$ I also see that $W_0 = 0$ and $W_m = W$. Therefore I get a chain of subspaces

$$0 = W_0 \subseteq W_1 \subseteq W_2 \subseteq \cdots \subseteq W_{m-1} \subseteq W_m = W$$

LEMMA 6.3.6. *For each i, define a linear mapping*

$$\psi_i : \frac{W_i}{W_{i-1}} \to \frac{W_{i-1}}{W_{i-2}}$$

by $\psi_i(\vec{w} + W_{i-1}) = \psi(\vec{w}) + W_{i-2}$ for $\vec{w} \in W_i$. Then ψ_i is well-defined and injective.

PROOF. Let $\vec{w}, \vec{w}' \in W_i$. First, $\psi(\vec{w}) \in W_{i-1}$ since $\psi^{i-1}(\psi(\vec{w})) = \psi^i(\vec{w}) = \vec{0}$. Second, I check that the mapping is well-defined. If $\vec{w} + W_{i-1} = \vec{w}' + W_{i-1}$ then $\vec{w} - \vec{w}' \in W_{i-1}$. Therefore $\psi^{i-1}(\vec{w} - \vec{w}') = \vec{0}$, and so $\vec{0} = \psi^{i-2} \circ \psi(\vec{w} - \vec{w}') = \psi^{i-2} \circ (\psi(\vec{w}) - \psi(\vec{w}'))$ Therefore, $\psi(\vec{w}) - \psi(\vec{w}') \in W_{i-2}$ so that $\psi(\vec{w}) + W_{i-2} = \psi(\vec{w}') + W_{i-2}$. This confirms that the mapping ψ_i is well-defined.

I now have to prove that ψ_i is injective. If $\psi_i(\vec{w} + W_{i-1}) = \vec{0} + W_{i-2}$ then $\psi(\vec{w}) \in W_{i-2}$ which means that $\vec{0} = \psi^{i-2}(\psi(\vec{w})) = \psi^{i-1}(\vec{w})$ so that $\vec{w} \in W_{i-1}$, or, in other words, that $\vec{w} + W_{i-1} = \vec{0} + W_{i-1}$. This proves that $\ker \psi_i$ is zero and hence that ψ_i is injective. □

This result shows me that if I define

$$d_i = \dim\left(\frac{W_i}{W_{i-1}}\right) \qquad 1 \leqslant i \leqslant m$$

then $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_m$. To refine this and help me to pick a good basis for W, I need a little technical lemma.

LEMMA 6.3.7. *Let $f : X \to Y$ be an injective linear mapping between the F-vector spaces X and Y. If $\{\vec{x}_1, \ldots, \vec{x}_t\}$ is a linearly independent set in X, then $\{f(\vec{x}_1), \ldots, f(\vec{x}_t)\}$ is a linearly independent set in Y.*

PROOF. As is usual for most of the proofs of linear independence in an abstract setting, you just need to sniff the air and then follow your nose. So let $\alpha_1, \ldots, \alpha_t \in F$ be scalars. Suppose that

$$\alpha_1 f(\vec{x}_1) + \cdots + \alpha_t f(\vec{x}_t) = \vec{0}_Y$$

Then the linearity of f allows me to rewrite this equation as

$$f(\alpha_1 \vec{x}_1 + \cdots + \alpha_t \vec{x}_t) = \vec{0}_Y$$

Since f is assumed to be injective, this means that $\alpha_1 \vec{x}_1 + \cdots + \alpha_t \vec{x}_t = \vec{0}_X$. As the set $\{\vec{x}_1, \ldots, \vec{x}_t\}$ are linearly independent, this implies that $\alpha_1 = \cdots = \alpha_t = 0$. Thus $\{f(\vec{x}_1), \ldots, f(\vec{x}_t)\}$ is a linearly independent set. □

I can now develop an algorithm to construct a basis of each W_i/W_{i-1}. The algorithm goes as follows:

