Keele
UNIVERSITY

MAT-30045: Linear Algebra and Rings

F. Olukoya

February 1, 2023

Table of contents

Welcome

Welcome to *MAT-30045: Linear Algebra and Rings*. This module is an option for Single Honours BSc and MMath and Combined Honours BSc and expands on two part-modules from the second year. In the first half we shall be studying ideas in Linear Algebra that expand on the introduction to this subject given in Exploring Algebra and Analysis (MAT-20035). In the second half we delve more deeply into the study of the algebraic object called a ring which was first introduced formally in Abstract Algebra (MAT-20025).

Structure

The module is comprised of the following parts:

Part I

1. Revision and the exchange lemma.
2. Linear mappings and the Rank-Nullity Theorem.
3. Eigenspaces.
4. Vector space isomorphisms.

Part II

5. Ring theory fundamentals.
6. Ideals.
7. Unique factorisation domains.

Intended Learning Outcomes (ILO's)

Upon successful completion of this module you will be able to:

- define a linear transformation, prove and apply associated results, including the use of linear transformations to change between bases in a vector space;
- define an eigenvalue and eigenvector of a linear transformation and apply these concepts to, inter alia, the diagonalisation of square matrices;
- define vector space isomorphisms;
- define different types of ring, and state and prove associated results;
- define ideals, maximal ideals and principal ideals and solve associated problems;
- recognise and define ideals and unique factorisation domains, prove associated results and/or solve associated problems.

Prerequisites

MAT-20025

Lecture notes and recommended reading

A full-set of gapped notes is available on KLE[1]. At the conclusion of a given chapter, the notes will be updated to include the missing parts of that chapter. For example at the conclusion of Chapter *n*, the notes will be updated to include the gaps in Chapter *n*.

In addition, the following non-essential texts are recommended as providing more in-depth discussion/ a different point of view on topics covered in lectures as well as additional practise examples.

- H. Anton & C. Rorres: Elementary Linear Algebra: applications version (7th edition).
- Peter J. Cameron: Introduction to Algebra (2nd edition).
- R. B. J. T. Allenby: Rings, Fields and Groups: an Introduction to Abstract Algebra (2nd edition).

[1] These are based on Neil Turner's excellent set of notes

Copies of the above are available in the library. In addition, Cameron is available as an e-book.

Logistics

Lectures

The lecture material will be delivered by way of 2.5 standard, face-to-face lectures each week (3 in even weeks and 2 in odd). If you have any questions while going through the content then *do* email me f.a.olukoya@keele.ac.uk. I am more than happy to arrange a meeting over teams or in person.

Example classes

In weeks 2, 4, 6, 8, and 10 the Thursday class will be an examples class given over to the study of specified problems. The expectation is that students will prepare solutions to these problems for discussion in the session; this is an important part of your learning process. Problem Sheets can be found at the end of the relevant section in the notes. Please note that you should only attend the example class to which you have been allocated.

Example Class	**Questions**
1	Sheet 1
2	Sheet 2 Q2.1 – Q2.16
3	Sheet 2 Q2.17 – Q2.21
4	Sheet 3 Q3.1 – 3.7
5	Sheet 3 Q 3.8 – 3.11 & Sheet 4

Table 1: Example Classes

Timetable

Details of all sessions (lectures and examples classes) will be available on your eVision timetable. Please make sure that you have the correct day, time and room for each session. You should check this regularly as there are occasionally changes, particularly in the first couple of weeks of the semester.

Table 2 displays a detailed schedule for the semester.

Lecturers

This semester Dr. Feyisayo (Shayo) Olukoya will be the lecturer on the module. As mentioned above you can reach me by **email**; you should also feel free to arrange an in-person meeting my office is **Mac2.30** in the Mackay Building; meeting virtually over teams is also an option.

KLE

All resources for the module (lecture notes, problem sheets, solutions e.t.c) will be made available on KLE at the appropriate time.

Assessment

Continuous Assessment

This will be made up of two take-home assessments (each contributing 15% of the overall module mark). An assessment schedule will be available on the Mathematics Noticeboard on the KLE. Note that the first assessment is called an *assignment*, whilst the second is called a *coursework*; this nomenclature is purely for administrative convenience.

Formative assessment

Problem sheets can be found at the end of the each chapter of the lecture notes. Although these sheets do not contribute to the continuous assessment component, you are strongly encouraged to attempt them as they are designed to consolidate your understanding and enhance your problem-solving skills. Full solutions are provided after the sheet has been covered in example classes.

Final Exam

This comprises 70% of the module mark. It is an unseen, closed-book examination, with all questions being compulsory. The use of calculators is governed by the University regulations. The examination will require you to state definitions, state (and possibly prove) results, and apply these to solving problems. You should be able to state every definition and result in the module unless they are marked in the lecture notes as non-examinable.

Student Support

For advice on any non-academic issue (including financial, international, personal or health matters) or if you are unsure who to go to for help, please contact Student Services. You can book a virtual appointment or email student.services@keele.ac.uk.

You can also contact the school's Student Experience and Support Officer by emailing student services student.services@keele.ac.uk.

Week Beginning	Day	Chapter	Material
23 Jan	M	1	Introduction and Revision
	T	1	Dimension and Sums of subspaces
	Thu	1	Sums of subspaces
30 Jan	M	1	Direct sums & row and column spaces
	T	1	Rank-Nullity Theorem of matrices
	Thu		**Example Class 1**
6 Feb	M	2	Linear Mappings
	T	2	Image and Kernel
	Thu	2	Rank-Nullity Theorem
13	M	2	Matrices from linear mappings
	T	2	Change of basis
	Thu		**Example Class 2**
20	M	2	Eigenvalues and Eigenvectors
	T	2	Diagonalisation
	Thu	2	Vector space isomorphisms
27	M	3	Ring theory introduction
	T	3	Polynomial and quadratic integer rings
	Thu		**Example Class 3** ***(Assignment)***
6 Mar	M	3	Division in a ring
	T	3	Zero divisors, and integral domains
	Thu	3	Integral domains and subrings ***(Assignment Due)***
13 Mar	M	3	Subrings examples
	T	3	Ring homomorphisms
	Thu		**Example Class 4**
20	M	3	Ideals
	T	3	Ideals II
	Thu	3	Ideals III
17 Apr	M	3	Factor rings: cosets
	T	3	Factor rings & the First Isomorphism Theorem
	Thu		**Example Class 5** ***(Coursework)***
24 Apr	M	4	Principal Ideal Domains (PIDs)
	T	4	Maximal Ideals and Prime Ideals
	Thu	4	$\mathbb{Z}[i]$ is a PID and Unique Factorisation Domains ***(Coursework due)***
1 May	M		
	T		
	Thu		***Revision***
8			***Exams***

Table 2: Timetable

Part I

Linear Algebra

Chapter 1

Introduction and Revision

This module expands on two part-modules from the second year. In the first half we shall be studying ideas in Linear Algebra that expand on the introduction to this subject expounded in Exploring Algebra and Analysis. In the second half we delve more deeply into the study of the algebraic object called a ring which was first introduced formally in Abstract Algebra.

1.1 Revision of Linear Algebra

We begin with a recap of some of the basic ideas and concepts from Linear Algebra which you have seen in the Exploring Algebra and Analysis module. The main difference to note here is that all of the results will be expressed in terms of vector spaces over a general field $\mathcal{F}$, rather than the specific field $\mathbb{R}$. There is a set of examples (questions R.1 – R.6 in Section 1.3 at the end of the chapter).

Definition 1.1 (Vector space)**.** Let $\mathcal{F}$ be a field. We say that a set V is a *vector space* over $\mathcal{F}$ if addition of elements of V and multiplication of elements of V by scalars from $\mathcal{F}$ are both defined such that the vector space axioms hold. These axioms are as follows:

A0. $\mathbf{x}, \mathbf{y} \in V \Rightarrow \mathbf{x} + \mathbf{y} \in V$.

A1. For all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$, $(\mathbf{x}+\mathbf{y})+\mathbf{z} = \mathbf{x}+(\mathbf{y}+\mathbf{z})$.

A2. For all $\mathbf{x}, \mathbf{y} \in V$, $\mathbf{x}+\mathbf{y} = \mathbf{y}+\mathbf{x}$.

A3. There exists an element $\mathbf{0} \in V$ such that $\mathbf{x}+\mathbf{0} = \mathbf{x}$ for all $\mathbf{x} \in V$.

A4. For all $\mathbf{x} \in V$, there exists $-\mathbf{x} \in V$ such that $\mathbf{x}+(-\mathbf{x}) = \mathbf{0}$.

M0. $\lambda \in \mathcal{F}, \mathbf{x} \in V \Rightarrow \lambda\mathbf{x} \in V$

M1. For all $\mathbf{x}, \mathbf{y} \in V$ and for all $\lambda \in \mathcal{F}$, $\lambda(\mathbf{x}+\mathbf{y}) = \lambda\mathbf{x}+\lambda\mathbf{y}$.

M2. For all $\mathbf{x} \in V$ and for all $\lambda, \mu \in \mathcal{F}$, $(\lambda+\mu)\mathbf{x} = \lambda\mathbf{x}+\mu\mathbf{x}$.

M3. For all $\mathbf{x} \in V$ and for all $\lambda, \mu \in \mathcal{F}$, $\lambda(\mu\mathbf{x}) = (\lambda\mu)\mathbf{x}$.

M4. For all $\mathbf{x} \in V$, $1\mathbf{x} = \mathbf{x}$.

Note

i. In a vector space V, we refer to the elements of V as *vectors*.

ii. A vector space cannot be empty by **A3**.

iii. For $\mathbf{x} \in V$, the vector $-\mathbf{x}$ is called the *negative* of $\mathbf{x}$.

iv. A vector space is sometimes called a *linear space*.

Recall the following lemmas, which we state without proof:

Lemma 1.1. *Let V be a vector space. There is only one zero vector in V.*

Lemma 1.2. *The negative of a vector in a vector space V is unique.*

Lemma 1.3. *Let V be a vector space. For all $\mathbf{x} \in V$, $0\mathbf{x} = \mathbf{0}$.*

Lemma 1.4. *Let V be a vector space. For all $\lambda \in \mathcal{F}$, $\lambda\mathbf{0} = \mathbf{0}$.*

Lemma 1.5. *Let V be a vector space. For all $\mathbf{x} \in V$, $\lambda \in \mathcal{F}$,*

$$\lambda\mathbf{x} = \mathbf{0} \Rightarrow \lambda = 0 \quad \text{or} \quad \mathbf{x} = \mathbf{0}.$$

We are often interested in whether or not a subset of vectors from a vector space satisfies the conditions to be a vector space in its own right. If so, it forms a subspace.

Definition 1.2 (Subspace)**.** Let V be a vector space over the field $\mathcal{F}$. We say that a subset $U \subseteq V$ which is a vector space in its own right is called a *subspace* of V.

It is not necessary to check all of the axioms to determine whether a subset forms a subspace; the following lemma says we need only check three things.

Lemma 1.6 (Checking Lemma)**.** *Let V be a vector space over the field $\mathcal{F}$. A subset $U \subseteq V$ is a subspace of V if the following three conditions hold:*

1. $U \neq \emptyset$;
2. $\mathbf{x}, \mathbf{y} \in U \Rightarrow \mathbf{x} + \mathbf{y} \in U$;
3. $\lambda \in \mathcal{F}, \mathbf{x} \in U \Rightarrow \lambda\mathbf{x} \in U$.

The following three lemmas concern important properties of subspaces:

Lemma 1.7. *Let V be a vector space over the field $\mathcal{F}$. The zero vector $\mathbf{0}$ belongs to every subspace of V.*

Lemma 1.8. *Let $A \in \mathcal{F}_{m\times n}$. The set*

$$N(A) = \{\mathbf{X} \in \mathcal{F}_{n\times 1} \mid A\mathbf{X} = \mathbf{0}\}$$

is a subspace of $\mathcal{F}_{n\times 1}$.

Lemma 1.9. *Let V be a vector space over the field $\mathcal{F}$ and let U and W be subspaces of V. Then $U \cap W$ is also a subspace of V.*

One of the most fundamental concepts in algebra is that of linear independence. This, in itself, is derived from the concept of a linear combination and we remind ourselves of the important definitions and results.

Definition 1.3 (Linear combination)**.** Let $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k$ be vectors in a vector space V. A *linear combination* of the sequence $(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k)$ is an expression of the form

$$\lambda_1\mathbf{x}_1 + \lambda_2\mathbf{x}_2 + ... + \lambda_k\mathbf{x}_k,$$

where $\lambda_1, \lambda_2, ..., \lambda_k \in \mathcal{F}$.

Definition 1.4 (Span)**.** Let V be a vector space and let $(\mathbf{x}_1, ..., \mathbf{x}_k)$ be a sequence of vectors in V. The *span* of the sequence $(\mathbf{x}_1, ..., \mathbf{x}_k)$ is the set of all linear combinations of the vectors in the sequence. Hence

$$\mathrm{span}(\mathbf{x}_1, ..., \mathbf{x}_k) = \{\lambda_1\mathbf{x}_1 + \lambda_2\mathbf{x}_2 + ... + \lambda_k\mathbf{x}_k \mid \lambda_1, \lambda_2, ..., \lambda_k \in \mathcal{F}\}.$$

We define the span of the empty sequence to be the set consisting of the zero vector, $\{\mathbf{0}\}$.

Lemma 1.10. *Let* $(\mathbf{x}_1, ..., \mathbf{x}_k)$ *be a sequence of vectors in a vector space* V*. Then* $\operatorname{span}(\mathbf{x}_1, ..., \mathbf{x}_k)$ *is a subspace of* V*.*

Definition 1.5 (Linear independence)**.** Let $(\mathbf{x}_1, ..., \mathbf{x}_k)$ be a sequence of vectors in a vector space V. We say that the sequence is *linearly independent* (or L.I.) if

$$\lambda_1\mathbf{x}_1 + \lambda_2\mathbf{x}_2 + ... + \lambda_k\mathbf{x}_k = \mathbf{0} \Rightarrow \lambda_1 = \lambda_2 = ... = \lambda_k = 0. \qquad (\lambda_i \in \mathcal{F})$$

Definition 1.6 (Linear dependence)**.** Let $(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k)$ be a sequence of vectors in a vector space V. The sequence is *linearly dependent* (or L.D.) if there exist scalars $\lambda_1, \lambda_2, ..., \lambda_k \in \mathcal{F}$, not all zero, such that

$$\lambda_1\mathbf{x}_1 + \lambda_2\mathbf{x}_2 + ... + \lambda_k\mathbf{x}_k = \mathbf{0}.$$

The following are important results on linear independence/dependence.

Lemma 1.11. *Let* $L = (\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k)$ *be a linearly independent sequence of vectors in a vector space* V*. If* $\mathbf{x} \in V$ *can be written as a linear combination of the vectors in* L*, then this representation is unique.*

Lemma 1.12. *If a sequence of vectors in a vector space* V *contains a repetition, then the sequence is linearly dependent.*

Lemma 1.13. *If a sequence of vectors in a vector space V contains the zero vector then the sequence is linearly dependent.*

Lemma 1.14. *Let V be a vector space and let $\mathbf{x} \in V$ be non-zero. Then the sequence $(\mathbf{x})$ is linearly independent.*

Two important theorems from the second year module are the Minus Theorem and the Plus Theorem.

Theorem 1.1 (Minus Theorem)**.** *Let V be a vector space. Suppose that the vectors $\mathbf{x}_1, ..., \mathbf{x}_k \in V$ are linearly dependent. Then there exists $j \in \{1, 2, ..., k\}$ such that*

$$\operatorname{span}(\mathbf{x}_1, ..., \mathbf{x}_{j-1}, \mathbf{x}_{j+1}, ..., \mathbf{x}_k) = \operatorname{span}(\mathbf{x}_1, ..., \mathbf{x}_k).$$

The way to think about this result is that we can remove a vector from a linearly dependent sequence without changing the span. However, we need to be careful with the wording 'there exists'; we cannot remove any vector, we need to choose carefully.

Theorem 1.2 (Plus Theorem)**.** *Let V be a vector space and suppose that the sequence $(\mathbf{x}_1, ..., \mathbf{x}_k)$ in V is linearly independent. Then, for any $\mathbf{a} \in V$,*

$$\mathbf{a} \notin \operatorname{span}(\mathbf{x}_1, ..., \mathbf{x}_k) \Rightarrow (\mathbf{x}_1, ..., \mathbf{x}_k, \mathbf{a}) \ \textit{ is linearly independent.}$$

The way to think of this theorem is that we can add a *certain* vector to a linearly independent sequence and still have a linearly independent sequence. But, we cannot just add any vector; it has to be a vector that is not a linear combination of the vectors in the set. These two theorems can be used to prove the following theorem, known as the ‘Exchange Lemma’, which we state without proof.

Theorem 1.3 (Exchange Lemma)**.** *Let V be a vector space and suppose that the sequence $(\mathbf{x}_1, ..., \mathbf{x}_m)$ in V is linearly independent and that the sequence $(\mathbf{y}_1, ..., \mathbf{y}_k)$ spans V. Then,*

i. $m \leq k$*,*

ii. there is a spanning sequence for V consisting of $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_m$ and $k-m$ of the vectors $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_k$.

The sequence $(\mathbf{y}_1, \ldots, \mathbf{y}_k)$ spans V, so *every* vector in V can be written as a linear combination of the $\mathbf{y}_i$. Part (i) says that a linearly independent sequence is not longer than a sequence that spans V. From part (ii) we see why it is called the ‘exchange’ lemma; we can exchange m of the $\mathbf{y}_i$ for the $\mathbf{x}_i$.

Another central concept in linear algebra is that of a basis:

Definition 1.7 (Finite dimension)**.** Let V be a vector space. We say that V is *finite dimensional* if there exists a finite sequence of vectors that spans V. Otherwise we say that V is infinite dimensional.

Definition 1.8 (Basis)**.** Let V be a vector space. We say that a finite sequence $(\mathbf{x}_1, ..., \mathbf{x}_k)$ of vectors in V is a *basis* of V if the sequence is (i) linearly independent and (ii) spans V.

Lemma 1.15. *Every finite dimensional vector space has a finite basis.*

Lemma 1.16. *Let V be a vector space and suppose that $(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n)$ is a basis of V (of length n). Then every sequence of more than n vectors in V is linearly dependent.*

Corollary 1.1. *In a finite dimensional vector space, all bases have the same length.*

So, what is meant by the 'dimension' of a vector space?

Definition 1.9 (Dimension)**.** The number of vectors in each and every basis of a vector space V is called the *dimension* of V and is denoted $\dim(V)$.

The following lemma says that a finite sequence of vectors in a vector space forms a basis if it satisfies two of three properties.

Lemma 1.17. *Let L be a finite sequence of vectors in a vector space V. We can conclude that L is a basis of V if we know that it possesses any two of the following properties:*

i. it spans V;

ii. it is linearly independent;

iii. it has length equal to $\dim(V)$.

Note that, thanks to the Exchange Lemma, we can extend a linearly independent sequence in a vector space to a basis.

Definition 1.10 (Coordinate vector)**.** Let $(\mathbf{x}_1, ..., \mathbf{x}_n)$ be a basis of the finite dimensional vector space V. Then for each $\mathbf{y} \in V$, we can express $\mathbf{y}$ uniquely as

$$\mathbf{y} = \gamma_1 \mathbf{x}_1 + ... + \gamma_n \mathbf{x}_n$$

for some $\gamma_1, ..., \gamma_n \in \mathcal{F}$. The n-tuple $(\gamma_1, ..., \gamma_n) \in \mathcal{F}^n$ is called the *coordinate vector* of $\mathbf{y}$ with respect to the basis $(\mathbf{x}_1, ..., \mathbf{x}_n)$.

Example 1.1. Show that the sequence $L_1 = (1 + x,\ 1 - x)$ in P_2 is linearly independent and use the Exchange Lemma to extend L_1 to a basis of P_2. Find the coordinate vector of $p(x) = 2 - x + 3x^2$ with respect to your basis.

Let $a, b \in \mathbb{R}$ and suppose that $a(1 + x) + b(1 - x) = 0$ (where 0 is the zero polynomial). Equating coefficients, it follows that $a + b = 0$ and and $a - b = 0$. Therefore $a = b = 0$ since adding the two equations gives $2a = 0$.

The set $B = (1, x, x^2)$ is the standard basis for P_2. By the Exchange Lemma, there is an element $v \in B$ such that $(1 + x, 1 - x, v)$ is a spanning set for P_2. Since all bases for P_2 have the same length then $(1 + x, 1 - x, v)$ must be a basis for P_2 as well (since otherwise we may find a basis for P_2 of length strictly less than 3!). Thus the vector $v \in B$ is any element of B which is not in the span of L_1. This follows since $(1 + x, 1 - x, v)$ must be linearly independent. Since x^2 does not occur in any of the vectors in P_2, then x^2 is the obvious choice for v. Indeed we have,

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

whereas if $a(1 + x) + b(1 - x) = x^2$ for $a, b \in \mathbb{R}$ then (equating coefficients) $a = b = 0$ which is a contradiction since $x^2 \neq 0$.

Therefore $B' = (1 + x, 1 - x, x^2)$ is a basis for P_2.

Using the formula above expressing 1 and x in terms of the basis B', we have

$$p(x) = 2-x+3x^2 = ((1+x)+(1-x))-\frac{1}{2}((1+x)-(1-x))+3x^2 = \frac{1}{2}(1+x)+\frac{3}{2}(1-x)+3x^3.$$

1.2 Some Further Results

Before we can progress with our study of linear mappings we require some further theory. The first few results you will have seen previously, the rest is new material.

1.2.1 Dimension of Subspaces

Lemma 1.18. *Let W be a subspace of a finite dimensional vector space V. Then*

i. *W is also finite dimensional,*

ii. $\dim(W) \leq \dim(V)$*,*

iii. *if $W \neq V$ then* $\dim(W) < \dim(V)$*,*

iv. *any basis of W can be extended to produce a basis of V.*

Proof. Let $n = \dim(V)$. Since W is a subspace of V, the length of a linearly independent sequence in W is at most n. Let m be maximum length of a linearly independent sequence in W and let $B = (w_1, w_2, \dots, w_m)$ be a linearly independent sequence in W of length m. We prove that b is a basis for w.

Let $w \in W$ and suppose that $w \neq \mathrm{span}(B)$. Then $B' = (w_1, w_2, \dots, w_m, w)$ is also linearly independent. By the Plus Theorem (Theorem 1.2). Therefore B' is a linearly independent subset of W of length $m+1$ which is a contradiction. We see that $w \in \mathrm{span}(B)$. Since $w \in W$ was arbitrarily chosen, $\mathrm{span}(B) = W$ and W is finite dimensional and has dimension less than or equal to n.

If the dimension of W is n, then any basis for W is a basis for V (any linearly independent subset of V of length n is a basis for V) and $W = V$. Therefore if $W \neq V$, then $\dim(W) < \dim(V)$.

The final part of the lemma is a consequence of the Exchange Lemma (Theorem 1.3).

□

Lemma 1.19. *Let S and T be finite dimensional subspaces of a vector space V such that*

1. *$S \subseteq T$ and*
2. *$\dim(S) = \dim(T)$.*

Then $S = T$.

Proof. This is a direct consequence of part iv. of Lemma 1.18 since as $S \subseteq T$ then S is a subspace of T as well.

□

ℹ Note

Note that in the statement of Lemma 1.19 although S and T are assumed to be finite dimensional, V is does not have to be finite dimensional.
For example we may take $V = \mathbb{R}[x]$, $S = P_4$ and $T = P_6$; S and T are finite dimensional subspaces of V, but V is not finite dimensional.

Definition 1.11 (Sum of subspaces)**.** Let S and T be subspaces of a vector space V. Then the sum of S and T is defined as

$$S + T = \{\mathbf{s} + \mathbf{t} \mid \mathbf{s} \in S,\ \mathbf{t} \in T\}.$$

Lemma 1.20. *Let V be a vector space and let S and T be subspaces of V. Then,*

a. *$S + T$ is also a subspace of V,*
b. *$S + T$ contains S and T as subsets,*
c. *$S + T$ is the smallest subspace of V that contains both S and T.*

Proof.

a. We use the Checking Lemma (Lemma 1.6).

   Clearly $S + T$ contains the zero vector since $\mathbf{0} + \mathbf{0} = \mathbf{0}$.

   Let $\mathbf{s}_1, \mathbf{s}_2 \in S$ and $\mathbf{t}_1, \mathbf{t}_2 \in T$, then $(\mathbf{s}_1 + \mathbf{t}_1) + (\mathbf{s}_2 + \mathbf{t}_2) = (\mathbf{s}_1 + \mathbf{s}_2) + (\mathbf{t}_1 + \mathbf{t}_2) \in S + T$.

   Let $\mathbf{s} \in S$, $\mathbf{t} \in T$ and $a \in \mathcal{F}$. Then $a(\mathbf{s} + \mathbf{t}) = a\mathbf{s} + a\mathbf{t} \in S + T$.

   Therefore $S + T$ is non-empty, closed under addition and closed under scalar multiplication — it is a subspace of V.

b. Let $\mathbf{s} \in S$ and $\mathbf{t} \in T$, then $\mathbf{s} = \mathbf{s} + \mathbf{0} \in S + T$ and $\mathbf{t} = \mathbf{0} + \mathbf{t} \in S + T$. Therefore $(S \cup T) \subseteq S + T$.

c. Let W be any other subspace containing both S and T. Then $S + T \subseteq W$ since W contains both S and T and is closed under addition.

□

Theorem 1.4. *Let V be a finite dimensional vector space and let S and T be subspaces of V. Then*

$$\dim(S + T) = \dim(S) + \dim(T) - \dim(S \cap T).$$

> ℹ Note
>
> The final term, $S \cap T$, accounts for the overlap between S and T.

Proof. Let $B_{S \cap T} = (\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_j)$ be a basis for $S \cap T$. Since $S \cap T$ is a subspace of both S and T, by the Exchange Lemma (Theorem 1.3) there are vectors $\mathbf{s}_1, \dots, \mathbf{s}_k \in S$ and $\mathbf{t}_1, \dots \mathbf{t}_l \in T$ such that

$$B_S = (\mathbf{c}_1, \dots, \mathbf{c}_j, \mathbf{s}_1, \dots, \mathbf{s}_k)$$

is a basis for S and

$$B_T = (\mathbf{c}_1, \dots, \mathbf{c}_j, \mathbf{t}_1, \dots, \mathbf{t}_l)$$

is a basis for T.

Consider the sequence

$$B := (\mathbf{c}_1, \dots, \mathbf{c}_j, \mathbf{s}_1, \dots, \mathbf{s}_k, \mathbf{t}_1, \dots, \mathbf{t}_l).$$

Clearly S and T are contained in the span of B and so B spans $S + T$ (by Lemma 1.20 part c.). We show that B is linearly independent.

First note that

$$\operatorname{span}(\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_l) \cap \operatorname{span}(\mathbf{c}_1, \dots, \mathbf{c}_j, \mathbf{s}_1, \dots, \mathbf{s}_k) = \{\mathbf{0}\}.$$

Since otherwise, there is an element $\mathbf{t} \neq \{0\} \in \operatorname{span}(\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_l)$ which is an element of S and so of $S \cap T$. Thus, $\mathbf{t}$ can be written as a linear combination of of the sequence $B_{S \cap T}$. This means that there is an element of T which can be written in two different ways as a linear combination of the sequence B_T contradicting the linear independence of B_T.

Now let $c_1, \dots, c_j, s_1, \dots, s_k, t_1, \dots, t_l \in \mathcal{F}$ and consider the equation:

$$\sum_{i=1}^{j} c_i \mathbf{c}_i + \sum_{i=1}^{k} s_i \mathbf{s}_i + \sum_{i=1}^{l} t_i \mathbf{t}_i = \mathbf{0}.$$

It must be the case that $t_i = 0$ for all $1 \leq i \leq k$ since otherwise $t = \sum_{i=1}^{l} t_i \mathbf{t}_i \neq 0$ and $t \in \operatorname{span}(\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_l) \cap \operatorname{span}(\mathbf{c}_1, \dots, \mathbf{c}_j, \mathbf{s}_1, \dots, \mathbf{s}_k)$ which is a contradiction.

However, if $t_i = 0$ for all $1 \leq i \leq k$, then the c_i's and s_i's must also be 0 since $B_S = (\mathbf{c}_1, \dots, \mathbf{c}_j, \mathbf{s}_1, \dots, \mathbf{s}_k)$ is a basis. Therefore, B is linearly independent.

Lastly observe that

$$|B| = |B_S| + |B_T| - |B_{S\cap T}| = \dim S + \dim T - \dim S \cap T$$

as required.

□

Example 1.2. Let S, T and U be subspaces of $\mathbb{R}^{2n-1}$ such that $\mathbb{R}^{2n-1} = S + T = S + U$ with $\dim(S) = n - 1$ and $S \cap T = S \cap U = \{\mathbf{0}\}$. By considering dimensions, show that $T \cap U \neq \{\mathbf{0}\}$.

> ℹ Note
>
> Although $S + T = T + U$ it is not necessarily the case that $T = U$.

Applying Theorem Theorem 1.4, consider the following:

$$2n - 1 = \dim(s) + \dim(T) - \dim(S \cap T)$$

rearranging, we have

$$n = 2n - 1 - n + 1 = 2n - 1 - \dim(s) = \dim(T) - \dim(S \cap T) = \dim(T) - 0$$

Therefore $\dim(T) = n$. In a similar way, we have that $\dim(T) = n$. Now observe that as $T + U$ is a subspace of $\mathbb{R}^{2n-1}$, $\dim(T + U) \leq 2n - 1$. We have:

$$2n - 1 \geq \dim(T + U) = \dim(T) + \dim(U) - \dim(T \cap U) = 2n - \dim(T \cap U).$$

Rearranging, we have that $\dim(T \cap U) \geq 1$, thus $T \cap U$ must contain at least one non-zero vector — $T \cap U \neq \{\mathbf{0}\}$.

Definition 1.12 (Direct sum)**.** Let V be a vector space over the field $\mathcal{F}$ and let S and T be subspaces of V. We say that a subspace W of V is a *direct sum* of the subspaces S and T if $W = S + T$ *and* $S \cap T = \{\mathbf{0}\}$. When the sum of S and T is direct we use the notation $W = S \oplus T$.

Lemma 1.21. *Let V be a vector space over the field $\mathcal{F}$ and suppose that S and T are subspaces of V such that $W = S \oplus T$. Then every element $\mathbf{w} \in W$ can be written uniquely in the form $\mathbf{w} = \boldsymbol{s} + \boldsymbol{t}$ where $\boldsymbol{s} \in S$ and $\boldsymbol{t} \in T$.*

Proof. Suppose there are elements $\mathbf{s}, \mathbf{s}' \in S$, $\mathbf{t}, \mathbf{t}' \in T$ such that $\mathbf{s} = \mathbf{t} = \mathbf{s}' + \mathbf{t}'$. It then follows that $\mathbf{s} - \mathbf{s}' = \mathbf{t}' - \mathbf{t}$. Therefore $\mathbf{s} - \mathbf{s}' = \mathbf{t}' - \mathbf{t} \in S \cap T$. Since $S \cap T = \{\mathbf{0}\}$, then $\mathbf{s} - \mathbf{s}' = \mathbf{0} = \mathbf{t} - \mathbf{t}'$ and so $\mathbf{s} = \mathbf{s}'$ and $\mathbf{t} = \mathbf{t}'$ as required.

□

Example 1.3.

Let $\mathbf{e}_x = (1, 0, 0)$, $\mathbf{e}_y = (0, 1, 0)$ and $\mathbf{e}_z = (0, 0, 1)$. Then, as these are the standard basis for $\mathbb{R}^3$ every vector in $\mathbb{R}^3$ can be written as a linear combination of $\mathbf{e}_x, \mathbf{e}_y$ and $\mathbf{e}_z$. That is $\mathbb{R}^3 = \operatorname{span}(\mathbf{e}_x) + \operatorname{span}(\mathbf{e}_y) + \operatorname{span}(\mathbf{e}_z)$. Notice that for any pair $(t, u) \in \{(x, y), (x, z), (y, z)\}$ $\operatorname{span}(\mathbf{e}_t) \cap \operatorname{span}(\mathbf{e}_u) = \{\mathbf{0}\}$. Moreover, for $v \in \{x, y, z\} \backslash \{t, u\}$ $(\operatorname{span}(\mathbf{e}_t) + \operatorname{span}(\mathbf{e}_u)) \cap (\operatorname{span}(\mathbf{e}_v)) = \{\mathbf{0}\}$.

It follows that $\mathbb{R}^3 = \operatorname{span}(\mathbf{e}_x) \oplus \operatorname{span}(\mathbf{e}_y) \oplus \operatorname{span}(\mathbf{e}_z)$.

Lemma 1.22. *Let V be a finite dimensional vector space over the field $\mathcal{F}$ and let S and T be subspaces of V such that the sum of S and T is a direct sum. Suppose that $(\boldsymbol{e}_1, \boldsymbol{e}_2, ..., \boldsymbol{e}_m)$ is a basis of S and $(\boldsymbol{f}_1, \boldsymbol{f}_2, ..., \boldsymbol{f}_n)$ is a basis of T. Then,*

1. $(\boldsymbol{e}_1, ..., \boldsymbol{e}_m, \boldsymbol{f}_1, ..., \boldsymbol{f}_n)$ *is a basis of* $S \oplus T$*,*
2. $\dim (S \oplus T) = \dim (S) + \dim (T)$*.*

Proof. We have by Theorem 1.4

$$\dim(S + T) = \dim(S) + \dim(T) - \dim(S \cap T) = \dim(S) + \dim(T)$$

since $S \cap T = \{\mathbf{0}\}$.