- Choose an arbitrary basis for W_m/W_{m-1}, say
$$\{\vec{v}_{m,1} + W_{m-1}, \vec{v}_{m,2} + W_{m-1}, \ldots, \vec{v}_{m,d_m} + W_{m-1}\}\,.$$
- Since $\psi_m : W_m/W_{m-1} \to W_{m-1}/W_{m-2}$ is injective by Lemma 6.3.6, Lemma 6.3.7 proves that $\{\psi(\vec{v}_{m,1}) + W_{m-2}, \psi(\vec{v}_{m,2}) + W_{m-2}, \ldots, \psi(\vec{v}_{m,d_m}) + W_{m-2}\}$ is a linearly independent set in W_{m-1}/W_{m-2}. Set $\vec{v}_{m-1,i} = \psi(\vec{v}_{m,i})$ for $1 \leqslant i \leqslant d_m$.
- Choose vectors $\{\vec{v}_{m-1,i} : d_m + 1 \leqslant i \leqslant d_{m-1}\}$ so that $\{\vec{v}_{m-1,i} + W_{s-2} : 1 \leqslant i \leqslant d_{m-1}\}$ is a basis of W_{m-1}/W_{m-2}.
- Repeat!

Let me be explicit about what happens with a repetition. At the i-th stage you will have chosen vectors $\vec{v}_{j,k}$ for $m + 1 - i \leqslant j \leqslant m, 1 \leqslant k \leqslant d_j$, so that $\{\vec{v}_{j,k} + W_{j-1} : 1 \leqslant k \leqslant d_j\}$ is a basis of W_j/W_{j-1}. This bunch of vectors has the additional property that $\psi(\vec{v}_{j,k}) = \vec{v}_{j-1,k}$ for $m + 1 - i < j \leqslant m$. You'll then define $\vec{v}_{m-i,k} = \psi(\vec{v}_{m+1-i,k})$ for $1 \leqslant k \leqslant d_{m+1-i}$. By Lemma 6.3.6 and Lemma 6.3.7 $\{\vec{v}_{m-i,k} + W_{m-i-1} : 1 \leqslant j \leqslant d_{m+1-i}\}$ is a linearly independent set in W_{m-i}/W_{m-i-1}. You

now choose $\{\vec{v}_{m-i,k} : d_{m+1-i}+1 \leqslant k \leqslant d_{m-i}\}$ so that $\{\vec{v}_{m-i,k} + W_{m-i-1} : 1 \leqslant k \leqslant d_{m-i}\}$ is a basis of W_{m-i}/W_{m-i-1}.

You reach the end of the algorithm when you have completed the m-th stage: this produces a basis for $W_1/W_0 = W_1$. Since $W_1 = \ker(\psi)$ all elements of this basis have the property that $\psi(\vec{v}_{1,k}) = \vec{0}$.

LEMMA 6.3.8. *The set of elements $\{\vec{v}_{j,k} : 1 \leqslant j \leqslant m, 1 \leqslant k \leqslant d_j\}$ constructed in the algorithm above is a basis for W.*

PROOF. I check spanning first. I will show a finer statement:

$$\text{For } 1 \leqslant i \leqslant m, \text{ the set of elements } \{\vec{v}_{j,k} : 1 \leqslant j \leqslant i, 1 \leqslant k \leqslant d_j\} \text{ spans } W_i.$$

Of course, a statement like that is set up for a proof by induction. It holds for $i = 1$ because $\{\vec{v}_{1,k} : 1 \leqslant k \leqslant d_1\}$ was constructed as a basis for W_1, so in particular a spanning set.

Assume that the finer statement holds for a given i. Let $\vec{v} \in W_{i+1}$ be an arbitrary element. Since $\{\vec{v}_{i+1,k} + W_i : 1 \leqslant k \leqslant d_{i+1}\}$ is a basis for W_{i+1}/W_i, there exist $\alpha_1, \ldots, \alpha_{d_{i+1}} \in F$ such that

$$\vec{v} + W_i = \alpha_1 \vec{v}_{i+1,1} + \cdots + \alpha_{d_{i+1}} \vec{v}_{i+1,d_{i+1}} + W_i$$

It follows that

$$\vec{v} - \alpha_1 \vec{v}_{i+1,1} - \cdots - \alpha_{d_{i+1}} \vec{v}_{i+1,d_{i+1}} \in W_i$$

By induction this element can be expressed as a linear combination of vectors from the set $\{\vec{v}_{j,k} : 1 \leqslant j \leqslant i, 1 \leqslant k \leqslant d_j\}$, and so $\vec{v}$ can be expressed as a linear combination of element of $\{\vec{v}_{j,k} : 1 \leqslant j \leqslant i+1, 1 \leqslant k \leqslant d_j\}$. This confirms the finer statement for $i+1$ and hence completes the induction.

Now I know that the set $\{\vec{v}_{j,k} : 1 \leqslant j \leqslant m, 1 \leqslant k \leqslant d_j\}$ spans $W = W_m$ and that it contains $\sum_{j=1}^m d_j$ elements. I'll now explain why $\dim W = \sum_{j=1}^m d_j$. With that fact in my pocket I can apply the Cardinality Criterion for Bases, Part (2) to deduce that the set is a basis.

To calculate $\dim(W)$ I use repeatedly the general formula of Exercise 58: if M is an F-vector space and N a subspace of M then $\dim(M/N) = \dim(M) - \dim(N)$. This gives:

$$\begin{aligned}
\dim(W) = \dim(W_m) &= \dim(W_m/W_{m-1}) + \dim(W_{m-1}) \\
&= \dim(W_m/W_{m-1}) + \dim(W_{m-1}/W_{m-2}) + \dim(W_{m-2}) \\
&\vdots \\
&= \dim(W_m/W_{m-1}) + \dim(W_{m-1}/W_{m-2}) + \cdots + \dim(W_1/W_0) \\
&= \sum_{j=1}^m d_j.
\end{aligned}$$

□

This lemma gives me a basis of W which I will order via the ordering on subscripts $(j,k) < (j',k')$ if and only if $k < k'$ or $k = k'$ and $j < j'$. So for instance $(3,2) < (1,3)$ and $(1,3) < (2,3)$ so that $\vec{v}_{1,3}$ would appear in the list after $\vec{v}_{3,2}$ but before $\vec{v}_{2,3}$.

PROPOSITION 6.3.9. *Let $\mathcal{B}$ be the ordered basis of W constructed above $(\vec{v}_{jk} : 1 \leqslant j \leqslant m, 1 \leqslant k \leqslant d_j)$. Then*

$$_{\mathcal{B}}[\psi]_{\mathcal{B}} = \operatorname{diag}(\underbrace{J(m), \ldots, J(m)}_{d_m \text{ times}}, \underbrace{J(m-1), \ldots, J(m-1)}_{d_{m-1}-d_m \text{ times}}, \ldots, \underbrace{J(1), \ldots, J(1)}_{d_1-d_2 \text{ times}})$$

where $J(r)$ denotes the nilpotent Jordan block of size r.

PROOF. It follows from the explicit construction of the basis $\mathcal{B}$ that

$$\psi(\vec{v}_{i,j}) = \begin{cases} \vec{v}_{i-1,j} & \text{if } i > 1 \\ 0 & \text{otherwise} \end{cases}$$

This tells me that the entries of the (i,j)-th column of the matrix ${}_{\mathcal{B}}[\psi]_{\mathcal{B}}$ are all zero if $i = 1$ and otherwise are zero everywhere except for a 1 in the $(i-1,j)$-th row. This is the property that defines the nilpotent Jordan blocks, so I get the description I claimed. □

This completes Step 2 of the proof: for all nilpotent endomorphisms there exists a basis such that the representing matrix can be written as a block diagonal matrix with nilpotent Jordan blocks along the diagonal.