Now since $S \oplus T$ contains both S and T, then $S \oplus T$ contains $S + T$. However as $S \oplus T$ is spanned by $(\mathbf{e}_1, ..., \mathbf{e}_m, \mathbf{f}_1, ..., \mathbf{f}_n)$, we have:

$$\dim(S) + \dim(T) \leq \dim(S \oplus T) \leq \dim(S) + \dim(T)$$

Therefore $\dim(S \oplus T) = \dim(S) + \dim(T)$ and $(\mathbf{e}_1, ..., \mathbf{e}_m, \mathbf{f}_1, ..., \mathbf{f}_n)$ is in fact a basis for $S \oplus T$.

□

1.2.2 Back To Matrices

Let $A = (a_{ij}) \in \mathbb{R}_{m \times n}$ and recall that the matrix product of A with a column $\mathbf{X} \in \mathbb{R}_{n \times 1}$ produces a column $A\mathbf{X} \in \mathbb{R}_{m \times 1}$ where the entry in the ith row is the element

$$a_{i1}x_1 + a_{i2}x_2 + ... + a_{in}x_n.$$

Of course we can view columns and rows in the matrix A as elements of $\mathbb{R}^m$ or $\mathbb{R}^n$ respectively.

Definition 1.13 (Row space and column space)**.** With the matrix A as above, we define the i^{th} row vector of A to be the vector $\mathbf{r}_i = (a_{i1}, a_{i2}, ..., a_{in}) \in \mathbb{R}^n$ and the jth column vector of A to be the vector $\mathbf{c}_j = (a_{1j}, a_{2j}, ..., a_{mj}) \in \mathbb{R}^m$. The *row space* of A is the subspace span$(\mathbf{r}_1, ..., \mathbf{r}_m) \subset \mathbb{R}^n$. This subspace is denoted $\operatorname{row}(A)$ The *column space* of A is the subspace span$(\mathbf{c}_1, ..., \mathbf{c}_n) \subset \mathbb{R}^m$. This subspace is denoted $\operatorname{col}(A)$.

There are some important points to note about row-echelon matrices.

! Important

A matrix is said to be in row-echelon form if the following conditions hold:

- the first non-zero entry in a row is 1 (called the pivot);
- any zero rows are grouped together at the bottom of the matrix;
- if row i is *above* row j (and both are non-zero), then the pivot in row i is to the left of the pivot in row j.

A matrix is said to be in ***reduced row-echelon form*** if it is in row-echelon form *and* each column containing a pivot has zeros in every entry excluding the pivot.

Lemma 1.23. *Let $A, B \in \mathbb{R}_{m\times n}$. If A and B are row-equivalent then* $\operatorname{row}(A) = \operatorname{row}(B)$.

Proof. Suppose B is obtained from A by an elementary row operation. This means that one row of B has been replaced by a linear combination of the rows of A. Therefore $\operatorname{row}(B) \subseteq \operatorname{row}(A)$.

To see that $\operatorname{row}(A) \subseteq \operatorname{row}(B)$ observe that the row of A that is missing from B can be obtained as a linear combination of the rows of B simply by re-arranging to obtain an expression for the missing row vector.

Therefore $\operatorname{row}(A) = \operatorname{row}(B)$. The result is now an easy application of induction.

□

If we want to understand $\operatorname{row}(A)$, then we need a basis, that is a sequence of vectors that spans and is linearly independent. The following helps:

Lemma 1.24. *The non-zero rows in a row-echelon matrix form an linearly independent sequence.*

Proof. The empty sequence is trivially linearly independent. Therefore if the sequence of non-zero rows of E is empty, the result holds.

We may assume that E has some non-zero rows. Let $\mathbf{r}_1, \mathbf{r_2}, \dots, \mathbf{r}_m$ be the non-zero rows (from top to bottom). Let $r_1, r_2, \dots, r_m \in \mathcal{F}$ and consider the expression:

$$r_1\mathbf{r}_1 + r_2\mathbf{r}_2 + \dots + r_m\mathbf{r}_m = \mathbf{0}.$$

By definition of the row-echelon form, the first non-zero position of $\mathbf{r}_1$ is to the left of all non-zero positions in the remaining row vectors $\mathbf{r}_2 \dots \mathbf{r}_m$. Therefore $r_1 = 0$. We may then repeat the argument to get $r_2 = 0, r_3 = 0, \dots, r_m = 0$.

Therefore the sequence $(\mathbf{r}_1, \mathbf{r_2}, \dots, \mathbf{r}_m)$ is linearly independent.

□

Consider the following example:

$$\begin{array}{r} r_1\times \\ +r_2\times \\ +r_3\times \end{array} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 7 & 8 \\ 0 & 0 & 0 & 1 & 9 \end{pmatrix}$$

The first leading entry, implies that $r_1 = 0$, the second implies that r_2 is equal to 0, and then r_3 must be zero as well.

Lemma 1.25. *The sequence of non-zero rows in a row-echelon matrix E is a basis for the row space,* $\mathrm{row}\,(E)$*, and for the row space of every matrix row-equivalent to E.*

Proof. Any matrix row-equivalent to E has the same row space as E so it suffices to show only the first half of the statement.

By Lemma 1.24, the non-zero rows of E are linearly independent. However, the row space of E is also spanned by the sequence of its non-zero rows (if they are all zero then $\mathrm{row}\,(E) = \{\mathbf{0}\}$ which is spanned by the empty sequence). Therefore the non-zero rows of E are a basis for $\mathrm{row}\,(E)$.

□

Example 1.4. Find a basis of the subspace, S, of $\mathbb{R}^4$ spanned by the sequence of vectors

$$((1,0,1,2),\ (2,3,0,1),\ (-1,1,1,-2),\ (1,5,3,-1)).$$

The first step is to interpret the vectors as the rows of some matrix M, then we apply elementary row operations to until we get a matrix E in row-echelon form row equivalent to M. The non-zero rows of E then give a basis for S.

We have:

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ -1 & 1 & 1 & -2 \\ 1 & 5 & 3 & -1 \end{pmatrix} \begin{matrix} \\ r_2 \to r_2 - 2r_1 \\ r_3 \to r_3 + r_1 \\ r_4 \to r_4 - r_1 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 3 & -2 & -3 \\ 0 & 1 & 2 & 0 \\ 0 & 5 & 2 & -3 \end{pmatrix}$$

$$\begin{matrix} r_2 \leftrightarrow r_3 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & -2 & -3 \\ 0 & 5 & 2 & -3 \end{pmatrix}$$

$$\begin{matrix} \\ \\ r_3 \to r_3 - 3r_2 \\ r_4 \to r_4 - 5r_2 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & -8 & -3 \\ 0 & 0 & -8 & -3 \end{pmatrix}$$

$$\begin{matrix} \\ \\ r_3 \to r_3/8 \\ r_4 \to r_4 - r_3 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 3/8 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Therefore the sequence $((1,0,1,2),(0,1,2,0),(0,0,1,3/8))$ is a basis for S.

Since we have identified the row and column subspaces, it makes sense to think about their dimensions.

Definition 1.14 (Rank)**.** With the matrix A as above, we define the *row rank* of A to be the quantity $\dim(\mathrm{row}(A))$ and the *column rank* of A to be the quantity $\dim(\mathrm{col}(A))$. The *nullity* of the matrix A is the quantity $\dim(N(A))$ with $N(A)$ being the subspace identified in Lemma 1.8. This will be denoted $\mathrm{nullity}(A)$.

ℹ Note

We remind the reader that

$$N(A) = \{\mathbf{x} \in \mathbb{R}_{n\times 1} \mid A\mathbf{x} = \mathbf{0}\}.$$

Theorem 1.5. *The row and column rank of a matrix $A \in \mathbb{R}_{m\times n}$ are equal.*

Proof. Let R be the reduced row-echelon form of A. Then $\mathrm{row}\,(A) = \mathrm{row}\,(R)$. It is not necessarily the case that $\mathrm{row}\,(R) = \mathrm{col}\,(A)$. However what is true is that if a column of A can be written as a linear combination of the other columns, the corresponding column of R can be written as a linear combination of the other columns of R — that is the columns of R and the columns of A satisfy the *same* linear dependence relations. (The easiest way to see this is to show that if B is row equivalent to A the the columns of A and the columns of B satisfy the same linear dependence relations and apply induction.) Thus the dimension of the column space of R is equal to the dimension of the column space of A.

Now the columns of R containing the pivots of R are linearly independent and span the column space of R. Therefore, $\dim(\mathrm{row}\,(R)) = \dim(\mathrm{col}\,(R)) = \dim(\mathrm{col}\,(A))$ is precisely the number of non-zero rows of R.

□

From now on we will use the notation $\mathrm{rank}\,(A)$ to denote the column/row rank of a matrix $A \in \mathbb{R}_{m\times n}$.

Example 1.5.

Consider the matrix

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

We can compute the reduced echelon form of A, this is the matrix R below:

$$R = \begin{pmatrix} 1 & -1 & 0 & -7 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Notice that the sequence of vectors consisting of columns one and three is linearly independent and the other two columns are in the span of this sequence. Thus we see that the rank of A is 2

Set

$$c_1 := \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \quad \text{and} \quad c_2 := \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$$

and notice that c_1 and c_2 are some of the standard basis vectors of $\mathbb{R}^3$.

Let us also compute the null space of A. For this we need to solve the equation: $A\mathbf{x} = \mathbf{0}$ (note that $\mathbf{x} \in \mathbb{R}^4$ for this multiplication to be defined). Writing

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix},$$

we have $A\mathbf{x} = 0$ if and only if the following system of linear equations hold:

$$\begin{aligned} x_1 - x_2 + 2x_3 - x_4 &= 0 \\ x_1 - x_2 + 3x_3 + 2x_4 &= 0 \\ -2x_1 + 2x_2 - 3x_3 + 5x_4 &= 0 \end{aligned}$$

The matrix of coefficients is A, and we can apply row operations to reduce A to its echelon form R, therefore, we can replace the system of equations above with the following equivalent one:

$$\begin{aligned} x_1 - x_2 + 0x_3 - 7x_4 &= 0 \\ 0x_1 + 0x_2 + x_3 + 3x_4 &= 0 \end{aligned}$$

. We have two equations in 4 unknowns, so we need 2 parameters, we can choose x_2 and x_4. From the second equation $x_3 = -3x_4$; from the first: $x_1 = x_2 + 7x_4$. We have

$$N(A) := \left\{ \begin{pmatrix} x_2 + 7x_4 \\ x_2 \\ -3x_4 \\ x_4 \end{pmatrix} : x_2, x_4 \in \mathbb{R} \right\} = \operatorname{span} \left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 7 \\ 0 \\ -3 \\ 1 \end{pmatrix} \right).$$

Therefore, the nullity of A is two since

$$\left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 7 \\ 0 \\ -3 \\ 1 \end{pmatrix} \right)$$

is a basis for the null space.

Observe that $\operatorname{rank}(A) + \operatorname{nullity}(A) = 4$ which is the dimension of $\mathbb{R}^4$.

1.3 Problem Sheet 1

For the example class in Week 2.

Question R.1

Verify that the set of all positive real numbers, $\mathbb{R}_{>0}$, is a vector space over $\mathbb{R}$ when given the addition and scalar multiplication defined below:

$$x \oplus y = xy, \qquad \lambda x = x^{\lambda}$$

for all positive real numbers $x, y \in \mathbb{R}_{>0}$ and for all $\lambda \in \mathbb{R}$.

Show Solution R.1 on P131

Question R.2

Consider $\mathbb{R}^2$ with the usual addition but with scalar multiplication defined as

$$\lambda(x, y) = (\lambda x, y)$$

for all $(x, y) \in \mathbb{R}^2$, $\lambda \in \mathbb{R}$. Show that $\mathbb{R}$ equipped with the usual addition and this scalar multiplication is not a vector space.

Show Solution R.2 on P133

Question R.3

Show that the subset

$$A = \{(x, y, z) \mid x + 2y + 3z = 0\}$$

is a subspace of $\mathbb{R}^3$.

Show Solution R.3 on P134

Question R.4

Determine whether each of the following sets are subspaces of $\mathbb{R}^2$. You should either prove that the set is a subspace or provide an appropriate counterexample as to why the set does not form a subspace.

a. $A = \{(x, y) \in \mathbb{R}^2 \mid y = 2x\}$.
b. $B = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0,\ \ y \geq 0\}$.
c. $C = \{(x, y) \in \mathbb{R}^2 \mid x = 0\}$.
d. $D = \{(x, y) \in \mathbb{R}^2 \mid xy \geq 0\}$.

Show Solution R.4 on P135

Question R.5

In $\mathbb{R}_{2\times 2}$, let

$$A = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ -2 & -3 \end{pmatrix},\ C = \begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix},\ D = \begin{pmatrix} 3 & 7 \\ -1 & 8 \end{pmatrix}.$$

a. Show that $A \in \operatorname{span}(B, C, D)$.
b. Find necessary and sufficient conditions on $a, b, c, d \in \mathbb{R}$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{span}(A, B)$.

Show Solution R.5 on P136

Question R.6

For each of the following vector spaces, find a basis and hence state the dimension of the given space.

a. $C(A) = \{B \in \mathbb{R}_{2\times 2} \mid AB = BA\}$ where $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

b. $\{p \in P_5 \mid \int_0^1 p(x)dx = 0\}$.

Show Solution R.6 on P138

Question 1.1

a. Show that the sequence $B_1 = ((1,1,1),(0,1,1),(0,0,1))$ is a basis of $\mathbb{R}^3$ and find the coordinate vector of $(2,3,-1)$ with respect to the basis B_1.

b. Consider the sequence

$$B_2 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right)$$

in $\mathbb{R}_{2\times 2}$. Show that B_2 is a basis of $\mathbb{R}_{2\times 2}$. Find the coordinate vector of $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ with respect to B_2.

c. Find the coordinate vector of $p(x) = 1 + 2x - x^2$ with respect to the basis

$$(1+x, x+x^2, 1+x^2)$$

of P_2.

Show Solution 1.1 on P141

Question 1.2

Verify that the sequence $L_2 = \left(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)$ is L.I. in $\mathbb{R}_{2\times 2}$ and hence use the Exchange Lemma to extend L_2 to a basis of $\mathbb{R}_{2\times 2}$.

Show Solution 1.2 on P145

Question 1.3

Consider the subspaces

$$U = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\},$$
$$W = \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y - 3z = 0\}.$$

of $\mathbb{R}^3$.

a. Find a basis of $U \cap W$.

b. Find $\dim U$ and $\dim W$ and hence state the value of $\dim (U + W)$. Deduce that $U + W = \mathbb{R}^3$.

Show Solution 1.3 on P146

Question 1.4

Let S, T_1 and T_2 be subspaces of $\mathbb{R}^7$ such that

$$\mathbb{R}^7 = S + T_1 = S + T_2.$$

with $\dim S = 3$.

a. Use the theorem on dimension of sums of subspaces to show that $\dim T_i \geq 4$ $(i = 1, 2)$

b. Deduce that $T_1 \cap T_2 \neq \{\mathbf{0}\}$.

Show Solution 1.4 on P148

Question 1.5

Find a basis of the subspace $N(A) = \{X \in \mathbb{R}_{4\times 1} \mid AX = \mathbf{0}\}$ where

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

Show Solution 1.5 on P149

Question 1.6

Find the rank of the matrix

$$A = \begin{pmatrix} 1 & 2 & -4 \\ 2 & -1 & 2 \\ 1 & 1 & -2 \end{pmatrix}.$$

Find also the dimension of the subspace $N(A) = \{X \in \mathbb{R}_{3\times 1} \mid AX = \mathbf{0}\}$.

Show Solution 1.6 on P151

Chapter 2

Linear Mappings

2.1 Definitions

Definition 2.1 (Linear mapping)**.** Let V and W be vector spaces. A mapping $T : V \to W$ is called a *linear mapping* if

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

b. $T(\lambda \mathbf{x}) = \lambda T(\mathbf{x})$ for all $\mathbf{x} \in V$, $\lambda \in \mathcal{F}$.

! Important

Both conditions above are essential for a map to be linear: satisfying one does not imply the other! That is a. does not imply b. and b. does not imply a..

For example, consider $T : \mathbb{C} \to \mathbb{C}$ (where $\mathbb{C}$ is viewed a space over itself) defined by $T(a + ib) = a$.

Then

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

So T satisfies a.. However, T does not satisfy b. for instance

$$T(i(1+i)) = T(i-1) = -1 \neq i(1+i) = i.$$

Therefore T is not a linear mapping on $\mathbb{C}$ as a vector space over itself.

Notice that if we view $\mathbb{C}$ as a vector space over $\mathbb{R}$, then T is a linear map!

Example 2.1.

1. Let V and W be any vector spaces and $T : V \to W$ be defined by $\mathbf{x} \mapsto \mathbf{0}_w$. Then T is a linear map.
2. Fix a matrix $A \in \mathcal{F}_{m\times n}$ and define $T : \mathcal{F}_{n\times 1} \to \mathcal{F}_{m\times 1}$ by $\mathbf{x} \mapsto A\mathbf{x}$. Then T is a linear map.
3. Let V be the real vector space of all real-valued differentiable functions and define $T : V \to \mathcal{F}(\mathbb{R})$ by $f \to tof'$ where $\mathcal{F}(\mathbb{R})$ is the vector space of all real valued functions in $\mathbb{R}$. Then T is a linear map. Note that elements of V are functions for instance $\cos, \sin, \exp$; indeed $T(\cos) = -\sin$, $T(\sin) = \cos$ and $T(\exp) = \exp$.
4. Define $T : \mathbb{R}_{n\times n} \to \mathbb{R}$ by $T(A) = \operatorname{trace}(A)$. Then T is a linear map.

Lemma 2.1. *Let $T : V \to W$ be a linear mapping. Let $\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k \in V$ and $\lambda_1, \dots, \lambda_k \in F$. Then*

i. $T(\mathbf{0}_V) = \mathbf{0}_W$,

ii. $T(-\mathbf{x}) = -T(\mathbf{x}) \ \ \forall\, \mathbf{x} \in V$,

iii. $T(\lambda_1\mathbf{x}_1 + \dots + \lambda_k\mathbf{x}_k) = \lambda_1 T(\mathbf{x}_1) + \dots + \lambda_k T(\mathbf{x}_k)$.

Proof.

i. We have $T(\mathbf{0}_V) = T(\mathbf{0}_V + \mathbf{0}_V) = T(\mathbf{0}_V) + T(\mathbf{0}_V)$. Subtracting $T(\mathbf{0}_v)$ from both sides, we have $T(\mathbf{0}_V) = \mathbf{0}_V$.

ii. It was shown in Exploring Algebra and Analysis that $-\mathbf{x} = (-1)\mathbf{x}$ for any $\mathbf{x} \in V$. Using this we have, $T(-\mathbf{x}) = T((-1)\mathbf{x}) = -1T(\mathbf{x}) = -T(\mathbf{x})$.

iii. This is most easily shown by induction. For the base case, $T(\lambda_1\mathbf{x}_1) = \lambda_1 T(\mathbf{x}_1)$ follows from Definition 2.1. Assume that $T(\lambda_1\mathbf{x}_1 + \ldots + \lambda_k\mathbf{x}_k) = \lambda_1 T(\mathbf{x}_1) + \ldots + \lambda_k T(\mathbf{x}_k)$ for $\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in V$ and $\lambda_1, \ldots, \lambda_k \in F$. For the inductive step let $\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k+1} \in V$ and $\lambda_1, \ldots, \lambda_{k+1} \in F$. Then

$$\begin{aligned} T(\lambda_1\mathbf{x}_1 + \ldots + \lambda_k\mathbf{x}_k + \lambda_{k+1}\mathbf{x}_{k+1}) &= T((\lambda_1\mathbf{x}_1 + \ldots + \lambda_k\mathbf{x}_k) + \lambda_{k+1}\mathbf{x}_{k+1}) \\ &= T(\lambda_1\mathbf{x}_1 + \ldots + \lambda_k\mathbf{x}_k) + T(\lambda_{k+1}\mathbf{x}_{k+1}) \\ &= T(\lambda_1\mathbf{x}_1 + \ldots + \lambda_k\mathbf{x}_k) + \lambda_{k+1}T(\mathbf{x}_{k+1}) \\ &= \lambda_1 T(\mathbf{x}_1) + \ldots + \lambda_k T(\mathbf{x}_k) + \lambda_{k+1}T(\mathbf{x}_{k+1}). \end{aligned}$$

□

2.2 Image and Kernel

Definition 2.2 (Image)**.** Let $T : V \to W$ be a linear mapping. The *image* of T is the set

$$\text{im}\,(T) = \{T(\mathbf{x}) \mid \mathbf{x} \in V\} \subseteq W.$$

Definition 2.3 (Kernel)**.** Let $T : V \to W$ be a linear mapping. The *kernel* of T is the set

$$\text{ker}\,(T) = \{\mathbf{x} \in V \mid T(\mathbf{x}) = \mathbf{0}_W\} \subseteq V.$$

Lemma 2.2. *Let $T : V \to W$ be a linear mapping. Then*

i. im$\,(T)$ is a subspace of W.

ii. ker$\,(T)$ is a subspace of V.

Proof. We use Lemma 1.6 in both cases:

i. Since $T(\mathbf{0}_V) = \mathbf{0}_W$, then im$\,(T)$ is non-empty. Let $\mathbf{x}, \mathbf{y} \in V$. Then $T(\mathbf{x}) + T(\mathbf{y}) = T(\mathbf{x} + \mathbf{y}) \in$ im$\,(T)$. Let $\lambda \in \mathcal{F}$. Then $\lambda T(\mathbf{x}) = T(\lambda \mathbf{x}) \in$ im$\,(T)$. Therefore, im$\,(T)$ is a subspace of V

ii. As above, $T(\mathbf{0}_V) = \mathbf{0}_W$, and so $\ker(T)$ is non-empty. Let $\mathbf{x}, \mathbf{y} \in \ker(T)$ and $\lambda \in \mathcal{F}$. Then

$$T(\mathbf{x} + \mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y}) = \mathbf{0}_W + \mathbf{0}_w = \mathbf{0}_W,$$

and,

$$T(\lambda \mathbf{x}) = \lambda T(\mathbf{x}) = \lambda \mathbf{0}_W = \mathbf{0}_W.$$

Therefore $\ker(T)$ is a subspace of V.

□

Example 2.2. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear mapping given by

$$T((x_1, x_2, x_3)) = (x_1 + x_2 + 2x_3,\ 2x_1 + x_2 + x_3,\ 3x_1 - x_2 - 6x_3).$$

Find bases of im$\,(T)$ and ker$\,(T)$.

We have

$$\begin{aligned}\text{im}\,(T) &= \{(x_1+x_2+2x_3,\ 2x_1+x_2+x_3,\ 3x_1-x_2-6x_3) : x_1,x_2,x_3 \in \mathbb{R}\} \\ &= \{x_1(1,2,3)+x_2(1,1,-1)+x_3(2,1,-6) : x_1,x_2,x_3 \in \mathbb{R}\} \\ &= \operatorname{span}((1,2,3),(1,1,-1),(2,1,-6)).\end{aligned}$$

A basis for $\operatorname{span}((1,2,3),(1,1,-1),(2,1,-6))$ are the non-zero rows of a row-echelon form of the matrix below

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 1 & -1\\ 2 & 1 & -6\end{pmatrix}$$

Applying row operations, we obtain the row echelon form:

$$\begin{pmatrix}1 & 2 & 3\\ 0 & 1 & 4\\ 0 & 0 & 0\end{pmatrix}.$$

Therefore a basis for im (T) is given by the sequence $((1,2,3),(0,1,4))$. Thus, $\dim(im(T)) = 2$.

For the kernel we solve $T(x_1,x_2,x_3) = (0,0,0)$ for x_1,x_2,x_3. That is, we want to find $(x_1,x_2,x_3) \in \mathbb{R}^3$ which satisfy the system of linear equations

$$\begin{aligned}x_1+x_2+2x_3 &= 0\\ 2x_1+x_2+x_3 &= 0\\ 3x_1-x_2-6x_3 &= 0.\end{aligned}$$

We form the augmented matrix

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

Applying row operations:

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

Reading off the solutions we see that $x_2 = -3x_3$ and $x_1 = x_3$. Therefore

$$\ker(T) = \{(x_3, -3x_3, x_3) : x_3 \in \mathbb{R}\} = \operatorname{span}((1, -3, 1)).$$

Thus, $\dim(\ker(T)) = 1$.

Notice that $\dim(\text{im}\,(T)) + \dim(\ker(T)) = 3 = \dim(\mathbb{R}^3)$.

Lemma 2.3. *Let $T : V \to W$ be a linear mapping. Then T is injective if and only if ker$(T) = \{\mathbf{0}_V\}$.*

Proof. Suppose that T is injective. Then for any $\mathbf{v} \in V$, $T(\mathbf{v}) = \mathbf{0}_W$ if and only if $\mathbf{v} = \mathbf{0}_V$ since $T(\mathbf{0}_V) = \mathbf{0}_W$. Hence ker $(T) = \{\mathbf{0}_V\}$.

Suppose ker $(T) = \{\mathbf{0}_V\}$. Let $\mathbf{x}, \mathbf{y} \in V$ be such that $T(\mathbf{x}) = T(\mathbf{y})$. Then $T(\mathbf{x}) - T(\mathbf{y}) = \mathbf{0}_W$. Using the fact that T is a linear map this means that

$$T(\mathbf{x} - \mathbf{y}) = \mathbf{0}_W.$$

Therefore $\mathbf{x} - \mathbf{y} \in$ ker $(T) = \{\mathbf{0}_V\}$. We conclude that $\mathbf{x} - \mathbf{y} = \mathbf{0}_V$ and so $\mathbf{x} = \mathbf{y}$.

□

Lemma 2.4. *Let $T : V \to W$ be a linear mapping and suppose that V is finite dimensional. Then im (T) is also finite dimensional.*

Proof. Since V is finite dimensions, it has a finite basis $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$.

It suffices to show that im (T) is spanned by $(T(\mathbf{x}_1), T(\mathbf{x}_2), \dots, T(\mathbf{x}_n))$ since this will imply that the size of any linearly independent subset of im (T) is at most n.

Let $\mathbf{w} \in$ im (T), there is some $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \mathbf{w}$. Since $\mathbf{v} \in V$, we can find $a_1, a_2, \dots, a_n \in \mathcal{F}$ such that

$$\mathbf{v} = a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \dots + a_n\mathbf{x}_n.$$

We therefore have:

$$\begin{aligned} \mathbf{w} = T(\mathbf{v}) &= T(a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \dots + a_n\mathbf{x}_n) \\ &= a_1T(\mathbf{x}_1) + a_2T(\mathbf{x}_2) + \dots + a_nT(\mathbf{x}_n) \end{aligned}$$

where the second equality follows from the linearity of T. Therefore $\mathbf{w}$ is n element of $\mathrm{span}\,((T(\mathbf{x}_1), T(\mathbf{x}_2), \dots, T(\mathbf{x}_n)))$.

□

Definition 2.4 (Rank, Nullity)**.** Let $T : V \to W$ be a linear mapping with V finite dimensional. The quantity $\dim$ (im (T)) is called the *rank* of T and will be denoted $\mathrm{rank}\,(T)$. The quantity $\dim$ (ker (T)) is called the *nullity* of T and will be denoted $\mathrm{nullity}\,(T)$.

ℹ Note

The kernel of T is finite dimensional since it is a subspace of V which is finite dimensional by assumption.

Theorem 2.1 (Rank-Nullity Theorem). *Let $T : V \to W$ be a linear mapping with V finite dimensional. Then*

$$\operatorname{rank}(T) + \operatorname{nullity}(T) = \dim(V).$$

Proof. Since ker (T) is a finite dimensional subspace of V, there is a basis $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m)$ forker (T). We can extend this basis to a basis $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m, \mathbf{x}_{m+1}, \dots, \mathbf{x}_{m+n})$ for V by Theorem 1.3.

We claim that $(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n}))$ is a basis for im (T).

We note that $\operatorname{span}(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n}))$ is equal im (T).

Clearly $\operatorname{span}(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n})) \subseteq$ im (T).

Now let $\mathbf{w} \in$ im (T), we can find $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \mathbf{w}$. There are $a_1, a_2, \dots, a_{m+n} \in \mathcal{F}$ such that

$$\mathbf{v} = a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \dots + a_m\mathbf{x}_m + a_{m+1}\mathbf{x}_{m+1} + \dots + a_{m+n}\mathbf{x}_{m+n}.$$

We have:

$$\begin{aligned}
\mathbf{w} = T(\mathbf{v}) &= T(a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \dots + a_m\mathbf{x}_m + a_{m+1}\mathbf{x}_{m+1} + \dots + a_{m+n}\mathbf{x}_{m+n}) \\
&= a_1T\mathbf{x}_1) + a_2T(\mathbf{x}_2) + \dots + a_mT(\mathbf{x}_m) + a_{m+1}T(\mathbf{x}_{m+1}) + \dots + a_{m+n}T(\mathbf{x}_{m+n}) \\
&= a_1\mathbf{0}_W + a_2\mathbf{0}_W + \dots + a_m\mathbf{0}_W + a_{m+1}T(\mathbf{x}_{m+1}) + \dots + a_{m+n}T(\mathbf{x}_{m+n}) \\
&= a_{m+1}T(\mathbf{x}_{m+1}) + \dots + a_{m+n}T(\mathbf{x}_{m+n}).
\end{aligned}$$

Hence $\mathbf{w} \in \mathrm{span}\,(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n}))$. Since $\mathbf{w} \in$ im (T) was arbitrarily chosen, we conclude that im $(T) \subseteq \mathrm{span}\,(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n}))$. Thus, $\mathrm{span}\,(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n})) =$ im (T).

Now suppose that there are elements $b_1, b_2, \dots, b_n \in \mathcal{F}$ such that

$$b_1 T(\mathbf{x}_{m+1}) + \dots + b_n T(\mathbf{x}_{m+n}) = \mathbf{0}_W.$$

Then, by linearity, we have

$$T(b_1\mathbf{x}_{m+1} + \dots + b_n\mathbf{x}_{m+n}) = \mathbf{0}_W.$$

Therefore, $b_1\mathbf{x}_{m+1} + \dots + b_n\mathbf{x}_{m+n} \in$ ker (T). This means that $b_1\mathbf{x}_{m+1} + \dots + b_n\mathbf{x}_{m+n}$ can also be expressed as a linear combination of the sequence $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m)$. However, since $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m, \mathbf{x}_{m+1}, \dots, \mathbf{x}_{m+n})$ this only happens precisely when $b_1 = b_2 \dots = b_n = \mathbf{0}$. This shows that the sequence $(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n}))$ is linearly independent.

Therefore $(T(\mathbf{x}_{m+1}), \dots, T(\mathbf{x}_{m+n}))$ is a basis for im (T) and $\dim$ (im $(T)) = n$.

Putting the above together, we have

$$\dim(V) = m + n = \dim(\ker(T)) + \dim(\text{im}\,(T))$$

as required.

□

Lemma 2.5. *Let $T : V \to W$ be a linear mapping. Then T is injective if and only if* $\mathrm{nullity}\,(T) = 0$.

Proof. This is a consequence of Lemma 2.3 since $\mathrm{nullity}\,(T) = \dim(\ker(T))$ and the dimension of subspace $\{\mathbf{0}_V\}$ is zero.

$\square$

Lemma 2.6. *Let $T : V \to W$ be a linear mapping with V and W finite dimensional. Then T is surjective if and only if* $\operatorname{rank}(T) = \dim(W)$.

Proof. If $\operatorname{rank}(T) = \dim(W)$, then $\dim(\text{im}(T)) = \dim(W)$. Therefore $\text{im}(T) = W$ since $\text{im}(T)$ is a subspace of W of the same dimension as W.

$\square$

Example 2.3. Find the kernel of the linear mapping $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T((a, b)) = (2a - b, a + 2b)$$

for all $(a, b) \in \mathbb{R}^2$. Deduce from the Rank-Nullity Theorem that T is a bijection.

If T is bijective then it is injective and consequently must satisfy $\ker(T) = \{(0, 0)\}$. A good place to start is to verify this.

Suppose $(a, b) \in \ker(T)$. Then $T((a, b)) = (2a - b, a + 2b) = (0, 0)$. We deduce that $a = b/2$, using this in the second coordinate, $5/2b = 0$ and so $b = a = 0$. It follows that $\ker(T) = \{(0, 0)\}$ and T is injective.

Now we use the Rank-Nullity Theorem (Theorem 2.1):

$$2 = \dim(\mathbb{R}^2) = \operatorname{rank}(T) + \operatorname{nullity}(T) = \operatorname{rank}(T) + 0.$$

We conclude that $\dim(\text{im}(T)) = 2$. This means that $\text{im}(T) = \mathbb{R}^2$ and so T is surjective.

We conclude that T is a bijection.

Example 2.4. Find the kernel of the linear mapping $T : P_2 \to \mathbb{R}^2$ defined by

$$T(p(x)) = (p(0), p(1))$$

for all $p \in P_2$. Hence state the nullity and rank of T.

Let $g := ax^2 + bx + c \in \mathsf{ker}\,(T)$. Then $T(g) = (c, b+c) = (0, 0)$. It follows that $c = b = 0$. Therefore $\mathsf{ker}\,(T) = \{ax^2 : a \in \mathbb{R}\}$.

Thus $\mathrm{nullity}\,(T) = \dim(\mathsf{ker}\,(T)) = 1$ since $\mathsf{ker}\,(T)$ is spanned by the x^2.

Using the fact that $\dim(P_2) = 3$, by the Rank-Nullity Theorem, we have:

$$\mathrm{rank}\,(T) = \dim(P_2) - \dim(\mathsf{ker}\,(T)) = 3 - 1 = 2.$$

Notice that $\mathsf{im}\,(T) = \mathbb{R}^2$ and T is surjective.