EXERCISE 81. Let $\psi : V \to V$ be a nilpotent endomorphism. Show that: the Jordan Normal Form of ψ is unique up to re-ordering of the nilpotent Jordan blocks. Explicitly, if $\mathcal{A}$ and $\mathcal{B}$ are bases of V such that

$${}_{\mathcal{A}}[\psi]_{\mathcal{A}} = \operatorname{diag}(J(a_1), \ldots, J(a_s)) \text{ and } {}_{\mathcal{B}}[\psi]_{\mathcal{B}} = \operatorname{diag}(J(b_1), \ldots, J(b_{s'}))$$

for some positive integers $a_1, \ldots, a_s$ and $b_1, \ldots b_{s'}$, then the multisets $\{a_1, \ldots, a_s\}$ and $\{b_1, \ldots, b_{s'}\}$ are equal.

Step 3: I now apply the outcome of Step 2 to each of the endomorphisms $(\phi - \lambda_i \operatorname{id}_V)$ restricted to $E^{\mathsf{gen}}(\lambda_i, \phi)$. This means each such endomorphism can be written as a block diagonal matrix of the form stated in Proposition 6.3.9 for a suitable choice of basis. The endomorphism $\lambda_i \operatorname{id}_V$ restricted to $E^{\mathsf{gen}}(\lambda_i, \phi)$ is of course $\lambda_i \operatorname{id}_{E^{\mathsf{gen}}(\lambda_i,\phi)}$ and so its matrix with respect to the chosen basis is just $\lambda_i I_{a_i}$. Therefore the matrix for $\phi = \lambda_i \operatorname{id}_V + (\phi - \lambda_i \operatorname{id}_V)$ is just $\lambda_i I_n$ plus the block diagonal matrix found above from Proposition 6.3.9. In other words it is a block diagonal matrix of the form stated in Proposition 6.3.9 where I replace each $J(r)$ that appears with $J(r, \lambda_i)$. This means that each matrix $B_i \in \mathsf{Mat}(a_i; F)$ appearing in Proposition 6.3.5 has exactly the form that I'm looking for in the statement of the Jordan Normal Form.

EXERCISE 82. Let $\psi : V \to V$ be an endomorphism. Show that: the Jordan Normal Form of ψ is unique up to re-ordering of the Jordan blocks. Explicitly, if $\mathcal{A}$ and $\mathcal{B}$ are bases of V such that

$${}_{\mathcal{A}}[\psi]_{\mathcal{A}} = \operatorname{diag}(J(a_1, \lambda_1), \ldots, J(a_s, \lambda_s)) \text{ and } {}_{\mathcal{B}}[\psi]_{\mathcal{B}} = \operatorname{diag}(J(b_1, \mu_1), \ldots, J(b_t, \mu_t))$$

for some positive integers $a_1, \ldots, a_s, b_1, \ldots b_t$ and some scalars $\lambda_1, \ldots, \lambda_s, \mu_1, \ldots, \mu_t \in F$, then the multisets $\{(a_1, \lambda_1), \ldots, (a_s, \lambda_s)\}$ and $\{(b_1, \mu_1), \ldots, (b_t, \mu_t)\}$ are equal.

6.4. Example of Jordan Normal Form

Let $A \in \mathsf{Mat}(4; \mathbb{C})$ be the following matrix

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

I calculate that $\chi_A(x) = (x-1)^3(x+1)$. Therefore $P_1(x) = (x+1)$, $P_2(x) = (x-1)^3$. To calculate the $Q_j(x)$ I work as follows: :

$$\begin{aligned} P_2(x) &= P_1(x) \cdot (x^2 - 4x + 7) - 8 \\ \text{so} \qquad 8 &= P_1(x) \cdot (x^2 - 4x + 7) - P_2(x) \end{aligned}$$

Thus I take

$$Q_1(x) = \frac{1}{8}(x^2 - 4x + 7),\ Q_2(x) = -\frac{1}{8}$$

Now let's get to work on the generalised eigenspaces. I am supposed to calculate $P_1(A)Q_1(A)$ and $P_2(A)Q_2(A)$. This is quite tedious, but produces

$$P_1(A)Q_1(A) = \frac{1}{2}\begin{pmatrix} 3 & 0 & 1 & 0 \\ -1 & 2 & -1 & 0 \\ -3 & 0 & -1 & 0 \\ 3 & 0 & 3 & 2 \end{pmatrix}, \quad P_2(A)Q_2(A) = \frac{1}{2}\begin{pmatrix} -1 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ 3 & 0 & 3 & 0 \\ -3 & 0 & -3 & 0 \end{pmatrix}$$

Thanks to the proof of Proposition 6.3.5(2) the space $E^{\mathsf{gen}}(1, A)$ is the column span of the first matrix, so spanned by the vectors $(0, 1, 0, 0)^{\mathsf{T}}$, $(0, 0, 0, 1)^{\mathsf{T}}$ and $(3, -1, -3, 3)^{\mathsf{T}}$, and the space $E^{\mathsf{gen}}(-1, A)$ is the column span of the second matrix, so spanned by the vector $(-1, 1, 3, -3)^{\mathsf{T}}$.

Now I calculate

$$A - I_4 = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ -2 & 1 & -2 & 1 \\ 2 & -1 & 2 & -1 \end{pmatrix}$$

The eigenspace $E(1, A)$ is then spanned by null vectors of this: say $(1, 0, -1, 0)^{\mathsf{T}}$ and $(0, 1, 0, -1)^{\mathsf{T}}$. I calculate again:

$$(A - I_4)^2 = \begin{pmatrix} -2 & 0 & -2 & 0 \\ 2 & 0 & 2 & 0 \\ 6 & 0 & 6 & 0 \\ -6 & 0 & -6 & 0 \end{pmatrix}$$

This now has nullvectors spanned by $(1, 0, -1, 0)^{\mathsf{T}}$, $(0, 1, 0, -1)^{\mathsf{T}}$ and $(0, 1, 0, 1)^{\mathsf{T}}$. This produces vectors in $E^{\mathsf{gen}}(1, A)$, and since I know that space to be 3-dimensional by the previous paragraph, these are a basis for it.

Similarly,

$$A + I_4 = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 0 & 3 & 0 & 1 \\ -2 & 1 & 0 & 1 \\ 2 & -1 & 2 & 1 \end{pmatrix}$$

which shows me that $E(-1, A)$ is spanned by $(-1, 1, 3, -3)^{\mathsf{T}}$. By the earlier work, I even know that this spans $E^{\mathsf{gen}}(-1, A)$ because that space is 1-dimensional.

I'm now ready to start the algorithm. For $E^{\mathsf{gen}}(-1, A)$ there's not much to do. I pick $\vec{u} = (-1, 1, 3, -3)$ as my basis for $E^{\mathsf{gen}}(-1, A)$. I know that if I apply A to that it gets multiplied by -1. Now I look to $E^{\mathsf{gen}}(1, A)$. I want to pick a vector $\vec{v}$ in this space such that $(A - I_4)^2\vec{v} = \vec{0}$ but $(A - I_4)\vec{v} \neq \vec{0}$. This just means that I have to avoid elements in $E^{\mathsf{gen}}(1, A)$ that are linear combinations of the eigenvectors $(1, 0, -1, 0)^{\mathsf{T}}$ and $(0, 1, 0, -1)^{\mathsf{T}}$. Let me take $\vec{v}_{2,1} = (0, 1, 0, 0)^{\mathsf{T}}$. Now I need to calculate $(A - I_4)\vec{v}_{2,1}$: it is $(-1, 1, 1, -1)^{\mathsf{T}}$. This is, as it has to be according to the theory expounded in Step 2, an eigenvalue of $A - I_4$. I label it by $\vec{v}_{1,1}$. I then need to find another element in $E(1, A)$ that extends $\vec{v}_{1,1}$ to a basis: I'll take $\vec{v}_{1,2} = (1, 0, -1, 0)^{\mathsf{T}}$.