2.3 Matrices from Linear Mappings

Throughout this section, V and W will denote non-zero, finite dimensional vector spaces over the field $\mathcal{F}$.

In this section we are concerned with representing a given linear mapping $T : V \longrightarrow W$ by a matrix M_T which in some sense corresponds to T.

Definition 2.5. Let $T : V \to W$ be a linear mapping and let $n = \dim(V)$ and $m = \dim(W)$. Let $L_V = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ be a basis of V and let $L_W = (\mathbf{f}_1, \dots, \mathbf{f}_m)$ be a basis of W. We define the matrix of T with respect to L_V and L_W to be the $m \times n$ matrix whose k^{th} column is the coordinate vector of $T(\mathbf{e}_k)$ with respect to L_W. We will denote this matrix by $M(T; L_V, L_W)$ or M_T when there is no doubt about which bases of V and W we are using.

Lemma 2.7. *Let $T : V \to W$, $L_V = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ and $L_W = (\mathbf{f}_1, \dots, \mathbf{f}_m)$ be as in the above definition. Let $M_T = (a_{ik})$ in our usual matrix notation (so that the $(i,k)^{th}$ entry of the matrix M_T is the scalar a_{ik}). Then,*

a. M_T is a $m \times n$ matrix i.e. a $(\dim(W)) \times (\dim(V))$ matrix.

b. For each $\mathbf{e}_k$ in L_V, $T(\mathbf{e}_k) = \sum_{i=1}^{m} a_{ik}\mathbf{f}_i$.

c. For every $\mathbf{x} \in V$,

(coordinate column vector of $T(\mathbf{x})$ with respect to L_W)=M_T×(coordinate column vector of $\mathbf{x}$ with respect to L_V).

d. If an $m \times n$ matrix N is such that

(coordinate column vector of $T(\mathbf{x})$ with respect to L_W)=N×(coordinate column vector of $\mathbf{x}$ with respect to L_V),

then $N = M_T$.

Proof.

a. This is a consequence of the definition. Since L_V has n elements, then M_T has n-columns, since L_W has m elements M_T has m-rows.

b. By definition the k^{th} column of M_T is the coordinate vector of $T(e_k)$ with respect to L_W, by definition then,

$$T(e_k) = \sum_{i=1}^{m} a_{ik}\mathbf{f}_i.$$

c. Let $\mathbf{x} \in V$, and suppose $(x_1, x_2, \dots, x_n)$ is the coordinate vector of $\mathbf{x}$ with respect to L_V. Thus,

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

Applying the map T, we have:

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

Using the fact that $T(\mathbf{e}_i) = \sum_{k=1}^{m} a_{ki}\mathbf{f}_k$, we have

$$\begin{aligned} T(\mathbf{x}) = \sum_{i=1}^{n} x_i T(\mathbf{e}_i) &= \sum_{i=1}^{n} x_i \sum_{k=1}^{m} a_{ki}\mathbf{f}_k \\ &= \sum_{i=1}^{n}\sum_{k=1}^{m} a_{ki}x_i\mathbf{f}_k \\ &= \sum_{k=1}^{m}\left(\sum_{i=1}^{n} a_{ki}x_i\right)\mathbf{f}_k. \end{aligned}$$

For $1 \leq k \leq m$ set $y_k = \sum_{i=1}^{n} a_{ki}x_i$ and observe that $(y_1, y_2, \ldots, y_m)$ is the coordinate vector with respect to L_W of $T(\mathbf{x})$.

Now notice that

$$M_T \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} a_{1i}x_i \\ \sum_{i=1}^{n} a_{2i}x_i \\ \vdots \\ \sum_{i=1}^{n} a_{mi}x_i \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

d. Let $\mathbf{E}_i \in \mathcal{F}_{n\times 1}$ be the coordinate vector of $\mathbf{e}_i$ with respect to L_V written as a column vector. Notice that $\mathbf{E}_i$ has entries 0 everywhere and 1 in row i. It follows, writing N_{ij} for the ij^{th} entry of the matrix N, that

$$N\mathbf{E}_i = \begin{pmatrix} N_{1i} \\ N_{2i} \\ \vdots \\ N_{mi} \end{pmatrix} = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{pmatrix} = M_T\mathbf{E}_i.$$

It follows that $N_{ij} = a_{ij}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$.

□

Example 2.5. Consider the linear mapping $T : \mathbb{R}^3 \to \mathbb{R}^2$ defined by

$$T((x_1, x_2, x_3)) = (x_1 + 2x_2 + 3x_3,\ 4x_1 + 5x_2 + 6x_3).$$

Find the matrix M_T of the linear mapping T with respect to the standard bases of $\mathbb{R}^3$ and $\mathbb{R}^2$.

The standard basis for $\mathbb{R}^3$ is

$$L_{\mathbb{R}^3} = ((1,0,0),(0,1,0),(0,0,1)) = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_2)$$

and for $\mathbb{R}^2$ the standard basis is

$$L_{\mathbb{R}^2}((1,0),(0,1)) = (\mathbf{f}_1, \mathbf{f}_2).$$

For each i between 1 and 3 we need to find the coordinate vector of $T(\mathbf{e}_i)$ with respect to $L_{\mathbb{R}^2}$. We have

$$\begin{aligned} T(\mathbf{e}_1) &= (1,4) = 1\mathbf{f}_1 + 4\mathbf{f}_2 \\ T(\mathbf{e}_2) &= (2,5) = 2\mathbf{f}_1 + 5\mathbf{f}_2 \\ T(\mathbf{e}_3) &= (3,6) = 3\mathbf{f}_1 + 6\mathbf{f}_2 \end{aligned}$$

So the matrix of T with respect to $L_{\mathbb{R}^3}$ and $L_{\mathbb{R}^2}$ is:

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

Example 2.6. Consider the linear mapping $T : P_2 \to P_2$ defined by

$$T(p(x)) = p(2x-1).$$

for all $p \in P_2$.

a. Find M_T with respect to the basis $(1, x, x^2)$ of P_2.

b. Use part a. to compute $T(3+2x-x^2)$. Verify your answer directly.

a. We proceed as in Example 2.5, we have:

$$\begin{aligned} T(1) &= 1 = 1 + 0x + 0x^2 \\ T(x) &= 2x-1 = (-1)1 + 2x + 0x^2 \\ T(x^2) &= 1 - 4x + 4x^2. \end{aligned}$$

Therefore the matrix of T with respect to the standard basis of P_2 is:

$$M_T = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & -4 \\ 0 & 0 & 4 \end{pmatrix}.$$

b. We use M_T to carry out this computation. We first find the coordinate vector of $3+2x-x^2$ with respect to the standard basis of P_2. This is $(3, 2, -1)$. Next we carry out the computation

$$M_T \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 8 \\ -4 \end{pmatrix}.$$

The element $(0, 8, -4)$ now gives the coordinate vector of $T(3+2x-x^2)$. It follows that $T(3+2x-x^2) = 8x - 4x^2$.

We can verify this directly:

$$\begin{aligned} T(3+2x-x^2) &= 3+2(2x-1)-(2x-1)^2 \\ &= (3-2-1)+(4+4)x-4x^2 \\ &= 0+8x-4x^2. \end{aligned}$$

Lemma 2.8. *Let* $\dim(V) = n$ *and* $\dim(W) = m$. *Let* L_V *and* L_W *be given bases of* V *and* W *and let* A *be an arbitrary matrix in* $\mathcal{F}_{m\times n}$. *Then there is precisely one linear mapping* $T : V \to W$ *such that* $M(T; L_V, L_W) = A$.

Proof. Let $L_V = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ and $L_W = (\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_m)$. We define a linear map $T : V \to W$ by specifying its action on the basis elements of V. For $1 \leq i \leq n$ set:

$$T(e_i) = \sum_{k=1}^{m} a_{ki}\mathbf{f}_k.$$

Clearly $A = M_T$.

If $S : V \to W$ is a linear map such that $M_S = M_T = A$, then for $1 \leq i \leq n$

$$S(e_i) = \sum_{k=1}^{m} a_{ki}\mathbf{f}_k = T(e_i).$$

It follows that $S = T$.

□

2.4 Change of Basis

Let V be a finite dimensional vector space with $\dim(V) = n$. Let $L_1 = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ be a basis of V. Let $L_2 = (\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_n)$ be a sequence of vectors in V. We might ask the important question "When is L_2 a basis of V?" We *know* that L_1 is a basis of V, so we can express each $\mathbf{f}_j$ as a linear combination of the $\mathbf{e}_i$. For example,

$$\mathbf{f}_1 = \lambda_{1,1}\mathbf{e}_1 + \lambda_{1,2}\mathbf{e}_2 + \ldots + \lambda_{1,n}\mathbf{e}_n.$$

In this way we get a linear mapping $T : V \to V$. The sequence L_2 forms a basis of V if and only if we can express each $\mathbf{e}_i$ as a linear combination of the $\mathbf{f}_j$ (by the "two out of three" rule) and this happens if and only if there is a linear mapping $S : V \to V$ going 'the other way'. In particular, in this case $ST = id$ (this makes sense as S and T are functions, so can be composed) and using the matrices for these maps we have $M_S M_T = I_n$, that is, M_T is invertible. So, L_2 forms a basis of V if and only if M_T is invertible.

Definition 2.6. Let V be a vector space with $\dim(V) = n$ and let $L_1 = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ and $L_2 = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ be two bases of V. The *change of basis* matrix from L_1 to L_2 is the $n \times n$ matrix whose k^{th} column is the coordinate vector of $\mathbf{f}_k$ with respect to L_1. We denote this matrix by $M(L_1 \to L_2)$.

Lemma 2.9. *Let V have bases L_1 and L_2 and let $P = M(L_1 \to L_2)$. Let an arbitrary vector $\mathbf{x} \in V$ have coordinate vectors X_1 and X_2 with respect to L_1 and L_2 respectively. Then $X_1 = PX_2$.*

Proof. Consider the map $\mathrm{id} : V \to V$ by $\mathrm{id}(\mathbf{x}) = \mathbf{x}$. This is a linear map.

Also observe that P is precisely the matrix $M(\mathrm{id}; L_W, L_V)$.

Let $\mathbf{x} \in V$ and let X_1 and X_2 be the coordinate vectors of $\mathbf{x}$ with respect to L_1 and L_2.

By Lemma 2.7 part c. the coordinate vector X_1 is precisely $M(\mathrm{id}; L_W, L_V)X_2 = PX_2$ since $\mathrm{id}(\mathbf{x}) = \mathbf{x}$.

□

Example 2.7. Let $B_1 = (1, x, x^2, x^3)$ be the standard basis of the space P_3 and let B_2 be the basis (p_1, p_2, p_3, p_4) where

$$p_1 = 1, \quad p_2 = x - 1, \quad p_3 = x^2 - x + 1, \quad p_4 = x^3 - x^2 + x - 1.$$

Find the change of basis matrix $M(B_2 \to B_1)$. Use this matrix to express the polynomial $1 + x + x^2 + x^3$ as a linear combination of the vectors in the basis B_2.

We express the vectors B_1 as a linear combination of those in B_2:

$$\begin{aligned} 1 &= p_1 + 0p_2 + 0p_3 + 0p_4 \\ x &= p_1 + p_2 + 0p_3 + 0p_4 \\ x^2 &= 0p_1 + p_2 + p_3 + 0p_4 \\ x^3 &= 0p_1 + 0p_2 + p_3 + p_4. \end{aligned}$$

The matrix $M(B_2 \to B_1)$ is therefore equal to

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

To express $1 + x + x^2 + x^3$ as a linear combination of the vectors in basis B_2 we find its coordinate vectors in terms of B_1 and pre-multiply it by $M(B_2 \to B_1)$

$$M(B_2 \to B_1) \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \\ 1 \end{pmatrix}.$$

Therefore, $2p_1 + 2p_2 + 2p_3 + p_4$ is the expression for $1 + x + x^2 + x^3$ in the basis B_2.

We can verify this:

$$\begin{aligned} 2p_1 + 2p_2 + 2p_3 + p_4 &= 2 + 2(x-1) + 2(x^2 - x + 1) + (x^3 - x^2 + x - 1) \\ &= (2 - 2 + 2 - 1) + (2 - 2 + 1)x + (2-1)x^2 + x^3 \\ &= 1 + x + x^2 + x^3. \end{aligned}$$

Lemma 2.10. *Let $T : V \to W$ be a linear mapping. Let L_1 and L_2 be two bases of V and let K_1 and K_2 be two bases of W. Set $A = M(T; L_1, K_1)$ and $B = M(T; L_2, K_2)$. Then*

$$B = R^{-1}AP$$

where $P = M(L_1 \to L_2)$ and $R = M(K_1 \to K_2)$.

Proof. Let $\mathbf{x} \in V$. Let X_1 and X_2 be the coordinate vectors of $\mathbf{x}$ with respect to the basis L_1 and L_2. Similarly let Y_1 and Y_2 be the coordinate vectors of $\mathbf{y} = T(\mathbf{x})$ with respect to the coordinate vectors K_1 and K_2.

By Lemma 2.7, $Y_1^t = AX_1^t$ and $Y_2^t = BX_2^t$. By Lemma 2.9 $Y_1^t = RY_2^t$ and $X_1 = PX_2^t$. Putting all these together we have:

$$Y_2^t = RY_1^t = APX_2^t$$

Meaning that $BX_2^t = Y_2^t = (R^{-1}AP)X_2^t$.

By Lemma 2.7 part d. $B = R^{-1}AP$.

□

Corollary 2.1. *Let $T : V \to V$ be a linear mapping and let L_1 and L_2 be two bases of V. Set $A = M(T; L_1)$ and $B = M(T; L_2)$. Then $B = P^{-1}AP$ where $P = M(L_1 \to L_2)$.*

Proof. This is a consequence of Lemma 2.10 with $V = W$.

□

Corollary 2.2. *Let $T : V \to V$ be a linear mapping and let A be the matrix of T with respect to some particular basis of V. Then the set of all matrices arising as the matrices of T with respect to the different possible bases of V is the set of matrices similar to A.*

> **i** Note
>
> Let A and B be $n \times n$ matrices. Then B is *similar* to A if and only if there is a nonsingular matrix P such that $B = P^{-1}AP$.

Example 2.8. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear mapping defined by

$$T((x, y)) = (5x - 4y, 3x - 2y).$$

Find the matrix of T with respect to the standard basis of $\mathbb{R}^2$ and use this to find the matrix of T with respect to the basis $((1,1),(4,3))$ of $\mathbb{R}^2$.

Let $L_1 = ((1,0),(0,1))$ be the standard basis for $\mathbb{R}^2$ and write L_2 for the basis $((1,1),(4,3))$.

We calculate $M(T;L_1)$ in the usual way:

$$\begin{aligned} T((1,0)) &= (5,3) = 5(1,0) + 3(0,1) \\ T((0,1)) &= (-4,-2) = -4(1,0) - 2(0,1). \end{aligned}$$

Therefore

$$M(T;L_1) = \begin{pmatrix} 5 & -4 \\ 3 & -2 \end{pmatrix}.$$

The matrix $M(T;L_2)$ is precisely $P^{-1}M(T;L_1)P$ where P is the matrix $M(L_1 \to L_2)$. We compute P as follows. First we express the elements of L_2 inn terms of L_1.

$$\begin{aligned} (1,1) &= 1(1,0) + 1(0,1) \\ (4,3) &= 4(1,0) + 3(0,1). \end{aligned}$$

The matrix P can now be computed as

$$\begin{pmatrix} 1 & 4 \\ 1 & 3 \end{pmatrix}.$$

We have:

$$M(T;L_2) = P^{-1}M(T;L_1)P = \begin{pmatrix} -3 & 4 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 5 & -4 \\ 3 & -2 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

2.5 Eigenvalues and Eigenvectors

In this section we connect knowledge of matrices with our new knowledge of the link between linear mappings and matrices. We saw in the last section that the matrices which arise as the matrix of a linear transformation with respect to different bases is just the set of all matrices similar to a given matrix of the transformation. Now recall the final result from Algebra:

Lemma 2.11. *Let A and B be $n \times n$ matrices which are similar. Then:*

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

ii. $\chi_A(t) = \chi_B(t)$.

iii. *A and B have the same eigenvalues.*

iv. *A is nonsingular if and only if B is nonsingular.*

Proof. Notice that iii. is a consequence of ii. and iv. is a consequence of i.

It remains to demonstrate i. and ii. Let P be such that $B = P^{-1}AP$, then

i.

$$\begin{aligned} \det(P^{-1}AP) &= \det(P^{-1})\det(A)\det(P) \\ &= \frac{1}{\det(P)}\det(A)\det(P) \\ &= \det(A). \end{aligned}$$

ii.

$$\begin{aligned}
\lambda_B(t) &= \det(B - xI) \\
&= \det(P^{-1}AP - tI) \\
&= \det(P^{-1}AP - P^{-1}tIP) \\
&= \det(P^{-1}(A - tI)P) \\
&= \det(P^{-1})\det(A - tI)\det(P) \\
&= \det(A - tI) = \lambda_A(t).
\end{aligned}$$

□

Definition 2.7. Let V be a non-zero, finite dimensional vector space and let $T : V \to V$ be a linear transformation. The characteristic polynomial $\chi_T(t)$ is the characteristic polynomial of each and every matrix representing T.

Definition 2.8 (Eigenvalue and eigenvector)**.** Let $T : V \to V$ be a linear transformation. We say that a scalar $\lambda \in \mathcal{F}$ is an *eigenvalue* of T if there exists a non-zero vector $\mathbf{x} \in V$ such that $T(\mathbf{x}) = \lambda\mathbf{x}$. When this is the case, we say that the vector $\mathbf{x}$ is an *eigenvector* of T corresponding to the eigenvalue λ.

Example 2.9. Find the eigenvalues and corresponding eigenvectors of the linear transformation $T : \mathbb{C}^2 \to \mathbb{C}^2$ defined by

$$T((x, y)) = (2x + y,\ 2x + 3y).$$

Let $B = ((1,0),(0,1))$ be the standard basis for $\mathbb{C}^2$. We compute M_T the matrix of T with respect to the basis B:

$$T((1,0)) = (2,2), \quad T((0,1)) = (1,3),$$

Therefore,

$$M_T = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}.$$

Now,

$$\begin{aligned} \chi_T(t) = \chi_{M_T}(t) = |tI - M| &= \\ \begin{vmatrix} t-2 & -1 \\ -2 & t-3 \end{vmatrix} &= (t-2)(t-3) - 2 \\ &= t^2 - 5t + 4 = (t-4)(t-1). \end{aligned}$$

Therefore the eigenvalues of T are 1 and 4.

To find the eigenvectors corresponding to an eigenvalue λ, we find all vectors $\mathbf{x}$ which are solutions to $(tI - M_T)\mathbf{x} = \mathbf{0}$. We take each eigenvalue in turn.

$\lambda_T = 1$**:** We solve $(I - M_T)\mathbf{x} = \mathbf{0}$ for $X = \begin{pmatrix} x \\ y \end{pmatrix}$

$$(I - M)\mathbf{x} = \begin{pmatrix} -1 & -1 \\ -2 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix}) \\ ) \end{pmatrix}.$$

The Augmented matrix is:

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

The second row is a multiple of the first thus we have one equation $x + y = 0$.

Therefore, the set of solutions is:

$$\left\{ \begin{pmatrix} -y \\ y \end{pmatrix} : y \in \mathbb{C} \right\} = \operatorname{span}\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix} \right).$$

It follows that the eigenvectors of T corresponding to the eigenvalue 1 are all non-zero vectors in $\operatorname{span}((1,-1))$.

$\lambda_t = 4$**:** We proceed as before. We solve $(4I - M_T)\mathbf{x} = \mathbf{0}$ for $\mathbf{x}$. This time the augmented matrix is:

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

Again the second row is a multiple of the first, thus we have one equation: $2x - y = 0$. The eigenvectors of M_T corresponding to the eigenvalue 4 are all non-zero vectors in

$$\operatorname{span}\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \right).$$

It follows that the eigenvectors of T corresponding to eigenvalue 4 are the non-zero vectors in $\operatorname{span}((1,2))$.

Now, let $T : V \to V$ be a linear transformation, where V is a finite dimensional vector space over some field $\mathcal{F}$. Fix an eigenvalue, λ of T and let

$$E(\lambda, T) = \{\mathbf{v} \in V \mid T(\mathbf{v}) = \lambda\mathbf{v}\}.$$

(Note that $\mathbf{0} \in E(\lambda, T)$ even though it is not an eigenvector by the definition.) If $\mathbf{u}, \mathbf{v} \in E(\lambda, T)$ then

$$\begin{aligned} T(\mathbf{u} + \mathbf{v}) &= T(\mathbf{u}) + T(\mathbf{v}) && T \text{ is linear} \\ &= \lambda\mathbf{u} + \lambda\mathbf{v} && \mathbf{u}, \mathbf{v} \in E(\lambda, T) \\ &= \lambda(\mathbf{u} + \mathbf{v}). \end{aligned}$$

So, $\mathbf{u}+\mathbf{v} \in E(\lambda, T)$ and hence $E(\lambda, T)$ is closed under addition. Similarly, if $\mathbf{v} \in E(\lambda, T)$ and $\mu \in F$, then

$$\begin{aligned} T(\mu\mathbf{v}) &= \mu T(\mathbf{v}) && T \text{ is linear} \\ &= \mu(\lambda\mathbf{v}) && \mathbf{v} \in E(\lambda, T) \\ &= \lambda(\mu\mathbf{v}). \end{aligned}$$

So, $\mu\mathbf{v} \in E(\lambda, T)$ and hence $E(\lambda, T)$ is closed under scalar multiplication. It then follows that $E(\lambda, T)$ is a subspace of V and so the set of all eigenvectors of T corresponding to λ, together with the zero vector, forms a vector space.

Definition 2.9 (Eigenspace)**.** Let $T : V \to V$ be a linear transformation and let λ be an eigenvalue of T. Then the set

$$E(\lambda, T) = \{\mathbf{x} \in V \mid T(\mathbf{x}) = \lambda\mathbf{x}\}$$

is called the *eigenspace* of T corresponding to λ.

Lemma 2.12. *Let $T : V \to V$ be a linear transformation and let λ and μ be different eigenvalues of T. Then $E(\lambda, T) \cap E(\mu, T) = \{\mathbf{0}\}$.*

Proof. Suppose $\mathbf{x} \in E(\lambda, T) \cap E(\mu, T)$. Then

$$\lambda\mathbf{x} = T(\mathbf{x}) = \mu\mathbf{x}.$$

It follows that $(\lambda - \mu)\mathbf{x} = \mathbf{0}$. Since $\lambda - \mu \neq 0$ (as $\lambda \neq \mu$), then $\mathbf{x}$ must be $\mathbf{0}$ as required.

□

Corollary 2.3. *Let $T : V \to V$ be a linear transformation and let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be different eigenvalues of T. Let $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be eigenvectors of T corresponding to the eigenvalues $\lambda_1, ..., \lambda_n$ respectively. Then the sequence $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is linearly independent.*

Proof. We prove this by induction.

The base case occurs when $n = 1$. The result trivially holds for this case since a single eigenvector is linearly independent (eigenvectors are non-zero).

Assume that for $\lambda_1, \lambda_2, \ldots, \lambda_n$ different eigenvalues of T and $\mathbf{x}_1, \ldots, \mathbf{x}_n$ eigenvectors of T corresponding to the eigenvalues $\lambda_1, \ldots, \lambda_n$ respectively, the sequence $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is linearly independent.

Now let $\lambda_1, \lambda_2, \ldots, \lambda_{n+1}$ be different eigenvalues of T and $\mathbf{x}_1, \ldots, \mathbf{x}_{n+1}$ eigenvectors of T corresponding to the eigenvalues $\lambda_1, ..., \lambda_{n+1}$.

Suppose there are scalars $a_1, a_2, \ldots, a_{n+1} \in \mathcal{F}$ such that

$$a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + ... + a_{n+1}\mathbf{x}_{n+1} = \mathbf{0}. \tag{2.1}$$

Rearranging we have:

$$a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + ... + a_n\mathbf{x}_n = -a_{n+1}\mathbf{x}_{n+1}. \tag{2.2}$$

Applying the map T:

$$T(a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + ... + a_n\mathbf{x}_n) = T(-a_{n+1}\mathbf{x}_{n+1}).$$

Using linearity:

$$a_1T(\mathbf{x}_1) + a_2T(\mathbf{x}_2) + ... + a_nT(\mathbf{x}_n) = -a_{n+1}T(\mathbf{x}_{n+1}).$$

Noting that $\mathbf{x}_i$ is an eigenvector with eigenvalue λ_i, we have

$$a_1\lambda_1\mathbf{x}_1 + a_2\lambda_2\mathbf{x}_2 + \ldots + a_n\lambda_n T(\mathbf{x}_n) = -a_{n+1}\lambda_{n+1}\mathbf{x}_{n+1}. \tag{2.3}$$

There are two possibilities either $\lambda_{n+1} = 0$ or $\lambda_{n+1} \neq 0$.

$\lambda_{n+1} = 0$: In this case $\lambda_i \neq 0$ for any $1 \leq i \leq n$ (since the eigenvalues are distinct). In particular:

$$a_1\lambda_1\mathbf{x}_1 + a_2\lambda_2\mathbf{x}_2 + \ldots + a_n\lambda_n T(\mathbf{x}_n) = \mathbf{0}.$$

However, since $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ is linearly independent, $a_i\lambda_i = 0$ for all $1 \leq i \leq n$. We conclude that $a_i = 0$ for all $1 \leq i \leq n$ since $\lambda_i \neq 0$. Equation 2.1 now implies that $a_{n+1} = 0$ as well. We conclude that the sequence $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{n+1})$ is linearly independent.

$\lambda_{n+1} \neq 0$: Dividing Equation 2.3 by λ_{n+1} and subtracting Equation 2.2 we have

$$a_1\left(\frac{\lambda_1}{\lambda_{n+1}} - 1\right)\mathbf{x}_1 + a_2\left(\frac{\lambda_2}{\lambda_{n+1}} - 1\right)\mathbf{x}_2 + \ldots + a_n\left(\frac{\lambda_n}{\lambda_{n+1}} - 1\right)\mathbf{x}_n = \mathbf{0}.$$

By The inductive assumption it must be the case that $a_i\left(\frac{\lambda_i}{\lambda_{n+1}} - 1\right) = 0$ for all $1 \leq i \leq n$. Now since $\lambda_i \neq \lambda_{n+1}$ for $1 \leq i \leq n$, it follows that $\frac{\lambda_i}{\lambda_{n+1}} \neq 1$ and so $\frac{\lambda_i}{\lambda_{n+1}} - 1 \neq 0$. Therefore $a_i = 0$ for all $1 \leq i \leq n$. As in the previous case, we conclude that $a_{n+1} = 0$ as well and the sequence $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{n+1})$ is linearly independent.

□

2.6 Diagonalisation

Lemma 2.13. *Let $T : V \to V$ be a linear transformation of a finite dimensional vector space over $\mathbb{C}$ and let $L = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ be a basis of V. Then the following statements are equivalent:*

1. *$M(T;L) = \operatorname{diag}(\alpha_1, ..., \alpha_n)$;*
2. *$\alpha_1, \dots, \alpha_n$ are eigenvalues of T and for each k, $\mathbf{e}_k$ is an eigenvector of T corresponding to the eigenvalue α_k.*

Proof. The proof below is unexaminable.

Suppose $M(T;L) = \operatorname{diag}(a_1, \dots, a_n)$. Then as column i of $M(T;L)$ is the coordinate vector of $T(\mathbf{e}_i)$ written as a column, we have:

$$T(\mathbf{e}_i) = 0\mathbf{e}_1 + \dots + 0\mathbf{e}_{i-1} + a_i\mathbf{e}_i + 0\mathbf{e}_{i+1} + \dots + 0\mathbf{e}_n = a_i\mathbf{e}_i.$$

Therefore $\mathbf{e}_i$ is an eigenvector of T corresponding to the eigenvalue a_i.

On the other hand, suppose that $\alpha_1, \dots, \alpha_n$ are eigenvalues of T and for each k, $\mathbf{e}_k$ is an eigenvector of T corresponding to the eigenvalue α_k. Then clearly the i^{th} column of $M(T;L)$ is the has entry a_i in position i and zero's everywhere else since

$$T(\mathbf{e}_i) = a_i\mathbf{e}_i = 0\mathbf{e}_1 + \dots + 0\mathbf{e}_{i-1} + a_i\mathbf{e}_i + 0\mathbf{e}_{i+1} + \dots + 0\mathbf{e}_n.$$

□

Definition 2.10 (Diagonalisable)**.** A linear transformation $T : V \to V$ is *diagonalisable* if there exists a basis L of V such that $M(T;L)$ is a diagonal matrix.

Theorem 2.2. *Suppose that the linear transformation $T : V \to V$ has n different eigenvalues $\alpha_1, \dots, \alpha_n$, where $n = \dim(V)$. For each k, let $\mathbf{e}_k$ be an eigenvector of T corresponding to α_k and let $L = (\mathbf{e}_1, \dots, \mathbf{e}_n)$. Then L is a basis of V and*

$$M(T;L) = \operatorname{diag}(\alpha_1, \dots, \alpha_n).$$

Proof. By Corollary 2.3, L is linearly independent, therefore L is a basis for V since $\dim(V) = n$.

By Lemma 2.13, $M(T; L) = \operatorname{diag}(\alpha_1, \dots, \alpha_n)$.

□

2.7 Algebraic and Geometric Multiplicities of Eigenvalues

Definition 2.11 (Algebraic and geometric multiplicity)**.** Let $T : V \longrightarrow V$ be a linear mapping with V finite dimensional and let $\lambda \in \mathcal{F}$ be an eigenvalue of T. Then

i. The power to which $(t - \lambda)$ appears in the characteristic polynomial $\chi_T(t)$ is called the *algebraic multiplicity* of λ as an eigenvalue of T.

ii. The quantity $\dim(E(\lambda, T))$ is called the *geometric multiplicity* of λ as an eigenvalue of T.

Lemma 2.14. *Let $T : V \longrightarrow V$ be a linear mapping with V nonzero and finite dimensional. Let $\lambda \in F$ be an eigenvalue of T. Then*

(geometric multiplicity of λ) $\leq$ (algebraic multiplicity of λ).

Proof. Let λ be an eigenvalue of T, let s be the algebraic multiplicity of T and r be its geometric multiplicity.

Since $\dim(E(\lambda, T)) = r$, there is a basis $l = (\mathbf{e}_1, \dots, \mathbf{e}_r)$ for (λ, T). We can extend l to a basis $L = (\mathbf{e}_1, \dots, \mathbf{e}_r, \dots, \mathbf{e}_{s+1}\mathbf{e}_n)$.

With respect to the basis L, we have,

$$M(T;L)=\begin{pmatrix}\lambda I_r & B\\ 0 & C\end{pmatrix}$$

Where I_r is the $r\times r$ identity matrix, B is an $r\times(n-r)$ matrix and C is an $(n-r)\times(n-r)$ matrix. Expanding the determinant of $(tI = M(T;L))$, we see that

$$\det(T)=\begin{vmatrix}tI_r-\lambda I_r & -B\\ 0 & tI_{(n-r)}-C\end{vmatrix}=(t-\lambda)^r\det(tI-C)=(t-\lambda)^r\chi_C(t).$$

It follows that $r\leq s$ since $\det(C)$ might have a power of $(t-\lambda)$ as a factor.

□

Theorem 2.3. *Let $T:V\longrightarrow V$ be a linear mapping with V finite dimensional and let $\lambda\in F$ be an eigenvalue of T. Then T is diagonalisable if and only if, for each eigenvalue λ of T, the algebraic and geometric multiplicities of λ coincide.*

Proof. Omitted.

□

Example 2.10. Consider the linear transformation of $\mathbb{C}^2$ defined by

$$T((x,y))=(x+y,\ 4x+y).$$

Show that T is diagonalisable.

With respect to the standard basis for $\mathbb{C}^2$,

$$M_T = \begin{pmatrix} 1 & 1 \\ 4 & 1 \end{pmatrix}.$$

Thus $\chi_T = (t-1)^2 - 4 = (t+3)(t-1)$. The eigenvalues of T are therefore -3 and 1.

Notice that $\dim(E(\lambda, T))$ is at least 1 for any eigenvalue of T (since eigenvectors by definition are non-zero). However by Lemma 2.14, $\dim(E(\lambda, T)) \leq 1$ for any eigenvalue of T since the algebraic multiplicity of each of the eigenvalues of T is 1 (from the expression of χ_T).

It follows that the algebraic and geometric multiplicities of each eigenvalue of T are equal and so T is diagonalisable by Theorem 2.3.

Example 2.11. Consider the linear transformation of $\mathbb{C}^2$ defined by

$$S((x,y)) = (x+y,\ y).$$

Show that S is not diagonalisable.

With respect to the standard basis for $\mathbb{C}^2$

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

Thus $\chi_S = (t-1)^2$ and s has a single eigenvalue namely 1.

We find $\dim(E(1,S))$. First we find a spanning set for $E(1,S)$, we have

$$\begin{aligned} E(1,S) &= \{(x,y) \in \mathbb{C}^2 : T((x,y)) = (x,y)\} \\ &= \{(x,y) \in \mathbb{C}^2 : (x+y,y) = (x,y)\} \\ &= \{(x,y) \in \mathbb{C}^2 : y = 0\} \\ &= \operatorname{span}((1,0)). \end{aligned}$$

It follows that $\dim(E(1,S)) = 1$ and the algebraic multiplicity of the eigenvalue 1 is strictly greater than its geometric multiplicity — S is not diagonalisable by Theorem 2.3.

2.8 Vector Space Isomorphisms

Definition 2.12 (Isomorphism)**.** Let V and W be vector spaces over $\mathcal{F}$ and let $T : V \longrightarrow W$ be a linear mapping. In the special case where T is a bijection we say that T is a *vector space isomorphism* and that the spaces V and W are *isomorphic*.

Lemma 2.15. *Let V be a finite dimensional vector space over $\mathcal{F}$ with $\dim V = n$. Then V is isomorphic to $\mathcal{F}^n$.*

Proof. Let $B := (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ be a basis for V. Let $T : V \to \mathcal{F}^n$ be defined by

$$T(a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \dots + a_n\mathbf{e}_n) = (a_1, a_2, \dots, a_n).$$

The map T is well-defined since, as B is a basis, every element of V can be expressed uniquely as a linear combination of elements of B. Clearly T is surjective and injective.

That T is linear is easily verified, in particular T is the unique linear map which maps $\mathbf{e}_i$ to the element $(0, \ldots, 0, 1, 0 \ldots, 0)$ where 1 occurs in position i.

Therefore T is an isomorphism of vector spaces and $V \cong \mathcal{F}^n$.

□

Corollary 2.4. *Let V and W be finite dimensional vector spaces over $\mathcal{F}$. Then*

$$V \cong W \Leftrightarrow \ \dim\, V = \dim\, W.$$

Proof. If $V \cong W$, then there exist is a vector space isomorphism $T : V \to W$. Applying the Rank-Nullity Theorem (Theorem 2.1)

$$\dim\,(V) = \dim\,(im(T)) + \dim\,(\ker(T)) = \dim\,(W) + 0 = \dim(W).$$

If $\dim\,(V) = \dim\,(W) = n$. Then $V \cong \mathcal{F}^n \cong W$ and so $V \cong W$.

□

2.9 Problem Sheet 2

_ Questions 2.1 – 2.16 for Week 4; Questions 2.17 – 2.21 for Week 6._

Question 2.1

Let $S : V \longrightarrow W$ and $T : U \longrightarrow V$ be mappings.

a. Prove that if $S \circ T$ is injective then T is also injective.

b. Prove that if $S \circ T$ is surjective then S is also surjective.

Show Solution 2.1 on P153

Question 2.2

For each of the following mappings $T : U \longrightarrow V$, decide whether T is linear.

a. $U = \mathbb{R}^4$, $V = \mathbb{R}^3$, $T((x_1, x_2, x_3, x_4)) = (x_2 + x_3,\ x_1 - x_2^2,\ x_3 + x_4)$,

b. $U = \mathbb{R}^3$, $V = \mathbb{R}^2$, $T((x_1, x_2, x_3)) = (x_2 - x_1,\ x_3 + 3x_2)$,

c. $U = P_2$, $V = P_5$, $T(p(x)) = xp(x^2) + p(1)$,

d. $U = \mathbb{R}^2$, $V = \mathbb{R}$, $T((x, y)) = xy$.

Show Solution 2.2 on P153

Question 2.3

A linear mapping $S : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ is such that

$$\begin{aligned} S((1,0,0)) &= (2,-1,0,4), \\ S((0,1,0)) &= (1,3,-4,7), \text{ and} \\ S((0,0,1)) &= (0,0,5,2) \end{aligned}$$

Find a general formula for $S((x_1, x_2, x_3))$.

Show Solution 2.3 on P156

Question 2.4

A linear mapping $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ is such that

$$\begin{aligned} T((1,1,1)) &= (1,-1,1) \\ T((1,1,0)) &= (-2,1,-1), \text{ and} \\ T((1,0,0)) &= (3,1,0). \end{aligned}$$

Obtain a general formula for $T((x_1, x_2, x_3))$.

Show Solution 2.4 on P156

Question 2.5

Let $T : V \longrightarrow W$ be a linear mapping. Prove that if the sequence $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ is linearly dependent in V then $(T(\mathbf{v}_1), \ldots, T(\mathbf{v}_k))$ is linearly dependent in W.

Show Solution 2.5 on P158

Question 2.6

Let $T : V \longrightarrow W$ be a linear mapping. Show that if the sequence $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ is linearly independent in V and $\ker(T)$ is trivial then the sequence $(T(\mathbf{v}_1), \ldots, T(\mathbf{v}_k))$ is linearly independent in W.

Show Solution 2.6 on P159

Question 2.7

Find bases of the image and kernel of the linear mapping $S : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ defined by

$$S((x, y, z)) = (x + 2y + z,\ x + 2y + z,\ 2x + 4y + 2z).$$

Show Solution 2.7 on P159

Question 2.8

Define $T : \mathbb{R}_{n\times n} \longrightarrow \mathbb{R}_{n\times n}$ by $T(A) = A^T$ for all $A \in \mathbb{R}_{n\times n}$.

Show that T is a linear mapping and find explicitly the kernel and image of T. State also the rank and nullity of T.

Show Solution 2.8 on P161

Question 2.9

Show that the mapping $T : P_2 \longrightarrow P_3$ defined by $T(p(x)) = xp(x)$ for all $p \in P_2$ is linear. Find the rank and nullity of T.

Show Solution 2.9 on P162

Question 2.10

Let W denote the vector space of all symmetric 2×2 real matrices. Find the nullity of the linear mapping $T : W \longrightarrow P_2$ defined by

$$T\left(\begin{pmatrix} a & b \\ b & c \end{pmatrix}\right) = (a-b) + (b-c)x + (c-a)x^2$$

and use this to deduce the value of rank(T) from the Rank-Nullity Theorem. Use this information to find a basis of im(T).

Show Solution 2.10 on P162

Question 2.11

Let V and W be vector spaces of dimensions 3 and 4 respectively and let $L_V = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ and $L_W = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4)$ be bases of V and W respectively. Given that

$$M(T; L_V, L_W) = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{pmatrix}$$

a. Write down $T(\mathbf{e}_2)$ as a linear combination of $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$.

b. By evaluating one matrix product, obtain $T(2\mathbf{e}_1 + \mathbf{e}_2 - \mathbf{e}_3)$ as a linear combination of $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$.

Show Solution 2.11 on P164

Question 2.12

Let $D : P_3 \longrightarrow P_2$ be the linear mapping defined by $D(p(x)) = p^{'}(x)$ for all $p \in P_3$. Let $B = (1, x, x^2, x^3)$ and $C = (1, x, x^2)$ be the standard bases for P_3 and P_2 respectively. Find the matrix of D with respect to B and C.

Show Solution 2.12 on P165

Question 2.13

Let $S : V \longrightarrow W$ and $T : U \longrightarrow V$ be linear mappings and let L_U, L_V, L_W be bases of U, V and W respectively. Show that $M(ST; L_U, L_W) = M(S; L_V, L_W)M(T; L_U, L_V)$.

(Here, as usual, ST means the composition $S \circ T$.)

Show Solution 2.13 on P165

Question 2.14

Consider the bases

$$B_1 = ((1,0,0),(0,1,0),(0,0,1))$$

and

$$B_2 = ((1,1,0),(0,1,1),(1,0,1))$$

of $\mathbb{R}^3$.

a. Find the change of basis matrices $M(B_1 \to B_2)$ and $M(B_2 \to B_1)$.

b. Use your answer to express $\mathbf{x} = (1,2,3)$ as a linear combination of the vectors in B_2.

Show Solution 2.14 on P166

Question 2.15

Consider the standard basis B_1 of $\mathbb{R}^3$ and the basis $B_2 = (\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3)$ where

$$\mathbf{w}_1 = (2,1,1), \quad \mathbf{w}_2 = (0,1,3), \quad \mathbf{w}_3 = (0,0,2).$$

a. Find the change of basis matrices $M(B_1 \to B_2)$ and $M(B_2 \to B_1)$.

b. Use an appropriate change of basis matrix to find the coordinate vector of $(x,y,z) \in \mathbb{R}^3$ w.r.t. the basis B_2. Verify your answer.

Show Solution 2.15 on P167

Question 2.16

(A number crunch workout) Consider the bases

$$B_1 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

and

$$B_2 = \left(\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

of $\mathbb{R}_{2\times 2}$.

a. Find the change of basis matrix $M(B_2 \to B_1)$.

b. Use part a. to express the matrix $A = \begin{pmatrix} 4 & 2 \\ 0 & -1 \end{pmatrix}$ as a linear combination of the matrices in B_2.

Show Solution 2.16 on P169

Question 2.17

Find the two eigenvalues of the linear mapping $T : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ defined by

$$T((x, y)) = (-x + 3y,\ 3x - y)$$

for all $(x, y) \in \mathbb{C}^2$. Find a basis of each corresponding eigenspace.

Show Solution 2.17 on P170

Question 2.18

Consider the linear mapping $T : P_2 \longrightarrow P_2$ defined by

$$T(p(x)) = p(3x + 2)$$

for all $p \in P_2$.

a. Find the eigenvalues of T and hence find bases of each corresponding eigenspace.
b. State a basis of P_2 with respect to which the matrix of T is a diagonal matrix. Verify this directly.

Show Solution 2.18 on P172

Question 2.19

Consider the linear transformation S of $\mathbb{C}^2$ defined by

$$S((x, y)) = (4x + 2y,\ 3x - y)$$

for all $(x, y) \in \mathbb{C}^2$. Find the eigenvalues of S and decide whether S is diagonalisable.

Show Solution 2.19 on P174

Question 2.20

Consider the linear transformation T of $\mathbb{C}^2$ defined by

$$T((x, y)) = (10x - 9y,\ 4x - 2y)$$

for all $(x, y) \in \mathbb{C}^2$. Find the eigenvalues of T and decide whether T is diagonalisable.

Show Solution 2.20 on P176

Question 2.21

Consider the linear transformation S of $\mathbb{C}^3$ defined by

$$S((x, y, z)) = (3x - 2z,\ y,\ x).$$

for all $(x, y, z) \in \mathbb{C}^3$. Given that $\chi_S(t) = (t-1)^2(t-2)$, find bases of the relevant eigenspaces. Is S diagonalisable?

Show Solution 2.21 on P177

Part II

Rings

Chapter 3

Ring Theory Fundamentals

3.1 Introduction

Rings are extremely important algebraic structures. A wide array of well known systems can be identified as rings. Our goal will be to study the structure of rings in the abstract setting in order to obtain some powerful results. The term ‘ring’ was first coined in the early 20th Century and the study of rings as algebraic structures is still a relatively modern concept. As always, we begin with a definition.

Definition 3.1 (Ring)**.** A *ring* is a triple consisting of a non-empty set R equipped with two binary operations that we denote $+$ and $\cdot$, such that the following are satisfied.

(R1) For all $a, b \in R$, $a + b \in R$ *(closure under* $+$*)*.

(R2) For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$ *(*$+$ *is associative on* R*)*.

(R3) There exists 0_R such that, $\forall\, a \in R, a + 0_R = 0_R + a = a$ *(*$+$ *has an identity)*.

(R4) For all $a \in R$, $\exists - a \in R$ such that $a + (-a) = (-a) + a = 0_R$ *(inverses under* $+$*)*.

(R5) For all $a, b \in R$, $a + b = b + a$ *(*$+$ *is commutative on* R*)*.

(R6) For all $a, b \in R$, $a \cdot b \in R$ *(closure under* $\cdot$*)*.

(R7) For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *($\cdot$ is associative on R).*

(R8) For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ *(distributive laws).*

Note that we will usually write ab for $a \cdot b$.

Commutative Rings

From the axioms we see that, while the addition operation is commutative in any ring, we do not require a ring to have a commutative multiplicative operation. In the case where a ring R has $ab = ba$ for all $a, b \in R$ we say that R is *commutative*. In this course we will mostly be dealing with commutative rings. The ring of integers $\mathbb{Z}$ is an example of a commutative ring, as is $\mathbb{Z}_n$. Note that, in a ring, elements do not need to have multiplicative inverses (unlike groups).

Definition 3.2 (Identity Elements)**.** An *identity element* in a ring R is a multiplicative identity. Hence, an identity element $1_R \in R$ is such that $a1_R = 1_Ra = a$ for all $a \in R$.

In this module we will assume that all rings have multiplicative identities. A ring with an identity element is sometimes referred to as a *ring with a one*.

Zero Ring

The *zero ring* is the ring $\{0_R\}$ consisting of just one element 0_R. It should be noted that in this ring, $1_R = 0_R$.

Definition 3.3 (Unit)**.** Let R be a ring and $a \in R$. Then a is said to be a *unit* in R if it has a multiplicative inverse in R, that is there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1_R$.

We denote and define the set of units of a ring R as

$$R^\times = \{a \in R \mid \exists\, b \in R \text{ such that } ab = 1_R\}.$$

Example 3.1.

- If R is the ring of integers, then $R^\times = \{-1, 1\}$.
- The set of units of a ring forms a group.

Division Rings

A *division ring* is a nonzero ring in which every nonzero element has a multiplicative inverse. Note that we do not demand that a division ring is commutative. If a division ring is commutative then it is a *field*. The familiar systems $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields. Note that $\mathbb{Z}$ is not a field as the only units in $\mathbb{Z}$ are the elements ± 1.

Matrix Rings

Let R be a ring. Then the set of all $n \times n$ matrices with entries from R is a ring under the usual matrix addition and multiplication. This ring is denoted $M_n(R)$. Observe that $M_n(R)$ is not a commutative ring (unless $n = 1$ and R itself is commutative).

Example 3.2.

In first year Algebra we considered only matrices with entries from $\mathbb{R}$. For such matrices, having a non-zero determinant is equivalent to being invertible. That is, for $A \in M_n(\mathbb{R})$, $\det(A) \neq 0$ if and only if there is some $B \in M_n(\mathbb{R})$ such that $AB = BA = I_n$.

However, having a non-zero determinant is not enough for invertibility in $M_n(R)$ for a general ring $\mathbb{R}$. As an example take $\mathbb{R} = \mathbb{Z}_4$ and consider the element $A \in M_2(\mathbb{Z}_4)$ below

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

Then $\det(A) = 2 \neq 0 \in \mathbb{Z}_4$ however, we claim that A does not have an inverse in $\mathbb{Z}_4$. Let us demonstrate this claim.

Suppose A has an inverse $B \in M_n(\mathbb{Z}_4)$. Suppose

$$B = \begin{pmatrix} a & b \\ c & d. \end{pmatrix}$$

Then,

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 2c & 2d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

It follows that $a = 1$, $b = 0$, $c = 0$ and $2d = 1$. However, there is no element $d \in \mathbb{Z}_4$ such that $2d = 1$.

If on the other hand we considered A as an element of $M_2(\mathbb{Z}_5)$, then we can solve the equation $2d = 1$. Since 3 is the unique element of $\mathbb{Z}_5$ satisfying $2 \times 3 = 1$. Therefore A is in fact invertible as an element of $M_2(\mathbb{Z}_5)$.

The difference is that every non-zero element of $\mathbb{Z}_5$ is a unit in $\mathbb{Z}_5$ since $\mathbb{Z}_5$ is a field ($\mathbb{Z}_n$ is a field when n is prime).

In fact what is true is that an element $A \in M_n(R)$, for R a *commutative* ring, is invertible if and only if its determinant is a unit in the ring.

Polynomial Rings

Let R be a commutative ring and let X be an indeterminate. We define the *ring of polynomials* $R[X]$ to be the set of all polynomials in X with coefficients from the ring R. Hence

$$R[X] = \left\{ \sum_{i=0}^{n} r_i X^i \mid r_i \in R,\ \ n \geq 0 \right\}.$$

Addition and multiplication are defined in the intuitive way. Hence if $f = a_0 + a_1 X + ... + a_m X^m$, $g = b_0 + b_1 X + ... + b_n X^n \in R[X]$ with $n > m$ then we have

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + ... + (a_m + b_m)X^m + b_{m+1}X^{m+1} + ... + b_n X^n$$

and

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + (a_0 b_2 + a_1 b_1 + a_2 b_0)X^2 + ... + a_m b_n X^{m+n}.$$

Contrast the situation with that of P_n forming a vector space, where P_n is the set of all polynomials of maximum degree n. Note that in the case of polynomials of some maximum degree, the set remains closed under the operations of addition and scalar multiplication in the vector space. However, in rings we have a multiplication operation, so we cannot have rings of polynomials of some fixed degree as the set would not remain closed under multiplication.

At this point it is worth recalling the *factor theorem* for polynomials over a *field*. Let $\mathcal{F}[X]$ be the set of all polynomials over the field $\mathcal{F}$ and let $f(x) \in \mathcal{F}[X]$. Then $f(x)$ has a factor $(x - k)$, say, if and only if $f(k) = 0$ (that is, k is a root).

Example 3.3.

Recall that for a ring$R$, $R^\times$ is the set of units (or invertible elements) of R.

If R is a field then $R[x]^{\times} = R^{\times}$. However this is not the case for an arbitrary ring R.

For example consider the ring $\mathbb{Z}_4$. The polynomials $(1 + 2x), (1 - 2x) \in \mathbb{Z}_4[x]$ satisfy:

$$(1 + 2x)(1 - 2x) = 1 + (2 - 2)x - 4x^2 = 1.$$

So the units of $\mathbb{Z}_4[x]$ is a strictly larger set than the units of $\mathbb{Z}_4$.

Quadratic Integer Rings

Let d be a square-free integer. Then the set denoted and defined by

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

is a ring.

In the specific case in which $d = -1$, the ring $\mathbb{Z}[i]$ is called the ring of Gaussian integers.

We could show that $\mathbb{Z}[\sqrt{d}]$ is a ring by checking all of the axioms, but we shall provide a much more slick, alternative proof a little later.

Example 3.4.

Let $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Define $\bar{x} = a - b\sqrt{d}$. Note that when d is a negative number, then x and $\bar{x}$ are both complex numbers and $\bar{x}$ is precisely the complex conjugate of x. If d is positive, then x is real and so is its own complex conjugate. In particular for x real $\bar{x}$ is not (in general) the complex conjugate of x. However, $\bar{x}$ generalises some properties of the complex conjugate.

Let $x \in \mathbb{Z}\sqrt{d}$, and write $N(x)$ for the product $x\bar{x} = a^2 - bd^2 \in \mathbb{Z}$. We call $N(x)$ the *norm* of x. (This can be thought of as generalising the modulus function for complex numbers $|z|^2 = z\bar{z}$.)

We can use the norm to characterise the units of $\mathbb{Z}[\sqrt{d}]$.

If x is a unit then there is some $y \in \mathbb{Z}[\sqrt{d}]$ such that $xy = 1$. Then $N(xy) = 1$. However, $N(xy) = N(x)N(y)$ and so $N(x)N(y) = 1$. This means that either $N(x) = N(y) = 1$ or $N(x) = N(y) = -1$. Therefore if x is a unit of $\mathbb{Z}[\sqrt{d}]$, then $N(x) = \pm 1$.

On the other hand if $N(x) = \pm 1$, then observe that $N(x)\bar{x}x = N(x)^2 = 1$ and x is a units.

Definition 3.4 (Division in a ring)**.** Let R be a commutative ring and let $a, b \in R$. We say that a *divides* b if $b = ta$ for some $t \in R$. We will often use the notation $a \mid b$ for this.

Example 3.5.

- In $\mathbb{Z}$ we have that $3|21$ and $-7|42$.
- In $\mathbb{R}[x]$, $(x^3+3)|(x^5+2x^3-x^2-3x-3)$ since

$$x^5+2x^3-x^2-3x-3 = (x^3-x-1)(x^2+3).$$

- In the ring of Gaussian integers, we have $-i|(2-3i)$ since $2-3i = (-i)(3+2i)$.

Definition 3.5 (Prime element)**.** Let R be a commutative ring. A nonzero element $p \in R$ is a *prime element* if, for all $x, y \in R$,

$$p \mid xy \Rightarrow p \mid x \text{ or } p \mid y.$$

Example 3.6.

- In $\mathbb{Z}$, the prime elements are precisely $\pm p$ where p is a prime number.
- Any polynomial of degree 1 is prime in $\mathbb{R}[x]$. Consider $ax{-}b \in \mathbb{R}[x]$ for $a, b \in \mathbb{R}$, $a \neq 0$. This has a unique root b/a. Let $f(x), g(x) \in \mathbb{R}[x]$ and suppose $(ax-b)|f(x)g(x)$. Then $f(x)g(x) = (ax-b)h(x)$ for some $h(x) \in \mathbb{R}[x]$. However, this now means that $f(b/a)g(b/a) = 0$ meaning that $f(b/a) = 0$ or $g(b/a) = 0$. We conclude that $(ax-b)|f(x)$ or $(ax-b)|g(x)$. Therefore $(ax-b)$ is prime in $\mathbb{R}[x]$.
- In the ring $\mathbb{Z}[\sqrt{-5}]$, 3 is not prime. For example $9 = (2+\sqrt{-5})(2-\sqrt{-5})$ but 3 does not divide $2+\sqrt{-5}$ or $2-\sqrt{-5}$. For instance if $2+\sqrt{-5} = 3(a+b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$, then $(2-3a)+(1-3b)\sqrt{-5} = 0$. This means that $2 = 3a$ and $1 = 3b$. However there are no integers a, b satisfying these equations. A similar argument shows that $3 \nmid (2-\sqrt{-5})$.

Definition 3.6 (Irreducible element)**.** Let R be a commutative ring. A nonzero element $x \in R$ is called *irreducible* if x is not a unit in R and, for $y, z \in R$, $x = yz \Rightarrow y$ is a unit or z is a unit.

Example 3.7.

- In $\mathbb{Z}$, the primes and their negatives are irreducible elements.
- In $\mathbb{R}[x]$ a quadratic is irreducible if it has no roots in $\mathbb{R}$. Consider the quadratic $2x^2+3$ in the ring of polynomials over $\mathbb{Q}$. Suppose $2x^2+3 = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{Q}[x]$. Since $2x^2+3$ cannot be factorised in $\mathbb{Q}[x]$, one of $f(x)$ or $g(x)$ must be a constant polynomial and so a unit.
- We saw that 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$. However it is irreducible. Suppose $3 =$

$(a+b\sqrt{-5})(c+d\sqrt{-5})$. Then,

$$9 = |3|^2 = |(a+b\sqrt{-5})(c+d\sqrt{-5})| = (a^2+5b^2)(c^2+5d^2).$$

Notice that there are no integers $a, b \in \mathbb{Z}$ such that $a^2+5b^2 = 3$. Therefore one of (a^2+5b^2) or (c^2+5d^2) must be equal to 1. Without loss of generality we may assume that $(a^2+5b^2) = 1$. This is only possible if $b = 0$ and $a = \pm 1$. Thus $a + b\sqrt{5} = a$ is a unit.

Definition 3.7 (Divisor of zero)**.** Let R be a ring and let $x \in R$ be nonzero. Then x is a *divisor of zero* in R if there exists $y \in R\backslash\{0_R\}$ such that $xy = 0_R$.

Example 3.8.

In $M_2(\mathbb{R})$, the element $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a zero divisor since

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

Technically, Definition 3.7 above is of a *left* zero divisor. There is an analogous definition for a *right* zero divisor. In the above, $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$ is a right zero divisor.

Definition 3.8 (Integral Domain)**.** An *integral domain* is a nonzero commutative ring in which there are no divisors of zero. Hence in an integral domain R, for all $x, y \in R$ we have

$$xy = 0_R \Rightarrow x = 0_R \text{ or } y = 0_R.$$

Lemma 3.1. *Let R be an integral domain and let $a, b, c \in R$ with $a \neq 0_R$. Then*

$$ab = ac \Rightarrow b = c.$$

Proof. We have

$$ab - ac = a(b - c) = 0.$$

Since R is an integral domain, and $a \neq 0$, then $b - c = 0$ and $b = c$ as required.

□

ℹ Note

- If R is an integral domain, then $R[x]$ is also an integral domain.
- $\mathbb{Z}_n$ is an integral domain if and only if n is prime.
- The ring $M_n(\mathbb{R})$ is not an integral domain.

Lemma 3.2. *Let R be a ring. For all $x \in R$,*

$$x0_R = 0_R x = 0_R.$$

Proof.

$$x0_R = x(0_R + 0_R) = x0_R + x0_R.$$

Subtracting $x0_R$ from both sides:

$$0_R = x0_R.$$

In a similar way, it can be shown that $0_R x = 0_R$.

□

Lemma 3.3. *Every field is an integral domain.*

Proof. Let $\mathcal{F}$ be a field and x be a non-zero element of $\mathcal{F}$. Suppose there is a $y \in \mathcal{F}$ such that $xy = 0_{\mathcal{F}}$. Then

$$y = 1y = (x^{-1}x)y = x^{-1}0_{\mathcal{F}} = 0_{\mathcal{F}}.$$

Thus if $xy = 0_{\mathcal{F}}$ for $x, y \in \mathcal{F}$ either $x = 0_{\mathcal{F}}$ or $y = 0_{\mathcal{F}}$.

□

ℹ Note

Every finite integral domain is a field.

The content that follows is non-examinable.

Definition 3.9 (Characteristic)**.** Let R be an integral domain. The *characteristic* of R (denoted char (R)) is the period of 1_R in the group $(R,+)$.
If 1_R has infinite period in $(R,+)$ then we define char $(R)=0$.

Theorem 3.1. *Let R be an integral domain. Then char(R) is either 0 or a prime.*

Proof. Let $m \in \mathbb{N}$ be period of 1_R in $(R,+)$. Then, $m1_R = 0_R$. If m is not prime, then there are elements $k,l \in \mathbb{N}$ such that $k,l < m$ and $m1_R = (kl)1_R = k1_R l1_R = 0_R$. As R is an integral domain either $k1_R = 0_R$ or $l1_R = 0_R$. In either case we get a contradiction as m is the smallest positive integer satisfying $m1_R = 0_R$. Therefore, m must be prime.

□

> **i** Note
>
> - Every field of characteristic zero has a copy of $\mathbb{Q}$ inside it.
> - Every field of characteristic p has a copy of $\mathbb{Z}_p$ inside it.

End of non-examinable content.

Lemma 3.4. *If R is an integral domain, then all prime elements are irreducible.*

Proof. Let p be a prime element of R and suppose $p = xy$ for some x and y in R.

Since $p|p$ then $p|(xy)$. As p is prime it follows that either $p|x$ or $p|y$. Without loss of generality we may assume that $p|x$. Then there is some $z \in R$ such that $x = pz$. It follows that $p = pzy$. By Lemma 3.1 it follows that $1 = zy$ and y is a unit. Therefore p is irreducible.

□

ℹ Note

All prime elements of an integral domain are irreducible but **not** all irreducible elements of an integral domain are prime. For example we have seen that 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$ but it is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Example 3.9.

- As $\mathbb{Q}$ is an integral domain, then $\mathbb{Q}[x]$ is also an integral domain. We have seen that all linear polynomials are prime, it follows that all linear polynomials are irreducible in $\mathbb{Q}[x]$.
- 19 is prime in $\mathbb{Z}$ therefore it is irreducible in $\mathbb{Z}$. We can verify this, for if $19 = xy$ for integers x, y, then either x or y is equal to 1.

3.2 Subrings

A subset S of a ring R is called a *subring* if S is itself a ring under the addition and multiplication given in R.

ℹ Note

In any ring R, $\{0_R\}$ and R are subrings of R.

Lemma 3.5. *Let R be a ring and let $S \subseteq R$. Then S is a subring of R if and only if the three conditions below are satisfied:*

i. S has an identity element;

ii. $a, b \in S \Rightarrow a - b \in S$;

iii. $a, b \in S \Rightarrow ab \in S$

Proof. The proof that follows is non-examinable.

Let R be a ring and let S be a subset of R.

$(\Rightarrow)$ First we show that if S is a subring of R then the three conditions hold.

i. As S is a subring then $1_S \in S$. By the definition of a subring $1_S = 1_R$, so $1_R \in S$.

ii. Now let $a, b \in S$. Since S is a ring it must be closed under addition. Further there is an additive inverse for b in S (R4) and since additive inverses are unique in R this inverse is the same as $-b$ in R. Hence $a - b = a + (-b) \in S$.

iii. Similarly, S is closed under multiplication.

$(\Leftarrow)$ Next we show that if S satisfies the three enumerated conditions then it is a subring of R, that is, S is a ring in itself with the operations on S being defined as the operations on R.

Non-empty: By i. S is non-empty.

(R3): Since S is non-empty, let $a \in S$. By ii., $a - a \in S$ and so $0_R \in S$. We claim that 0_R is an additive identity for S. For any $s \in S$, we have $0_R + s = s$, since $s \in R$ and since 0_R is the additive identity in R. Thus 0_R is an additive identity for S.

(R4): Let $a \in S$. Then, by ii. we have $0_S - a \in S$. But $0_S - a = 0_S + (-a)$, where $-a$ is the additive inverse of a in R. So $-a \in S$ and $-a$ is an additive inverse for a in S.

(R1): Let $a, b \in S$. Then $-b \in S$ and $-(-b) = b$, since if $-b$ is an additive inverse for b, then b is an additive inverse for $-b$. Thus, $a + b = a - (-b) \in S$, by ii., so S is closed under addition.

(R5): Let $a, b \in S$. Then $a + b \in S$ as S is closed under addition and, since $a, b \in R$, we have $a + b = b + a$ by commutativity of addition in R.

(R2): Let $a, b, c \in S$. Then, since $a, b, c \in R$, we have that $a + (b + c) = (a + b) + c$ and closure ensures that these sums are in S.

Multiplicative identity: This is assumed by i.

(R7): Let $a, b, c \in S$. Since $a, b, c \in R$ then $a(bc) = (ab)c$ in R and since S is closed under multiplication then $a(bc) = (ab)c$ in S.

(R6): This follows from iii..

(R8): Similarly to (R2), this follows as (R8) holds in R and S is a subset of R.

□

Example 3.10.

- The ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of $\mathbb{R}$ which is a subring of $\mathbb{C}$.
- Consider the ring $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$, $i^2 = -1$.
  - i. $\mathbb{Z}[i]$ has the identity element $1 = 1 + 0i$.
  - ii. Let $x_1 = a_1 + b_1 i$ and $x_2 = a_2 + b_2 i$ be elements of $\mathbb{Z}[i]$. Then:

$$\begin{aligned} x_1 - x_2 &= (a_1 + b_1 i) - (a_2 + b_2 i) \\ &= (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Z}[i]. \end{aligned}$$

  - iii.

$$\begin{aligned} x_1 x_2 &= (a_1 + b_1 i)(a_2 + b_2 i) \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i \in \mathbb{Z}[i] \end{aligned}$$

So $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Example 3.11. Let R be a ring and let $a \in R$. Show that the subset

$$C(a) = \{x \in R \mid xa = ax\}$$

is a subring of R.

The set $C(a)$ is non-empty as it contains the identity element 1 of R.

Let $x, y \in C(a)$

$$(x - y)a = xa - ya = ax - ay = a(x - y).$$

Therefore $x - y \in C(R)$. Furthermore

$$(xy)a = xay = axy$$

and $xy \in C(a)$.

It follows that $C(a)$ is a subring of R.

> **Note**
>
> When R has an identity element 1_R it does not always follow that $1_R = 1_S$. An important example is the subring $S = \{0_R\}$ which is a subring of every ring. Note that in this case $1_S = 0_R$.

Example 3.12.

- Let $R = \mathbb{Z}_{10}$. The multiplicative identity if 1. Set $S = \{0, 2, 4, 6, 8\}$ is a subring of

$\mathbb{Z}_{10}$ with multiplicative identity 6 as:

$$\begin{aligned} 0 \times 6 &= 0 \\ 2 \times 6 &= 2 \\ 4 \times 6 &= 4 \\ 6 \times 6 &= 6 \\ 8 \times 6 &= 8. \end{aligned}$$

- Consider $R = M_2(\mathbb{R})$ and take

$$S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

Then S us a subring of R. However, the identity I_S of S is not equal to the identity I_R of R.

$$I_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_R.$$

3.3 Ring Homomorphisms

Definition 3.10. Let R and S be rings and let $\theta : R \longrightarrow S$ be a mapping. We say that θ is a *ring homomorphism* if, for all $a, b \in R$,

$$\theta(a + b) = \theta(a) + \theta(b)$$

and

$$\theta(ab) = \theta(a)\theta(b).$$

Lemma 3.6. *Let R and S be rings and let $\theta : R \longrightarrow S$ be a ring homomorphism. Then*

a. $\theta(0_R) = 0_S$

b. $\theta(-x) = -\theta(x)$ *for all* $x \in R$.

Proof. a. Observe that

$$\theta(0_R) = \theta(0_R + 0_R) = \theta(0_R) + \theta(0_R).$$

Subtracting $\theta(0_R)$ from both sides then gives the result: $\theta(0_R) = 0_S$.

b. We have

$$\begin{aligned} 0_S &= \theta(0_R) = \theta(x + (-x)) \\ &= \theta(x) + \theta(-x). \end{aligned}$$

Subtracting $\theta(x)$ from both sides:

$$-\theta(x) = \theta(-x)$$

as required.

□

ℹ Note

A bijective ring homomorphism is a ring *isomorphism*.

Example 3.13 (Examples of ring homomorphisms)**.**

- The map $\theta : \mathbb{Z} \to \mathbb{Z}_2$ defined by $\theta(a) = \begin{cases} 0 \text{ if } a \text{ is even,} \\ 1 \text{ if } a \text{ is odd} \end{cases}$ is a ring homomorphism.

    - The map is additive since the sum of two odd or even integers is even and the sum of an odd and even integer is odd.
    - The map is multiplicative since the product of two odd integers if odd and the product of an even integer with an even or odd integer is even.
- Let $\theta : \mathbb{Q}[x] \to \mathbb{Q}$ be defined by $\theta(p(x)) = p(0)$. This is a ring homomorphism since,
    - the constant term of the sum of two polynomials is the sum of their constant terms, and,
    - the constant term of the product of two polynomials is the product of their constant terms.