The theory now tells me that if use $(\vec{u}, \vec{v}_{1,1}, \vec{v}_{2,1}, \vec{v}_{1,2})$ as an ordered basis for $\mathbb{C}^4$ and then calculate $A\circ : \mathbb{C}^4 \to \mathbb{C}^4$ with respect to this basis the corresponding matrix will be in Jordan Normal Form. Explicitly this will mean

$$P^{-1}AP = \mathrm{diag}(J(-1, 1), J(2, 1), J(1, 1))$$

where P is the change of basis matrix from the above basis to the standard basis. Written out in gory detail, it states:

$$\begin{pmatrix} -1 & -1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 3 & 1 & 0 & -1 \\ -3 & -1 & 0 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 2 & 0 & 1 \\ -2 & 1 & -1 & 1 \\ 2 & -1 & 2 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 3 & 1 & 0 & -1 \\ -3 & -1 & 0 & 0 \end{pmatrix} = \left(\begin{array}{c|cc|c} -1 & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

6.5. A Brief Explanation of the Final Step in PageRank as an Application of the Jordan Normal Form

After the proof of Theorem 4.7.10 I mentioned that the *practical* key to finding $\vec{v}$, the positive eigenvector with eigenvalue 1 of the Markov matrix M there, was that for an arbitrary $\vec{w} \geqslant \vec{0}$ with $|\vec{w}| = 1$

$$\lim_{k\to\infty} M^k \vec{w} = \vec{v}$$

The proof of this is relatively straightforward using Jordan Normal Form, given the following Lemma whose proof is a variation on the methods used in the proof of Theorem 4.7.10.

LEMMA 6.5.1. *If $M \in \mathsf{Mat}(n;\mathbb{R})$ is a Markov matrix all of whose entries are positive. Consider M as a complex matrix, all of whose entries happen to be real. If $\lambda \in \mathbb{C}$ is an eigenvalue of M then either $\lambda = 1$ or $|\lambda| < 1$.*

SKETCH OF PROOF. Assume that $\lambda \neq 1$. Let $\vec{w} \in \mathbb{C}^n$ be an eigenvector of M with eigenvalue λ. Define $\vec{w}^+$ to be the vector whose i-th entry is $|w_i|$, the absolute value of w_i. Clearly, $\vec{w}^+ \in \mathbb{R}^n$ and in fact $\vec{w}^+ \geqslant 0$. Using a version of the triangle inequality, which you met in Corollary 5.2.6, and the positivity of M it follows that:

$$(M\vec{w}^+)_i = \sum_{j=1}^{n} |M_{ij}||w_j| \geqslant |\sum_{j=1}^{n} M_{ij}w_j| = |\lambda w_i| = |\lambda|\vec{w}_i^+$$

The triangle inequality is an equality if and only if all the w_i are on a single ray in the complex plane out from the origin. If this ray makes an angle of θ radians with the positive real axis, then I could rotate this line to the positive real line; rotation corresponds to multiplying by $e^{-\sqrt{-1}\theta}$, so I'd deduce that $e^{-\sqrt{-1}\theta}\vec{w} \in \mathbb{R}^n_{>0}$. In this case, $e^{-\sqrt{-1}\theta}\vec{w}$ is a positive real eigenvector and so Step 3 of the proof of Theorem 4.7.10 shows that $\lambda = 1$, a contradiction. Hence the triangle inequality gives a strict inequality above and $M\vec{w}^+ > |\lambda|\vec{w}^+$. Thus, using the notation of Step 2 of the proof of Theorem 4.7.10,

$$1 = R(\vec{v}) \geqslant R(\vec{w}^+) > |\lambda|$$

This confirms the claim! □

How does this help? Well take $W = \langle \vec{w} \in \mathbb{R}^n : |\vec{w}| = 0 \rangle$. Since M is a Markov matrix, for any $\vec{w} \in W$

$$|M\vec{w}| = \sum_{i=1}^{n} (M\vec{w})_i = \sum_{i=1}^{n}\sum_{j=1}^{n} M_{ij}w_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} M_{ij}\right) w_j = \sum_{j=1}^{n} w_j = 0.$$