Definition 3.11 (Kernel)**.** Let R and S be rings and let $\theta : R \longrightarrow S$ be a ring homomorphism. The *kernel* of θ is the set

$$\text{ker}\,(\theta) = \{x \in R \mid \theta(x) = 0_S\} \subseteq R.$$

Lemma 3.7. *Let $\theta : R \longrightarrow S$ be a ring homomorphism. Then θ is injective if and only if ker$(\theta) = \{0_R\}$.*

Proof. If θ is injective, then ker$\,(\theta) = \{0_R\}$. This follows as $\theta(0_R) = 0_S$ and injectivity means that $\theta(x) = 0_S$ if and only if $x = 0_R$.

Now suppose ker$\,(\theta) = \{0_R\}$. Let $x, y \in \mathbb{R}$ and suppose that $\theta(x) = \theta(y)$. This means that

$$\theta(x - y) = \theta(x) - \theta(y) = 0_S.$$

Therefore $(x - y) \in$ ker$\,(\theta)$ and so $x - y = 0_R$. Adding y to both sides now gives $x = y$.

□

Definition 3.12 (Image)**.** Let $\theta : R \longrightarrow S$ be a ring homomorphism. The *image* of R is the set

$$\mathrm{im}\,(\theta) = \{\theta(x) \mid x \in R\} \subseteq S.$$

Lemma 3.8. *Let $\theta : R \longrightarrow S$ be a ring homomorphism. Then im (θ) is a subring of S.*

Proof. Notice that im (θ) is non-empty since it contains 0_S.

For any $x \in R$,

$$\theta(1_R)\theta(x) = \theta(1_R x) = \theta(x) = \theta(x 1_R) = \theta(x)\theta(1_R).$$

It follows that $\theta(1_R)$ is the identity of im (θ).

Let $x, y \in R$. Then

$$\theta(x) - \theta(y) = \theta(x - y) \in \mathrm{im}\,(\theta)$$

and

$$\theta(x)\theta(y) = \theta(xy) \in \mathrm{im}\,(\theta).$$

It follows that im (θ) is a subring of S.

□

Definition 3.13. We define the following:

1. An injective ring homomorphism is called a *monomorphism*.
2. A surjective ring homomorphism is called an *epimorphism*.
3. A bijective ring homomorphism is called an *isomorphism*

When there is an isomorphism $\theta : R \longrightarrow S$ of rings we say that the rings R and S are *isomorphic* and we write $R \cong S$ to represent this.

When two rings are isomorphic we are basically looking at two copies of the same ring. (structurally speaking)

Definition 3.14 (Automorphism)**.** Let R be a ring. A *ring automorphism* is a ring isomorphism from R to R. The set of all ring automorphisms of R is a group called the automorphism group of R. This group is denoted Aut (R).

3.4 Ideals

We now turn our attention to a special type of subset of a ring.

Definition 3.15 (Ideal)**.** Let R be a ring and let $I \subseteq R$ be a subgroup of the abelian group $(R, +)$. We say that I is an *ideal* of R if, for all $x \in I$ and for all $r \in R$, the element $xr \in I$ and also the element $rx \in I$. When I is an ideal of R we use the notation $I \trianglelefteq R$ to denote this.

> **i Note**
>
> In fact what we have just defined is a two-sided ideal. A subgroup I of $(R, +)$ satisfying $xr \in I \; \forall \, x \in I, r \in R$ is called a *right ideal* of R. Similarly, a subgroup I of $(R, +)$ satisfying $rx \in I \; \forall \, x \in I, r \in R$ is called a *left ideal* of R. In commutative ring theory any one-sided ideal is automatically two-sided. Note also that as I is a subgroup of the additive group $(R, +)$ we have $0_R \in I$.

Example 3.14.

- In any ring R, the subsets R and $\{0_R\}$ are ideals of R.
- In the ring $\mathbb{Z}$, the subset $2\mathbb{Z} = \{2x : x \in \mathbb{Z}\}$ of even integers is an ideal of $\mathbb{Z}$.

Lemma 3.9. *Let R be a ring and let $I \subseteq R$. Then I is an ideal of R if and only if the following conditions hold :*

i. $I \neq \phi$;

ii. $a, b \in I \Rightarrow a - b \in I$;

iii. $x \in I$ *and* $r \in R \Rightarrow xr$ *and* rx *both belong to* I.

Proof. This is left as an exception.

□

ℹ Note

The first condition is different from the first condition in the test for a subring. Obviously $(I, +)$ is a subgroup of $(R, +)$ and so $0_R \in I$. We use this in examples to establish property i.

Definition 3.16. Let R be a ring and let $a \in R$. We define the subset

$$aR = \{ar \mid r \in R\}.$$

Lemma 3.10. *Let R be a commutative ring. For each $a \in R$ the subset aR is an ideal of R and aR is the smallest ideal of R to which a belongs.*

Proof. Clearly aR is non-empty since it contains 0_R and $a = a1_R$.

Let $x, y \in aR$. There are $u, v \in R$ such that $x = au$ and $y = av$. Then

$$x - y = au - av = a(u - v) \in aR.$$

Let $au \in aR$ and $r \in R$, then $aur = rau \in aR$.

Let I be any ideal of R containing a. Then $ax \in I$ for any $x \in R$ and so $aR \subseteq I$. Thus aR is the smallest ideal of R containing a.

□

> ℹ Note
>
> It is essential that R is commutative here to get a two-sided ideal. If R is not commutative, aR is just a right ideal of R in general.

Definition 3.17 (Principal Ideal)**.** For a commutative ring, R, the ideal aR is called the *principal ideal* of R generated by the element a.

Example 3.15.

- For $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$, it is the set of all multiples of n. It can be shown that every ideal of Z if of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.
- Consider the principal ideal $I = (x-1)\mathbb{R}[x]$ of $\mathbb{R}[x]$. If $f(x) \in I$, then $f(x)$ is of the from $(x-1)g(x)$ for some $g(x) \in \mathbb{R}[x]$. In particular $f(1) = 0$.

  On the other hand, if $f(x) \in \mathbb{R}[x]$ satisfies $f(1) = 0$, then $f(x) = (x-1)g(x)$ for some $g(x) \in \mathbb{R}[x]$ and $f(x) \in I$.

Definition 3.18. Let R be a ring and let $I \trianglelefteq R$.

1. We say that I is a *non-trivial* ideal if $I \neq \{0_R\}$.
2. We say that I is a *proper* ideal if $I \neq R$.

Lemma 3.11. *Let R be a ring and let $I \trianglelefteq R$. If I contains a unit then $I = R$.*

Proof. Notice that if I contains 1_R then $I = R$. Therefore it suffices to show that $1_R \in I$. Let $x \in I$ be a unit. Then $x^{-1}x = 1_R \in I$. This concludes the proof.

□

In particular, note that if an ideal contains 1_R then $I = R$.

Theorem 3.2. *Let R be a nonzero, commutative ring. Then R is a field if and only if the only ideals of R are $\{0_R\}$ and R.*

Proof. Suppose R is a field. Let I be any ideal of R. If I contains an element $x \neq 0_R$, then I contains $1_R xx^{-1}$. Therefore $I = R$.

Suppose the only ideals of R are $\{0_R\}$ and R. Since R is a commutative ring, if we can show that every non-zero element of R has a multiplicative inverse, then we can conclude that R is a field.

Let $x \in R$ be a non-zero element. The principal ideal xR must be equal to R by assumption (since $xR \neq \{0_R\}$ as it contains x). Therefore xR contains 1_R and there is an element $x^{-1} \in R$ such that $xx^{-1} = x^{-1}x = R$. Thus, x has a multiplicative inverse in R.

□

Example 3.16. Let

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in \mathbb{R} \right\}$$

and

$$I = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}.$$

Show that I is an ideal of R.

We use Lemma 3.9.

We note that $I \neq \emptyset$ since I contains the 0 matrix.

Let $A = \begin{pmatrix} x_1 & y_1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} x_2 & y_2 \\ 0 & 0 \end{pmatrix}$ be elements of I and $C = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ be an element of R. Then

$$A - B = \begin{pmatrix} x_1 - x_2 & y_1 - y_2 \\ 0 & 0 \end{pmatrix} \in I,$$

$$AC = \begin{pmatrix} x_1 x & x_1 y + y_1 z \\ 0 & 0 \end{pmatrix} \in I$$

and,

$$CA = \begin{pmatrix} x x_1 & x y_1 \\ 0 & 0 \end{pmatrix} \in I.$$

It follows that I is an ideal of R.

Let $D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in R$. Observe that

$$DR := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in R \right\} = I.$$

Thus one might be tempted to conclude based on this that I is an ideal. However, R is not a commutative ring, and so the fact that $I = DR$ is enough only to show that I is a right ideal of R.

Lemma 3.12. *Let I and J be ideals of a ring R. Then $I \cap J$ is also an ideal of R and is the largest ideal contained in both I and J.*

Proof. Notice that if K is any ideal contained in both I and J, then K is contained in $I \cap J$. Therefore if $I \cap J$ is an ideal, it is the largest ideal contained in both I and J. We show below that $I \cap J$ is indeed and ideal of R.

I and J both contain 0_R and so $0_R \in I \cap J$.

Let $x, y \in I \cap J$ and $r \in R$. Then

$$x - y \in I \cap J$$

since $x - y \in I$ and $x - y \in J$, and,

$$rx, xr \in I \cap j$$

since $rx, xr \in I$ and $rx, xr \in J$. It follows that $I \cap J$ is an ideal of R.

□

Lemma 3.13. *Let R be a ring and let I and J be ideals of R. Then*

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

is also an ideal of R which contains I and J. Further, $I + J$ is the smallest ideal of R to contain both I and J.

Proof. Notice that $I = \{i + 0_R : i \in I\} \subseteq I + J$ since $0_R \in J$. Likewise $J \subseteq I + J$.

We note that if $I+J$ is an ideal, then it has to be the smallest ideal of R containing both I and J. For, if K is any ideal of R containing both I and J, then K must contain $I+J=\{i+j : i \in I, j \in j\}$.

We now show that $I+J$ is an ideal of R.

Let $i_1+j_1, i_2+j_2 \in I+J$, where $i_1, i_2 \in I$ and $j_1, j_2 \in J$, and let $r \in R$. Then:

$$\begin{aligned} (i_1+j_1)-(i_2+j_2) &= (i_1-i_2)(j_2-j_2) \in I+J, \\ r(i_1+j_1) &= ri_1+rj_1 \in I+j \text{ and} \\ (i_1+j_1)r &= i_1r = j_1r \in I+J. \end{aligned}$$

□

Lemma 3.14. *Let $\theta : R \longrightarrow S$ be a ring homomorphism. Then ker (θ) is an ideal of R.*

Proof. Note that ker (θ) is non-empty since it contains 0_R.

Let $x, y \in$ ker (θ) and $r \in R$. Then:

$$\begin{aligned} \theta(x-y) &= \theta(x)-\theta(y) = 0_S - 0_S = 0_S, \\ \theta(rx) &= \theta(r)\theta(x) = \theta(r)0_S = 0_S \text{ and} \\ \theta(xr) &= \theta(x)\theta(r) = 0_S\theta(r) = 0_S \end{aligned}$$

It follows that $x-y$, rx and rx are elements of ker (θ). Therefore ker (θ) is an ideal.

□

3.5 Factor Rings

Definition 3.19 (Coset)**.** Let R be a ring and let I be an ideal of R. Let $a \in R$. The *coset* of I in R determined by a is the set

$$a + I = \{a + b \mid b \in I\}.$$

So, $a + I$ is a subset of R; it consists of all those elements of R that differ from a by an element of I. Note that $a + I$ does not generally have algebraic structure in its own right, it is typically not closed under the addition or multiplication of R.

Example 3.17.

- Consider the ring $\mathbb{Z}$ and the ideal $I = 5\mathbb{Z}$. The distinct cosets of $5\mathbb{Z}$ are

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

  Note that $7, 12 \in 2+5\mathbb{Z}$, but $7+12 = 19$ is an element of $4+5\mathbb{Z}$ and *not* $2+5\mathbb{Z}$. Cosets are not necessarily closed under addition. Similarly, $8, 13 \in 3+5\mathbb{Z}$, but $8x13 \in 4+5\mathbb{Z}$ and not $3 + 5\mathbb{Z}$. Cosets are not necessarily closed under multiplication.

- Consider the ring $\mathbb{Q}[x]$. Let I be the ideal $(x^2 - 1)\mathbb{Q}[x]$. Then $(x - 1) \notin I$ and $(x - 1) + I$ is a non-trivial coset of I. Similarly $(x + 1) \notin I$ and so $(x + 1) + I$ is another non-trivial coset of I. Notice that $(x - 1)(x + 1) = x^2 - 1 \in I$.

Lemma 3.15. *Let a and b be elements of a ring R in which I is a two-sided ideal.*

1. *If $a - b \in I$, then $a + I = b + I$.*
2. *If $a - b \notin I$, the cosets $a + I$ and $b + I$ are disjoint subsets of R.*

Proof. 1. Suppose $a - b \in I$. Then there is an element $i \in I$ such that $a = i + b$ and

$b = a - i$. Let $j \in I$. Then

$$\begin{aligned} a + j &= i + b + j = b + (i + j) \in b + I \\ b + j &= a - i + j = a + (j - i) \in a + I. \end{aligned}$$

Therefore $a + I = b + I$.

2. Suppose $a - b \notin I$. Suppose $(a + I) \cap (b + I) \neq \emptyset$. Then there are $i_1, i_2 \in I$ such that $a + i_1 = b + i_2$. Rearranging:

$$a - b = (i_2 - i_1) \in I$$

which is a contradiction. Therefore $a + I \cap b + I = \emptyset$.'

□

Lemma 3.15 shows that the different cosets of I in R are disjoint subsets of R. Note that their union is all of R since every element a of R belongs to some coset of I in R ($a \in a+I$). The set of all cosets of I in R is denoted by R/I. Hence

$$R/I = \{a + I \mid a \in R\}.$$

It transpires that we can define addition and multiplication in R/I. However, we do have to ensure that the coset sum and the coset product do not depend on the choice of representative of the respective cosets. That is the subject of the following lemma.

Lemma 3.16. *Let R be a ring and $I \trianglelefteq R$. Then*

$$(a + I) + (b + I) = (a + b) + I$$

and

$$(a + I)(b + I) = ab + I$$

for all $a, b \in R$.

Proof. First we observe that $(a+b)+I$ is a subset of $(a+I)+(b+I)$. Similarly, $ab+I$ is a subset of $(a+I)(b+I)$. We now show that $(a+b)+I \subseteq (a+I)+(b+I)$ and $ab+I \subseteq (a+I)(b+I)$.

Let $i_1, i_2 \in I$ and consider:

$$(a+i_1)+(b+i_2) = (a+b)+(i_2+i_2) \in (a+b)+I$$

and

$$(a+i_1)(b+i_2) = ab+ai_2+i_1b+i_1i_1 = ab+(ai_2+i_1b+i_1i_1) \in ab+I$$

since $ai_1, i_1b \in I$ as I is an ideal.

Thus, $(a+b)+I \subseteq (a+I)+(b+I)$ and $ab+I \subseteq (a+I)(b+I)$. We conclude that $(a+b)+I = (a+I)+(b+I)$ and $ab+I = (a+I)(b+I)$

Now if $a', b' \in R$ are such that $a+I = a'+I$, and $b+I = b'+I$, then

$$(a'+I)+(b'+I) = (a+I)+(b+I) = (a+b)+I$$

and

$$(a'+I)(b'+I) = (a+I)(b+I) = (a+b)+I.$$

However, since $a' \in a'+I$ and $b' \in b'+I$, it follows that $(a'+b') \in (a+b)+I$. Therefore by Lemma 3.15 $(a'+b')+I = (a+b)+I$. Similarly, $a'b' \in (a'+I)(b'+I)$ and so $a'b' \in ab+I$. It follows by Lemma 3.15 that $a'b'+I = ab+I$.

Thus, coset sum and coset product are well-defined binary operations on R/I, the result is independent of the choice of coset representative.

□

Theorem 3.3. *The set R/I, when endowed with the addition and multiplication defined above, is a ring.*

Proof. That coset sum and coset product are closed follows from the definition. Thus to show that R/I is a ring, we only need verify the other ring axioms. We leave this as an exercise noting that the remaining axioms all follow from the fact that R is a ring. For example to see that coset sum is associative:

Let $a+I, b+I, c+I \in R/I$, we have:

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

□

Definition 3.20 (Factor ring)**.** Under the addition and multiplication given above, we define the resulting ring R/I to be the *factor ring* of R modulo I.

Theorem 3.4 (First Isomorphism Theorem)**.** *Let $\theta : R \longrightarrow S$ be a ring homomorphism. Then*

$$R/\mathit{ker}(\theta) \cong \mathit{im}(\theta).$$

Proof. Set $K = \ker(\theta)$.

Let $\phi : R/K \to \mathrm{im}\,(\theta)$ be defined by $\phi(r + K) = \theta(r)$.

First we show that ϕ is well-defined.

Let $r, r' \in R$ be such that $r + K = r' + K$. Then, using Lemma 3.15, there is a $k \in K$ such that $r' = r + k$. It follows that

$$\phi(r') = \theta(r + k) = \theta(r) + \theta(k) = \theta(r) + 0_S = \theta(r).$$

Thus ϕ is well-defined.

Now we show that ϕ is an isomorphism.

It is clear that ϕ is surjective. To see that ϕ is injective, let $r + K, r' + K \in R/K$ and suppose that $\phi(r + K) = \phi(r' + K)$. Then

$$\theta(r) = \theta(r')$$

and so

$$\theta(r - r') = \theta(r) - \theta(r') = 0_S.$$

It follows that $r - r' \in K$. Thus, by Lemma 3.15 $r + kr' + k$. Thus ϕ is injective.

To see that ϕ is a homomorphism, let $r + K, r' + K \in R/K$, then

$$\begin{aligned}
\phi((r + K) + (r' + k)) &= \phi((r + r') + K) \\
&= \theta(r + r') \\
&= \theta(r) + \theta(r') \\
&= \phi(r + K) + \phi(r' + k)
\end{aligned}$$

and

$$\begin{aligned}\phi((r+K)(r'+k)) &= \phi((rr')+K) \\ &= \theta(rr') \\ &= \theta(r)\theta(r') \\ &= \phi(r+K)\phi(r'+k).\end{aligned}$$

□

3.6 Problem Sheet 3

Questions 3.31 – 3.7 for Week 8; Questions 3.8 – 3.11 for Week 10.

Question 3.1

Let R be a ring. The centre of R is defined as

$$Z(R) = \{a \in R : ab = ba \quad \text{for all} \quad b \in R\}.$$

Prove that $Z(R)$ is a subring of R.

Show Solution 3.1 on P178

Question 3.2

Let R be a ring. Prove that if $a \in R$ is a unit then its inverse is unique.

Show Solution 3.2 on P179

Question 3.3

A ring R is called *Boolean* if every element of R is idempotent (i.e. for all $x \in R$, $x^2 = x$)

a. Show that if R is Boolean then any nonzero element $x \in R$ has period two in the group $(R, +)$.

b. Show that any Boolean ring is necessarily commutative.

Show Solution 3.3 on P179

Question 3.4

Let

$$S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

Prove that S is a subring of $M_2(\mathbb{R})$.

[Note that the S and $M_2(\mathbb{R})$ each have identity elements but they are not the same]

Show Solution 3.4 on P180

Question 3.5

Let R be a ring. Show that, for a positive integer n, the ring $M_n(R)$ of $n \times n$ matrices over R is commutative if and only if $R = \{0\}$, or $n = 1$ and R is commutative.

Show Solution 3.5 on P181

Question 3.6

Let D be an integral domain.

a. Show that, for all $x \in D$,

$$x^2 = 1 \Rightarrow x = 1 \text{ or } x = -1.$$

b. Deduce that if D contains only finitely many units then the product of these units equals -1.

c. Finally show that, for every prime integer p,

$$(p-1)! \equiv -1 \pmod{p}.$$

This is Wilson's Theorem.

Show Solution 3.6 on P182

Question 3.7

Let R be a commutative ring. Show that

$$Z(M_n(R)) = \{aI_n : a \in R\}.$$

[For the trickier $\subseteq$ containment, it might be useful to consider the *matrix unit* which is the matrix $E_{ik} \in M_n(R)$ where the (i,k)th entry of E_{ik} is the integer 1 and all other entries are zero. Then any $A = (a_{ik}) \in M_n(R)$ can be written as $A = \sum_{i,k=1}^{n} a_{ik}E_{ik}$.]

Show Solution 3.7 on P183

Question 3.8

Let R be a commutative ring and let $a \in R$. Show that the set

$$I = \{x \in R : xa = 0\}$$

is an ideal of R. (This ideal is sometimes called the *annihilator* of $a \in R$)

Show Solution 3.8 on P184

Question 3.9

Let R be the set of all matrices of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

over $\mathbb{Q}$ such that $a = d$ and $b = 0$. Let I be the subset of R such that $a = d = 0$. Show that

$$R/I \cong \mathbb{Q}.$$

[Hint : think about defining a homomorphism...]

Show Solution 3.9 on P184

Question 3.10

Let R be a ring and let $J \trianglelefteq R$. Show that $R \diagup J$ is commutative if and only if $xy - yx \in J$ for all $x, y \in R$.

Deduce that, if $K_1, K_2 \trianglelefteq R$ and both $R \diagup K_1$ and $R \diagup K_2$ are commutative, then $R \diagup (K_1 \cap K_2)$ is also commutative.

Show Solution 3.10 on P186

Question 3.11

Let D be an integral domain and let $0 \neq I, J \trianglelefteq D$. Show that $I \cap J \neq 0$.

Show Solution 3.11 on P186

Chapter 4

Special Types of Rings and Ideals

4.1 Principal Ideal Domains

Definition 4.1 (Principal Ideal Domain)**.** An integral domain in which every ideal is principal is called a *principal ideal domain*, or PID for short.

Lemma 4.1. *The ring $\mathbb{Z}$ is a PID*

Proof. Let I be any ideal of $\mathbb{Z}$. Then $(I, +)$ is a subgroup of $(\mathbb{Z}, +)$. Since $(\mathbb{Z}, +)$ is a cyclic group generated by 1, and every subgroup of a cyclic group is cyclic, it follows that $(I, +)$ is cyclic generated by some $m \in \mathbb{Z}$. Thus, $I =, \mathbb{Z} = \{mk : k \in \mathbb{Z}\}$.

□

Example 4.1. What about other PID's? The following are examples of PID's:

- Polynomials in one variable over a field
- $\mathbb{Z}[\sqrt{2}]$ is a PID.
- $\mathbb{Z}[i]$ is a PID (as we will see later).

We now reconsider an old idea in terms of principal ideals.

Lemma 4.2. *Let R be a commutative ring and let $a, b \in R$. Then $a \,|\, b$ if and only if $bR \subseteq aR$.*

Proof. **(⇒)** Suppose that $a \,|\, b$. Then $b = as$ for some $s \in R$. It follows that

$$bR = \{br : r \in R\} = \{asr : r \in R\} \subseteq aR.$$

(⇐) Suppose that $bR \subseteq aR$. Now $b = b1_R \in bR$ and so $b \in aR$. This means we can find an $s \in R$ such that $b = as$ as required.

□

Example 4.2.

Let $R = \mathbb{Z}$ and consider the principal ideal $3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$. Now $6\mathbb{Z} = \{\dots, -12, -6, 0, 6, 12, \dots\}$ is clearly a subset of $3\mathbb{Z}$ and $3|6$.

4.2 Maximal Ideals

Definition 4.2 (Maximal ideal). Let R be a ring and let I be an ideal of R. We say that I is a *maximal* ideal of R if $I \neq R$ and, whenever J is an ideal of R then

$$I \subseteq J \subseteq R \Rightarrow I = J \text{ or } J = R.$$

Example 4.3.

- In the ring $R = \mathbb{Z}$, for a prime p, the ideal $p\mathbb{Z}$ is maximal. Suppose $p\mathbb{Z} \subseteq J$ for an ideal J of $\mathbb{Z}$. Now as $\mathbb{Z}$ is a PID, $J = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. By Lemma 4.2, since $p\mathbb{Z} \subseteq m\mathbb{Z}$, it follows that $m|p$. Thus $m = 1$ or $m = p$. In which case $m\mathbb{Z} = p\mathbb{Z}$ or $m\mathbb{Z} = \mathbb{Z}$.

- Consider $R = \mathbb{Z}_{12}$. We claim that $2R$ is a maximal ideal. Let J be any ideal of R such that $2R \subseteq J$. There are two ways to proceed, since $(J, +)$ is a subgroup of $(\mathbb{Z}_{12}, +)$ and $(\mathbb{Z}_{12}, +)$ is cyclic generated by 1, it follows that $J = mR$ for some $m \in \mathbb{Z}_{12}$. By Lemma 4.2 again, it follows that $m|2$ and so $m = 1$ or $m = 2$. Thus mR is either $2R$ or R.

  An alternative argument is as follows. Suppose that $J \neq R$. We will show that $J = 2R$. Since $J \neq R$, then Jt cannot contain any of the units of R. The units of R are precisely, $1, 5, 7$ and 11 (all elements of $\mathbb{Z}_{12}$ co-prime to 12.) Now, if $J \neq 2R$, then J must contain both 3 or 9 (since 9 is the additive inverse of 3 in Z_{12} and so if J contains 3 is must also contain 9 and vice versa). However if $3 \in J$, since $2R \subseteq J$, it follows that $2 + 3 = 5 \in J$, in which case $J = R$ yielding a contradiction. Thus, it must be the case that $J = 2R$ as required.

Lemma 4.3. *Let R be a commutative ring and let $I \trianglelefteq R$. Then R/I is a field if and only if I is a maximal ideal.*

Proof.

(⇒) Suppose R/I is a field. Let J be any ideal of R such that $I \subseteq J$. We observe that J/I is an ideal of R/I. Clearly J/I is a subring of R/I. Let $r + I \in R/I$ and

$j+I \in J/I$. Then

$$(r+I)(j+I) = (rj)+I = (jr)+I = (j+I)(r+I) \in J/I.$$

Therefore J/I is an ideal of R/I. Since R/I is a field, then by Theorem 3.2, J/I is either equal to $\{0_{R/I}\}$ or R/I. If $J/I = \{0_{R/I}\}$, then $J = I$, while if $J/I = R/I$ then $J = R$. Therefore, as J was an arbitrarily chosen ideal containing I, it follows that I is a maximal ideal of R.

($\Leftarrow$) Suppose I is a maximal ideal of R. We may assume that R/I is non-zero since otherwise we are done. Let $r+I$ be any non-zero element of R/I. It follows that $r \neq I$. Set $J = (rR+I)$. Notice that J is an ideal of R (since the sum of two ideals is again an ideal) and $I \subsetneq J$ since $r = r1_R + 0_R \in J\backslash I$. Since I is maximal then J is either I or R. Thus J must be equal to R as $J/I \neq \{0_R + I\}$. This means there is an element $s \in R$ and an element $l \in I$ such that $rs + l = 1_R$. Therefore $rs - 1_R \in I$. It follow then that

$$(r+I)(s+I) = (rs)+I = (sr)+I = (s+I)(r+I) = I$$

by Lemma 3.9. Therefore $(r+I)$ is an invertible element of (R/I). We conclude, since $(r+I)$ was an arbitrarily chosen non-zero element of R/I, that every non-zero element of R/I is invertible and R/I is a field.

□

Example 4.4.

We have seen that all ideals of $\mathbb{Z}$ have the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. The question now arises: for which n is the ideal $n\mathbb{Z}$ maximal?

Define the homomorphism $\theta : \mathbb{Z} \to n\mathbb{Z}$ given by $\theta(a) = [a]_n$. It is an exercise to verify that θ is a ring homomorphism.

Notice that

$$\ker(\theta) = \{a \in \mathbb{Z} : [a]_n = [0]_n\} = \{a \in \mathbb{Z} : n|a\} = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}.$$

By the First Isomorphism Theorem (Theorem 3.4) $R/\ker(\theta) \cong \mathbb{Z}_n$. By Lemma 4.3 $\mathbb{Z}_n$ is a field if and only if $n\mathbb{Z}$ is a maximal ideal. We know that $\mathbb{Z}_n$ is a field if and only if n is prime. It follows that $n\mathbb{Z}$ is a maximal ideal if and only if n is prime.

Theorem 4.1. *If R is a PID, then for a non-zero, non-unit element $x \in R$, xR is maximal if and only if x is irreducible.*

Proof.

(⇒) Suppose xR is maximal and $x = yz$ for some $y, z \in R$. Then by Lemma 4.2, $xR \subseteq yR$. Since xR is maximal, then $yR = R$ or $yR = xR$. If $yR = R$ then y is a unit. If $yR = xR$, then there is an $r \in R$ such that $y = xr$. It follows that $x = yz = xrz$. Since R is an integral domain, and $x \neq 0_R$, we conclude that $rz = zr = 1_R$ and z is a unit.

(⇐) Suppose x is irreducible. Let J be any ideal such that $xR \subseteq J$. Since R is a PID, there is a $y \in R$ such that $J = yR$. Since $xR \subseteq yR$, then $x = yz$ for some $z \in R$. Since x is irreducible, then y or z is a unit. If y is a unit, we are done. If z is a unit. Then $xz^{-1} = y$, in which case $yR \subseteq xR$ and so $J = yR = xR$.

□

4.3 Prime ideals

Definition 4.3 (Prime ideal)**.** Let R be a commutative ring. An ideal P of R is a *prime ideal* if $P \neq R$ and

$$xy \in P \Rightarrow x \in P \text{ or } y \in P.$$

Example 4.5.

- Consider the $R = \mathbb{Z}$ and p a prime. Then $p\mathbb{Z}$ is a prime ideal. For if $xy \in p\mathbb{Z}$, then $p|xy$. Since p is prime, then $p|x$ or $p|y$.
- In $\mathbb{Z}[x]$, then the ideal $I = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$ is a prime ideal. This is the ideal of all polynomials over $\mathbb{Z}$ with an even constant term.

Lemma 4.4. *Let R be a commutative ring and let $I \trianglelefteq R$. Then R/I is an integral domain if and only if I is a prime ideal.*

Proof.

($\Rightarrow$) Suppose R/I is an integral domain. Let $x, y \in R$ be such that $xy \in I$. Then it follows that $(x + I)(y + I) = (xy) + I = 0_R + I$. Since R/I is an integral domain, then $x + I = 0_R + I$ or $y + I = 0_R + I$. Thus, $x \in I$ or $y \in I$.

($\Leftarrow$) Suppose that I is a prime ideal. Let $x+I, y+I \in R/I$ be such that $(x+I)(y+I) = xy + I = 0_R + I$. It follows that $xy \in I$. Since I is a prime ideal, $x \in I$ or $y \in I$. In which case, $x + I = 0_R + I$ or $y + I = 0_R + I$ and R/I is an integral domain.

□

Theorem 4.2. *Let R be a PID. Then:*

1. *every nonzero prime ideal is maximal;*

2. *every irreducible element is prime.*

Proof. 1. Let I be a nonzero prime ideal of R. Let J be any ideal of I such that $I \subseteq J$. There are $x, y \in R$ such that $I = xR$ and $J = yR$. Since $I \subseteq J$ it follows that $x = yz$ for some $z \in R$. Thus $yz \in I$. Since I is a prime ideal, then $y \in I$ or $z \in I$. If $y \in I$, then $yR \subseteq xR$ and $I = J$. If $z \in I$, then $z = xt$ for some $t \in R$. In which case $x = yxt = xyt$. Since x is nonzero, (as xI is nonzero), and R is a PID, then $yt = 1_R$ and $yR = R$. It follows that any ideal which contains I is either equal to I or R.

2. Let x be an irreducible element of R. Then xR is a maximal ideal and so R/xR is a field. A field is an integral domain and so xR is a prime ideal. Thus, if $x|yz$ for some $y, z \in R$, then $yz \in xR$ and so $y \in xR$ or $z \in xR$, in other words, $x|y$ or $x|z$. Therefore x is prime.

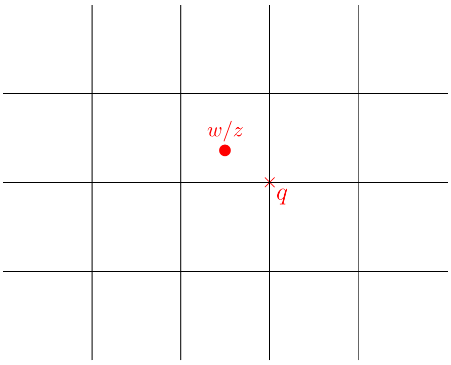
□

Example 4.6. The ring of Gaussian Integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ is a PID.

Since $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, then $\mathbb{Z}[i]$ is an integral domain. Set $R = \mathbb{Z}[i]$ and let I be any nonzero ideal of R. Let $z \in I$ be a non-zero element such that $|z|$ is minimal amongst the elements of $I \backslash \{0\}$. We note that z exists since I is non-zero.

We show that $I = zR$. Clearly, as $z \in I$, then $zI \subseteq I$. It remain show then that $I \subseteq zI$.

Let $w \in I$ be any non-zero element. Consider the element $w/z \in \mathbb{C}$. We can find a $q \in R$ such that $|w/z - q|^2 \leq 1/2$.



Set $r = w - qz$, and observe that $r \in I$ since both w and qz are elements of I. We compute

$$|r|^2 = |w - qz|^2 = |z|^2 |w/z - q|^2 \leq |z|^2/2.$$

Thus, $|r| < |z|$ and so r must be equal to 0_R (since $|z|$ is smallest amongst all non-zero elements of R). We conclude that $w = qz$ and so $I = zR$.

4.4 Unique Factorisation Domains

Consider in $\mathbb{Z}$ the factorisation of the integer 308 :

$$2^2 \times 7 \times 11$$

and

$$11 \times 7 \times 2^2.$$

Clearly these two factorisations should be regarded as the same since $\mathbb{Z}$ is commutative. We also observe that these factorisations for 308 are complete and so are superior to, say, $308 = 14 \cdot 22$.

Causing us slightly more trouble is the notion that we can change the sign of some of the integers without altering the fact that we have a factorisation e.g.

$$(-2)^2 \times 7 \times 11.$$

We now set ourselves the task of assessing when two factorisations of an element in an arbitrary commutative ring are 'essentially the same'.

Definition 4.4. Let R be a ring and let $x, y \in R$. We say that x is *associated* to y if there exists a unit $u \in R$ such that $ux = y$.

Now let $r \in R$ be such that

$$r = x_1 x_2 ... x_s = y_1 y_2 ... y_t.$$

Then we say that these factorisations for $r \in R$ are *essentially the same* if

1. $s = t$, and
2. there exists a permutation $\sigma \in S_s$ such that, for each i, $x_{\sigma(i)}$ is associated to y_i.

Definition 4.5 (Unique Factorisation Domain)**.** Let R be an integral domain. We say that R is a *unique factorisation domain* (or UFD) if every nonzero non-unit of R can be expressed as a product of irreducibles in an essentially unique way.

Example 4.7.

- The ring $\mathbb{Z}$ is a unique factorisation domain.
- The ring $\mathbb{Z}[i]$ is a unique factorisation domain.

Definition 4.6 (Greatest common divisor)**.** Let R be a commutative ring and let $a, b \in R$. We say that an element $d \in R$ is a *common divisor* of a and b if $d \,|\, a$ and $d \,|\, b$.

We say that a common divisor $d \in R$ of a and b is a *greatest common divisor* of a and b if, for all $c \in R$, $c \,|\, a$ and $c \,|\, b \Rightarrow c \,|\, d$. In this case we write $d = \text{gcd}\,(a, b)$.

Greatest common divisors in a PID

Let R be a PID and let m and n be elements of R. Consider the ideal $I = mR + nR$. Since R is a PID, there is an $l \in R$ such that $I = lR$. It follows that $l|m$ and $l|n$ since $m, n \in I = lR$. Therefore l is a common divisor of m and n.

Suppose k is an element of R such that $k|m$ and $k|n$. Then $mR \subseteq kR$ and $nr \subseteq kR$. Therefore $I = (mR + kR) \subseteq kR$. It follows that $k|t$. Therefore, t is a greatest common divisor of m and n.

Example 4.8. Let $\alpha = 6 + i$, $\beta = 1 + 2i \in \mathbb{Z}[i]$. Find a greatest common divisor of α and β and hence find $\gamma \in \mathbb{Z}[i]$ such that $\gamma\mathbb{Z}[i] = \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$.

Let $\gamma = x + iy$, $x, y \in \mathbb{Z}$ be an element of $\mathbb{Z}[i]$ such that $\gamma \,|\, \alpha$ and $\gamma \,|\, \beta$. It follows that $|\gamma|^2 \,|\, |\alpha|^2 = 37$ and $|\gamma|^2 \,|\, |\beta|^2 = 5$. Therefore $|\gamma|^2 = 1$. Since x and y are integers, either $x^2 = 1$ and $y = 0$ or $y^2 = 1$ and $x^2 = 0$. Since ± 1 and $\pm i$ divide any element of $\mathbb{Z}[i]$, it follows that $\{\pm 1, \pm i\}$ is the full list of (greatest) common divisors of α and β. Therefore, $\gamma \in \{\pm 1, \pm i\}$. Notice that $\gamma\mathbb{Z}[i] = \mathbb{Z}[i]$ for any such choice of γ, since ± 1 and $\pm i$ are units. Therefore, if $\gamma\mathbb{Z}[i] = \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$, then γ is a common divisor of α and β and $\gamma\mathbb{Z}[i] = \mathbb{Z}[i]$.

Now suppose $\alpha = 4 + 3i$ and $\beta = 2 - i$.

Let $\gamma = x + iyin\mathbb{Z}[i]$ be such that γ divides both α and β. We find that $|\gamma|^2 \,|\, 25$ and $|\gamma|^2 \,|\, 5$.

if $|\gamma|^2 \,|\, 5$, and $|\gamma|^2 \neq 1$ then $|\gamma|^2 = 5$. Therefore $x^2 + y^2 = 5$. The only integer solutions to this are $x = \pm 2$ and $y = \pm 1$ or $x = \pm 1$ and $y^2 = \pm 2$.

First observe that since $i(x + iy) = -y + ix$, then any possible common divisors γ with $|\gamma|^2 = 5$ is a product of a unit times an element of $\{2+i, 2-i\}$. Therefore if α and β have a common divisor γ with $|\gamma|^2 = 5$, then either $2 + i$ or $2 - i$ is a common divisor of α and β.

First we try $\gamma = 2 + i$. Let $a, b \in \mathbb{Z}$ and suppose $(2 + i)(a + ib) = 4 + 3i$. Then $(2a - b) + i(a + 2b) = 4 + 3i$. Solving these simultaneous equations, we get that $5a = 11$, but there is no integer a satisfying this equation. We conclude that $(2 + i)$ does not divide a.

Next we try $\gamma = 2 - i$. Let $a, b \in \mathbb{Z}$ and suppose $(2 - i)(a + ib) = 4 + 3i$. Then $(2a + b) + i(-a + 2b) = 4 + 3i$. Solving this system of equations, we get $a = 1$ and $b = 2$. Therefore $\gamma \,|\, a$. Notice that $b = \gamma$ and so $\gamma \,|\, b$.

It follows that $\gamma = 2 - i$ is a common divisor of a and b. Notice that $\gamma = 2 - i$ must be a greatest common divisor of a and b since any other divisor is either a unit or the product of γ and a unit.

Therefore,an element $\gamma \in \mathbb{Z}[i]$ satisfying $\gamma\mathbb{Z}[i] = \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$ is $(2 - i)$.

4.5 Problem Sheet 4

For Week 10.

Question 4.1

Let R be a ring. Prove that the ideals of the ring $M_n(R)$ are the subsets of the form $M_n(Q)$ where $Q \trianglelefteq R$.

Show Solution 4.1 on P187

Question 4.2

Let R be a PID and $a, b \in R$ be both nonzero. Show that there is a $c \in R$ such that

a. $a|c$ and $b|c$;

b. If $a \mid d$ and $b \mid d$ then $c \mid d$.

Show Solution 4.2 on P188

Question 4.3

Let R be a commutative ring and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be a chain of *proper* ideals of R. Prove that

$$I = \bigcup_{i=1}^{\infty} I_i$$

is a proper ideal of R.

Show Solution 4.3 on P189

Question 4.4

Let R be a PID show that there is *not* an infinite sequence of ideals $J_1, J_2, J_3, \ldots$ such that $J_n \subsetneq J_{n+1}$ for all $n \in N$.

Show Solution 4.4 on P189

Question 4.5

Let R be a PID, prove that R is a UFD.

Show Solution 4.5 on P190

Question 4.6

Let $\mathcal{F}$ be a field. Show that $\mathcal{F}[x]$ is a principal ideal domain.

[You may use the fact that given $f, g \in \mathcal{F}[x]$, there exist unique $q, r \in \mathcal{F}[x]$ such that $f = qg + r$ and either $r = 0$ or the degree of r is strictly less than the degree of G.]

Show Solution 4.6 on P192

Question 4.7

Consider the ring $R = \mathbb{Q}[x]$.

i. Show that $x^5 - 7$ is a prime.

ii. Let $I = (x^5 - 7)R$. Show that R/I is a field.

Show Solution 4.7 on P192

Question 4.8

Consider the guassian integers $\mathbb{Z}[i]$. Let $\alpha = 10 + 11i$ and $\beta = 8 + i$. Find $\gamma \in \mathbb{Z}[i]$ such that $\gamma\mathbb{Z}[i] = \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$.

Show Solution 4.8 on P193

Appendix A

All Solutions

A.1 Chapter 1 solutions

Solution R.1

Verify that the set of all positive real numbers, $\mathbb{R}_{>0}$, is a vector space over $\mathbb{R}$ when given the addition and scalar multiplication defined below:

$$x \oplus y = xy, \qquad \lambda x = x^{\lambda}$$

for all positive real numbers $x, y \in \mathbb{R}_{>0}$ and for all $\lambda \in \mathbb{R}$.

Observe that here we need to check ALL the vector space axioms.

A0. This Holds since for all $x, y \in \mathbb{R}_{>0}$, $x \oplus y = xy \in \mathbb{R}_{>0}$.

A1. Holds since for all $x, y, z \in \mathbb{R}_{>0}$,

$$\begin{aligned} x \oplus (y \oplus z) &= x \oplus yz \\ &= x(yz) \\ &= (xy)z \\ &= xy \oplus z \\ &= (x \oplus y) \oplus z. \end{aligned}$$

A2. Holds since for all $x, y \in \mathbb{R}_{>0}$, $x \oplus y = xy = yx = y \oplus x$.

A3. Holds since $1 \in \mathbb{R}_{>0}$ and, for all $x \in \mathbb{R}_{>0}$, $x \oplus 1 = x1 = x$ and $1 \oplus x = 1x = x$. (Note, in particular, that the role of the zero vector here is played by the real number 1).

A4. Holds since, for all $x \in \mathbb{R}_{>0}$, $1/x \in \mathbb{R}_{>0}$ and $x \oplus 1/x = x(1/x) = 1$ and $1/x \oplus x = (1/x)x = 1$. Hence the negative of $x \in \mathbb{R}_{>0}$ is the element $1/x$.

M0. Holds since for all $x \in \mathbb{R}_{>0}$, $\lambda \in \mathbb{R}$, $\lambda x = x^{\lambda} \in \mathbb{R}_{>0}$.

M1. Holds since for all $x, y \in \mathbb{R}_{>0}$ and for all $\lambda \in \mathbb{R}$,

$$\begin{aligned}\lambda(x \oplus y) &= \lambda(xy)\\ &= (xy)^{\lambda}\\ &= x^{\lambda}y^{\lambda}\\ &= \lambda x \oplus \lambda y.\end{aligned}$$

M2. Holds since for all $x \in \mathbb{R}_{>0}$ and for all $\lambda, \mu \in \mathbb{R}$,

$$\begin{aligned}(\lambda + \mu)x &= x^{\lambda+\mu}\\ &= x^{\lambda}x^{\mu}\\ &= \lambda x \oplus \mu x.\end{aligned}$$

M3. Holds since for all $x \in \mathbb{R}_{>0}$ and for all $\lambda, \mu \in \mathbb{R}$,

$$\begin{aligned}\lambda(\mu x) &= \lambda x^{\mu} \\ &= (x^{\mu})^{\lambda} \\ &= x^{\mu\lambda} \\ &= x^{\lambda\mu} \\ &= (\lambda\mu)x.\end{aligned}$$

M4. Holds since for all $x \in \mathbb{R}_{>0}$ we have $1x = x^1 = x$.

This shows that all the vector space axioms hold and hence $\mathbb{R}_{>0}$ equipped with this scalar multiplication and addition is a vector space.

Return to Question R.1 on P33

Solution R.2

Consider $\mathbb{R}^2$ with the usual addition but with scalar multiplication defined as

$$\lambda(x, y) = (\lambda x, y)$$

for all $(x, y) \in \mathbb{R}^2$, $\lambda \in \mathbb{R}$. Show that $\mathbb{R}$ equipped with the usual addition and this scalar multiplication is not a vector space.

Here we just need to find one axiom where it all goes a bit pear-shaped and obviously it will be something to do with this scalar multiplication.

Axiom (M2) is the one which causes us trouble here. Consider the vector $\mathbf{x} = (1, 1) \in \mathbb{R}^2$ and $\lambda = \mu = 1$. Then

$$\lambda\mathbf{x} + \mu\mathbf{x} = (1, 1) + (1, 1) = (2, 2).$$

However

$$(\lambda + \mu)\mathbf{x} = 2(1,1) = (2,1).$$

Hence $(\lambda + \mu)\mathbf{x} \neq \lambda\mathbf{x} + \mu\mathbf{x}$ and so (M2) fails and $\mathbb{R}^2$ with this addition and scalar multiplication is not a vector space.

Return to Question R.2 on P33

Solution R.3

Show that the subset

$$A = \{(x,y,z) \mid x + 2y + 3z = 0\}$$

is a subspace of $\mathbb{R}^3$***.***

Observe that $A \subset \mathbb{R}^3$. Now $(0,0,0) \in A$ since $0 + 2 \times 0 + 3 \times 0 = 0$ and so $A \neq \phi$.

Let $(a,b,c),(x,y,z) \in A$. Then $a + 2b + 3c = x + 2y + 3z = 0$. Now $(a,b,c) + (x,y,z) = (a+x, b+y, c+z)$ and

$$\begin{aligned} a + x + 2(b+y) + 3(c+z) &= a + x + 2b + 2y + 3c + 3z \\ &= (a + 2b + 3c) + (x + 2y + 3z) \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Hence $(a,b,c) + (x,y,z) \in A$.

Finally, let $(x,y,z) \in A$ and $\lambda \in \mathbb{R}$. Then $\lambda(x,y,z) = (\lambda x, \lambda y, \lambda z)$ and

$$\lambda x + 2\lambda y + 3\lambda z = \lambda(x + 2y + 3z) = \lambda(0) = 0.$$

Hence $\lambda(x,y,z) \in A$ and A is a subspace of $\mathbb{R}^3$.

Return to Question R.3 on P33

Solution R.4

Determine whether each of the following sets are subspaces of $\mathbb{R}^2$. You should either prove that the set is a subspace or provide an appropriate counterexample as to why the set does not form a subspace.

a. $A = \{(x, y) \in \mathbb{R}^2 \mid y = 2x\}$.

b. $B = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0, \; y \geq 0\}$.

c. $C = \{(x, y) \in \mathbb{R}^2 \mid x = 0\}$.

d. $D = \{(x, y) \in \mathbb{R}^2 \mid xy \geq 0\}$.

a. A is a subspace of $\mathbb{R}^2$. Note that $A \subset \mathbb{R}^2$. The zero vector $(0, 0) \in A$ so $A \neq \phi$.

Now let $(x, 2x), (y, 2y) \in A$. Then

$$(x, 2x) + (y, 2y) = (x + y, 2x + 2y) = (x + y, 2(x + y)) \in A.$$

Finally, let $(x, 2x) \in A$ and $\lambda \in \mathbb{R}$. Then

$$\lambda(x, 2x) = (\lambda x, 2(\lambda x)) \in A.$$

Hence A is a subspace of $\mathbb{R}^2$.

b. B is not a subspace of $\mathbb{R}^2$. Consider the vector $\mathbf{x} = (1, 1) \in B$. Then we have

$$-1\mathbf{x} = (-1, -1) \notin B.$$

Hence B is not closed under scalar multiplication and so is not a subspace of $\mathbb{R}^2$.

c. C is a subspace of $\mathbb{R}^2$. Note that $C \subset \mathbb{R}^2$. The zero vector $(0, 0) \in C$ so $C \neq \phi$.

Now let $\mathbf{x} = (0, a), \mathbf{y} = (0, b) \in C$. Then

$$\mathbf{x} + \mathbf{y} = (0, a + b) \in C.$$

Finally, let $\mathbf{x} = (0, a) \in C$ and $\lambda \in \mathbb{R}$. Then

$$\lambda \mathbf{x} = (0, \lambda a) \in C.$$

Hence C is a subspace of $\mathbb{R}^2$.

d. D is not a subspace. The vectors $(1, 1)$ and $(-2, 0)$ are both in the set D but

$$(1, 1) + (-2, 0) = (-1, 1) \notin D.$$

Hence D is not closed under addition and is not a subspace of $\mathbb{R}^2$.

Return to Question R.4 on P34

Solution R.5

In $\mathbb{R}_{2\times 2}$***, let***

$$A = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & -3 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 3 & 7 \\ -1 & 8 \end{pmatrix}.$$

a. ***Show that*** $A \in \mathbf{span}\,(B, C, D)$***.***

b. ***Find necessary and sufficient conditions on*** $a, b, c, d \in \mathbb{R}$ ***for*** $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{span}\,(A, B)$***.***

a. We require

$$\begin{aligned}\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} &= \alpha \begin{pmatrix} 1 & 0 \\ -2 & -3 \end{pmatrix} + \beta \begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix} + \gamma \begin{pmatrix} 3 & 7 \\ -1 & 8 \end{pmatrix} \\ &= \begin{pmatrix} \alpha & 0 \\ -2\alpha & -3\alpha \end{pmatrix} + \begin{pmatrix} 0 & 3\beta \\ -\beta & \beta \end{pmatrix} + \begin{pmatrix} 3\gamma & 7\gamma \\ -\gamma & 8\gamma \end{pmatrix}.\end{aligned}$$

This gives rise to the system of equations

$$\begin{aligned} \alpha + 3\gamma &= 2 \\ 3\beta + 7\gamma &= -1 \\ -2\alpha - \beta - \gamma &= 0 \\ -3\alpha + \beta + 8\gamma &= 1. \end{aligned}$$

As you should verify via standard echelon reduction, this system has the unique solution $\alpha = \frac{1}{2}$, $\beta = -\frac{3}{2}$ and $\gamma = \frac{1}{2}$. Hence $A \in \operatorname{span}(B, C, D)$ since

$$A = \frac{1}{2}B - \frac{3}{2}C + \frac{1}{2}D.$$

b. We require

$$\begin{aligned}\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \alpha \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 1 & 0 \\ -2 & -3 \end{pmatrix} \\ &= \begin{pmatrix} 2\alpha & -\alpha \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ -2\beta & -3\beta \end{pmatrix}.\end{aligned}$$

This leads to the system of equations

$$\begin{aligned} 2\alpha + \beta &= a \\ -\alpha &= b \\ -2\beta &= c \\ \alpha - 3\beta &= d \end{aligned}$$

with augmented matrix

$$\left(\begin{array}{cc|c} 2 & 1 & a \\ -1 & 0 & b \\ 0 & -2 & c \\ 1 & -3 & d \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & -b \\ 0 & 1 & 2b+a \\ 0 & 0 & 2a+4b+c \\ 0 & 0 & 3a+7b+d \end{array}\right).$$

Hence necessary and sufficient conditions for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{span}(A, B)$ are $3a + 7b + d = 0$ and $2a + 4b + c = 0$.

Return to Question R.5 on P34

Solution R.6

For each of the following vector spaces, find a basis and hence state the dimension of the given space.

a. $C(A) = \{B \in \mathbb{R}_{2\times 2} \mid AB = BA\}$ ***where*** $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

b. $\{p \in P_5 \mid \int_0^1 p(x)dx = 0\}$.

a. Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}_{2\times 2}$. Then

$$\begin{aligned} B \in C(A) &\Leftrightarrow AB = BA \\ &\Leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \\ &\Leftrightarrow c = 0,\ \ a = d. \end{aligned}$$

Hence

$$C(A) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

Hence if $B = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in C(A)$, then

$$B = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Thus the sequence

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$$

spans $C(A)$. Now suppose that

$$\alpha\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \quad (\alpha, \beta \in \mathbb{R})$$

Then

$$\begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and so equating entries, we see that we must have $\alpha = \beta = 0$. This demonstrates that the sequence

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right)$$

is L.I. It follows that the above sequence is a basis of $C(A)$ and so $\dim(C(A)) = 2$.

b. Let

$$S = \{p \in P_5 \mid \int_0^1 p(x)dx = 0\}.$$

$$\begin{aligned}
&p(x) = a + bx + cx^2 + dx^3 + ex^4 + fx^5 \in S \\
&\Leftrightarrow \int_0^1 a + bx + cx^2 + dx^3 + ex^4 + fx^5 \, dx = 0 \\
&\Leftrightarrow \left[ax + \frac{bx^2}{2} + \frac{cx^3}{3} + \frac{dx^4}{4} + \frac{ex^5}{5} + \frac{fx^6}{6} \right]_0^1 = 0 \\
&\Leftrightarrow a + \frac{b}{2} + \frac{c}{3} + \frac{d}{4} + \frac{e}{5} + \frac{f}{6} = 0 \\
&\Leftrightarrow a = -\frac{f}{6} - \frac{e}{5} - \frac{d}{4} - \frac{c}{3} - \frac{b}{2} \\
&\Leftrightarrow p(x) = (-\frac{f}{6} - \frac{e}{5} - \frac{d}{4} - \frac{c}{3} - \frac{b}{2}) + bx + cx^2 + dx^3 + ex^4 + fx^5 \\
&= b(-\frac{1}{2} + x) + c(-\frac{1}{3} + x^2) + d(-\frac{1}{4} + x^3) + e(-\frac{1}{5} + x^4) + f(-\frac{1}{6} + x^5).
\end{aligned}$$

Hence the sequence $(-\frac{1}{2} + x, \ -\frac{1}{3} + x^2, \ -\frac{1}{4} + x^3, \ -\frac{1}{5} + x^4, \ -\frac{1}{6} + x^5)$ spans

S. Now suppose that

$$\lambda_1(-\frac{1}{2}+x)+\lambda_2(-\frac{1}{3}+x^2)+\lambda_3(-\frac{1}{4}+x^3)+\lambda_4(-\frac{1}{5}+x^4)+\lambda_5(-\frac{1}{6}+x^5) = 0(\lambda_i \in \mathbb{R})$$

Then

$$(-\frac{\lambda_1}{2}-\frac{\lambda_2}{3}-\frac{\lambda_3}{4}-\frac{\lambda_4}{5}-\frac{\lambda_5}{6})+\lambda_1 x+\lambda_2 x^2+\lambda_3 x^3+\lambda_4 x^4+\lambda_5 x^5 = 0$$

and so equating up coefficients of powers of x we see that we must have $\lambda_1 = ... = \lambda_5 = 0$. This shows that the sequence

$$(-\frac{1}{2}+x,\ -\frac{1}{3}+x^2,\ -\frac{1}{4}+x^3,\ -\frac{1}{5}+x^4,\ -\frac{1}{6}+x^5)$$

is a basis of S and hence dim$S = 5$.

Return to Question R.6 on P34

Solution 1.1

a. ***Show that the sequence*** $B_1 = ((1,1,1),(0,1,1),(0,0,1))$ ***is a basis of*** $\mathbb{R}^3$ ***and find the coordinate vector of*** $(2,3,-1)$ ***with respect to the basis*** B_1.

b. ***Consider the sequence***

$$B_2 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right)$$

in $\mathbb{R}_{2\times 2}$. ***Show that*** B_2 ***is a basis of*** $\mathbb{R}_{2\times 2}$. ***Find the coordinate vector of*** $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ ***with respect to*** B_2.

c. ***Find the coordinate vector of*** $p(x) = 1 + 2x - x^2$ ***with respect to the basis***

$$(1+x, x+x^2, 1+x^2)$$

of P_2**.**

a. Suppose that

$$\lambda_1(1,1,1)+\lambda_2(0,1,1)+\lambda_3(0,0,1)=(0,0,0). \quad (\lambda_i \in \mathbb{R})$$

Then

$$(\lambda_1,\ \lambda_1+\lambda_2,\ \lambda_1+\lambda_2+\lambda_3)=(0,0,0).$$

Hence from the first components, $\lambda_1 = 0$, then from the second components we see that $\lambda_2 = 0$ and finally from the third components, $\lambda_3 = 0$. This demonstrates that the sequence $B_1 = ((1,1,1),(0,1,1),(0,0,1))$ is L.I. Hence the sequence B_1 is L.I. and has length equal to dim$(\mathbb{R}^3) = 3$ and so it follows that the sequence B_1 is a basis of $\mathbb{R}^3$.

To find the coordinate vector of $(2,3,-1)$ w.r.t. B_1, we must consider the equation

$$\alpha(1,1,1)+\beta(0,1,1)+\gamma(0,0,1)=(2,3,-1). \quad (\alpha,\beta,\gamma \in \mathbb{R})$$

For α, β and γ to satisfy this equation, we require

$$\begin{aligned} \alpha &= 2 \\ \alpha+\beta &= 3 \\ \alpha+\beta+\gamma &= -1. \end{aligned}$$

Hence we require $\alpha = 2, \beta = 1$ and $\gamma = -4$. Thus, the coordinate vector we require is $(2,1,-4)$.

b. Suppose that

$$\alpha\begin{pmatrix}1&0\\0&0\end{pmatrix}+\beta\begin{pmatrix}1&1\\0&0\end{pmatrix}+\gamma\begin{pmatrix}1&1\\1&0\end{pmatrix}+\delta\begin{pmatrix}1&1\\1&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

for $\alpha,\beta,\gamma,\delta\in\mathbb{R}$. Then

$$\begin{pmatrix}\alpha+\beta+\gamma+\delta & \beta+\gamma+\delta\\ \gamma+\delta & \delta\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

Equating up entries shows that we must have $\alpha=\beta=\gamma=\delta=0$. This demonstrates that the sequence B_2 is L.I. It follows that B_2 is an L.I. sequence in $\mathbb{R}_{2\times 2}$ with length equal to dim$(\mathbb{R}_{2\times 2})=4$ and so B_2 is a basis of $\mathbb{R}_{2\times 2}$.

To find the coordinate vector of $A=\begin{pmatrix}1&2\\3&4\end{pmatrix}$ w.r.t. B_2, we need to consider the equation

$$\lambda_1\begin{pmatrix}1&0\\0&0\end{pmatrix}+\lambda_2\begin{pmatrix}1&1\\0&0\end{pmatrix}+\lambda_3\begin{pmatrix}1&1\\1&0\end{pmatrix}+\lambda_4\begin{pmatrix}1&1\\1&1\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}.$$

for $\lambda_i\in\mathbb{R}$. i.e.

$$\begin{pmatrix}\lambda_1+\lambda_2+\lambda_3+\lambda_4 & \lambda_2+\lambda_3+\lambda_4\\ \lambda_3+\lambda_4 & \lambda_4\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}.$$

leading to the system of equations

$$\begin{aligned}\lambda_1+\lambda_2+\lambda_3+\lambda_4&=1\\ \lambda_2+\lambda_3+\lambda_4&=2\\ \lambda_3+\lambda_4&=3\\ \lambda_4&=4.\end{aligned}$$

Back substitution yields the solution $\lambda_1 = -1, \lambda_2 = -1, \lambda_3 = -1, \lambda_4 = 4$. Hence the required coordinate vector is $(-1, -1, -1, 4)$.

c. We have

$$p(x) = 1 + 2x - x^2 = \alpha(1 + x) + \beta(x + x^2) + \gamma(1 + x^2)$$

for some $\alpha, \beta, \gamma \in \mathbb{R}$.\\ That is,

$$1 + 2x - x^2 = (\alpha + \gamma) + (\alpha + \beta)x + (\beta + \gamma)x^2.$$

Equating coefficients gives

$$\begin{aligned} \alpha + \gamma &= 1 \\ \alpha + \beta &= 2 \\ \beta + \gamma &= -1 \end{aligned}$$

This leads to the augmented matrix

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

So, we have the unique solution

$$\alpha = 2, \quad \beta = 0, \quad \gamma = -1.$$

Hence

$$p(x) = 2(1 + x) + 0(x + x^2) - 1(1 + x^2),$$

and so the coordinate vector of $p(x)$ with respect to the given basis is $(2, 0, -1)$.

Return to Question 1.1 on P35

Solution 1.2

Verify that the sequence $L_2 = \left(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)$ ***is L.I. in*** $\mathbb{R}_{2\times 2}$ ***and hence use the Exchange Lemma to extend*** L_2 ***to a basis of*** $\mathbb{R}_{2\times 2}$.

Suppose that

$$\lambda_1 \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \qquad (\lambda_i \in \mathbb{R})$$

i.e.

$$\begin{pmatrix} \lambda_2 & \lambda_1 + \lambda_2 \\ 0 & \lambda_1 + \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Equating up entries gives $\lambda_1 = \lambda_2 = 0$. This demonstrates that the sequence L_2 is L.I.

To apply the Exchange Lemma, we require a L.I. sequence and a spanning sequence. In this example, we take the L.I. sequence L_2 and the we use the standard basis as our spanning sequence. This is the sequence

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

Remember the Exchange Lemma says we want to chuck away some of our spanning matrices and let the L.I. ones take their places. We start with the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ from L_2. We write this as a linear combination of the matrices in the standard basis. Hence

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

The coefficient of the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nonzero and hence the sequence

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

spans $\mathbb{R}_{2\times 2}$.

Now

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

Hence the sequence

$$\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

spans $\mathbb{R}_{2\times 2}$. Note that the length of this sequence is $4 = \dim(\mathbb{R}_{2\times 2})$ and so we have a spanning sequence with length equal to the dimension of the space. It follows that

$$\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

is a basis of $\mathbb{R}_{2\times 2}$.

Return to Question 1.2 on P35

Solution 1.3

Consider the subspaces

$$U = \{(x,y,z) \in \mathbb{R}^3 \mid x+y+z=0\},$$
$$W = \{(x,y,z) \in \mathbb{R}^3 \mid x+2y-3z=0\}.$$

of $\mathbb{R}^3$***.***

a. Find a basis of $U \cap W$***.***

b. Find $\dim U$ ***and*** $\dim W$ ***and hence state the value of*** $\dim(U+W)$***. Deduce that*** $U+W=\mathbb{R}^3$***.***

a.

$$\begin{aligned}\mathbf{x}=(x,y,z)\in U\cap W &\Leftrightarrow \mathbf{x}\in U \text{ and } \mathbf{x}\in W\\ &\Leftrightarrow x+y+z=0 \text{ and } x+2y-3z=0.\end{aligned}$$

This system has augmented matrix

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

So $x=-5t$, $y=4t$ for some $t\in\mathbb{R}$. Hence $\mathbf{x}=(-5t,4t,t)=t(-5,4,1)$ for some $t\in\mathbb{R}$.

It follows that $U\cap W$ is 1-dimensional and a basis is $((-5,4,1))$.

b. Let $\mathbf{x}=(x,y,z)\in U$. Then $x+y+z=0 \Rightarrow z=-x-y$. Hence

$$\mathbf{x}=(x,y,-x-y)=x(1,0,-1)+y(0,1,-1).$$

So the sequence $L_1=((1,0,-1),(0,1,-1))$ spans U. Additionally,

$$\alpha(1,0,-1)+\beta(0,1,-1)=(0,0,0) \qquad (\alpha,\beta\in\mathbb{R})$$

implies that $(\alpha,\beta,-\alpha-\beta)=(0,0,0)$ and hence $\alpha=\beta=0$. It follows that L_1 is L.I. and so is a basis of U and dim$U=2$.

Similarly, if $\mathbf{y}=(a,b,c)\in W$ then $a+2b-3c=0\Rightarrow a=3c-2b$. Hence

$$\mathbf{y}=(3c-2b,b,c)=b(-2,1,0)+c(3,0,1).$$

Hence the sequence $L_2 = ((-2,1,0),(3,0,1))$ spans W.

Now

$$\alpha(-2,1,0)+\beta(3,0,1)=(0,0,0) \qquad (\alpha,\beta\in\mathbb{R})$$

implies that $(3\beta-2\alpha,\alpha,\beta)=(0,0,0)$ and hence $\alpha=\beta=0$. This shows that L_2 is L.I. and it follows that L_2 is a basis of W. Hence dim$W=2$.

Now

$$\dim(U+W)=\dim U+\dim W-\dim(U\cap W)=2+2-1=3.$$

$U+W\subseteq\mathbb{R}^3$ and hence we must have $U+W=\mathbb{R}^3$ by Lemma 1.19.

Return to Question 1.3 on P36

Solution 1.4

Let** S, T_1 **and** T_2 **be subspaces of** $\mathbb{R}^7$ **such that

$$\mathbb{R}^7=S+T_1=S+T_2.$$

with $\dim\, S=3$.

- ***a. Use the theorem on dimension of sums of subspaces to show that*** $\dim\, T_i\geq 4$ ***(***$i=1,2$***)***
- ***b. Deduce that*** $T_1\cap T_2\neq\{\mathbf{0}\}$.

a. We have

$$\dim(S+T_1)=\dim(S+T_2)=\dim(\mathbb{R}^7)$$

i.e.

$$\dim S+\dim T_1-\dim(S\cap T_1)=7$$

and

$$\dim S+\dim T_2-\dim(S\cap T_2)=7.$$

Hence

$$\dim T_1 = 7 - \dim S + \dim(S \cap T_1) = 4 + \dim(S \cap T_1) \geq 4$$

and similarly

$$\dim T_2 = 7 - \dim S + \dim(S \cap T_2) = 4 + \dim(S \cap T_2) \geq 4.$$

b. Now $T_1 + T_2 \subseteq \mathbb{R}^7$ and so dim$(T_1 + T_2) \leq 7$. Hence

$$\dim(T_1 \cap T_2) = \dim T_1 + \dim T_2 - \dim(T_1 + T_2) \geq 4 + 4 - 7 = 1$$

and so $T_1 \cap T_2 \neq \{\mathbf{0}\}$.

Return to Question 1.4 on P36

Solution 1.5

Find a basis of the subspace $N(A) = \{X \in \mathbb{R}_{4\times 1} \mid AX = \mathbf{0}\}$ ***where***

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

Let $X = \mathrm{col}(x_1, x_2, x_3, x_4)$. Then

$$X \in N(A) \Leftrightarrow AX = 0$$

$$\Leftrightarrow \begin{pmatrix} 1 & 1 & -1 & 1 \\ 2 & -1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The augmented matrix here is

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

Hence the solution set is

$$N(A) = \left\{ \begin{pmatrix} \frac{1}{3}s - t \\ \frac{2}{3}s \\ s \\ t \end{pmatrix} : s, t \in \mathbb{R} \right\}.$$

Take an arbitrary column

$$\begin{pmatrix} \frac{1}{3}s - t \\ \frac{2}{3}s \\ s \\ t \end{pmatrix} \in N(A).$$

Then

$$\begin{pmatrix} \frac{1}{3}s - t \\ \frac{2}{3}s \\ s \\ t \end{pmatrix} = \frac{s}{3} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix} + t \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Hence the sequence

$$L = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

spans $N(A)$.