Thus $M(W) \subseteq W$ and so I can take a basis $\mathcal{B} = (\vec{v}, \vec{b}_1, \ldots, \vec{b}_{n-1})$ of $\mathbb{R}^n$ where $(\vec{b}_1, \ldots, \vec{b}_{n-1})$ is a basis of W and then see that if P is the change of basis matrix from $\mathcal{B}$ to the standard basis then

$$M = P^{-1}KP$$

where K is a block diagonal matrix

$$K = \begin{pmatrix} 1 & 0 \\ 0 & L \end{pmatrix}$$

and L is an $(n-1 \times n-1)$-real matrix all of whose eigenvalues have absolute value less than 1. If I choose the basis $(\vec{b}_1, \ldots, \vec{b}_{n-1})$ to be the basis appearing in the Jordan Normal Form theorem then I will even know that the matrix L has the form

$$L = \operatorname{diag}(J(r_1, \lambda_1), \ldots, J(r_t, \lambda_t))$$

where $r_1 + \cdots + r_t = n-1$ and where the $\lambda_i \in \mathbb{C}$ are the eigenvalues of M not equal to 1. In particular $L = D + N$ where N is nilpotent, D is a diagonal matrix with λ_i's along the diagonal, and $DN = ND$. Therefore

$$\lim_{k\to\infty} L^k = \lim_{k\to\infty} (D+N)^k = \lim_{k\to\infty} \left(\sum_{j=1}^{k} \binom{n}{j} D^j N^{k-j} \right)$$

Now, since N is nilpotent, it must be that $N^{n-1} = 0$ and therefore this limit is actually

$$\lim_{k\to\infty} \left(\sum_{j=k-n+1}^{k} \binom{n}{j} D^j N^{k-j} \right)$$

But D^j is a diagonal matrix whose entries are powers λ_i^j and by Lemma 6.5.1, each λ_i has absolute value strictly less than 1. So as j increases the absolute value of all the non-zero entries of D^j tend to zero. This proves that $\lim_{k\to\infty} L^k = 0$. From this, I deduce the claim

$$\lim_{k\to\infty} M^k = \lim_{k\to\infty} P^{-1} \begin{pmatrix} 1 & 0 \\ 0 & N^k \end{pmatrix} P = \lim_{k\to\infty} P^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P$$

Now take $\vec{w} \geqslant \vec{0}$ with $|\vec{w}| = 1$. Decompose it with respect to the basis $\mathcal{B}$ to get $\vec{w} = c\vec{v} + \sum_{i=1}^{n-1} c_i \vec{b}_i$ with $c, c_i \in \mathbb{R}$. This implies that $1 = |\vec{w}| = |c||\vec{v}| + \sum_{i=1}^{n-1} |c_i||\vec{v}_i| = |c|$ so that $c = \pm 1$. Positivity of $\vec{w}$ implies that $c = 1$ rather than -1. Thus $P\vec{w} = (1, c_1, \ldots, c_{n-1})^{\mathsf{T}}$. Finally,

$$P^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P\vec{w} = P^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} (1, c_1, \ldots, c_{n-1})^{\mathsf{T}} = P^{-1}(1, 0, \ldots, 0)^{\mathsf{T}} = \vec{v}.$$

Therefore, as claimed

$$\lim_{k\to\infty} M^k \vec{w} = \vec{v}$$

So the world of mathematics is in order.

LONG MAY THAT LAST!