Now suppose that

$$\lambda_1 \begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \quad (\lambda_1, \lambda_2 \in \mathbb{R}).$$

Then

$$\begin{pmatrix} \lambda_1 - \lambda_2 \\ 2\lambda_1 \\ 3\lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

and hence $\lambda_1 = \lambda_2 = 0$ on equating up the entries in rows 3 and 4 (say).

Hence the sequence L is L.I. so is a basis of $N(A)$.

Return to Question 1.5 on P37

Solution 1.6

Find the rank of the matrix

$$A = \begin{pmatrix} 1 & 2 & -4 \\ 2 & -1 & 2 \\ 1 & 1 & -2 \end{pmatrix}.$$

Find also the dimension of the subspace $N(A) = \{X \in \mathbb{R}_{3\times 1} \mid AX = \mathbf{0}\}$***.***

We have

$$\begin{pmatrix} 1 & 2 & -4 \\ 2 & -1 & 2 \\ 1 & 1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence the rank of A is 2 (the number of nonzero rows in RRE form).

Now let $X = \text{col}(x, y, z)$. Then

$$\begin{aligned} X \in N(A) &\Leftrightarrow AX = 0 \\ &\Leftrightarrow \begin{pmatrix} 1 & 2 & -4 \\ 2 & -1 & 2 \\ 1 & 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \end{aligned}$$

The augmented matrix here is

$$\left(\begin{array}{ccc|c} 1 & 2 & -4 & 0 \\ 2 & -1 & 2 & 0 \\ 1 & 1 & -2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

and it follows that

$$N(A) = \left\{ \begin{pmatrix} 0 \\ 2t \\ t \end{pmatrix} \mid t \in \mathbb{R} \right\}.$$

So, if

$$\begin{pmatrix} 0 \\ 2t \\ t \end{pmatrix} \in N(A)$$

then

$$\begin{pmatrix} 0 \\ 2t \\ t \end{pmatrix} = t \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

and so a basis of $N(A)$ is

$$\left(\begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} \right)$$

(The spanning property is clearly seen and recall that a sequence with just one vector is always linearly independent.) Hence dim$(N(A)) = 1$.

Return to Question 1.6 on P37

A.2 Chapter 2 solutions

Solution 2.1

Let $S : V \longrightarrow W$ and $T : U \longrightarrow V$ be mappings.

- ***a. Prove that if $S \circ T$ is injective then T is also injective.***
- ***b. Prove that if $S \circ T$ is surjective then S is also surjective.***

a. Let $x, y \in U$. Then

$$\begin{aligned} T(x) = T(y) &\Rightarrow S(T(x)) = S(T(y)) \\ &\Rightarrow (S \circ T)(x) = (S \circ T)(y) \\ &\Rightarrow x = y \end{aligned}$$

since $S \circ T$ is injective. Hence T is injective.

b. Let $y \in W$. Then, since $S \circ T$ is surjective, $y = (S \circ T)(x)$ for some $x \in U$ i.e. $y = S(T(x)) \in \mathrm{im}(S)$. Hence S is surjective.

Return to Question 2.1 on P71

Solution 2.2

For each of the following mappings $T : U \longrightarrow V$, decide whether T is linear.

- ***a.*** $U = \mathbb{R}^4$, $V = \mathbb{R}^3$, $T((x_1, x_2, x_3, x_4)) = (x_2 + x_3,\ x_1 - x_2^2,\ x_3 + x_4)$,
- ***b.*** $U = \mathbb{R}^3$, $V = \mathbb{R}^2$, $T((x_1, x_2, x_3)) = (x_2 - x_1,\ x_3 + 3x_2)$,
- ***c.*** $U = P_2$, $V = P_5$, $T(p(x)) = xp(x^2) + p(1)$,

d. $U = \mathbb{R}^2$***,*** $V = \mathbb{R}$***,*** $T((x, y)) = xy$***.***

a. This is not linear. For example, take $\mathbf{x} = (0, 1, 0, 0) \in U$ and $\lambda = 2$. Then

$$T(\lambda\mathbf{x}) = T((0, 2, 0, 0)) = (2, -4, 0).$$

However,

$$\lambda T(\mathbf{x}) = 2T((0, 1, 0, 0)) = 2(1, -1, 0) = (2, -2, 0).$$

Hence we have $T(\lambda\mathbf{x}) \neq \lambda T(\mathbf{x})$ and so T is not linear.

b. This is linear. Let $\mathbf{x} = (x_1, x_2, x_3), \mathbf{y} = (y_1, y_2, y_3) \in U$ and $\lambda \in \mathbb{R}$. Then

$$\begin{aligned}
T(\mathbf{x} + \mathbf{y}) &= T((x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3)) \\
&= (x_2 + y_2 - (x_1 + y_1),\ x_3 + y_3 + 3(x_2 + y_2)) \\
&= (x_2 - x_1 + y_2 - y_1,\ x_3 + 3x_2 + y_3 + 3y_2) \\
&= (x_1 - x_1,\ x_3 + 3x_2) + (y_2 - y_1,\ y_3 + 3y_2) \\
&= T(\mathbf{x}) + T(\mathbf{y})
\end{aligned}$$

and

$$\begin{aligned}
T(\lambda\mathbf{x}) &= T(\lambda(x_1, x_2, x_3)) \\
&= T(\lambda x_1, \lambda x_2, \lambda x_3) \\
&= (\lambda x_2 - \lambda x_1,\ \lambda x_3 + 3(\lambda x_2)) \\
&= \lambda(x_2 - x_1,\ x_3 + 3x_2) \\
&= \lambda T(\mathbf{x}).
\end{aligned}$$

c. This is linear. Let $p, q \in P_2$ and $\lambda \in \mathbb{R}$. Then

$$\begin{aligned} T((p+q)(x)) &= x(p+q)(x^2) + (p+q)(1) \\ &= xp(x^2) + xq(x^2) + p(1) + q(1) \\ &= (xp(x^2) + p(1)) + (xq(x^2) + q(1)) \\ &= T(p(x)) + T(q(x)) \end{aligned}$$

and

$$\begin{aligned} T((\lambda p)(x)) &= x(\lambda p)(x^2) + (\lambda p)(1) \\ &= \lambda(xp(x^2)) + \lambda(p(1)) \\ &= \lambda(xp(x^2) + p(1)) \\ &= \lambda T(p(x)). \end{aligned}$$

d. This is not linear. For example, consider $\mathbf{x} = (1,1) \in U$ and $\lambda = 2$. Then

$$T(\lambda x) = T(2(1,1)) = T((2,2)) = 2 \times 2 = 4.$$

However

$$\lambda T(\mathbf{x}) = 2T((1,1)) = 2(1 \times 1) = 2.$$

Hence $T(\lambda \mathbf{x}) \neq \lambda T(\mathbf{x})$ and so T is not linear.

Return to Question 2.2 on P72

Solution 2.3

A linear mapping $S : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ ***is such that***

$$\begin{aligned} S((1,0,0)) &= (2,-1,0,4), \\ S((0,1,0)) &= (1,3,-4,7), \text{ and} \\ S((0,0,1)) &= (0,0,5,2) \end{aligned}$$

Find a general formula for $S((x_1, x_2, x_3))$.

Since S is a linear mapping, $S(\lambda \mathbf{x}) = \lambda S(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^3$, $\lambda \in \mathbb{R}$. Hence

$$\begin{aligned} S((x_1,0,0)) &= x_1 S((1,0,0)) = (2x_1, -x_1, 0, 4x_1) \\ S((0,x_2,0)) &= x_2 S((0,1,0)) = (x_2, 3x_2, -4x_2, 7x_2) \\ S((0,0,x_3)) &= x_3 S((0,0,1)) = (0,0,5x_3,2x_3). \end{aligned}$$

Now, once again since S is linear,

$$\begin{aligned} S((x_1,x_2,x_3)) &= S((x_1,0,0)+(0,x_2,0)+(0,0,x_3)) \\ &= S((x_1,0,0)) + S((0,x_2,0)) + S((0,0,x_3)) \\ &= (2x_1,-x_1,0,4x_1) + (x_2,3x_2,-4x_2,7x_2) + (0,0,5x_3,2x_3) \\ &= (2x_1+x_2, -x_1+3x_2, -4x_2+5x_3, 4x_1+7x_2+2x_3). \end{aligned}$$

Return to Question 2.3 on P72

Solution 2.4

A linear mapping $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ ***is such that***

$$\begin{aligned} T((1,1,1)) &= (1,-1,1) \\ T((1,1,0)) &= (-2,1,-1), \text{ and} \\ T((1,0,0)) &= (3,1,0). \end{aligned}$$

Obtain a general formula for $T((x_1, x_2, x_3))$.

We have

$$\begin{aligned} T((0,1,0)) &= T((1,1,0) - (1,0,0)) \\ &= T((1,1,0)) - T((1,0,0)) \quad (T \text{ linear}) \\ &= (-2,1,-1) - (3,1,0) \\ &= (-5,0,-1). \end{aligned}$$

In addition,

$$\begin{aligned} T((0,0,1)) &= T((1,1,1) - (1,1,0)) \\ &= T((1,1,1)) - T((1,1,0)) \quad (T \text{ linear}) \\ &= (1,-1,1) - (-2,1,-1) \\ &= (3,-2,2). \end{aligned}$$

Hence

$$\begin{aligned} T((x_1,0,0)) &= x_1 T((1,0,0)) \quad (T \text{ linear}) \\ &= (3x_1, x_1, 0). \end{aligned}$$

$$\begin{aligned} T((0,x_2,0)) &= x_2 T((0,1,0)) \quad (T \text{ linear}) \\ &= (-5x_2, 0, -x_2). \end{aligned}$$

$$\begin{aligned} T((0,0,x_3)) &= x_3 T((0,0,1)) \quad (T \text{ linear}) \\ &= (3x_3, -2x_3, 2x_3). \end{aligned}$$

Finally,

$$\begin{aligned} T((x_1,x_2,x_3)) &= T((x_1,0,0)+(0,x_2,0)+(0,0,x_3)) \\ &= T((x_1,0,0))+T((0,x_2,0))+T((0,0,x_3)) \quad (T \text{ linear}) \\ &= (3x_1,x_1,0)+(-5x_2,0,-x_2)+(3x_3,-2x_3,2x_3) \\ &= (3x_1-5x_2+3x_3,x_1-2x_3,-x_2+2x_3). \end{aligned}$$

Return to Question 2.4 on P72

Solution 2.5

Let $T : V \longrightarrow W$ be a linear mapping. Prove that if the sequence $(\mathbf{v}_1, ..., \mathbf{v}_k)$ is linearly dependent in V then $(T(\mathbf{v}_1), ..., T(\mathbf{v}_k))$ is linearly dependent in W.

Since the sequence $(\mathbf{v}_1, ..., \mathbf{v}_k)$ is linearly dependent there exists scalars $\lambda_1, ..., \lambda_k \in F$ not all zero such that

$$\lambda_1\mathbf{v}_1 + ... + \lambda_k\mathbf{v}_k = \mathbf{0}_V.$$

Hence

$$T(\lambda_1\mathbf{v}_1 + ... + \lambda_k\mathbf{v}_k) = T(\mathbf{0}_V).$$

Since T is linear, this implies that

$$\lambda_1 T(\mathbf{v}_1) + ... + \lambda_k T(\mathbf{v}_k) = \mathbf{0}_W.$$

Hence we see that a non-trivial linear combination of the vectors $T(\mathbf{v}_1), ..., T(\mathbf{v}_k)$ is equal to the zero vector and so the sequence $(T(\mathbf{v}_1), ..., T(\mathbf{v}_k))$ is linearly dependent.

Return to Question 2.5 on P73

Solution 2.6

Let $T : V \longrightarrow W$ be a linear mapping. Show that if the sequence $(\mathbf{v}_1, ..., \mathbf{v}_k)$ is linearly independent in V and ker(T) is trivial then the sequence $(T(\mathbf{v}_1), ..., T(\mathbf{v}_k))$ is linearly independent in W.

Suppose that

$$\lambda_1 T(\mathbf{v}_1) + ... + \lambda_k T(\mathbf{v}_k) = \mathbf{0}_W \qquad (\lambda_i \in \mathcal{F})$$

Then, since T is linear,

$$T(\lambda_1 \mathbf{v}_1 + ... + \lambda_k \mathbf{v}_k) = \mathbf{0}_W.$$

Hence $\lambda_1 \mathbf{v}_1 + ... + \lambda_k \mathbf{v}_k \in \ker(T) = \{\mathbf{0}_V\}$.

Thus,

$$\lambda_1 \mathbf{v}_1 + ... + \lambda_k \mathbf{v}_k = \mathbf{0}_V.$$

Now since the sequence $(\mathbf{v}_1, ..., \mathbf{v}_k)$ is linearly independent we have $\lambda_1 = ... = \lambda_k = 0$.

Hence the sequence $(T(\mathbf{v}_1), ..., T(\mathbf{v}_k))$ is linearly independent.

Return to Question 2.6 on P73

Solution 2.7

Find bases of the image and kernel of the linear mapping $S : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ defined by

$$S((x, y, z)) = (x + 2y + z,\ x + 2y + z,\ 2x + 4y + 2z).$$

im (S) is the set of all vectors of the form

$$(x + 2y + z,\ x + 2y + z,\ 2x + 4y + 2z) = x(1, 1, 2) + y(2, 2, 4) + z(1, 1, 2)$$

so im $(S) =$ $\operatorname{span}((1,1,2),\ (2,2,4),\ (1,1,2))$. Now

$$\begin{pmatrix} 1 & 1 & 2 \\ 2 & 2 & 4 \\ 1 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence a basis of im (S) is $((1,1,2))$ and $\operatorname{rank}(S) = 1$. It follows from the Rank-Nullity Theorem that $\operatorname{nullity}(S) = \dim(\mathbb{R}^3) - \operatorname{rank}(S) = 3 - 1 = 2.$.

Now let $(x,y,z) \in \mathbb{R}^3$. Then

$$\begin{aligned} (x,y,z) \in \ker(S) &\Leftrightarrow T((x,y,z)) = (0,0,0) \\ &\Leftrightarrow x + 2y + z = 0, \quad x + 2y + z = 0, \quad 2x + 4y + 2z = 0. \end{aligned}$$

We have the augmented matrix

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 1 & 2 & 1 & 0 \\ 2 & 4 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence ker $(S) = \{(-2s - t, s, t) : s, t \in \mathbb{R}\}$. Let $(-2s - t, s, t) \in$ ker (S). Then

$$(-2s - t, s, t) = s(-2,1,0) + t(-1,0,1).$$

Hence a basis of ker (S) is $((-2,1,0),\ (-1,0,1))$ by the 2 of 3 properties proposition.

Return to Question 2.7 on P73

Solution 2.8

Define $T : \mathbb{R}_{n\times n} \longrightarrow \mathbb{R}_{n\times n}$ ***by*** $T(A) = A^T$ ***for all*** $A \in \mathbb{R}_{n\times n}$.

Show that T ***is a linear mapping and find explicitly the kernel and image of*** T***. State also the rank and nullity of*** T***.***

Let $A, B \in \mathbb{R}_{n\times n}$ and $\lambda \in \mathbb{R}$. Then

$$T(A+B) = (A+B)^T = A^T + B^T = T(A) + T(B)$$

and

$$T(\lambda A) = (\lambda A)^T = \lambda A^T = \lambda T(A).$$

Hence T is linear. Now T is surjective since for all $A \in \mathbb{R}_{n\times n}$,

$$A = (A^T)^T = T(A^T)$$

and hence im $(T) = \mathbb{R}_{n\times n}$ and $\mathrm{rank}\,(T) = \dim\,(\mathbb{R}_{n\times n}) = n^2$.

Also,

$$\begin{aligned} A \in \text{ker}\,(T) &\Leftrightarrow T(A) = 0 \\ &\Leftrightarrow A^T = 0 \\ &\Leftrightarrow A = 0. \end{aligned}$$

Hence ker $(T) = \{\mathbf{0}\}$ and $\mathrm{nullity}\,(T) = 0.\}$

Return to Question 2.8 on P73

Solution 2.9

Show that the mapping $T : P_2 \longrightarrow P_3$ defined by $T(p(x)) = xp(x)$ for all $p \in P_2$ is linear. Find the rank and nullity of T.

Let $p, q \in P_2$ and $\lambda \in \mathbb{R}$. Then

$$T((p+q)(x)) = x(p+q)(x) = x(p(x)+q(x)) = xp(x)+xq(x) = T(p(x))+T(q(x))$$

and

$$T((\lambda p)(x)) = x(\lambda p)(x) = x\lambda p(x) = \lambda(xp(x)) = \lambda T(p(x))$$

Hence T is linear.

$\text{im}\,(T) = \{ax + bx^2 + cx^3 : a, b, c \in \mathbb{R}\}$. Hence a basis for $\text{im}\,(T)$ is (x, x^2, x^3) and so $\mathrm{rank}\,(T) = 3$. Now

$$\begin{aligned} p(x) = a + bx + cx^2 \in \ker(T) &\Leftrightarrow T(p(x)) = 0 \\ &\Leftrightarrow ax + bx^2 + cx^3 = 0 \\ &\Leftrightarrow a = b = c = 0 \\ &\Leftrightarrow p(x) = 0 \end{aligned}$$

Hence $\ker(T) = \{\mathbf{0}\}$ and $\mathrm{nullity}\,(T) = 0.\}$

Return to Question 2.9 on P74

Solution 2.10

Let W denote the vector space of all symmetric 2×2 real matrices. Find the nullity of the linear mapping $T : W \longrightarrow P_2$ defined by

$$T\left(\begin{pmatrix} a & b \\ b & c \end{pmatrix}\right) = (a-b) + (b-c)x + (c-a)x^2$$

and use this to deduce the value of rank(T) from the Rank-Nullity Theorem. Use this information to find a basis of im(T).

We have

$$\begin{aligned} A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \ker(T) &\Leftrightarrow T(A) = 0 \\ &\Leftrightarrow (a-b) + (b-c)x + (c-a)x^2 = 0 \\ &\Leftrightarrow a-b = 0,\ b-c = 0,\ c-a = 0 \\ &\Leftrightarrow a = b = c. \end{aligned}$$

Hence ker$\,(T) = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \right\}$ and so a basis for ker$\,(T)$ is $\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right)$ and $\text{nullity}\,(T) = 1.$

It follows from the Rank-Nullity Theorem that $\text{rank}\,(T) = \dim W - \text{nullity}\,(T) = 3 - 1 = 2.$

Now im$\,(T) = \{a(1-x^2) + b(-1+x) + c(-x+x^2) : a, b, c \in \mathbb{R}\}$. Hence

$$\text{im}\,(T) = \text{span}\,(1-x^2,\ -1+x,\ -x+x^2).$$

The sequence $(1-x^2,\ -1+x,\ -x+x^2)$ has length 3 and hence must be linearly dependent as rank$(T) = 2$. It follows from the Minus Theorem that we should be able to throw away one of the vectors in this sequence and retain a spanning sequence for im$\,(T)$. We have

$$-x + x^2 = -(1-x^2) - (-1+x)$$

Hence the sequence $(1-x^2,\ -1+x)$ still spans im$\,(T)$ by the Minus Theorem and has length equal to $\operatorname{rank}(T)$ so by the 'two of three' properties proposition, $(1 - x^2,\ -1 + x)$ is a basis of im (T).

Return to Question 2.10 on P74

Solution 2.11

Let V and W be vector spaces of dimensions 3 and 4 respectively and let $L_V = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ and $L_W = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4)$ be bases of V and W respectively. Given that

$$M(T; L_V, L_W) = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{pmatrix}$$

a. Write down $T(\mathbf{e}_2)$ as a linear combination of $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$.

b. By evaluating one matrix product, obtain $T(2\mathbf{e}_1 + \mathbf{e}_2 - \mathbf{e}_3)$ as a linear combination of $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$.

a. We have

$$T(\mathbf{e}_2) = 2\mathbf{f}_1 + 5\mathbf{f}_2 + 8\mathbf{f}_3 + 11\mathbf{f}_4.$$

b. We evaluate

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 7 \\ 13 \\ 19 \end{pmatrix}.$$

Hence $T((2, 1, -1)) = \mathbf{f}_1 + 7\mathbf{f}_2 + 13\mathbf{f}_3 + 19\mathbf{f}_4$.

Return to Question 2.11 on P74

Solution 2.12

Let** $D : P_3 \longrightarrow P_2$ **be the linear mapping defined by** $D(p(x)) = p^{'}(x)$ **for all** $p \in P_3$**. Let** $B = (1, x, x^2, x^3)$ **and** $C = (1, x, x^2)$ **be the standard bases for** P_3 **and** P_2 **respectively. Find the matrix of** D **with respect to** B **and** C**.

We have

$$\begin{aligned} D(1) &= 0 \\ D(x) &= 1 \\ D(x^2) &= 2x \\ D(x^3) &= 3x^2. \end{aligned}$$

Hence the matrix of D w.r.t. the bases B and C is

$$M_D = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Return to Question 2.12 on P75

Solution 2.13

Let** $S : V \longrightarrow W$ **and** $T : U \longrightarrow V$ **be linear mappings and let** L_U, L_V, L_W **be bases of** U, V **and** W **respectively. Show that** $M(ST; L_U, L_W) = M(S; L_V, L_W)M(T; L_U, L_V)$**.

(Here, as usual,** ST **means the composition** $S \circ T$**.)

Let $\mathbf{x}$ be an arbitrary vector in U. Let the coordinate column vectors of $\mathbf{x}$, $T(\mathbf{x})$ and $(ST)(\mathbf{x})$ (with respect to L_U, L_V and L_W respectively) be X, Y and Z. Then $Y = M_T X$ and $Z = M_S Y$. Hence $Z = (M_S M_T)X$. Since $\mathbf{x} \in U$ was arbitrary, it follows that $M_{ST} = M_S M_T$ as required.

Return to Question 2.13 on P75

Solution 2.14

Consider the bases

$$B_1 = ((1,0,0),(0,1,0),(0,0,1))$$

and

$$B_2 = ((1,1,0),(0,1,1),(1,0,1))$$

of $\mathbb{R}^3$***.***

a. ***Find the change of basis matrices*** $M(B_1 \to B_2)$ ***and*** $M(B_2 \to B_1)$***.***

b. ***Use your answer to express*** $\mathbf{x} = (1,2,3)$ ***as a linear combination of the vectors in*** B_2***.***

a. To find the change of basis matrix $M(B_1 \to B_2)$ we must express each of the basis vectors in B_2 as linear combinations of the basis vectors in B_1. We have

$$\begin{aligned}(1,1,0) &= 1(1.0,0) + 1(0,1,0)\\(0,1,1) &= 1(0,1,0) + 1(0,0,1)\\(1,0,1) &= 1(1,0,0) + 1(0,0,1)\end{aligned}$$

Hence

$$M(B_1 \to B_2) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Now via EROs on the augmented system $(P \mid I)$ where $P = M(B_1 \longrightarrow B_2)$, we see that

$$P^{-1} = M(B_2 \to B_1) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

b. Finally, to express $(1,2,3)$ in terms of the basis B_2, we calculate the product

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

and so

$$(1,2,3) = 2(0,1,1) + 1(1,0,1).$$

Return to Question 2.14 on P75

Solution 2.15

Consider the standard basis B_1 of $\mathbb{R}^3$ and the basis $B_2 = (\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3)$ where

$$\mathbf{w}_1 = (2,1,1), \quad \mathbf{w}_2 = (0,1,3), \quad \mathbf{w}_3 = (0,0,2).$$

a. Find the change of basis matrices $M(B_1 \to B_2)$ and $M(B_2 \to B_1)$.

b. Use an appropriate change of basis matrix to find the coordinate vector of $(x,y,z) \in \mathbb{R}^3$ w.r.t. the basis B_2. Verify your answer.

a. The change of basis matrix from B_1 to B_2 is

$$M(B_1 \to B_2) = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 3 & 2 \end{pmatrix}.$$

Now let $\mathbf{e}_1 = (1,0,0)$, $\mathbf{e}_2 = (0,1,0)$ and $\mathbf{e}_3 = (0,0,1)$ so that $B_1 =$

$(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$. Then

$$\begin{aligned}
(0,0,1) &= \frac{1}{2}\mathbf{w}_3 \\
(0,1,0) &= \mathbf{w}_2 - \frac{3}{2}\mathbf{w}_3 \\
(1,0,0) &= \frac{1}{2}(\mathbf{w}_1 - \mathbf{e}_2 - \mathbf{e}_3) = \frac{1}{2}\mathbf{w}_1 - \frac{1}{2}\mathbf{w}_2 + \frac{1}{2}\mathbf{w}_3.
\end{aligned}$$

Hence

$$M(B_2 \to B_1) = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & 1 & 0 \\ \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix}.$$

Obviously we could have used the fact that if $P = M(B_1 \to B_2)$ then $M(B_2 \to B_1) = P^{-1}$ as we did in Q1 and calculated P^{-1} by applying EROs to the augmented matrix $(P \mid I)$.

b. Now to find the coordinate column vector of $\mathbf{x} = (x, y, z)$ w.r.t. B_2 we just need to calculate the product

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & 1 & 0 \\ \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{2}x \\ -\frac{1}{2}x + y \\ \frac{1}{2}x - \frac{3}{2}y + \frac{1}{2}z \end{pmatrix}.$$

To verify,

$$\begin{aligned}
&\frac{1}{2}x(2,1,1) + (-\frac{1}{2}x + y)(0,1,3) + (\frac{1}{2}x - \frac{3}{2}y + \frac{1}{2}z)(0,0,2) \\
&= (x,\ \frac{1}{2}x + (-\frac{1}{2}x + y),\ \frac{1}{2}x + (-\frac{3}{2}x + 3y) + (x - 3y + z)) \\
&= (x, y, z).
\end{aligned}$$

Return to Question 2.15 on P76

Solution 2.16

(A number crunch workout) Consider the bases

$$B_1 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

and

$$B_2 = \left(\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

of $\mathbb{R}_{2\times 2}$***.***

a. ***Find the change of basis matrix*** $M(B_2 \to B_1)$***.***

b. ***Use part a. to express the matrix*** $A = \begin{pmatrix} 4 & 2 \\ 0 & -1 \end{pmatrix}$ ***as a linear combination of the matrices in*** B_2***.***

a. We must first of all express each basis matrix in B_1 as a linear combination of the basis matrices in B_2. For example, to express $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ in terms of the matrices in B_2 we need

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \alpha \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} + \beta \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} + \gamma \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \delta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

leading to the system of equations

$$\begin{aligned} \alpha + 2\beta + \gamma + \delta &= 1 \\ 2\alpha + \beta + \gamma &= 0 \\ \beta &= 0 \\ -\alpha + \gamma + \delta &= 0. \end{aligned}$$

This has the unique solution $\alpha = \frac{1}{2}$, $\beta = 0$, $\gamma = -1$, $\delta = \frac{3}{2}$. Once we have expressed the other matrices in B_1 as lin combs of the matrices in B_2, we see that the change of basis matrix is then

$$M(B_2 \to B_1) = \begin{pmatrix} \frac{1}{2} & 0 & -1 & -\frac{1}{2} \\ 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & 1 \\ \frac{3}{2} & -1 & -2 & -\frac{1}{2} \end{pmatrix}.$$

b. Now the coordinate vector of $A = \begin{pmatrix} 4 & 2 \\ 0 & -1 \end{pmatrix}$ w.r.t. B_1 is $(4, 2, 0, -1)$ and hence we can find the coordinate vector of A w.r.t. B_2 by finding the matrix product

$$\begin{pmatrix} \frac{1}{2} & 0 & -1 & -\frac{1}{2} \\ 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & 1 \\ \frac{3}{2} & -1 & -2 & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 4 \\ 2 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} \frac{5}{2} \\ 0 \\ -3 \\ \frac{9}{2} \end{pmatrix}.$$

Hence

$$\begin{pmatrix} 4 & 2 \\ 0 & -1 \end{pmatrix} = \frac{5}{2} \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} - 3 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \frac{9}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Return to Question 2.16 on P76

Solution 2.17

Find the two eigenvalues of the linear mapping $T : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ ***defined by***

$$T((x, y)) = (-x + 3y,\, 3x - y)$$

for all $(x, y) \in \mathbb{C}^2$***. Find a basis of each corresponding eigenspace.***

We calculate the matrix M_T of T w.r.t the standard basis $((1,0),(0,1))$ of $\mathbb{C}^2$. Hence

$$M_T = \begin{pmatrix} -1 & 3 \\ 3 & -1 \end{pmatrix}.$$

Now we calculate the eigenvalues of M_T. We have

$$\begin{aligned} \det(\lambda I - M_T) &= \begin{vmatrix} \lambda+1 & -3 \\ -3 & \lambda+1 \end{vmatrix} \\ &= (\lambda+1)^2 - 9 \\ &= \lambda^2 + 2\lambda - 8 \\ &= (\lambda+4)(\lambda-2) \end{aligned}$$

Hence the eigenvalues of T are the roots of this polynomial. Hence we have the two eigenvalues $\lambda_1 = -4$ and $\lambda_2 = 2$.

We now find corresponding eigenvectors of M_T:

$\lambda_1 = -4$: We have the homogeneous system $(-4I - M_T)X = 0$ where $X = \mathrm{col}(x,y)$ with augmented matrix

$$\left(\begin{array}{cc|c} -3 & -3 & 0 \\ -3 & -3 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right).$$

Hence we require $x+y=0 \Rightarrow y=-x$. So the eigenspace $E(-4,T)$ consist of all vectors of the form $(t,-t) = t(1,-1)$. Hence $E(-4,T)$ is one-dimensional and a basis is $((1,-1))$.

$\lambda_2 = 2$: We have the homogeneous system $(2I - M_T)X = 0$ where $X = \mathrm{col}(x,y)$

with augmented matrix

$$\left(\begin{array}{cc|c} 3 & -3 & 0 \\ -3 & 3 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & -1 & 0 \\ 0 & 0 & 0 \end{array}\right).$$

Hence we require $x - y = 0 \Rightarrow x = y$. So the eigenspace $E(2, T)$ consists of all vectors of the form $(t, t) = t(1, 1)$. Hence $E(2, T)$ is one-dimensional and a basis is $((1, 1))$.

Return to Question 2.17 on P77

Solution 2.18

Consider the linear mapping $T : P_2 \longrightarrow P_2$ ***defined by***

$$T(p(x)) = p(3x + 2)$$

for all $p \in P_2$.

a. Find the eigenvalues of T ***and hence find bases of each corresponding eigenspace.***

b. State a basis of P_2 ***with respect to which the matrix of*** T ***is a diagonal matrix. Verify this directly.***

a. We find the matrix of T w.r.t. the standard basis $(1, x, x^2)$ of P_2. We have

$$\begin{aligned} T(1) &= 1 \\ T(x) &= 2 + 3x \\ T(x^2) &= (3x + 2)^2 = 4 + 12x + 9x^2. \end{aligned}$$

Hence

$$M_T = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 12 \\ 0 & 0 & 9 \end{pmatrix}$$

and so M_T is upper triangular. It follows that the eigenvalues are $\lambda_1 = 1$,

$\lambda_2 = 3$ and $\lambda_3 = 9$. (NO CALCULATION REQUIRED!)

Now we consider the homogenous system $(\lambda I - M_T)X = 0$ where $X =$ col(x, y, z).

$\lambda_1 = 1$**:** The augmented matrix of the homogeneous system here is

$$\left(\begin{array}{ccc|c} 0 & -2 & -4 & 0 \\ 0 & -2 & -12 & 0 \\ 0 & 0 & -8 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right).$$

Hence the eigenvectors of M_T corresponding to $\lambda_1 = 1$ all have the form $\mathrm{col}(t, 0, 0) = t \times \mathrm{col}(1, 0, 0)$ for nonzero t and hence the **coordinate vector** of the basis vector of the eigenspace $E(1, T)$ is $(1, 0, 0)$. On transferring back to T, the eigenspace $E(1, T)$ is 1-dimensional with basis (1).

$\lambda_2 = 3$**:** The augmented matrix of the homogeneous system here is

$$\left(\begin{array}{ccc|c} 2 & -2 & -4 & 0 \\ 0 & 0 & -12 & 0 \\ 0 & 0 & -6 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence the eigenvectors of M_T corresponding to $\lambda_2 = 3$ all have the form $\mathrm{col}(t, t, 0) = t \times \mathrm{col}(1, 1, 0)$ for nonzero t and so the **coordinate vector** of the basis vector of the eigenspace $E(3, T)$ is $(1, 1, 0)$. On transferring back to T, the eigenspace $E(3, T)$ is 1-dimensional with basis $(1 + x)$.

$\lambda_3 = 9$**:** The augmented matrix of the homogeneous system here is

$$\left(\begin{array}{ccc|c} 8 & -2 & -4 & 0 \\ 0 & 6 & -12 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence the eigenvectors of M_T corresponding to $\lambda_3 = 9$ all have the form $\text{col}(t, 2t, t) = t \times \text{col}(1, 2, 1)$ for nonzero t and so the **coordinate vector** of the basis vector of the eigenspace $E(9, T)$ is $(1, 2, 1)$. On transferring back to T, the eigenspace $E(9, T)$ is 1-dimensional with basis $(1 + 2x + x^2)$.

b. The algebraic multiplicity of each eigenvalue is equal to its geometric multiplicity and so T is diagonalisable. Take $B = (1,\ 1 + x,\ 1 + 2x + x^2)$. Then B is a basis of P_2 and $M(T; B) = \text{diag}(1, 3, 9)$. This can be verified directly. We have

$$\begin{aligned} T(1) &= 1 \\ T(1 + x) &= 1 + (3x + 2) = 3 + 3x = 3(1 + x) \\ T(1 + 2x + x^2) &= 1 + 2(3x + 2) + (3x + 2)^2 = 9 + 18x + 9x^2 \\ &= 9(1 + 2x + x^2). \end{aligned}$$

Hence

$$M(T; B) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{pmatrix} = \text{diag}(1, 3, 9)$$

as expected.

Return to Question 2.18 on P77

Solution 2.19

Consider the linear transformation S of $\mathbb{C}^2$ defined by

$$S((x, y)) = (4x + 2y,\ 3x - y)$$

for all $(x, y) \in \mathbb{C}^2$. Find the eigenvalues of S and decide whether S is diagonalisable.

The matrix of S w.r.t. the standard basis $((1,0),\ (0,1))$ is

$$M_S = \begin{pmatrix} 4 & 2 \\ 3 & -1 \end{pmatrix}.$$

Now we have

$$\begin{aligned} \det(\lambda I - M_S) &= \begin{vmatrix} \lambda - 4 & -2 \\ -3 & \lambda + 1 \end{vmatrix} \\ &= (\lambda - 4)(\lambda + 1) - 6 \\ &= \lambda^2 - 3\lambda - 10 \\ &= (\lambda - 5)(\lambda + 2) \end{aligned}$$

Hence the eigenvalues are the roots of this polynomial so we have the distinct eigenvalues $\lambda_1 = -2$ and $\lambda_2 = 5$, each with algebraic multiplicity 1.

Now we find an eigenvector of M_S corresponding to $\lambda_1 = -2$. We have the homogeneous system $(-2I - M_S)X = 0$ where $x = \text{col}(x, y)$ with augmented matrix

$$\left(\begin{array}{cc|c} -6 & -2 & 0 \\ -3 & -1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 3 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

Hence eigenvectors of M_S corresponding to $\lambda_1 = -2$ take the form $(t, -3t)$ for some nonzero $t \in \mathbb{C}$. It follows that a basis of $E(-2, S)$ is $((1, -3))$.

Next we find an eigenvector of M_S corresponding to $\lambda_2 = 5$. We have the homogeneous system $(5I - M_S)X = 0$ where $X = \text{col}(x, y)$ with augmented matrix

$$\left(\begin{array}{cc|c} 1 & -2 & 0 \\ -3 & 6 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & -2 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

Hence eigenvectors of M_S corresponding to $\lambda_2 = 5$ take the form $(2t, t)$ for nonzero

$t \in \mathbb{C}$. It follows that a basis of $E(5, S)$ is $((2, 1))$. Hence the geometric multiplicity of each eigenvalue of S is equal to its algebraic multiplicity and so S is diagonalisable. Take the basis $B = ((1, -3),\ (2, 1))$ of $\mathbb{C}^2$. Then the matrix of S w.r.t this basis is diagonal. Precisely, $M(S; B) = \text{diag}(-2, 5).\}$

Return to Question 2.19 on P78

Solution 2.20

Consider the linear transformation T of $\mathbb{C}^2$ defined by

$$T((x, y)) = (10x - 9y,\ 4x - 2y)$$

for all $(x, y) \in \mathbb{C}^2$. Find the eigenvalues of T and decide whether T is diagonalisable.

The matrix of T w.r.t. the standard basis $((1, 0),\ (0, 1))$ of $\mathbb{C}^2$ is

$$M_T = \begin{pmatrix} 10 & -9 \\ 4 & -2 \end{pmatrix}$$

Now we have

$$\begin{aligned} \det(\lambda I - M_T) &= \begin{vmatrix} \lambda - 10 & 9 \\ -4 & \lambda + 2 \end{vmatrix} \\ &= (\lambda - 10)(\lambda + 2) + 36 \\ &= \lambda^2 - 8\lambda + 16 \\ &= (\lambda - 4)^2. \end{aligned}$$

The eigenvalues of M_T are the roots of this polynomial and so we have the repeated eigenvalues $\lambda_1 = \lambda_2 = 4$. The algebraic multiplicity of 4 as an eigenvalue is 2.

Now we find corresponding eigenvectors. We consider the homogeneous system

$$(4I - M_T)X = 0$$

where $X = \text{col}(x, y)$ with augmented matrix

$$\left(\begin{array}{cc|c} -6 & 9 & 0 \\ -4 & 6 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} -2 & 3 & 0 \\ 0 & 0 & 0 \end{array}\right).$$

Hence eigenvectors of M_T corresponding to the eigenvalue 4 take the form $(3t, 2t)$ for nonzero $t \in \mathbb{C}$ and so a basis of $E(4, T)$ is $((3, 2))$. The geometric multiplicity of 4 as an eigenvalue is therefore $\dim(E(4, T)) = 1$ which is not equal to the algebraic multiplicity of 4 as an eigenvalue and so it follows that T is not diagonalisable.

Return to Question 2.20 on P78

Solution 2.21

Consider the linear transformation S of $\mathbb{C}^3$ defined by

$$S((x, y, z)) = (3x - 2z,\ y,\ x).$$

for all $(x, y, z) \in \mathbb{C}^3$. Given that $\chi_S(t) = (t-1)^2(t-2)$, find bases of the relevant eigenspaces. Is S diagonalisable?

We have the three eigenvalues $\lambda_1 = \lambda_2 = 1$ and $\lambda_3 = 2$. The important idea here is to find the geometric multiplicity of 1 as an eigenvalue. We have

$$\begin{aligned} (x, y, z) \in E(1, S) &\Leftrightarrow S((x, y, z)) = (x, y, z) \\ &\Leftrightarrow (3x - 2z,\ y,\ x) = (x, y, z) \\ &\Leftrightarrow x = z. \end{aligned}$$

Hence eigenvectors of S corresponding to the eigenvalue 1 take the form $(t, s, t) = t(1, 0, 1) + s(0, 1, 0)$ for nonzero $s, t \in \mathbb{C}$. It follows that a basis of $E(1, S)$ is $((1, 0, 1),\ (0, 1, 0))$ and so the geometric multiplicity of 1 as an eigenvalue of S is equal to its algebraic multiplicity. Hence S is diagonalisable. Now

$$\begin{aligned}(x, y, z) \in E(2, S) &\Leftrightarrow S((x, y, z)) = 2(x, y, z)\\ &\Leftrightarrow (3x - 2z,\ y,\ x) = (2x,\ 2y,\ 2z)\\ &\Leftrightarrow x = 2z,\ y = 0.\end{aligned}$$

Hence eigenvectors of S corresponding to the eigenvalue 1 take the form $(2t, 0, t) = t(2, 0, 1)$ for nonzero $t \in \mathbb{C}$ and so $((2, 0, 1))$ is a basis of the eigenspace $E(2, S)$. Take $B = ((1, 0, 1),\ (0, 1, 0),\ (2, 0, 1))$. Then B is a basis of $\mathbb{C}^3$ and $M(S; B) = \mathrm{diag}(1, 1, 2)$.

Return to Question 2.21 on P78

A.3 Chapter 3 solutions

Solution 3.1

Let R be a ring. The centre of R is defined as

$$Z(R) = \{a \in R : ab = ba \quad \textbf{for all} \quad b \in R\}.$$

Prove that $Z(R)$ is a subring of R.

We have

$$1_R b = b 1_R = b$$

for all $b \in R$ and so $1_R \in Z(R)$ and $Z(R) \neq \phi$.

Now let $x, y \in Z(R)$. Then $xa = ax$ and $ya = ay$ for all $a \in R$. Hence

$$(x - y)a = xa - ya = ax - ay = a(x - y)$$

and so $x - y \in Z(R)$.

Finally we have

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

and so $xy \in Z(R)$ and $Z(R)$ is a subring of R.

Return to Question 3.1 on P113

Solution 3.2

Let R be a ring. Prove that if $a \in R$ is a unit then its inverse is unique.

Let $a \in R$ be a unit and assume that $b, c \in R$ are both inverses of a. Then $ab = ba = 1_R$ and $ac = ca = 1_R$. Hence

$$b = b1_R = b(ac) = (ba)c = 1_R c = c.$$

Return to Question 3.2 on P113

Solution 3.3

A ring R is called *Boolean* if every element of R is idempotent (i.e. for all $x \in R$, $x^2 = x$)

a. Show that if R is Boolean then any nonzero element $x \in R$ has period two in the group $(R, +)$.

b. Show that any Boolean ring is necessarily commutative.

a. We have

$$\begin{aligned} 2x = x + x = (x+x)^2 \\ &= x^2 + 2x + x^2 \\ &= x + 2x + x \\ &= 4x. \end{aligned}$$

Hence $2x = 0$ i.e. $x + x = 0$ and x has order 2 in $(R, +)$.

b. Let $x, y \in R$. We have

$$\begin{aligned} x + y = (x+y)^2 &= x^2 + xy + yx + y^2 \\ &= x + xy + yx + y. \end{aligned}$$

Hence $xy + yx = 0 \Rightarrow xy = -yx = yx$ by part (a). It follows that R is commutative.

Return to Question 3.3 on P113

Solution 3.4

Let

$$S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

Prove that S is a subring of $M_2(\mathbb{R})$.

[Note that the S and $M_2(\mathbb{R})$ each have identity elements but they are not the same]

The element $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ acts as an identity element in S as, for all $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in S$

we have

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

Now let $A = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} \in S$. Then

$$A - B = \begin{pmatrix} x-y & 0 \\ 0 & 0 \end{pmatrix} \in S$$

and

$$AB = \begin{pmatrix} xy & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Hence S is a subring of $M_2(\mathbb{R})$.

Return to Question 3.4 on P114

Solution 3.5

Let R be a ring. Show that, for a positive integer n, the ring $M_n(R)$ of $n \times n$ matrices over R is commutative if and only if $R = \{0\}$, or $n = 1$ and R is commutative.

$M_n(\{0\})$ is clearly commutative and $M_1(R)$ is essentially the same as R so is commutative if R is commutative.

Now assume that $M_n(R)$ is commutative and that $R \neq \{0\}$. Let E_{ik} be the $n \times n$ matrix whose entries are all zero except for the (i, k)th entry which is 1. Then $E_{nn} = E_{n1}E_{1n} = E_{1n}E_{n1} = E_{11}$. So $n = 1$ as $M_1(R)$ is essentially the same as R, R must be commutative.

Return to Question 3.5 on P114

Solution 3.6

Let D be an integral domain.

a. ***Show that, for all $x \in D$,***

$$x^2 = 1 \Rightarrow x = 1 \textbf{ or } x = -1.$$

b. ***Deduce that if D contains only finitely many units then the product of these units equals -1.***

c. ***Finally show that, for every prime integer p,***

$$(p-1)! \equiv -1 \pmod{p}.$$

This is Wilson's Theorem.

a. $x^2 = 1 \Rightarrow x^2 - 1 = 0 \Rightarrow (x-1)(x+1) = 0$. Now D is an integral domain and hence we must have $x - 1 = 0$ or $x + 1 = 0$ i.e. $x = 1$ or $x = -1$.

b. We note that part a. gives us the result that, if an element in D is self-inverse then it is ± 1. Hence all other units in D must come in distinct pairs (a_i, a_i^{-1}) $(i = 1, 2, ..., t)$ say with $a_i \neq a_i^{-1}$. (Recall that if a_i is a unit in D then a_i^{-1} is also a unit in D with $(a_i^{-1})^{-1} = a_i$) Now the finite product of the units in D is

$$1 \times (-1) \times \prod_{i=1,2,...,t} a_i a_i^{-1} = -1 \times 1 = -1.$$

c. For the final part, take $D = \mathbb{Z}_p$. (set of congruence classes mod p) Apply the the result of part (b)

Then $\mathbb{Z}_p$ is a field and hence every nonzero element is a unit. These are the elements $\{1, 2, ..., p-1\}$. Hence the product of these is -1 in $\mathbb{Z}_p$. i.e.

$$(p-1) \times (p-2) \times ... \times 2 \times 1 \equiv -1 (\text{mod } p) \Rightarrow (p-1)! \equiv -1 (\text{mod } p)$$

Return to Question 3.6 on P114

Solution 3.7

Let R be a commutative ring. Show that

$$Z(M_n(R)) = \{aI_n : a \in R\}.$$

[For the trickier $\subseteq$ containment, it might be useful to consider the matrix unit which is the matrix $E_{ik} \in M_n(R)$ where the (i,k)th entry of E_{ik} is the integer 1 and all other entries are zero. Then any $A = (a_{ik}) \in M_n(R)$ can be written as $A = \sum_{i,k=1}^{n} a_{ik}E_{ik}$.]

Let $X \in M_n(R)$ and $a \in R$. Then

$$X(aI_n) = a(XI_n) = aX = a(I_nX) = (aI_n)X.$$

So $aI_n \in Z(M_n(R))$.

Now let $A \in Z(M_n(R))$. Then $A = \sum_{i,k=1}^{n} a_{ik}E_{ik}$ where $a_{ik} \in R$ and E_{ik} is the matrix unit. For $p, q = 1, ..., n$ we have

$$E_{qp}A = AE_{qp}$$

i.e.

$$E_{qp}\sum_{i,k=1}^{n} a_{ik}E_{ik} = \sum_{i,k=1}^{n} a_{ik}E_{ik}E_{qp}$$

i.e.

$$\sum_{k=1}^{n} a_{pk}E_{qk} = \sum_{i=1}^{n} a_{iq}E_{ip}.$$

i.e. $a_{pp} = a_{qq}$, $a_{pk} = 0 (p \neq k)$, $a_{iq} \neq 0 (i \neq q)$ $(i, k = 1, 2, ..., n)$.

Hence $A = aI_n$ for some $a \in R$. Hence $Z(M_n(R)) = \{aI_n : a \in R\}$.

Return to Question 3.7 on P115

Solution 3.8

Let R be a commutative ring and let $a \in R$. Show that the set

$$I = \{x \in R : xa = 0\}$$

is an ideal of R. (This ideal is sometimes called the *annihilator* of $a \in R$)

We have $0_R a = 0_R$ and so $0_R \in I$.

Now let $x, y \in I$. Then $xa = ya = 0$. Hence $(x - y)a = xa - ya = 0 - 0 = 0$. So $x - y \in I$.

Finally let $x \in I$ and $r \in R$. Then we have

$$(rx)a = r(xa) = r0 = 0.$$

and (using the fact that R is commutative)

$$(xr)a = (rx)a = r(xa) = r0 = 0.$$

Hence $rx, xr \in I$ and I is an ideal of R.

Return to Question 3.8 on P115

Solution 3.9

Let R be the set of all matrices of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

over $\mathbb{Q}$ such that $a = d$ and $b = 0$. Let I be the subset of R such that $a = d = 0$. Show that

$$R/I \cong \mathbb{Q}.$$

[Hint : think about defining a homomorphism...]

Define a mapping

$$\theta : R \longrightarrow \mathbb{Q}$$

given by

$$\theta\left(\begin{pmatrix} a & 0 \\ c & a \end{pmatrix}\right) := a.$$

Then if $A = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix}$, $B = \begin{pmatrix} x & 0 \\ y & x \end{pmatrix} \in R$, we have

$$\theta(A+B) = \theta\left(\begin{pmatrix} a+x & 0 \\ c+y & a+x \end{pmatrix}\right) = a+x = \theta(A) + \theta(B)$$

and

$$\theta(AB) = \theta\left(\begin{pmatrix} ax & 0 \\ cx+ay & ax \end{pmatrix}\right) = ax = \theta(A)\theta(B).$$

It follows that θ is a ring homomorphism and

$$\begin{aligned} \ker(\theta) &= \left\{A = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \in R : \theta(A) = 0\right\} \\ &= \left\{A \in R : a = 0\right\} \\ &= \left\{\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} : c \in \mathbb{Q}\right\} \\ &= I. \end{aligned}$$

Additionally we have $\text{im}(\theta) = \mathbb{Q}$. By the First Isomorphism Theorem for rings,

$$R/I \cong \mathbb{Q}.$$

Return to Question 3.9 on P116

Solution 3.10

Let R be a ring and let $J \trianglelefteq R$. Show that R/J is commutative if and only if $xy - yx \in J$ for all $x, y \in R$.

Deduce that, if $K_1, K_2 \trianglelefteq R$ and both R/K_1 and R/K_2 are commutative, then $R/(K_1 \cap K_2)$ is also commutative.

Let $x + J, y + J \in R/J$. Then R/J is commutative iff $(x + J)(y + J) = (y + J)(x + J)$ i.e. iff $xy + J = yx + J$ i.e iff $xy - yx \in J$.

For the second part, let $x, y \in R$. Since R/K_1 is commutative, $xy-yx \in K_1$. Since R/K_2 is commutative, we also have $xy - yx \in K_2$ and hence $xy - yx \in K_1 \cap K_2$. Hence, since $x, y \in R$ were arbitrary, $R/(K_1 \cap K_2)$ is commutative.

Return to Question 3.10 on P116

Solution 3.11

Let D be an integral domain and let $0 \neq I, J \trianglelefteq D$. Show that $I \cap J \neq 0$.

Let $0 \neq a \in I$ and $0 \neq b \in J$. (This is possible since each of the ideals are nonzero) Then $ab \in I$ (since $I \trianglelefteq R$) but also $ab \in J$. (since $J \trianglelefteq R$) Hence $ab \in I \cap J$. But also, since R is an integral domain, we have $ab \neq 0$. Hence $0 \neq ab \in I \cap J$ and so $I \cap J \neq 0$.

Return to Question 3.11 on P116

A.4 Chapter 4 solutions

Solution 4.1

Let R be a ring. Prove that the ideals of the ring $M_n(R)$ are the subsets of the form $M_n(Q)$ where $Q \trianglelefteq R$.

Clearly for an ideal Q of R, $M_n(Q)$ is an ideal of R. This follows since for $B = (b_{ik}) \in M_n(Q)$ and $A = (a_{ik})$ in R, AB and BA are both elements of $M_n(Q)$. For instance for $1 \leq i, j \leq n$, the ik^{th} entry of AB is

$$\sum_{l=1}^{n} a_{il} b_{lk}$$

now $A_{il}B_{lj} \in Q$ for all $1 \leq l \leq n$, and as Q is a subring of R we have that $(AB)_{ij} \in Q$. A similar argument holds for BA.

Let I be an ideal of $M_n(R)$. Set

$$Q := \{a_{11} : A \in I\}.$$

We first demonstrate that $M_n(Q) = I$. Then we show it is an ideal of R.

For $1 \leq a, b \leq n$ let E_{ab} be the matrix with entry 1_R in position ab and zero every where else. For $1 \leq i, j \leq n$ we write $(E_{ab})_{ij}$ for the ij^{th} entry of E_{ab}.

Let $A = (a_{ij}) \in I$ be arbitrary. Fix $1 \leq i \leq k$. We show that the matrix $a_{ik}E_{11}$ is an element of I.

Consider the product the pq$^{\text{th}}$ entry of the product $E_{ki}AE_{kk}$

$$\sum_{l=1}^{n} \left(\sum_{m=1}^{n} (E_{ki})_{pm} a_{ml} \right) (E_{kk})_{lq}.$$

Since $(E_{ki})_{ab} = 0_R$ unless $a = k$ and $b = i$ and $(E_{kk})_{ab} = 0_R$ unless $a = k$ and $b = k$, the pq^{th} entry of the product $E_{ki}AE_{ki}$ is zero whenever $(p, q) \neq (k, k)$. If

$p = k$ and $q = k$, then the kk$^{\text{th}}$ entry of $E_{ki}AE_{kk}$ is

$$\sum_{l=1}^{n}\left(\sum_{m=1}^{n}(E_{ki})_{km}a_{ml}\right)(E_{kk})_{lk} = \sum_{l=1}^{n}a_{il}(E_{kk})_{lk} = a_{ik}.$$

Therefore

$$E_{ik}AE_{kk} = a_{ik}E_{kk} \in I.$$

Now observe that

$$E_{11} = E_{1k}E_{kk}E_{k1}.$$

Therefore

$$a_{ik}E_{11} = E_{1k}a_{ik}E_{kk}E_{k1}$$

is an element of I. It follows that $a_{ik} \in Q$.

Since $A \in I$ was arbitrarily chosen, we deduce $I = M_n(Q)$. That Q is an ideal of R. Follows from the fact that I is an ideal of R and for $a, b \in R$, $aE_{11} + bE_{11} = (a+b)E_{11}$ and $aE_{11}bE_{11} = (ab)E_{11}$.

Return to Question 4.1 on P128

Solution 4.2

Let R be a PID and $a, b \in R$ be both nonzero. Show that there is a $c \in R$ such that

- **a.** $a|c$ ***and*** $b|c$***;***
- **b.** ***If*** $a \mid d$ ***and*** $b \mid d$ ***then*** $c \mid d$***.***

Let $c \in R$ be such that $aR \cap bR$. Such a c exists because $aR \cap bR$ is an ideal of R and R is a PID.

a. Note that $cR \subseteq aR$ and $cR \subseteq bR$. It follows that $a|c$ and $b|c$.

b. By Lemma 3.12 $cR = aR \cap bR$ is the largest ideal of R that is contained in both aR and bR. Now since $a|d$, and $b|d$, then, then $dR \subseteq aR$ and $dR \subseteq bR$. It follows that dR is contained in cR and so $c|d$.

Return to Question 4.2 on P128

Solution 4.3

Let R be a commutative ring and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ be a chain of proper ideals of R. Prove that

$$I = \bigcup_{i=1}^{\infty} I_i$$

is a proper ideal of R.

We need to demonstrate two things. Firstly, that $I \subsetneq R$ and secondly that I is an ideal of R.

If $I = R$, then $1_R \in I$. This means that $1_R \in I_i$ for some i. However, this forces $I_i = R$ and so I_i would not be a proper ideal of R — a contradiction. Therefore I is a proper subset of R.

We now demonstrate that I is an ideal.

Clearly I is non-empty.

Let $a, b \in I$ and $r \in R$. There is an $i \in \mathbb{N}$ such that $a, b \in I_i$ it follows that $a+b \in I_i$ and $rb, br \in I_i$. We conclude that I is closed under addition is an ideal of R.

Return to Question 4.3 on P129

Solution 4.4

Let R be a PID show that there is not an infinite sequence of ideals $J_1, J_2, J_3, ...$ such that $J_n \subsetneq J_{n+1}$ for all $n \in N$.

Using Question 4.3 we know that $J = \cup_{i=1}^{\infty} J_i$ is a proper ideal of R. It follows, as

R is a PID, that $J = aR$ for some $a \in R$. Now, as $a \in J$, there is some i, such that $a \in J_i$ and so $aI = J \subseteq J_i \subseteq J$. We then we conclude that $J_i = J_{i+1}$ ... which contradicts the fact that $J_i \subsetneq J_{i+1}$.

Return to Question 4.4 on P129

Solution 4.5

Let R be a PID, prove that R is a UFD.

We need to demonstrate two things. Firstly that R is a factorisation domain and secondly that it is a unique factorisation domain.

Let $r \in R$ be an arbitrary nonzero non-unit element. Suppose for a contradiction that r cannot be written as a finite product of irreducible elements of R. Note that r cannot be irreducible as a consequence of this. Therefore there are nonzero non-unit elements $r_1 s_1 \in R$ such that $r = r_1 s_1$. Now if both r_1 and s_1 can be written as a finite product of irreducible elements of R, then so can r. Therefore one of r_1 or s_1 is not a product of irreducible elements of R. Without loss of generality (since R is a commutative ring) we may assume that r_1 is not a product of irreducibles. Notice that $rR \subsetneq r_1 R$. Since if $rR = r_1 R$, then there is an $a \in R$ such that $r_1 = ar = r_1 a s_1$. This now means, since R is a PID, that $as_1 = 1_R$ and s_1 is a unit — a contradiction.

We may thus repeat the argument above with r_1 in place of r. Inductively, we see that for any $n \in N$, there is a sequence $r = r_0, r_1, r_2, \dots, r_n$ of non-irreducible, nonzero, non-unit, elements of R such that $r_i \,|\, r_{i-1}$ and $r_{i-1} R \subsetneq r_i R$.. This gives rise to a sequence of ideals $r_0 R \subsetneq r_1 R \subsetneq r_2 R \subsetneq \dots$.

However, using Question 4.4, it must be the case, as R is a PID, that there is an i such that $r_i R = r_{i+1} R$. This yields the desired contradiction. We conclude that r can be written as a finite product of irreducible elements of R.

We now argue that R is a unique factorisation domain. We do so by induction on the length of the smallest factorisation into irreducibles.

We establish the base case. This occurs for elements which can be written as a product of a single irreducible elements — i.e for irreducible elements of R.

Let r be an irreducible element of R. Suppose there are irreducible elements $x_1, x_2, \dots, x_k \in R$ such that $r = x_1 x_2 \dots x_k$. Since R is a PID then every irreducible element of R is prime. Now, as $r \,|\, (x_1 x_2 \dots x_k)$ and r is prime, then $r|x_i$ for some i. Without loss of generality (since R is commutative) we may assume that $i = 1$. Thus, $x_1 = ru$ for some unit $u \in R$ (u must be a unit since both x_1 and r are irreducible). It follows that

$$r - x_1 x_2 \dots x_k = r(1_R - u x_2 \dots x_k).$$

Thus, $1_R = u x_2 \dots x_k$ since r is irreducible. If $k > 1$, then x_i is a unit for all $2 \leq i \leq k$ since $x_i u x_2 \dots x_{i-1} x_{i+1} \dots x_k = 1_R$. However, this contradicts the fact that x_i, for $2 \leq i \leq k$ is irreducible. Therefore, we conclude that $k = 1$ and r can be expressed in an essentially unique way as a product of irreducibles (since x_1 is associated to r).

Assume by induction that any nonzero non-unit element of R which can be expressed as a product of n irreducible elements of R has an essentially unique factorisation as a product of irreducible elements of R.

Let $r \in R$ be a nonzero non-unit element. Suppose there are irreducibles $x_1, x_2, \dots x_{n+1}, x_{n+1}, y_1, y_2, \dots, y_s \in R$ such that $r = x_1, x_2, \dots x_{n+1}, x_{n+1} = y_1, y_2, \dots, y_s$. Now since x_1 is irreducible, it is prime, so as in the base case, we may assume, without loss of generality that $y_1 = x_1 u$ for a unit $u \in R$. Thus $r = x_1 x_2 \dots x_{n+1} = x_1 u y_2 \dots y_s$. Using the fact that R is an integral domain and x_1 is irreducible we conclude that $r' = x_2 \dots x_{n+1} = y_2' y_3 \dots y_s$, where $y_2' = u y_2$.

We may now apply the induction hypothesis to conclude that $s = n + 1$ and x_i is associated to y_i for all $3 \leq i \leq n + 1$ and x_2 is associated to y_2 (since x_2 is associated to y_2' which is associated to y_2) . Now, since x_1 is associated to y_1, it follows that x_i is associated to y_i for all $1 \leq i \leq n + 1$. We conclude that r has an essentially unique factorisation into irreducibles.

The result now follows by induction.

Return to Question 4.5 on P129

Solution 4.6

Let $\mathcal{F}$ be a field. Show that $\mathcal{F}[x]$ is a principal ideal domain.

[You may use the fact that given $f, g \in \mathcal{F}[x]$, there exist unique $q, r \in \mathcal{F}[x]$ such that $f = qg + r$ and either $r = 0$ or the degree of r is strictly less than the degree of G.]

Let I be any ideal of $\mathcal{F}[x]$. Let $a \in I$ be an element with the smallest degree in I. We note that a exists. Let f be any other element of I. Then using the hint, there are $q, r \in \mathcal{F}[x]$ such that $f = qa + r$ and either $r = 0$ or the degree of r is strictly less than the degree of a. Since a has the smallest degree in I, and $r = f - qa \in I$ (since $a, f \in I$), it follows that $r = 0$ and $f = qa$. We conclude, as $f \in I$ was chosen arbitrarily, that $I = a\mathcal{F}[x]$.

Return to Question 4.6 on P129

Solution 4.7

Consider the ring $R = \mathbb{Q}[x]$.

- ***i. Show that $x^5 - 7$ is a prime.***
- ***ii. Let $I = (x^5 - 7)R$. Show that R/I is a field.***

i. Since R is a PID (by Question 4.6) it suffices to show that $x^5 - 7$ is irreducible.

First observe that by De Moivre's Theorem, we may write

$$x^5 - 7 = \prod_{i=0}^{4} x - |7|^{\frac{1}{5}} \left(\exp^{i\frac{2i\pi}{5}}\right).$$

Set $p_i(x) = x - |7|^{\frac{1}{5}} \left(\exp^{i\frac{2i\pi}{5}}\right)$ for $0 \leq i \leq 4$. Suppose $f(x), g(x) \in \mathbb{Q}[x]$ are such that $x^5 - 7 = f(x)g(x)$. Then the sum of the degrees of $f(x)$ and $g(x)$ must be equal to 5 and $f(x)$ and $g(x)$ can both be expressed as products of the $p_i(x)$'s.

If one of $f(x)$ and $g(x)$ has degree 4, then the other must be equal to $p_i(x)$ for some i. However, $p_i(x)$ is not an element of $\mathbb{Q}[x]$ for any i. So this is not possible.

If one of $f(x)$ and $g(x)$ has degree 3, then the other has degree 2 and is a product $p_i(x)p_j(x)$ for $0 \leq i, j \leq 4$ and $i \neq j$. However, notice that $|p_i(0)p_j(0)| = |7|^{2/5} \notin \mathbb{Q}$. Therefore $p_i(x)p_j(x) \notin \mathbb{Q}[x]$ for any distinct i and j. Therefore, this is not a possibility either.

It follows that if $x^5 - 7 = f(x)g(x)$, then one of $f(x)$ and $g(x)$ has degree 5 and the other is therefore a unit. We conclude that $x^5 - 7$ is an irreducible, and so prime, element of $\mathbb{Q}[x]$.

ii. Since $\mathbb{Q}[x]$ is a PID and $(x^5 - 7)$ is irreducible then $I = (x^5 - 7)\mathbb{Q}[x]$ is a maximal ideal of $\mathbb{Q}[x]$. It then follows that $\mathbb{Q}[x]/I$ is a field.

Return to Question 4.7 on P130

Solution 4.8

Consider the guassian integers $\mathbb{Z}[i]$***. Let*** $\alpha = 10 + 11i$ ***and*** $\beta = 8 + i$***. Find*** $\gamma \in \mathbb{Z}[i]$ ***such that*** $\gamma\mathbb{Z}[i] = \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$.

Notice that since $\mathbb{Z}[i]$ is a PID, then there is a $\gamma \in \mathbb{Z}[i]$ such that $\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i] = \gamma\mathbb{Z}[i]$.

Let $\gamma \in \mathbb{Z}[i]$ be such that $\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i] = \gamma\mathbb{Z}[i]$. Since, $\alpha, \beta \in \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$, it follows that γ divides both α and β.

If $\gamma \in \mathbb{Z}[i]$ divides both α and β, then $|\gamma|^2$ divides $|\alpha|^2$ and $|\beta|^2$. Thus, $|\gamma|^2$ divides both 221 and 65. It follows that $|\gamma|^2$ is either 1 or 13.

We first try $|\gamma|^2 = 13$. Set $\gamma = a + ib$, then $a^2 + b^2 = 13$. Solving for $a, b \in \mathbb{Z}$ then gives $(a, b) \in \{(\pm 2, \pm 3), (\pm 3, \pm 2)\}$. Notice that $-i(a + ib) = (b - ia)$ and $i(a - ib) = (b + ia)$. Since the units of $\mathbb{Z}[i]$ are precisely $\{\pm 1, \pm i\}$, and $\gamma\mathbb{Z}[i] = (\gamma t)\mathbb{Z}[i]$ for any unit t, we only need consider the possibilities $\gamma = z$ and $\gamma = \bar{z}$ for $z = 3 + 2i$.

Now observe that if $z = 3 + 2i$ divides both α and β, then $\bar{z}$ does not divide both α and β. This follows since if there are $u, v \in \mathbb{Z}[i]$ such that $\alpha = zu = \overline{z}v$, then $|u| = |v|$ (since $|z| = |\bar{z}|$). Thus either $\bar{u} = v$ (in which case $\bar{\alpha} = \overline{zu} = \bar{z}v = \alpha$ which is a contradiction) or $u = vt$ for a unit t of $\mathbb{Z}[i]$ (in this case, since $\mathbb{Z}[i]$ is a PID, we conclude that $z = \overline{z}t$, but there is a no unit $t \in \mathbb{Z}[i]$ such that $z = \overline{z}t$.) Thus either exactly one of z and $\bar{z}$ divides both α and β or neither z nor $\bar{z}$ divides α and β.

We check first if z divides both α and β. Let $c + di, e + fi \in \mathbb{Z}[i]$ be such that $(3 + 2i)(c + di) = 10 + 11i$ and $(3 + 2i)(e + fi) = 8 + i$. We have

$$\begin{aligned} 3c - 2d &= 10 \\ 2c + 3d &= 11 \end{aligned} \qquad\qquad \begin{aligned} 3e - 2f &= 8 \\ 2e + 3f &= 1 \end{aligned}$$

Solving both of these simultaneous equations gives $c = 4, d = 1$ and $e = 2, f = -1$. Therefore z divides both α and β. It follows that $\bar{z}$ does not divide both α and β.

We conclude that $(\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]) = (3 + 2i)\mathbb{Z}[i]$ since any non-unit element of $\mathbb{Z}[i]$ which divides both α and β must be equal to $(3 + 2i)t$ for a unit t of $\mathbb{Z}[i]$.

Return to Question 4.8 on P130